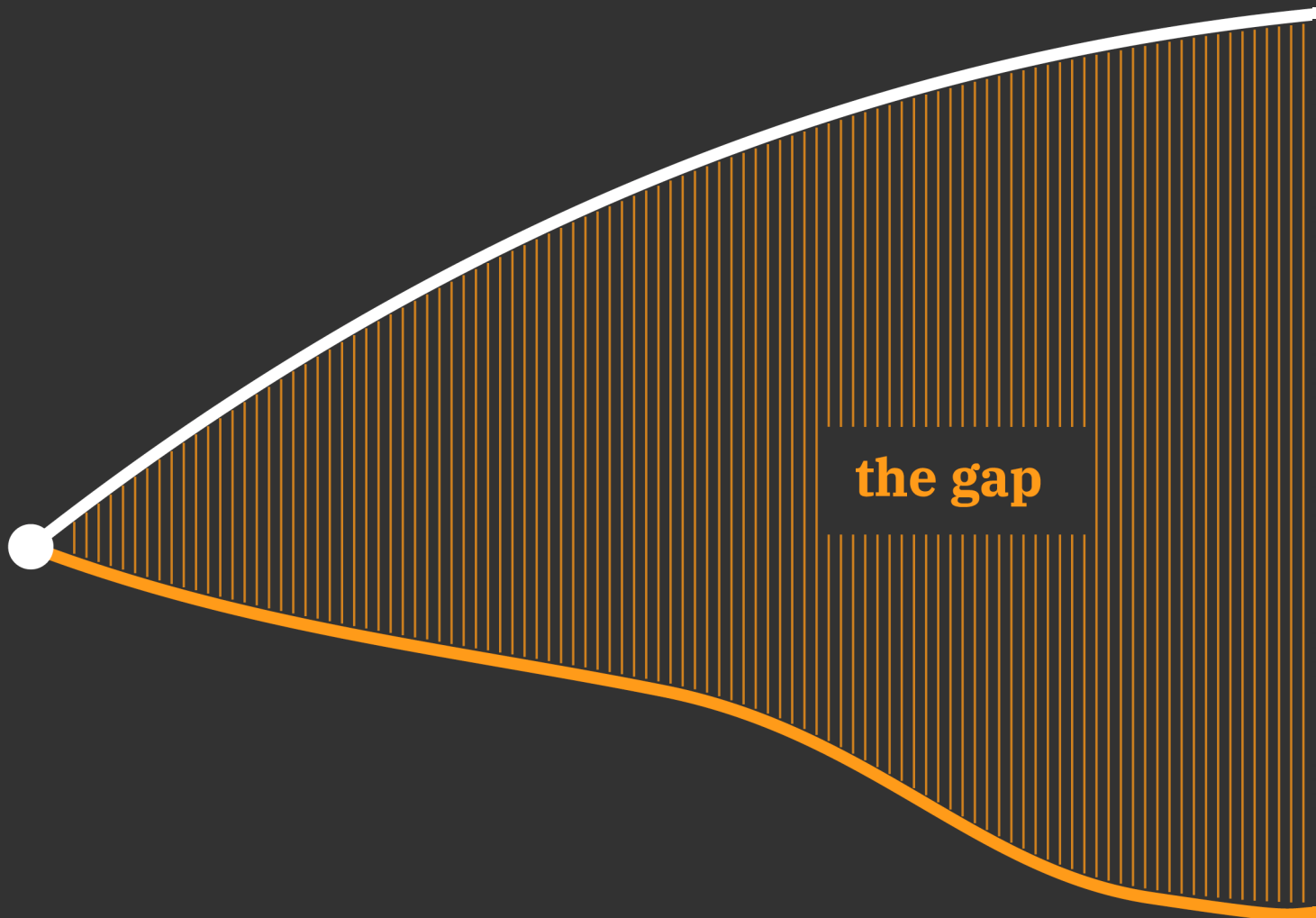


Oh, Behave!

Full report

The Annual Cybersecurity
Attitudes and Behaviors
Report **2026-2027**

WHAT WE SAY



WHAT WE DO

Contents

MORE BS* THAN A RÉSUMÉ WRITTEN BY CHATGPT	4	2. Reliance and responsibility (AKA teamwork and who the buck stops with)	39
Optimism in the air, chaos in the feeds	4	2.1 Calling for backup: Who's helping who?	39
So, what's the vibe in '26?	4	2.2 Who's on the hook? Personal vs. office data	42
Strong egos, sticky notes	5	3. Cybercrime victimization & reporting	45
Oversharing with the bots	5	3.1 Attitudes toward victimization: Panic, paralysis, or peace of mind?	46
People. Even messier than your browser tabs	5	3.2 Cybercrime in the wild: How bad is it really?	50
REPORT AIM & STRUCTURE	6	3.3 Cybercrime reporting: Who speaks up, who stays silent, and why?	59
KEY TERMS	8	3.4 Cyberbullying: The digital shadow	63
EXECUTIVE SUMMARY	12	4. Cybersecurity training: The good, the bad, and the ignored	66
Critical takeaways	12	4.1 Who's getting trained (and who's left behind)	66
The 'bot'-tom line on artificial intelligence (AI)	13	4.2 Barriers to attendance (why people skip out)	71
Safe and sound, or just stressed out? Attitudes, beliefs & perceptions about online security	15	4.3 Preferred format – how people want to learn	72
Scam-o-rama: When bad clicks happen to good people. Cybercrime victimization & reporting	17	4.4 The final showdown: What impact did training have?	75
School of hard hacks: Who's getting taught? Cybersecurity training	19	5. Cybersecurity behaviors	78
Lock it down or just sticky-note it? Cybersecurity behaviors	20	5.1 If your name's not down, you're not coming in: Authentication in the real world	80
MAIN FINDINGS (WHAT WE REELED IN)	24	5.1.1 Making the cut: How we build our passwords (and pet names)	80
1. Attitudes, beliefs & perceptions about online security	25	5.1.2 Password management: The great notebook revival	84
1.1 The personal security vibe check	26	5.1.3 MFA: Security need or total nuisance?	87
1.2 Misconceptions and concerns (tech myths and big brother fears)	31	5.1.4 Beyond passwords: Biometrics & passkeys	92
1.3 The 9-to-5 security tightrope: Cybersecurity culture in the workplace	34		
1.4 Doomscrolling and media hype	36		

5.2 Snooze or software patch? How we handle Update Available pop-ups	96	APPENDIX B: COUNTRY COMPARISONS	149
5.3 Back it up, pack it in: Backing up data	99	Attitudes, beliefs & perceptions about online security	149
5.4 Catch me if you can: Recognizing & reporting phishing messages	100	Cybercrime victimization	156
5.4.1 Spotting the bait: How good are we at catching phishes?	101	Cybersecurity training	164
5.4.2 Sounding the alarm: Reporting phishing messages	106	Cybersecurity behaviors	169
6. Artificial intelligence (AI) – the bot next door	110	AI	175
6.1 The bot takeover (because everyone and their grandma is prompting now)	110	ABOUT	181
6.2 AI at work: Ninja productivity tool or corporate risk?	116	National Cybersecurity Alliance	181
6.3 Bot or not? Our (unwarranted?) confidence in spotting AI creations	122	CybSafe	181
6.4 Brains, bots and benefits: Public attitudes and AI anxieties	126	Carnegie Mellon University and CyLab	181
CONCLUSION	135	Authors	182
AI is officially a coworker. Time to teach it some manners	135	Expert contributors	182
Know your audience (or watch them hit ‘skip’)	136	Acknowledgments	182
Knowledge ≠ behavior (or why smart people use not-so-smart passwords)	137		
Privacy fatalism persists. AKA: ‘I’m getting hacked anyway, so why bother?’	138		
Too cool for cyber school: The Gen Z & Millennial paradox	139		
APPENDIX A: METHODOLOGY	141		
Survey design	141		
Procedure	142		
Sample	143		
Data quality	147		
Data analysis	147		
AI disclosure	147		

More **BS*** than a résumé written by ChatGPT

**Welcome to the 2026-2027 Annual
Cybersecurity Attitudes and
Behaviors Report.**

**Or, as it's known in this neck of the
woods, *Oh, Behave!***

Optimism in the air, chaos in the feeds

If last year was about asking whether we should trust the tech, 2026 is the year we realized human behavior remains the ultimate wildcard.

The overall vibe? Cautiously optimistic, but still pretty chaotic if we're honest (which, luckily for you, we are). A staggering 83% of people say digital security is a top priority, and 70% believe staying safe is completely achievable. But beneath that sunny exterior, the cracks are well and truly showing (relatable).

Half of us still naively assume our devices just protect themselves, a third think data privacy is a lost cause, and distrust runs so deep that people fear their own government snooping on their apps just as much as a foreign power. Yikes.

In short: the spirit is willing, but the
(digital) flesh is weak.

**Behavioral science, of course.*

So, what's the vibe in '26?

To build this year's picture, we surveyed 5,000 adults across five global hubs: the United States, the United Kingdom, India, Brazil, and Singapore.

We then looked at the numbers through the lenses of age and employment, to pinpoint where the real vulnerabilities lie. And this year (plot spoiler) the generational contrasts are wilder than ever:

- **The Millennial paradox:** Millennials are the ultimate power users, feeling the most in control (66%) and the most confident in recognizing AI-generated content and most types of phishing. Yet they're also the most overwhelmed by information overload (54%), the most paranoid about government data misuse (62%), and the most likely to view their own coworkers as a walking security hazard (53%).
- **The Gen Z opt-out:** Gen Z have the highest rate of personal cybercrime victimization (64%), yet when offered workplace security training, they're the single most likely generation to skip it entirely (21%).
- **The silent lone rangers:** Older generations remain notably isolated from digital support systems. Baby Boomers and the Silent Generation are the least likely to ask for cybersecurity help, and the least likely to be asked. ...The Silent Gen really living up to their name there.

Strong egos, sticky notes

The defining theme of 2026 is the stubborn persistence of the knowing/doing gap. People know the rules, but convenience wins (nearly) every time.

Case in point: 73% of people know how to build a strong password, yet nearly half still stuff them with dictionary words or personal details. Password managers? Not really on the radar. Instead, people are still far more likely to scribble secret codes in a physical notebook (28%) or rely on raw memory (23%) than use a dedicated vault app (11%).

Oversharing with the bots

Then there's AI. (Cue the dramatic music). Not so much the elephant in the room anymore, as the elephant now trying to steer the room, with its not-very-delicate feet. Its sense of direction and ability to steer the right way can't always be trusted.

An overwhelming 80% of adults now use AI tools, and half the entire participant pool use them on the job ...But corporate guardrails haven't caught up: 52% of employees using AI have received zero security training on it.

The result? Unauthorized information sharing with AI tools is running rampant. One-third of those using AI at work admit to copy-pasting confidential company data into AI bots without their boss ever knowing.

On a personal level, users are confessing their deep secrets, health records, passwords, and even banking details to chatbots. We're worried about AI cybercrime, sure – 67% of us fear AI-driven scams – but that hasn't stopped us from treating the chatbot like a digital therapist and administrative assistant all rolled into one.

People. Even messier than your browser tabs

From sticky-note passwords to unsanctioned bot queries and deepfake anxiety, the behavioral picture this year is as messy as it gets. But people aren't the problem. They never have been. They're just ... human. Which means fallible, emotional, and not always rational or predictable. So not always easy to protect.

Half the global pool of participants has fallen victim to cybercrime, yet the human story behind the stats shows resilience, misplaced trust, and a desperate need for better habits over empty theory.

And that's why this report *really* matters. It's comprehensive, to the point, and brimming with BS*.

So settle in, grab a coffee, close those tabs (yes, all of them), and join us as we unpack the human side of cybersecurity in 2026. Buckle up, it's quite a ride.

Here's to safer behaviors, safer people, and a safer digital world.

Oz & Lisa



Oz Alashe, MBE

CEO & Founder,
CybSafe



Lisa Plaggemier

Executive Director,
The National Cybersecurity Alliance

Report aim & structure

Our sixth¹ Cybersecurity Attitudes and Behaviors, Oh, Behave! 2026-2027 report aims to provide a comprehensive international snapshot of people's cybersecurity attitudes and behaviors across representative global samples.

We built on half a decade's worth of findings and focused on the following security behaviors, presented in four different subchapters:

1. Authentication methods
 1. Password creation habits² – specifically, password length, use of personal information, and single dictionary words
 2. Use of separate passwords³
 3. Password management techniques⁴
 4. Use of MFA⁵, biometrics⁶ and passkeys⁷
2. Installing the latest software updates⁸
3. Backing up data⁹
4. Checking messages¹⁰ and websites¹¹ for signs of phishing and reporting¹² them

1 Well, seventh, if we count the [5-year comparison report](#) we published in Jan 2026, where we compared five years of data (2021–2025) to uncover the trends and challenges in cybersecurity attitudes and behaviors.

2 SebDB behavior: [\[SB003\] Authenticates with a strong password \(or passphrase\)](#)

3 SebDB behavior: [\[SB016\] Authenticates with a unique password \(or passphrase\)](#)

4 SebDB behavior: [\[SB130\] Stores a password \(or passphrase\) securely](#), [\[SB209\] Uses an approved or official password manager application](#), [\[SB210\] Uses an approved browser-based password manager](#)

5 SebDB behavior: [\[SB001\] Authenticates with MFA](#)

6 SebDB behavior: [\[SB203\] Authenticates with biometrics](#)

7 SebDB behavior: [\[SB112\] Authenticates with a passkey](#)

8 SebDB behavior: [\[SB024\] Keeps software up-to-date](#)

9 SebDB behavior: [\[SB061\] Backs up data](#)

10 SebDB behavior: [\[SB081\] Checks a message for signs of deception](#)

11 SebDB behavior: [\[SB058\] Checks a website for signs of deception](#)

12 SebDB behavior: [\[SB087\] Reports a suspicious message](#)

REPORT AIM & STRUCTURE

We've organized our findings into the following research themes:

- What are people's attitudes toward cybersecurity, and what are their concerns, if any?
- Who do people rely on when it comes to cybersecurity, and whose responsibility do they think it is, at home and at work?
- What types of cybercrimes do people experience? Do they report them?
- Who has access to training, and do they use it? If so, how do they feel about it?
- How do people engage with cybersecurity in terms of specific security behaviors?
- How do people feel about AI and its impact on their personal and professional lives?

We delve deeply into cybersecurity attitudes and perceptions, examining the reasoning behind them and their links to relevant security behaviors. By analyzing both quantitative data and qualitative responses, we aim to uncover the motivations and concerns that drive individuals' cybersecurity behaviors. Ultimately, our goal is to offer actionable insights that can inform cybersecurity professionals, policymakers, and educators in developing more effective strategies to enhance online security for everyone.

Finally, in the appendices, we detail our research methodology, participant demographics, and the country-specific findings.

Key terms

The key terms we've used throughout the report:

Artificial Intelligence (AI): The capability of machines to mimic human cognitive functions such as learning, reasoning, and problem-solving. AI systems are designed to perform tasks that typically require human intelligence.

AI tools: Software programs that use AI techniques to achieve specific goals.

AI-related cybercrime: Criminal activity that uses AI to improve the effectiveness of cyberattacks. Criminals leverage AI's capabilities for automation, personalization, and target selection. For example, using AI to personalize phishing scams or develop new strains of malware.

(Security) attitude: A psychological disposition we have toward making an evaluative judgment about security (i.e., the way we think or feel about it). For reporting attitudes, we have used 5- and 10-point Likert scales (e.g., 'strongly disagree' to 'strongly agree') to examine positive and negative views people hold about particular security topics.

Backing up: The process of copying data for recovery purposes in case the original data is lost or corrupted.

(Security) behaviors: A discrete, observable action that individuals can take to protect information, systems, or assets. For this report, we've narrowed down our investigation to behaviors across four areas ([there are many more](#)). These include: authentication methods (creating and storing strong, unique passwords, using MFA, passkeys, and biometrics), installing software updates, backing up data, and checking messages for signs of phishing and reporting them.

Cryptocurrency investment fraud: Scammers, through various means of manipulation, convince people to deposit more (and more) money into financial 'investments' using cryptocurrency. In reality, these investments are fake, and the funds are controlled and ultimately stolen by cybercriminals.

Cyberbullying: Cyberbullying occurs on digital platforms. It includes sending, posting, or sharing negative, harmful, false, or mean content about someone else.

KEY TERMS

It can include sharing personal or private information about someone else, causing embarrassment or humiliation.

Cybercrime: Cybercrime has been defined in several ways, but is essentially regarded as any crime (traditional or new) that can be conducted through, enabled by, or using digital technologies (e.g., phishing attempts).

Cybercrime victimization: The result of criminal behavior in which harm or loss is caused to a person or organization, and information and communication technology plays a notable role in the execution of the offense.

Deepfakes: Synthetic media, typically videos or images, created using AI to realistically alter or fabricate a person's appearance or actions. They're often used to create convincing but false representations of individuals.

Delivery scam: Scammers impersonate delivery companies (e.g., Royal Mail, FedEx, UPS), by sending fake notifications claiming a parcel is awaiting delivery. They trick people into clicking malicious links or paying a fee, which leads to personal or financial information being stolen.

Identity theft: When a cybercriminal steals someone's personal information and uses it to assume their identity. This can involve the criminal applying for credit and loans, or even filing taxes using the victim's identity, potentially damaging their credit status.

Job scam: Scammers post fake job advertisements or contact people directly with fraudulent job offers. They trick victims into providing personal or financial information, paying upfront fees for training or equipment, or processing fraudulent payments on the scammer's behalf.

(Security) knowledge: Awareness and understanding of cybersecurity principles, practices, and potential threats.

Lottery/prize scam: Scammers contact people claiming they've won a lottery, prize, or competition. To claim the prize, victims are asked to pay upfront fees or taxes, or to provide personal and financial information. No prize exists, and the funds or information are stolen by the scammer.

Multi-factor authentication (MFA): The process of using two or more pieces of information to log in to an account. This can be a password and code sent to a phone. Also known as Two-Factor Authentication (2FA) and Two-Step Verification (2SV).

KEY TERMS

Online dating scam: Cybercriminals adopt a fake online identity to create the illusion of a romantic or close relationship to manipulate and/or steal from the victim. They often use highly emotive requests for money, claiming they need emergency medical care or must pay for transport costs to visit the victim if they're overseas.

Online marketplace scam: Scammers pose as buyers or sellers on online platforms (e.g., eBay, Facebook Marketplace, Craigslist). Sellers may receive fake payment confirmations and ship goods without receiving money, while buyers may pay for items that never arrive or are misrepresented.

Password hygiene: Creating long, unique and separate passwords for sensitive online accounts, managing passwords using browser or stand-alone applications, and the tactics of changing passwords.

Password management application: A password manager is a stand-alone program that stores, generates, and manages passwords for local applications and online services.

Phishing: Cybercriminals trick people into providing information or installing dangerous software to steal money or data from them. This is often done via fake emails that appear to be from trusted senders, encouraging people to click malicious links or open malicious attachments.

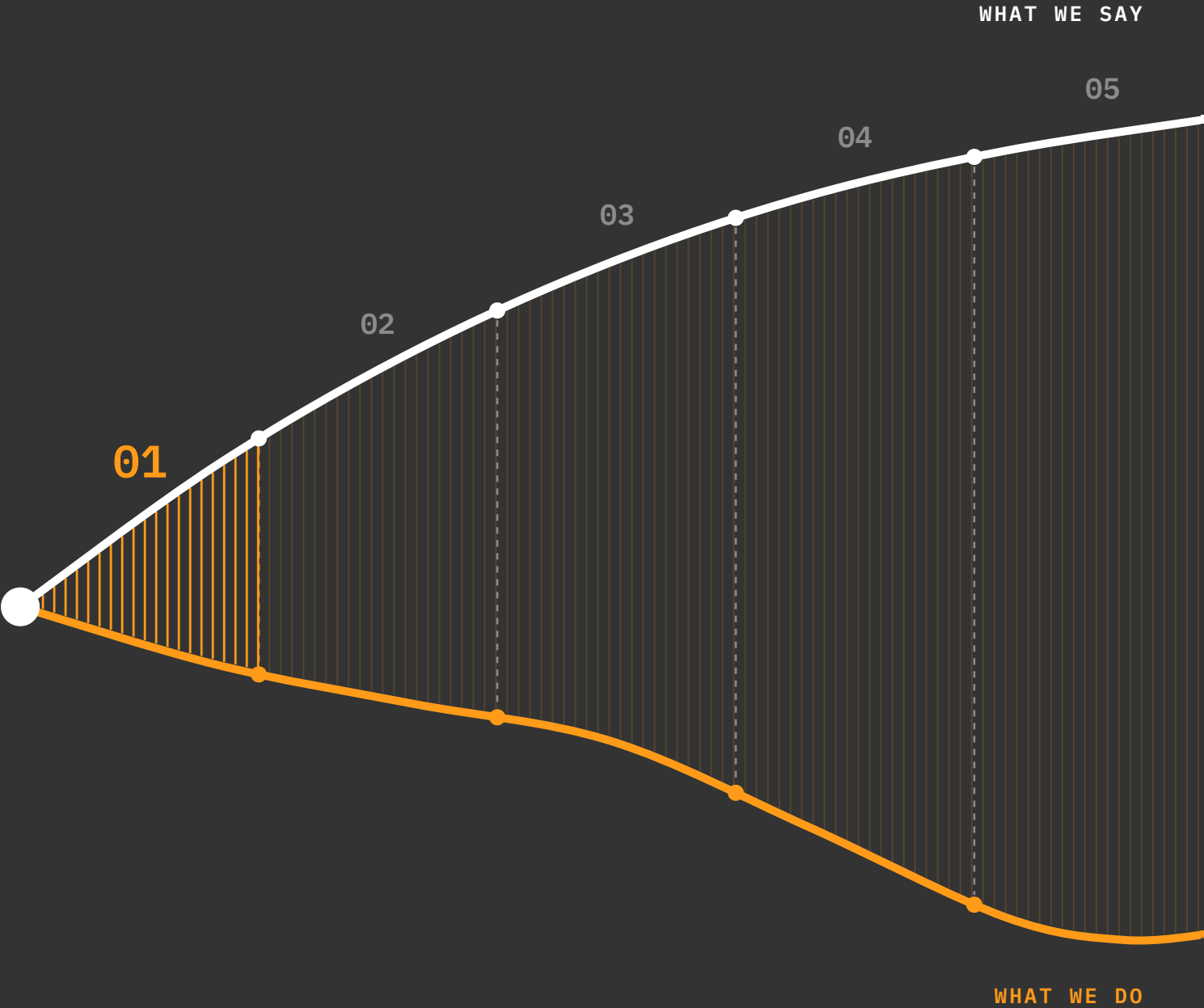
Sensitive (important) online accounts: Online accounts holding details of identity, address, and bank cards (e.g., payment-related sites, social media accounts, and work accounts).

Tech support scam: Scammers impersonate tech support from legitimate companies (e.g., Microsoft or Apple), claiming issues with a device. They trick people into paying for fake repairs or granting remote access to steal data or install malware.

(Security) training: Education and practice aimed at improving skills and behaviors to protect against cybersecurity threats.

SECTION 01

Executive summary



Executive summary

This report is based on a survey of 5,000 adults (age 18+), evenly sampled across five countries – the United States, United Kingdom, India, Brazil, and Singapore – and fielded between April 28 and May 19, 2026. Detailed findings, methodology, and demographic information are available in the full report.

Critical takeaways

Nearly a third of employees who use AI at work (32%) have shared sensitive company information with these tools without their employer's knowledge, and 56% of all AI users have never received any AI-specific security training.

Digital natives are the most exposed: 64% of Gen Z and 57% of Millennials have already lost money or data to a scam, compared with just 33% of Baby Boomers.

Deepfake scams have gone mainstream: 42% of Gen Z and 48% of Millennials have been targeted by a deepfake phone or video call.

88% of employees who complete cybersecurity training say it's useful. But half of all respondents have no access to any cybersecurity training at all.

Nearly half of employees (48%) view their own colleagues as a security risk, even in workplaces where leadership visibly champions security.

Just 39% of people use passkeys, despite 70% saying they're at least somewhat familiar with them.

The ‘bot’-tom line on artificial intelligence (AI)

AI adoption has outpaced AI governance. Four out of five people (80%) now use AI tools, and for 44%, use spans both home and work. Adoption declines sharply with age: 92% of Millennials and 90% of Gen Z use AI tools, compared with 52% of Baby Boomers and 25% of the Silent Generation.

People are assuming AI can be trusted and readily share sensitive information: 40% have shared health information, 32% have shared personal feelings normally reserved for someone they know well, and 18% have confided a secret they have never told another person.

At work, half of all respondents (50%) now use AI: 41% started using AI on their own initiative, and 44% because their employer required or encouraged it.

Employers are encouraging AI use, but not necessarily the training to go with it. A head-scratching 56% of AI users (and 52% of working folks) receive no AI security or privacy risk training. None. Employers aren't helping: 43% fail to clearly explain what's okay to feed the machine.

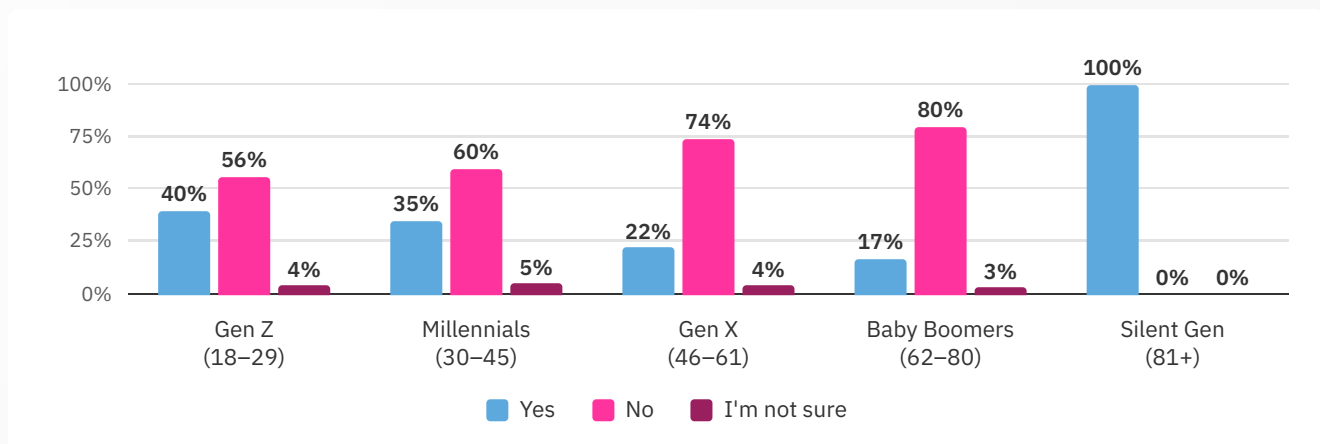
👉 NEWS YOU CAN USE

It's entirely possible these folks acknowledged AI policies that they didn't read, or even took some training on AI that didn't stick. Go beyond policy acknowledgement and give people concrete examples of what's OK and what's not. Make it practical and easy to understand.

Naturally, that radio silence has created a few corporate wildcards. Nearly a third of participants who use AI at work (32%) have snuck sensitive company info into a prompt behind their boss's back. This is obviously concerning, so we asked them what type of information they'd included.

Most often, they said internal documents or customer data (50%) and financial data (47%). Sharing is highest among younger employees: 40% of Gen Z and 35% of Millennials, compared with 17% of Baby Boomers (Figure i).

Figure i. ‘Have you ever shared sensitive work information with AI tools without your employer’s knowledge?’ by generation.



Base: US, UK, India, Brazil, Singapore. Total number of participants: 2,481 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

When it comes to playing detective, people feel pretty slick at spotting AI-generated images and video (57% confidence each), as well as text (52%), but [voice deepfakes](#) still throw them off (46%). Overall, the vibes remain decidedly cautious.

Concern outweighs enthusiasm: 67% worry about AI-driven cybercrime, and 63% expect [scams](#) to become more sophisticated because of it. In the end, only about half see AI as a net positive for society (55%), or believe its benefits outweigh its risks (50%).

COUNTRY COMPARISONS

AI adoption & workplace use

- **Overall adoption:** Highest in Brazil (91%), Singapore (90%), and India (89%), outpacing the US (69%) and the UK (60%).
- **Workplace use:** Peaks in Brazil (63%) and drops to its lowest in the UK (36%).

Security, training and oversharing

- **AI security training:** Singapore leads the way (48%), while India lags furthest behind (27%).
- **Unsanctioned workplace oversharing:** Those who use AI at work in Brazil are the most likely to share sensitive info without telling their employer (46%), while Singaporeans are the most discreet (23%).

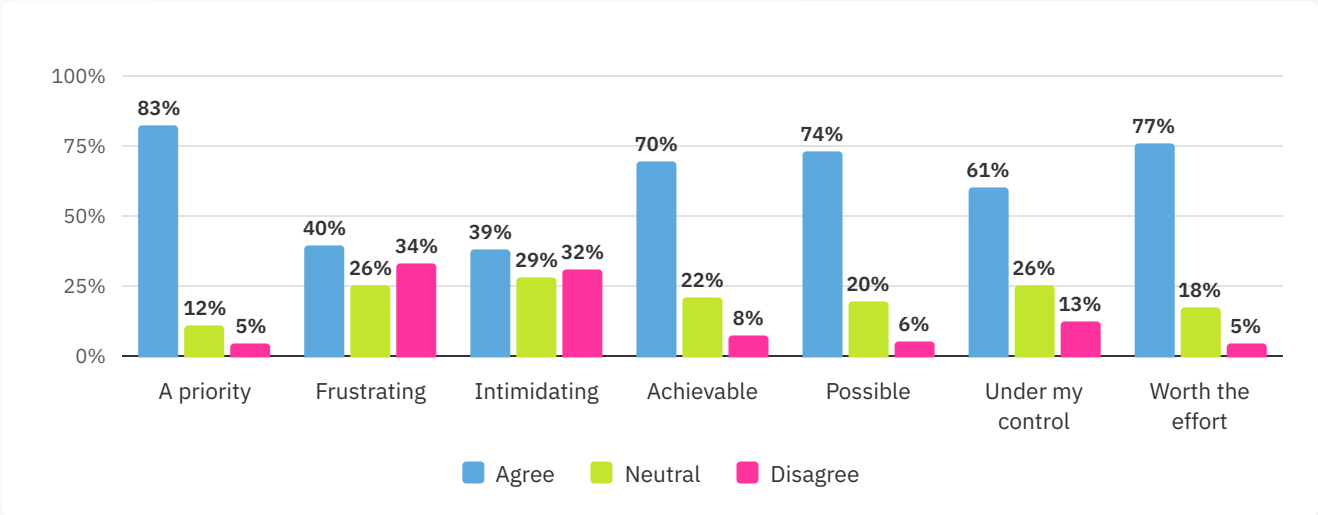
Spotting fakes & public sentiment

- **Spotting AI content:** India reports the highest confidence in detecting AI-generated content (57–69% across formats), whereas the UK feels the least confident (33–46%).
- **Society's outlook:** Optimism mirrors confidence – 69% of participants in India believe AI is good for society, compared to just 37% in the UK.

Safe and sound, or just stressed out? Attitudes, beliefs & perceptions about online security

People feel more confident about online safety than their actual habits justify, a knowing/doing gap that recurs throughout this report. Overall sentiment is positive (Figure ii): 83% of people consider online security a top priority, 77% think it is worth the effort, and 70% believe it’s achievable. 61% feel staying secure is within their control, though frustration (40%) and intimidation (39%) remain common.

Figure ii. ‘I feel that staying secure online is...’



Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

Millennials show the sharpest contrast: they lead every generation in feeling in control (66%), finding security easy (66%), and believing it is achievable (75%), yet they are also the most likely to feel overwhelmed by it all (54%). This pairing of high confidence with high overwhelm recurs throughout the data.

👉 NEWS YOU CAN USE

Feelings of frustration, intimidation and overwhelm are all signals to watch your language! You might think terms like ‘threats’, ‘defenses’, and ‘attacks’ are attention-getters, but language can contribute to the negative feelings and cause people to disengage.

EXECUTIVE SUMMARY

A few persistent myths remain widespread: half of respondents (50%) assume their devices are automatically secure, and 55% think fully protecting themselves online is expensive. Distrust in government runs deep: 57% are concerned about their own government accessing their data through apps, nearly matching the 58% concerned about foreign governments doing the same, and 53% worry either government could use apps to influence what they see or think.

In the workplace, 60% say leadership visibly champions cybersecurity and 64% feel safe habits are embedded in daily routines. But nearly half of workers (48%) also see their own colleagues as a security risk – a reminder that insider risk, whether accidental or not, remains a concern even where culture and leadership support are strong.

Media coverage plays a dual role: it motivates action for 66% of people and keeps 64% informed, but also fuels fear (51%) and confusion (51%). When coverage does prompt action, the most common responses are enabling MFA (57%) and scrutinizing AI-generated content more closely (56%).

COUNTRY COMPARISONS

US: Participants in the US reported the highest frustration (47%) and intimidation (45%) about staying secure online.

UK: They scored the lowest (i.e., the best, compared to their peers) on almost every negative attitude, including intimidation (34%), confusion (33%), and overwhelm (44%) as it relates to staying secure.

India: A total paradox. They blew away the competition in swagger – when it comes to staying secure online, they lead on achievability (74%), personal control (65%), and ease (64%) – yet *also* swept the top scores for confusion (51%), overwhelm (59%), and holding back on online activities out of fear (62%).

Big Brother fears: Domestic app-snooping freaks out India and Brazil the most (63–64%), while the UK remains the least concerned (46%).

Office vibe check: India leads the world in bosses championing cybersecurity (63%) and embedding good habits (71%), while the UK sits quietly at the back on both (54% and 61%).

Scam-o-rama: When bad clicks happen to good people.

Cybercrime victimization & reporting

Half of all respondents have already experienced cybercrime, and fear of victimization is nearly twice as common as the expectation of it. Two-thirds of respondents (66%) fear becoming a cybercrime victim, but only 37% actually expect to be targeted.

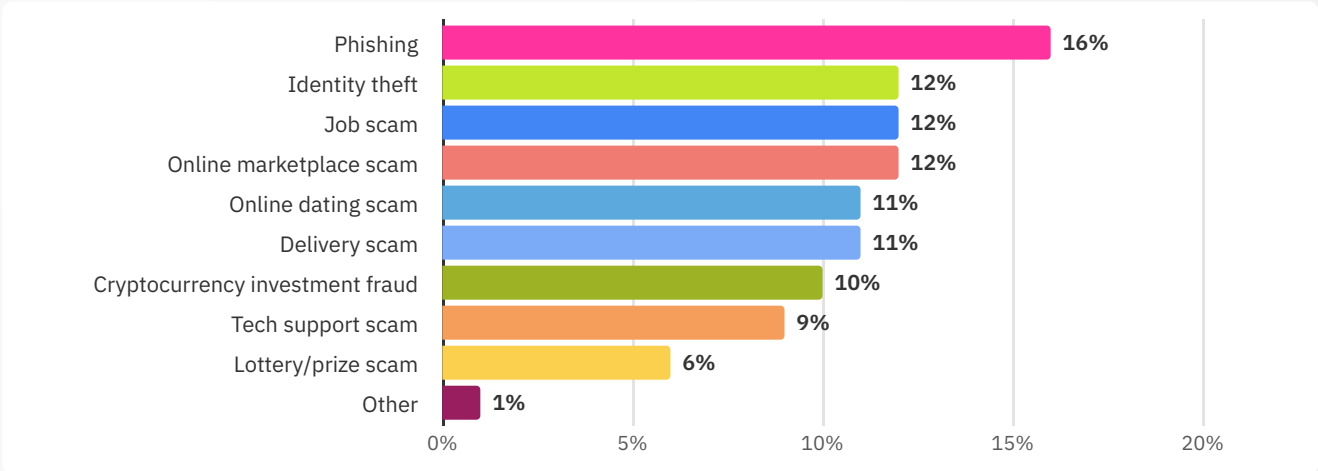
A meaningful share has also grown fatalistic: about a third consider losing money (33%) or having personal data stolen (39%) an unavoidable cost of being online. Concerns about those defending against cybercrime are widespread too: 57% doubt law enforcement has the capability and capacity to fight cybercrime effectively, and 63% believe attackers are more advanced than defenders.

👉 NEWS YOU CAN USE

Consider communicating security success stories across your org. This can be empowering for the security culture and for the security team.

The data bears this out: 50% of participants have fallen victim to a scam, totaling 5,662 incidents across the sample. Phishing is the most common incident type (16%), with job scams, identity theft, and online marketplace scams tied for second (12% each, Figure iii).

Figure iii. Types of cybercrime incidents.



Base: US, UK, India, Brazil, Singapore. Total number of cybercrime incidents: 5,662 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

EXECUTIVE SUMMARY

Growing up online does not appear to confer protection; in fact, just the opposite: 64% of Gen Z and 57% of Millennials have lost money or data to scams, compared with 33% of Baby Boomers and 23% of the Silent Gen.

Younger generations are also the most exposed to [deepfake scams](#): 42% of Gen Z and 48% of Millennials have been targeted by a deepfake call. Overall, 36% of all respondents have received a deepfake phone or video call, and 40% of those lost money or data as a result.

NEWS YOU CAN USE

One size doesn't fit all when it comes to awareness content and training. Tailor your deepfake-awareness content to younger employees, knowing that they're targeted more, and more vulnerable. Use language and imagery that will get their attention.

Most incidents were [reported](#) to at least one channel (89%), most often a bank or credit card company, followed by the police or other law enforcement. Formal reporting was much lower, however: reporting to the police ranged from 27% to 41% depending on crime type, and reporting to a government agency from 22% to 36%. Among the 11% who did not report, the main reasons were feeling the loss was too small, not knowing who to contact, and embarrassment.

Meanwhile, cyberbullying impacted 19% of people, with Gen Z taking the biggest brunt of the online shade (30%).

COUNTRY COMPARISONS

India: Holding the title for maximum fatalism and maximum fallout. They led the world in feeling losses were inevitable (50% for cash, 54% for data) and hit the highest overall victim rate (63%). They also swept almost every scam category, including lottery scams (52%), and got battered by deepfakes (49% targeted, 55% of those losing cash/data).

UK: Cruising on easy mode. The UK kept it cool with the lowest fatalism (only 20% expecting cash losses, 24% data), the lowest victim rate (40%), and the lowest overall worry about becoming a cybercrime victim (56%).

Brazil: The anxiety capital. A whopping 80% of participants here spend their days worrying about falling victim to cybercrime.

US: The identity theft HQ. The US took top billing for suffering stolen identities (30%), though they proved shockingly tough against deepfakes – only 28% lost cash/data despite 39% being targeted.

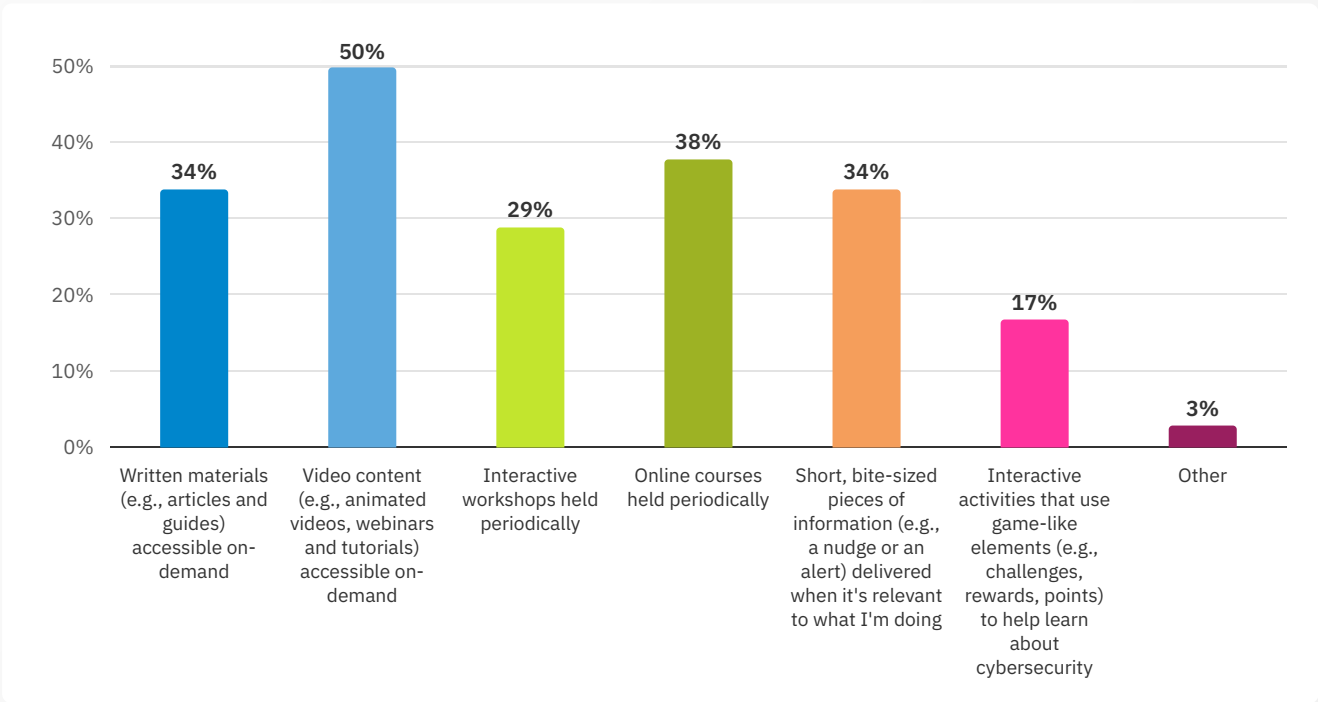
Singapore: Where the crypto pirates hang out 🇸🇬, or at least where they target – 25% of all crypto fraud victims are here, second only to India (30%).

School of hard hacks: Who's getting taught? Cybersecurity training

Half of respondents have no access to cybersecurity training at all. Where training does exist, it skews toward younger employees (64% of Millennials and 56% of Gen Z have access, compared with 26% of Baby Boomers) and higher-risk industries like IT (76%) and Finance (75%); hospitality workers are least likely to have access (58% report none). Fewer than half of working respondents (47%) have any mandatory training.

When people do engage with training, format matters (Figure iv). Video is the most preferred format (50%), followed by online courses (38%). For the first time, bite-sized mini-lessons and written materials are tied for third (34% each). Video is the top choice across every generation except the Silent Generation, who still prefer written content (45%).

Figure iv. ‘What format do you prefer to consume cybersecurity training information?’



Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

The most common reasons for skipping available training: lack of time (21%), already feeling knowledgeable enough (19%), and, tied at 17% each, doubting that training reduces personal risk and not viewing cybersecurity as a priority.

👉 NEWS YOU CAN USE

Borrow from Marketing and refer to your training as being 'quick and easy to access' (as long as you're delivering on those things and not still assigning an hour of training once a year). Tell success stories from employees who avoided a personal scam or cyber issues because of training they took at work. We bet if you posed that question in Slack or Teams to employees, those stories would organically write themselves.

Among those who attended training, 88% found training useful, 54% reported improved phishing detection, 49% set up MFA, and 46% adopted a password manager. Translating training into action remains the harder problem, though: most key behaviors are still not adopted by a majority of attendees.

🌐 COUNTRY COMPARISONS

Singapore: The star student! ★ Leads the world in training access (66%) and actually shows up to class, boasting the highest actual usage among those with access (51%).

Brazil: The ultimate class skipper. 🙅 Trained at the very bottom for actual usage among those with training access (25%) and mandatory workplace training (33%).

India: Big on rules. Takes top prize for forcing employees into mandatory security training (59%).

UK: Total creature of habit. Loves forcing the classic once-a-year refresher (56%), though they're surprisingly lukewarm about video content (only 38% preference) compared to eager binge-watchers in India (57%) and the US (50%).

US: Over half of employed American participants (55%) aren't required to complete mandatory training at their workplace. Among those who are, training tied to starting a role and training once a year were equally common, and jointly the most reported practices there (47% each).

Lock it down or just sticky-note it? Cybersecurity behaviors

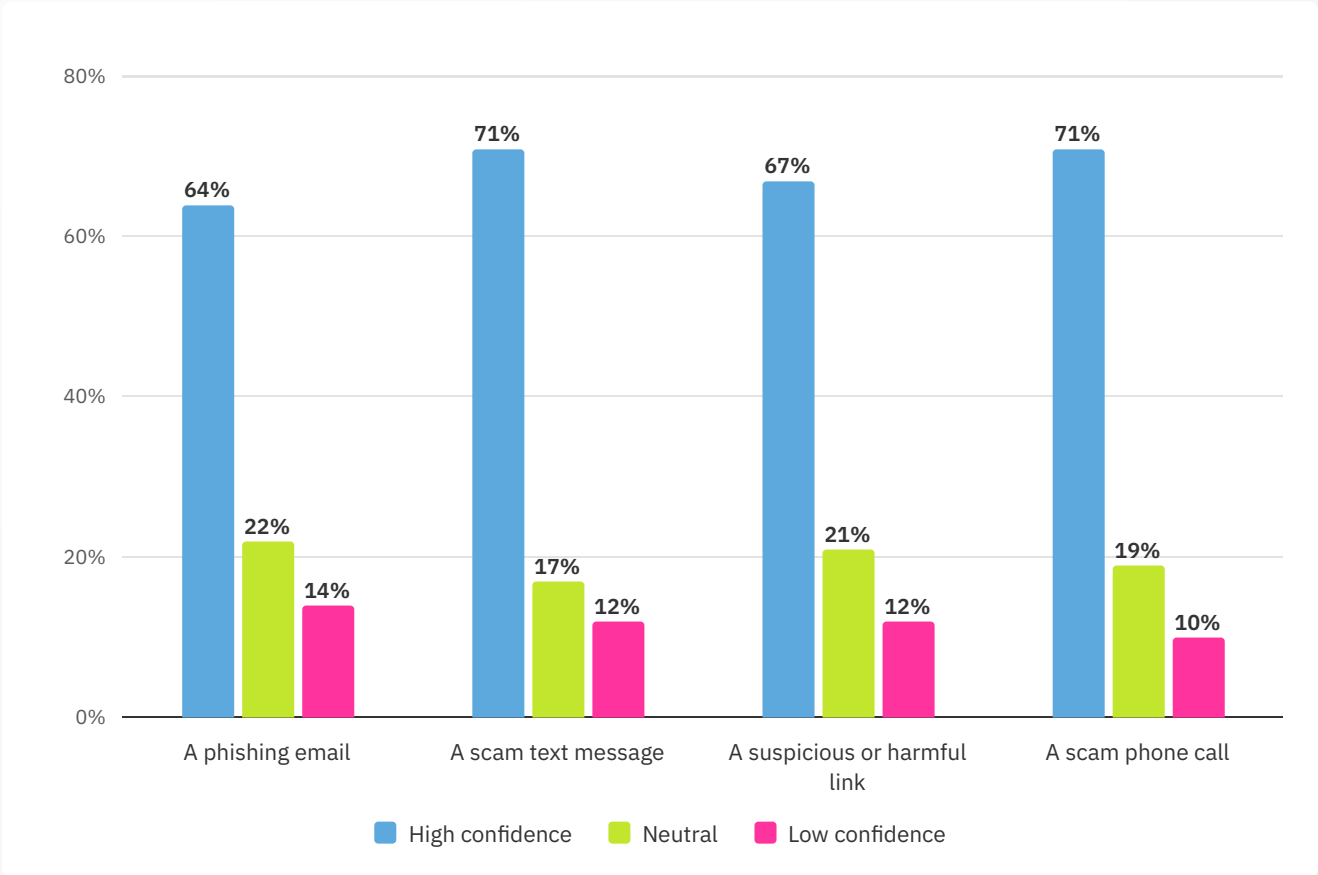
Knowledge and behavior remain disconnected: most people say they know best practices, but adoption of the practices that matter most, password managers, MFA, and passkeys, stays low. Seventy-three percent say they know how to create a [strong password](#) and do so, yet personal information (38%) and dictionary words (46%) appear in a large share of passwords. Overall, 53% don't use [MFA](#) regularly, including 21% who know how to but have stopped or don't use it.

EXECUTIVE SUMMARY

When time is short, convenience wins: 60% prefer reusing or slightly modifying a familiar password; only 34% create a unique one, either on their own (25%) or with a password manager (9%). Paper notebooks (28%) are still more common than password manager apps (11%) or browser-based savers (8%).

Confidence in spotting scams varies by format: people feel most confident identifying a scam text or phone call (71% each), somewhat less confident with a suspicious link (67%), and least confident with a phishing email (64%, Figure v). Millennials report the highest confidence across most categories (76% for scam texts, 74% for suspicious links, 71% for phishing emails); the Silent Generation shows the widest spread of any generation, with the lowest confidence for phishing emails (45%) but highest for scam calls (80%).

Figure v. ‘How confident are you in your ability to identify each of the following?’



Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

EXECUTIVE SUMMARY

Confidence does not translate into consistent behavior: only 61% regularly check messages for warning signs, and only 41% report suspicious messages when they see them.

Just 39% use [passkeys](#), despite 70% having at least some familiarity with them. Over half (53%) use biometrics, and among those who don't, the main barrier is privacy, not understanding, as 33% of non-users cite privacy concerns about sharing their biometric data.

👉 NEWS YOU CAN USE

Create some awareness content on how biometric data actually works and typically stays on the device rather than being shared with apps or websites, to address people's privacy and security concerns. Remind people that we willingly share images of our faces, for example, when we get a new driver's license or passport, and we've been doing that for decades.

🌐 COUNTRY COMPARISONS

India: The ultimate password rebels. They lead the world in stuffing logins with personal info (50%) and dictionary words (60%), but redeem themselves (slightly) by being further up the global rankings for regular data backups (52%).

UK: The star pupil for safe habits. ⭐ They play it most cautiously with passwords (only 31% personal info, 36% dictionary words), lead the pack in always installing updates when notified (38%), and top MFA usage (59%). The punchline? They're the absolute lazy champions when it comes to reporting phishing messages (37%).

Singapore: Highest confidence in identifying malicious links (71%) and phishing emails (68%), while regular MFA use (58%) comes in just behind the UK (59%).

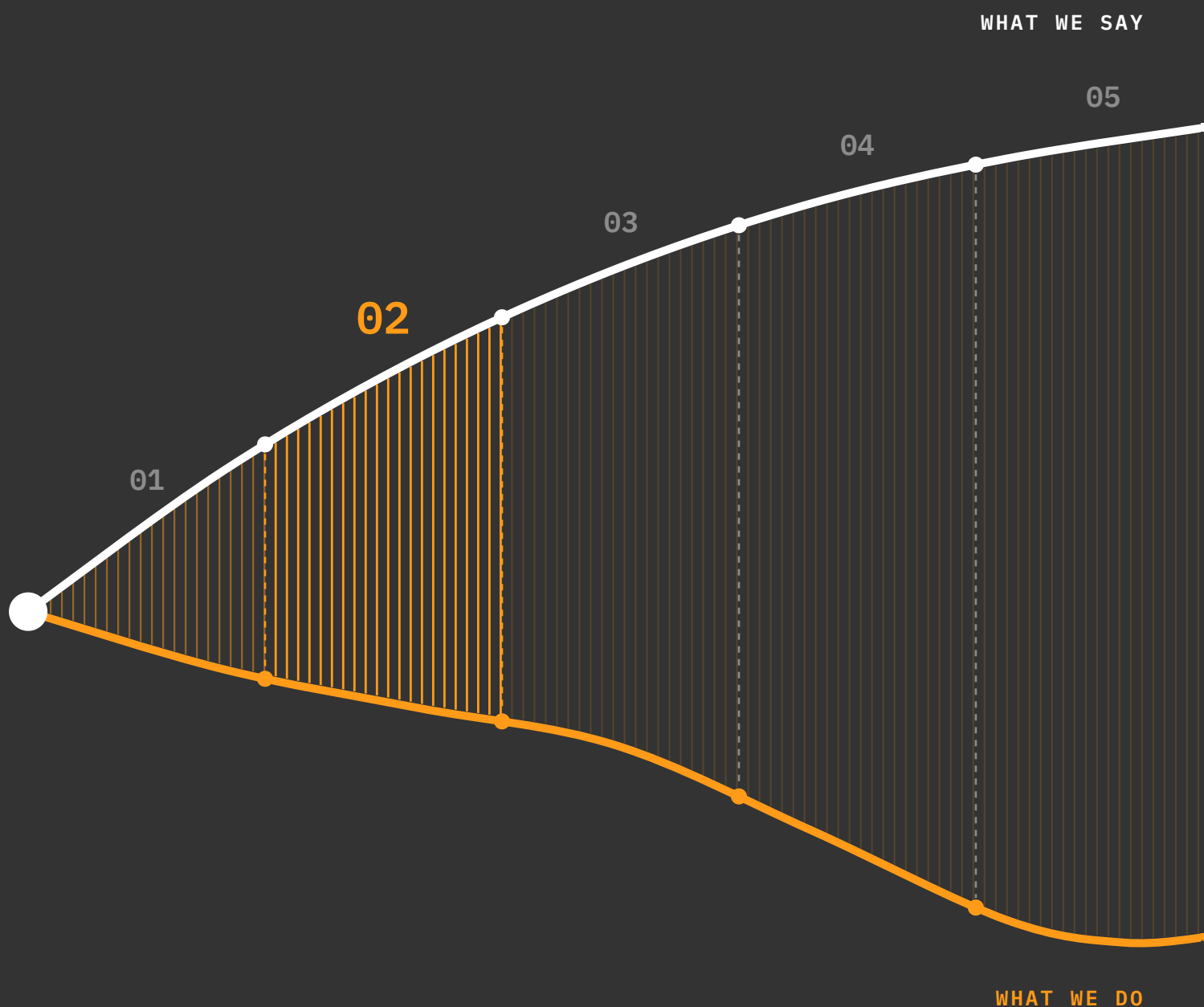
Brazil: Living life on the edge. They scored the lowest for MFA usage (33%) – with 28% having never even heard of it – had the highest share of update procrastinators (18%), and trailed the world in regularly backing up their data (44%).

US: Out of all countries surveyed, the highest percentage of those writing their passwords in a notebook was in the US (35%). It also had the highest share who said they'd never seen a way to report phishing messages (8%), compared to 5 to 6% in all other countries.

SECTION 02

Main findings

(what we reeled in 🧲)



Main findings

(what we reeled in )

So, how exactly did we land this absolute whale of a data catch? Forgive us a quick recap if you've already read the intro, but we know how you data-heads operate ...you probably skipped the appetizers and dove straight into the Moby Dick of a main course. (It's ok, we're the same. Solidarity for the impatience. 🐟)

When?

We rolled out our sixth Cybersecurity Attitudes and Behaviors survey online between April **28** and May **19, 2026**.

Where?

The folks at Toluna rounded up representative samples (perfectly balanced by age and gender) across five countries: the United States, the United Kingdom, India, Brazil, and Singapore. Which gives us a grand total of **5,000** respondents.

Who?

We targeted adults aged **18** and older. Our average participant clocked in at **45** years old ($SD = 16.63$), and **65%** were grinding away in full- or part-time employment. (If you're a total nerd for demographic charts, Appendix A is just for you.)

What?

Just as we've done in past years, we sliced and diced the numbers by age group and employment status. (And if you're curious about country-by-country quirks, Appendix B has all those juicy regional details.)

1. Attitudes, beliefs & perceptions about online security

Before anyone opens a shady-looking email, hits ‘Remind me later’ on a software update for the twentieth time, or reuses their pet's name for their bank password (yes, we’ve all done it), they’ve already made up their mind about cybersecurity.

By which we mean they’ve decided whether it's important, whether it’s a pain in the neck, or whether it's even their problem to begin with. 🙄

This chapter dives headfirst into those internal mindsets – the views, attitudes, core beliefs and perceptions that shape how people handle their digital lives (and specifically their own security) ...long before they even click anything.

Enter the Knowledge-Attitude-Behavior (KAB)¹³ model. This framework reminds us that what people know (knowledge) shapes their feelings and opinions (attitudes), which in turn influence their actions (behaviors).

These attitudes, beliefs, and perceptions – which live right at the heart of human behavior and affect how individuals engage with online security – are the mental sparks before the action occurs. For instance, research shows that employees with an upbeat, positive outlook on cybersecurity engage in far less risky behavior¹⁴ at work. By getting inside people's heads, we get a front-row seat to why they choose to embrace good security habits ...or indeed throw caution to the wind.

Breakdown of Chapter 1:

1.1 Navigating personal security: How people feel about the daily chore of staying safe. Is it smooth sailing, or a massive headache? Here, we explore their feelings about the ease, frustration, and overall possibility of staying safe online.

1.2 Misconceptions and concerns: Common tech myths, cost worries, and concerns related to governmental data misuse.

1.3 Cybersecurity culture in the workplace: How the 9-to-5 crowd views leadership, company habits, and their own risky coworkers.

1.4 Media’s role in shaping attitudes: Does the news inspire us to secure our lives, or does it just scare us into hiding under a rock?

¹³ Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security*, 42, 165-176.

¹⁴ Fatoki, J. G., Shen, Z., & Mora-Monge, C. A. (2024). Optimism amid risk: How non-IT employees' beliefs affect cybersecurity behavior. *Computers & Security*, 141, 103812.

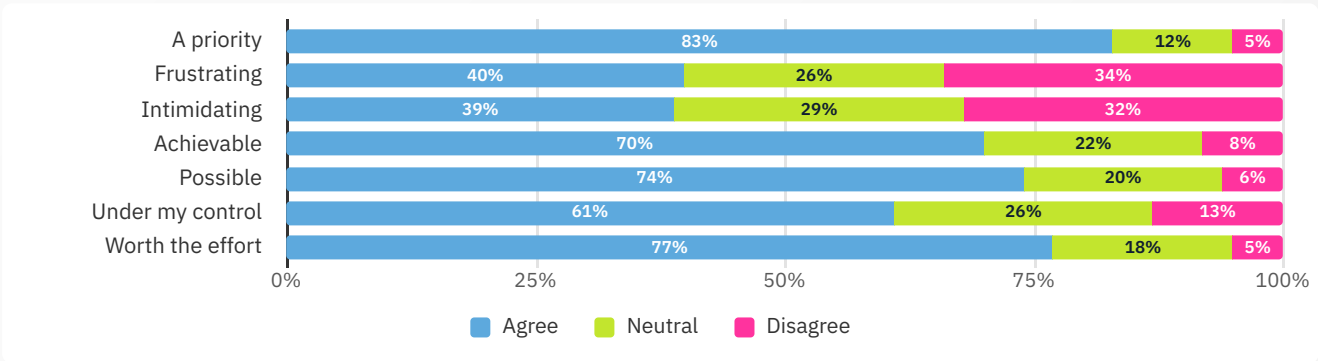
1.1 The personal security vibe check

Let’s kick off with some good news. Overall feelings toward online security are surprisingly bright this year (Figure 1). Positive attitudes have either held steady or climbed slightly higher compared to 2025, while negative attitudes keep shrinking.

When asked about keeping their digital lives secure:

- 83% say it’s a priority (+1% from 2025).
- 77% feel it’s worth the effort (holding steady from 2025).
- 74% agree it’s possible (same as 2025).
- 70% believe it’s achievable (+1% from 2025).
- 61% feel it’s directly under their control (a nice +3% bump from 2025).

Figure 1. ‘I feel that staying secure online is...’



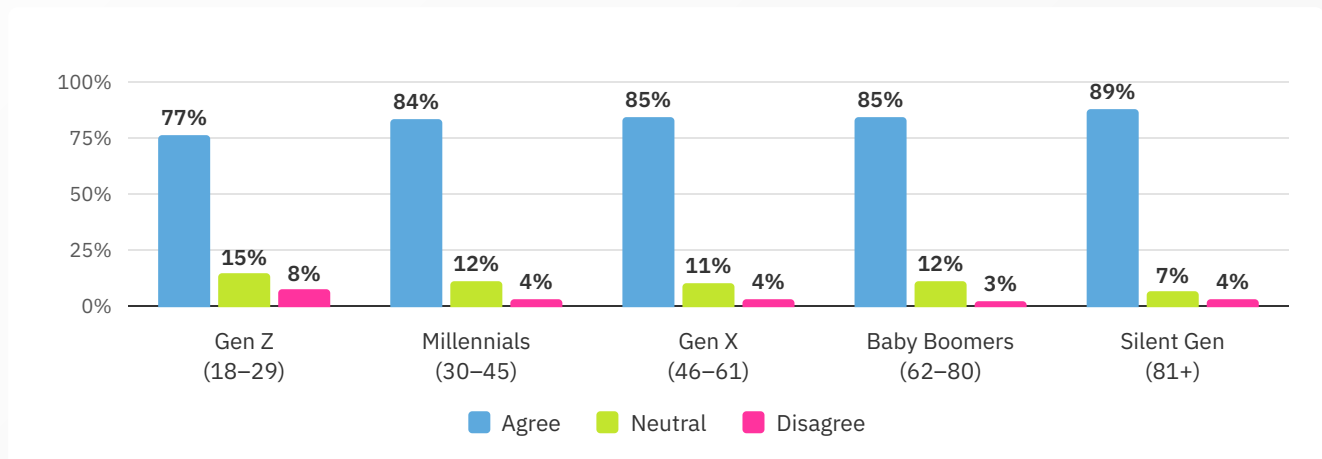
Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

Of course, it’s not all sunshine and rainbows. Alas. A chunk of participants still find the whole thing a bit exhausting: 40% admit security feels frustrating, and 39% find it intimidating. The silver lining? Those numbers are down by 2% and 4% respectively since last year.

The generational divide: Who cares most?

While these broad feelings hold fairly true across age brackets, a few fun generational quirks popped up. Take prioritization (Figure 2): Gen Z (77%) is the least likely to call online security a priority. From there, the sense of urgency climbs as people get older, rising to 84% for Millennials and peaking at 89% for the Silent Gen.

Figure 2. 'I feel that staying secure online is a priority' by generation.



Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

However, the biggest, wildest plot twist appeared when we asked people if they feel in control of their security (Figure 3). Unlike the priority finding, this doesn't rise or fall steadily with age. Instead, control hits a massive peak in mid-adulthood.

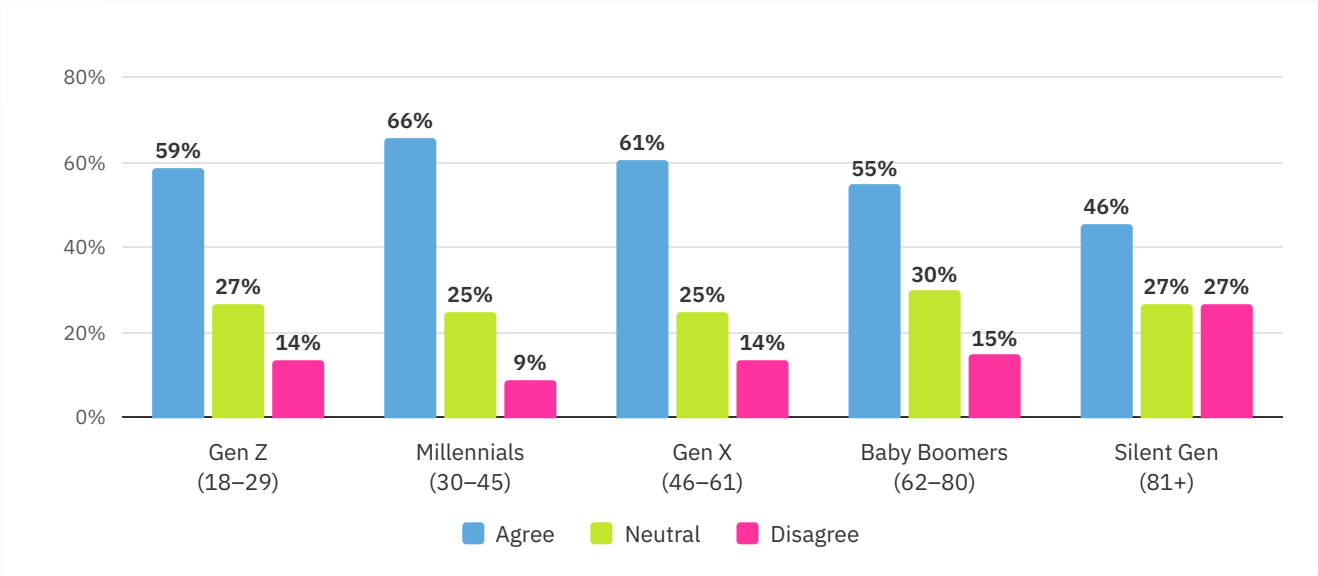
- Millennials (66%) feel most in control.
- Gen X (61%) and Gen Z (59%) sit comfortably in the middle.
- Baby Boomers (55%) and the Silent Generation (46%) trail behind.

That leaves a whopping 20% confidence gap between peak-control Millennials and the Silent Gen.

This mid-adulthood hump (as we're choosing to refer to it) shows up all over the place. Want to know if security feels achievable? It peaks with Millennials (75%) and bottoms out with Baby Boomers (67%). Think staying secure is possible? Millennials lead at 77%, while Baby Boomers and the Silent Gen sit at 71%.

In short: confidence in the ability to stay secure rockets up through early adulthood before sliding downward later in life (like so many things 🙄), even while the belief that security matters keeps marching upward as people age (Figure 2). Yet seeing security as worth the effort scales from 71% in Gen Z all the way up to 84% in the Silent Gen.

Figure 3. 'I feel that staying secure online is under my control' by generation.



Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

Is it easy, or just downright exhausting?

When it comes to perceptions of ease, the stats haven't changed much since last year. Exactly 58% of participants feel staying secure online is easy (identical to 2025), while those finding security info confusing dropped slightly from 45% to 43% (Figure 4).

However, there's a sting in the tail:

- 49% of participants feel completely overwhelmed by the sheer flood of online security information and advice out there.
- 50% confess that online security anxieties have forced them to limit what they do online.

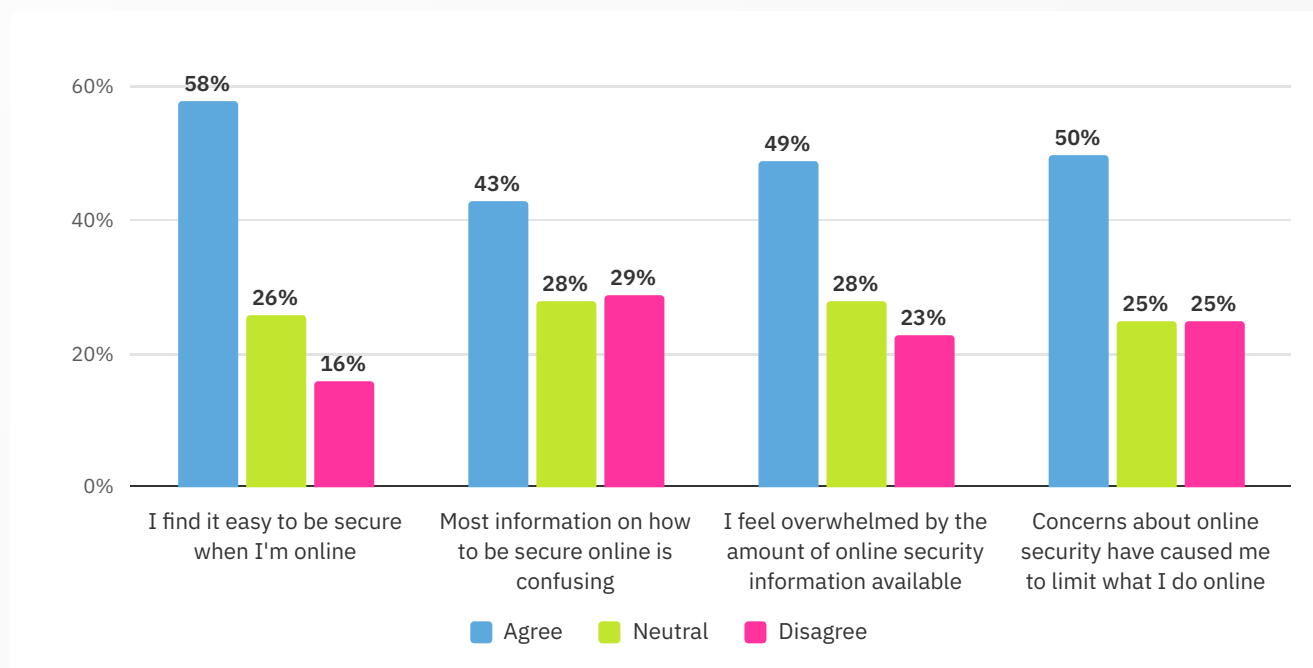
It doesn't take a detective to connect those dots (although call us Columbo if you want): when people get hit with info overload, their ultimate defense mechanism is simply to pull back from digital life altogether.

49%

feel completely overwhelmed by the sheer flood of online security information and advice out there.

FIGURE 4

Figure 4. Participants' levels of agreement with online security ease, clarity, and impact.



Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

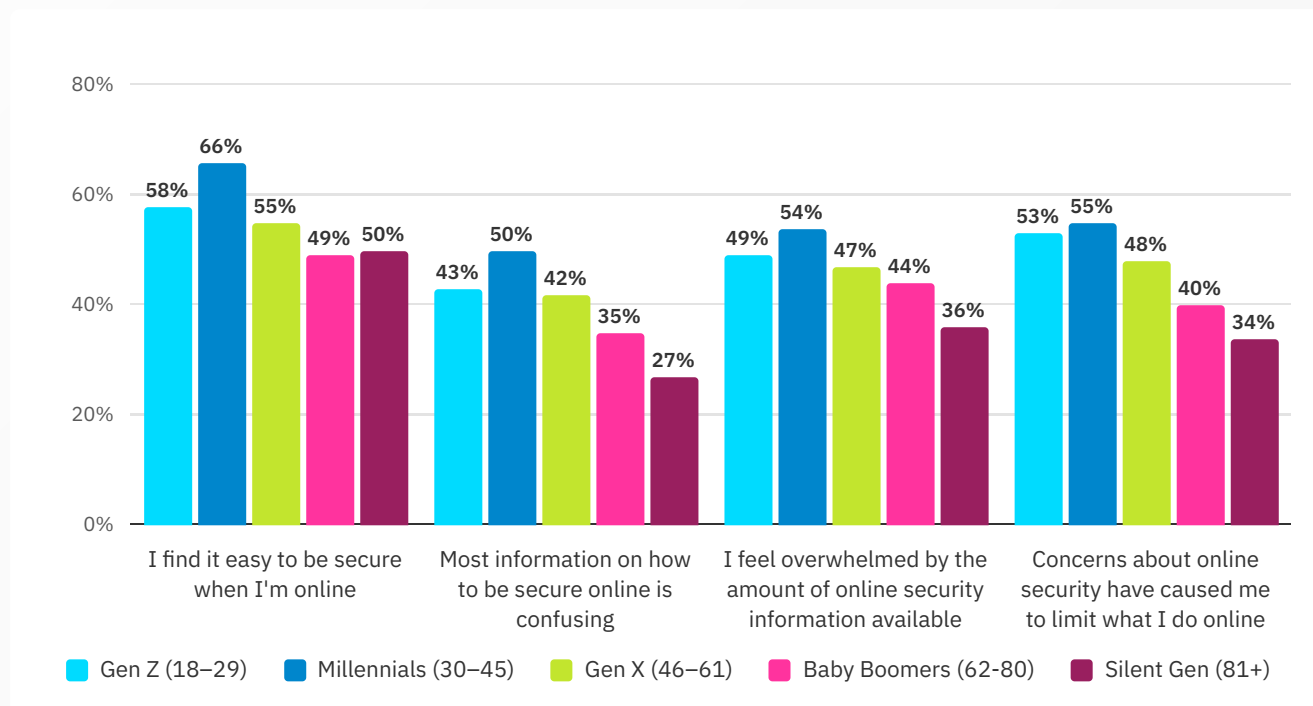
When we break these four experiences down by age group (Figure 5), they all trace the exact same rollercoaster arc seen in Figure 3, i.e., peaking with Millennials before dropping off among older folks*:

- Ease: Reaches its height with Millennials (66%) and hits bottom with Baby Boomers (49%).
- Confusion: Spikes at 50% for Millennials before plummeting to just 27% for the Silent Gen.
- Overwhelm: Peaks at 54% for Millennials and drops to 36% for the Silent Gen.
- Limiting online activity due to security concerns: Ranges from a high of 55% among Millennials down to 34% among the Silent Gen.

While it looks like older generations suffer far less friction and overload, don't celebrate just yet. This lower stress might simply mean they engage less with complex digital tools, rather than having cybersecurity superpowers.

*Older in relative terms. You're not old, you're wise. That's what we tell ourselves, anyway.

Figure 5. Participants' levels of agreement with online security ease, clarity, and impact, by generation.



Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

📌 KEY TAKEAWAYS: SUBCHAPTER 1.1

01

The vibes are mostly good:

People largely see online security as a priority, achievable and worth doing, though plenty still find it frustrating or intimidating.

02

Confidence lives right next to

overwhelm: Most people think security is easy, yet half are overwhelmed by instructions or limit their activity because of it, showing that confidence and burden go hand in hand.

03

Millennials are the most confident ...and the most

stressed (relatable): Confidence, overwhelm, and friction rise together through early adulthood, reach a fever pitch with Millennials, and then taper off in later years (control and overwhelm drop among the Silent Gen).

1.2 Misconceptions and concerns (tech myths and big brother fears)

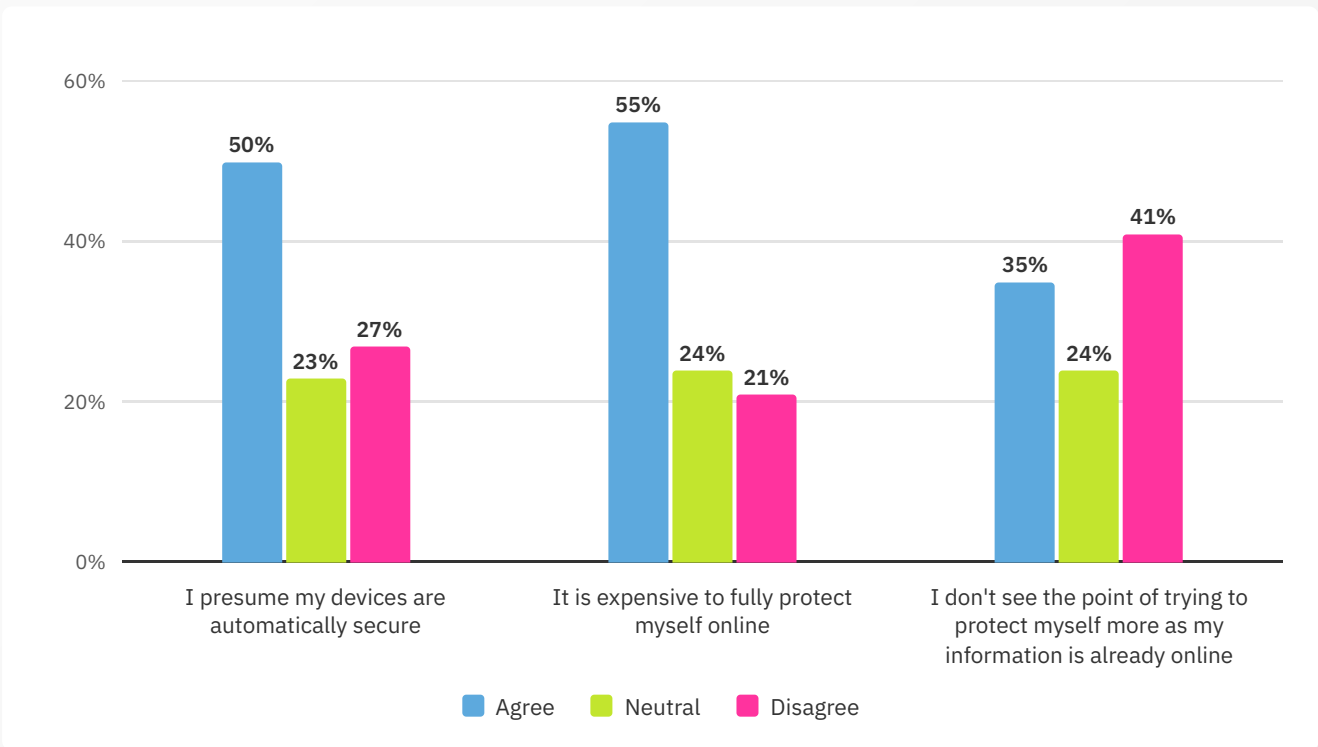
Tech myths die hard (like Bruce Willis) (Figure 6). Just like last year, a full 50% of participants assume their phones and laptops are automatically secure right out of the box.

Meanwhile, 55% (up 2% from 2025) complain that proper protection is way too expensive, and 35% (up 1% from 2025) have thrown their hands in the air, believing there's no point in trying to protect themselves more because their information is already online.

BRAIN SNACKS

This aligns closely with findings from Pew Research: while most people trust their own ability to make smart choices online, a majority remain skeptical that anything they actually do will make much difference.¹⁵

Figure 6. Perceptions of device security and cost of online protection.



Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

15 McClain, C., Faverio, M., Anderson, M., & Park, E. (2023, October 18). *How Americans View Data Privacy*. Pew Research Center. <https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/>

Big brother is watching ...but which one?

Worries over government app surveillance are everywhere (Figure 7). But here's the kicker: people are almost equally spooked by their own government as they are by foreign ones.

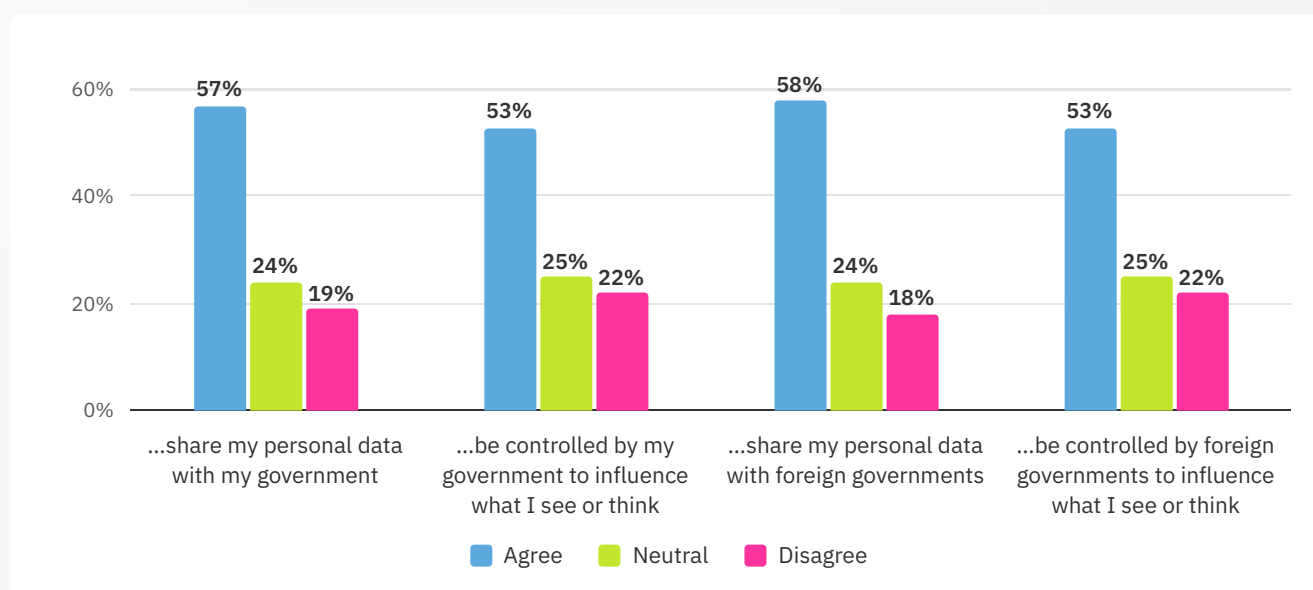
57% worry apps leak data to their home government, compared to 58% worrying about foreign governments.

53% fear apps are being used to secretly manipulate what they see or think – and that figure is identical (53%) for both domestic and international authorities.

BRAIN SNACKS

The fact that everyday folks hold the exact same level of skepticism toward their own leaders as foreign powers is an eye-opening reality check, but tracks with broader data trends: Pew Research notes that most Americans feel they have little or no control over how companies or governments handle their personal information, with government-specific privacy fears climbing steadily in recent years.¹⁵

Figure 7. 'I'm concerned that my apps may...'



Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

Generational paranoia

Concern about misuse of apps isn't spread evenly across generations (Figure 8). Millennials are the most concerned generation on every measure, from apps being used to share data with their own (62%) and foreign governments (62%), to apps being used by their own (60%) and foreign governments (59%) to influence what they see or think.

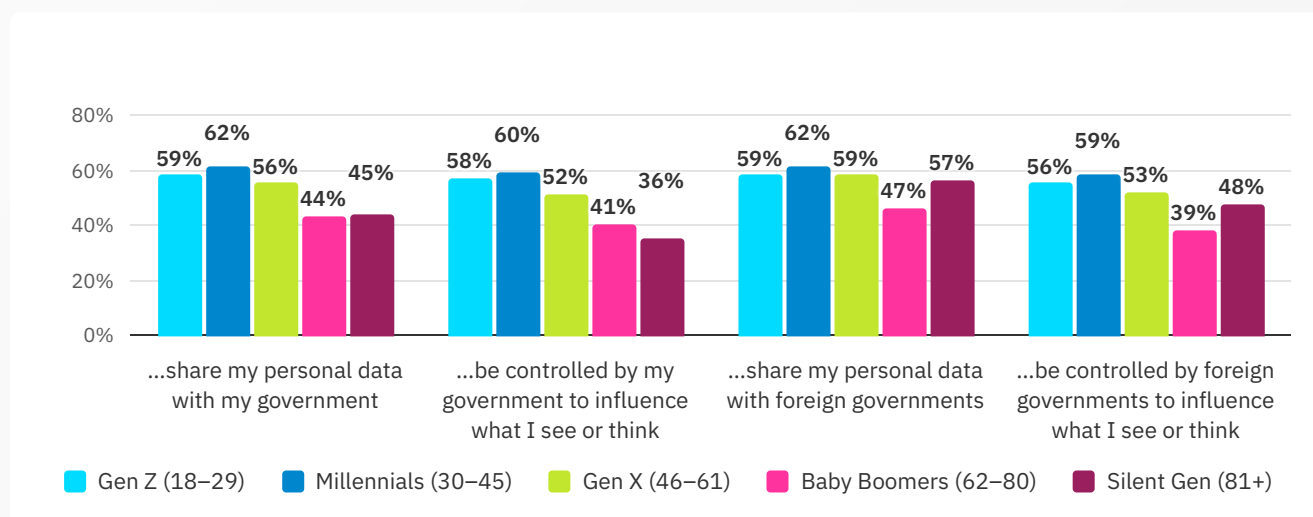
MAIN FINDINGS 1. ATTITUDES, BELIEFS & PERCEPTIONS ABOUT ONLINE SECURITY

Baby Boomers, on the other hand, have the lowest concern about apps being used for data sharing with either government (44% domestic, 47% foreign), and about apps being used to influence them on behalf of a foreign government (39%).

When looking at concern about apps sharing personal data with domestic versus foreign governments:

- Younger generations are equally concerned about domestic and foreign governments: Gen Z (59% for both) and Millennials (62% for both).
- Older generations are more concerned about foreign governments than their own: Gen X (59% foreign vs. 56% domestic), Baby Boomers (47% foreign vs. 44% domestic), and the Silent Gen (57% foreign vs. 45% domestic).

Figure 8. 'I'm concerned that my apps may...', by generation.



Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

📌 KEY TAKEAWAYS: SUBCHAPTER 1.2

01

Old myths are alive and kicking:

Half of all adults assume their devices protect themselves, more than half think fully protecting themselves online is expensive, and over a third see no point in doing more because their data is already out there.

02

Equal-opportunity distrust:

Concern about apps sharing personal data, or being used to shape what people see or think, is nearly identical whether it's done by a domestic or foreign government.

03

Millennials lead the panic:

Millennials show the highest paranoia overall across both domestic and foreign fronts, whereas the Silent Gen is the generation most wary of foreign governments compared to their own.

1.3 The 9-to-5 security tightrope: Cybersecurity culture in the workplace

Workplace culture is such a massive beast that it deserves its own report, but as an alternative to that, we still wanted to include a dedicated section following the journey we started in last year's report.

In that spirit, and armed with a brand-new set of questions, we uncovered some fascinating office dynamics (and we're not talking blossoming romances around the water cooler ...not this time, anyway).

So, what is cybersecurity culture anyway? The UK's National Cyber Security Centre (NCSC) puts it brilliantly:

*'The collective understanding of what is normal and valued in the workplace with respect to cybersecurity. It sets expectations on behavior and relationships, influencing people's ability for collaboration, trust, and learning.'*¹⁶

Understanding these cultural elements is crucial for assessing an organization's true security posture. Our findings shed light on how participants perceive their workplace's cybersecurity environment.

How does the office stack up?

Our survey of working adults ($n = 3,269$) shows that employees genuinely feel their companies care about security (Figure 9):

- 64% say good cyber habits are deeply embedded into daily operations.
- 60% report that senior executives visibly champion cybersecurity.

BRAIN SNACKS

To give some real-world context to that, the UK Government's Cyber Security Breaches Survey 2025/2026¹⁷ found that 72% of businesses and 60% of charities rated cybersecurity as a top priority for leadership (though keep in mind, the survey reflects organizations assessing themselves, rather than employees assessing leadership from outside).

Here's the plot twist: 48% of workers openly identified internal staff (their own coworkers, and indeed themselves) as a major security threat, whether due to honest mistakes or malicious intent.

16 UK National Cyber Security Centre (NCSC). (2025, June 4). *Cyber security culture principles*. NCSC.GOV.UK. <https://www.ncsc.gov.uk/collection/cyber-security-culture-principles>

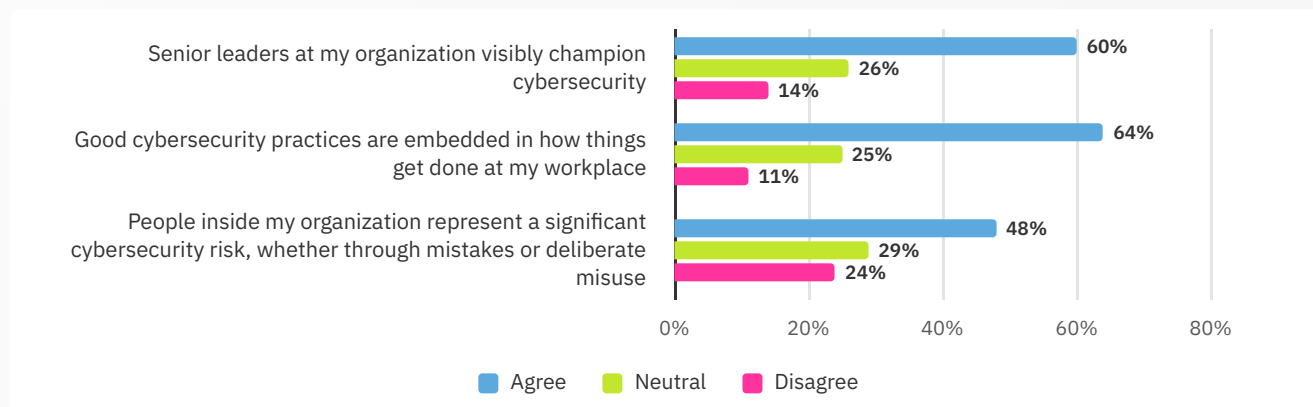
17 Department for Science, Innovation and Technology, & Home Office. (2026, April 30). *Cyber security breaches survey 2025/2026*. GOV.UK. <https://www.gov.uk/government/statistics/cyber-security-breaches-survey-20252026/cyber-security-breaches-survey-20252026>

MAIN FINDINGS 1. ATTITUDES, BELIEFS & PERCEPTIONS ABOUT ONLINE SECURITY

So, employees clearly recognize that the biggest security risk isn't just an abstract hacker, wearing a black hoodie in a darkened room (as they are so oft' portrayed) ...it's the person sitting at the desk next to them, with a photo of their dog, and a small cactus on their desk.

This shows people get it: they and their teammates play a very real part in company risk, rather than just appearing as some abstract rule in the employee handbook (which, let's be honest, only a few people ever read). 🧐

Figure 9. Attitudes toward cybersecurity in the workplace.



Base: US, UK, India, Brazil, Singapore. Total number of participants: 3,269 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

The Millennial workplace lens

Consistent with the pattern seen elsewhere in this chapter, Millennials report the highest confidence in their organization's practices:

- They're the most confident in leadership's commitment (66%, compared to 54-56% for other generations¹⁸).
- They're the most likely to say security is built into everyday tasks (70%, compared to 58-62% for others).
- They're also the most eagle-eyed regarding insider threats (53%, compared to 39-47% for others).

📌 KEY TAKEAWAYS: SUBCHAPTER 1.3

01

Leaders get high marks, but coworkers get side-eyed: Most employees feel leadership champions security and good practices are embedded in their organizations, yet nearly half also see colleagues as a genuine risk.

02

Millennials see both the best and worst at work: They're the generation most likely to believe leadership champions security and good practices are embedded, and also the generation most likely to see colleagues as a risk.

¹⁸ Only asked of employed participants. Silent Gen excluded due to insufficient sample size ($n = 1$).

1.4 Doomscrolling and media hype

News headlines love a juicy cyberattack story, but how does all that media noise affect real-world habits?

On the bright side (Figure 10):

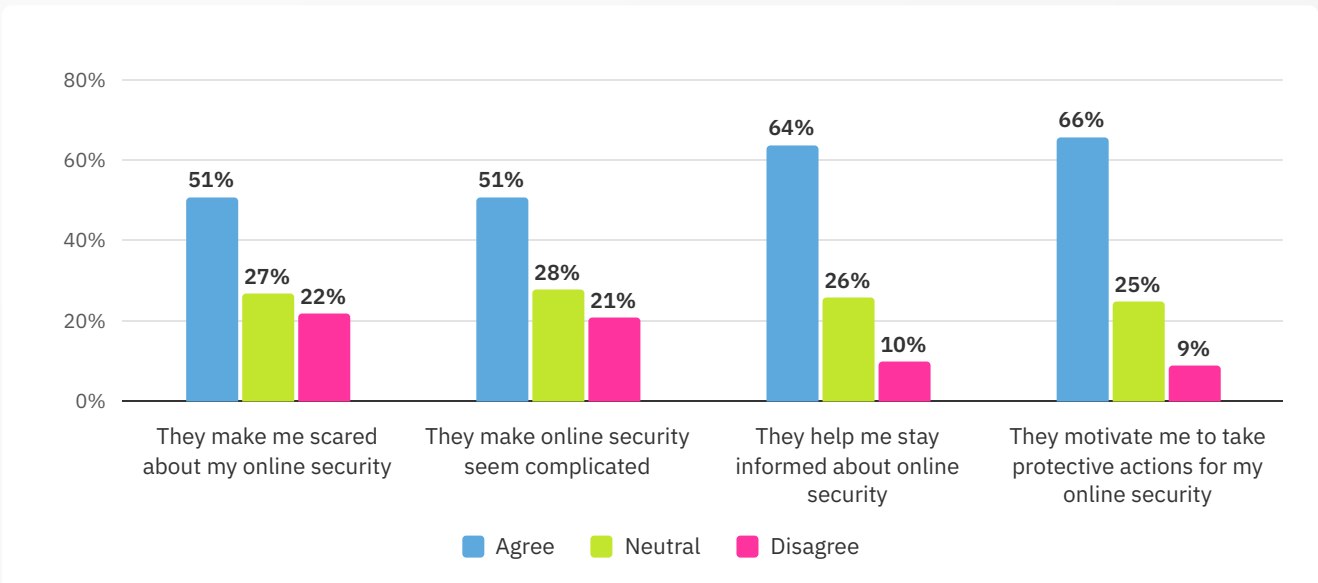
- 66% say news coverage motivates them to take protective action (up 1% from 2025).
- 64% say it helps them stay informed (up 2% from 2025).

On the flip side:

- 51% confess news stories make them scared about online safety (down 3% from 2025).
- 51% feel news coverage makes cybersecurity seem overly complicated (down 4% from 2025).

All in all, the trajectory since 2025 is remarkably positive: the constructive impacts are rising, while fear and confusion are dropping. 🎉

Figure 10. ‘What impact does the media/news have on your views toward online security?’



Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

Turning news into action

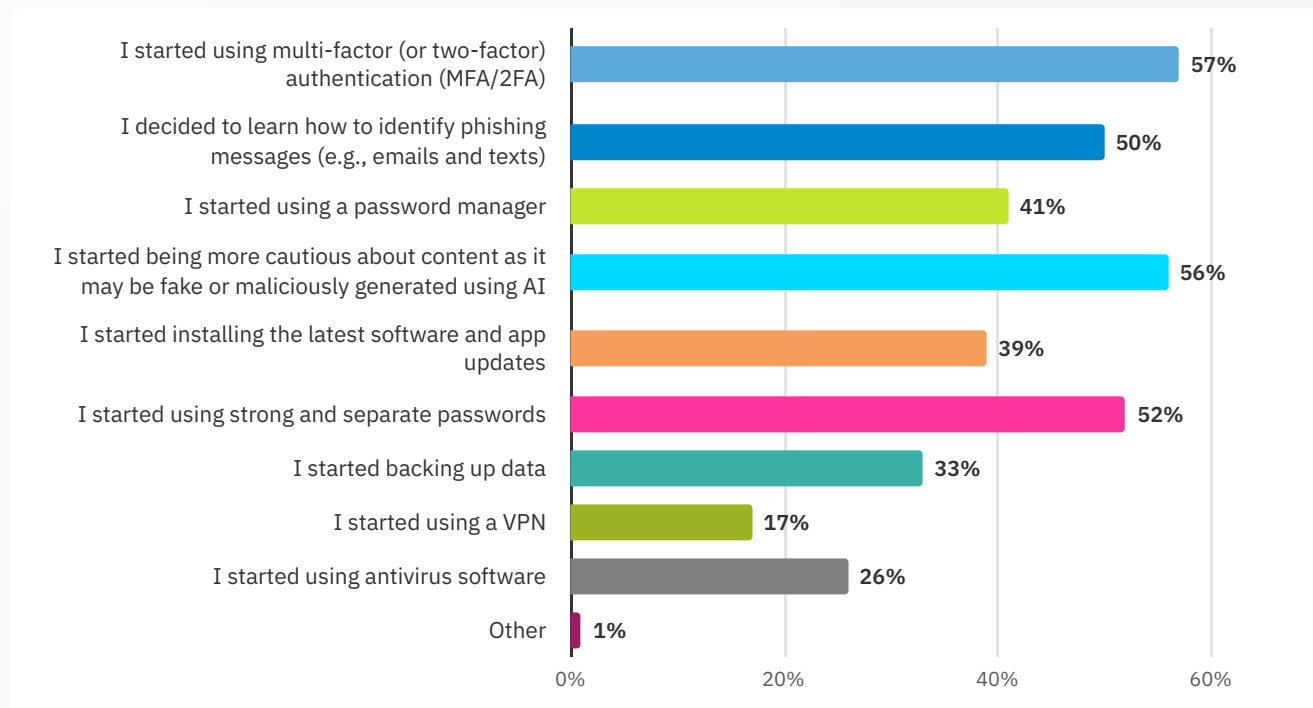
When the news does manage to spur people into action ($n = 3,931$), what steps are they actually taking (Figure 11)?

- Setting up MFA: 57% (a huge 9% surge from 2025).
- Staying alert for fake or AI-generated content: 56% (up 5% from 2025).
- Using unique, strong passwords: 52% (up 1% from 2025).
- Learning to spot phishing scams: 50% (up 5% from 2025).

MAIN FINDINGS 1. ATTITUDES, BELIEFS & PERCEPTIONS ABOUT ONLINE SECURITY

Every single security action increased compared to 2025. It's particularly awesome to see AI-threat awareness skyrocket to the #2 spot, proving that media chatter is successfully training the public to spot deepfakes and AI tricks.

Figure 11. Impact of media coverage on motivating protective online security actions.



Base: US, UK, India, Brazil, Singapore. Total number of participants: 3,931 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

KEY TAKEAWAYS: SUBCHAPTER 1.4

01

A double-edged sword that works: Roughly two-thirds say the media motivates them to take protective steps and keeps them informed about online security, and around half say it scares them or makes online security seem complicated.



Chapter 1 summary cheat-sheet

Optimism reigns supreme: Most people view security as a priority (83%), achievable (70%), and worth the effort (77%), though a notable number still find it frustrating (40%) or intimidating (39%).

Persistent myths: Half of adults think devices protect themselves automatically, 55% think protection is too pricey, and 35% don't see the point of trying to protect themselves more, as their information is already online.

Government distrust is equal-opportunity: People are just as distrustful of their own government as of foreign ones. Concern about apps sharing personal data (57% own, 58% foreign) or shaping what people see or think (53% both) is nearly identical in either direction.

Workplace reality: Workers believe good practices are embedded (64%) and bosses champion security (60%), but 48% view their own colleagues as walking risk factors.

Media drives real action: News motivates protective steps (66%) and keeps people informed (64%), even as it fuels fear (51%) and complexity (51%); among those it motivates, adopting MFA (57%) and caution about AI-generated content (56%) are the most common actions.

GENERATIONAL HIGHLIGHTS

The Millennial paradox: Millennials report feeling the highest sense of control, with 66% saying they find it easy to stay safe online. Yet they also suffer from the highest levels of info overload (54%), government data fears (62%), and 53% say they're most likely to see their own colleagues as a workplace security risk.

2. Reliance and responsibility (AKA teamwork and who the buck stops with)

Who do we call when tech goes haywire? Who's leaning on us for help? And when a breach happens, who's taking accountability?

Understanding these helper/helpee relationships is the key to designing security strategies that *actually* work in the real world. After all, digital safety isn't an isolated, solo journey – it's a team sport woven right into our families, workplaces, and social circles. (Which makes digital security sound more fun than it is, but we're nothing if not optimists).

This chapter breaks down two major ideas:

- Reliance: How much we depend on others for cyber help, and who relies on us.
- Responsibility: Who we believe should *actually* be on the hook for keeping our personal and company data safe.

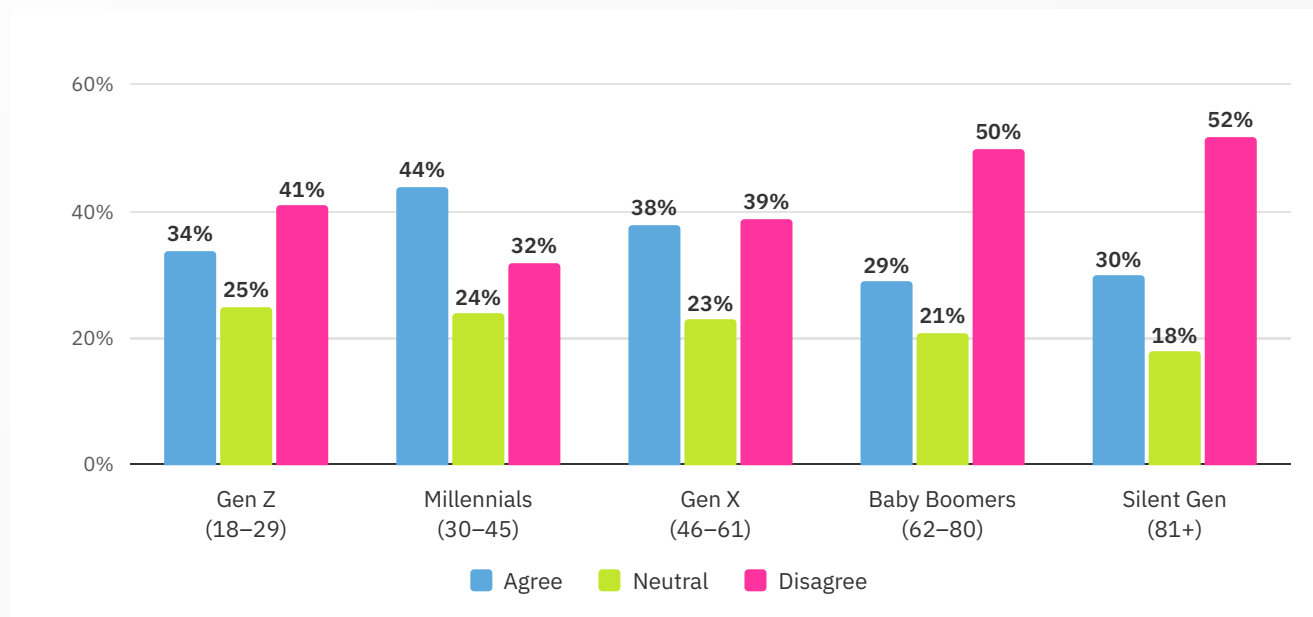
2.1 Calling for backup: Who's helping who?

More people are leaning on outside help this year. Overall reliance on others for staying safe online rose to 37% (a 2% bump from last year, following a 3% increase the year before).

Looking across age brackets (Figure 12), Millennials (44%, +2%) and Gen X (38%, +5%) rely on others the most. Gen Z (34%) was the only group where reliance actually dropped (-2%).

Meanwhile, Baby Boomers (29%) and the Silent Gen (30%) rely on others the least, though their reliance is actually growing faster than that of younger age groups (+4% and +2% respectively since 2025).

Figure 12. ‘I rely on others (e.g., family, colleagues) to keep me secure online’ by generation.



Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

Who are we calling for help? (Hint: it’s not Ghostbusters)

When we asked the reliant group ($n = 2,330$) who they turn to when tech gets scary, the answers were loud and clear:

- Family: 63% (The undisputed #1 helpdesk. And they have snacks.)
- IT companies: 39%
- Friends: 37%
- Government: 31%
- Work colleagues: 29%

“ **‘I will do whatever my advisor suggests.’**

P4796, UK

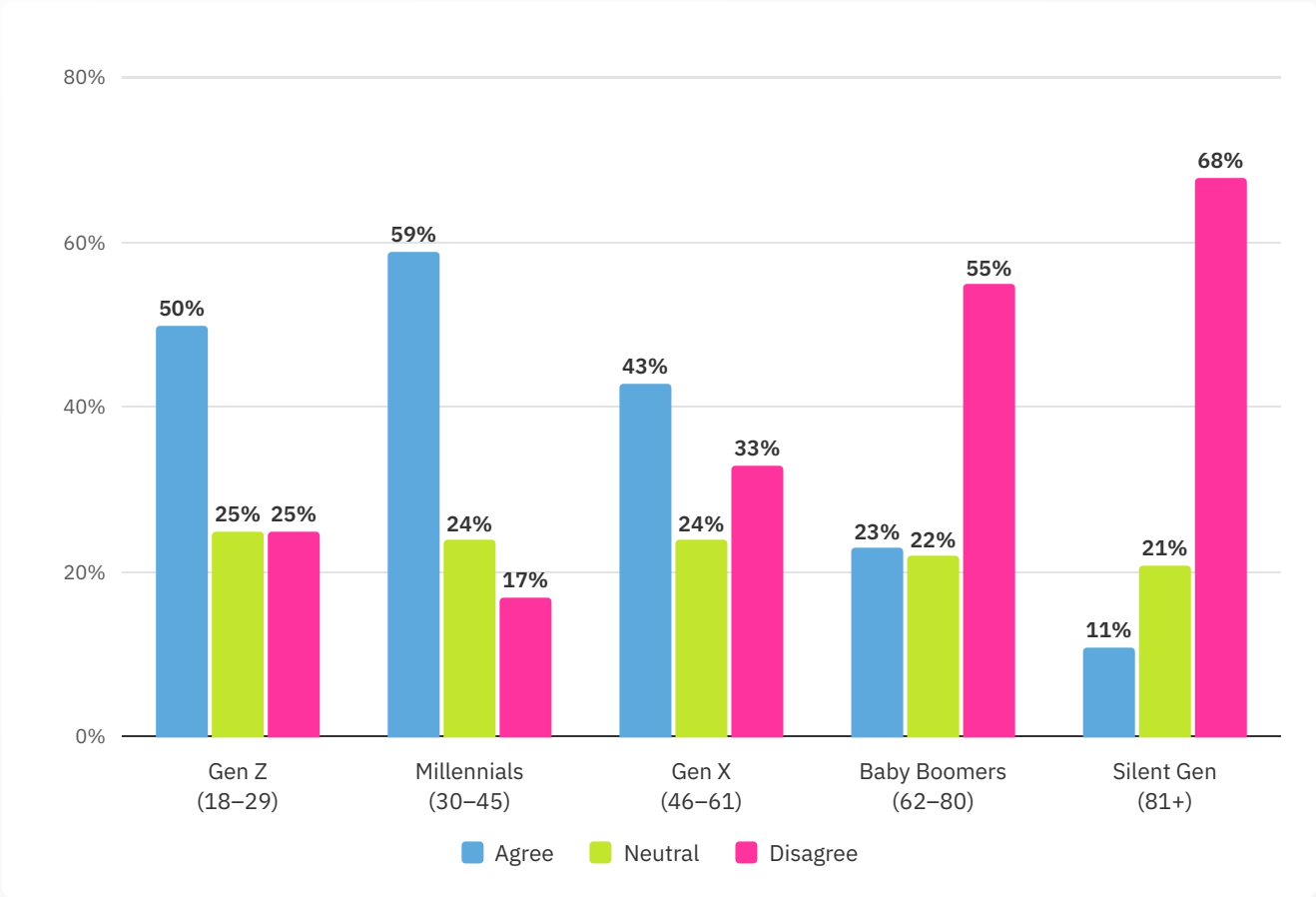
Is it a bird? Is it a plane? No! It’s the unsung IT heroes

On the flip side, 45% of all participants (down 1% from 2025) reported that other people depend on them to stay safe online (Figure 13).

Once again, Millennials (59%, +1% from 2025) and Gen Z (50%, -4%) act as the designated (unpaid and unqualified 🤖) cybersecurity resource and tech support for their friends and families. By comparison, 43% (-2%) of Gen X, 23% (-2%) of Baby Boomers, and 11% (-7%) of the Silent Gen reported being relied on by others.

This highlights a clear trend, as seen in Figure 12: older adults are both the least likely to ask for help and the least likely to be asked.

Figure 13. ‘Others (e.g., family) rely on me to keep them secure online’ by generation.



Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

📌 KEY TAKEAWAYS: SUBCHAPTER 2.1

01

More givers than receivers:
Nearly half of adults act as tech caretakers for others, while just over a third admit to needing help themselves.

02

Family over tech support: When people need help, most go straight to family members over professional tech companies or friends.

03

Older adults live on a digital island: Baby Boomers and the Silent Gen sit at the bottom for both seeking help and giving it out, standing apart from the other generations, who show more reliance in both directions.

2.2 Who’s on the hook?

Personal vs. office data

To better understand people’s relationship with cybersecurity, we asked them about who they think is responsible for keeping their information out of the wrong hands ...and specifically the protection of their personal and workplace information.

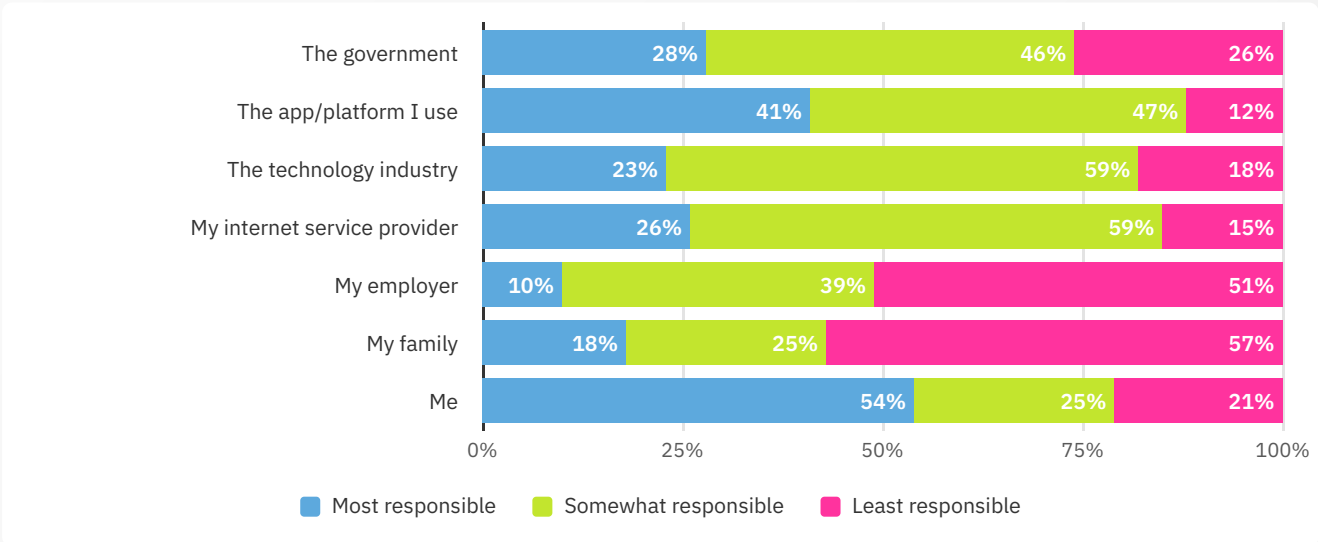
Personal data? It's on me

When it comes to personal info (Figure 14), people overwhelmingly hold themselves accountable (54%, down 4% from 2025):

- Myself: 54%
- The app/platform used: 41% (down 1%)
- The government: 28% (up 4%)
- Internet service providers (ISPs): 26% (down 3%)
- Family: 18% (up 1%)
- Employers: 10% (same as 2025)

Notice anything interesting? The government officially overtook ISPs to claim this year’s #3 spot. This may reflect a growing public appetite for government involvement in data protection more broadly: in the US, 72% say there should be more regulation of how companies handle personal data.¹⁵

Figure 14. ‘Who is most responsible for protecting your personal information?’



Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

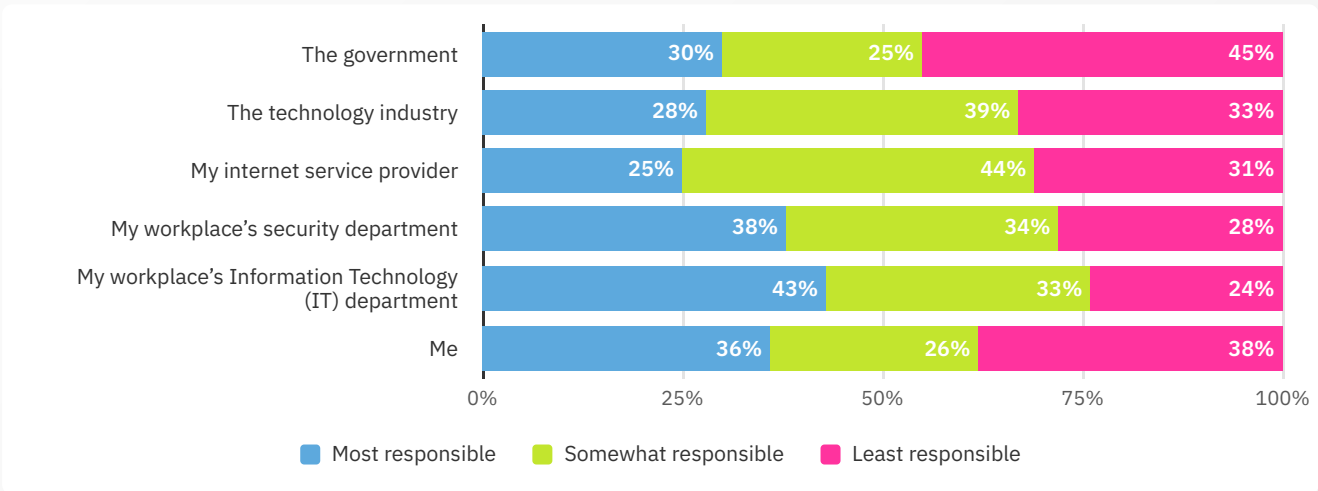
Workplace data? Call IT!

When shifting the focus to company data ($n = 3,269$), personal accountability drops into third place as employees pass the torch to dedicated professionals (Figure 15):

- 1. IT department: 43%
- 2. Security department: 38%
- 3. Myself/individual employee: 36%
- 4. Government: 30%
- 5. Tech industry at large: 28%
- 6. Internet service providers: 25%

Just like personal data, public expectation for government involvement at work ticked upward (30%, +2% from 2025).

Figure 15. ‘Who is most responsible for protecting your workplace’s information?’



Base: US, UK, India, Brazil, Singapore. Total number of participants: 3,269 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

📌 KEY TAKEAWAYS: SUBCHAPTER 2.2

01

Personal vs. work split: People take primary responsibility for their personal data, but gladly pass the torch to IT and security teams when sitting at their office desks.

02

Personal first, platforms second: While people hold themselves most responsible for protecting personal information, apps and platforms rank next – far ahead of family members, the tech industry or internet service providers.



Chapter 2 summary cheat-sheet

The reliance paradox. More helpers than seekers. Close to half (45%) report that others actively rely on them to keep their digital lives safe, compared to only 37% who admit to relying on others.

Family comes first (sorry, tech support). Of those who say they need a hand with cybersecurity, 63% turn to family first. Official IT companies (39%) and friends (37%) follow well behind, while the government (31%) and coworkers (29%) round out the bottom.

Personal data: you're on your own. For personal data, people look at themselves (54%) as the #1 responsible party for their privacy, followed by the apps and platforms (41%) they use. The government (28%) overtook ISPs (26%) as the third most responsible party, while family (18%) and employers (10%) are seen as the least responsible.

Workplace information: passing the torch. When switching to company data, employees pass responsibility to the experts: the IT (43%) and Security departments (38%). Interestingly, 36% of workers still place personal responsibility near the top, ranking individual effort higher than external players like the government (30%), the tech industry (28%), or ISPs (25%).

GENERATIONAL HIGHLIGHTS

The silent lone rangers. Older generations are both the least likely to rely on others and the least likely to be relied upon. Baby Boomers (29% reliant, 23% relied upon) and the Silent Gen (30% reliant, 11% relied upon) sit at the bottom on both measures, standing apart from hyper-connected Millennials and Gen Z, who show more reliance in both directions.

Unsurprisingly, Millennials (59%) and Gen Z (50%) act as the primary family helpdesk, though Gen Z was the only generation where needing help actually dropped.

3. Cybercrime victimization & reporting

When it comes to cybercrime, the question at the heart of the matter is: how do people *actually* view their own risk? Do we secretly think we're invisible to scammers, or are we constantly looking over our shoulders?

This chapter unpacks those attitudes. We look at our collective resignation toward losing money or data online (a sad state of affairs, but sadly indicative of the number of times we've all been burned in one way or another), alongside how much faith we actually put in modern cyber defenses.

From there, we dive into the hard numbers, i.e., tracking victimization rates across classic threats like phishing, identity theft, online dating scams, crypto fraud, and tech support traps.

Then, we shine a spotlight on some fresh additions to this year's list (like job scams, delivery scams, online marketplace scams and lottery/prize scams ...all the fun stuff). And to wrap it all up, we take a deep dive into reporting rates (and why so many people stay silent) as well as the ongoing reality of cyberbullying.

Some of it is a bit gloomy, we grant you. But looking into this stuff more closely is how we prevent these shiesters from getting one over on us, our businesses and our hard-earned data (and bank accounts). So it's well worth sifting through the grim facts of the matter.

Here's how we're breaking it down:

3.1 Attitudes toward victimization: Panic, paralysis, or peace of mind?:

Public worry, personal risk perception, digital resignation, and faith in law enforcement and cyber defenses.

3.2 Cybercrime in the wild: How bad is it *really*?: Victimization rates across traditional and emerging scam tactics, demographic breakdowns, high-tech deepfake threats, and the emotional aftermath.

3.3 Cybercrime reporting: Who speaks up, who stays silent, and why?:

Incident reporting frequencies across different crime types, where victims turn for help, and the underlying barriers to coming forward.

3.4 Cyberbullying: The digital shadow: Prevalence and generational spreads of online harassment, alongside the channels victims use to report it.

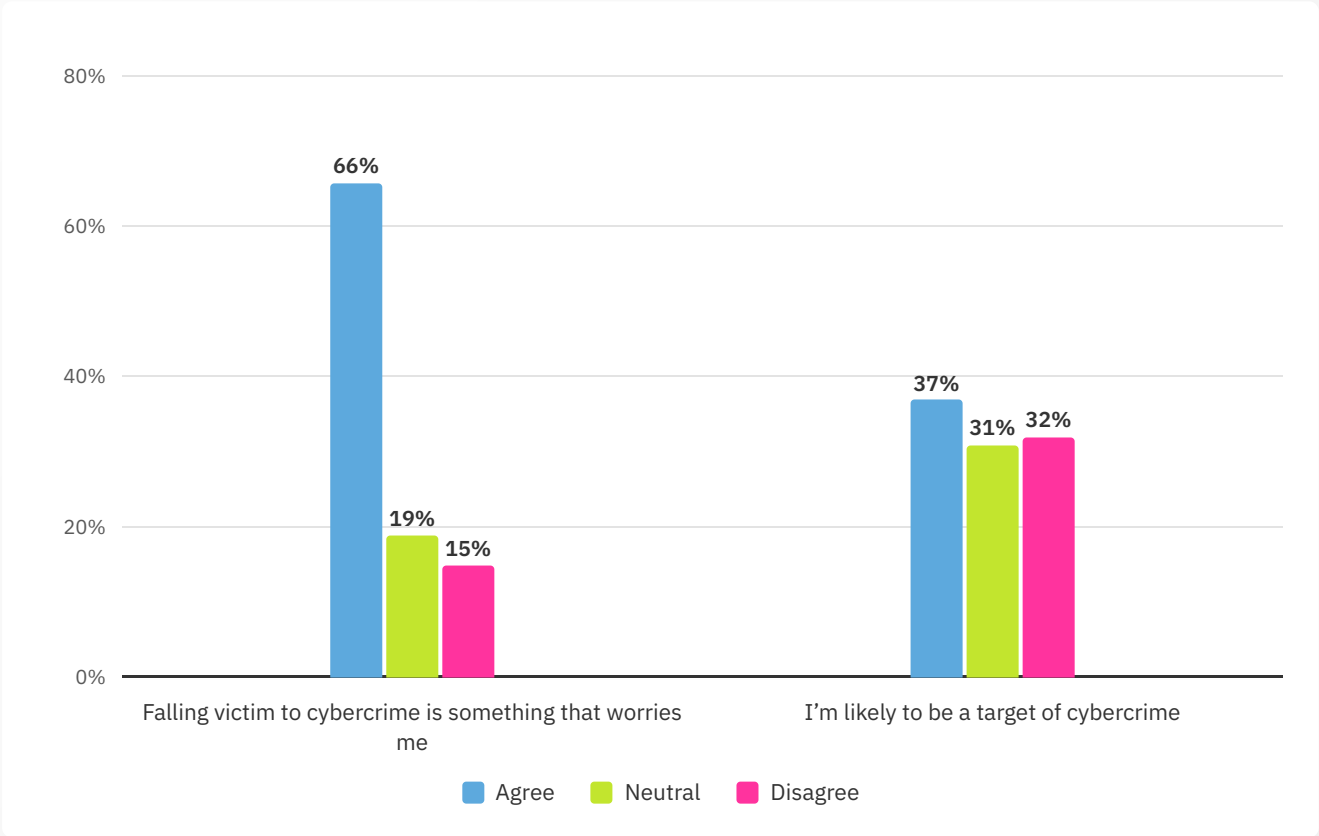
3.1 Attitudes toward victimization: Panic, paralysis, or peace of mind?

How much sleep are people actually losing over cybercrime? This subchapter checks the pulse on public worry, personal risk perception, digital resignation, and whether anyone actually trusts law enforcement, security tech, or other defenses to be on the ball and save the day.

Let’s kick off with how people feel about their odds:

- 66% of participants worry about falling victim to a cybercrime (-2% from 2025).
- 37% believe they are likely targets of cybercrime (-4% from 2025, Figure 16).

Figure 16. Attitudes toward victimization.

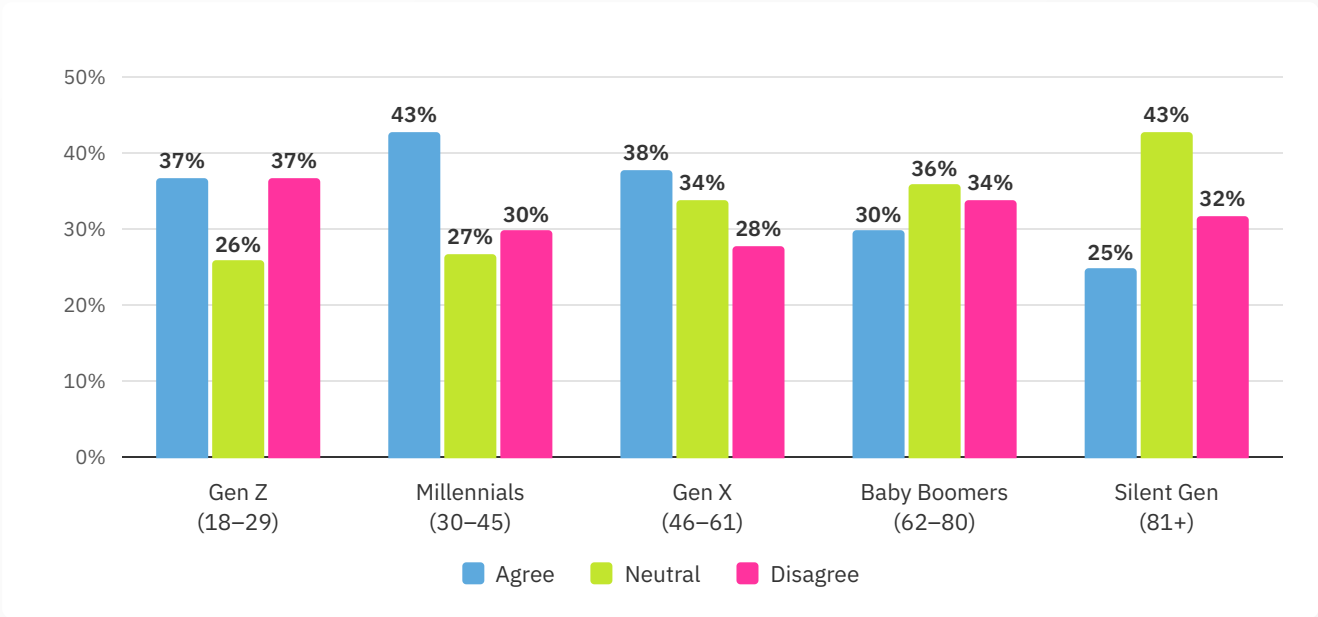


Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

Target on my back? The generational divide

While worry levels stayed pretty steady across age groups (ranging from 61% for Baby Boomers to 68% for Millennials), things got much more split when asking people if they feel like painted targets (Figure 17): This belief is highest among Millennials (43%), followed by Gen X (38%) and Gen Z (37%), and only 25% of the Silent Gen think of themselves as likely targets.

Figure 17. ‘I’m likely to be a target of cybercrime.’ by generation.



Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

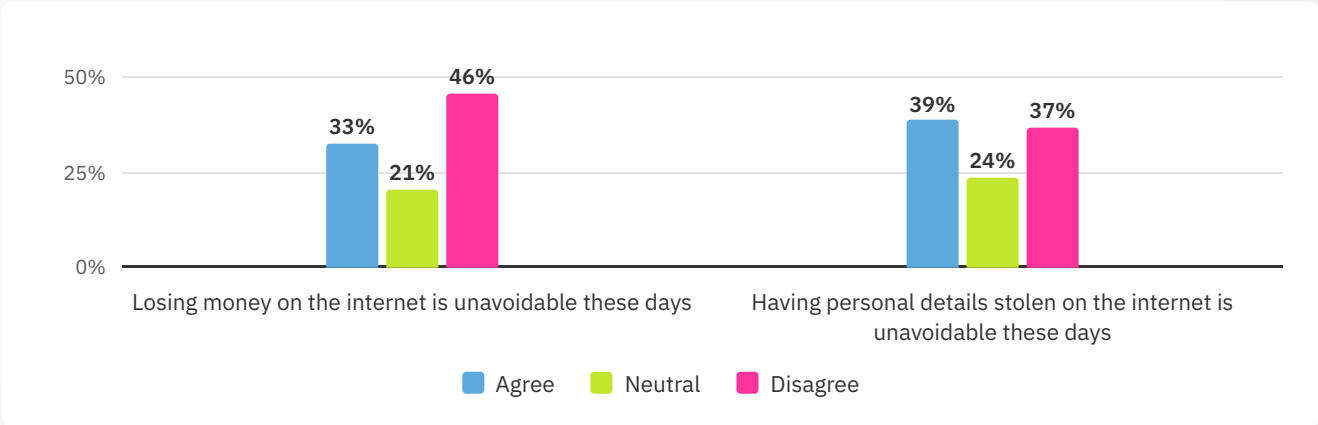
Digital doomism: ‘Losing data is just life now’

It seems a lot of us have thrown our hands up in the air in despair* (Figure 18):

- 33% of participants (+2% from 2025) feel that losing money on the internet is completely unavoidable.
- 39% (-1% from 2025) feel the exact same way about having their personal data stolen by criminals.

*As opposed to throwing our hands in the air like we just don’t care. Which is, I think we can all agree, much more fun.

Figure 18. Perceptions on the avoidability of losing money or personal details on the internet.



Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

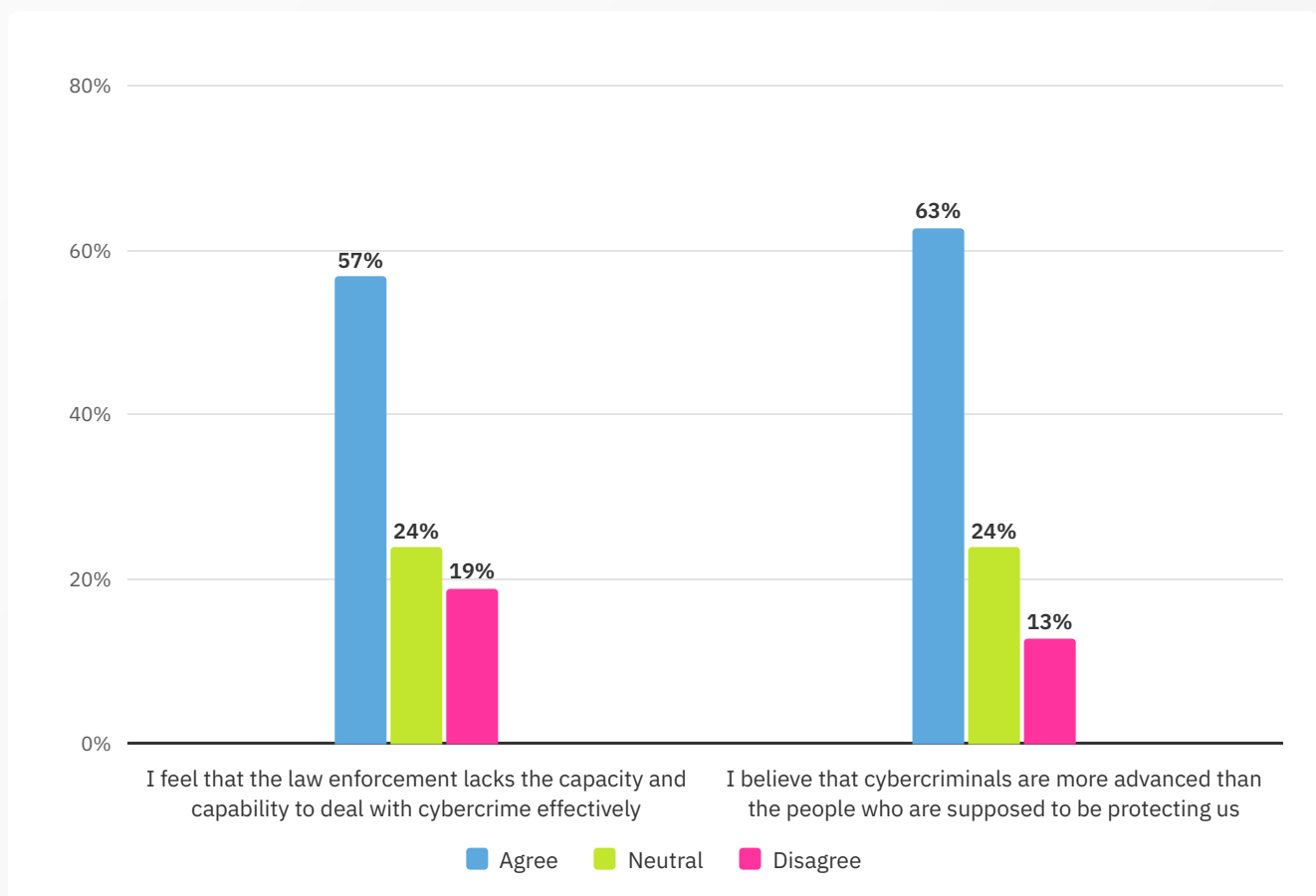
Let's get skeptical, skeptical*

When evaluating the actual armor we have against cybercriminals, participants expressed plenty of doubt (Figure 19):

- 57% (-7% from 2025) feel law enforcement lacks the capacity and capability to deal with cybercrime effectively.
- 63% (-6% from 2025) believe cybercriminals are simply more advanced than the people who are meant to be protecting us.

*To be internally read/sung to the tune of Olivia Newton-John's *Let's Get Physical*. Obviously.

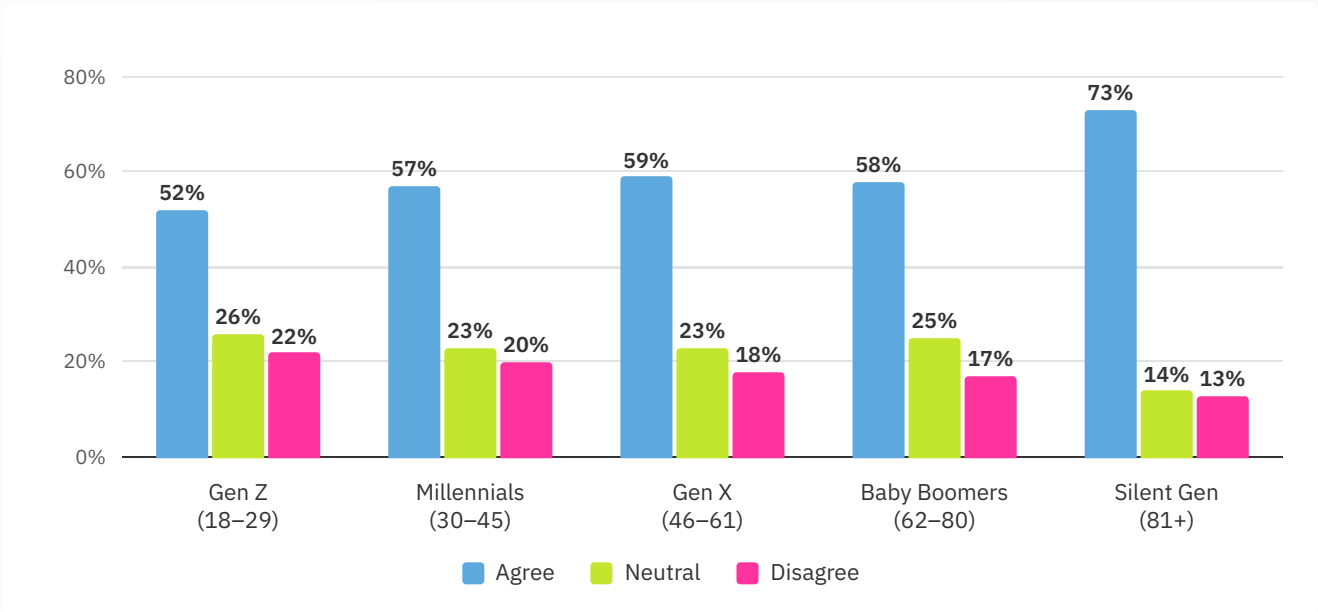
Figure 19. Perceptions of cybercrime defense effectiveness.



Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

Doubting law enforcement's digital toolkit seems to grow right alongside age (Figure 20). The Silent Gen was found to be the most skeptical by a long shot (73%), while Gen Z showed the most optimism, coming in as the least skeptical (52%).

Figure 20. ‘I feel that the law enforcement lacks the capacity and capability to deal with cybercrime effectively’ by generation.



Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

📌 KEY TAKEAWAYS: SUBCHAPTER 3.1

01

Worrying is more common than feeling targeted: Two-thirds of people worry about cybercrime, but only a little over a third actually expect to be picked out as a target.

02

Resignation is real, trust is low: A third or more view data and financial loss online as an unavoidable fate, while a clear majority feel cybercriminals are outsmarting defenses and leaving law enforcement outmatched.

03

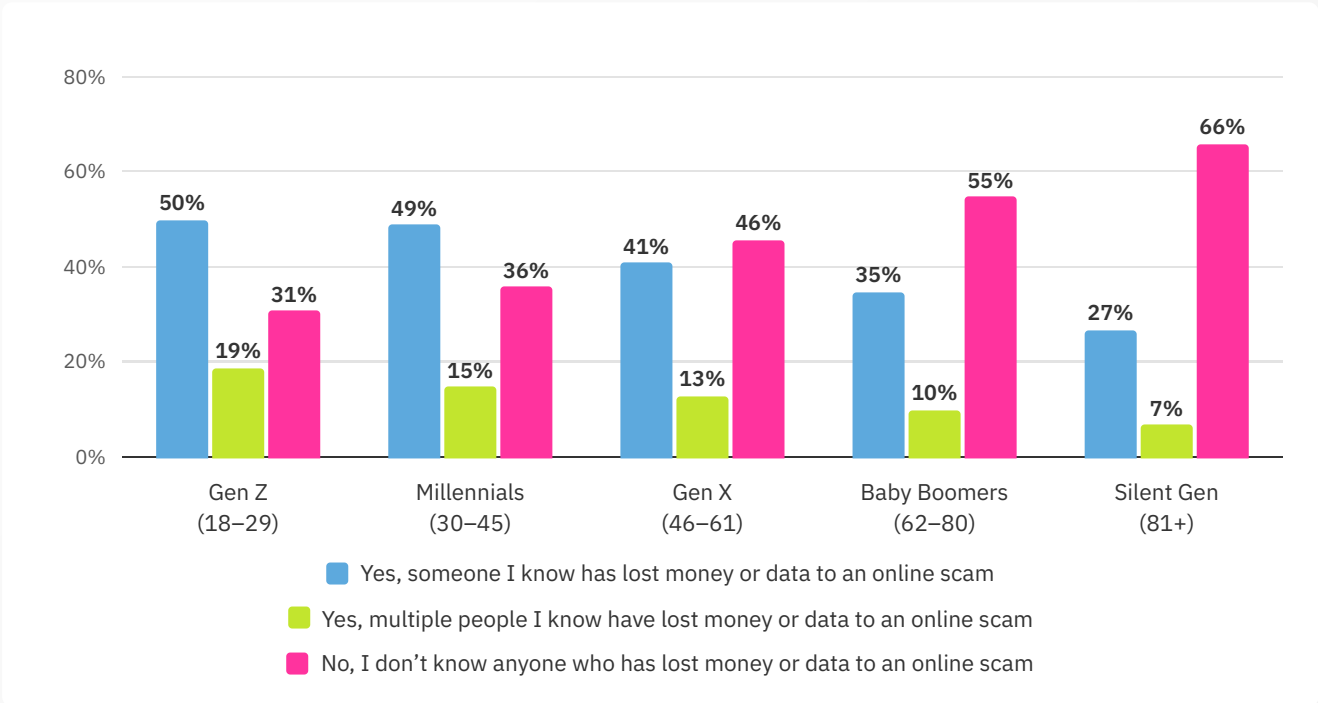
Generations swap seats on concern vs. confidence: Millennials feel the most personally targeted while Silent Gen feels the least. Flip to law enforcement confidence, though, and the roles reverse (Silent Gen is the most skeptical, Gen Z the least).

3.2 Cybercrime in the wild: How bad is it really?

Before we jump into everyone's personal horror stories 🧟 , here's a quick appetizer: 59% (+1% from 2025) of participants said they know at least one person in their personal circles who has been hit by cybercrime.

Break that down by generation, and a clear pattern shows up (Figure 21). Younger generations' social circles were far more likely to be victims (69% of Gen Z and 64% of Millennials) compared to older ones (45% of Baby Boomers and 34% of Silent Gen).

Figure 21. 'Has anyone you know been a victim of online scams where they have lost money or data?' by generation.



Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

Counting the casualties: The hard numbers

When asked about their own personal experiences, our survey group disclosed 5,662 separate cybercrime incidents¹⁹ that resulted in lost money or stolen data. (Ugh).

¹⁹ This survey measured nine specific types of cybercrime incidents: phishing scam, identity theft, online dating scam, cryptocurrency investment fraud, tech support fraud, job scam, delivery scam, online marketplace scam and lottery/prize scam. A free text 'Other' option was also provided to gather more insights and inform the cybercrime options provided in future *Oh, Behave!* reports.

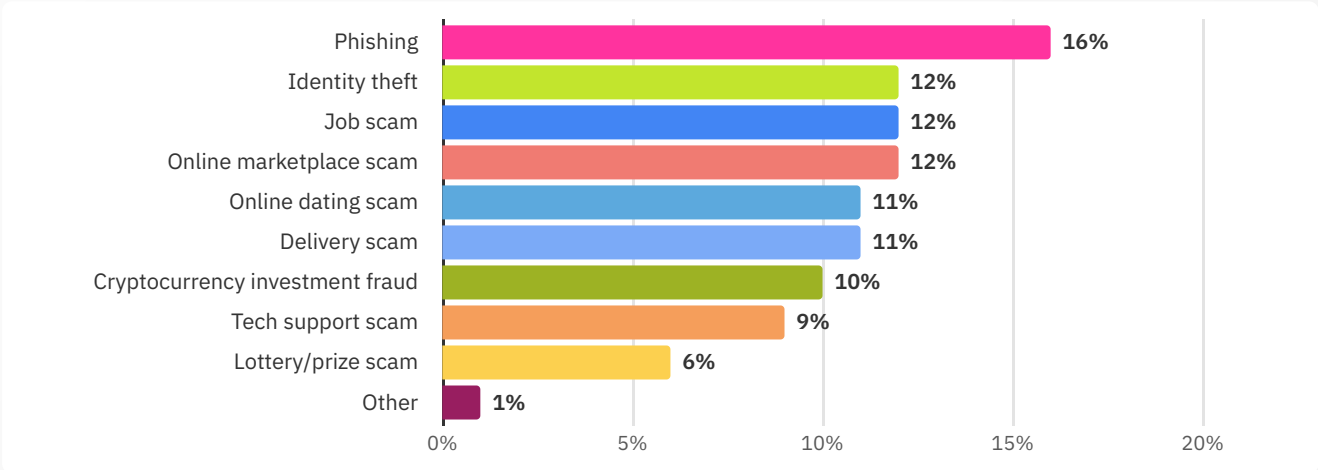
Altogether, 50% of participants have been personal victims of cybercrime, which spans phishing, dating scams, identity theft, crypto fraud, tech support traps, job scams, delivery scams, marketplace fraud, lottery schemes, and 'other' incidents. That's a 6% bump up from 2025.

Which scams hit the hardest?

Phishing stays on top 🦈 : Out of the 2,515 respondents who fell victim to online scams, 36% were baited by phishing, which holds steady with past trends.

Incident breakdown: Looking at the entire pool of 5,662 incidents resulting in loss of money or data (Figure 22), phishing racked up the highest share (16%), closely followed by a multi-way tie between job scams, identity theft, and online marketplace scams (12% each), with dating scams and delivery scams right behind (11% each).

Figure 22. Types of cybercrime incidents.



Base: US, UK, India, Brazil, Singapore. Total number of cybercrime incidents: 5,662 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

Unmasking the curveballs: The ‘other’ write-ins

To make sure no bad experience was left out (or indeed for those who felt the existing options didn’t align closely enough with their experiences), we gave respondents an ‘Other’²⁰ option where they could write about what happened. And we’re glad we did tbh, because the write-ins gave us a fascinating look into the fringe tactics scammers are using:

- **Financial account fraud:** Direct card details stolen for illicit online spree, or direct withdrawals from bank accounts without an explicit scam conversation.
- **Upfront/advance fee schemes:** Victims promised a tempting loan, reward, or payout ...provided they pay an ‘upfront fee’ that (unsurprisingly) ✨ magically disappears into thin air ✨.
- **Direct account hijacking:** Social media handles and online bank accounts getting broken into without warning.
- **Fake kidnapping calls:** Participants in Brazil specifically called out phone hoaxes demanding ransom for ‘kidnapped’ loved ones.
- **Impersonation schemes:** Scammers impersonating familiar contacts to beg for money (a trend we revisit shortly).

“ *‘I’ve had various attempts for things such as crypto fraud etc., but I spotted them. I have had someone creating a fake page on Facebook that wasn’t me.’*

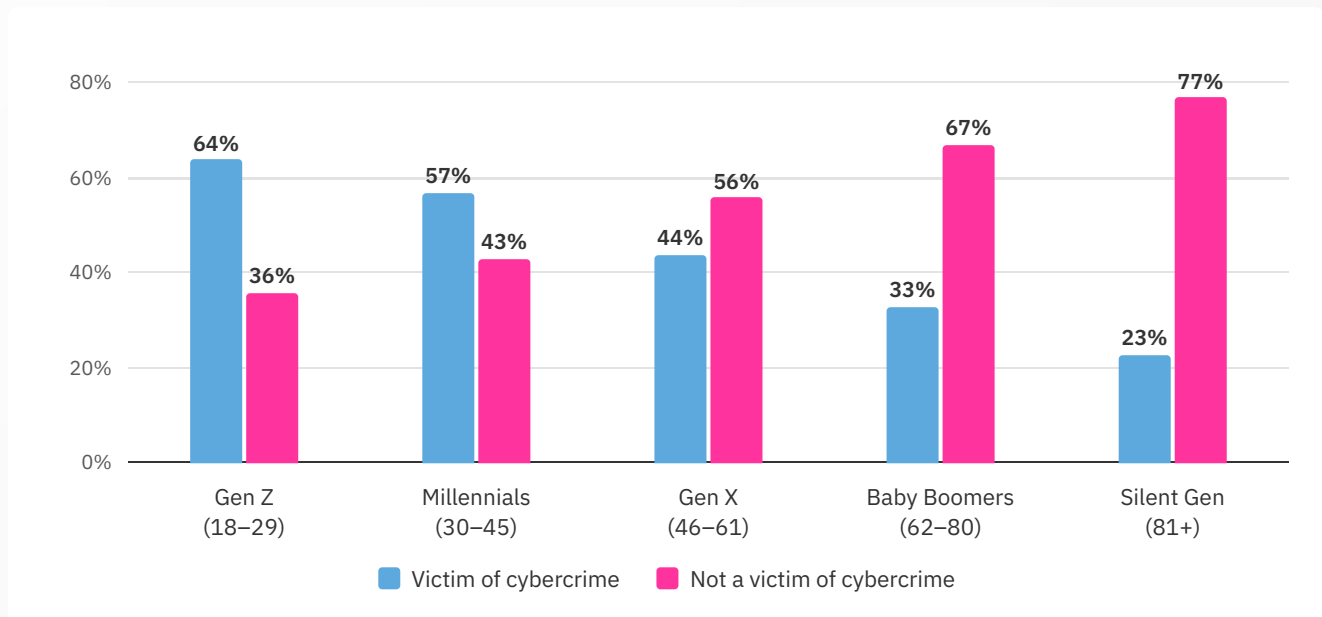
P2524, United Kingdom

Youth in the crosshairs: Who gets hit most?

Personal victimization skewed much higher for younger crowds and steadily dropped as age went up (Figure 23). Sixty-four percent of Gen Z reported losing cash or data to scams, followed by 57% of Millennials. On the flip side, Baby Boomers (33%) and Silent Gen (23%) fared considerably better.

²⁰ Much like mainstream categories, most of these ‘Other’ attacks still relied on classic phishing tricks (like fake links, spoofed contacts, or sneaky messages) to get their foot in the door and initiate or enable the scam.

Figure 23. Victimization by generation.



Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

Millennials top the charts across almost all scam types that led to a loss of money or data, followed by Gen Z, then Gen X.

Out of the total number of victims for each crime, Millennials accounted for:

- 36% of phishing scams
- 44% of online dating scams
- 39% of identity thefts
- 43% of crypto investment fraud
- 38% of tech support scams
- 37% of job scams
- 39% of delivery scams
- 34% of online marketplace scams.

The single scam category where Gen Z took #1 over Millennials (34% vs 30%) was lottery and prize scams. Interestingly, Gen Z and Gen X ran neck and neck on two fronts: online marketplace scams (27% each) and crypto investment fraud (26% and 25%, respectively).

Types of scams	Gen Z (18–29)	Millennials (30–45)	Gen X (46–61)	Baby Boomers (62–80)	Silent Gen (81+)
Phishing scam (n = 906)	28%	36%	24%	11%	1%
Online dating scam (n = 625)	26%	44%	23%	7%	0%
Identity theft (n = 667)	28%	39%	22%	11%	0%
Cryptocurrency investment fraud (n = 549)	26%	43%	25%	6%	0%
Tech support scam (n = 528)	27%	38%	22%	13%	0%
Job scam (n = 697)	33%	37%	23%	7%	0%
Delivery scam (n = 636)	27%	39%	25%	9%	0%
Online marketplace scam (n = 686)	27%	34%	27%	11%	1%
Lottery/prize scam (n = 305)	34%	30%	25%	10%	1%
Other (n = 63)	13%	17%	35%	35%	0%

When AI calls: The rise of deepfake imposters

We didn't stop at traditional text and web scams, no siree ...we also dug into high-tech imposter tactics like deepfake phone and video calls.

Overall, 36% of participants (+2% from 2025) got targeted by a scam voice or video call where the caller convincingly impersonated someone they recognized.

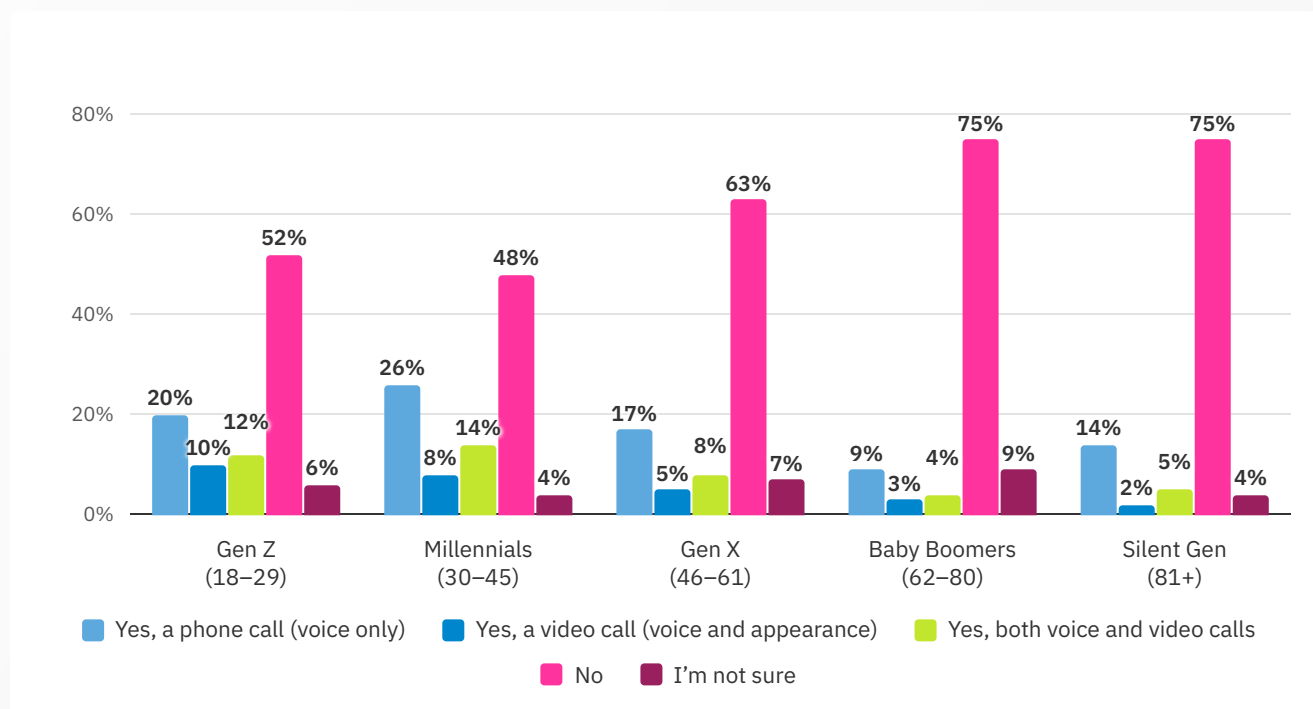
Matching our earlier patterns, deepfake targets were overwhelmingly younger (Figure 24):

- 48% of Millennials
- 42% of Gen Z
- 21% of Silent Gen
- 16% of Baby Boomers

This matches wider industry reports²¹ showing younger demographics report far higher exposure to deepfake content, ranging from non-consensual deepfake imagery to high-tech financial fraud. As AI tools evolve, telling real human interactions apart from fake ones is becoming an uphill battle.

21 For example: Sippy, T., Enock, F., Bright, J., & Margetts, H. (2025). *Behind the deepfake: 8% create; 90% concerned*. The Alan Turing Institute. <https://www.turing.ac.uk/news/publications/behind-deepfake-8-create-90-concerned>

Figure 24. ‘Have you ever received a phone or video call where the caller’s voice or appearance seemed to closely match someone you recognize (e.g., a family member, friend, colleague, or public figure), but it turned out to be a scam?’ by generation.



Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

Who were the scammers pretending to be? (Figure 25)

1. Family members (39%)
2. Friends (38%)
3. Banks or financial institutions (31%)

Some respondents even cited celebrities in the ‘Other’ section (1%).
Scammers are inventive, we’ll give them that.

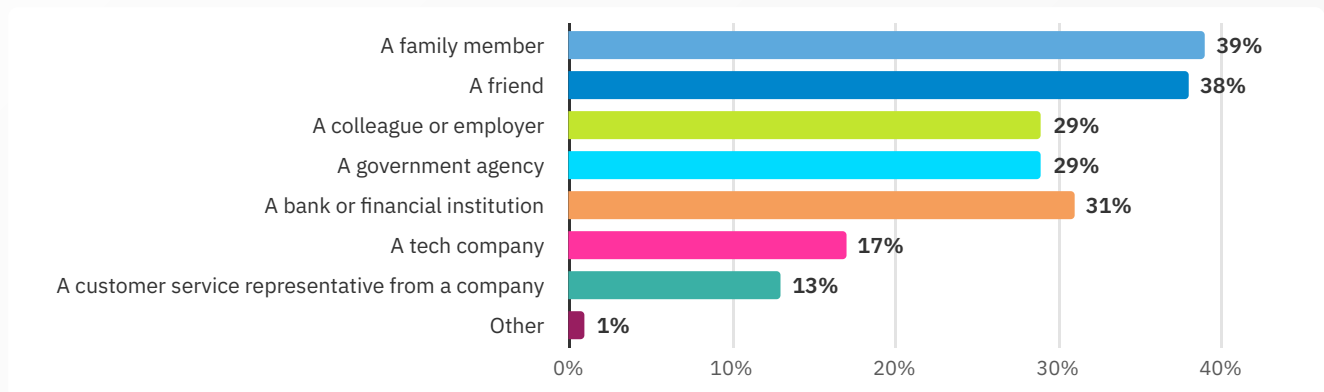
“ **‘Someone impersonated a friend and asked for financial help.’**

P778, USA

“ **‘An unknown person and the voice of a famous Hindi movie actor.’**

P7896, India

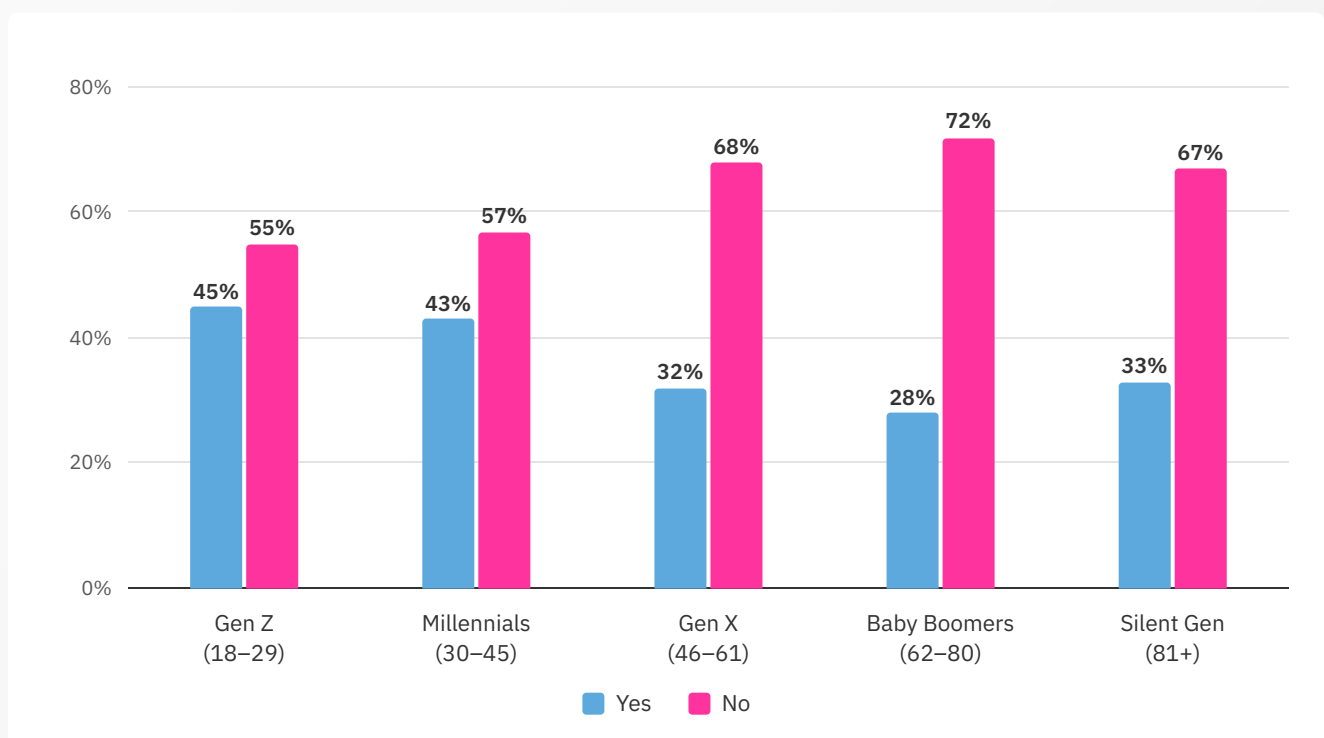
Figure 25. ‘Who did the caller pretend to be?’



Base: US, UK, India, Brazil, Singapore. Total number of those who received a deepfake phone and/or video call: 1,790 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

Deepfakes aren't just unsettling, they're effective. 40% of the 1,790 respondents who received a deepfake call lost cash or data. Once again, younger generations took the brunt of the damage: 45% of Gen Z and 43% of Millennials who received a deepfake call ended up taking a loss (Figure 26).

Figure 26. ‘Did you or your employer (if applicable) lose money or data as a result of the deepfake voice or video call you received?’ by generation.



Base: US, UK, India, Brazil, Singapore. Total number of participants: 1,790 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

The aftershocks: The real-world emotional toll

Cybercrime isn't just a hit to the wallet; it comes with a whole lot of emotional baggage too. We asked victimized respondents ($n = 2,523$) what lingering effects they felt after losing money or data.

Eighty-eight percent suffered real emotional, mental, or physical repercussions, not just direct financial or data loss.

The most common emotions experienced by victims were anger and stress (both 42%), followed by anxiety (38%), fear (32%), and embarrassment or self-blame (27%). A quarter said their sense of online safety was impacted, and just over a fifth (21%) said their trust in social media was impacted negatively.

'Which, if any, of the following things happened to you as a result of the online scam where you have lost money or data?'

I experienced anger	42%
I experienced stress	42%
I experienced anxiety	38%
I experienced fear	32%
I felt embarrassed/ashamed/self-blame or similar	27%
My sense of safety online was negatively impacted	25%
My trust in social media was negatively impacted	21%
My willingness to use the internet to perform necessary tasks decreased	19%
I felt alone	19%
My sense of safety offline was negatively impacted	18%
My trust in other people was negatively impacted	18%
My willingness to use social media decreased, leading me to delete my profile(s)	14%
Difficulty sleeping/fatigue	13%
Stress-related illness/condition	9%
Panic or anxiety-related illness	8%
None of these have happened to me	12%

Looking at the numbers, the aftermath follows a clear structure:

1. **Immediate emotional reactions:** High-intensity feelings like anger (42%), stress (42%), and anxiety (38%) top the list.
2. **Shift in trust:** Moderate impacts show up in digital trust, like losing confidence in online safety (25%) or social media (21%).
3. **Physical health complications:** Direct physical tolls like insomnia (13%) or stress-induced illnesses (9%) are rarer, but still very real.

BRAIN SNACKS

Our findings align with the broader academic literature²², which similarly identifies psychological effects, including worry, embarrassment, and shame, as a distinct and significant category of harm resulting from cyber-incidents.

KEY TAKEAWAYS: SUBCHAPTER 3.2

01

Half of participants have fallen victim, with phishing leading the charge: Half have suffered data or money loss from cybercrime. Phishing takes the top spot, trailed by job scams, identity theft, and online marketplace scams.

02

Younger demographics take the biggest hit: Gen Z and Millennials see the highest victimization rates – both personally and across their friend groups. Millennials specifically dominate victim rates in almost every individual scam category.

03

Scams inflict a heavy psychological toll: The vast majority of victims carry emotional baggage afterward – most commonly anger and stress. Very few walked away feeling totally unfazed.

²² Agrafiotis, I., Nurse, J. R. C., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity*, 4(1), tty006.

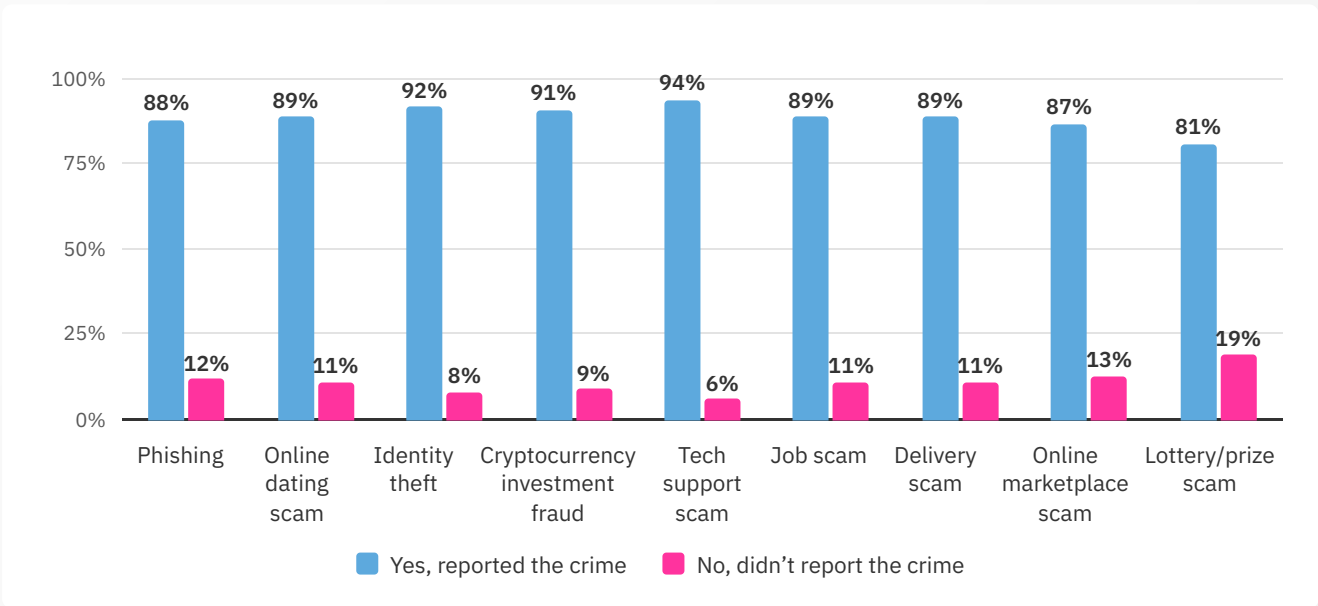
3.3 Cybercrime reporting: Who speaks up, who stays silent, and why?

When digital trouble strikes, do victims sound the alarm or quietly sweep it under the rug? As it turns out, an overwhelming majority actually speak up. Overall, an impressive 89% of cybercrime incidents were reported by victims to at least one channel.

That said, reporting habits definitely varied depending on the scam (Figure 27):

- **Tech support fraud** took the crown for the highest reporting rate at 94%.
- **Identity theft** came in a close second at 92%.
- **Crypto fraud** held strong at 91%.
- **Lottery/prize scams** brought up the rear with the lowest reporting rate at 81% – notably making it the *only* crime type to drop below 87%.

Figure 27. Crime reporting frequency by crime type.



Base: US, UK, India, Brazil, Singapore. Total number of cybercrime victims (age 18+): Phishing = 906; Online dating scam = 625; Identity theft = 667, Cryptocurrency investment fraud = 549; Tech support scam = 528, Job scam = 697, Delivery scam = 636, Online marketplace scam = 686, Lottery/prize scam = 305. Dates conducted: April 28, 2026 - May 19, 2026.

Where do victims turn?

Looking at where victims reported their crimes specifically, a bank or credit card company and the police or other law enforcement were the two most common reporting channels for nearly every crime type (Table 1), except for lottery/prize scams, where most told their family (40%), followed by a bank or credit card company (38%).

It's important to highlight that while nearly every crime type was reported to at least one channel, the share reaching formal authorities specifically was comparatively low, even where police or law enforcement ranked second most common. Reporting to the police, or other law enforcement, ranged from 27% (lottery/prize scams) to 41% (identity theft). Reporting to a government agency or organization ranged from 22% (online marketplace and lottery/prize scams) to 36% (identity theft).

Table 1. Who were the cybercrimes reported to?

	Phishing	Online dating scam	Identity theft	Cryptocurrency investment fraud	Tech support scam	Job scam	Delivery scam	Online marketplace scam	Lottery/prize scam
Bank/credit card company	56%	43%	48%	40%	44%	38%	38%	45%	38%
Police, or other law enforcement	34%	40%	41%	38%	39%	34%	35%	31%	27%
A government agency or organization	24%	33%	36%	34%	29%	28%	25%	22%	22%
The designated person or department at my work or place of education	19%	31%	29%	31%	33%	30%	27%	20%	22%
Network/broadband or phone provider	19%	22%	24%	31%	30%	24%	27%	20%	21%
Email or online search provider (e.g., Gmail)	18%	26%	20%	23%	28%	26%	23%	20%	20%
The service/application provider where I lost money/data	21%	26%	22%	24%	25%	26%	31%	27%	25%
My online security provider (e.g., Norton, McAfee)	12%	15%	N/A	14%	17%	15%	17%	14%	20%
I told my family, who then took action on my behalf	21%	17%	16%	21%	18%	23%	24%	30%	40%
Total number of victims	906	625	667	549	528	697	636	686	305

“*‘Reported through available channels at the time; but I never received any feedback about what was done regarding the incident.’*

P10452, Brazil

The sound of silence: Why some scams go unreported

Why do some people choose not to speak up? Looking at the non-reporting numbers (Table 2), the reasons shift depending on the type of scam.

1. 'It's too small to matter'

Feeling like the amount of money or data lost was simply too small or unimportant was found to be the most common reason across the largest variety of crimes:

- **Tech support scams:** 37%
- **Lottery/prize scams:** 29%
- **Phishing:** 28%
- **Delivery scams:** 28%
- **Online marketplace scams:** 22%

2. 'I don't know who to tell'

Not knowing who to report to was another massive wall. It tied for the leading hurdle for:

- **Crypto investment fraud:** 33% (tied with feeling no action would be taken)
- **Delivery scams:** 28% (tied with feeling the loss was too small)
- **Job scams:** 26% (tied with feeling too ashamed)

3. 'Nothing will happen anyway'

- **Online marketplace scams:** 22% (tied with feeling the loss was too small)
- **Crypto investment fraud:** 33% (tied with not knowing who to report)

4. The shame factor & process confusion

- **Online dating scams:** This was the only crime type where shame was the undisputed top reason for staying silent (30%).
- **Identity theft:** This was the only crime type where not knowing *how* to report (rather than *who* to report to) took the top spot (25%).

Table 2. Reasons given for not reporting incidents, by crime type.

	Phishing	Online dating scam	Identity theft	Cryptocurrency investment fraud	Tech support scam	Job scam	Delivery scam	Online marketplace scam	Lottery/prize scam
I didn't have the time	13%	12%	16%	14%	10%	10%	6%	7%	10%
I didn't know who to report it to	24%	27%	21%	33%	33%	26%	28%	17%	28%
I didn't know how to report it	17%	11%	25%	20%	27%	21%	26%	20%	22%
The process was too much effort (couldn't be bothered)	10%	12%	18%	22%	20%	9%	19%	18%	17%
There was no point as no action would have been taken	12%	20%	11%	33%	10%	16%	19%	22%	22%
I forgot	11%	5%	9%	10%	0%	5%	7%	11%	16%
I was too ashamed to have fallen for the scam	18%	30%	21%	24%	13%	26%	12%	21%	19%
The amount of money/data lost was too small or unimportant to me	28%	15%	14%	24%	37%	22%	28%	22%	29%
Other	9%	6%	9%	2%	3%	0%	4%	1%	3%
Total number of non-reporters	111	66	56	49	30	77	68	87	58

KEY TAKEAWAYS: SUBCHAPTER 3.3

01

Most incidents get reported: The majority of cybercrime incidents were reported to at least one channel, from banks and police to family members. Tech support fraud leads the pack for reporting, while lottery/prize scams trail behind.

02

Banks and police are defaults, but far from alone: Financial institutions and law enforcement handle the bulk of reports, but workplace reps, service or app platforms, and family members play huge roles depending on the crime – especially family for lottery scams.

03

Small losses and lost directions keep people quiet: Feeling like a loss was too trivial or simply not knowing who to contact were the top reasons people skipped reporting. Meanwhile, embarrassment was the primary barrier for dating scam victims.

3.4 Cyberbullying: The digital shadow

Cyberbullying is a threat that crosses generational lines, though, as the data reveals, it certainly doesn't hit everyone equally. This subchapter breaks down its prevalence, generational spreads, and where victims reach out for support when it happens.

Across our entire survey group, 19% of participants (*n* = 929) reported being victims of cyberbullying. That marks a 4% decrease from 2025.

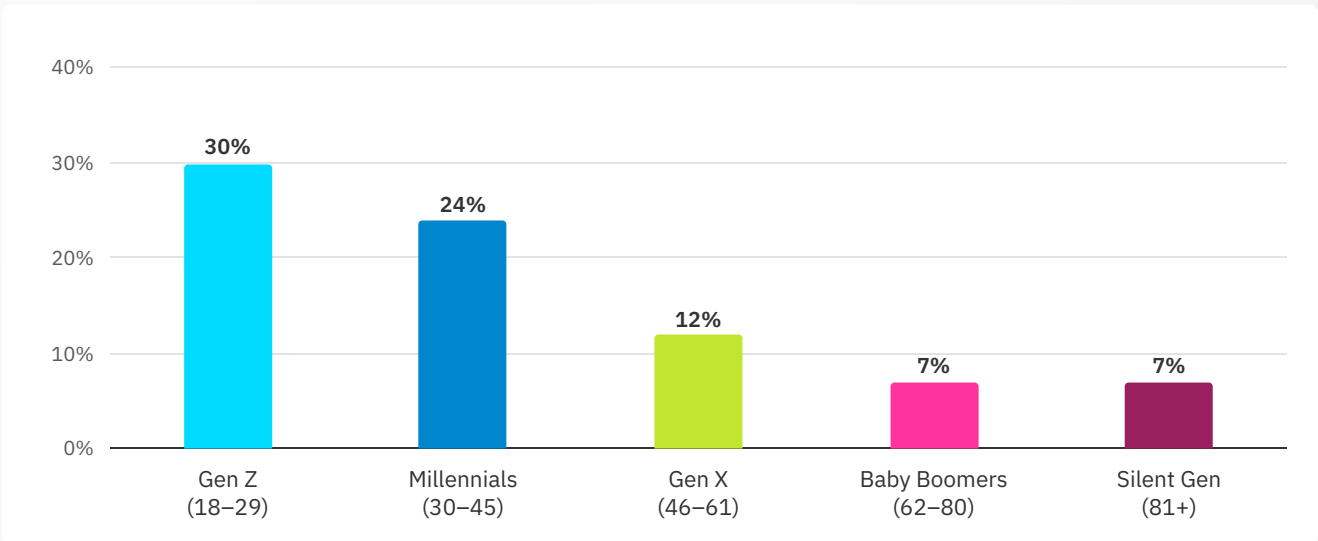
Younger people continue to bear the brunt of online harassment:

- **Gen Z:** 30% reported being cyberbullied (-8% from 2025).
- **Millennials:** 24% reported being cyberbullied (also -8% from 2025).

While older demographics saw noticeably lower figures, online harassment remains a universal issue across the board (Figure 28):

- **Gen X:** 12% (-2% from 2025)
- **Baby Boomers:** 7% (+1% from 2025)
- **Silent Gen:** 7% (-2% from 2025)

Figure 28. Victim of cyberbullying, by generation.



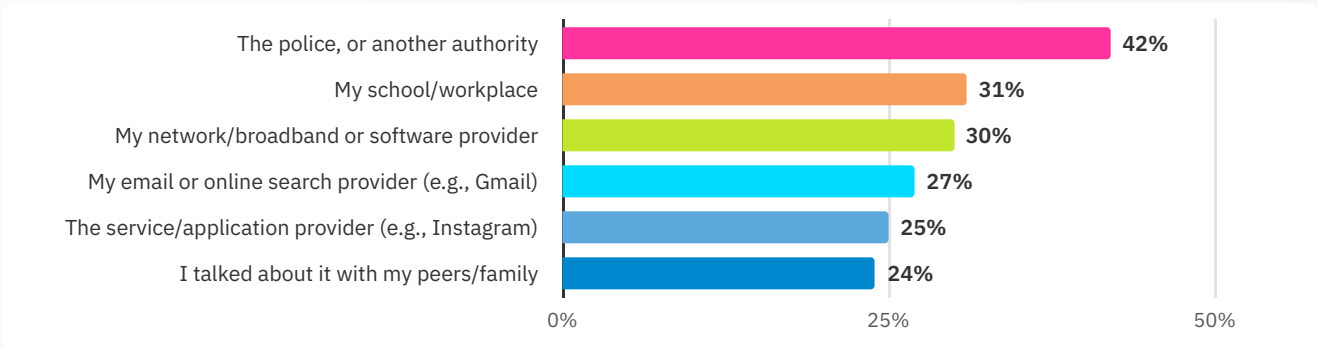
Base: US, UK, India, Brazil, Singapore. Total number of cyberbullying victims: 929 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

When cyberbullying happens, people rarely suffer in complete silence (thankfully): 87% of victims reported the incident (down just 1% from 2025).

So, where did victims turn for help? (Figure 29)

- 1. **Law enforcement / government agencies:** 42% reported to the police or an official authority (-7% from 2025).
- 2. **Workplace or school:** 31% reported to their educational or professional institution (unchanged from 2025).
- 3. **Tech & telecom providers:** 30% reported to their network, broadband, or software provider (-1% from 2025).
- 4. **Family or peers:** 24% confided in family members or friends (+2% from 2025).

Figure 29. Agencies where cyberbullying is reported to.



Base: US, UK, India, Brazil, Singapore. Total number of cyberbullying victims who reported the incident: 809 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

 KEY TAKEAWAYS: SUBCHAPTER 3.4

01

Cyberbullying hits nearly 1 in 5, but victims take action: Nearly a fifth of respondents have experienced cyberbullying, and the majority of victims reported it – most frequently turning to police or official government channels.

02

Younger demographics are in the primary splash zone 🌊: Gen Z and Millennials face the highest rates of digital harassment by far, though Gen X, Boomers, and Silent Gen are still impacted.



Chapter 3 summary cheat-sheet

High anxiety and deep fatalism. Worry outpaces personal risk perception, with 66% of people worrying about cybercrime while only 37% see themselves as likely targets. Resignation is high, as 33% believe losing money online is unavoidable and 39% feel the same about data theft. Meanwhile, faith in existing armor is low – 57% feel law enforcement lacks capacity to handle cybercrime, and 63% believe criminals are more advanced than official defenses.

High victimization and heavy emotional tolls. Half the participants (50%) have fallen victim to cybercrime, with phishing reigning supreme at 16% of all reported incidents. Scams leave lasting human marks: 42% experienced anger, 42% felt stress, and 38% suffered anxiety, leaving only 12% who walked away completely unbothered.

Action-oriented victims with clear reporting gaps. Reporting rates are high overall, with 89% of incidents reported – usually to banks or law enforcement. Where victims stay silent, small financial losses, confusing reporting procedures, and personal shame (especially in dating scams) remain the primary reasons.

GENERATIONAL HIGHLIGHTS

Belief in being a likely cybercrime target and confidence in law enforcement move in opposite directions with age. Belief in being a likely target peaks with Millennials (43%) and is lowest among the Silent Gen (25%), while skepticism of law enforcement's capacity to deal with cybercrime is highest among the Silent Gen (73%) and lowest among Gen Z (52%).

Victimization is more common among younger generations. Gen Z (64%) and Millennials (57%) had the highest personal victimization rates, and were most likely to know a cybercrime victim in their circle (69% and 64%, respectively).

Younger generations were also hit hardest by deepfake scams. 48% of Millennials and 42% of Gen Z received deepfake calls, and of those, 45% of Gen Z and 43% of Millennials lost money or data as a result.

Cyberbullying reaches every generation, though not equally. Gen Z (30%) and Millennials (24%) had the highest rates, but Gen X (12%), Baby Boomers (7%), and the Silent Gen (7%) were affected too.

4. Cybersecurity training: The good, the bad, and the ignored

This town ain't big enough for the two of us. Stick 'em up, punk. (Insert other cowboy-based revelry here, at your leisure).

Welcome to Chapter 4, partner. In this stretch of the trail, we're peeling back the layers on cybersecurity training. We'll look at who actually gets access to it, whether it's mandatory, how people prefer to learn, and the annoying barriers that stop folks from tuning in. And finally, we'll wrangle whether all this effort actually changes how people behave online. The final showdown, if you will.

Here's how we're breaking down Chapter 4:

4.1 Who's getting trained (and who's left behind): Access patterns across demographics, employment statuses, and specific industries, alongside how organizations deploy optional vs. mandatory requirements.

4.2 Barriers to attendance (why people skip out): The key reasons people pass on available training – from lack of time to rising confidence in existing knowledge.

4.3 Preferred format – how people want to learn: How overall learning preferences stack up (with video leading the way) and how these choices vary across generations and employment types.

4.4 The final showdown: What impact did training have?: Whether training actually translates into real-world action and long-term security behavior changes.

4.1 Who's getting trained (and who's left behind)

First up, who's actually getting trained here? Let's look at the numbers:

- **The engaged:** 37% of participants reported having access to and using cybersecurity training (+5% from 2025).
- **The bystanders:** 13% reported having access but opting not to use it (same as 2025).
- **The excluded:** Half of all participants (50%) still do not have access to training at all (though on the bright side, that's a 5% improvement from 2025).

The generational divide

As in previous years, training access and usage skewed much higher among younger demographics (Figure 30).

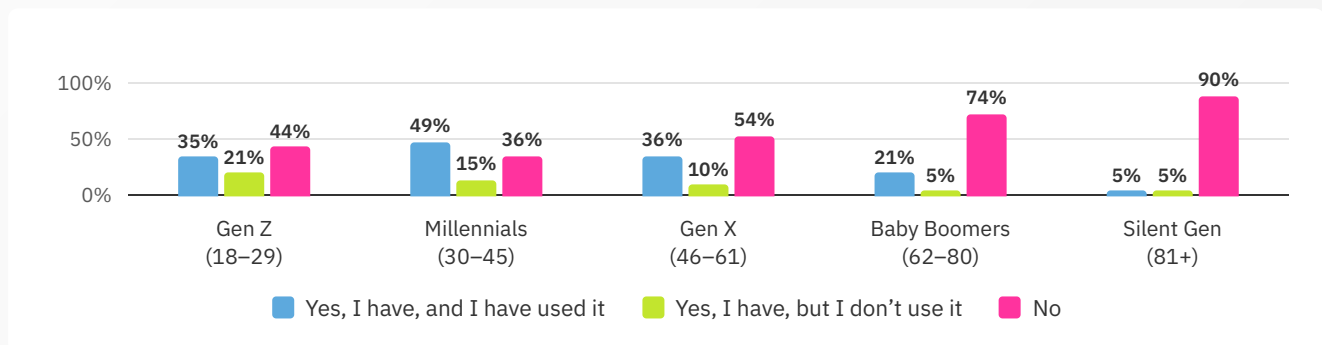
- Millennials took top prize with the highest access and usage at 49% (+4% from 2025).
- Gen X came in second at 36% (+8% from 2025).
- Gen Z sat closely behind at 35% (-8% from 2025).

Meanwhile, older generations continue to report much lower levels:

- Baby Boomers: 21% (+11% from 2025).
- Silent Gen: 5% (+3% from 2025).

Fun fact: Access and usage increased across every single generation this year, except for Gen Z.

Figure 30. ‘Do you have access to cybersecurity training (e.g., at work, school, or library)?’ by generation.



Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

Employment status & sector breakdown

Unsurprisingly, training access and completion were highest among employed participants at 46% (+2% from 2025).

By comparison, the numbers drop off sharply for other groups:

- Students: 24%
- Retired participants: 22%
- Not in active employment: 15%

When we slice the employment data by sector, clear winners and high-risk gaps emerge (Figure 31). Over half of participants within the following sectors had access to and used training:

Sectors leading the pack (over 50% access & usage):

1. Information technology & telecommunications: 62%
2. Finance & insurance: 62%
3. Nonprofit & charity organizations: 53%

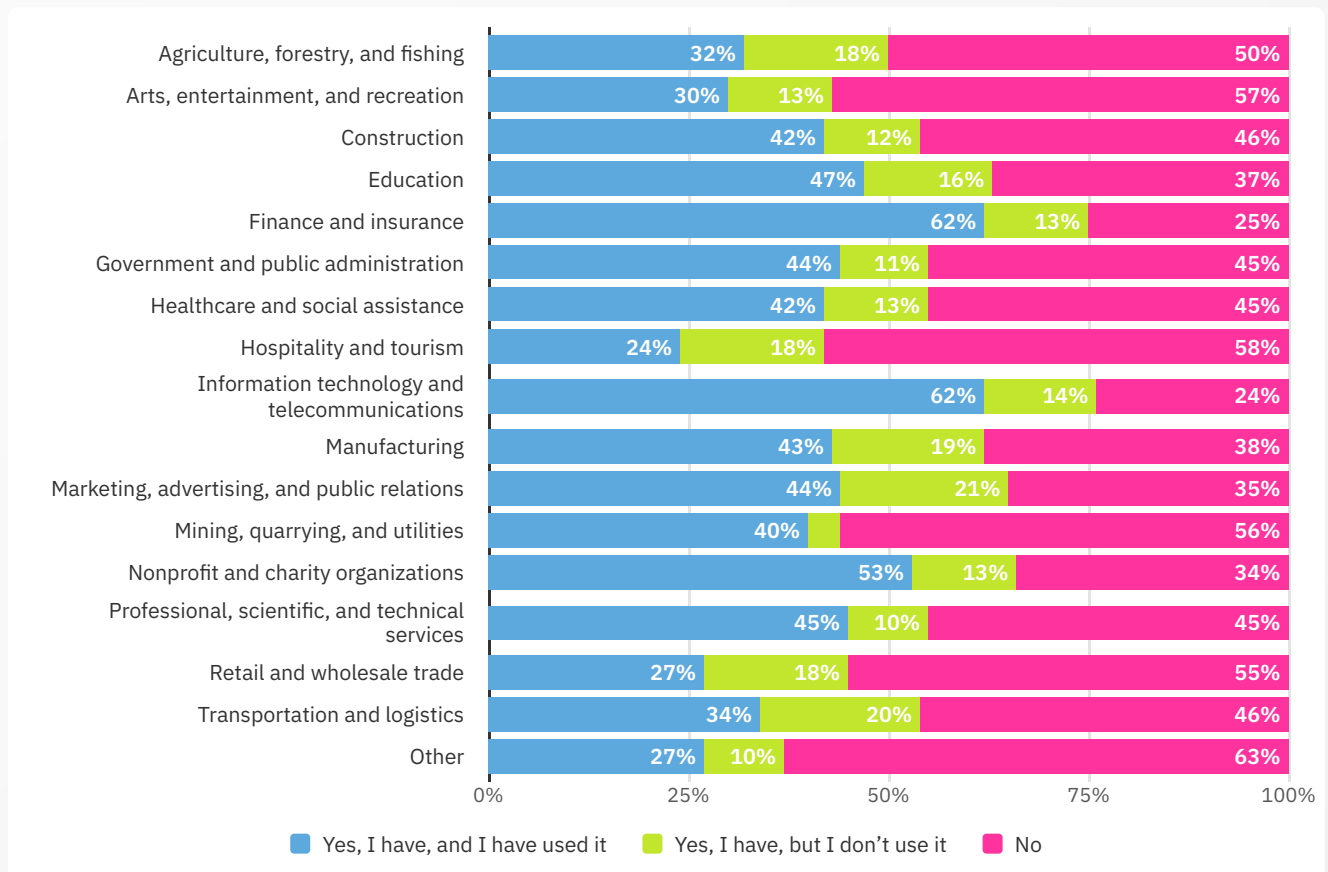
Sectors left in the dark (highest % without access):

1. Other sectors (including options not listed in the sectors provided): 63%
2. Hospitality & tourism: 58%
3. Arts, entertainment, & recreation: 57%
4. Mining, quarrying, & utilities: 56%
5. Retail & wholesale trade: 55%
6. Agriculture, forestry, & fishing: 50%

The ‘thanks, but no thanks’ sectors (highest % who have access but skip it):

- Marketing, advertising, & public relations: 21%
- Transportation & logistics: 20%
- Manufacturing: 19%

Figure 31. ‘Do you have access to cybersecurity training (e.g., at work, school, or library)?’ by sector.



Base: US, UK, India, Brazil, Singapore. Total number of participants: 3,269 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

Hospitality's low access rate (58% lacking access) is particularly eye-opening. The sector has suffered high-profile breaches in recent years, including major ransomware attacks on MGM Resorts and Caesars Entertainment, alongside the massive Marriott International breach.²³

Is training required, or optional?

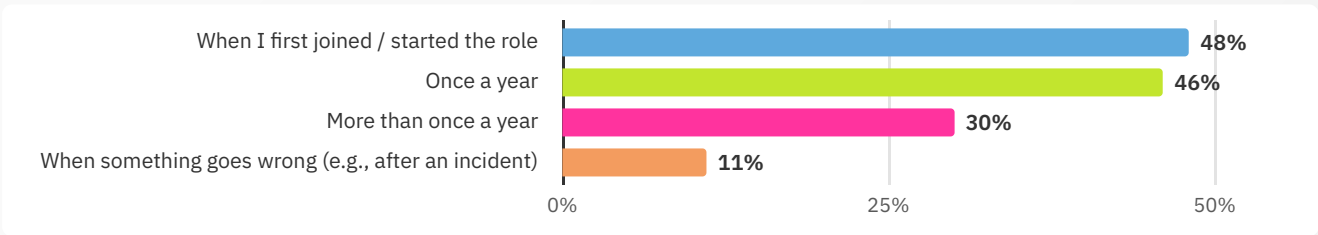
For employed participants, workplace requirements are pretty much a gamble (and we all know how that goes, cowboy or not):

- **Mandatory:** 47%
- **Not mandatory:** 48%
- **Not sure:** 5%

Among those required to take training (*n* = 1,543) (Figure 32):

- 48% are required to complete it when first joining their role.
- 46% are required to complete it once a year.
- 30% do it more than once a year.
- 11% only get trained reactively (i.e., when something goes wrong).

Figure 32. ‘When are you required to complete training?’



Base: US, UK, India, Brazil, Singapore. Total number of participants: 1,543 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

23 See, e.g., NPR. (2023, September 15). Cyberattacks strike casino giants Caesars and MGM. <https://www.npr.org/2023/09/15/1199681234/cyberattacks-strike-casino-giants-caesars-and-mgm>
Federal Trade Commission. (2024, October 9). FTC takes action against Marriott and Starwood over multiple data breaches. <https://www.ftc.gov/news-events/news/press-releases/2024/10/ftc-takes-action-against-marriott-starwood-over-multiple-data-breaches>

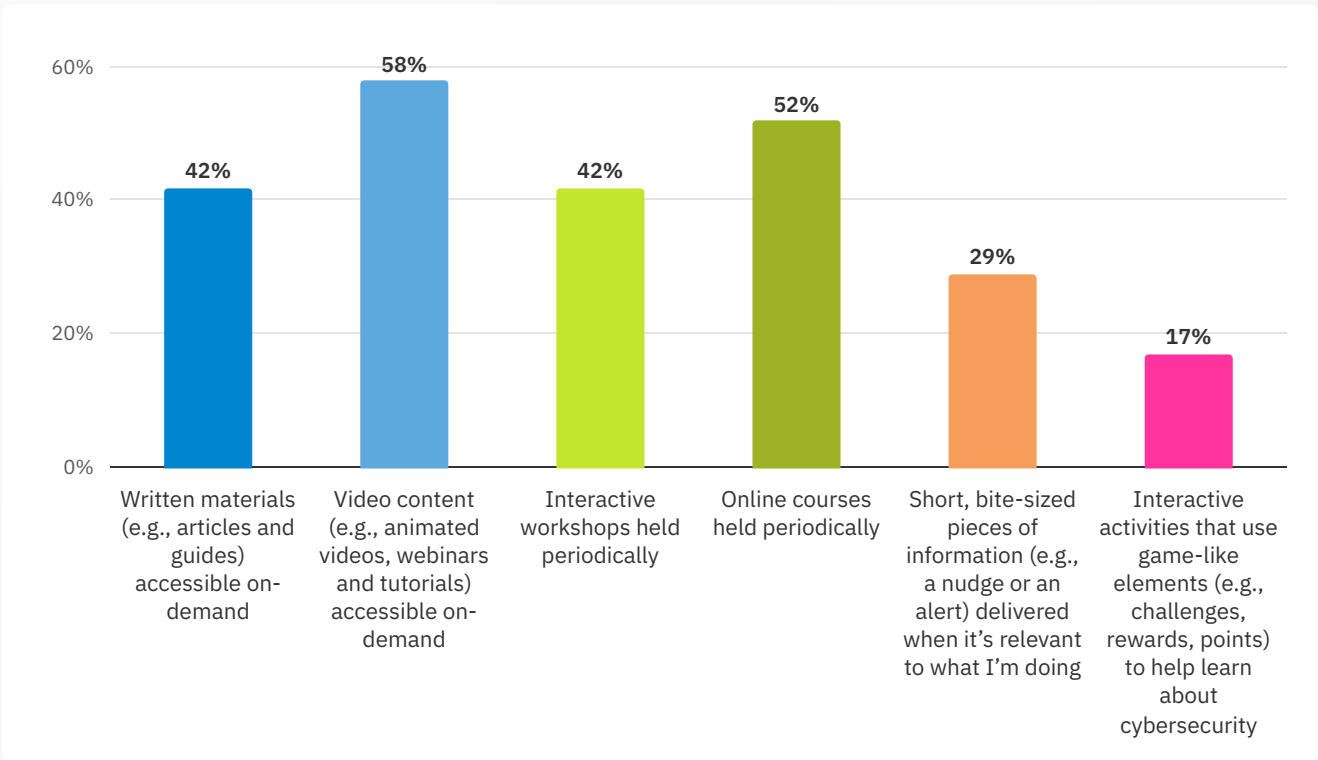
Delivery formats: How companies deploy training

We also asked those required to complete mandatory training about the format their workplace uses for delivering it (Figure 33). We found formats broadly matched 2025 trends. Employers rely most heavily on:

- **Video content:** 58% (+4% from 2025)
- **Periodic online courses:** 52% (+2% from 2025)
- **Written materials:** 42% (+2% from 2025)
- **Interactive workshops:** 42% (+3% from 2025)

Surprisingly, only 29% reported their organization using bite-sized content like nudges or alerts (+4% from 2025). Interactive, gamified activities remain the least common format at 17% (+2% from 2025).

Figure 33. Cybersecurity training formats used by organizations.



Base: US, UK, India, Brazil, Singapore. Total number of participants: 1,543 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

📌 KEY TAKEAWAYS: SUBCHAPTER 4.1

01

Half of all participants still have no access to cybersecurity training: Access is far from universal, skewing heavily toward younger generations and industries like IT and finance, while hospitality lags far behind.

02

Mandatory training is basically a coin flip, and video dominates: Requirements for employed participants are split almost evenly between mandatory and optional. Where training is delivered, video content is used more than any other format.

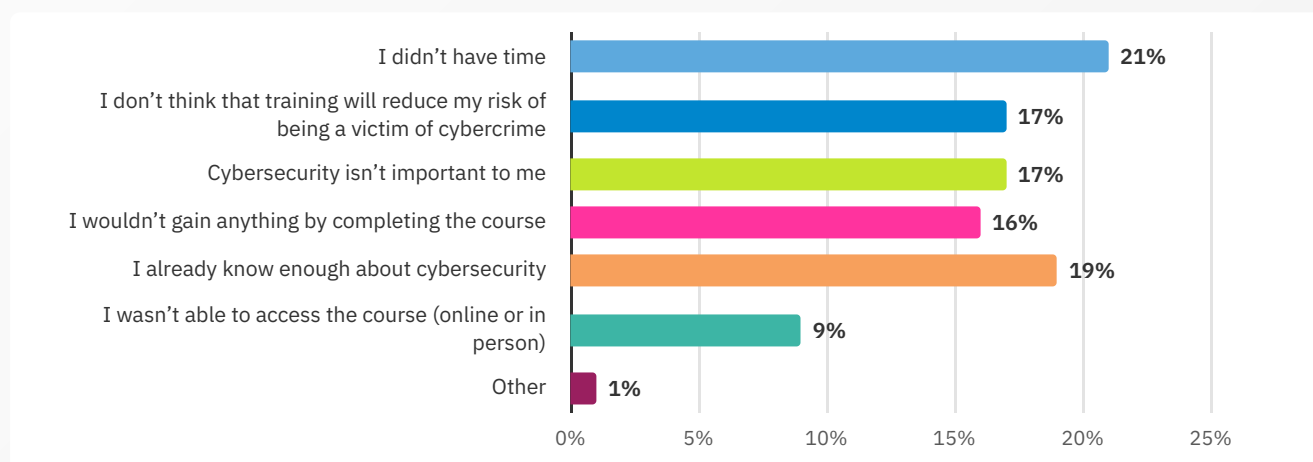
4.2 Barriers to attendance (why people skip out)

Why skip training if you have access (Figure 34)? We asked those who didn't attend ($n = 638$).

The top reason remains not having enough time (21%). However, confidence in their own cybersecurity knowledge (19%, +3% from 2025) has officially overtaken skepticism to become the second most common reason.

Tied at 17% each were the belief that training would not reduce their risk of being a victim of cybercrime (-3% from 2025) and the view that cybersecurity isn't important to them (same as 2025). A further 16% felt they would not gain anything from completing the course.

Figure 34. 'What is the main reason you didn't use the opportunity to attend a cybersecurity training course?'



Base: US, UK, India, Brazil, Singapore. Total number of participants: 638 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

“***'I don't need nor want it [sic] [re. cybersecurity training].'***

P2612, UK

KEY TAKEAWAYS: SUBCHAPTER 4.2

01

Lack of time and overconfidence lead the excuses: Lack of time and belief in their own knowledge are the top reasons for skipping training.

02

Skepticism plays its part too: Beyond time and confidence, participants are equally likely to doubt training's risk-reduction ability, feel cybersecurity isn't important, or assume they won't gain anything from completing it.

4.3 Preferred format – how people *want* to learn

When it comes to training format (Figure 35), participants continued to mostly prefer video content (50%, +6% from 2025), followed by periodic online courses (38%, +4% from 2025), just as in 2025. Written materials and short, bite-sized pieces of information were preferred equally by 34% of the participants, representing 4% and 6% increases respectively.

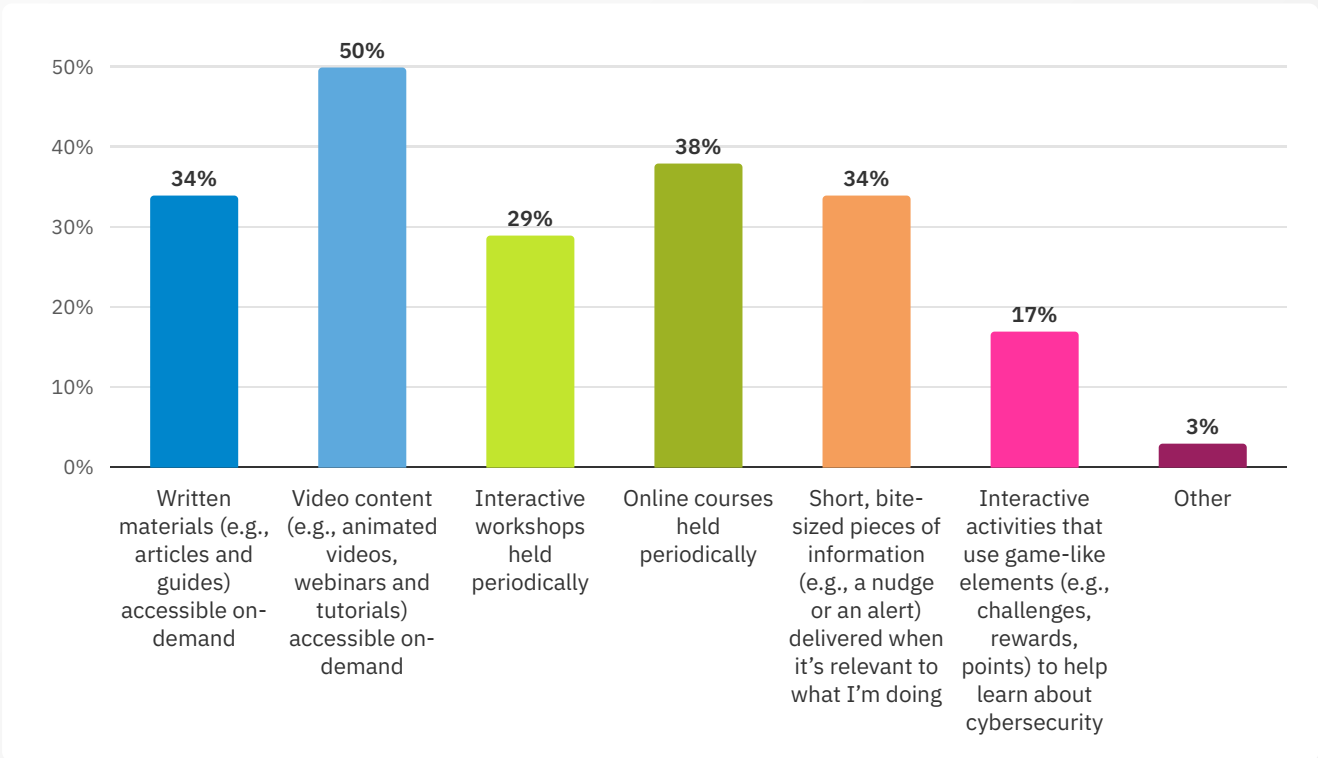
This is the first year since we introduced this question in 2024 that bite-sized content has made it into the top three.

In spite of the minor increase, the least preferred format is still interactive activities that use game-like elements (17%, +4% from 2025), just as in previous years.

The results in numbers (for the data devotees):

- **Video content:** 50% (+6% from 2025). The reigning champion.
- **Periodic online courses:** 38% (+4% from 2025)
- **Written materials:** 34% (+4% from 2025)
- **Bite-sized information:** 34% (+6% from 2025). First time in the top three since tracking began in 2024.
- **Interactive gamified activities:** 17% (+4% from 2025). Still the least preferred option.

Figure 35. ‘What format do you prefer to consume cybersecurity training information?’

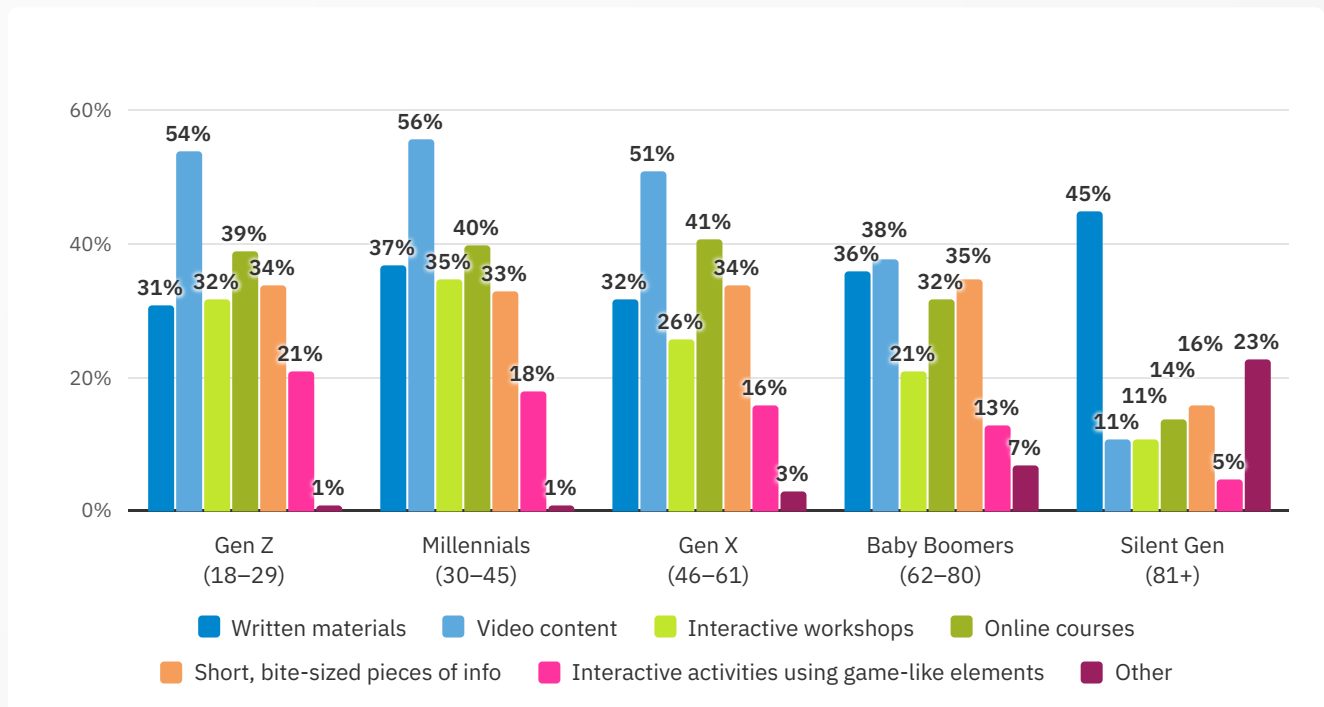


Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

Preference slices: By generation (Figure 36)

- **Video** was the top choice across almost all age groups, peaking with Millennials (56%) and Gen Z (54%), while dropping with age down to Silent Gen (11%).
- **Second choices:** Gen X (41%), Millennials (40%), and Gen Z (39%) preferred periodic online courses. Baby Boomers preferred written materials (36%), closely followed by bite-sized content (35%).
- **The outlier:** The Silent Gen broke the trend entirely, consistently preferring written content (45%).

Figure 36. ‘What format do you prefer to consume cybersecurity training information?’ by generation.

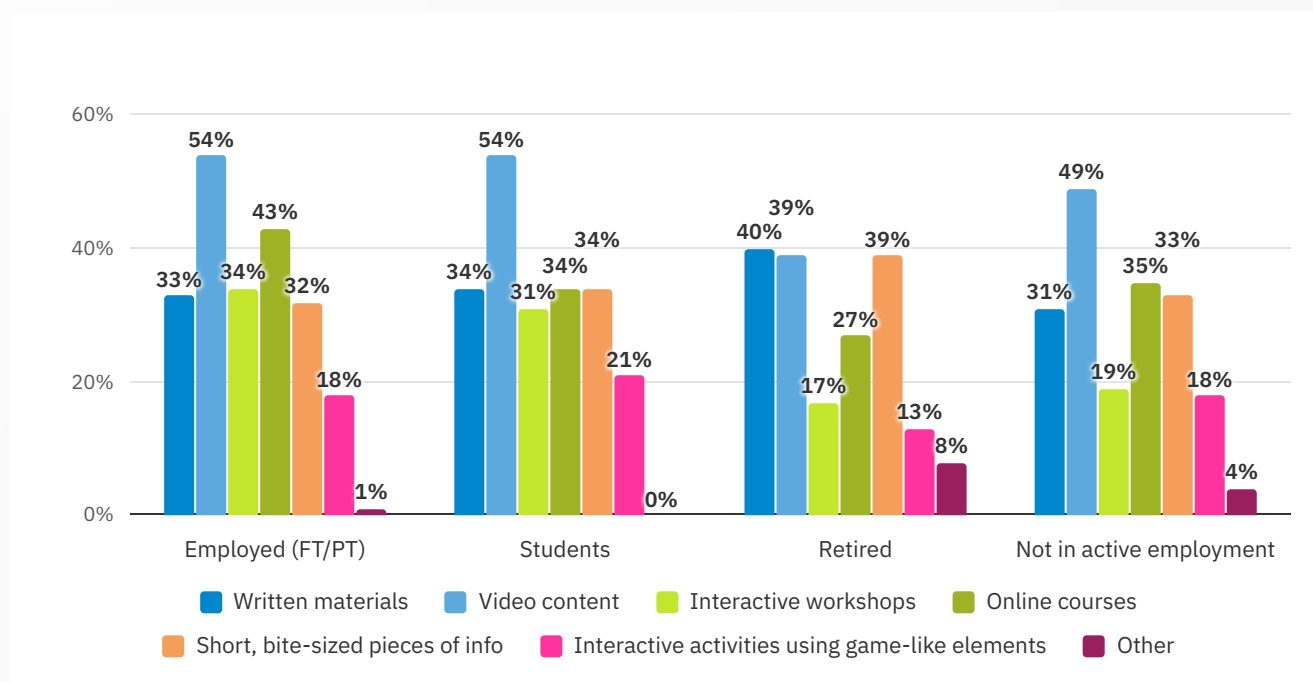


Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

Preference slices: By employment status (Figure 37)

- **Employed participants:** Preferred video (54%), followed by online courses (43%).
- **Students:** Showed an identical preference for video (54%), with written materials, online courses, and bite-sized content tied for second (34% each).
- **Retired participants:** Video (39%) wasn't a clear favorite here; written materials (40%) and bite-sized content (39%) were preferred just as much or more.

Figure 37. ‘What format do you prefer to consume cybersecurity training information?’ by employment.



Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

BRAIN SNACKS

Our findings line up nicely with broader digital habits²⁴: with 85% of US adults using YouTube²⁵ (more than any other online platform), the preference for video training²⁶ appears to be a natural extension of a wider societal shift toward video as the go-to way people consume information.

KEY TAKEAWAYS: SUBCHAPTER 4.3

01

Video is the runaway favorite, but not for everyone. Video content is preferred across almost every age group, employed individuals, and students. Though the Silent Gen and retirees prefer to lean toward written materials instead.

24 Tschakert, K. F., & Ngamsuriyaraj, S. (2019). Effectiveness of and user preferences for security awareness training methodologies. *Heliyon*, 5(6), e02010.

25 Dannenbaum, C. (2025, February 28). *5 facts about Americans and YouTube*. Pew Research Center. <https://www.pewresearch.org/short-reads/2025/02/28/5-facts-about-americans-and-youtube/>

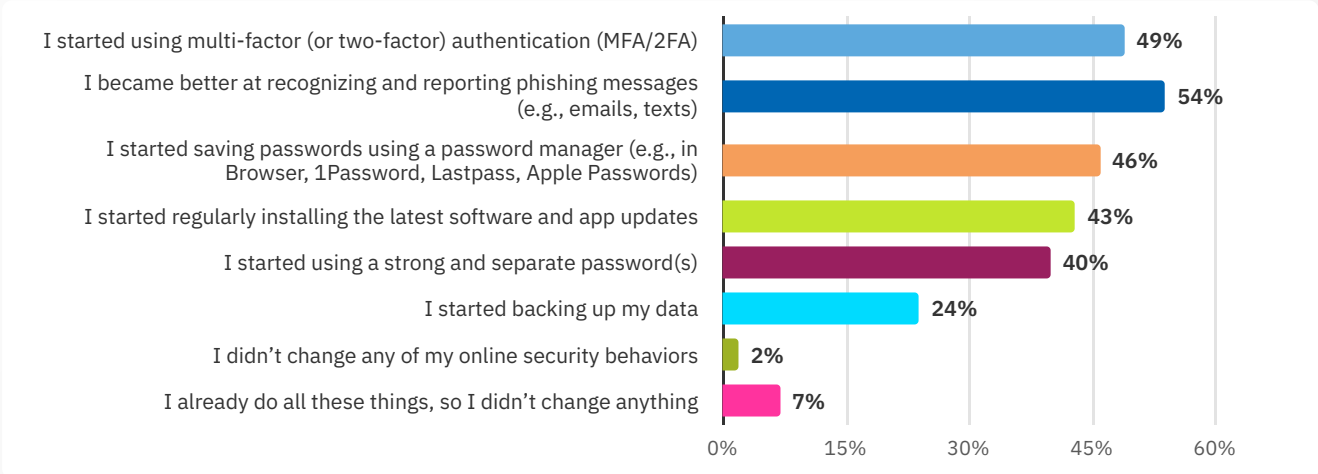
26 Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, 33(3), 237-248.

4.4 The final showdown: What impact did training have?

The majority of those who attended training ($n = 1,844$) found it useful (88%, with a 5% increase from 2025). But what impact did the attendees say the training had on their security behaviors (Figure 38)?

- 54% got better at recognizing and reporting phishing messages (+7% from 2025).
- 49% started using MFA (+7% from 2025).
- 46% began using a password manager (+8% from 2025).
- Only 2% felt training didn't change *any* of their security behaviors (-2% from 2025).

Figure 38. ‘When you attended cybersecurity training, how did it influence your security behaviors?’



Base: US, UK, India, Brazil, Singapore. Total number of participants: 1,844 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

While these figures are encouraging, most critical security behaviors were still adopted by fewer than half of attendees post-training. This aligns with broader research findings: awareness initiatives excel at raising knowledge, but often struggle to convert that knowledge into real-world action.²⁷ For instance, one study²⁸ highlighted that only 39% of participants reported improved security behavior following training.

 KEY TAKEAWAYS: SUBCHAPTER 4.4

01

Training is rated useful, but habit adoption trails behind: While the majority of attendees found training helpful and many reported improvements – like spotting phishing or using MFA – key security behaviors were still only adopted by fewer than half of overall attendees. So we’re not where we need to be yet.

²⁷ Chaudhary, S. (2024). Driving behaviour change with cybersecurity awareness. *Computers & Security*, 142, 103858.

²⁸ Kävrestad, J., Furnell, S., & Nohlberg, M. (2024). User perception of Context-Based Micro-Training—a method for cybersecurity training. *Information Security Journal: A Global Perspective*, 33(2), 121-137.



Chapter 4 summary cheat-sheet

Access is far from universal and unevenly distributed. Half of all participants (50%) have no training access. Where available, it concentrates in sectors like IT (62%) and finance (62%), leaving industries like hospitality (58% no access) behind.

Time and overconfidence are the main roadblocks. Lack of time (21%) is the top barrier, closely followed by people believing they already know enough (19%), cyber not being important to them, and thinking that training won't reduce their risk of being a cybercrime victim (17% both).

Video reigns supreme, while gamification trails. Video is the top format (50%), followed by online courses (38%). Written content and bite-sized info tied for third (34%), while gamified activities sat at the bottom (17%).

Training gets praise, but habits need work. While 88% found training useful and many reported becoming better at recognizing phishing (54%) or adopting MFA (49%), these behaviors were still adopted by fewer than half of all attendees. Old (risky) habits die hard (with a vengeance*).

*There are two Bruce Willis references in this report. Are we going to apologize for that? Nah. ...so you may as well get on board. Or, as John McClane would say, 'welcome to the party, pal!'

GENERATIONAL HIGHLIGHTS

Millennials lead in access; Gen Z leads in opting out. Millennials reported the highest access/usage (49%), followed by Gen X (36%) and Gen Z (35%). However, Gen Z was the most likely generation to have access but actively skip it (21%, vs. 15% for Millennials and 10% or lower for others).

Demographics dictate secondary preferences. Video dominates across most age groups for consuming cybersecurity training, but second choices vary: Gen Z (39%), Millennials (40%), and Gen X (41%) prefer online courses, Baby Boomers pick written materials (36%), and the Silent Gen rejects video entirely in favor of written content (45%).

5. Cybersecurity behaviors

Oh, Behave!*

...Yes, it's time to take a long, hard (and occasionally incredulous) look at how people actually behave. **But** this is *always* through the lens that they aren't the problem, they're just human. Which means inconsistent, unpredictable, and emotional. Which isn't wrong, it's just ...human. And that's what we have to bear 🐻 in mind when designing any cybersecurity framework.

So, without further ado, let's dive into the glorious messiness of human behavior.

Using [SebDB](#) – the world's cybersecurity behavior database – this chapter pulls back the curtain on what people do online. We've broken everyday behaviors down into four core battlegrounds:

5.1 Authentication methods: How we build, recycle, and juggle our passwords, our (hesitant) embrace of MFA, and why we're surprisingly suspicious of biometrics and passkeys.

5.2 Software updates: The eternal standoff between 'Update now' and 'Remind me later'. Here, we look at who patches immediately, who snoozes indefinitely, and why automation is trying to save us from ourselves.

5.3 Backing up data: Digital insurance for our memories and files. We examine who routinely builds safety nets, who plays high-stakes roulette with their hard drives, and how corporate IT skews the numbers.

5.4 Recognizing and reporting phishing: How sharp our spidey-senses *really* are when suspicious messages land in our inboxes ...and whether we actually hit report or just look the other way. 🙄

Here's the full map of the SebDB behaviors tracked across this chapter:

*In case this reference has thus far completely passed you by, I hereby refer you (via your search engine of choice) to *Austin Powers: International Man of Mystery*.

The SebDB behavior blueprint

Subchapters	SebDB behavior
5.1 If your name's not down, you're not coming in: authentication in the real world	
5.1.1 Making the cut: how we build our passwords (and pet names)	 SB003: Authenticates with a strong password (or passphrase)
5.1.2 Password management: the great notebook revival	 SB016: Authenticates with a unique password (or passphrase)  SB130: Stores a password (or passphrase) securely  SB209: Uses an approved or official password manager application  SB210: Uses an approved browser-based password manager
5.1.3 MFA: security need or total nuisance?	 SB001: Authenticates with MFA
5.1.4 Beyond passwords: Biometrics & passkeys	 SB112: Authenticates with a passkey  SB203: Authenticates with biometrics
5.2 Snooze or software patch? How we handle Update Available pop-ups	 SB024: Keeps software up-to-date
5.3 Back it up, pack it in: backing up data	 SB061: Backs up data
5.4 Catch me if you can: recognizing & reporting phishing messages	
5.4.1 Spotting the bait: how good are we at catching phishes?	 SB081: Checks a message for signs of deception  SB082: Verifies a suspicious message using known contact details  SB058: Checks a website for signs of deception
5.4.2 Sounding the alarm: reporting phishing messages	 SB087: Reports a suspicious message

5.1 If your name's not down, you're not coming in: Authentication in the real world

Knowing what you *should* do and actually doing it are two very different beasts. Previous chapters looked at what people think, what they've experienced, and what training they've sat through. This section gets into the real work: the daily security behaviors that decide whether an account, a device, or an organization stays secure or gets compromised.

To set the stage, we asked participants what authentication methods they use to log in to their online accounts. The results? Honestly, pretty predictable:

- 70% stick with tried-and-true passwords or passphrases
- 53% tap into biometrics (like TouchID or FaceID)
- 39% use passkeys
- 35% rely on one-time codes sent via email, text, or phone calls

In this subchapter, we'll deep dive into password hygiene (5.1.1 & 5.1.2), break down general MFA adoption (5.1.3), and unpack the unexpected hesitation surrounding biometrics and passkeys (5.1.4).

5.1.1 Making the cut: How we build our passwords (and pet names)

Let's talk about how people build their digital keys.

The National Institute of Standards and Technology (NIST) offers clear guidelines²⁹ for solid password hygiene:

- Check passwords against a blocklist of breached, common, or compromised words (and context-specific terms like usernames).
- Skip forced complexity rules requiring special mixtures of character types.
- Require a minimum length of 15 characters for standalone passwords, or 8 characters when paired with another authentication factor.
- Don't force periodic password resets unless there's evidence of compromise.
- Support the use of password managers and autofill tools.

²⁹ <https://pages.nist.gov/800-63-4/>

Most of these have been reflected in all participating countries and/or regions: NCA³⁰, NCSC³¹, CERT-In³², CERT.br³³ and CSA³⁴.

Across this subchapter (5.1.1) and the next (5.1.2), we examine participants' password hygiene by looking at:

- Password creation tactics – length, use of personal info, and single dictionary words
- Use of separate passwords
- Password management strategies

The knowledge gap: Do we practice what we preach?

When asked about their know-how, a confident 73% (+3% from 2025) claimed they know how to create strong passwords ...and actually do it. 21% (-1% from 2025) admitted they know *how* to build a strong password, but intentionally choose not to. Only 6% (-2% from 2025) confessed they don't know how to build a strong password at all.

So the vast majority say they've got the skills ...but do their actual passwords pass the test? Let's talk length:

- 36% (-4% from 2025) create passwords that are 9-11 characters long.
- 34% (+3% from 2025) build passwords with 7-8 characters.
- 5% (+4% from 2025) create even shorter passwords.
- Only 25% hit the gold standard of more than 12 characters.

This habit doesn't change much across generations either (Figure 39). Most age groups stick to 9-11 characters (ranging from 35% of Millennials to 41% of the Silent Gen, where it's tied with 7-8 characters). Meanwhile, 36% of Gen Z opt for 7-8 characters.

30 <https://www.staysafeonline.org/articles/passwords>

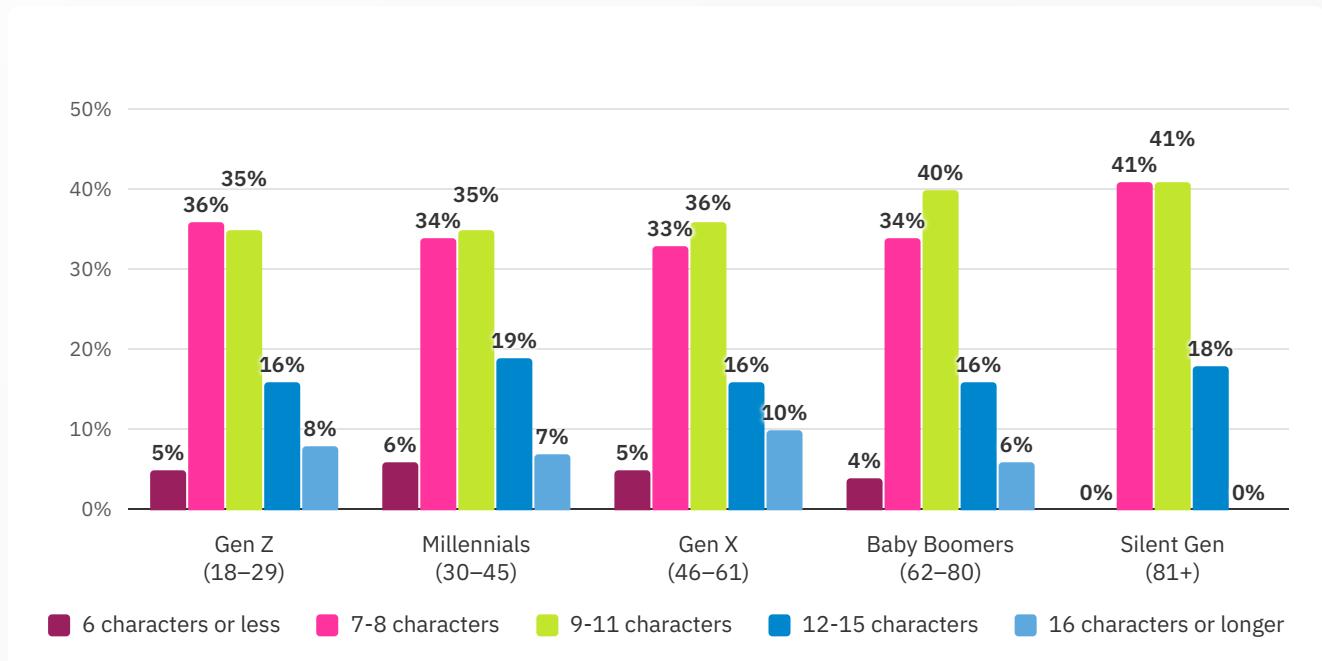
31 <https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/three-random-words>

32 <https://www.cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES02&VLCODE=CIAD-2022-0026>

33 <https://cartilha.cert.br/dicas-rapidas/>

34 <https://www.csa.gov.sg/our-programmes/cybersecurity-outreach/cybersecurity-campaigns/better-cyber-safe-than-sorry-campaign/use-strong-passwords-and-enable-2fa/>

Figure 39. ‘When creating a password for a new account where the website or app does not specify a minimum length, how long do you usually make your password’ by generation.



Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

Bad password creation habits are creeping up again:

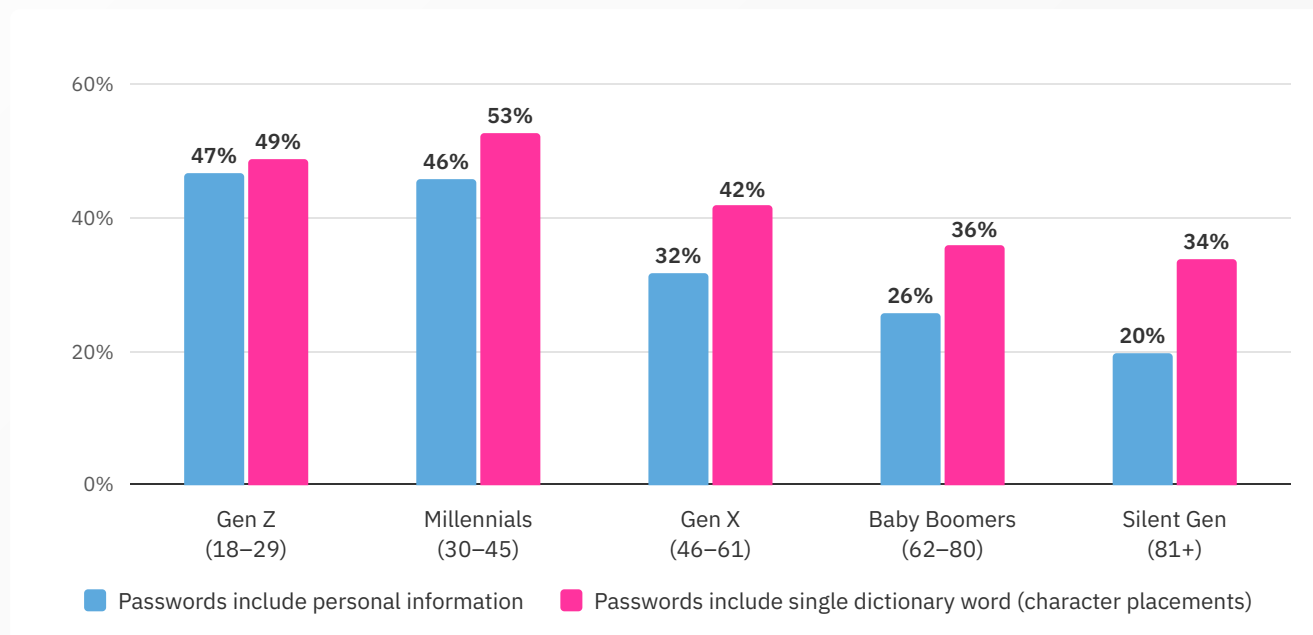
Using personal info: For the fourth straight year, the share of people stuffing personal details into their passwords rose by 1%, hitting 38%.

Dictionary word substitutions: The share of people using a single dictionary word with swapped characters (think @wes0me or Li11y) grew by 4%, hitting 46%.

And same as last year (and the year before), these shortcuts are most popular among younger users (Figure 40):

- 47% of Gen Z (-1% from 2025) and 46% of Millennials (-1% from 2025) admit to using pet names, family names, dates, or personal details in their passwords. Compare that to 26% of Baby Boomers (+4% from 2025) and 20% of the Silent Gen (-6% from 2025).
- 53% of Millennials (+2% from 2025) and 49% of Gen Z (-1% from 2025) take a single dictionary word or name and swap in numbers or symbols.

Figure 40. Password creation techniques used by participants, by generation.



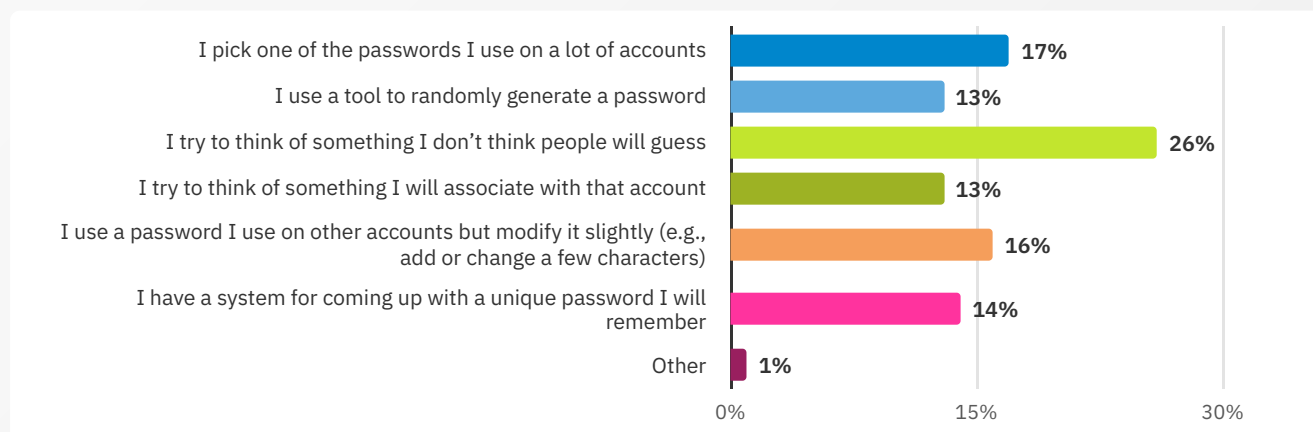
Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

What's the go-to strategy for a new account?

We introduced a brand-new question this year to pinpoint how people select passwords on the fly 🪲 (Figure 41):

- 26% try to think of something they *hope* no one else will guess.
- 17% resort to reusing a password they already use on a bunch of other accounts. (Pass the smelling salts.)
- 16% take an old password and tweak a character or two.
- 13% rely on a tool to randomly generate a brand-new string.

Figure 41. 'What best describes your typical approach to selecting a password for a new account?'



Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

5.1.2 Password management: The great notebook revival

We know how people create their passwords, but how do they keep track of them?

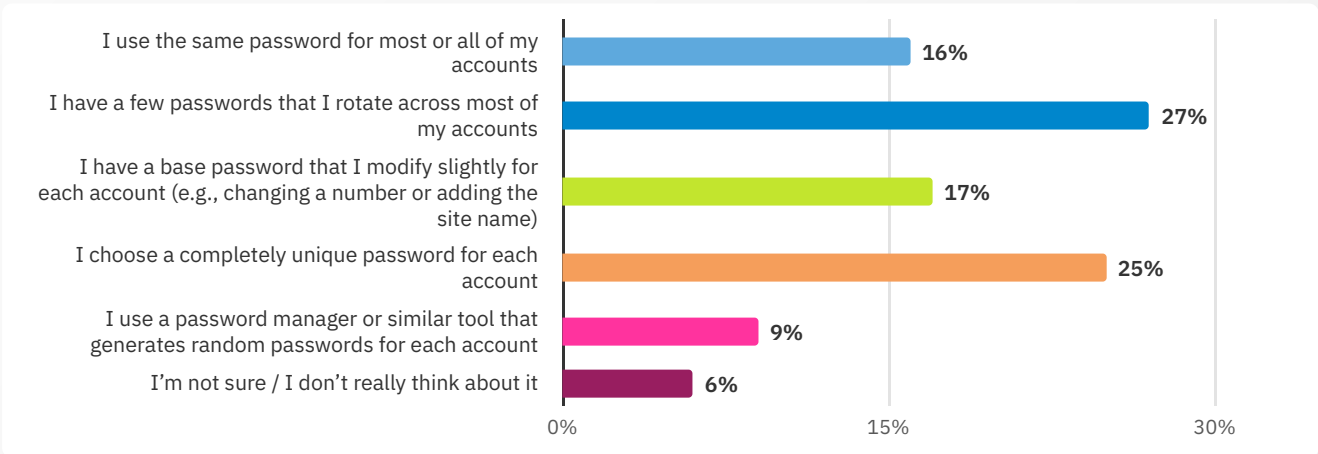
In another brand-new question exploring password management across accounts (Figure 42), we found that:

- 27% rotate a small handful of favorite passwords across different sites.
- 25% create a completely unique password for every single account.
- 17% take a single ‘base’ password and tweak it slightly per site.
- 16% use the exact same password for most or all accounts.
- 9% rely on a password manager to auto-generate and save unique strings.
- 6% admit they aren't sure or don't really think about it.

TL;DR: That means 60% of people rely on some form of password reuse, be that a single password across most accounts, a handful of passwords on rotation, or a base password with small tweaks. 34% play it safe, though, with unique credentials for every account. They either choose it themselves or get a password manager to do the job.

SEBDB BEHAVIOR [SB016: Authenticates with a unique password \(or passphrase\)](#)

Figure 42. ‘Which of the following best describes how you manage passwords across your online accounts?’



Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

When asked about their preferred storage method (Figure 43):

- 28% (-3% from 2025) prefer writing passwords down in a physical notebook.
- 23% (+2% from 2025) rely purely on memory without writing anything down anywhere.
- 30% (+1% from 2025) use informal digital shortcuts (like typing them into emails, notes apps, or hitting ‘reset password’ every time they log in).
- 19% (same as in 2025) use a dedicated app or browser-based password manager.

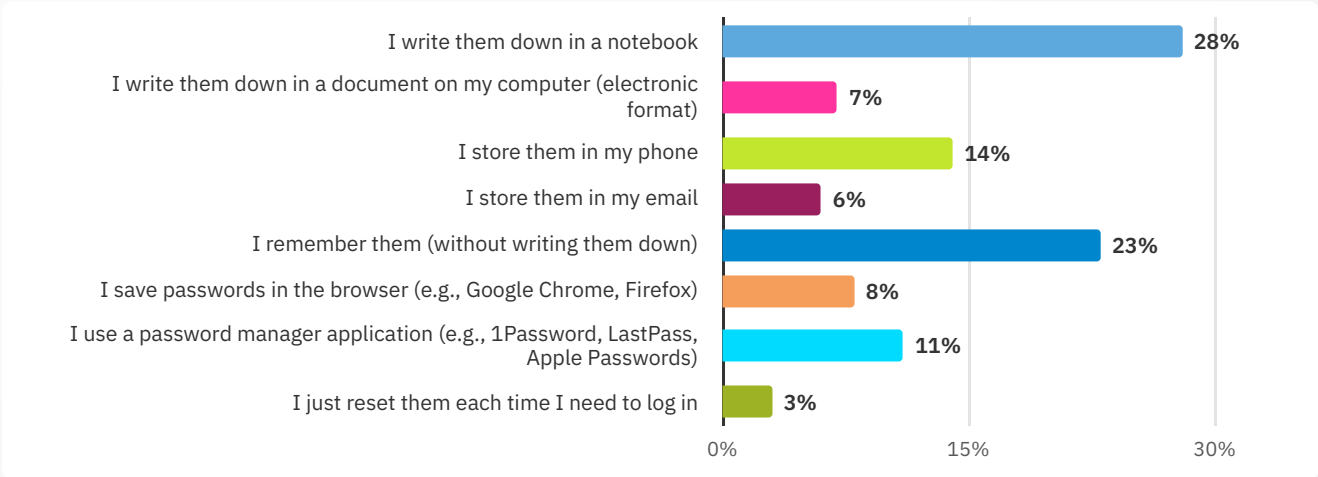
SEBDB BEHAVIORS

SB130: Stores a password (or passphrase) securely

SB209: Uses an approved or official password manager application

SB210: Uses an approved browser-based password manager

Figure 43. Preferred password management strategies.



Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

The generational notebook gap

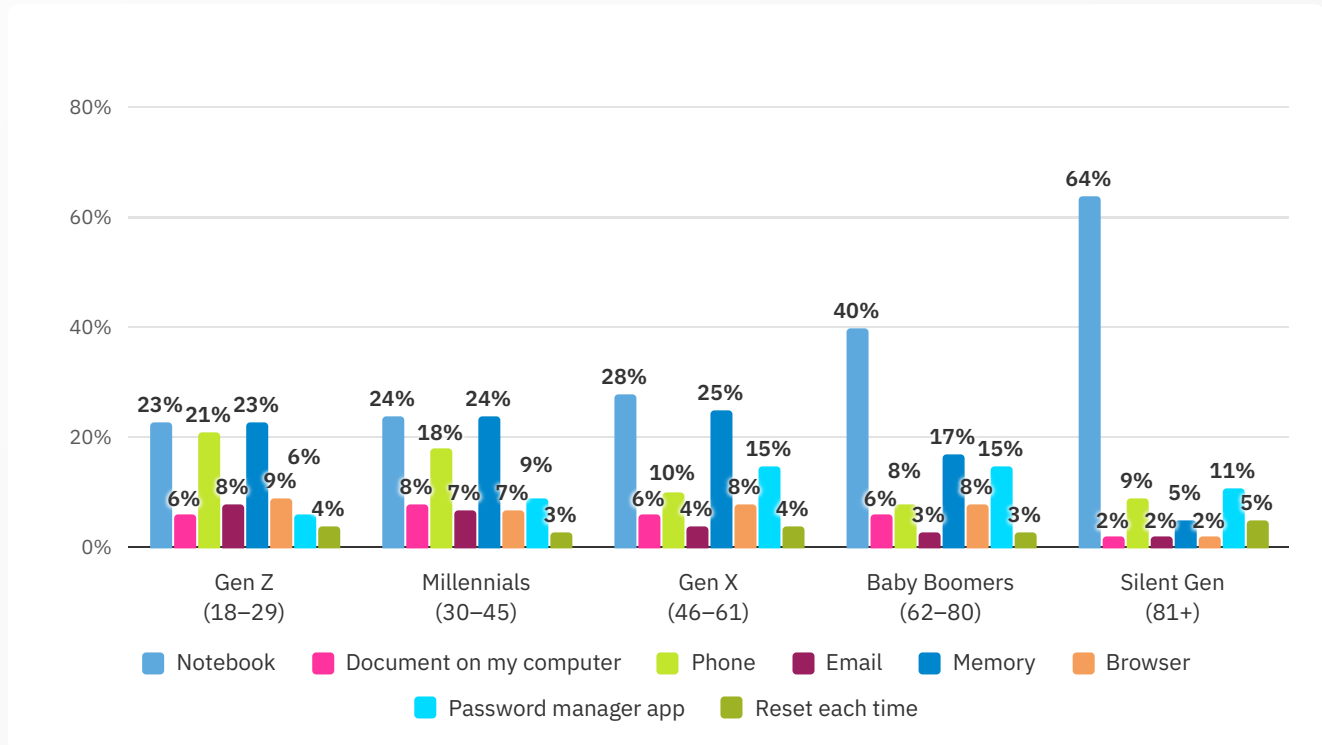
Notebook* reliance scales wildly with age (Figure 44). While 23% of Gen Z and 24% of Millennials keep a paper logbook, that number climbs to 28% for Gen X, rockets to 40% for Baby Boomers, and hits a staggering 64% among the Silent Gen – nearly tripling from youngest to oldest.

*Nothing to do with Ryan Gosling, sadly.

Meanwhile, password manager usage (combining browser vaults and dedicated apps) doesn't follow a simple linear path:

- **Gen X & Baby Boomers:** Lead the pack at 23% each.
- **Millennials:** 16%
- **Gen Z:** 15%
- **Silent Gen:** Brings up the rear at 13%.

Figure 44. Preferred password management strategies, by generation.



Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

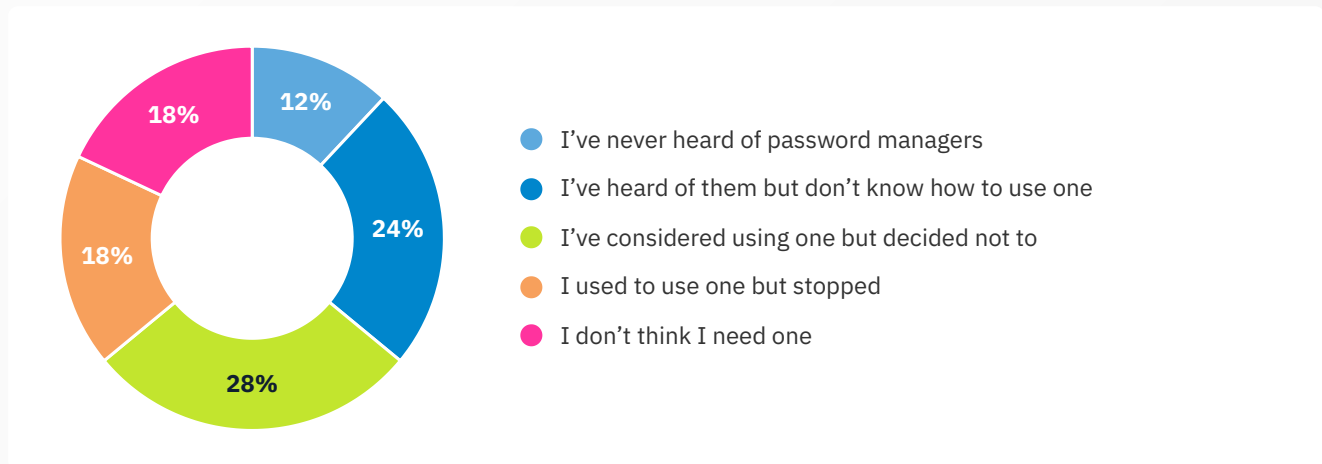
Why aren't people using password managers?

Year after year, password manager adoption, whether to manage (Figure 43) or create new passwords (Figure 42), remains surprisingly sluggish. To figure out why people are holding back, we asked non-users ($n = 4,048$) to explain their situation (Figure 45):

- 28% considered using a password manager before, but actively decided against it.
- 24% have heard of them, but have no idea how to actually set one up or use it.
- 12% have never heard of password managers at all.
- 18% tried one in the past, but gave up and stopped using it.

This all means that over a third of non-users (36%) aren't rejecting password managers out of skepticism ...they simply lack the knowledge to get started. And that's a completely different challenge than convincing the 28% who actively weighed the options and opted out.

Figure 45. 'You didn't select a password manager as one of the ways you keep track of your passwords. Which of the following best describes your situation?'



Base: US, UK, India, Brazil, Singapore. Total number of participants: 4,048 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

We asked those who don't use password managers, because they either don't think they need one, used to but stopped, or considered one but decided against it ($n = 2,578$), for their reasons why. Their top 5 reasons were:

1. 'I prefer my own password management methods because I'm more in control' (32%)
2. 'It's unnecessary to use a password manager if it isn't required' and 'Using a password manager won't stop cybercriminals' (23%)
3. 'I don't trust password managers' (22%)
4. 'I don't know which password manager to use' (17%)
5. 'There are no benefits for me to use a password manager' (16%)

5.1.3 MFA: Security need or total nuisance?

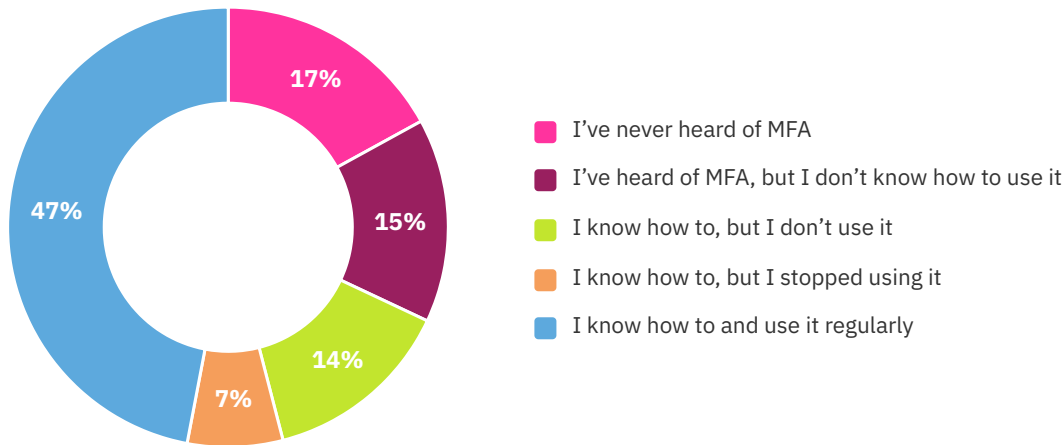
With passwords covered, let's turn to MFA. This section breaks down adoption trends, generational shifts, where MFA gets enabled, and which verification channels people actually find convenient.

For the first time since 2022, regular MFA usage bumped up to 47% (+6% from 2025, Figure 46). That's a step in the right direction, but it still leaves more than half of our total participant pool unprotected. Doh.

- 17% have never heard of MFA (-6% from 2025).
- 15% have heard of it, but don't know how to set it up (-1% from 2025).
- 21% know how to use MFA, but intentionally choose not to (+1% from 2025).



Figure 46. ‘Do you know how to use multi-factor authentication (MFA)?’



Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

Who is actually using MFA?

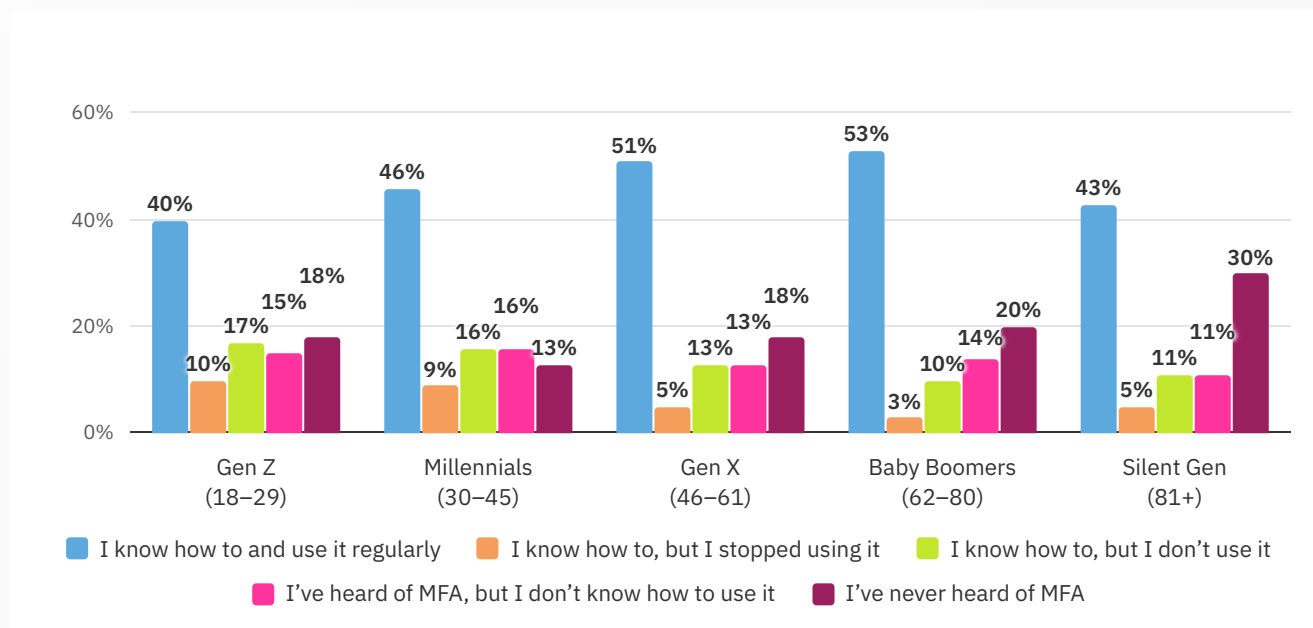
Just as in 2025, Baby Boomers took the crown 👑 for regular MFA usage at 53% (+4% from 2025), closely followed by Gen X at 51% (+8% from 2025, Figure 47).

Younger generations were less regular MFA users, and were more likely to abandon or reject MFA entirely:

- 17% of Gen Z and 16% of Millennials know how to use MFA, but choose not to.
- 10% of Gen Z and 9% of Millennials used to use MFA, but stopped.
- 40% of Gen Z and 46% of Millennials use MFA regularly.

The highest percentage of those who have never heard of MFA were the Silent Gen (30%).

Figure 47. ‘Do you know how to use multi-factor authentication (MFA)?’ by generation.



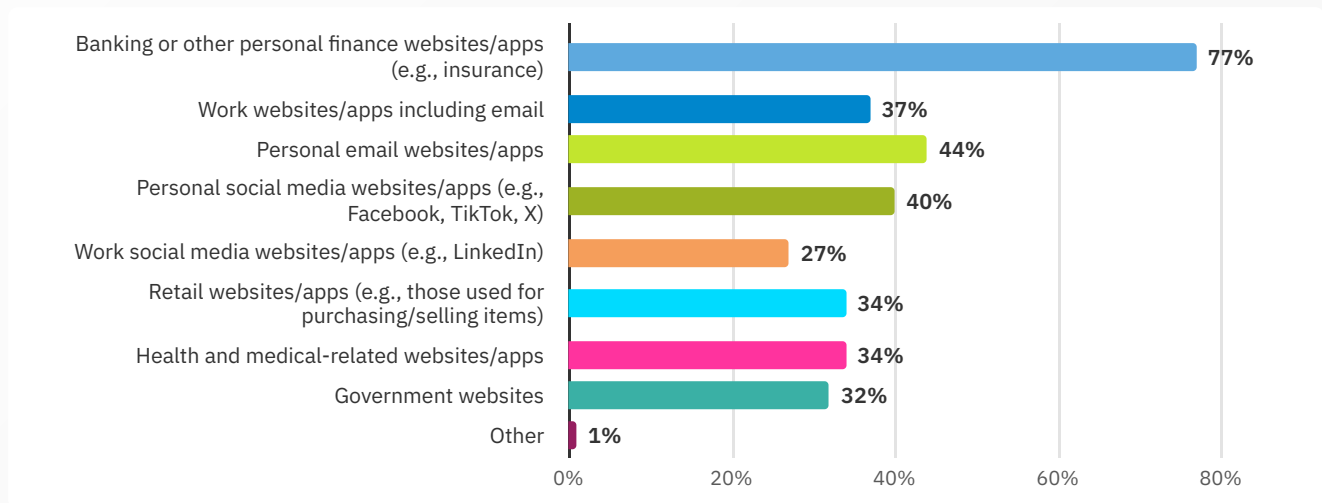
Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

Where do people enable MFA?

Among active MFA users ($n = 2,365$), financial tools dominated the field (Figure 48):

- Banking & finance apps/sites: 77%
- Personal email accounts: 44%
- Personal social media: 40%
- Work websites/apps (including email): 37%
- Work social media (e.g., LinkedIn): 27%

Figure 48. ‘Where have you enabled MFA?’



Base: US, UK, India, Brazil, Singapore. Total number of participants: 2,365 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

Why enable MFA? Personal choice vs. enforced rules

In another fresh question (we know, call us industrious if you want), we asked MFA users why they turned it on in the first place:

- 27% enabled it because the account forced them to.
- 27% turned it on purely for extra security.
- 46% turned it on for a mix of both these reasons. 🙌

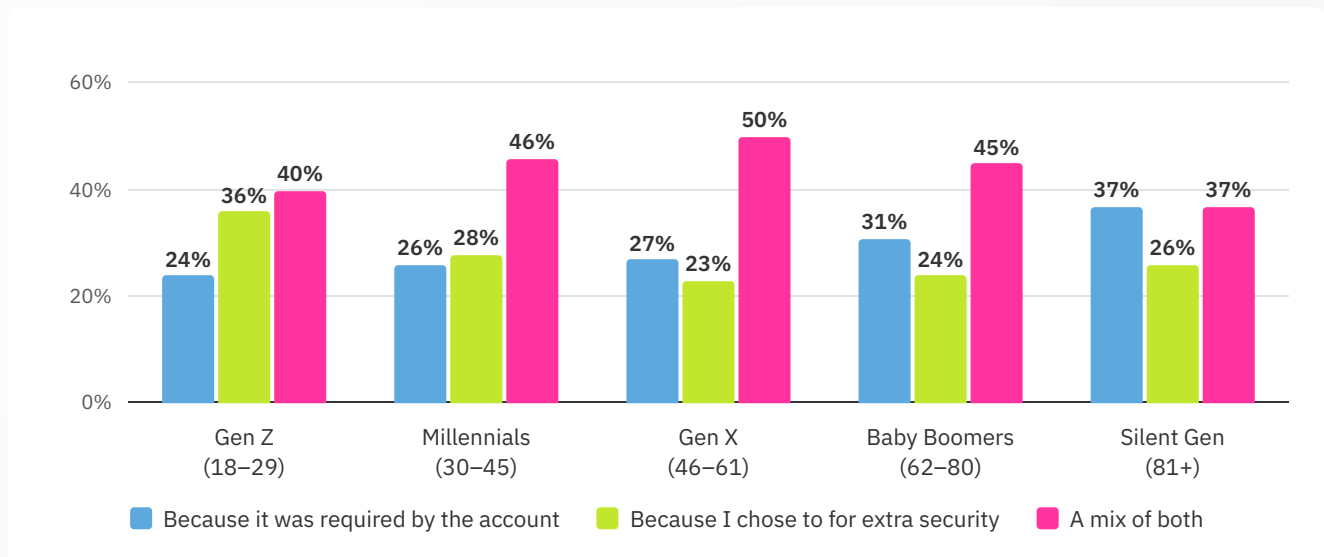
The generational trends here are striking (Figure 49). Younger users are far more likely to turn MFA on proactively for extra security:

- Gen Z: 76%
- Millennials: 74%
- Gen X: 73%
- Baby Boomers: 69%
- Silent Gen: 63%

By contrast, older users are much more likely to enable MFA only when forced by the platform: Looking strictly at people who turned on MFA solely because it was required (with zero personal choice involved): Gen Z (24%), Millennials (26%), Gen X (27%), Baby Boomers (31%), and Silent Gen (37%) – showing a clean, steady rise in parallel with age.

So, interestingly, younger users seem to proactively seek out extra security, while older generations tend to adopt security features when platforms mandate them. Keep up ol’ timers.

Figure 49. 'For the accounts where you use MFA, would you say you enabled it mostly...' by generation.



Base: US, UK, India, Brazil, Singapore. Total number of participants: 2,365 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

Why non-users opt out and what convenience looks like

When we pressed non-MFA users ($n = 1,785$) on why they hold out, their top 5 responses were:

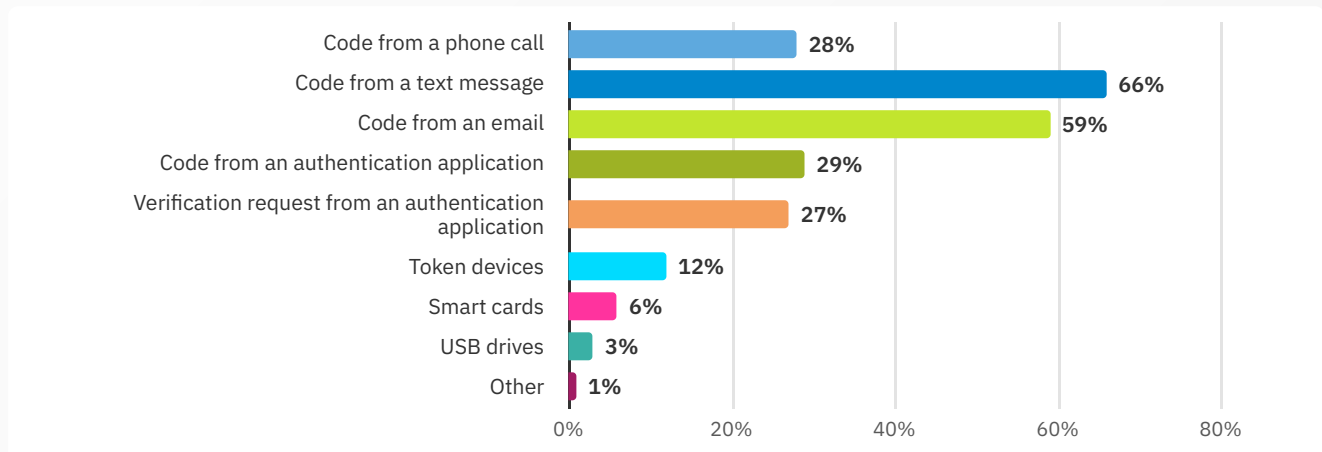
1. 'My password alone is strong enough' (30%)
2. 'I don't understand how to use MFA' (28%)
3. 'It's unnecessary to use MFA if my device works as it should' and 'I have no confidence in my ability to use MFA' (20%)
4. 'There aren't any benefits for me to use MFA' and 'I don't always have my phone with me to verify' (19%)
5. 'I don't have the time to use MFA' (18%)

And talking about MFA, we asked participants which second-factor authentication methods they find convenient to use (Figure 50):

- SMS text codes: 66% (Most convenient)
- Email codes: 59%
- Auth app codes: 29%
- Phone calls: 28%
- Auth app push prompts: 27%
- Smart cards: 6%
- USB security keys: 3% (Least convenient)

It's wild that 66% of people view SMS codes as their go-to method, considering NIST officially deprecated SMS-based 2FA over a decade ago due to SIM-swapping and interception vulnerabilities, i.e., because it's not considered secure.³⁵

Figure 50. 'After entering your password to log in to a website or app, you may be asked to use another method to verify your identity. Which one of these would you find convenient to use?'



Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

5.1.4 Beyond passwords: Biometrics & passkeys

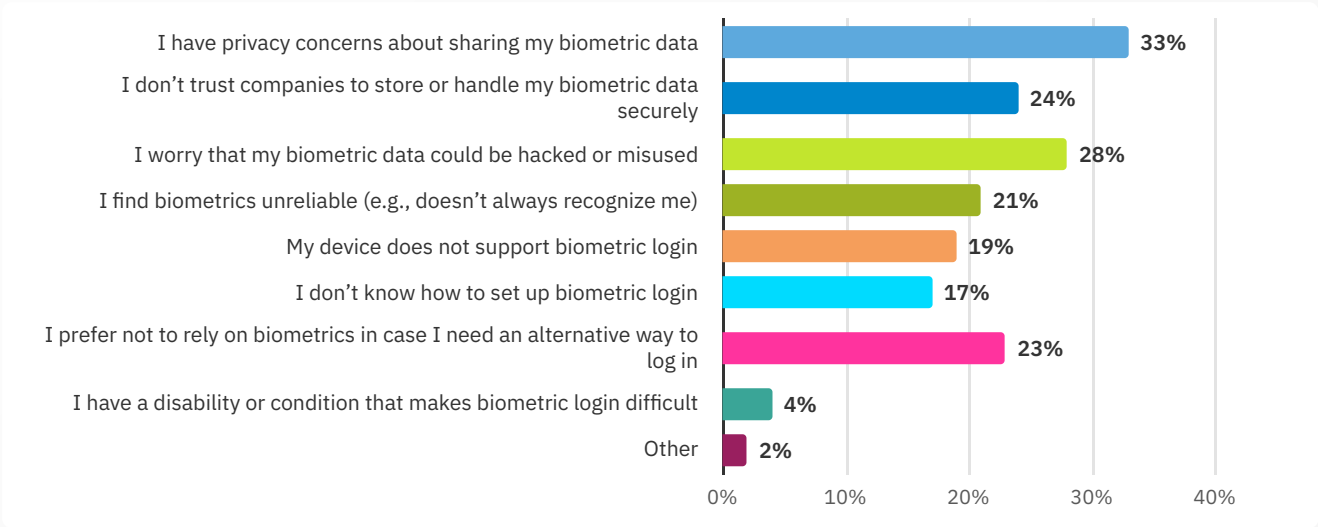
As noted earlier, only 53% of people use biometrics to log in to their accounts. Given how fast biometric tech has expanded, we wanted to understand why the remaining 47% are digging their heels in (think donkey/mule and you won't be far off). 🐴

The top reasons for skipping biometrics (Figure 51):

- **Privacy concerns:** 33% worry about sharing biometric data in general.
- **Fear of breaches:** 28% worry biometric data could be hacked or misused.
- **Distrust of corporate storage:** 24% don't trust companies to handle their data safely.
- **Alternative access fears:** 23% want a backup log-in method if biometrics fail.
- **Reliability doubts:** 21% simply find biometrics glitchy or unreliable.

³⁵ Coldewey, D. (2016, July 25). *NIST declares the age of SMS-based 2-factor authentication over*. TechCrunch. <https://techcrunch.com/2016/07/25/nist-declares-the-age-of-sms-based-2-factor-authentication-over/>

Figure 51. ‘What are your reasons for not using biometrics to log in to your online accounts?’



Base: US, UK, India, Brazil, Singapore. Total number of participants: 2,342 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

In their own words: Major biometric fears

When non-users detailed their concerns in open-ended write-ins, four primary worries emerged:

1. **The irreversibility factor:** Passwords can be reset if compromised; face geometry and fingerprints can't.

“*‘My main concern is that unlike a password, biometric data cannot be changed if it is hacked or stolen, which creates a permanent privacy risk.’*

P1678, USA

“*‘I can't change it if it leaks. If it's stolen I can't get new face or fingerprints. I will be stuck with compromised biometrics for life. If a password gets stolen, I can reset it.’*

P5174, India

2. **Corporate custody distrust:** Suspicion over where biometric scans are stored, who gets access, and whether data gets sold behind closed doors.

“*‘I'd worry about how my biometric data is stored and whether it could be stolen if the system gets hacked. I also don't like the idea of companies having permanent access to something as personal as my fingerprints or face.’*

P1510, USA

3. **Physical coercion threats:** Fear of being forced to unlock devices under duress.

“ ***‘I don't use biometric data to log in because if I am forced by a person to log in, they can easily use my biometric data such as fingerprint or face data.’*** ”

P3715, India

4. **AI-enabled spoofing:** Deepfake models and synthetic replication beating biometric sensors. A notable subset of respondents raised concerns about AI-enabled spoofing, expressing worry that generative AI could be used to replicate their face or fingerprints to gain unauthorized access to their accounts.

“ ***‘If someone could reproduce my image without consent using artificial intelligence, they could access accounts I try to protect.’*** ”

P10441, Brazil

“ ***‘I believe biometric data could be used by bad actors to surveille people and create AI impersonators.’*** ”

P57491, USA

The passkey knowledge trap

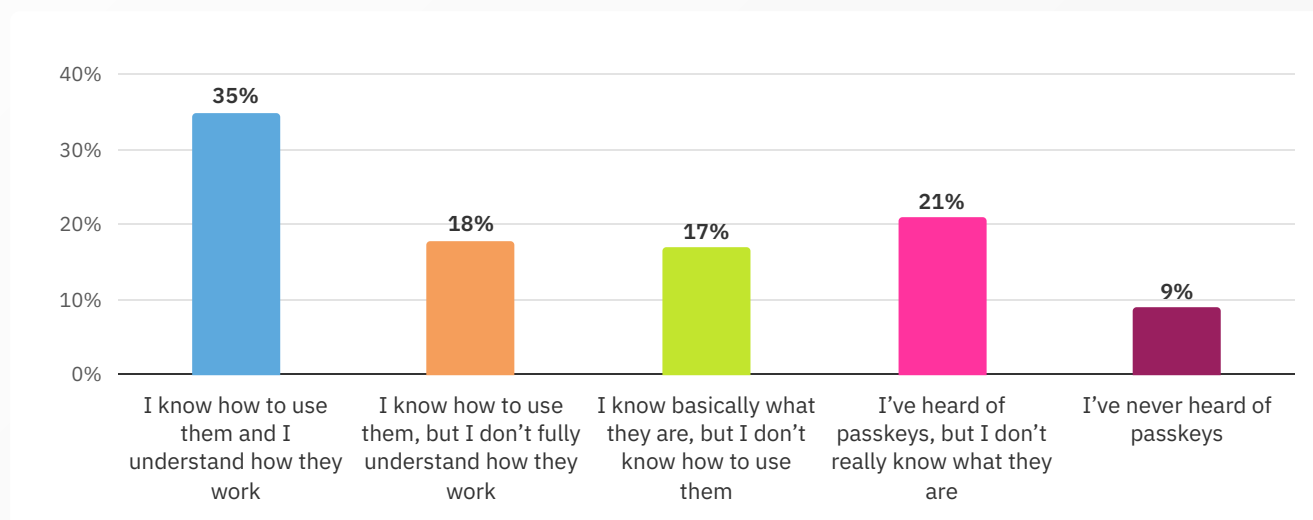
So, as we mentioned, only 39% of our overall sample uses passkeys. But the question this raises, is why? Could adoption be low because people don't know what they are?

When we asked participants about passkey awareness (Figure 52):

- 35% know how to use passkeys and understand how they work.
- 18% know how to use them, but don't fully get the underlying tech.
- 17% understand the basic concept, but don't know how to set them up.
- 21% have heard the term, but don't know what passkeys actually are.
- 9% have never heard of passkeys at all.

So, the majority of people know (or sort of know) what passkeys are and how to use them. Yet adoption is at 39%. This suggests there are other friction points at play when it comes to low adoption. (Stay tuned: we could dig into those underlying blockers in next year's report. 🤔)

Figure 52. 'Do you know what passkeys are?'



Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

📌 KEY TAKEAWAYS: SUBCHAPTER 5.1

01

Good intentions don't equal good passwords: Most people claim they know how to make strong passwords, yet personal info and single dictionary words are everywhere, especially among Gen Z and Millennials.

02

Password reuse reigns supreme: More people recycle base passwords across sites (or use slightly modified ones) than create genuinely unique passwords for every account.

03

Notebooks beat password managers: Writing passwords down in physical paper notebooks is far more popular than using password manager apps or browser vaults. Over a third of non-users simply don't know how password managers work.

04

MFA use driven purely by account requirement (rather than personal choice) increases with age: Over half of people skip MFA. Among those who use it, younger users opt in for extra security, while older generations turn it on because platforms force them to. (They're a compliant bunch, we'll give them that).

05

The #1 reason people skip MFA? They believe their password alone is strong enough: Other common reasons include not understanding how MFA works, thinking it's unnecessary if their device works, and having no confidence in their ability to use it.

06

Low adoption of passkeys and biometrics isn't a knowledge problem: Most people understand the basics of how passkeys work, though far fewer actually use them. Hesitation about biometrics stems from permanent privacy risks and corporate distrust.

5.2 Snooze or software patch? How we handle Update Available pop-ups

Keeping devices safe is a continuous, never-ending game of cat-and-mouse ...and (precariously) it hinges heavily on pressing ‘Update now’. Security updates and software patches are our first line of defense against brand-new vulnerabilities and zero-day threats. But that button is easy to press, and (yep, you guessed it) just as easy *not* to press.

In this subchapter, we examine participants’ self-reported habits around installing updates, looking at overall adoption trends, generational habits, and the exact timing (and frequency) of when people actually click ‘Install’.

When asked if they know how to install updates:

- 64% of participants reported knowing how to and installing the latest software and application updates across their devices – a 4% increase since 2025.
- The share of people who know how to update but choose not to anyway dropped by 3%, down to 20%.
- 16% say they don’t know how to install updates (-1% from 2025).

When asked how often they installed updates:

- Over half (55%) update their devices ‘always’ or ‘very often’ (-1% from 2025).
- 30% update ‘sometimes’ (+1% from 2025).
- 10% ‘rarely’ perform software updates (-1% from 2025).
- Only 5% (*n* = 223) admit they never update their devices.

The generational snooze-fest: Who updates immediately?

When it comes to clicking ‘Update’, there’s a massive divide between generations (Figure 53). Older age groups are far more disciplined about patching immediately, while younger crowds prefer to play the waiting game.

The fast patchers:

- **Baby Boomers:** 38% (-3% from 2025) always update as soon as they receive a notification.
- **Silent Gen:** 36% (-1% from 2025) always update immediately.

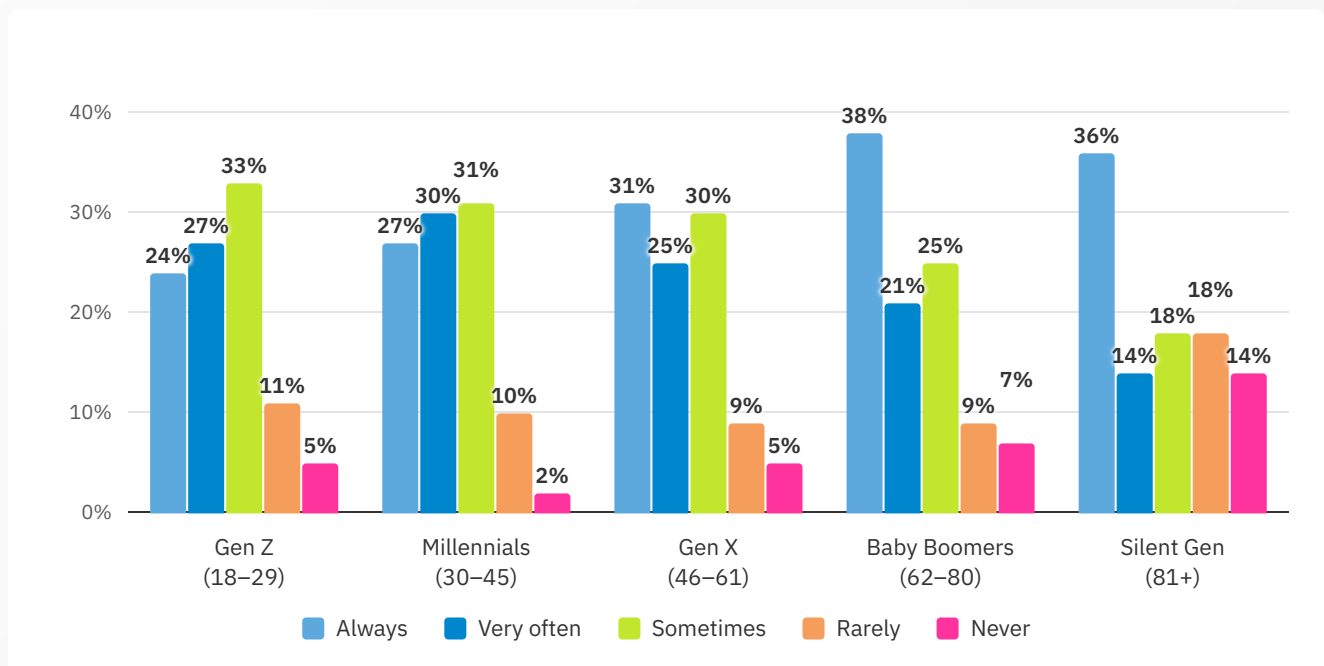
- **Gen X:** 31% (-4% from 2025) always update right away.

The 'I'll do it later' crew:

- **Gen Z:** 33% (-1% from 2025) only perform software updates 'sometimes'.
- **Millennials:** 31% (-2% from 2025) also only 'sometimes' hit 'Update' (though 30% do it 'very often').

SEBDB BEHAVIOR SB024: Keeps software up-to-date

Figure 53. 'How often do you install the latest software or application updates to your devices when notified that they are available?' by generation.



Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

Timing is everything: When do updates *actually* happen?

Among the participants who update their devices at least *sometimes* ($n = 4,289$), we looked at their go-to strategies for getting it done:

- 38% turned on automatic updates (the ultimate set-and-forget victory).
- 32% update immediately upon receiving a notification pop-up.
- 19% hit 'Remind me later' a few times before finally giving in.
- 11% only update when they are away from or not using their devices.

 TOP TIPS: DEFEATING THE 'REMIND ME LATER' TRAP

Getting people to stop hitting 'Remind me later' isn't easy, but smart behavioral nudges can tip the scales:

1. **Default to auto-update:** People naturally go with the flow. Making automatic updates the out-of-the-box default is an effortless win for any organization.
2. **Roll out updates people trust:** Nothing kills update adoption faster than a buggy patch that crashes apps. Rigorous pre-deployment testing keeps user trust intact.
3. **Respect people's schedules:** Give users flexibility. Allowing updates to run over lunch breaks or at the end of the workday ensures security fits smoothly into daily routines.

 Further reading:

- [Stay Safe Online's Why Software Updates Matter](#) – A practical guide on how patches defend against emerging threats.
- [CybSafe's Blog: Why Are You Snoozing Updates?](#) – A deeper look into the behavioral hurdles stopping people from updating.

 KEY TAKEAWAYS: SUBCHAPTER 5.2**01**

Most people update, but some opt out: The majority of people surveyed know how to update their software (and actively do so) with more than half installing updates 'always' or 'very often' when notified, and only a small share never doing so. About a fifth of participants know how to update their devices but choose not to.

02

Older generations lead the charge on immediate updates: Baby Boomers, Silent Gen, and Gen X are far more likely to update immediately upon notification compared to Gen Z and Millennials, who default to 'sometimes'.

03

Automated updates take the crown 🏆: Among active updaters, setting systems to update automatically is the single most common approach, outperforming manual immediate updates and snoozing.

5.3 Back it up, pack it in: Backing up data

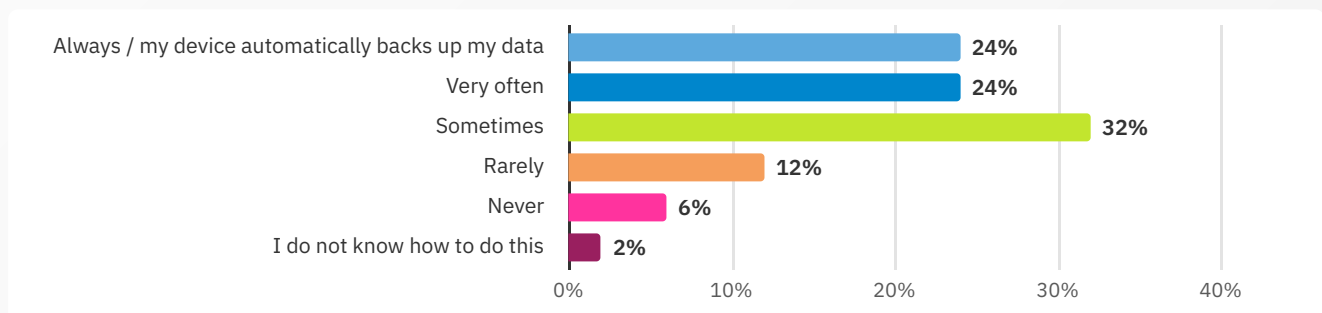
Having a backup strategy is like having car insurance ...you hope you never need it, but if disaster strikes, it's a total lifesaver. 🛟

When we asked participants how frequently they back up their most important digital files (Figure 54):

- 48% (+1% from 2025) report backing up important data 'always' or 'very often'.
- 32% (+1% from 2025) report backing up 'sometimes'.
- 18% (-1% from 2025) report that they 'rarely' or 'never' back up their data.

SEBDB BEHAVIOR SB061: Backs up data

Figure 54. 'How often do you back up your most important data?'



Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

While having 80% of participants backing up at least occasionally sounds hugely encouraging, context is critical here:

- **At work:** In most modern professional environments, data backups are automated, centrally managed, and handled in the background by IT departments – requiring zero direct effort from individuals.
- **At home:** In personal lives, the burden shifts entirely to the individual. Keeping personal photos, tax forms, and documents safe relies heavily on manual effort or user-configured cloud subscriptions.

📌 KEY TAKEAWAYS: SUBCHAPTER 5.3

01

Nearly half are consistent backup champions:

They 'always' or 'very often' back up their critical data.

02

A third are hit-or-miss: They only back up 'sometimes', while nearly a fifth 'rarely or never' back up their information.

 TOP TIPS: BOOSTING BACKUPS & BUILDING SAFETY NETS

Backups are only lifesavers if they actually exist before a crisis happens. So, in exactly that spirit, here are five practical ways to drive adoption:

1. **The 3-2-1 gold standard:** Keep three copies of important data across two different media types, with one offsite. Simplify this by providing encrypted flash drives or secure cloud storage.
2. **Automate everything:** Schedule automatic cloud syncs and system-level defaults. When backups require zero user effort, compliance skyrockets.
3. **Shout about the ease:** People often assume backing up is tedious and complicated. Show them how quick and painless it actually is to raise adoption rates.
4. **Build a 'set-and-forget' backup culture:** Treat backups as a standard operational habit, not an optional extra. Make automated cloud backups as standard as locking the front door.
5. **Celebrate the backup champions:** Spotlight people who keep their backups up to date. Positive recognition and gentle monthly reminders move the needle far better than scare tactics.

 Further reading:

- [CybSafe's Guide to Making Data Backups Habitual](#) – How to make backing up a seamless part of daily life.
- [Stay Safe Online's Backup Guide](#) – Essential tips for securing critical digital files.

5.4 Catch me if you can: Recognizing & reporting phishing messages

As cybercriminals get more sophisticated – especially with generative AI in their dastardly toolkit – phishing remains one of the most persistent, widespread and highly effective digital threats.

In past reports, we measured phishing detection confidence with a single 'umbrella' question. But cybercriminals don't stick to emails anymore ...they've branched out. So, this year, we've broken things down across four distinct channels:

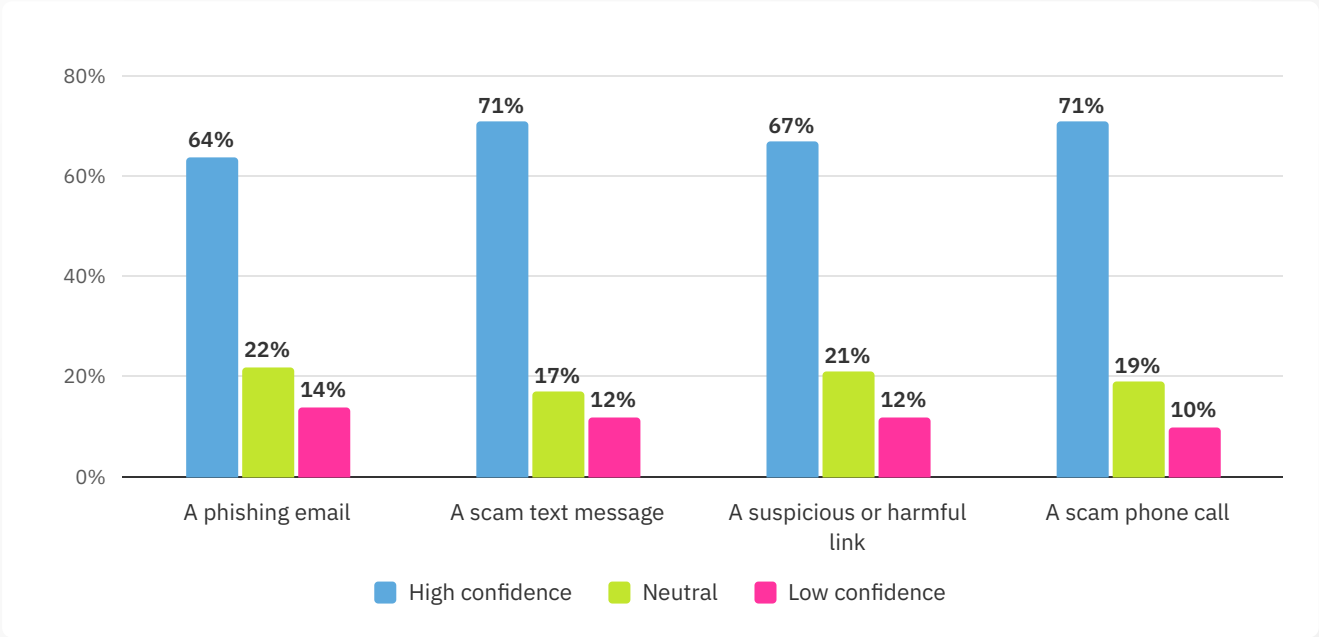
- Phishing emails
- Scam text messages
- Suspicious or harmful links
- Scam phone calls

5.4.1 Spotting the bait: How good are we at catching phishes?

In this section, we take a peek at the human side of the digital cat-and-mouse game. We compare how confident people *feel* about spotting shady messages versus what they *actually do* when a weird message lands in their inbox (from playing detective with spelling mistakes to directly contacting the sender for confirmation). Finally, we look at how often people actually push that Report Phishing button ...and the (occasionally surprising) roadblocks that stop them from hitting it.

Here’s what we found (Figure 55): People feel most confident about calling out scam texts (71%) and dodgy phone calls (71%). Identifying a sneaky link comes in second (67%), while phishing emails make people sweat the most (64%).

Figure 55. ‘How confident are you in your ability to identify each of the following?’



Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

Mirror, mirror on the wall, who’s the most confident of them all? (by generation)

When we slice the data by age groups (Figure 56), Millennials confidently take the crown across almost every category (Slay queens):

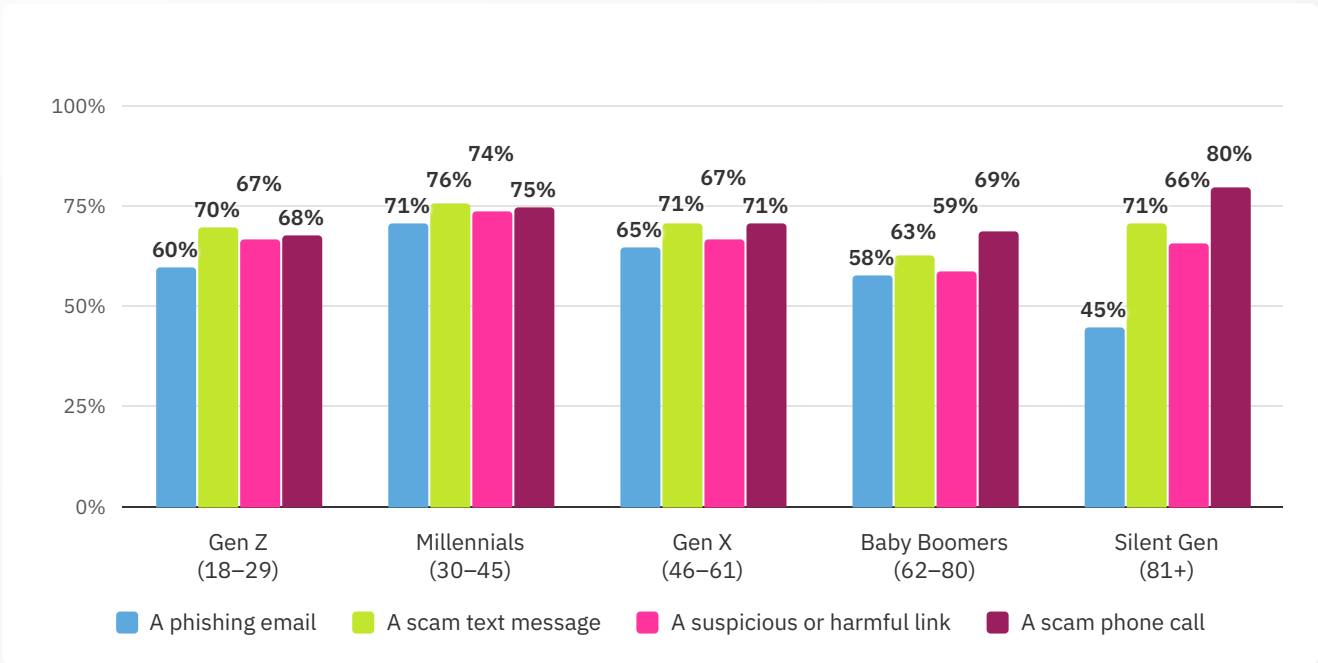
- 76% feel confident spotting scam texts.
- 74% feel confident spotting suspicious links.
- 71% feel confident identifying phishing emails.

Baby Boomers, on the other hand, sit at the bottom of the scoreboard for two categories: scam text messages (63%) and suspicious/harmful links (59%). Putting the ‘boo’ in boomer, if you will. Gen Z, meanwhile, reports the lowest confidence of any generation on scam phone calls (68%), making this the one category where the generation seen as most digitally native isn't leading the pack. You can’t win ‘em all, Gen Z.

💡 Special shoutout: The Silent Generation

The Silent Gen showed a fascinating split personality with their confidence levels. They reported the absolute lowest confidence of any generation when it came to phishing emails (45%), but turned right around to claim the highest confidence among all generations when identifying scam phone calls (80%). That's a massive gap ...far wider than any other age group.

Figure 56. ‘How confident are you in your ability to identify each of the following?’ by generation.



Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

The workplace advantage: Employment status

Does having a day job make you sharper at spotting scams? ...

The numbers say yes.

Participants in full- or part-time employment reported the highest confidence across all four categories, ranging from 69% for phishing emails up to 75% for scam texts.

Meanwhile, confidence took a noticeable dip among other groups:

- **Students:** 52% to 68% confidence across categories
- **Retirees:** 57% to 68% confidence across categories
- **Not in active employment:** 52% to 63% confidence across categories

Those not in active employment reported the lowest confidence levels for three out of the four threats (scam texts, suspicious links, and fraudulent phone calls).

Fact vs. fiction: Do our behaviors match our confidence?

Sure, overall confidence is high, but do people actually put on their detective hats before clicking? 🕵️ Let’s look at their actual habit of inspecting messages before engaging (Figure 57).

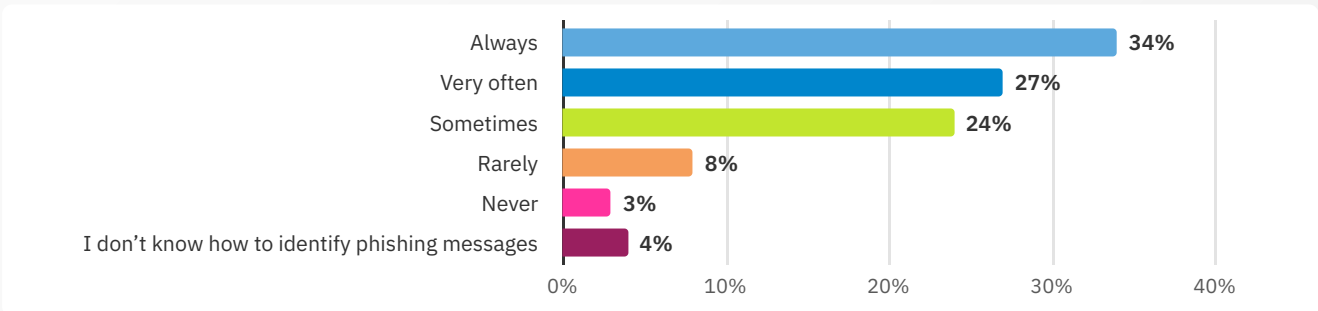
- 61% say they ‘always’ or ‘very often’ inspect messages for signs of phishing before clicking or replying. (A slight 2% drop from 2025).
- 11% admit they ‘rarely’ or ‘never’ check before clicking. (Up 1% from 2025).
- 4% openly confess they simply don't know how to spot a phishing message. (Unchanged from 2025).



SEBDB BEHAVIOR

[SB081: Checks a message for signs of deception](#)

Figure 57. Frequency of checking messages for signs of phishing before taking action.



Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

Playing detective: What steps do people actually take?

We asked the participants who inspect their messages at least occasionally (*n* = 4,635) to give us a peek at their playbook. What do they look for when evaluating a message?

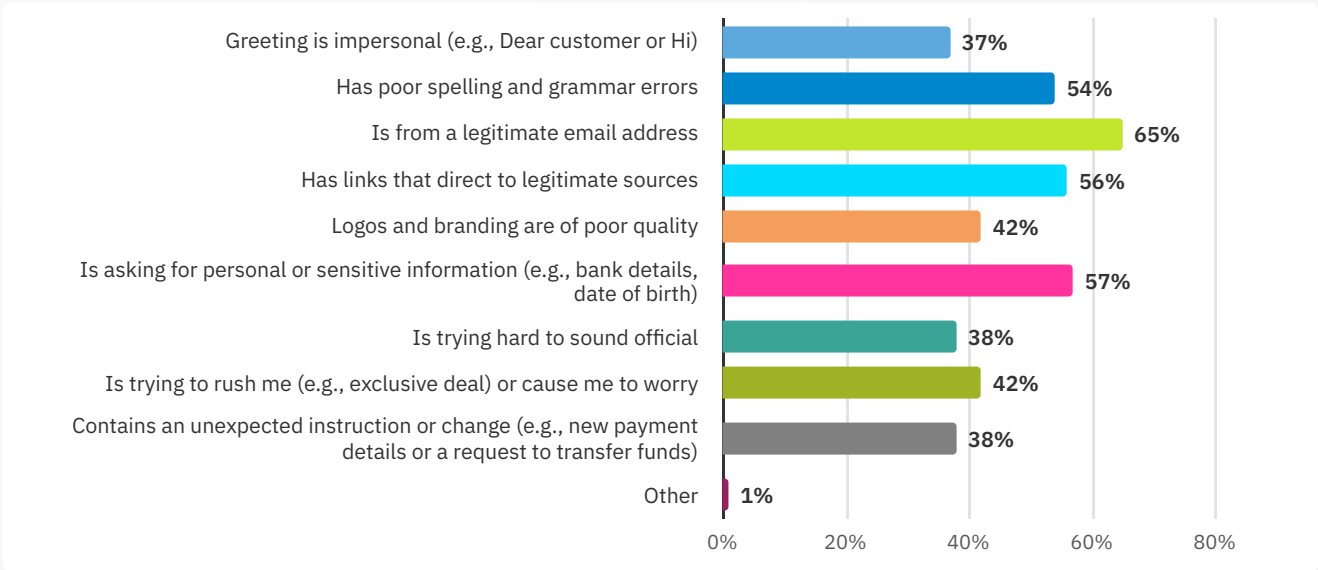
The most common verification step was checking whether the message is from a legitimate email address (65%, Figure 58). This was followed by checking whether the message is asking for personal or sensitive information (57%), whether it has links that direct to legitimate sources (56%), and whether it has poor spelling and grammar errors (54%).

Participants were less likely to check for poor-quality logos and branding, or whether the message was trying to rush them into acting (42% each), and less likely still to check whether it sounded overly official or contained an unexpected instruction or change (38% each). Checking whether the greeting was impersonal was the least common step of all (37%).

“*If I am suspicious of it [a phishing message], I just delete the thing.*”
P2612, UK

SEBDB BEHAVIOR SB081: Checks a message for signs of deception

Figure 58. Steps taken to verify message legitimacy – ‘I check whether the message...’



Base: US, UK, India, Brazil, Singapore. Total number of participants: 4,635 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

Checking in: Reaching out to the sender directly

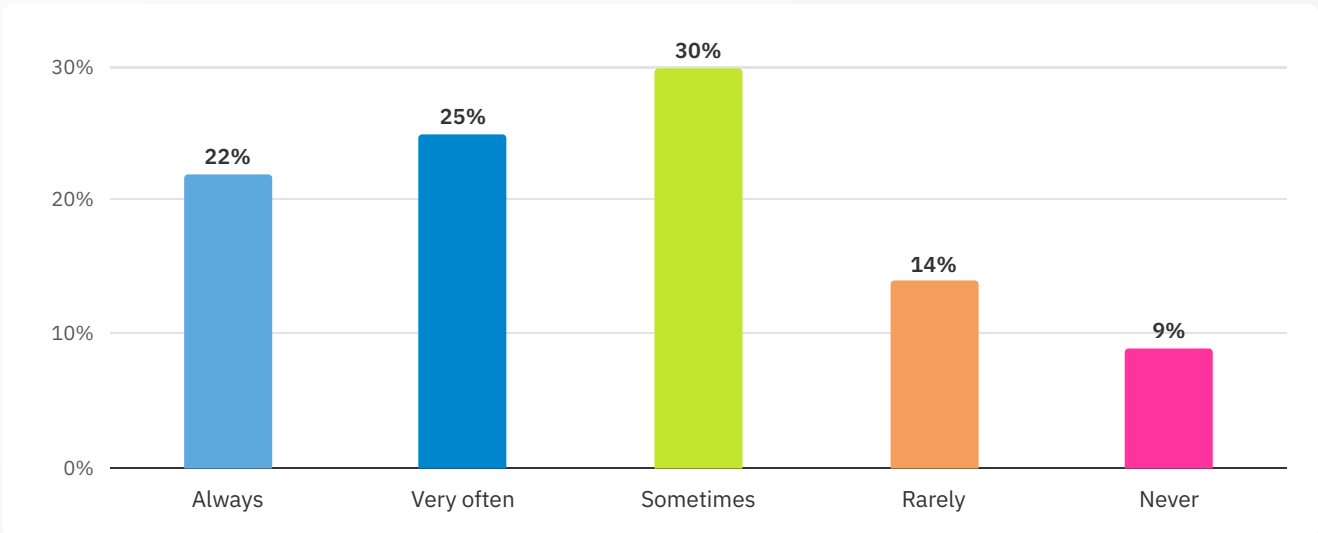
What about picking up the phone or sending a separate message to confirm if a request is real (Figure 59)?

- 47% now ‘always’ or ‘very often’ verify directly with the sender before clicking links or opening attachments when they’re unsure. (A fantastic +6% improvement from 2025.)
- 23% say they ‘rarely’ or ‘never’ contact the sender directly. (Down 9% from 2025).
- 30% fall in the middle, verifying directly only ‘sometimes’. (Up 3% from 2025).



SEBDB BEHAVIOR SB082: Verifies a suspicious message using known contact details

Figure 59. ‘How often do you check with the sender directly before clicking a link or opening an attachment in a message you’re unsure about?’



Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

Inspecting the web: How people spot fake sites

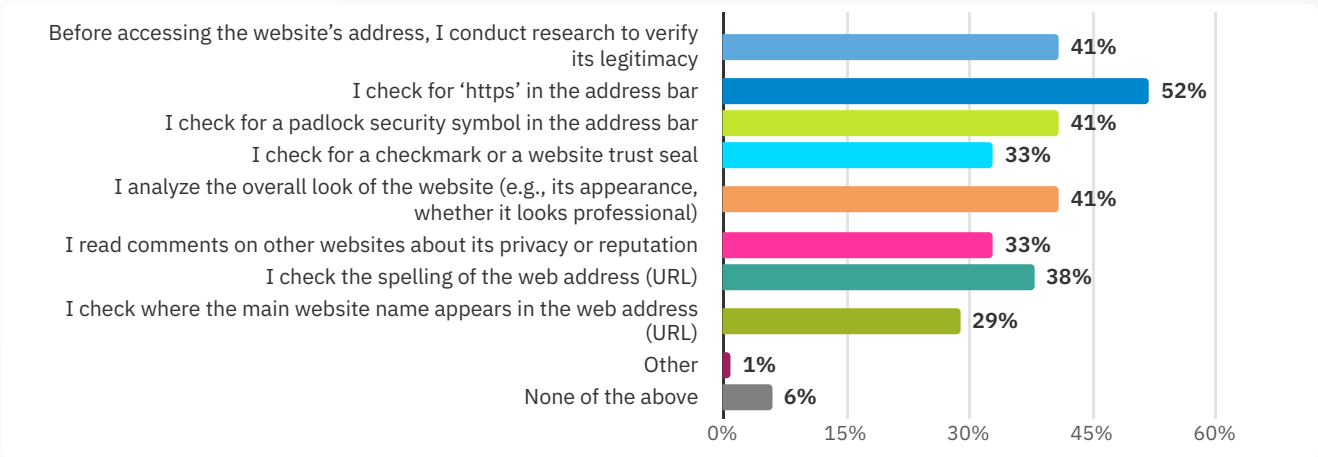
Before browsing or typing in details, what steps do people take to ensure a website is safe (Figure 60)?

The top verification methods were:

- **Checking for 'https:' in the address bar:** 52%
- **Looking for the padlock symbol:** 41%
- **Eyeballing the overall look/feel of the site:** 41%
- **Doing background research on the site first:** 41%

SEBDB BEHAVIOR SB058: Checks a website for signs of deception

Figure 60. Steps taken to verify website legitimacy.



Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

5.4.2 Sounding the alarm: Reporting phishing messages

Recognizing a scam is one thing, but alerting the authorities (or your IT department) is quite another. So, how good are we at actually reporting these so-called 'bad actors' (Figure 61)?

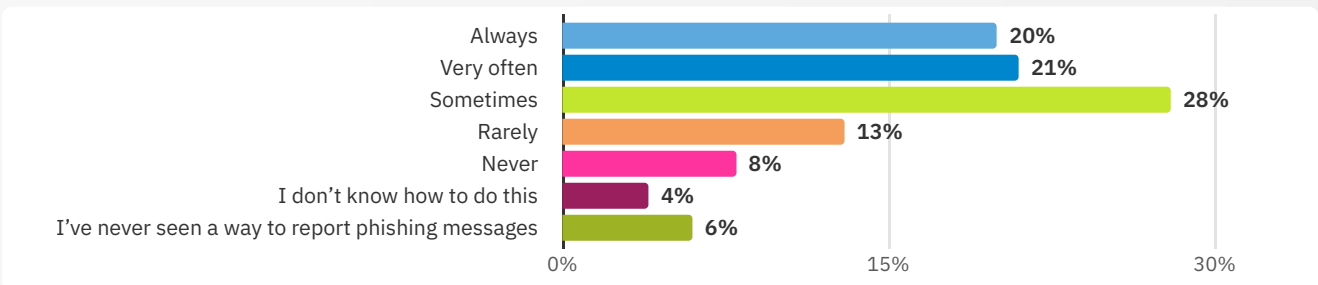
Turns out, not as good as we could be:

- 41% 'always' or 'very often' report phishing messages. (-4% from 2025).
- 21% 'rarely' or 'never' bother reporting. (Unchanged from 2025).
- 10% don't know how to report phishing, or have never seen an option to do so. (+2% from 2025).

That leaves 31% of people taking no action against cybercriminals when they come across a scam. 🙄

SEBDB BEHAVIOR SB087: Reports a suspicious message

Figure 61. 'How often do you report phishing messages (e.g., email or social media) by using the 'spam' or 'report phishing' button?'



Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

‘I would report it, if...’: What would drive action?

We asked the non-reporters (n = 1,049) what would motivate them to start pressing that report button. Here’s what would push them to take action:

'I would report phishing emails, if...'	
It helped to stop cybercriminals	65%
It would stop spam messages from getting into my inbox	63%
I understood how to report them	60%
I had confidence in my ability to correctly identify phishing emails	59%
I trusted the phishing reporting process	58%
Something would happen when I report them	57%
I had time to report them	53%
There were some benefits for me to report them	49%
I saw negative consequences of people falling for phishing emails	49%

 KEY TAKEAWAYS: SUBCHAPTER 5.4

01

Confidence is high, but emails are tricky: People feel super confident spotting scam texts and calls, but drop their guard slightly for links and emails. Millennials take the crown as the most confident generation in most categories – they report the highest confidence in recognizing phishing emails, scam texts, and suspicious links, though the Silent Generation edges ahead on scam phone calls. Close to a clean sweep there, Millennials ...but no cigar.

03

Reporting lags behind detection: Less than half of participants regularly hit the report button when they spot a scam, leaving nearly a third taking no action at all to stop bad actors.

02

Checking habits need a boost: Overconfidence might be making us lazy. 🤪 Only 3 out of 5 people consistently check messages for warning signs before clicking links or replying.

04

Motivation and feedback are missing: Non-reporters want to help stop criminals and clear out spam, but they get held back by confusing reporting tools, lack of confidence, and a feeling that their report just goes into a black hole.

 TOP TIPS: STAYING SAFE FROM PHISHING

Protecting your team from phishing isn't about turning everyone into a cybersecurity expert (if only that were possible, we could all rest easy, and maybe take more holidays 🌴). It is about building quick habits, encouraging open reporting, and focusing on real behavior change rather than just test scores.

1. Keep guidance simple and actionable

Don't overload users with complex technical checks. Teach people to ask three quick questions:

1. Does the 'from' address actually match the sender?
2. Is this asking me to do something out of the ordinary?
3. Does it include a link or attachment I wasn't expecting?

2. Look far beyond click rates

Stop measuring security success purely by how many people fell for a simulated phishing email. Focus on *why* they clicked. Use quick point-of-click surveys or integrate psychology-based templates to uncover root causes, then craft personalized follow-ups beyond just more training.

3. Make reporting seamless and rewarding

Eliminate friction. The reporting process should take one click. Send instant automated thank-yous and periodic updates on what action was taken (e.g., *'Your report helped block 50 spam emails today'*). Crucially, banish blame culture, i.e., punishing people who fall for tests only makes them hide real mistakes.

 Further reading and resources

- [NCSC Phishing Guidance](#) – Practical advice for individuals and teams.
- [CybSafe on Simulated Phishing](#) – How to get real value out of phishing tests.
- [Stay Safe Online Phishing Hub](#) – Tips on protecting your personal accounts.



Chapter 5 summary cheat-sheet

The knowing vs. doing gap: Seventy-three percent say they know how to create a strong password and do so, yet personal information (38%) and dictionary words (46%) still appear in a large share of passwords. Similarly, 20% know how to install software updates but don't, and 53% don't use MFA regularly, including 21% who understand how it works and simply choose not to use it. And while confidence in spotting a phishing email or scam text message (64% and 71%) is generally high, only 61% regularly check them for signs of phishing and only 47% verify with the sender if something is suspicious.

Convenience beats security: Convenience and habit often win out over stronger security options, as more people reuse or lightly modify a password (33%) than create a unique one for every account (25%).

Analog methods dominate: When it comes to remembering passwords, writing them down in a notebook (28%) and simply remembering them without writing them down (23%) are both more common than using a password manager, whether browser-based (8%) or a dedicated app (11%).

Trust over unfamiliarity: Low adoption of newer authentication methods isn't mainly a knowledge problem ...most participants understand at least the basics of passkeys (70%), yet only 39% actually use one. And biometrics non-users are more concerned about privacy (33%), the risk of data being hacked or misused (28%), and trust in companies handling their biometric data (24%) than about whether the technology works (21%), pointing to trust as a bigger barrier than unfamiliarity.

GENERATIONAL HIGHLIGHTS

The Millennial paradox: Millennials report the highest confidence identifying phishing emails (71%), scam texts (76%), and suspicious links (74%), yet they (46%) and Gen Z (47%) show the riskiest habits by using personal information in passwords, relying on dictionary words (Millennials 53%, Gen Z 49%), and intentionally opting out of or abandoning MFA despite knowing how to use it (Gen Z 27%, Millennials 25%).

The older generation divide: Baby Boomers (53%) and Gen X (51%) lead in regular MFA adoption, while the Silent Gen has the highest share of people who have never even heard of MFA (30%).

The Silent Gen phone anomaly: The Silent Generation reports the lowest confidence identifying phishing emails (45%), yet (somewhat unexpectedly) boasts the highest confidence of any generation when it comes to spotting scam phone calls (80%). 📞

6. Artificial intelligence (AI) – the bot next door

AI hasn't just knocked on the door of our daily lives and workplaces ... it's moved in, unpacked its bags, and taken over the spare room. This chapter looks beyond how people feel about AI and dives into what they're actually doing with it.

Here's how we're breaking it down:

6.1 The bot takeover: General usage habits, what people are prompting AI to do, and the surprisingly personal secrets they're feeding algorithms.

6.2 AI at work: How AI tools sneak into the office, the massive security training black hole, and the sensitive corporate data being quietly uploaded to public chatbots.

6.3 Bot or not?: Our confidence in spotting synthetic text, deepfake videos, altered images, and AI voice clones – and why our eyes feel far more reliable than our ears.

6.4 Brains, bots, and benefits: Public attitudes, AI anxieties, and whether we trust tech companies to handle the risks responsibly.

6.1 The bot takeover (because everyone and their grandma is prompting now)

Right. With no further ado, let's launch straight into general usage habits, what people are actually prompting AI to do, and the surprisingly personal details they're willing to share with algorithms in 2026.👁️👁️

Resistance is futile: 80% of us have gone full cyborg

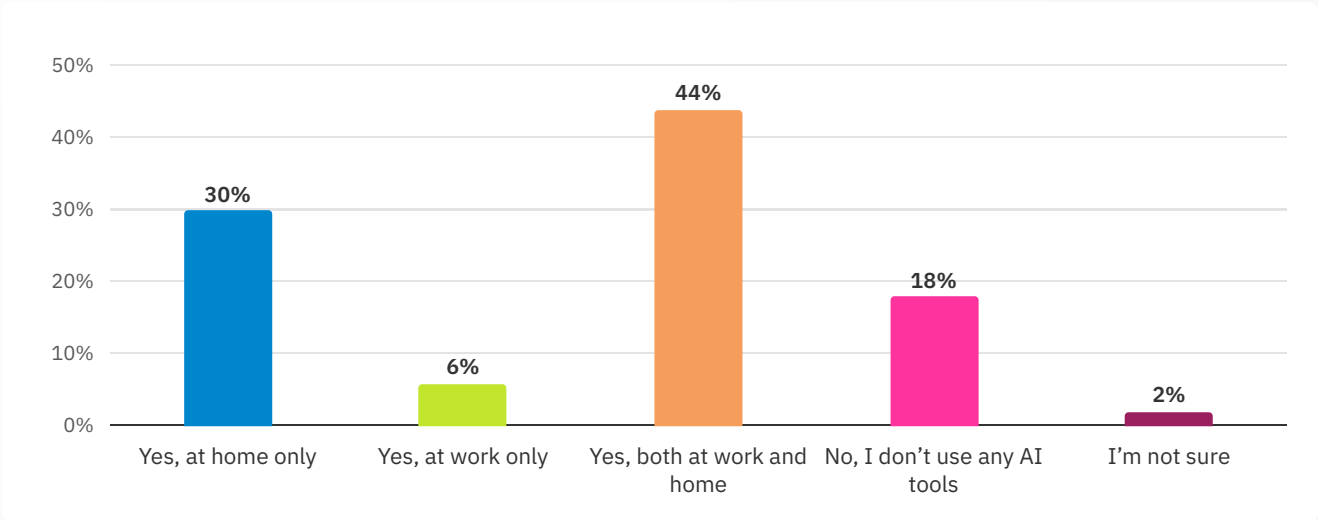
Here's a staggering stat to kick things off: a massive 80% of our total participant pool now uses AI tools (Figure 62). To put that into perspective:

- **Only 18%** report using no AI tools whatsoever.
- **2%** aren't sure if they used AI or not (maybe the bots are stealthy?).
- **80%** actively use AI tools.

And where are people using these tools?

- **At both home and work:** 44%.
- **At home only:** 30%.
- **At work only:** 6%.

Figure 62. ‘Do you use any AI tools at home or at work?’



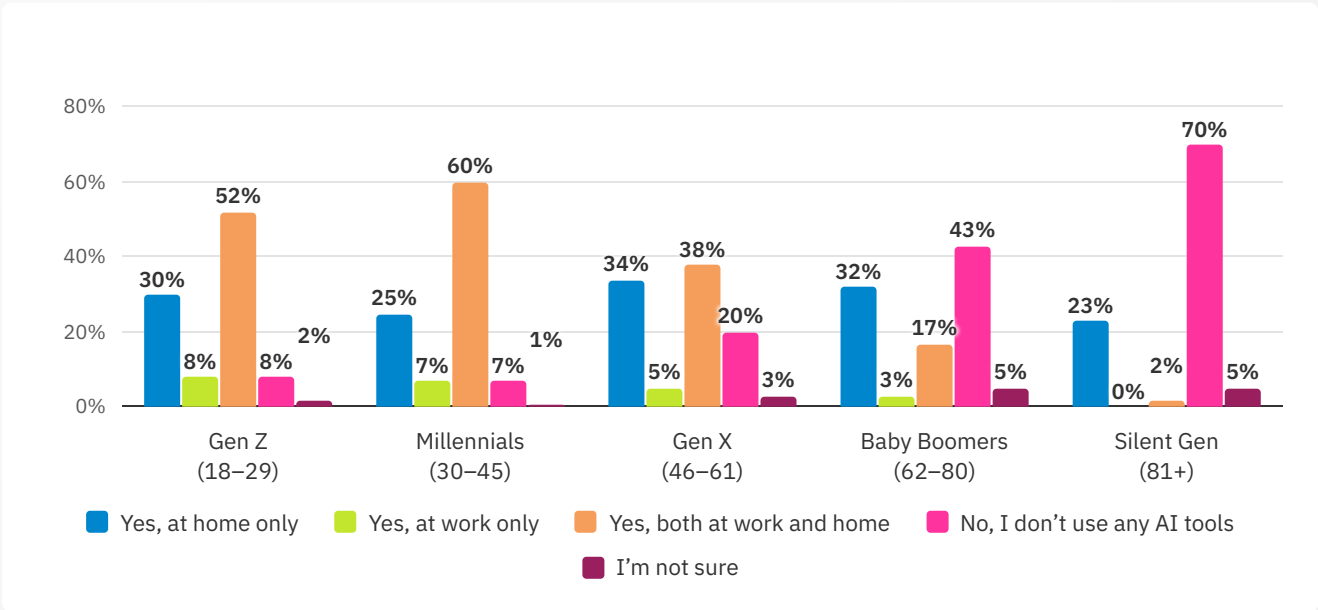
Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

Young people use AI more (call us Captain Obvious if you want, but we speak the truth)

AI usage stays highest among younger crowds and steadily drops off as participants get older (Figure 63), with 90% of Gen Z, 92% of Millennials, 77% of Gen X, 52% of Baby Boomers, and 25% of the Silent Generation report using AI tools.

Work-only adoption (ranging from 8% of Gen Z down to 0% of Silent Gen) and dual home-and-work adoption (60% of Millennials down to 2% of Silent Gen) mirror this exact decline. However, Gen X claims the crown for ‘home-only’ AI use, taking top spot at 34%.

Figure 63. ‘Do you use any AI tools at home or at work?’ by generation.



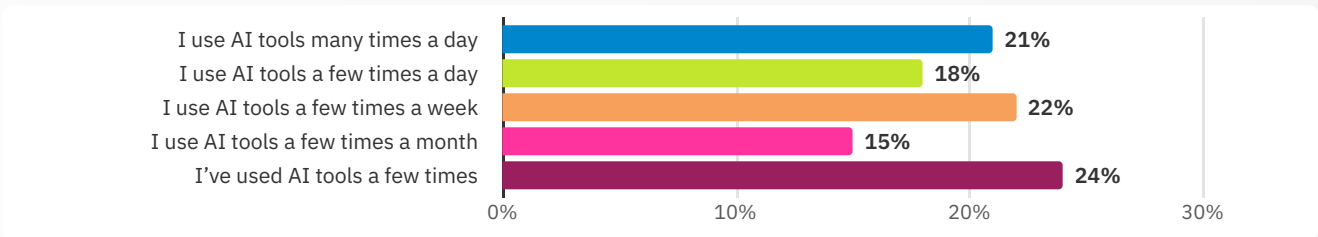
Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

How often are we talking to the algorithms?

This year, we decided to explore AI adoption in more depth, so we asked our AI-using group (n = 3,981) how often they check in with their favorite bots (Figure 64):

- 24% have only used AI tools a few times overall (just dipping a pinky toe in).
- 22% use AI tools a few times a week.
- 21% use AI tools many times a day (living the full sci-fi life).

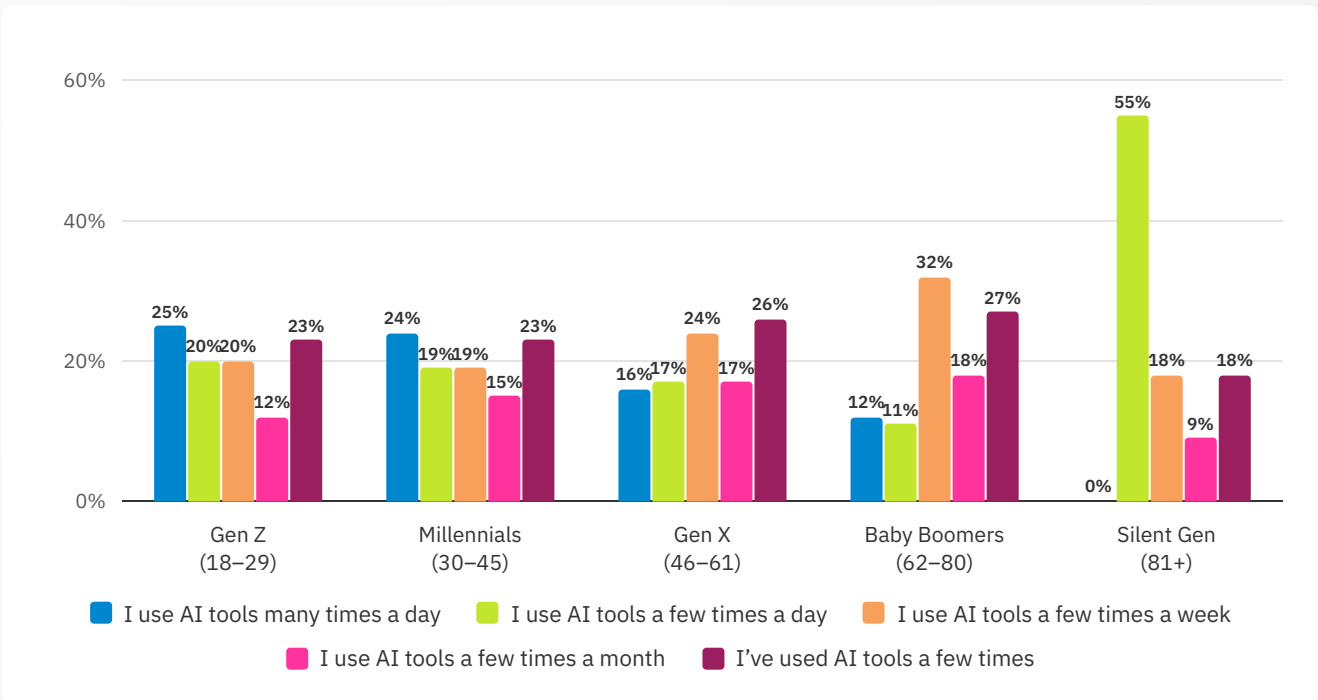
Figure 64. ‘How often do you use AI tools?’



Base: US, UK, India, Brazil, Singapore. Total number of participants: 3,981 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

Unsurprisingly, younger generations are heavy power users (Figure 65): 25% of Gen Z use AI multiple times a day, followed by 24% of Millennials, 17% of Gen X, 12% of Baby Boomers, and 0% of Silent Gen.

Figure 65. ‘How often do you use AI tools?’ by generation.



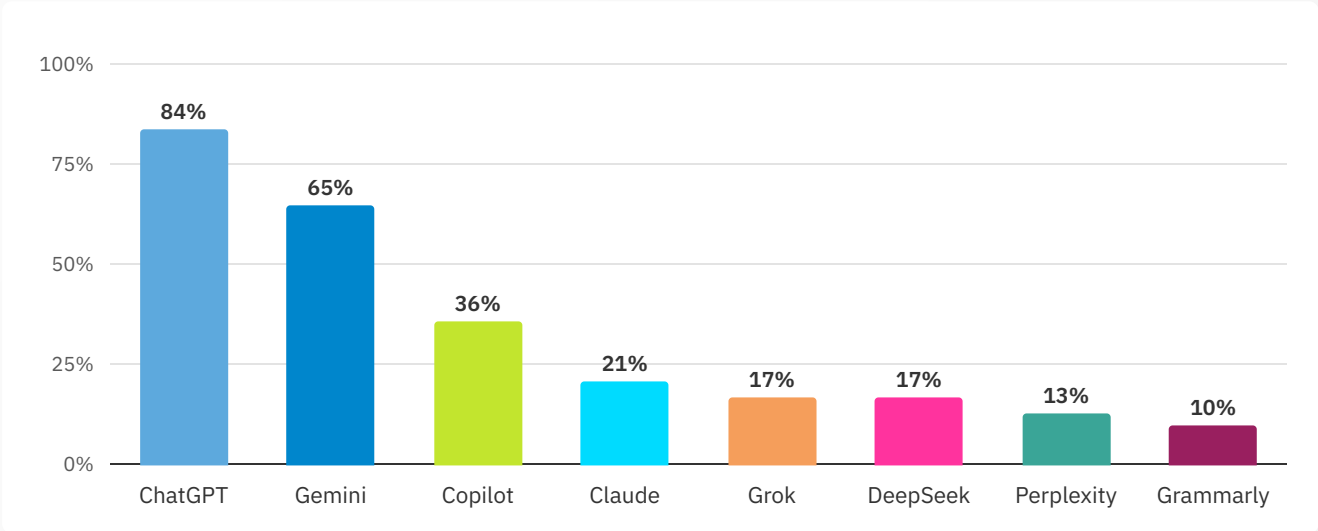
Base: US, UK, India, Brazil, Singapore. Total number of participants: 3,981 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

Among AI users (n = 3,981), ChatGPT continues its streak as the reigning champion, but competitors are closing in fast (Figure 66).

- ChatGPT is the most popular, with 84% (+7% from 2025)
- Gemini (65%, +16% from 2025)
- Copilot (36%, +10% from 2025)
- Claude (21%)
- Grok and DeepSeek (both 17%).

Other popular AI tools include Perplexity, Grammarly, and based on the qualitative responses, we also noted mentions of Meta AI, Alexa, and Kimi.

Figure 66. ‘What AI tools do you use?’



Base: US, UK, India, Brazil, Singapore. Total number of participants: 3,981 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

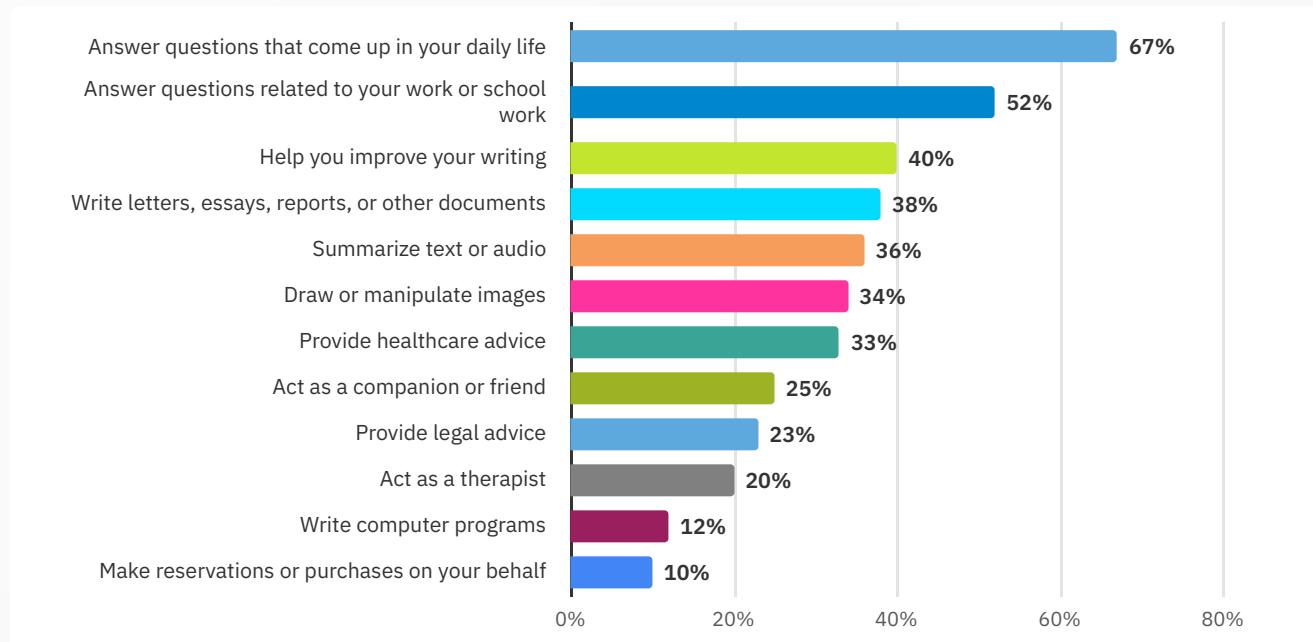
Taskmaster AI: What are we outsourcing to the bots?

For the first time this year, we asked AI users what chores, brain-teasers, and creative things they hand over to their digital assistants:

- Settling daily life debates & queries: 67%
- Homework & office problem solving: 52%
- Polishing rough draft writing: 40%
- Ghostwriting essays, reports, and letters: 38%
- TL;DR-ing long texts or audio recordings: 36%
- Doodling & wizarding up images: 34%
- Playing Dr. AI for health advice: 33%

While everyday advice, work, and writing dominate, people are also turning to AI for emotional support: 25% use AI as a digital buddy, and 20% use it as a budget therapist (Figure 67).

Figure 67. ‘What types of things have you used AI tools to do?’



Base: US, UK, India, Brazil, Singapore. Total number of participants: 3,981 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

Spill the tea ☕ : Secrets we feed the AI (but probably shouldn't)

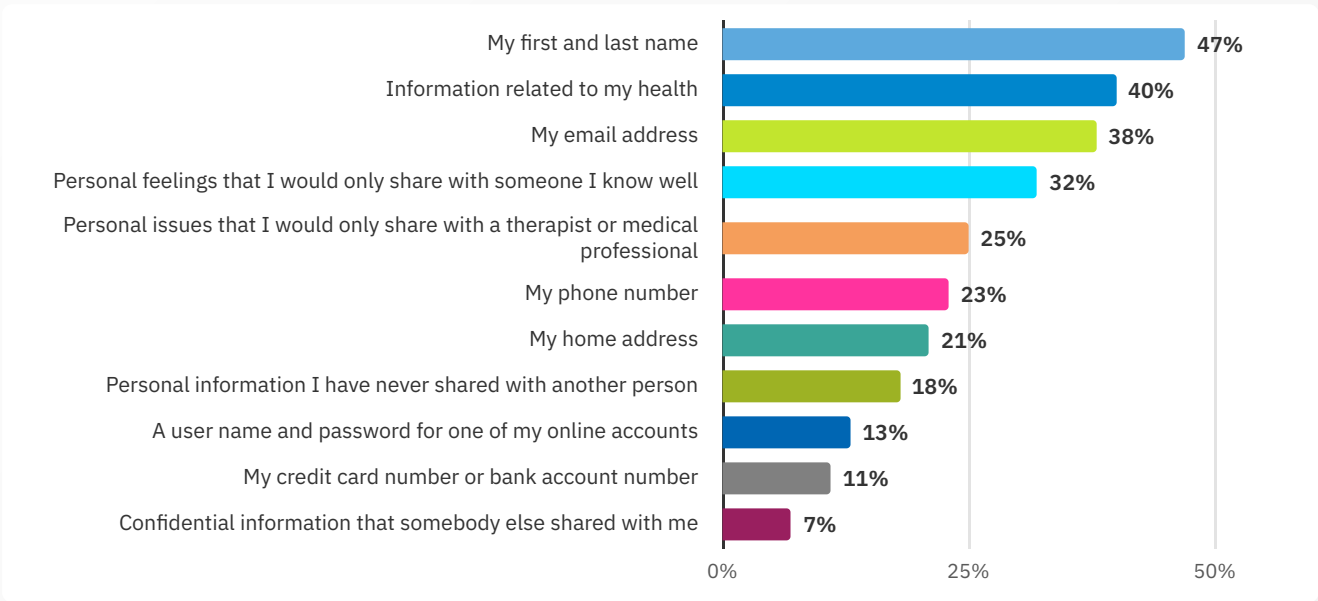
When we asked AI users ($n = 3,981$) what juicy details they type into prompt boxes, the results were honestly fairly eye-popping (Figure 68):

- First and last name: 47%
- Medical histories & health symptoms: 40%
- Personal email addresses: 38%
- Deep feelings meant for close friends: 32%
- Therapy-level emotional confessions: 25%
- Phone numbers: 23%
- Home addresses: 21%
- Login credentials & passwords: 13%
- Credit card or banking info: 11% (💰)
- Gossip or confidential info about someone else: 7%

AI: The ultimate secret-keeper?

18% of AI users admitted they have confessed things to an AI tool that they have never told another living human being. Overall, people are way more willing to spill their deepest feelings and medical ailments to an algorithm than they are to hand over their online banking logins.

Figure 68. ‘What types of information have you shared with an AI tool?’



Base: US, UK, India, Brazil, Singapore. Total number of participants: 3,981 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

KEY TAKEAWAYS: SUBCHAPTER 6.1

01

Mainstream status unlocked: The majority of participants use AI tools, and for most, it’s woven into both home and work life. Younger groups lead the pack in frequency and adoption.

02

The bot gets all the gossip: Health records and personal secrets are regularly typed into prompts, with nearly 1 in 5 sharing things with AI they’ve never told a soul.

6.2 AI at work: Ninja productivity tool or corporate risk?

New subchapter alert. 🚨

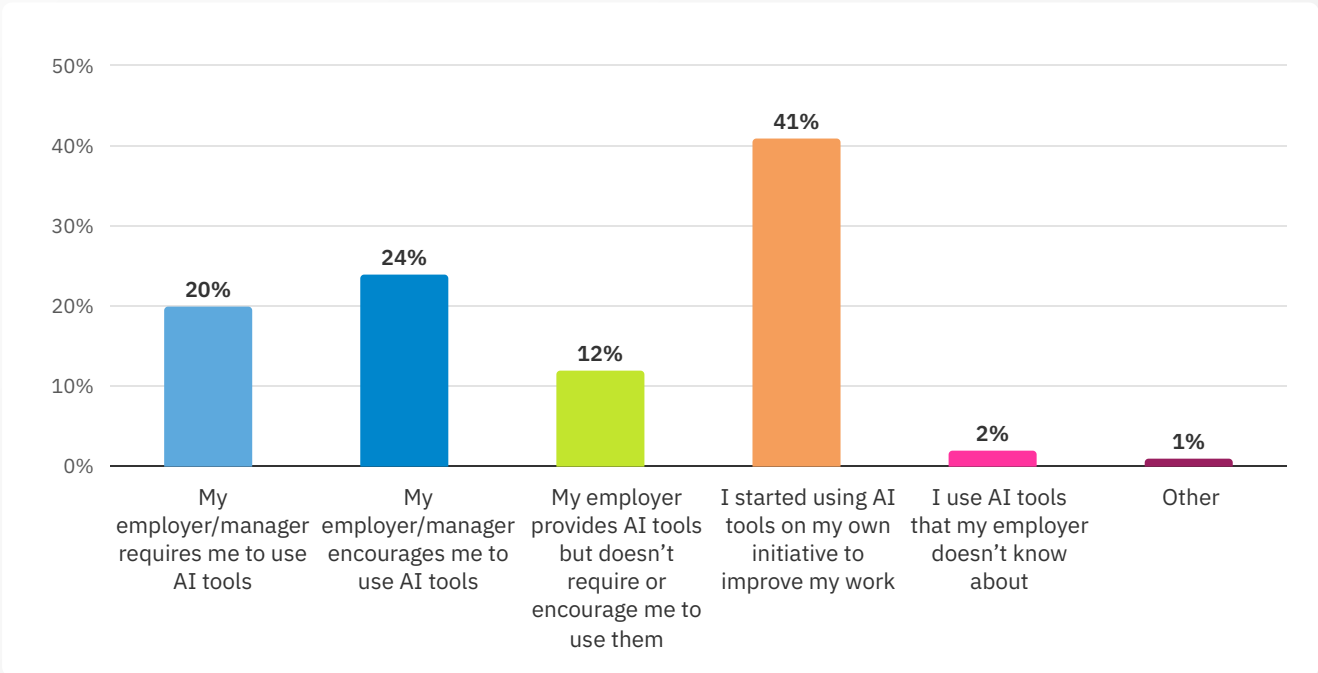
This year, we gave workplace AI its very own spotlight to see how tools sneak into the office, whether anyone actually gets any training or a safety manual, whether their employer has told them what they can and can't share with these tools, and whether they've shared anything with AI tools without their employer's knowledge, and if so, what. (Argh.)

Rogue workers or company mandate? How AI entered the office

We asked workplace AI users (*n* = 2,481) how their AI journey at work began (Figure 69):

- **'I wanted a shortcut!' (self-initiated):** 41% brought AI into their workflow on their own to make life easier.
- **'Boss said it was cool' (employer encouraged):** 24%
- **'Boss made me do it' (employer required):** 20%
- **'It was just sitting there' (tool provided, optional):** 12%
- **'Don't tell the boss' (under the radar):** 2%
- **'It's complicated' (other routes):** 1%.

Figure 69. 'How did you start using AI tools for work?'



Base: US, UK, India, Brazil, Singapore. Total number of participants: 2,481 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

Flying blind: The massive AI training black hole

Circling back to all AI users (n = 3,981) for a minute, we asked them whether they'd received any training on the security and privacy risks associated with AI, and 56% said they haven't (-2% from 2025).

Breaking this down by employment status (Figure 70), training gaps are widest for those outside the traditional workforce: 71% of those not in active employment and 63% of students say they haven't received any training, both higher than retirees (62%).

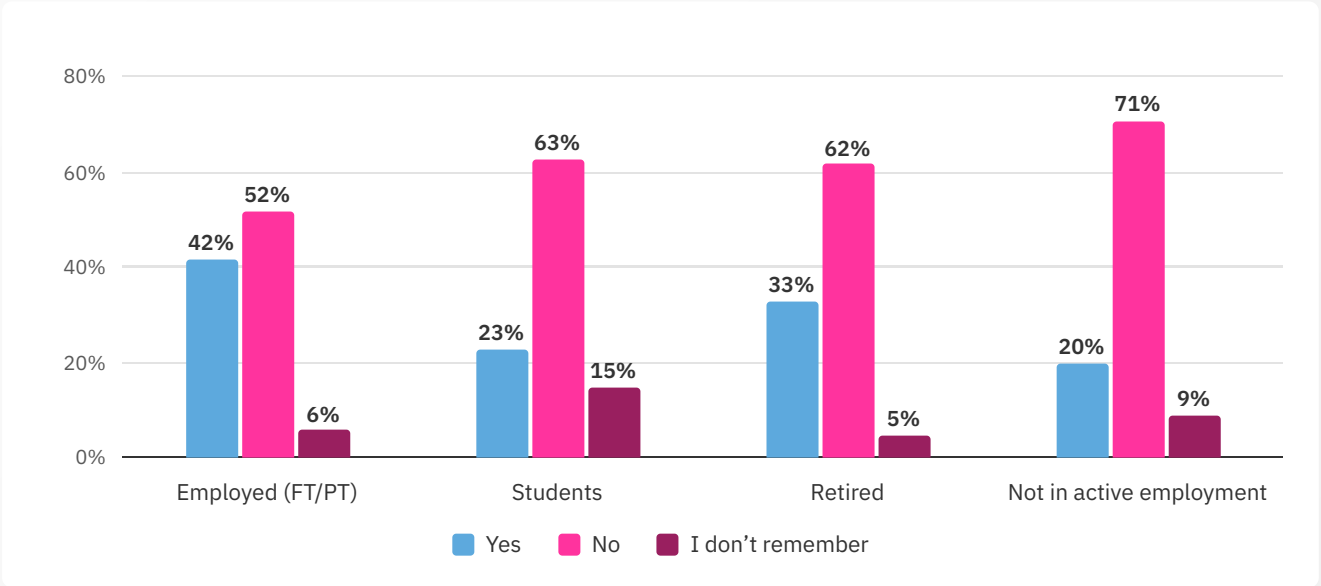
Even among employed participants, who are the most likely of any group to have received training, over half (52%) still haven't (scarily).

 BRAIN SNACKS

This mirrors wider findings³⁶ that a majority of employees believe they are not being trained properly, contributing to a massive ‘AI adoption gap’ where tools are often misused, underutilized, or generally misunderstood.

More recent reports, such as a global survey of 6,000 enterprise employees by Lenovo³⁷ found that 31% of AI users say their employer doesn't provide any training on how to use AI, and that even among those who do receive training, many describe it as irregular or ineffective.

Figure 70. ‘Have you received any training about the security and privacy risks of AI tools?’ by employment.



Base: US, UK, India, Brazil, Singapore. Total number of participants: 3,981 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

36 Help Net Security. (2025, June 18). *Employees are using AI where they know they shouldn't*. <https://www.helpnetsecurity.com/2025/06/18/employees-ai-potential/>

37 Lenovo. (2026). *Work Reborn Research Series 2026: Leading your workforce to AI triumph*. https://s7d1.scene7.com/is/content/Lenovoassetsprod/Lenovo_DWS_Work_Reborn_Report_5_ww_enpdf

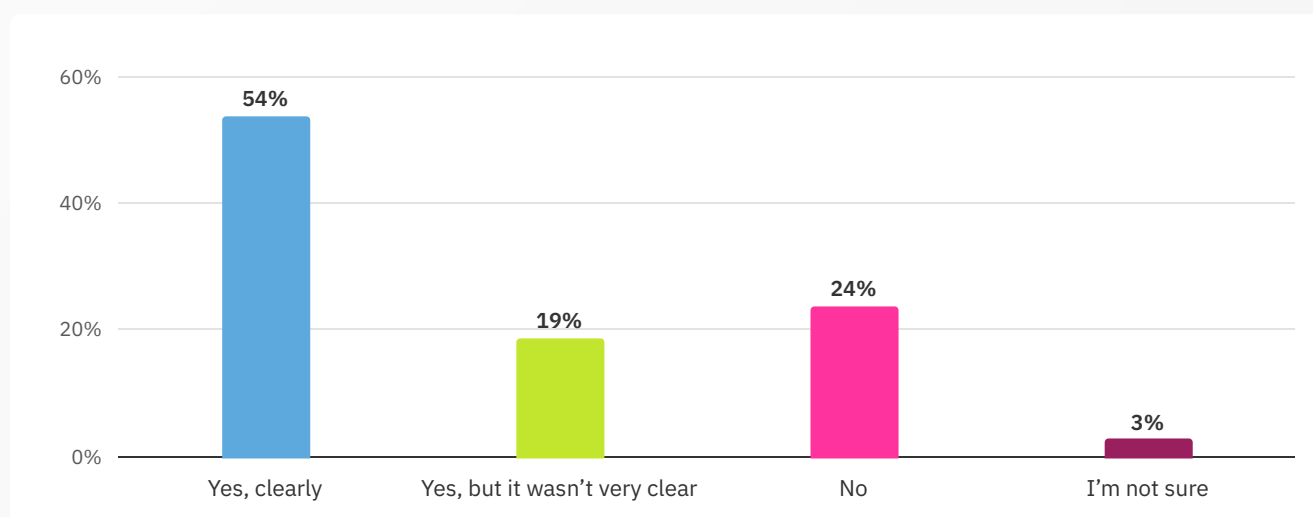
Clear boundaries or wild west guidelines?

Have employers clearly communicated what can and cannot be shared with AI (Figure 71)?

- **‘Yes, they gave us clear rules’:** 54%
- **‘Cricket ...no policy at all’:** 24%
- **‘Clear as mud’ (vague guidelines):** 19%

And while over half said that their employers clearly communicated what they can and can’t share with AI tools, there’s a notable 24% whose employers didn’t do so, and a further 19% whose employers weren’t actually very clear about it. Combined, that’s 43% of employees left guessing what is (and isn’t) safe to type into a prompt.

Figure 71. ‘Has your employer communicated what you can/can’t share?’



Base: US, UK, India, Brazil, Singapore. Total number of participants: 2,481 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

The secret corporate leaks

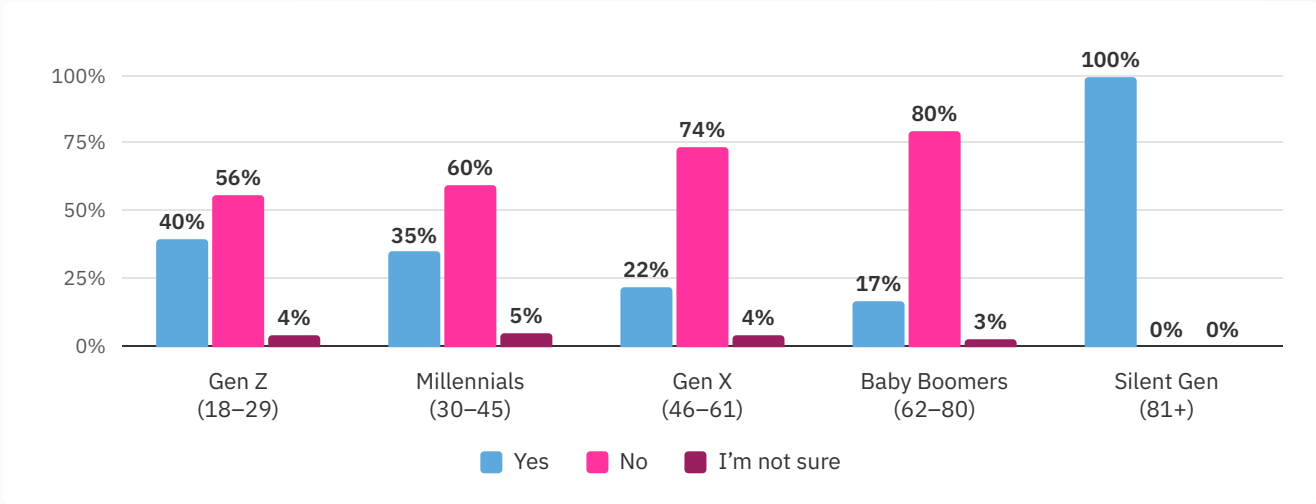
Without clear rules and proper training, 32% of those who use AI at work admit to sharing sensitive company data with AI tools without their employer's knowledge (and an extra 4% weren't sure). They're quietly pasting corporate secrets into public chatbots. You couldn't make it up (but, as we all know, AI frequently does).

Let's look at the generational difference for a better understanding of the context here. Just as in previous years, sensitive data sharing with AI tools was more common among younger generations (Figure 72).

- **Gen Z:** 40% admit to sharing unauthorized sensitive work data.
- **Millennials:** 35%
- **Gen X:** 22%
- **Baby Boomers:** 17%

SEBDB BEHAVIOR SB156: Shares sensitive information only on an approved or official website or application

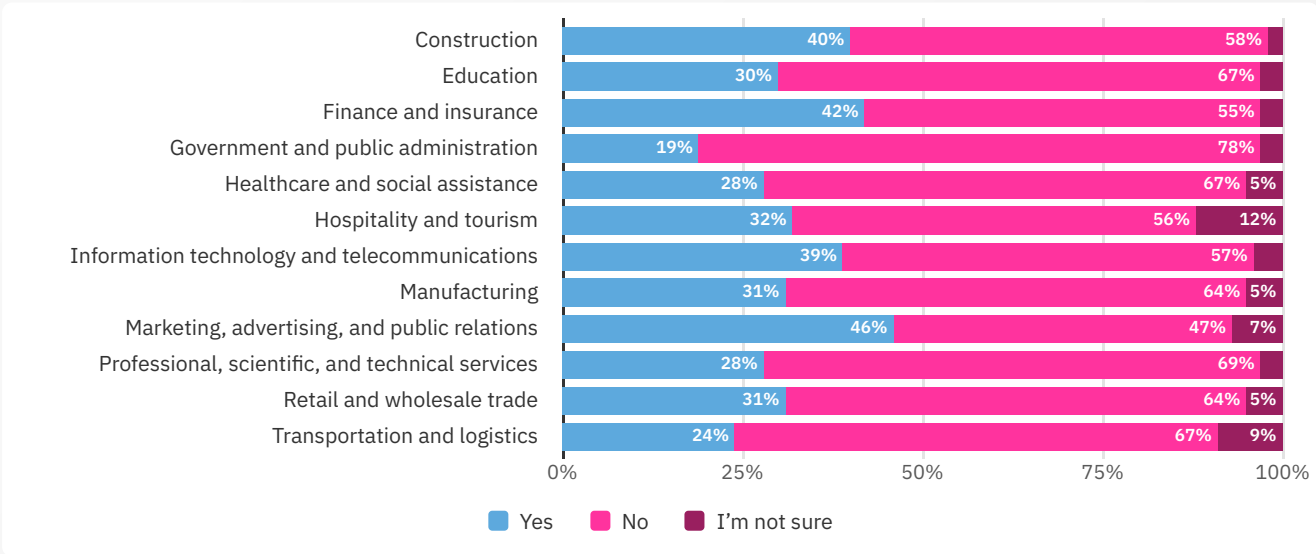
Figure 72. ‘Have you ever shared sensitive work information with AI tools without your employer’s knowledge?’ by generation.



Base: US, UK, India, Brazil, Singapore. Total number of participants: 2,481 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

What about different sectors³⁸ (Figure 73)? Participants working in marketing, advertising, and public relations report the highest percentage of those admitting to sharing sensitive work information with AI tools without an employer's knowledge (46%), followed by finance and insurance (42%), construction (40%), and information technology and telecommunications (39%). Close to a third of participants working in hospitality & tourism (32%), manufacturing (31%), and retail & wholesale trade (31%) admit to doing so.

Figure 73. ‘Have you ever shared sensitive work information with AI tools without your employer’s knowledge?’ by sector.



Base: US, UK, India, Brazil, Singapore. Total number of participants: 2,481 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

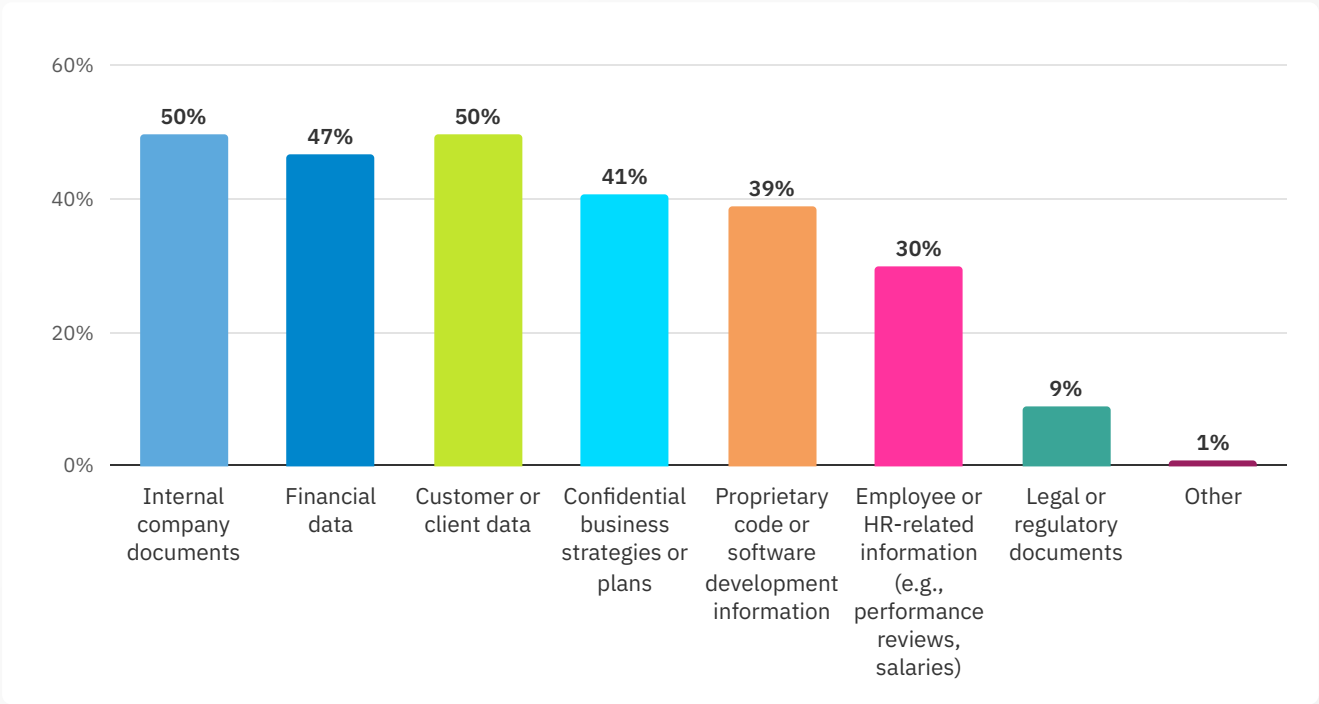
38 Sectors with fewer than 50 respondents are excluded from this breakdown due to unreliable base sizes.

What company secrets are we uploading?

Among the participants who shared work data without permission (n = 791), here’s what got pasted into the prompt box (Figure 74):

- **Internal company documents:** 50%
- **Client or customer details:** 50%
- **Financial blueprints & numbers:** 47%
- **Top-secret business strategies:** 41%
- **Proprietary code & dev secrets:** 39%
- **Employee HR files & records:** 30%

Figure 74. ‘What kind of sensitive work information did you share with AI tools?’



Base: US, UK, India, Brazil, Singapore. Total number of participants: 791 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

 BRAIN SNACKS

These findings match wider corporate trends. A global report by Okta³⁹ found that 52% of employees admit to using unapproved AI tools, even while 95% of executives remain blissfully confident that their staff use AI responsibly. (Awkward). Employees said they most commonly share internal comms, HR-related information, and confidential company documents.

 KEY TAKEAWAYS: SUBCHAPTER 6.2

01

AI adoption at work is (slightly) more employer-driven: More people started using AI at work because their employer required or encouraged it, than those who started on their own initiative, but only by a narrow margin.

02

Zero security briefings: More than half of employed AI users have received zero training on AI safety or data privacy risks.

03

Unauthorized data sharing with AI tools: A third of those who use AI at work have shared confidential data (like company files, code, or customer records) with AI tools without their employer's knowledge. Notably, this was most common among younger generations.

³⁹ Okta. (2026). *AI agents at work 2026: Securing the agentic enterprise*. <https://www.okta.com/newsroom/articles/ai-agents-at-work-2026-agentic-enterprise-security/>

💡 TOP TIPS: THE 2026-2027 AI RISK MANAGEMENT SURVIVAL GUIDE

Managing AI adoption isn't about locking down innovation (we'd be the *last* people to suggest that), so much as giving your team clear guardrails so they can move at speed without breaking any compliance guidelines. Here's how to turn high-level AI risk strategy into practical, everyday habits for your workforce:

1. Ditch the jargon: Create a traffic light AI rulebook

Don't bury rules in legal textbook pages. Build a simple visual policy:

-  Green light: Approved tools & public data (e.g., summarizing public articles).
-  Yellow light: Internal notes with personal identifying info removed.
-  Red light: Client PII, unreleased source code, financial records, and confidential strategies.

2. Turn security training into practical AI worklabs

Textbook lectures don't work - well, unless you're at college. Deliver interactive sessions showing staff *how* AI models retain training data, how prompts leak information, and how deepfake verification works so they understand the 'why' behind the rules.

3. Give them safe tools so they don't have to cheat

Employees use unvetted AI tools because they want to work faster and smarter. Provide secure, enterprise-grade AI environments with built-in privacy walls – when the official tool works great, workers won't need to sneak company secrets into shady public bots.

6.3 Bot or not? Our (unwarranted?) confidence in spotting AI creations

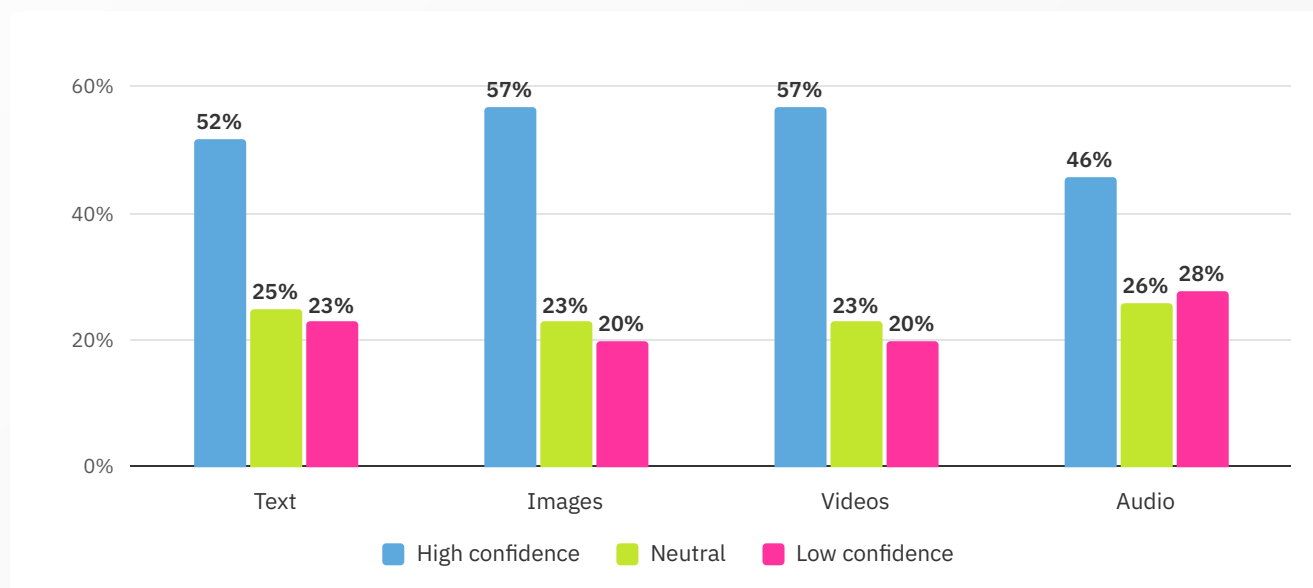
We've talked about how people use AI and how it's sneaking into the workplace, but what about the stuff these digital brains are actually creating? We wanted to know: when a bot churns out text, images, video, or audio, how confident do people feel about calling it out as AI?

Eyes vs. ears: We trust our eyeballs, not our earphones

It turns out our eyes feel a lot more reliable than our ears. People reported the highest confidence when evaluating visual content created by AI, while synthetic voices left most folks scratching their heads:

People expressed the highest confidence recognizing images and videos created by AI, both at 57% (Figure 75). Text was a bit lower, at 52%, and AI audio seemed to be the trickiest to recognize, with only 46% feeling confident in their ability to do so.

Figure 75. ‘How confident are you in your ability to recognize AI-generated content?’



Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

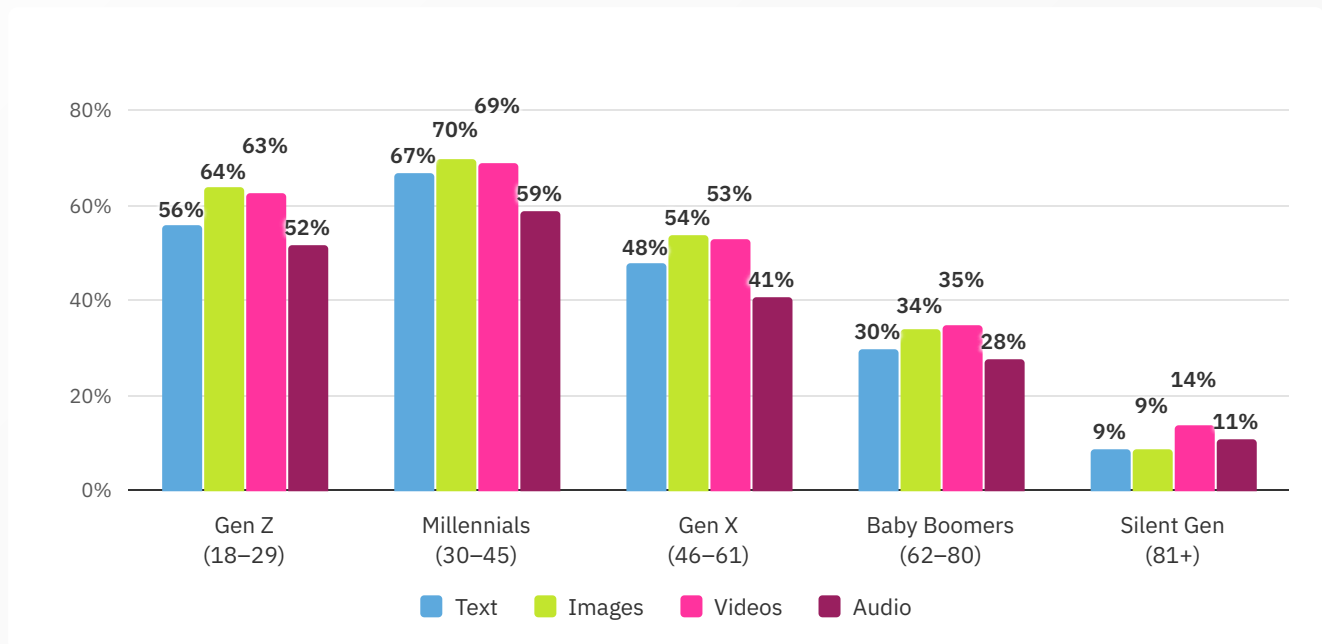
The generational radar: Who has the ultimate fake-buster radar?

Confidence in spotting fake content follows a crystal-clear generational slope, and it drops off steadily as age goes up across all four content formats (Figure 76):

- **Millennials (the self-proclaimed detectives):** Take top honors across the board! They feel most relaxed spotting AI images (70%) and AI videos (69%).
- **Gen Z:** Follow right behind Millennials, showing solid confidence in identifying images (64%) and videos (63%).
- **Gen X:** Confidence starts to slip down to 54% for images and 53% for videos.
- **Baby Boomers:** Experience a steep drop, with only 34% confident in spotting AI images and 35% for AI videos.
- **Silent Generation:** Sitting at the bottom by a wide margin, reporting just 9% confidence for images and 14% for videos.

The ranking between content types holds surprisingly steady across every single age bracket: images and videos are seen as the easiest to spot, text sits in the middle, and audio is consistently the hardest. When it comes to audio detection confidence, Millennials top the charts at 59%, while the Silent Generation bottoms out at a tiny 11%.

Figure 76. ‘How confident are you in your ability to recognize AI-generated content?’ by generation.



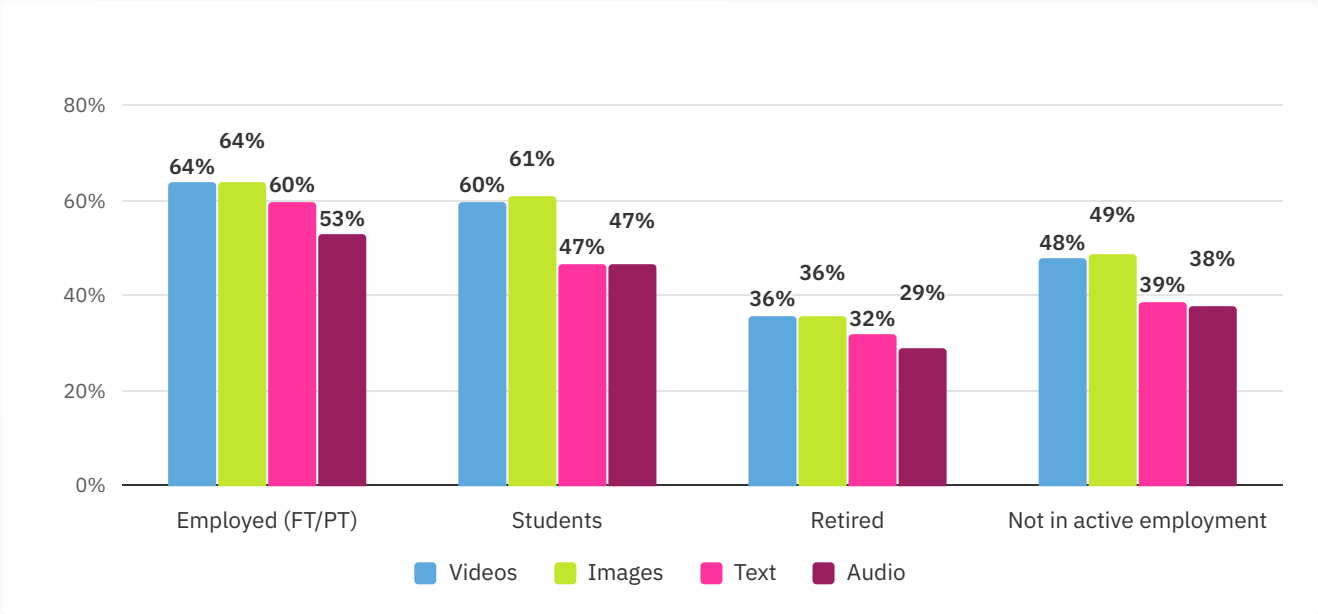
Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

Desk job vs. detectives: Does your daily grind sharpen your AI radar?

When we slice the data by employment status (Figure 77), a person's daily routine seems to play a big role in how confident they feel:

- Employed participants and students flex similar confidence levels for videos (64% vs. 60%) and images (64% vs. 61%).
- However, employed workers feel noticeably sharper than students at picking out AI text (60% vs. 47%) and AI audio (53% vs. 47%).
- Retirees logged the absolute lowest confidence across all four content types, ranging from 36% for images and videos down to just 29% for audio.
- Those not in active employment land right in the middle ground, ranging from 49% for images down to 38% for audio.

Figure 77. ‘How confident are you in your ability to recognize AI-generated content?’ by employment.



Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

 KEY TAKEAWAYS: SUBCHAPTER 6.3

01

Visuals win over voices: People feel way more confident spotting AI in images and videos, less so in text, and even less in audio files.

02

Age is more than a number: Millennials and Gen Z lead the pack in AI-detection confidence, while the Silent Generation reports the lowest confidence by a landslide.

6.4 Brains, bots and benefits: Public attitudes and AI anxieties

In this final subchapter, we’re taking the public temperature on artificial intelligence: do we love it, fear it, or have faith in its responsible implementation (and trust tech companies not to accidentally build Skynet)?

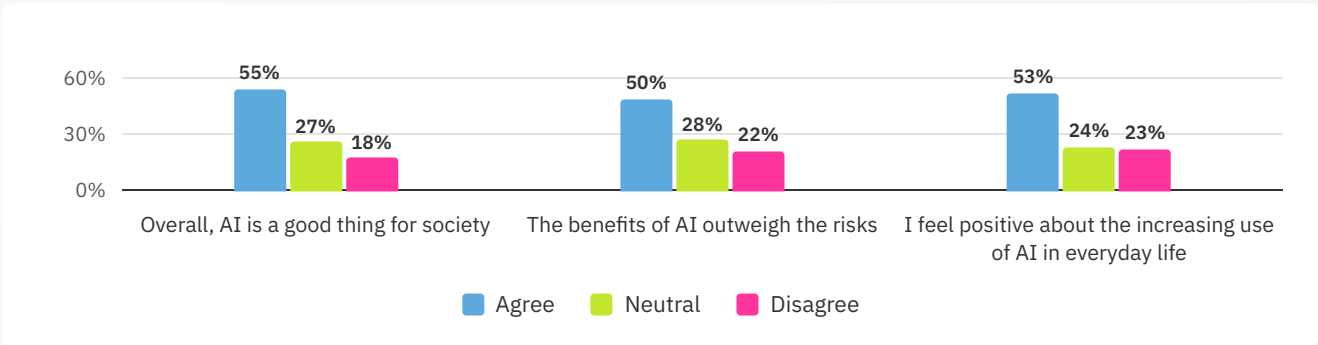
The general vibe check: Cautiously optimistic (with a dash of dread)

Overall, public sentiment toward AI leans positive, but nobody is throwing a ticker-tape parade just yet. It’s a classic case of ‘cautious optimism’ (Figure 78).

- 55% believe AI is a good thing for society overall.
- 53% feel positive about AI becoming a bigger part of everyday life.
- 50% feel the benefits of AI outweigh its risks.

Translation? A slim majority sees the value, but a huge chunk remains on the fence or deeply skeptical.

Figure 78. Attitudes toward AI.



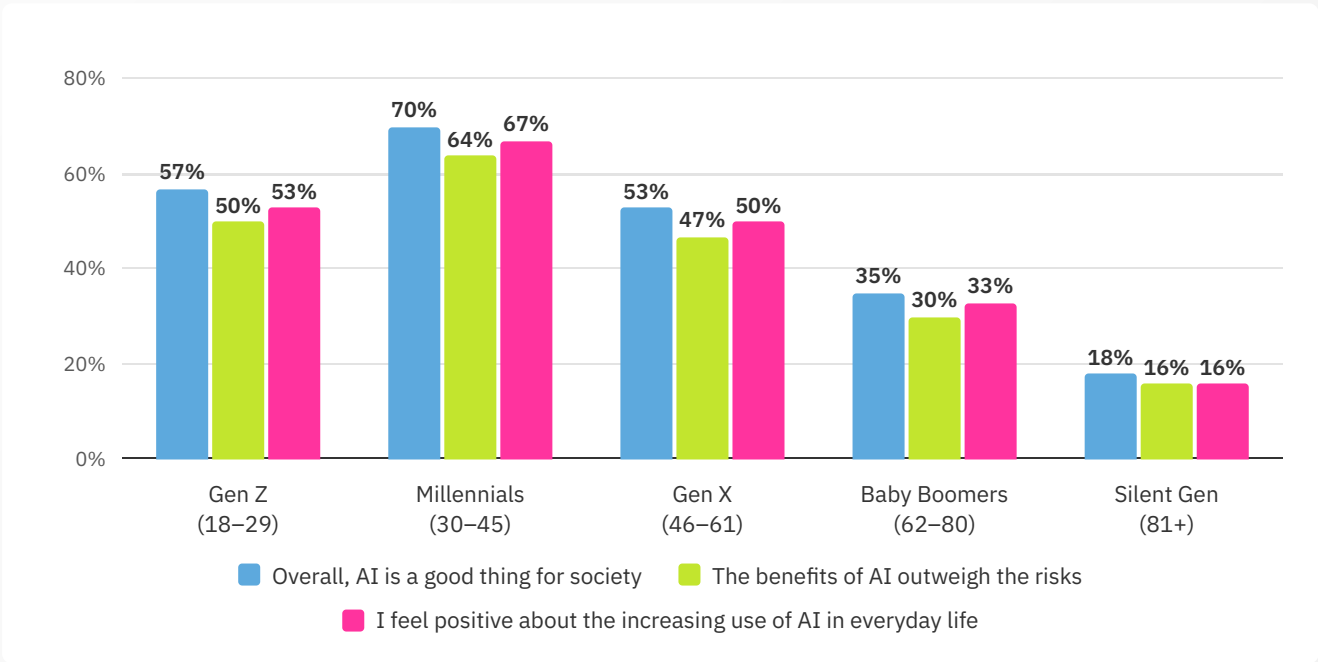
Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

Generational hype train: Who’s fanboying over the bots?

Generational attitudes toward AI mirror the confidence trend – the younger you are, the more eager you are to embrace our new digital overlords (Figure 79):

- **Millennials (the ultimate fan club):** 70% say AI is good for society, 67% welcome its daily use, and 64% think benefits outweigh the risks.
- **Gen Z:** Next in line, with 57% calling it good for society, 53% happy about everyday integration, and 50% agreeing benefits beat risks.
- **Gen X:** Sits right in the middle at 53% (good for society), 50% (everyday use), and 47% (benefits beat risks).
- **Baby Boomers & Silent Gen:** Far less enthusiastic. Only 30% of Boomers and a meager 16% of the Silent Gen believe AI’s benefits outweigh its drawbacks.

Figure 79. Attitudes toward AI, by generation.



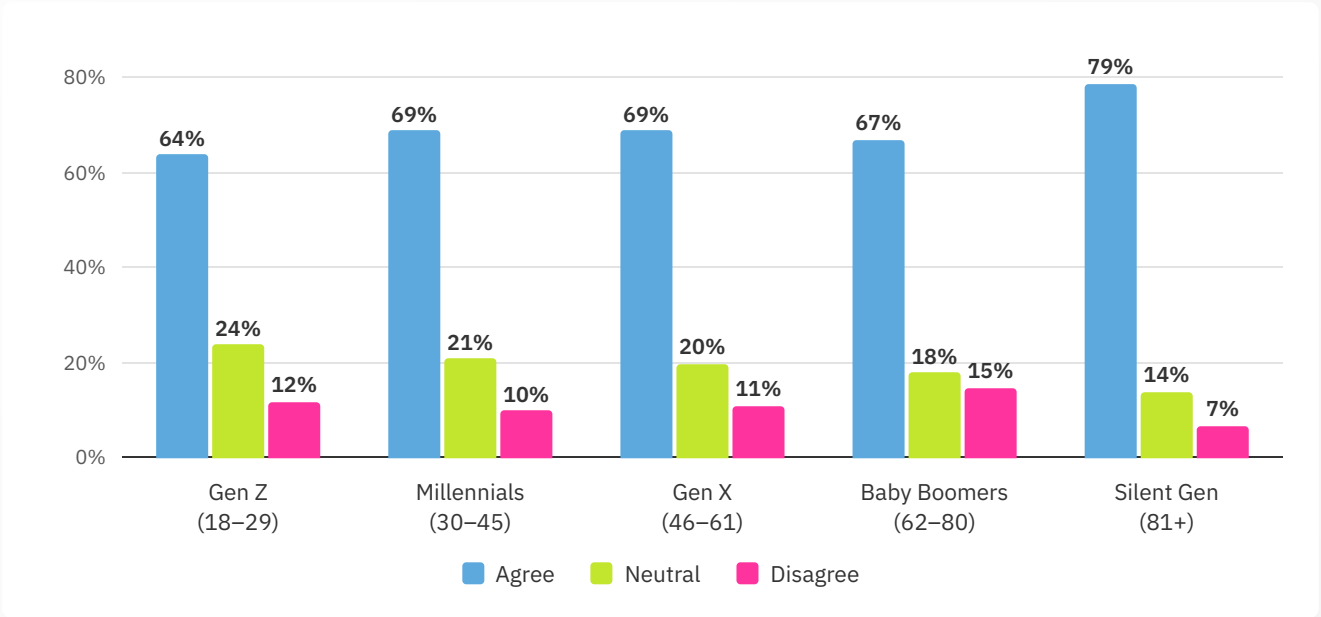
Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

The dark side of prompts: Cybercrime spookiness

While people like the convenience of AI, they are terrified of how bad actors might abuse it. A whopping 67% of the total participant pool reported being genuinely concerned about AI-related cybercrime.

Concern peaks among our oldest cohort (the Silent Generation) at 79%, while remaining high (though notably lower) across every other age group, ranging from 64% of Gen Z to 69% of both Millennials and Gen X (Figure 80).

Figure 80. ‘I’m concerned about AI-related cybercrime.’ by generation.

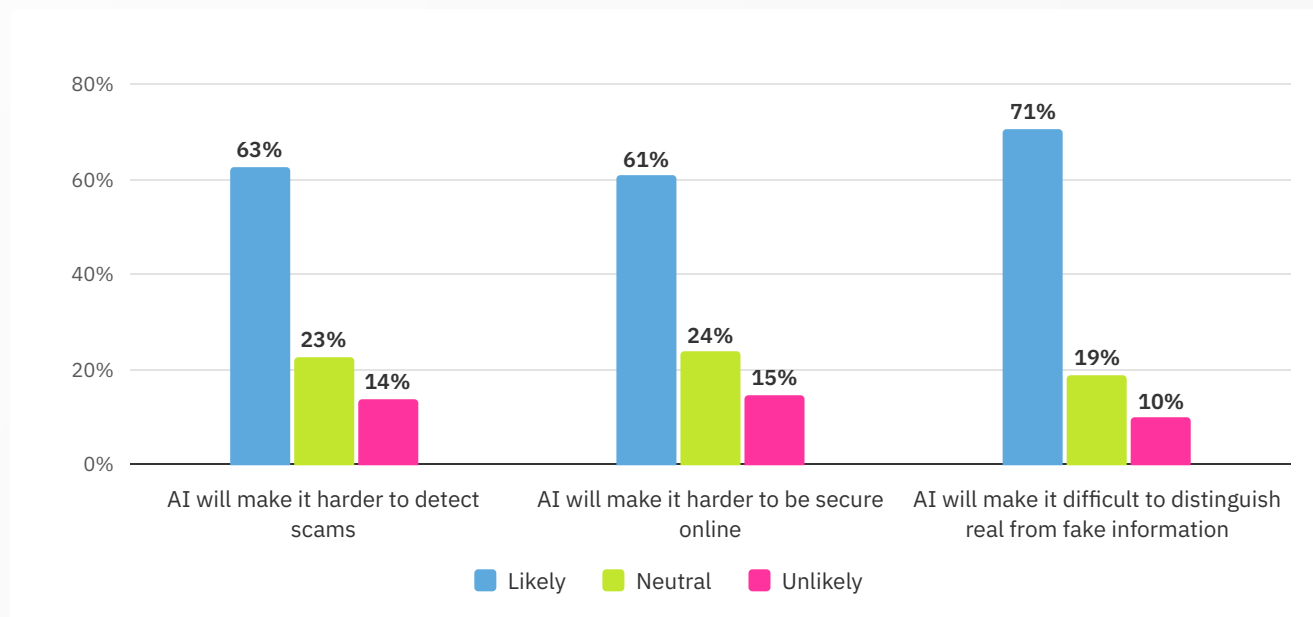


Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

People aren't just worried about abstract sci-fi threats, they’re specific about what makes AI security so scary.

Participants expressed a high level of concern about the negative security implications of AI (Figure 81). Slightly over sixty percent believe AI will make it harder to detect scams (63%, +9% from 2025) and to be secure online (61%, +7% from 2025). The most pronounced concern is spotting manipulated content: 71% (+4% from 2025) think AI will make it difficult to distinguish real from fake.

Figure 81. Perceptions of AI's impact on scams and online security.



Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

People's concerns about AI tools in relation to their online security are evident, but how do they feel about cybercriminals using these tools specifically?

Unsurprisingly, the majority of participants felt that AI will make it easier for cybercriminals to impersonate others (71%, +6% from 2025) and that it will be used by cybercriminals to get around security systems (70%, +3% from 2025, Figure 82).

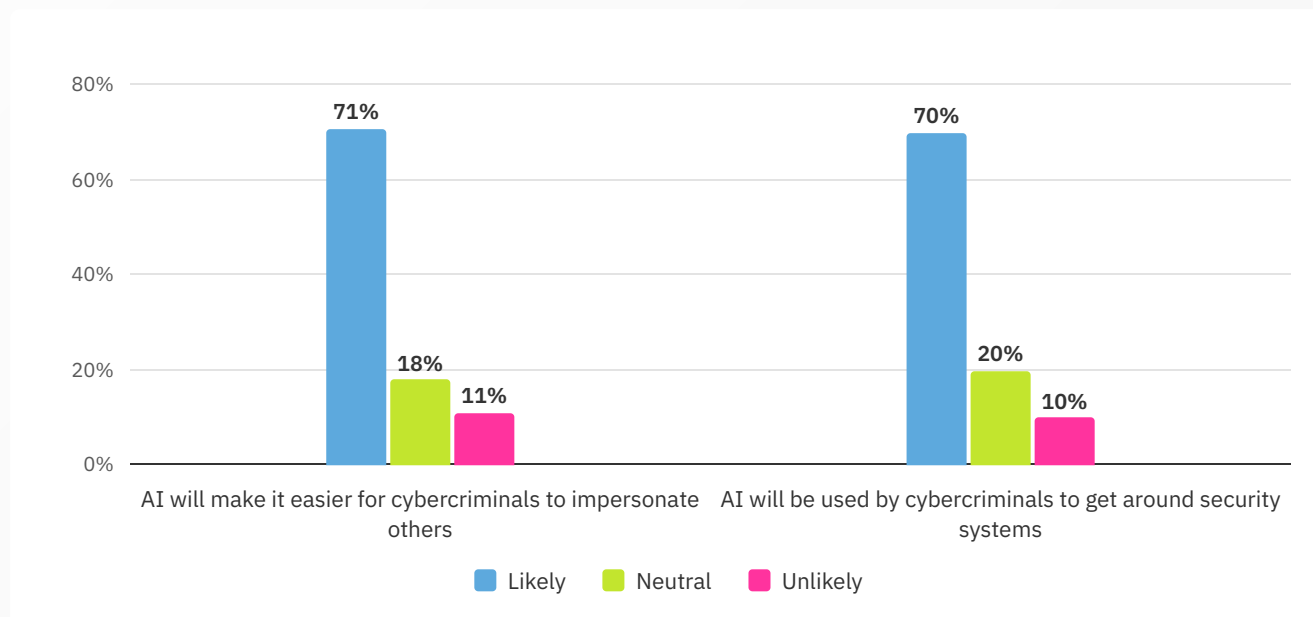
BRAIN SNACKS

Real-world nightmare: Alas, this isn't mere paranoia. Back in 2024, UK engineering giant Arup was scammed out of \$25 million when an employee was fooled by deepfake video calls impersonating the CFO and other colleagues.⁴⁰ Deepfake fraud has exploded into an industrial-scale operation, making sophisticated scamming tools cheap and accessible to almost anyone with a web browser.⁴¹

40 Magramo, K. (2024, May 17). *British engineering giant Arup revealed as \$25 million deepfake scam victim*. CNN Business. <https://www.cnn.com/2024/05/16/tech/arup-deepfake-scam-loss-hong-kong-intl-hnk>

41 Down, A. (2026, February 6). *Deepfake fraud taking place on an "industrial scale," study finds*. The Guardian. <https://www.theguardian.com/technology/2026/feb/06/deepfake-taking-place-on-an-industrial-scale-study-finds>

Figure 82. Perceptions of AI as a tool for cybercriminals.



Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

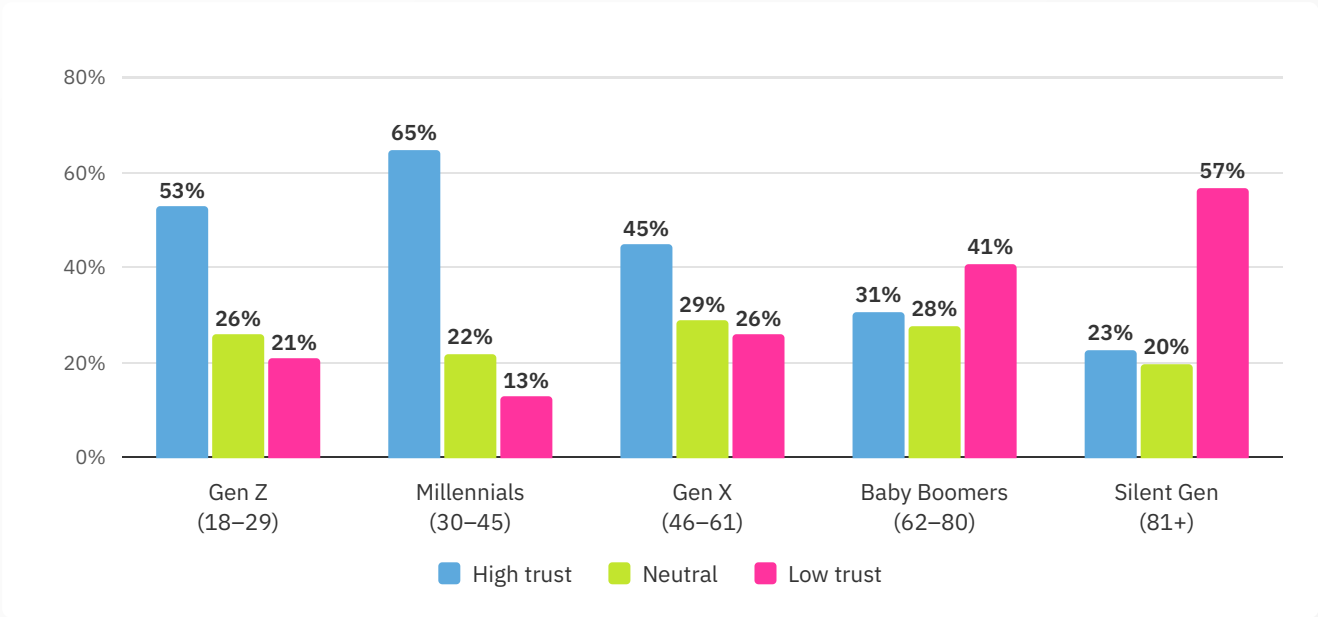
Corporate side-eye: Do we trust big tech with the AI steering wheel?

With shiny new AI startups popping up every week, do people actually trust these tech creators to act responsibly?

- **High trust:** 50% trust companies to implement AI responsibly (+5% from 2025).
- **Neutral:** 26% remain on the fence (-1% from 2025).
- **Low trust:** 24% have low trust in corporate AI ethics (-4% from 2025).

Older generations are deeply suspicious (Figure 83): 57% of the Silent Gen (up 9% from 2025) and 41% of Baby Boomers (down 3% from 2025) report low trust. Conversely, Millennials lead high trust at 65% (up 9%), followed by Gen Z at 53% (up 3%).

Figure 83. Participants’ level of trust in companies to implement AI responsibly, by generation.



Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

Peering into the crystal ball: Wild (and weird) future predictions

We asked participants what AI-fueled events they genuinely expect to experience in the near future. Here is what made the list, ranked from helpful everyday shortcuts to straight-up nightmare scenarios:

The event participants felt most certain would happen to them in the next few months was a chatbot helping them do something that saves them time (46%), followed by a chatbot giving them an incorrect answer to a question (38%), and helping them solve a personal problem (36%). Around a third also believe they'll think they're talking to a human on the phone when it's actually an AI (31%).

Worth noting, though, is that further down the list sit some genuinely serious possibilities: 19% think a chatbot might give them dangerous advice, and 13% think someone might use an AI tool to create a naked image or video of them.

Which of the following do you think might happen to you in the next few months?

A chatbot helps you do something that saves you time	46%
A chatbot gives you an incorrect answer to a question you ask it	38%

Which of the following do you think might happen to you in the next few months?

A chatbot helps you solve a personal problem	36%
You think you are talking on the phone with a human but it is actually an AI	31%
A chatbot remembers something about you that you did not want it to	24%
You are shown an ad about something that you have only ever shared with a chatbot	22%
A chatbot takes an action (e.g., sending an email or making a purchase) that you did not want it to	20%
A chatbot gives you dangerous advice	19%
Someone uses an AI tool to create a naked image or video of you	13%

 KEY TAKEAWAYS: SUBCHAPTER 6.4

01

Positive vibes, bigger worries:

People feel cautiously optimistic about AI's potential, but widespread fears about AI-powered cybercrime overshadow those warm feelings.

02

Scams will get slicker: Most participants believe AI will make impersonation and bypassing security systems a walk in the park for cybercriminals.

03

Expecting the good but also the ugly: Most people expect chatbots to save them time or solve problems soon, but an alarming share also expect their personal information to be misused, and some anticipate more serious harms like unsafe advice or non-consensual imagery being created of them.



Chapter 6 summary cheat-sheet

AI has entered the mainstream (and we're oversharing): A massive 80% of people now use AI tools – mostly for quick life queries (67%) and work tasks (52%). But in doing so, users regularly type in sensitive info: passwords (13%), bank details (11%), health records (40%), and deep personal secrets (32%).

Workplace AI has outrun the rules: Half of the entire participant pool (50%) use AI on the job. 44% do so because their employer either encourages or requires it, and 41% started of their own volition. Yet 52% of those who use AI at work have received zero risk or security training. The result? 32% admit to sharing confidential company data with AI tools without their boss knowing.

Fear of AI crime beats tech excitement: While 55% think AI is generally good for society and 50% think its benefits outweigh any potential risks it poses, concerns about AI cybercrime (67%), slicker scams (63%), and online safety challenges (61%) run much higher.

Optimistic expectations, but real risks loom: Over the next few months, people expect bots to save them time (46%) or help with problems (36%). However, significant numbers anticipate dangerous advice (19%) or malicious deepfake imagery (13%).

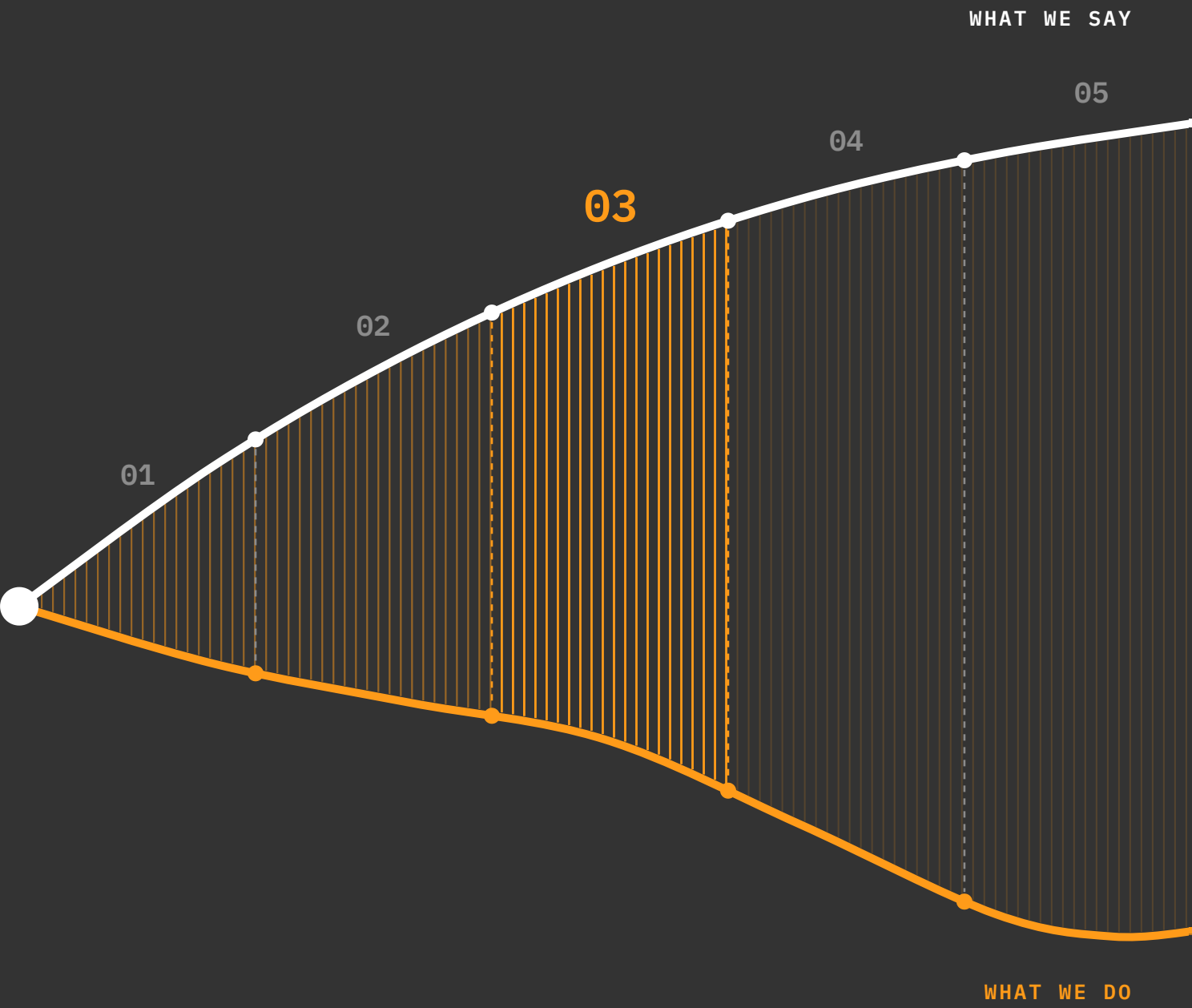
GENERATIONAL HIGHLIGHTS

Millennials are the ultimate AI power users: They use AI more than any other generation (92%), and are the most positive about it, believing it's a good thing for society (70%), that its benefits outweigh the risks (64%), and feeling positive about its increasing use in everyday life (67%). They're also more confident than any other generation about recognizing AI-generated content (e.g., 70% for images).

Older generations remain wary: Baby Boomers and the Silent Generation are far less likely than younger generations to say AI is a good thing for society (35% and 18%), that its benefits outweigh the risks (30% and 16%), or that they feel positive about its increasing use in everyday life (33% and 16%).

SECTION 03

Conclusion



Conclusion

AI is officially a coworker. Time to teach it some manners

AI has officially moved from ‘cool party trick’ to ‘how we get stuff done’. A massive 80% of people are now using AI tools – mostly for everyday Q&As, drafting emails, and summarizing endless text (sensible, we’d say ... so far, so good).

But ...and it’s a big ‘but’ (and we cannot lie*) ...plenty of us are also using AI for health advice, or even treating it like a digital companion, friend, or therapist. Half of the participants are using AI tools at work: 44% fired them up because their boss urged or required them to, slightly edging out the 41% who jumped in on their own initiative.

And here’s the plot twist: many employers pushing this AI revolution haven’t *actually* set up any ground rules. Governance? ...They don’t know her. 52% of AI-using workers have received *zero* training on the security or privacy risks of these shiny new(ish) tools.

On top of that, 43% of those using AI at work say their company’s guidelines on what *not* to feed the AI monster were either completely absent or clear as mud. Translation? We’re rolling out AI at work, but forgetting to hand out the safety goggles and the manual. So, it should shock absolutely no one that 32% admit to leaking sensitive work details to AI tools behind their employer’s back – usually (shockingly) internal documents, customer data, or financial information.

And guess who’s leading the charge? Younger employees, who double as both the biggest AI fans and the fastest adopters. ...Come on, guys. You’re the future!

Companies need a wake-up call. Because quirky fringe hobby this is not. What it *is*, is a massive, unmanaged risk. But don’t go in all guns blazing here ...banning AI isn’t the answer (good luck with that, even if you tried).

*For those unfamiliar with the inimitable work of Sir Mix-a-Lot, may we suggest a short peruse in his direction on your search engine of choice.

CONCLUSION

Instead, businesses need rock-solid policies, secure tools, clear guidance, and easy systems that empower staff to use AI safely. Only then can they turn AI into a secure, superpowered asset.

Real-world plays like AI tool registries, role-tailored support, and internal audits will help organizations shift from a restrictive, scolding posture of ‘don’t even think about it’ to a slick system of controlled enablement. Or, in other words, unlocking AI’s magic while keeping the scary (and ever-evolving) risks in check. Magic: ✅. Scary risk: ❌.

If AI has already moved into your office (and spoiler alert: it definitely has), solid [AI governance](#) needs to be sitting right beside it.

Know your audience (or watch them hit ‘skip’)

When cybersecurity training is competing with a mountain of daily work, it better be fast, hyper-relevant, and impeccably timed.

The era of one-size-fits-all cybersecurity training is over. Our data shows that while shiny videos are the top favorite for training, plenty of people still love bite-sized content, periodic online check-ins, and good old-fashioned written guides. Age plays a huge role here: younger generations naturally flock to video, while older teammates and retirees lean heavily toward reading.

People skip training for all sorts of reasons, too. Sure, ‘I don’t have time’ is the heavyweight champion of excuses, but ‘I already know this stuff’, ‘I don’t think that training will reduce my risk of being a victim of cybercrime’ and ‘cyber isn’t important to me’ are wildly common runners-up.

Unpacking *why* people skip out (and what formats actually click for them) is the secret to building training people will willingly, voluntarily finish. It’s hardly a newsflash that static, copy-paste training programs will always flop in a diverse workplace. If you want real engagement, you have to meet people where they are: adapt your formats, use bite-sized microlearning to save their (precious) time, and use real-world examples that actually match their job. By meeting people where they are, organizations can increase engagement and, more importantly, translate knowledge into consistent and reliable security behaviors. (AKA the holy grail. 🏆)

When it comes to training, real change comes from relevance. The trick is [matching the method to the person](#).

Knowledge ≠ behavior (or why smart people use not-so-smart passwords)

Once again, this year's data reveals a massive knowing/doing gap. People know the rules, they just aren't following them. 🙄 A staggering 73% boast that they know how to make a bulletproof password and do it regularly, yet personal details and basic dictionary words keep clogging up password logs. Hmm...

Six out of ten participants are shameless password reusers ...either recycling one master password everywhere, playing musical chairs with a handful of codes, or taking a base password and slapping a tiny tweak on the end. (Which, by the way, makes a hacker's job absurdly easy once a single account gets cracked. You're essentially giving them a gift. 📁 How kind of you.)

Meanwhile, 53% don't use MFA regularly, including 21% who fully understand how it works and just refuse to use it anyway. 🙄 Oh, and good luck getting people onto password managers; people are still vastly more likely to scribble passwords in a paper notebook than use an app or browser tool. Yes, really. 🙄

We see the exact same stubbornness with newer tech. Nearly three-quarters (70%) of our participants know (or sort of know) what passkeys are, but only 39% actually use them. Only 53% use biometrics, and the most common reasons for not adopting them are privacy concerns and distrust of the technology, rather than unfamiliarity. So, the barrier isn't a lack of knowledge, so much as a lack of trust and motivation to act on that knowledge.

That's because *knowing* things is only half the battle. Throwing info or mandatory slide decks at people isn't enough to drive lasting behavior change.⁴² Enter the COM-B model for behavior change, which proposes that for real Behavior (B) to happen, you need three magic ingredients: Capability (C), Opportunity (O), and Motivation (M).

Old-school training only checks the Capability box, which is why progress feels so chaotic. We have to look past boring lectures and fix Opportunity and Motivation. That means building friction-free systems that are a breeze to use, offering instant high-fives for good security moves, and creating a culture that celebrates smart choices instead of dunking on honest mistakes. The dream target? The goal must be to make the secure choice the easiest and most intuitive choice.⁴³

42 Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour?. *International Conference on Cyber Security for Sustainable Society*.

43 Nurse, J. R. C., Creese, S., Goldsmith, M., & Lamberts, K. (2011, September). Guidelines for usable cybersecurity: Past and present. In *2011 Third International Workshop on Cyberspace Safety and Security (CSS)* (pp. 21-26). IEEE.

CONCLUSION

Did someone say Human Risk Management? You know, that cool, data-driven approach that predicts employee risk, drops real-time micro-nudges, and builds a thriving security culture? Start with the [definitive guide to HRM](#). And if you're still hungry for more – which we (somewhat immodestly) suspect you will be – [this whitepaper](#) is your personal feast.

Privacy fatalism persists. AKA: 'I'm getting hacked anyway, so why bother?'

For a huge chunk of people, losing money or having their identity stolen doesn't feel like a preventable threat ...it just feels like an inevitable tax of existing online. This heavy fatalism goes hand in hand with a deep cynicism toward the system: tons of participants doubt the police can handle cybercrooks, and firmly believe hackers are way smarter than the people trying to stop them. Which is somewhat disheartening.

While general fear of cybercrime is sky-high, surprisingly few people think they will personally be targeted. Hello, optimism bias⁴⁴...it's the classic human reflex: 'Bad stuff only happens to other people.' Cybercrime feels like an abstract movie plot, making it super easy to acknowledge in theory, but also effortlessly easy to ignore in real life. 🙄

Overwhelmed by digital chaos, half of all participants have started pulling back from using online services as much. But retreating isn't defending, and it leaves you just as vulnerable as before. 🙄 Worse yet, over a third of people have thrown their hands up entirely, figuring: 'Why bother securing my data? My information is already online anyway.'

This cocktail 🍸 of feeling exposed, doubting authorities, and hiding under a rock is a massive roadblock for security. When people decide losing their privacy or security is inevitable, they lose all motivation to take simple, protective actions that are, in fact, totally in their control.⁴⁵

Psychologically, this is a massive reflective motivation slump (yep, the COM-B model again, hi motivation old pal 🙌). People simply don't believe their efforts will pay off, and dropping more terrifying threat stats won't fix a problem caused by people who've given up hope.

Stop reminding people that the digital monster is under the bed ...they already know that. Instead, give them hard proof that protective actions actually work. Public trust and a sense of personal agency need to be rebuilt on that basis, directly and quickly: people need to understand how security relates to them, and to see proof that individual actions and systemic protections make a tangible difference.

44 Weinstein, N. D. (1980). Unrealistic optimism about future life events. *Journal of Personality and Social Psychology*, 39(5), 806–820.

45 Penney, J. W. (2026). Privacy fallacies and fatalism. *Lex Electronica*, 31(2), 60–77.

CONCLUSION

In practice, that means binning fear-mongering lectures and replacing them with practical steps. Think inspiring stories or social proof (i.e., showing real people who took simple security steps and lived happily ever after).

Too cool for cyber school: The Gen Z & Millennial paradox

Millennials and Gen Z are the undisputed heavyweights of AI usage, adoption, and digital swagger. They also boast the absolute highest confidence in spotting AI-generated text, images, video, and audio. Millennials also report the highest confidence in identifying fishy phishing attempts across email, scam texts, and suspicious links. 🐟

And yet ...these exact same two generations are the absolute most likely to secretly dump confidential work data into AI tools, and they report the worst password hygiene of any generation ...routinely using dictionary words and personal info. Yikes. 🤖

Even wilder? They suffered the highest overall crime rates of any age group (64% for Gen Z, 57% for Millennials), taking the biggest hit across almost every cybercrime category, including sophisticated deepfake scams.

Read that again: The youngest, most tech-confident generations are also the most likely to get successfully scammed. This wild paradox is classic overconfidence bias – the human tendency to wildly overestimate our abilities, which can have a significant impact on decision-making, particularly in the context of risk-taking⁴⁶. In the context of cybersecurity, overconfidence can drive individuals to underestimate cyber threats, skip preventive measures, and make poorer security decisions⁴⁷.

Overconfidence thrives in the gap between what people *think* they know versus what they *actually* know (i.e., the discrepancy between perceived and actual skills). The best way to snap people out of it? Instant, direct feedback that politely shows them where their confidence is completely detached from reality.

Supporting people as they deal with online risk matters immensely here: if your training only uses laughably easy, obvious scam examples, people leave feeling invincible ...and then get wrecked by real-world scams. Familiarity is a trap. Just because a platform or sender feels familiar doesn't mean it's safe, a lesson tech-immersed generations desperately need to learn.

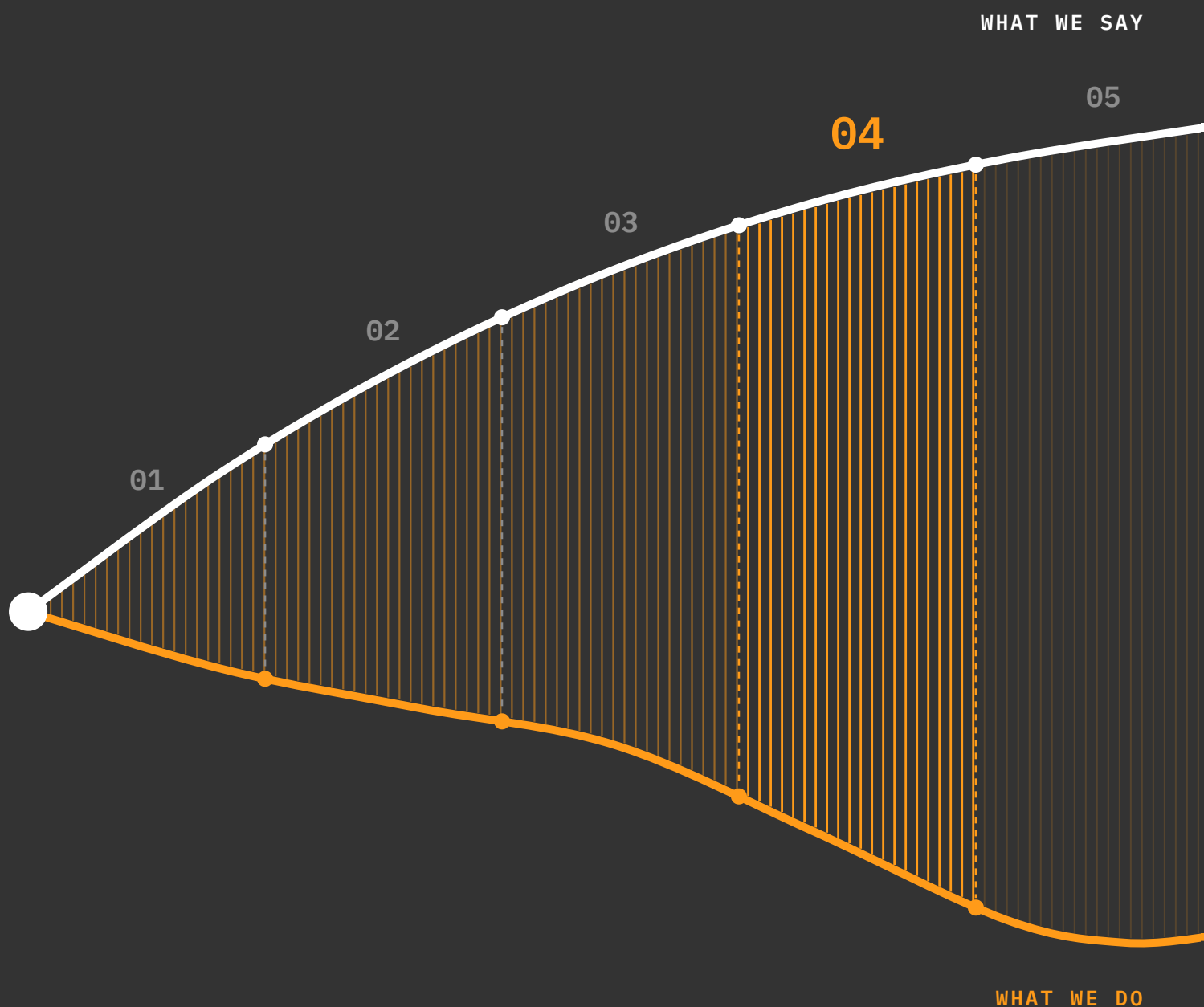
46 Dhannur, V., & Kusane, S. (2023). Managing Overconfidence Bias in Decision Making: A Review of the Literature. *Education and Society*, 46(3), 394-399.

47 Wang, J., Li, Y., & Rao, H. R. (2016). Overconfidence in phishing email detection. *Journal of the Association for Information Systems*, 17(11), 759–783. Alnifie, K. M., & Kim, C. (2023). Appraising the manifestation of optimism bias and its impact on human perception of cyber security: A meta analysis. *Journal of Information Security*, 14(2), 93-110.

SECTION 04

Appendix A

Methodology



Appendix A: Methodology

Survey design

We designed this survey to explore a wide variety of everyday attitudes toward cybersecurity and AI. We also wanted to dive into key digital security behaviors, such as keeping up good password hygiene, using MFA and biometrics, installing software updates promptly, backing up data regularly, and spotting or reporting phishing attempts. On top of that, we took a closer look at personal experiences with cybercrime (including various online scams and deepfakes) as well as cyberbullying.

Each year, we review and refresh the survey questions, and make adjustments based on the previous year's findings, related consumer and academic research or the evolving landscape of digital life. This year, we also collaborated with [Dr. Lorrie Cranor](#) and her team from Carnegie Mellon University CyLab to redesign our survey questions. As a direct result of that teamwork, we made the following updates:

- **19 brand new questions were added:** These mostly cover AI adoption, how often people use AI, and general attitudes toward it (like Figure 69, which highlights how employees started using AI tools for work). We also added questions about authentication methods (such as Figure 52, asking 'Do you know what passkeys are?'). In Chapter 3, we also expanded our cybercrime measurements by adding four new scam types: job scams, delivery scams, online marketplace scams, and lottery/prize scams. Each of these came with a follow-up question asking whether the victim reported the incident.
- **44 existing questions were modified:** We updated these by adding, removing, or significantly rewording answer options. For example, a single question about concern regarding foreign and domestic governments was broken out into four separate statements. This allowed us to cover both types of governments while clearly distinguishing between governments sharing personal data versus using data to influence what people see or think (Figure 7).

- **Response formats were expanded:** Certain questions that previously allowed only a single answer choice were updated to multi-select. This gives us a much clearer picture of what participants are thinking, particularly when it comes to barriers to healthy security behaviors (for example, the reasons people give for not using a password manager in Figure 45).

When you count the demographic questions, the full survey featured 46 core questions given to every single participant, alongside 49 targeted follow-up questions.

To keep things straightforward, the survey mostly used multiple-choice and single-choice questions. These offered either 5-point or 10-point Likert scales anchored at the ends (such as ‘Strongly agree’ to ‘Strongly disagree’) or descriptive answer options (ranging from ‘Always’ to ‘Never’). For specific questions, respondents had an ‘Other, please specify’ option so they could write in their own thoughts. Finally, to gather rich, in-depth feedback on why some people choose not to use biometrics for authentication, one question relied entirely on an open essay text box for a qualitative response.

Procedure

A call for participation was placed by the Toluna⁴⁸ platform for the United States, the United Kingdom, India, Brazil and Singapore. The survey was administered in English except in Brazil, where participants received and responded to the survey in Brazilian Portuguese. The survey was designed to be completed in under 30 minutes.

Participants who completed the survey were compensated for their time. They were briefed about the survey, and their informed consent was required before they could begin. We explicitly asked participants not to share any personal information in their responses and reassured them that all data would be fully anonymized. It was stressed that participation was entirely voluntary, and respondents had the right to withdraw whenever they pleased. The Science and Research (S&R) team at CybSafe did not collect any personally identifiable information.

Data collection officially ran from April 28, 2026, through May 19, 2026.

⁴⁸ <https://uk.toluna.com>

Sample

Toluna recruited a representative sample (balanced for gender and age) of 1,000 participants per country, which gave us a grand total of 5,000 respondents. Every participant was at least 18 years old, and the average age across the board was 45 years old ($SD = 16.63$). If you want to check out the detailed demographic breakdown by country – including gender, age, and employment status – you can find all those details laid out in Table 3 (below).

There was a relatively even distribution across the generations:

- **Millennials:** 30.6%
- **Gen X:** 28.1%
- **Gen Z:** 22.3%
- **Baby Boomers:** 18.1%
- **Silent Generation:** 0.9%

When it comes to work life, the clear majority (65.4%) of participants were employed either full-time or part-time, which includes working students (2%). Roughly a third of our respondents (34.6%) reported that they were not employed (which includes 18.6% of retired participants).

Table 3. Participant demographics, by country.

Demographic		United States (n = 1,000)	United Kingdom (n = 1,000)	India (n = 1,000)	Brazil (n = 1,000)	Singapore (n = 1,000)	Total (N = 5,000)
Gender (N = 5,000)	Female	486 48.6%	490 49.0%	511 51.1%	484 48.4%	492 49.2%	2463 49.2%
	Male	514 51.4%	509 50.9%	489 48.9%	509 50.9%	508 50.8%	2529 50.6%
	Non-binary / third gender	0 0.0%	1 0.1%	0 0.0%	7 0.7%	0 0.0%	8 0.2%
	Prefer not to say / Prefer to self-describe	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%
Age (N = 5,000)	Gen Z (18-29)	197 19.7%	131 13.1%	328 32.8%	254 25.4%	205 20.5%	1115 22.3%
	Millennials (30-45)	316 31.6%	260 26.0%	327 32.7%	329 32.9%	297 29.7%	1529 30.6%
	Gen X (46-61)	229 22.9%	314 31.4%	255 25.5%	278 37.8%	329 32.9%	1405 28.1%
	Baby Boomers (62-80)	242 24.2%	272 27.2%	88 8.8%	138 13.8%	167 16.7%	907 18.1%
	Silent Generation (81+)	16 1.6%	23 2.3%	2 0.2%	1 0.1%	2 0.2%	44 0.9%
Employment status (N = 5,000)	Employed	644 64.4%	642 64.2%	616 61.6%	627 62.7%	641 64.1%	3170 63.4%
	Full-time	516 51.6%	476 47.6%	519 51.9%	513 51.3%	582 58.2%	2606 52.1%
	Part-time	128 12.8%	166 16.6%	97 9.7%	114 11.4%	59 5.9%	564 11.3%
	Students	30 3.0%	28 2.8%	143 14.3%	94 9.4%	74 7.4%	369 7.4%
	Not working	21 2.1%	20 2.0%	109 10.9%	71 7.1%	49 4.9%	270 5.4%
	Working student	9 0.9%	8 0.8%	34 3.4%	23 2.3%	25 2.5%	99 2.0%
	Retired	225 22.5%	248 24.8%	105 10.5%	135 13.5%	219 21.9%	932 18.6%
	Don't work or study outside home	101 10.1%	82 8.2%	136 13.6%	144 14.4%	66 6.6%	529 10.6%

Participants' highest level of education for each country is listed in Table 4. The most common qualification was an undergraduate degree, held by 37.3% of the total participants.

Table 4. Participants' education levels, by country.

Highest level of qualification (N = 5,000)	US (n = 1,000)	UK (n = 1,000)	India (n = 1,000)	Brazil (n = 1,000)	Singapore (n = 1,000)	Total (N = 5,000)
No formal education	17 1.7%	6 0.6%	4 0.4%	3 0.3%	2 0.2%	32 0.6%
Primary education	96 9.6%	7 0.7%	37 3.7%	9 0.9%	6 0.6%	155 3.1%
Secondary education	207 20.7%	249 24.9%	310 3.1%	91 9.1%	112 11.2%	969 19.4%
Vocational or technical qualification (post-secondary and below bachelor's)	178 17.8%	215 21.5%	139 13.9%	56 5.6%	232 23.2%	820 16.4%
Undergraduate degree (bachelor's or equivalent)	294 29.4%	317 31.7%	343 34.3%	411 41.1%	500 50.0%	1865 37.3%
Postgraduate degree (master's, doctorate, or professional degree)	192 19.2%	192 19.2%	163 16.3%	419 41.9%	136 13.6%	1102 22.0%
Prefer not to say	16 1.6%	14 1.4%	4 4.0%	11 1.1%	12 1.2%	57 1.1%

Table 5 gives you a detailed overview of the various professional sectors for our working participants (n = 3,269). Employment spanned across a vast mix of industries, though a few sectors naturally stood out with higher concentrations of workers. Across the entire sample, the top three industries were:

- **Information technology and telecommunications:** 20.9%
- **Education:** 10.5%
- **Finance and insurance:** 9.4%

Table 5. Industries employed participants work in, by country.

Industry (n = 3,269)	US (n = 653)	UK (n = 650)	India (n = 650)	Brazil (n = 650)	Singapore (n = 666)	Total (n = 3,269)
Agriculture, forestry, and fishing	19 2.9%	8 1.2%	12 1.8%	11 1.7%	10 1.5%	60 1.8%
Arts, entertainment, and recreation	22 3.4%	18 2.8%	8 1.2%	19 2.9%	16 2.4%	83 2.5%
Construction	44 6.7%	48 7.4%	18 2.8%	31 4.8%	44 6.6%	185 5.7%
Education	42 6.4%	68 10.5%	92 14.2%	73 11.2%	67 10.1%	342 10.5%
Finance and insurance	43 6.6%	48 7.4%	91 14.0%	31 4.8%	95 14.3%	308 9.4%
Government and public administration	9 1.4%	29 4.4%	13 2.0%	38 5.8%	34 5.1%	123 3.8%
Healthcare and social assistance	75 11.5%	81 12.5%	35 5.4%	31 4.8%	69 10.3%	291 8.9%
Hospitality and tourism	21 3.2%	33 5.1%	15 2.3%	14 2.2%	26 3.9%	109 3.3%
Information technology and telecommunications	161 24.7%	116 17.8%	182 28.0%	145 22.3%	78 11.7%	682 20.9%
Manufacturing	44 6.7%	41 6.3%	47 7.2%	29 4.5%	64 9.6%	225 6.9%
Marketing, advertising, and public relations	16 2.4%	5 0.8%	33 5.1%	23 3.5%	9 1.4%	86 2.6%
Mining, quarrying, and utilities	7 1.1%	1 0.2%	5 0.8%	5 0.8%	7 1.0%	25 0.8%
Nonprofit and charity organizations	8 1.2%	12 1.8%	3 0.4%	2 0.3%	7 1.0%	32 1.0%
Professional, scientific, and technical services	36 5.5%	48 7.4%	43 6.6%	39 6.0%	47 7.1%	213 6.5%
Retail and wholesale trade	66 10.1%	51 7.8%	30 4.6%	87 13.4%	41 6.2%	275 8.4%
Transportation and logistics	22 3.4%	20 3.1%	9 1.4%	36 5.5%	35 5.2%	122 3.7%
Other	18 2.8%	23 3.5%	14 2.2%	36 5.5%	17 2.6%	108 3.3%

Data quality

Our survey provider built in quality control steps to protect the integrity of the data. If a respondent turned in low-quality data (like leaving answers incomplete), they were removed from the study and replaced with a new participant, so we could hit our targeted sample size. We also included two explicit attention-check questions to filter out automated 'bots' or speed-runners who were just clicking through options without actually reading the questions.

Data analysis

Descriptive statistical analyses were conducted on all Likert-based questions, providing frequencies (N) and proportions (%). Proportions were presented using various data visualization techniques, including tables and charts.

To keep the charts clean and straightforward to digest, all original 5-point and 10-point Likert scale options (e.g., 'Strongly agree' to 'Strongly disagree') were regrouped into 3 simplified categories (e.g., 'Agree', 'Neutral', and 'Disagree').

Qualitative data were analyzed using thematic analysis. We pulled out the most compelling direct quotes to help illustrate major themes, adding real human depth and color to the numerical findings in the report. Any qualitative comments submitted in Brazilian Portuguese were translated into US English using automated machine translation tools.

Finally, in Appendix B, we flagged notable trends and comparisons against our *Oh, Behave! 2025-26* report. Since this year marked our first time collecting data from Singapore, no year-over-year comparison data exists yet.

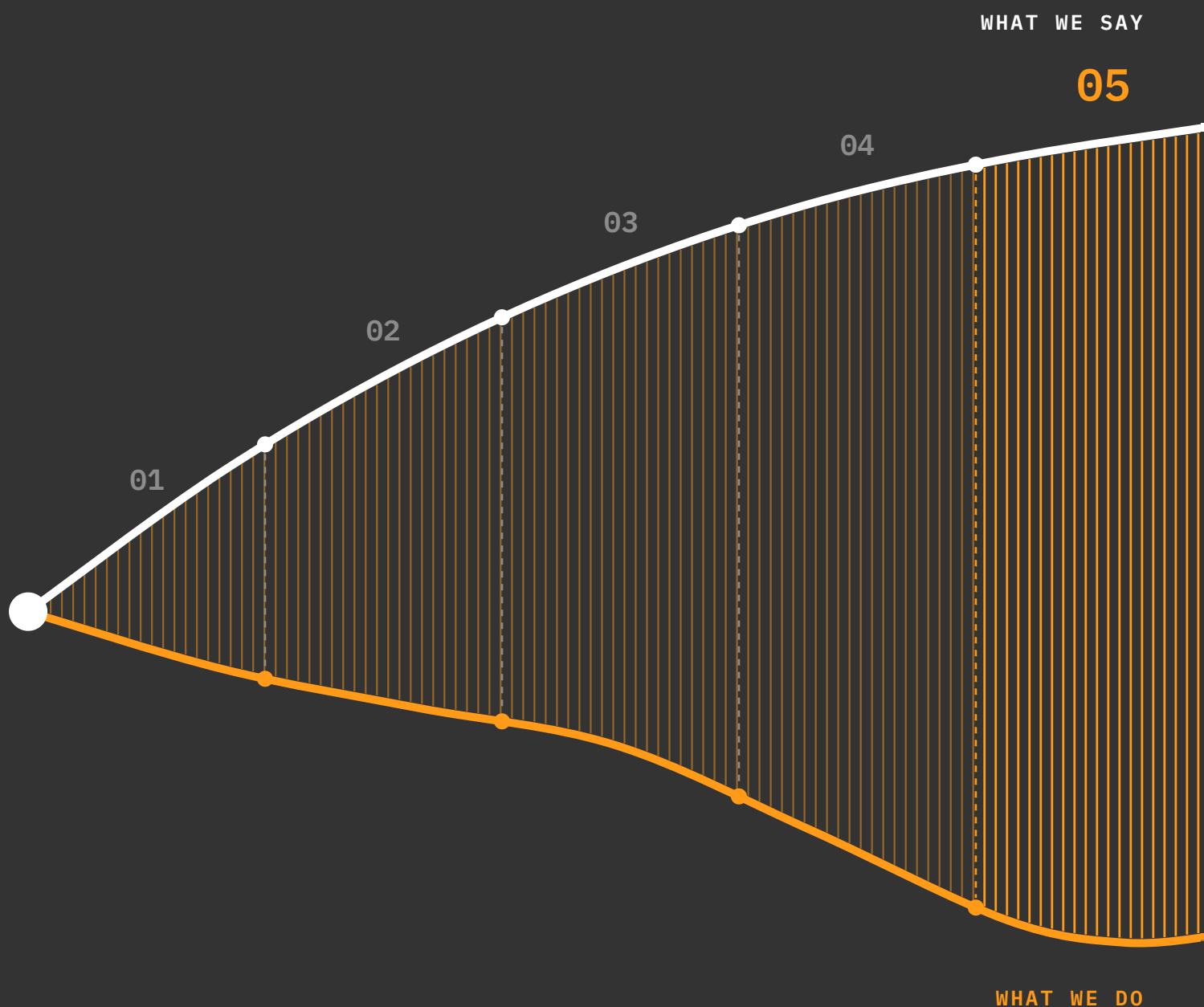
AI disclosure

Generative AI, specifically Claude (Anthropic), was used to support the preparation of this report. This included assisting with checking grammar and clarity, and verifying reported statistics against the underlying survey dataset. AI was not used to generate the survey data itself, to analyze the survey data, to make analytical or editorial decisions, or to draw conclusions on our behalf. All statistics, interpretations, and conclusions in this report were reviewed, verified, and approved by the CybSafe team.

SECTION 05

Appendix B

Country comparisons



Appendix B: Country comparisons

This appendix provides a country-by-country comparison of some of the core survey findings among our participating countries: the United States, the United Kingdom, India, Brazil, and Singapore⁴⁹.

The analysis that follows covers the same topics as the [Main findings](#), organized into matching chapters:

- Attitudes, beliefs & perceptions about online security
- Cybercrime victimization
- Cybersecurity training
- Cybersecurity behaviors
- AI

Even though respondents shared plenty of common ground, we were particularly interested in digging into where the five countries differed. This approach allows us to better understand how national trends and cultural contexts may influence cybersecurity attitudes, behaviors and decision-making.

Attitudes, beliefs & perceptions about online security

Let's explore how attitudes toward online security shift around the world, by looking at everything from feelings of personal control and everyday frustration, to worries about government app misuse, the reach of media influences, and overall workplace security cultures.

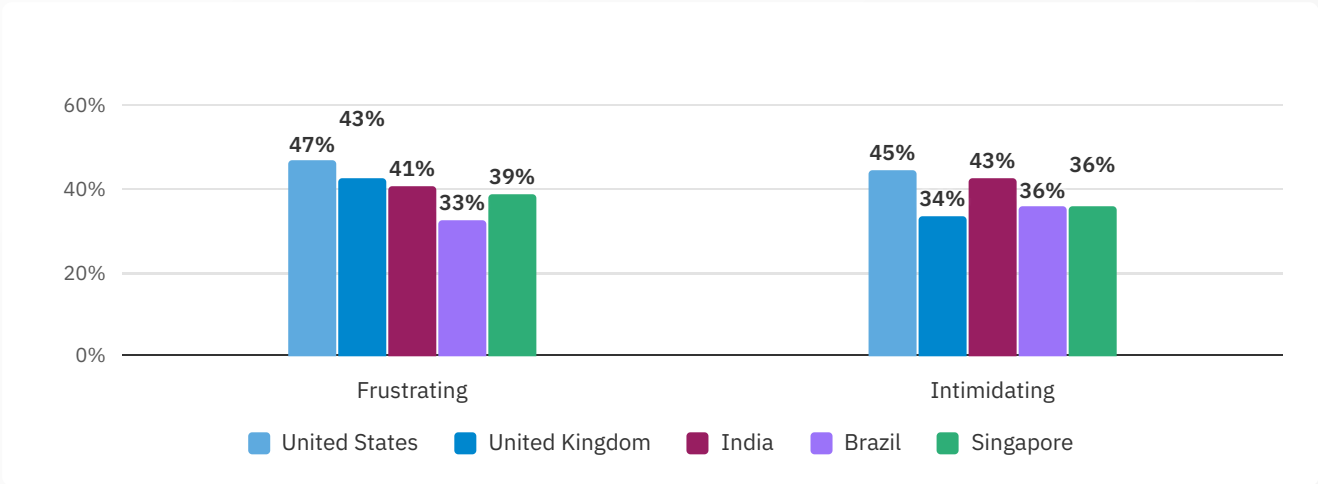
When asked whether they find staying secure online frustrating and intimidating (Figure 84), participants in the United States logged the highest percentages for both emotions, with 47% feeling frustrated (a 3% drop from 2025) and 45% feeling intimidated (down 2% from 2025).

Following the US on the frustration scale, the UK came in second at 43% (a 5% rise from 2025), closely followed by India at 41% (down 2% from 2025) and Singapore at 39%. On the other end of the spectrum, only 33% of respondents in Brazil found online security frustrating (up 1% from 2025).

⁴⁹ Where comparisons are made to last year's report, it's worth noting that the participating countries changed between years. *Oh, Behave!* 2025-26 included seven countries (Germany, Australia, and Mexico were also included, but are not part of this year's survey), while this year includes five, with Singapore appearing for the first time. Year-on-year comparisons are shown only where the same country and question were surveyed in both years.

Interestingly, while a fair chunk of UK participants (43%) found staying secure online to be frustrating, far fewer viewed it as intimidating, with just 34% agreeing (down 1% from 2025). Participants in Brazil and Singapore felt very similarly on the intimidation question, both coming in at 36%.

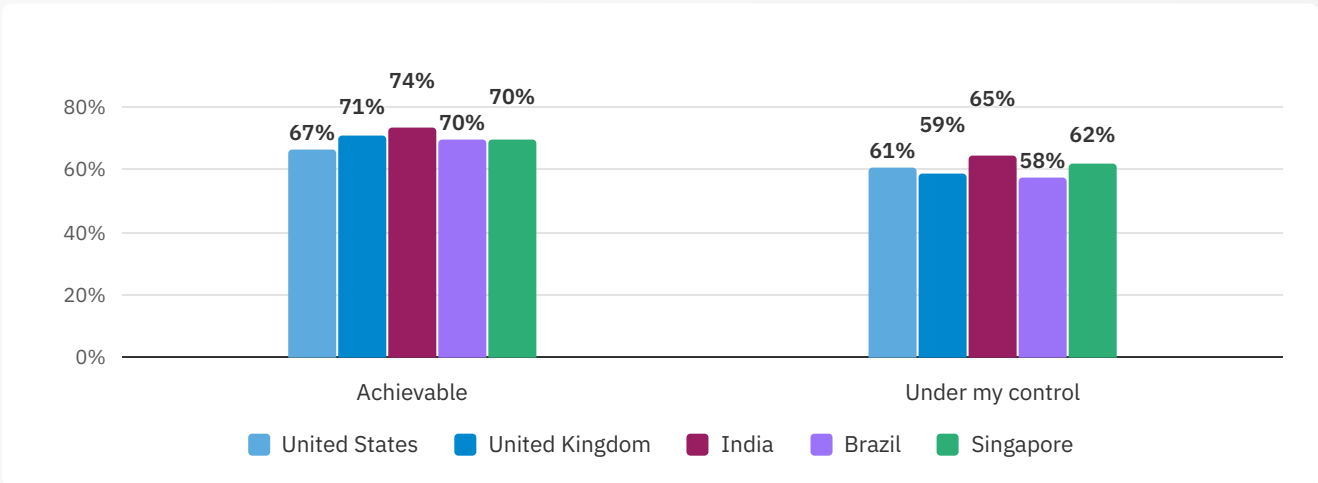
Figure 84. ‘I feel that staying secure is frustrating & intimidating.’ by country.



Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

Even though a solid portion of participants in India expressed that staying secure feels frustrating (41%) and intimidating (43%, down 6% from 2025), respondents from India simultaneously had the highest percentages when asked if digital security feels achievable and within their power to control (74% and 65% respectively, though these reflect 3% and 5% drops from 2025, Figure 85).

Figure 85. ‘I feel that staying secure is achievable and under my control.’ by country.



Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

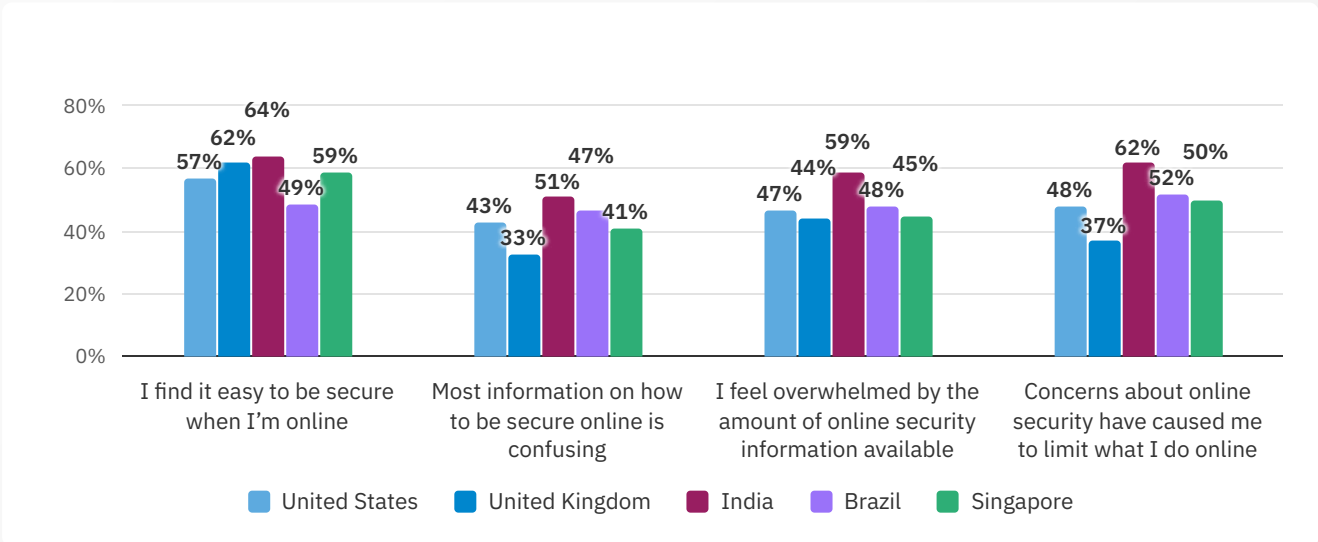
APPENDIX B: COUNTRY COMPARISONS

Clear country-level differences also popped up when we asked participants how easy, clear, and manageable online security feels in their day-to-day lives (Figure 86). Respondents in India (64%, down 1% from 2025) and the UK (62%, up 5% from 2025) were the most likely to agree that maintaining online security is easy, followed by Singapore at 59% and the US at 57% (down 1% from 2025). Brazil stood out as a noticeable outlier on this question, with under half of its participants (49%, identical to 2025) agreeing that staying secure is easy.

However, the picture completely flips upside down when you look at the more negative sentiments. India topped the charts across all five nations on every negative measure: 51% felt security information is confusing (down 5% from 2025), 59% felt completely overwhelmed by the sheer mountain of security information out there, and 62% admitted that cybersecurity worries have forced them to restrict their online activities. The UK sat at the complete opposite end of the spectrum for every single one of these negative points, logging the lowest rates of confusion (33%, down 1% from 2025), overwhelm (44%), and limiting online behavior due to concerns (37%).

Brazil and Singapore comfortably settled in the middle ground across these three negative areas. Even though Brazilian participants were the least likely to view security as easy, their levels of confusion (47%, up 2% from 2025), feeling overwhelmed (48%), and restricting online behavior (52%) were fairly moderate.

Figure 86. Participants’ levels of agreement with online security ease, clarity, and impact, by country.



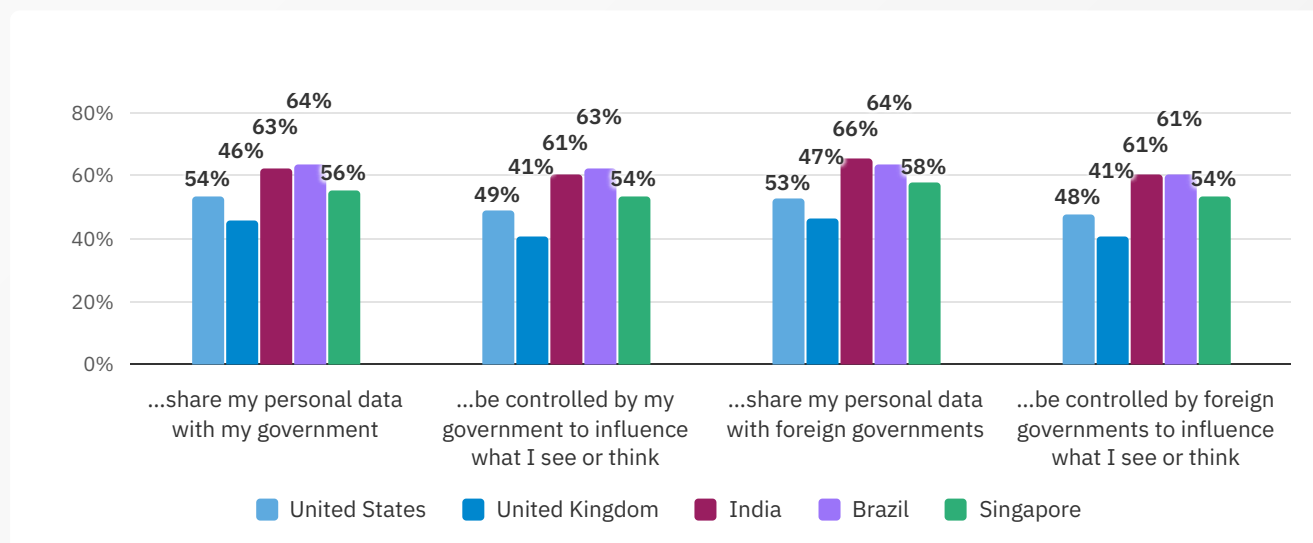
Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

Concerns about government misuse of apps also varied notably by country (Figure 87). When asked about apps handing over personal data to foreign governments, anxiety peaked in India (66%) and Brazil (64%), contrasting sharply with 53% in the US and a modest 47% in the UK. We saw this exact same geographical dynamic when asking about domestic governments: India (63%) and Brazil (64%) recorded the highest concerns, while the US sat at 54% and the UK registered the lowest concern at 46%.

Concerns about apps being used to influence what citizens see or think followed the exact same country ranking, albeit with slightly lower figures overall. Worries regarding foreign governments sharing personal data ranged from 61% in both India and Brazil down to 41% in the UK. For domestic government influences, figures ranged from a high of 63% in Brazil to a low of 41% in the UK.

Across all four of these specific survey statements, respondents in India and Brazil consistently showed the highest levels of concern, while participants in the UK consistently showed the lowest, regardless of whether the question targeted a foreign or domestic government, or focused on data collection versus narrative control.

Figure 87. 'I'm concerned that my apps may...' by country.



Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

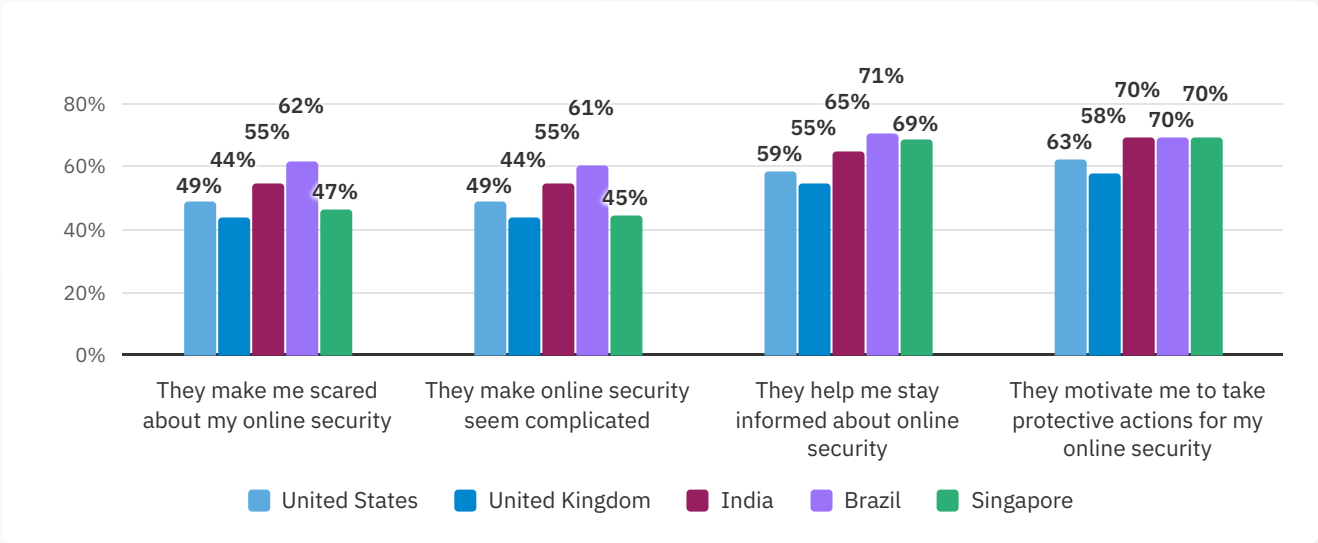
When analyzing how media coverage influences public perceptions of cybersecurity, country trends remained identical across both encouraging and unsettling measures (Figure 88). The majority of respondents in every single nation agreed that news reports help them stay informed about online security.

This view was strongest in Brazil (71%, up 2% from 2025) and Singapore (69%), followed by India (65%, dropping 9% from 2025), the US (59%, holding steady with 2025), and the UK (55%, down 1% from 2025). The exact same top three nations led the pack when asked if media coverage motivates them to take action to protect themselves, with Brazil, India, and Singapore all hitting 70% agreement, compared to 63% in the US and 58% in the UK.

However, this constructive impact came with a clear downside. Brazil (62%, up 4% from 2025) and India (55%, down 9% from 2025) recorded the highest proportion of respondents who admitted that news stories leave them feeling scared about their digital safety. These same two countries also led the world in feeling that media coverage makes cybersecurity seem way too complicated (61% in Brazil and 55% in India). UK and US participants logged the lowest agreement across both negative measures, with percentages spanning between 44% and 49%.

Put simply, across all four media metrics, Brazil and India consistently reported the strongest media impact (both positive and negative) while respondents in the UK and US consistently experienced the mildest effects.

Figure 88. ‘What impact does the media/news have on your views toward online security?’ by country.



Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

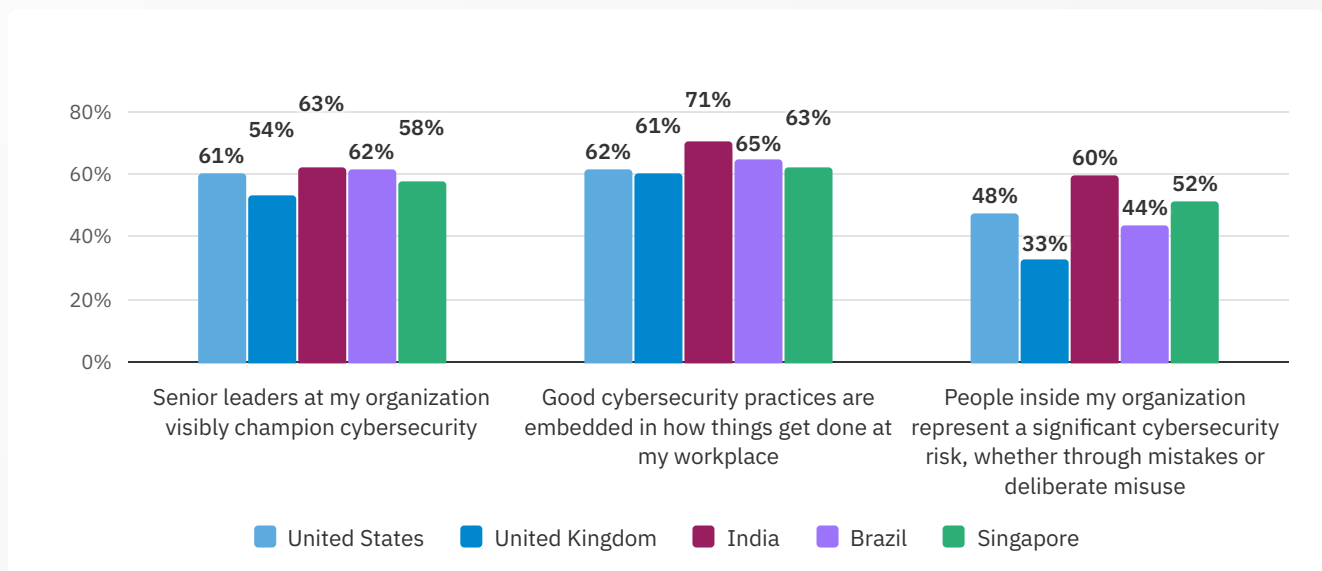
How does workplace cybersecurity culture hold up across the countries surveyed? Employed participants across all five countries generally felt that their organizations take digital security seriously, though the strength of that belief varied (Figure 89).

APPENDIX B: COUNTRY COMPARISONS

A majority of workers in every country agreed that executive leadership visibly champions cybersecurity, led by India (63%) and Brazil (62%), down to the UK at 54%, with the US (61%) and Singapore (58%) sitting in the middle. We also observed a similar, slightly higher agreement pattern regarding whether good cybersecurity practices are baked directly into day-to-day work routines: India led again with 71%, followed by Brazil (65%), Singapore (63%), the US (62%), and the UK at the bottom (61%).

Opinions on internal security risks, however, diverged much more sharply. Workers in India (60%) and Singapore (52%) were most likely to view fellow employees as a significant cybersecurity risk (whether through accidental slip-ups or intentional misuse). That compares to 48% in the US and 44% in Brazil. The UK stood out as a clear exception here: only 33% agreed with this view, making it the only surveyed nation where fewer than four in ten workers viewed internal staff as a cybersecurity risk.

Figure 89. Attitudes toward cybersecurity in the workplace, by country.



Base: US, UK, India, Brazil, Singapore. Total number of participants: 3,269 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.



Summary cheat-sheet

Country comparisons: Attitudes, beliefs & perceptions about online security

US participants expressed the highest frustration (47%) and intimidation (45%) about staying secure.

Brazil reported the lowest frustration rate (33%), and the lowest share who found it intimidating was in the UK (34%). The **UK** also had the lowest share of those who found it confusing (33%), overwhelming (44%), or felt that it limited their behavior due to concerns (37%).

India recorded the highest percentage of those who believe staying secure is achievable (74%), under their control (65%), and easy to maintain (64%). However, Indian respondents were also the most likely to say security details are confusing (51%), overwhelming (59%), and have caused them to restrict their online activities (62%).

Government app misuse worries were highest in India and Brazil, and lowest in the UK. For instance, 63% of respondents in India and 64% in Brazil worried about apps sharing data with their domestic government, versus 46% in the UK. Concern about apps being used by foreign governments to influence what people see or think hit 61% in both India and Brazil, compared to 41% in the UK.

Media impact on views toward online security was strongest in Brazil and India, and mildest in the UK and US across all positive and negative measures. Brazil (71%) and Singapore (69%) recorded the highest percentages who found news coverage most helpful, yet Brazil (62%) and India (55%) were also most likely to say news stories make them feel scared or confused about security. Meanwhile, the UK and US had the lowest shares on both the positive and negative measures throughout.

Workplace culture: India logged the highest agreement that leadership champions security (63%) and that good habits are built into daily work routines (71%), while the UK had the lowest agreement with both (54% and 61%). India (60%) and Singapore (52%) were most likely to view colleagues as a serious security risk, compared to just 33% in the UK.

Cybercrime victimization

Before diving into comparing the victimization rates between countries, let's examine public attitudes toward cybercrime – ranging from the feeling that financial loss is inevitable, to how well people think security defenses work.

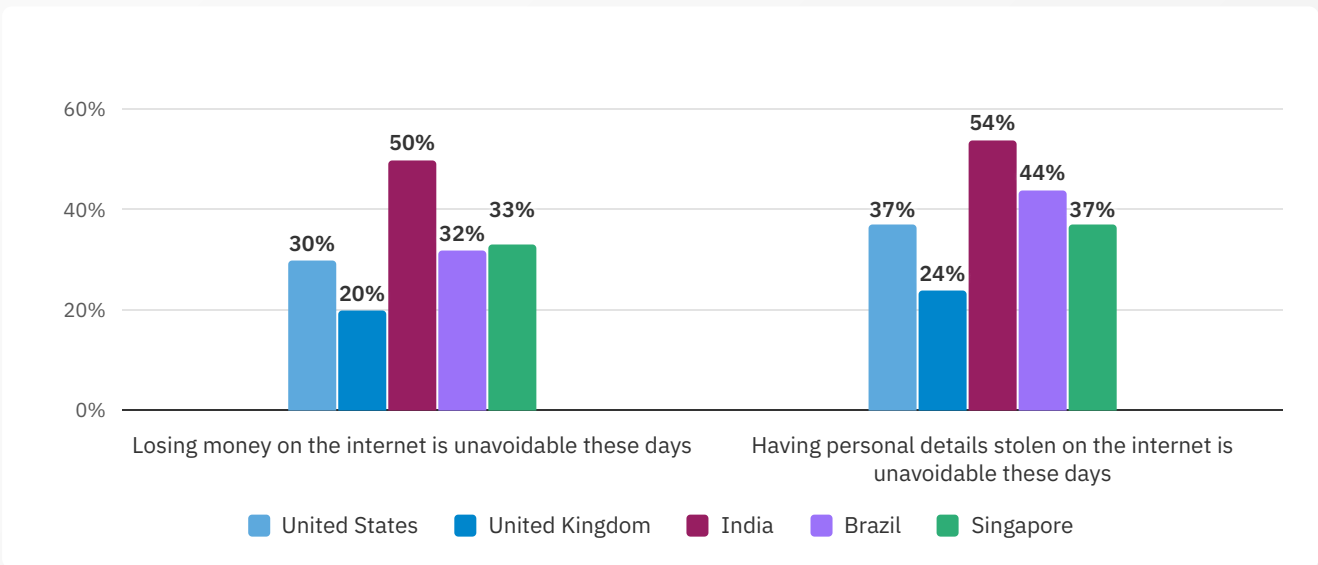
When evaluating how people view cybercrime, we uncovered sharp international differences, starting with whether losing money or personal information online feels like an unavoidable reality of modern life (Figure 90).

The perception that losing money online is unavoidable was lowest in the UK (20%, +3% from 2025), followed by the US (30%, -5% from 2025), Brazil (32%, +6% from 2025), and Singapore (33%).

The pattern was similar for the inevitability of having personal details stolen online. Participants in the UK again reported the lowest percentage (24%, +1% from 2025), followed by the US and Singapore (37% each, -3% from 2025 in the US) and Brazil (44%, -1% from 2025).

Participants from India reported the highest agreement that both losing money (50%) and having personal details stolen (54%, -2% from 2025) online are just unavoidable facts of modern life.

Figure 90. Perceptions on the avoidability of losing money or personal details on the internet, by country.

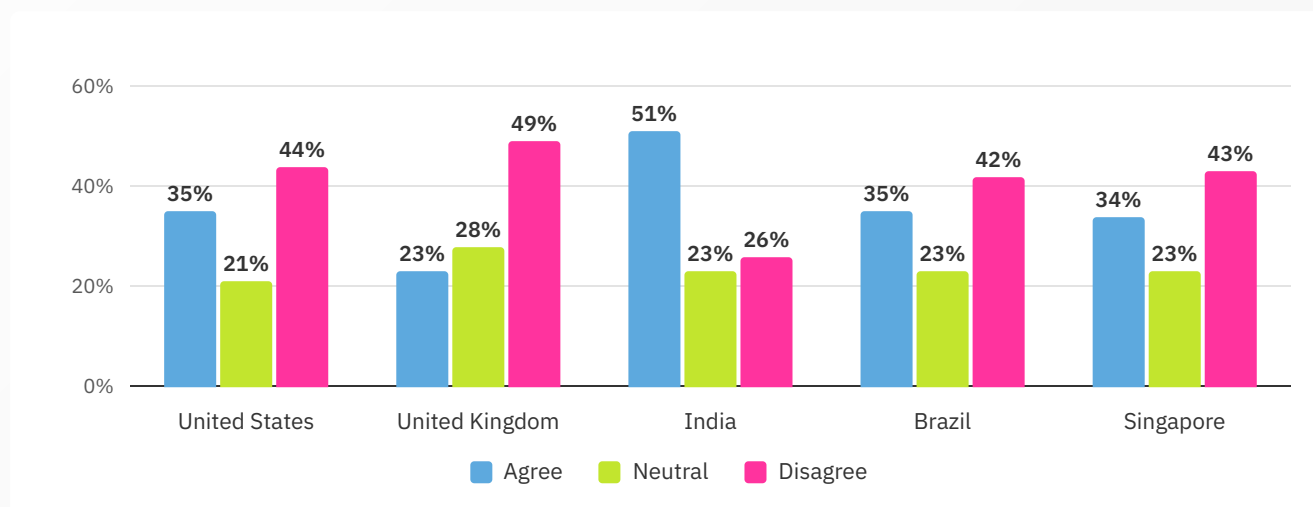


Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

The sentiment that there is no point in trying to protect oneself more as personal information is already online was highest in India (51%, +1% from 2025), compared to 35% in the US (-3% from 2025) and Brazil (+4% from 2025), 34% in Singapore, and just 23% (+1% from 2025) in the UK (Figure 91).

The UK also stood out for having the highest percentage of participants who disagreed with the statement (49%, -6% from 2025).

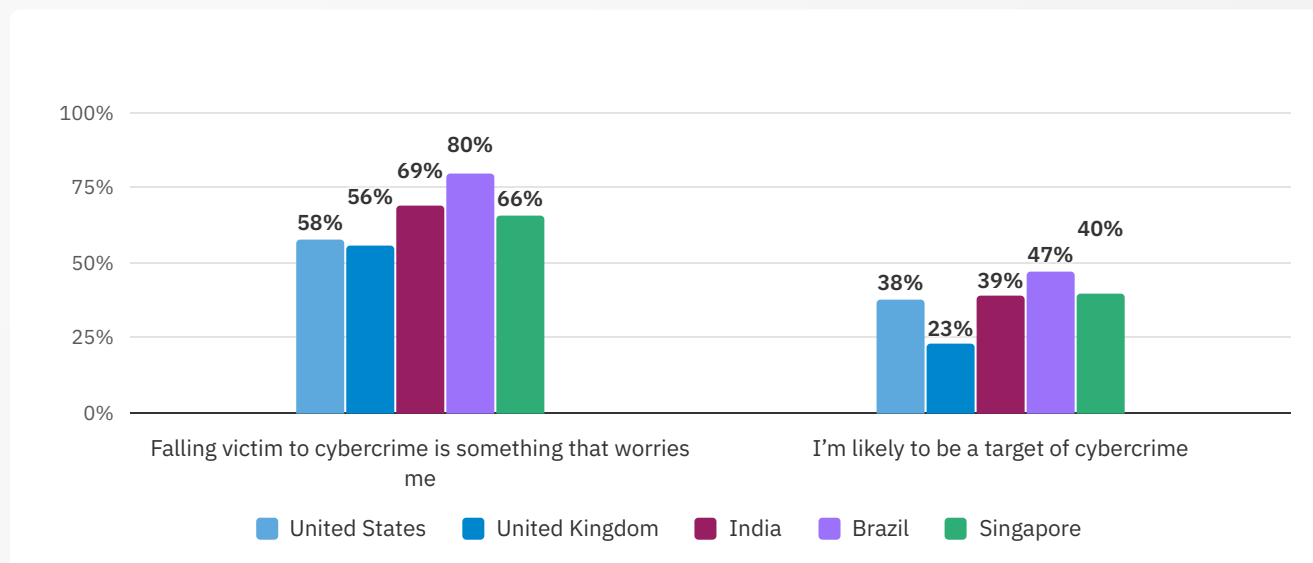
Figure 91. ‘I don’t see the point of trying to protect myself more as my information is already online.’ by country.



Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

General anxiety about falling victim to cybercrime was highest in Brazil (80%, down 4% from 2025), followed by India (69%, down 4% from 2025) and Singapore (66%), while the US (58%, down 3% from 2025) and the UK (56%, down 7% from 2025) reported the lowest worry (Figure 92). However, when asked if they personally felt like a likely target, numbers dropped across every nation ...though Brazil still recorded the highest percentages here (47%, down 5% from 2025) and the UK remained at the bottom (23%, down 6% from 2025).

Figure 92. Attitudes toward victimization, by country.

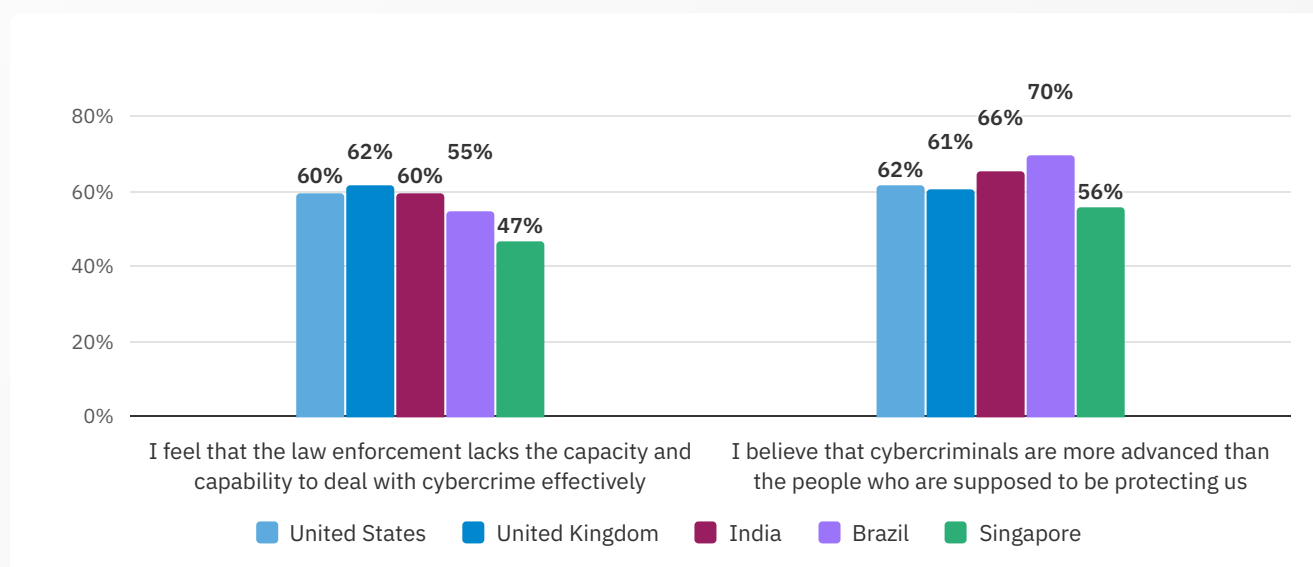


Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

The belief that law enforcement lacks the capacity to deal with cybercrime effectively was highest in the UK (62%, -1% from 2025), closely followed by the US and India (60% both, Figure 93). By contrast, under half of Singapore's respondents (47%) held this view.

The belief that cybercriminals are more advanced than the security professionals trying to stop them was highest in Brazil (70%, -2% from 2025), closely followed by India (66%, -5% from 2025). This belief was also lowest in Singapore, though still 56% expressed it.

Figure 93. Perceptions of cybercrime defense effectiveness, by country.



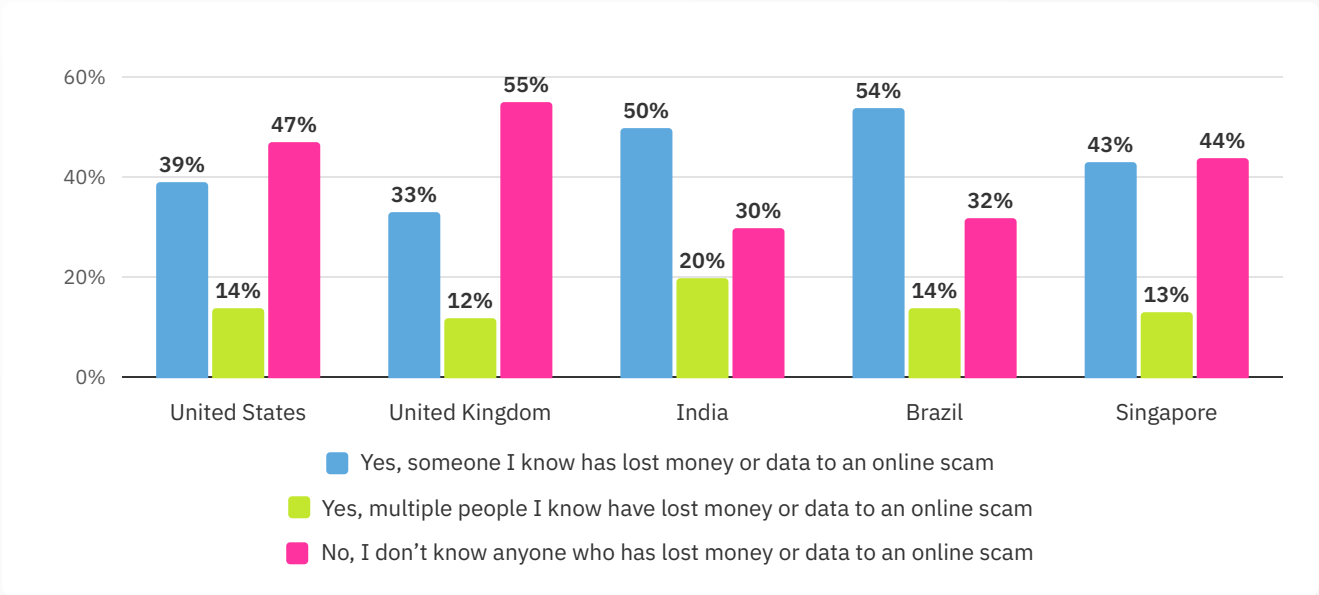
Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

Now, let's explore the differences between countries in victimization rates and experiences with deepfake attacks.

The data revealed notable differences in victimization across the participants' social circles (Figure 94). The majority of participants in India (70%, -3% from 2025) and Brazil (68%, -7% from 2025) reported knowing at least one person who had lost money or data in an online scam. India had the highest proportion of people who knew multiple scam victims (22%, -2% from 2025).

But even in other countries, over half of the participants knew at least one person who had lost money or data in an online scam (56% in Singapore and 53% in the USA). The only country where more than half of the participants reported not knowing anyone affected was the UK (55%, -1% from 2025).

Figure 94. ‘Has anyone you know been a victim of online scams where they have lost money or data?’ by country.

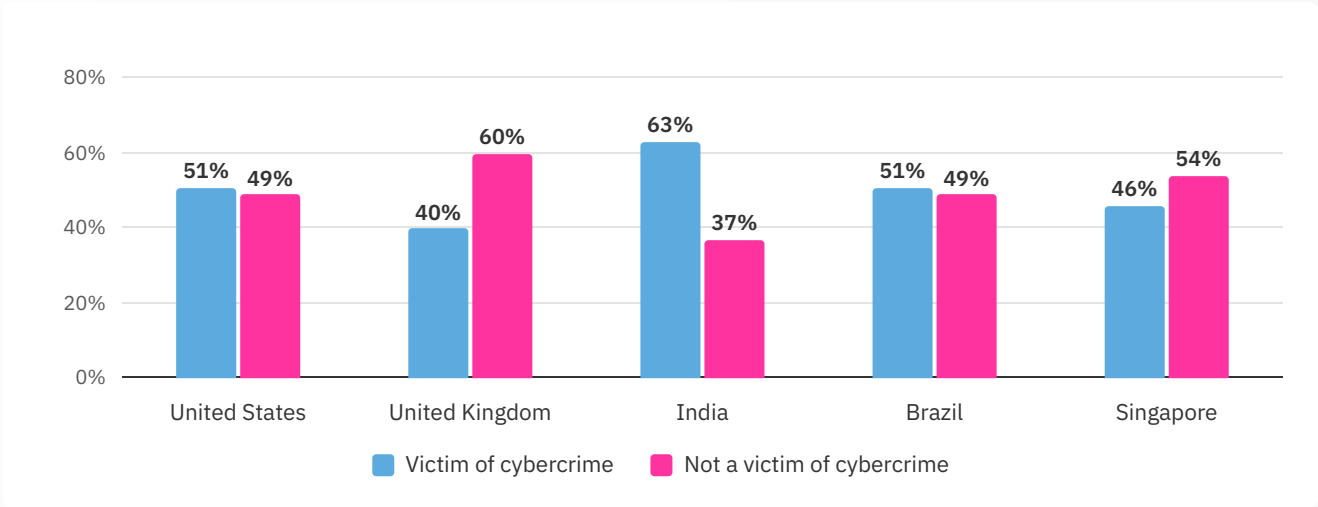


Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

At the individual level, the UK (40%, up 7% from 2025) recorded the lowest percentage of personal cybercrime victims (Figure 95), followed by Singapore (46%). These were the only two countries where under half of the participants had been personally victimized.

In both the US and Brazil, 51% of respondents reported falling victim to cybercrime (representing increases of 2% and 9%, respectively). India stood out as recording the highest overall personal victimization rate by a wide margin, standing at 63% (a 5% rise from 2025).

Figure 95. Victimization by country.



Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

Participants in India were the most likely to fall victim to almost every category of cybercrime we measured⁵⁰, except for identity theft, where the US had the highest share of victims (30%), followed by India (25%). Generally, the US followed India regarding high victimization rates for most scams, like phishing (22%) or online dating scams (25%), though Singapore recorded the second highest percentage for cryptocurrency fraud (25%), and Brazil came second for online marketplace scams (27%).

The UK recorded the lowest victimization rates for tech support scams (12%), crypto (12%), job (8%) and lottery/prize (8%) scams, and identity theft (13%). Brazil had the lowest rates of phishing (16%) and online dating scam victims (11%), and Singapore had the lowest share of delivery (14%) and online marketplace scam victims (13%).

The table below details how victims of each specific scam type were distributed across the five countries:

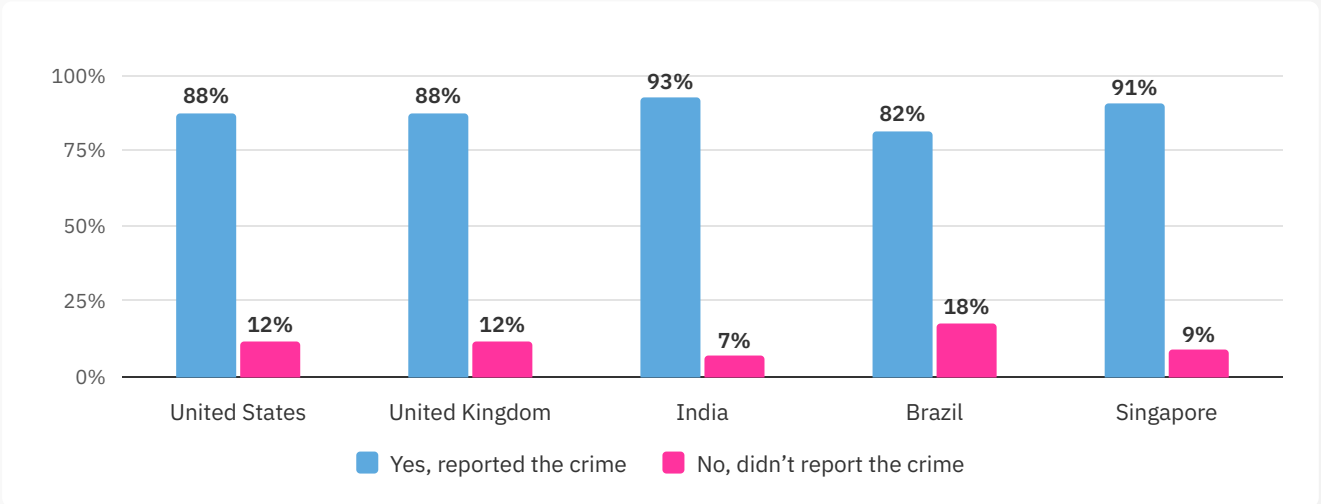
Types of scams	United States	United Kingdom	India	Brazil	Singapore
Phishing scam (n = 906)	22%	18%	25%	16%	19%
Online dating scam (n = 625)	25%	12%	31%	11%	21%
Identity theft (n = 667)	30%	13%	25%	14%	18%

50 Participants were provided with the ‘Other’ option to share cybercrime victimization experiences that were not covered in the nine existing categories. While the ‘Other’ option is included in the figures in the Main findings, we omitted it in Appendix B for simplification.

Types of scams	United States	United Kingdom	India	Brazil	Singapore
Cryptocurrency investment fraud (n = 549)	19%	12%	30%	14%	25%
Tech support scam (n = 528)	21%	12%	32%	17%	18%
Job scam (n = 697)	20%	8%	37%	16%	19%
Delivery scam (n = 636)	17%	15%	38%	16%	14%
Online marketplace scam (n = 686)	18%	14%	28%	27%	13%
Lottery/prize scam (n = 305)	17%	8%	52%	12%	11%

Across all countries, crime reporting rates among victims were consistently high (Figure 96). India led the way with 93% of victims reporting the incident, followed closely by Singapore at 91%. Brazil registered the lowest reporting rate among the five nations, though a solid 82% of victims there still reported the crime.

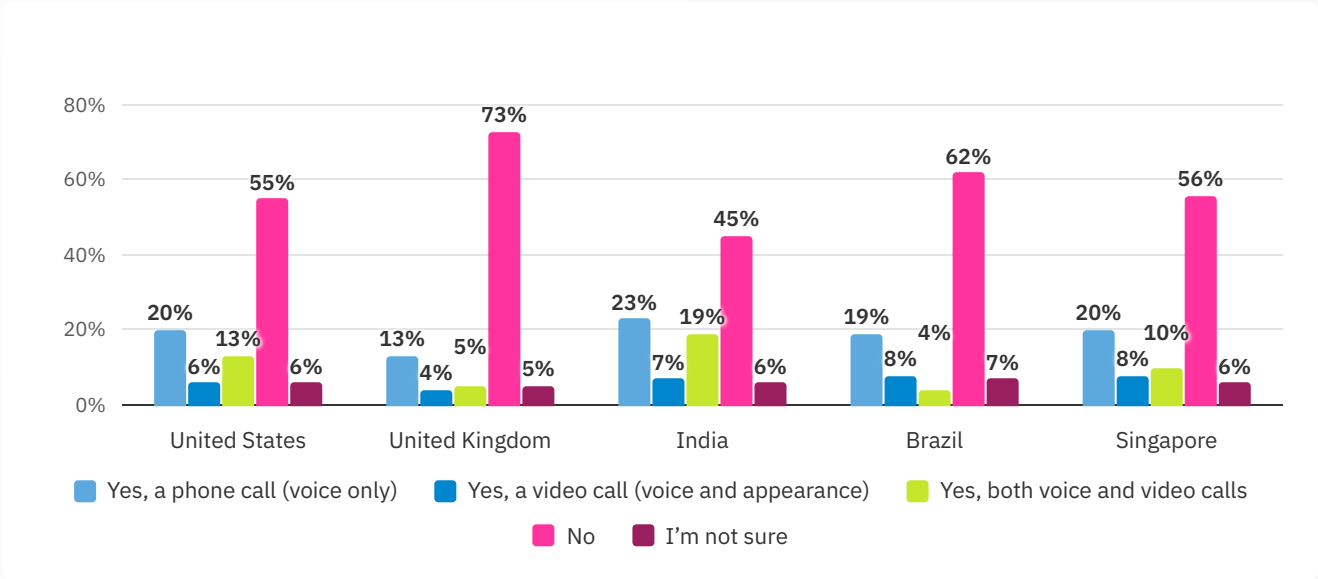
Figure 96. Crime reporting frequency, by country.



Base: US, UK, India, Brazil, Singapore. Total number of incidents (18+): 5,599 (without the ones described by participants in the 'Other' category).
Dates conducted: April 28, 2026 - May 19, 2026.

When it came to deepfakes, exposure varied dramatically (Figure 97). Nearly half of respondents in India (49%, down 4% from 2025) reported receiving a deepfake call, compared to 39% in the US (up 1% from 2025) and 38% in Singapore. Conversely, the vast majority of participants in the UK (73%, up 1% from 2025) and Brazil (62%, down 3% from 2025) stated they had never been targeted.

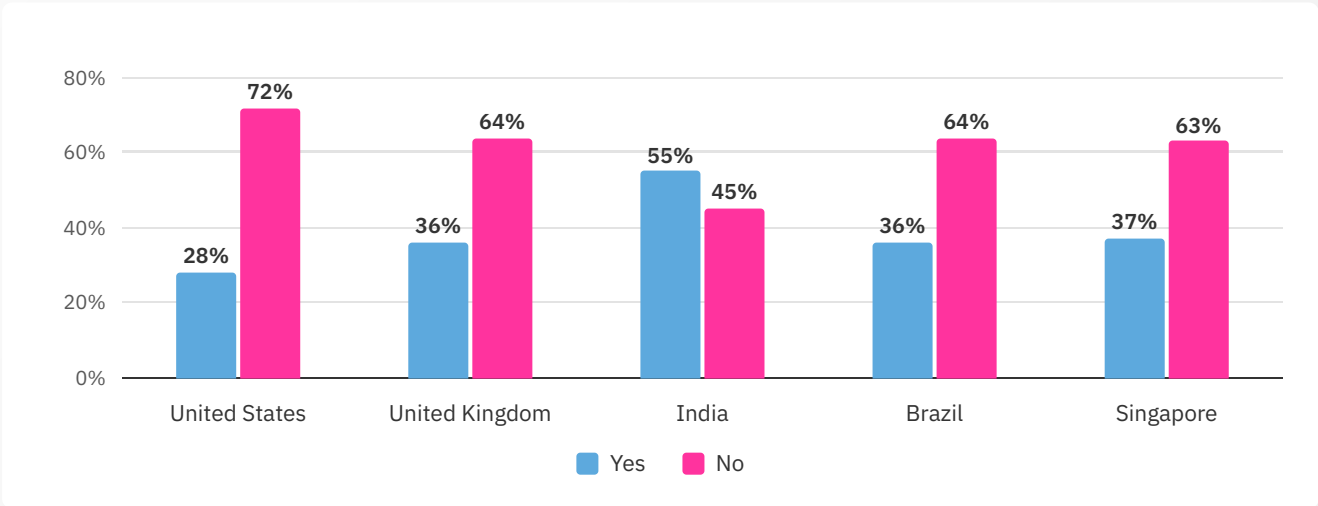
Figure 97. ‘Have you ever received a phone or video call where the caller’s voice or appearance exactly matched someone you know, but it turned out to be a scam?’ by country.



Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

But exposure doesn’t always mean loss (Figure 98). The highest percentage of participants who’ve lost money or data was in India (55%, +5% from 2025), and the lowest was in the USA, with 28% (-20% from 2025) ending up losing money or data as a result of a deepfake scam.

Figure 98. ‘Did you lose money or data as a result of the deepfake voice or video call you received?’ by country.



Base: US, UK, India, Brazil, Singapore. Total number of participants: 1,790 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.



Summary cheat-sheet

COUNTRY COMPARISONS: CYBERCRIME VICTIMIZATION

Fatalistic beliefs about inevitable money or data loss were highest in India (50% and 54%) and lowest in the UK (20% and 24%). India also led in resignation about self-protection (51% saw no point in trying harder since their information is already out there), whereas only 23% of UK participants shared that feeling.

Cybercrime worry and perceived personal risk peaked in Brazil (80% worried, 47% felt like a target) and hit their lowest levels in the UK (56% worried, 23% felt like a target).

Trust in cybersecurity defenses was weakest in the UK (62% doubted law enforcement capabilities) and Brazil (70% felt criminals outpace defenders). Singapore expressed the most confidence in defenses, though skepticism remained high (47% and 56%).

Social circle impacts: India (70%) and Brazil (68%) had the highest percentage of people who knew a scam victim, while 55% of UK respondents didn't know anyone who had fallen victim.

Personal victimization was highest in India (63%). The UK (40%) and Singapore (46%) were the only two countries where less than half of participants were victims.

Scam varieties: India led in almost every scam category (e.g., 52% for lottery scams), but the US led in identity theft (30%), Singapore led in crypto fraud (25%), and Brazil led in marketplace scams (27%). Reporting rates were highest in India (93%) and lowest in Brazil (82%).

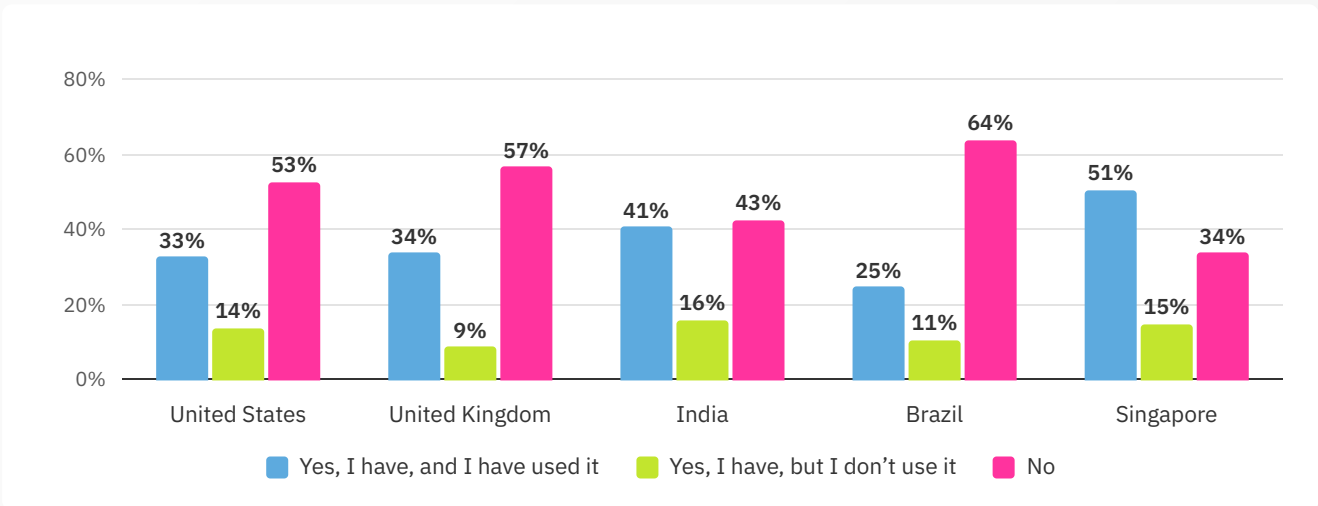
Deepfake attacks hit India hardest (49% targeted, 55% lost money/data). While 39% of Americans were targeted by deepfakes, the US achieved the lowest rate of actual money or data loss (28%).

Cybersecurity training

Access to cybersecurity training varied notably by country (Figure 99). Most participants from Brazil (64%, +1% from 2025) reported having no access to training, followed by the UK (57%, -3% from 2025) and the US (53%, +1% from 2025) where access rates were slightly higher, but still over half were without access. In contrast, the majority in Singapore reported having access to training (66%).

Among those with access, Singapore also had the highest share who had actually used it (51%), followed by India (41%, -5% from 2025). Brazil had the lowest usage rate (25%, -2% from 2025).

Figure 99. ‘Do you have access to cybersecurity training (e.g., at work, school, library, or other public location)?’ by country.

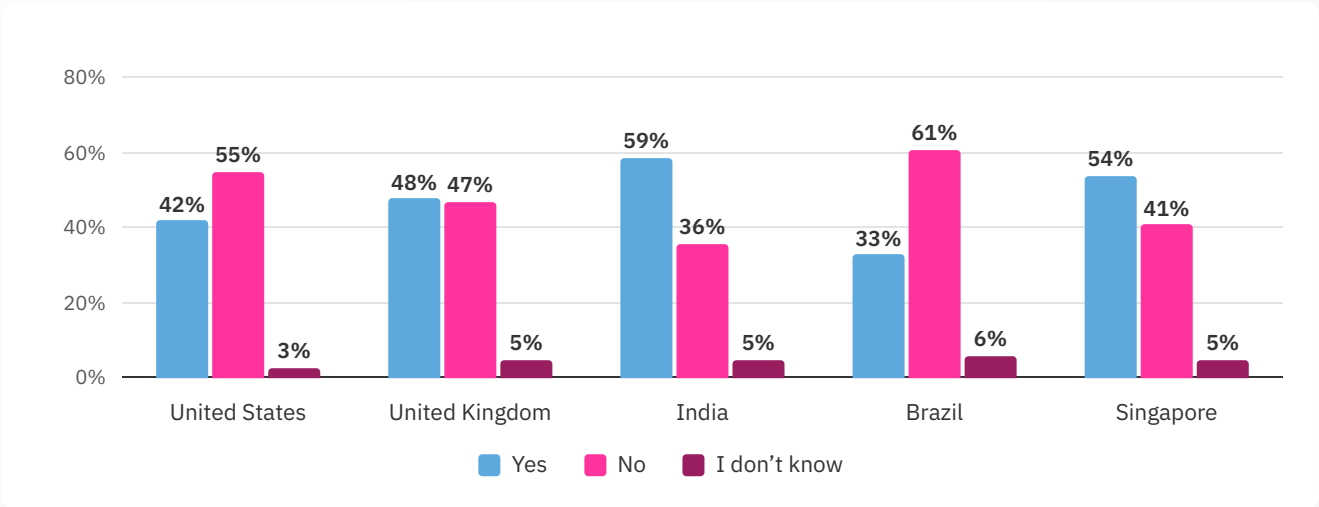


Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

Whether cybersecurity training is mandatory at work also varied by country (Figure 100). India had the highest proportion of employed respondents required to complete workplace training (59%), followed closely by Singapore (54%). Brazil had the lowest rate of mandatory workplace training (33%), mirroring its lower training access and usage figures, as mentioned above.

The US is also worth highlighting here: over half of employed American participants (55%) aren't required to complete mandatory cybersecurity training at their workplace.

Figure 100. ‘Are you required to complete mandatory cybersecurity training at your workplace?’ by country.



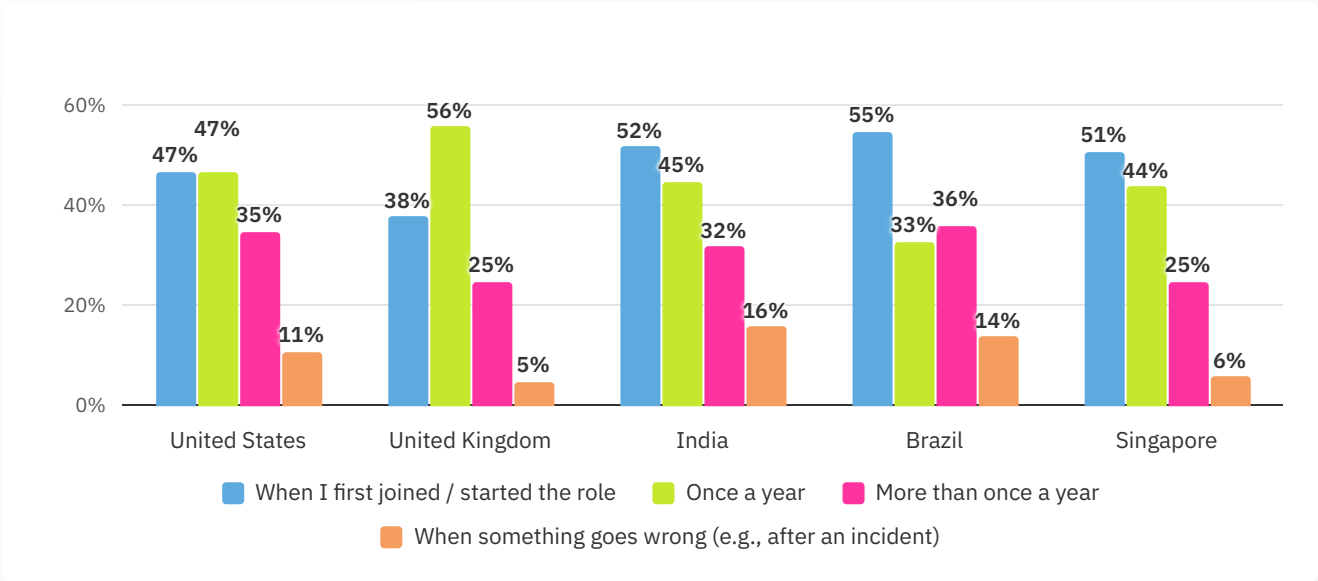
Base: US, UK, India, Brazil, Singapore. Total number of participants: 3,269 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

Among employed participants required to complete training, the UK stood out for relying far more heavily on an annual schedule: 56% reported training once a year, the highest of any country (Figure 101). The UK also had the lowest share of those having to complete training when joining their workplace or starting their role (38%), more than once a year (25%) or when something goes wrong (5%).

In the US, mandatory training when starting a new role and annual training were equally common, tying as the most popular schedules at 47% each.

Having to complete mandatory cybersecurity training when joining a new workplace or starting a new role was the most common practice in every other country, ranging from 51% in Singapore to 55% in Brazil.

Figure 101. ‘When are you required to complete training?’ by country.



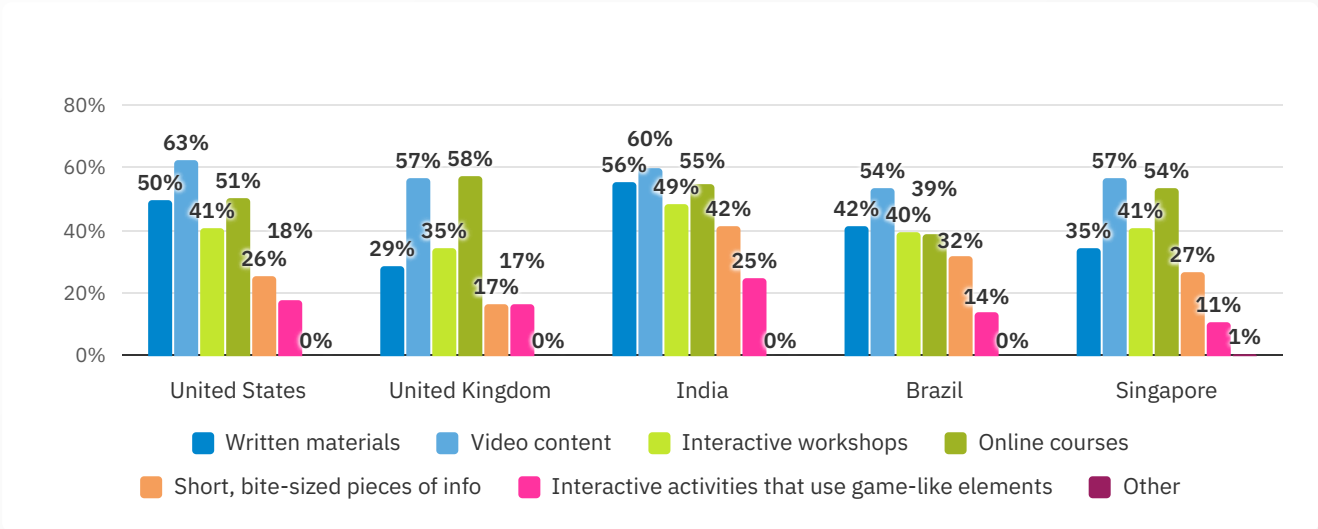
Base: US, UK, India, Brazil, Singapore. Total number of participants: 1,543 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

Video content was the most common training format provided by organizations across all countries (Figure 102), ranging from 54% (-1% from 2025) in Brazil to 63% (+9% from 2025) in the US, except in the UK, where online courses were slightly more common (58% vs 57%, both up 1% from 2025).

Written training materials were far more prevalent in India (56%, up 7% from 2025) and the US (50%, up 8% from 2025) than in Singapore (35%) or the UK (29%, down 3% from 2025).

India stood out for its overall diversity of training methods, reporting the highest global usage across interactive workshops (49%, up 2% from 2025), quick bite-sized pieces of info (42% – more than double the UK's 17%), and gamified learning activities (25%, up 4% from 2025).

Figure 102. Cybersecurity training formats used by organizations, by country.

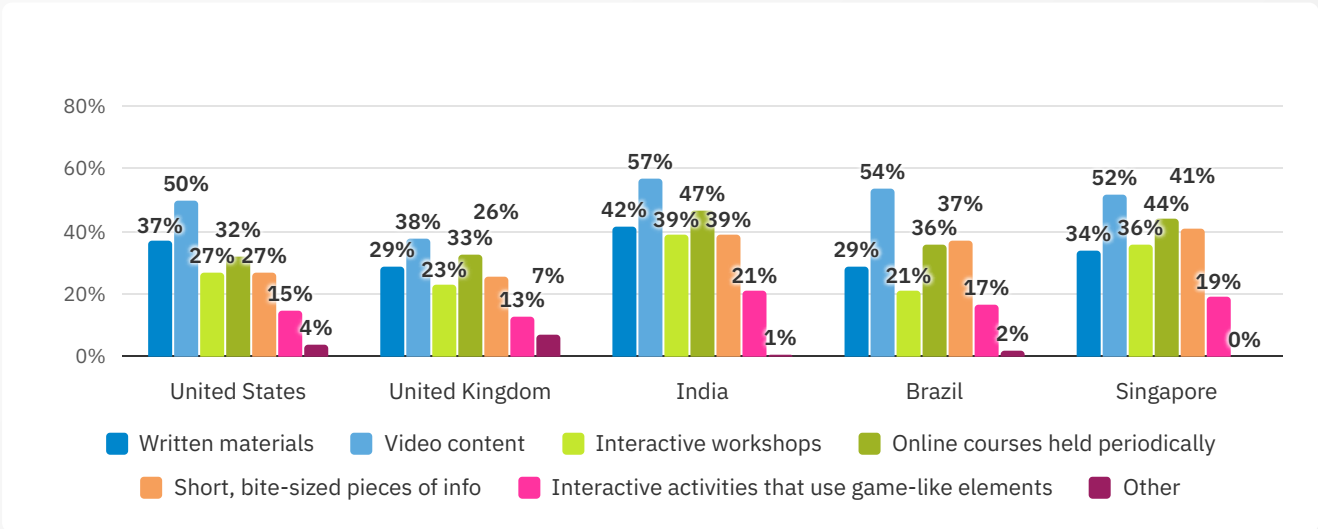


Base: US, UK, India, Brazil, Singapore. Total number of participants: 1,543 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

When it comes to preferred formats (Figure 103), video content once again came out on top across most countries. Preference for video training was highest in India (57%, +1% from 2025), closely followed by Brazil (54%, same as in 2025), Singapore (52%) and the USA (50%, +11% from 2025). While video remained the most popular format in the UK, only 38% of UK respondents selected it (down 1% from 2025).

Written content was the second most preferred format in the US only (37%, +7% from 2025). In India (47%, +3% from 2025), Singapore (44%) and the UK (33%, -2% from 2025) periodic online courses came second. Brazil stood out as the only country where preference for short bite-sized pieces of information (37%, +6% from 2025) was slightly more preferred than online courses (36%, +1% from 2025).

Figure 103. ‘What format do you prefer to consume cybersecurity training information?’ by country.



Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.



Summary cheat-sheet

COUNTRY COMPARISONS: CYBERSECURITY TRAINING

Training access was highest in Singapore (66%) and lowest in Brazil (36%), while over half of UK (57%) and US (53%) respondents lacked access. Singapore also led in actual training usage (51%), whereas Brazil recorded the lowest usage rate (25%).

Mandatory workplace training was most widespread in India (59%) and least common in Brazil (33%). In the US, 55% of working respondents had no mandatory workplace training.

Training frequency: The UK (56%) relied on fixed annual training much more than any other nation, compared to 33% in Brazil to 47% in the US. The UK also had the lowest rates for onboarding training (38%), training more than once a year (25%), or post-incident training (5%). Onboarding training was the most common practice in Singapore (51%), India (52%), and Brazil (55%), while the US split evenly between onboarding and annual practices (47% each).

Provided formats: Video was the primary format used everywhere except the UK, where online courses slightly edged it out (58% vs 57%). India led in adopting diverse formats like bite-sized nudges (42%), workshops (49%), and gamified activities (25%).

Preferred formats: Video was the favorite learning format across all five nations, though UK preference was much softer (38% vs 50%–57% elsewhere). Written content ranked second in the US (37%). Elsewhere, online courses ranked second, except in Brazil, where short, bite-sized pieces of information (37%) narrowly outranked online courses (36%).

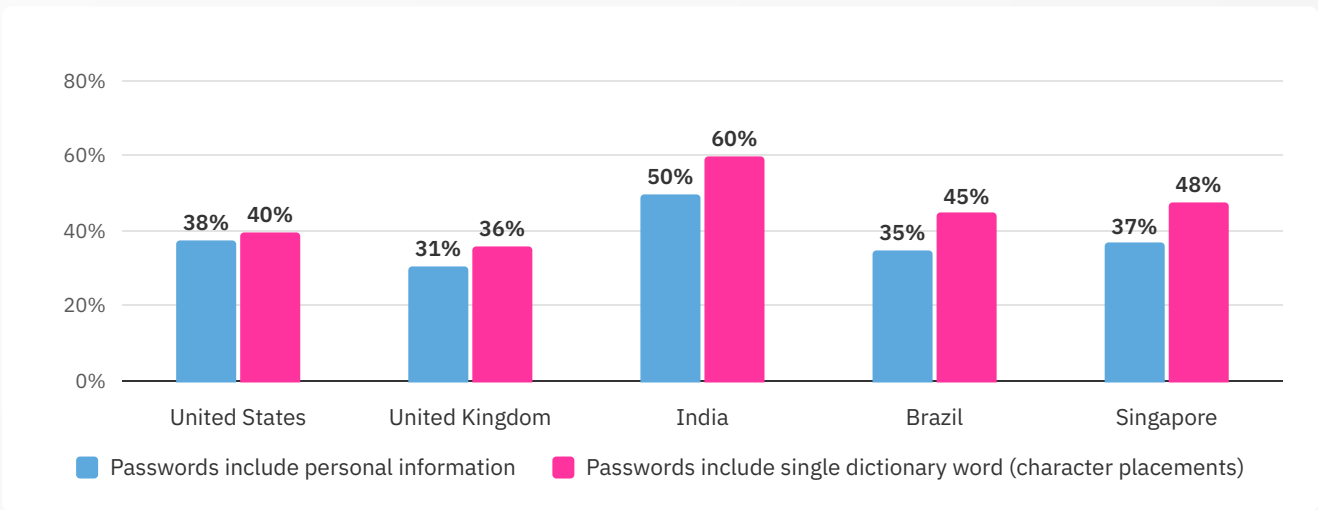
Cybersecurity behaviors

When looking at differences between countries in password creation techniques, India was an outlier, with by far the largest proportions of participants including personal information (50%, -3% from 2025) or a single dictionary word (60%, +1% from 2025) in their passwords (Figure 104).

By contrast, respondents from the UK were less likely to follow risky password creation practices, with 31% (-1% from 2025) including personal information and 36% (-1% from 2025) including a single dictionary word.

The remaining countries fell between these two. Across every single nation surveyed, relying on a single dictionary word was found to be more common than weaving in personal information, though that gap was narrowest among participants in the US (40% using a dictionary word versus 38% using personal info, with both metrics dropping 3% from last year).

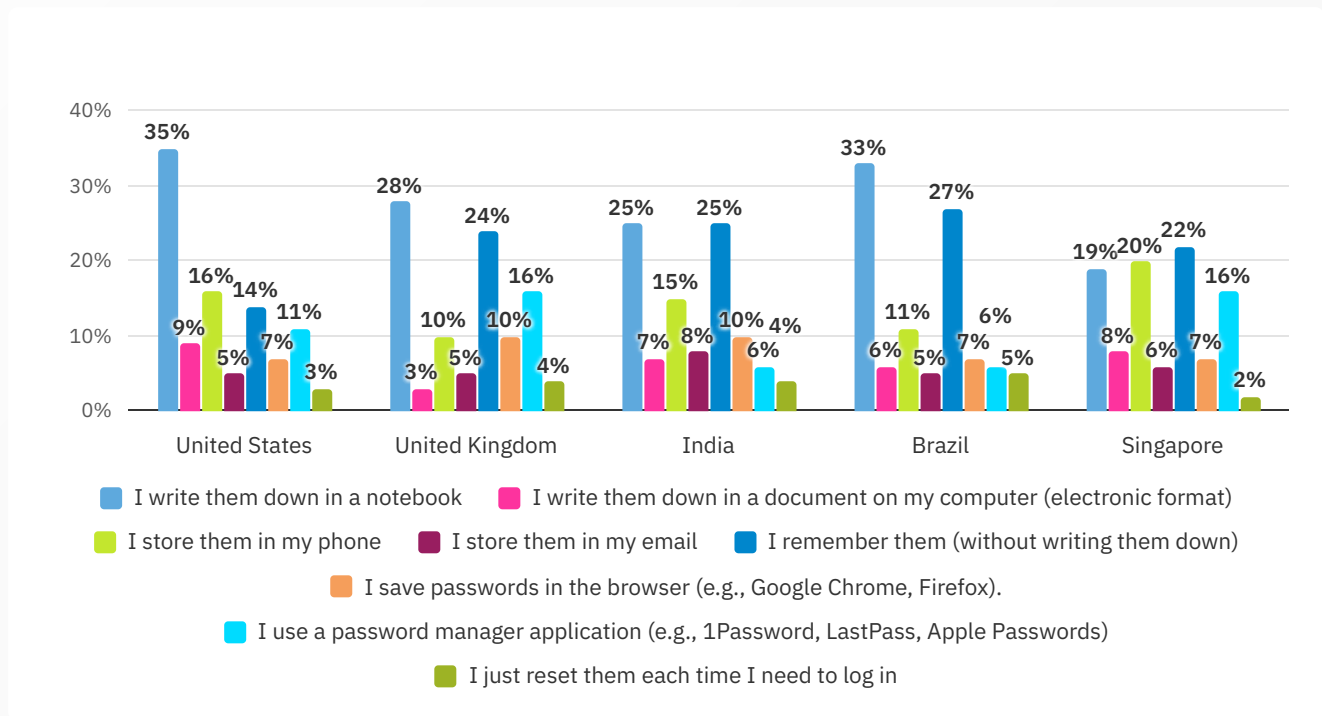
Figure 104. Password creation techniques used by participants, by country.



Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

Preferred password management and storage strategies also varied by country (Figure 105). Writing passwords down in a notebook was the most common method in the US (35%, +5% from 2025), Brazil (33%, -6% from 2025), and the UK (28%, +2% from 2025), while participants in India were about as likely to write them down (25%, same as in 2025) as to rely on memory alone (25%, +1% from 2025). In Singapore, however, relying on memory was the most common method (22%), closely followed by storing passwords on a phone (20%), then writing them in a notebook (19%).

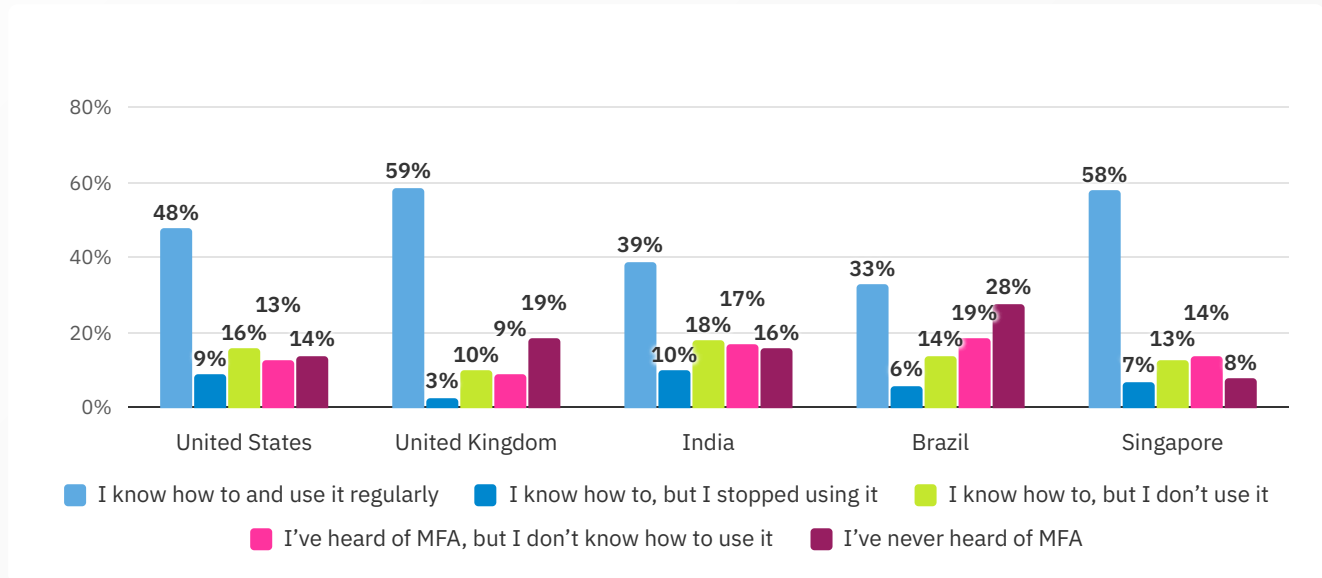
Reliance on built-in browser tools or dedicated password manager apps was highest in the UK (26%, -1% from 2025) and Singapore (23%), and lowest in Brazil (13%, +2% from 2025).

Figure 105. Preferred password management strategies, by country.

Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

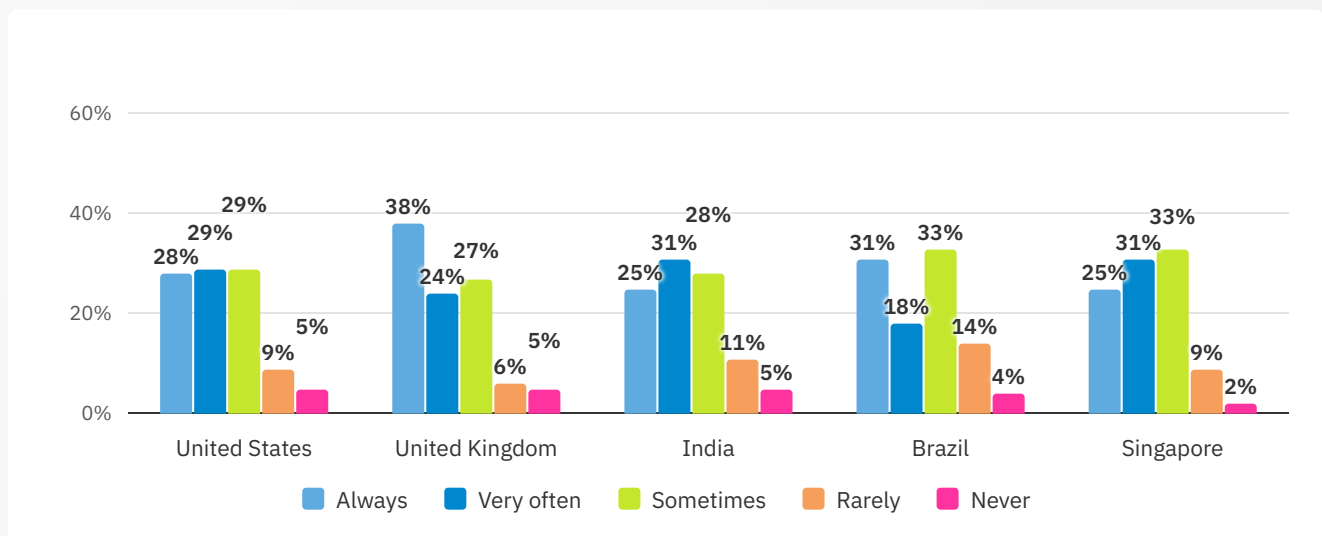
Regular, routine MFA use was highest in the UK (59%, +5% from 2025) and Singapore (58%), followed by the US (48%, Figure 106). It was lowest in Brazil (33%, -2% from 2025), which also had by far the highest share of participants who had never heard of MFA (28%, same as in 2025).

India was found to be a notable exception once again: it logged the highest proportion of respondents who know how to set up and use MFA but choose not to (18%, same as 2025) or have abandoned using it altogether (10%, up 1% from 2025). The US followed right behind India on this behavior, with 16% of American respondents skipping MFA (down 1% from 2025) and 9% giving up on it (up 2% from 2025), despite knowing how the technology works.

Figure 106. ‘Do you know how to use multi-factor authentication (MFA)?’ by country.

Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

When examining how routinely people update their devices (Figure 107), the UK took the crown for having the highest percentage of participants who *always* install updates promptly when alerted (38%, +4% from 2025), followed by Brazil (31%, -4% from 2025), and the US (28%, -4% from 2025). Brazil had the highest proportion of those who rarely or never update (18%, +2% from 2025), followed by India (16%, -1% from 2025), and the US (14%, -4% from 2025).

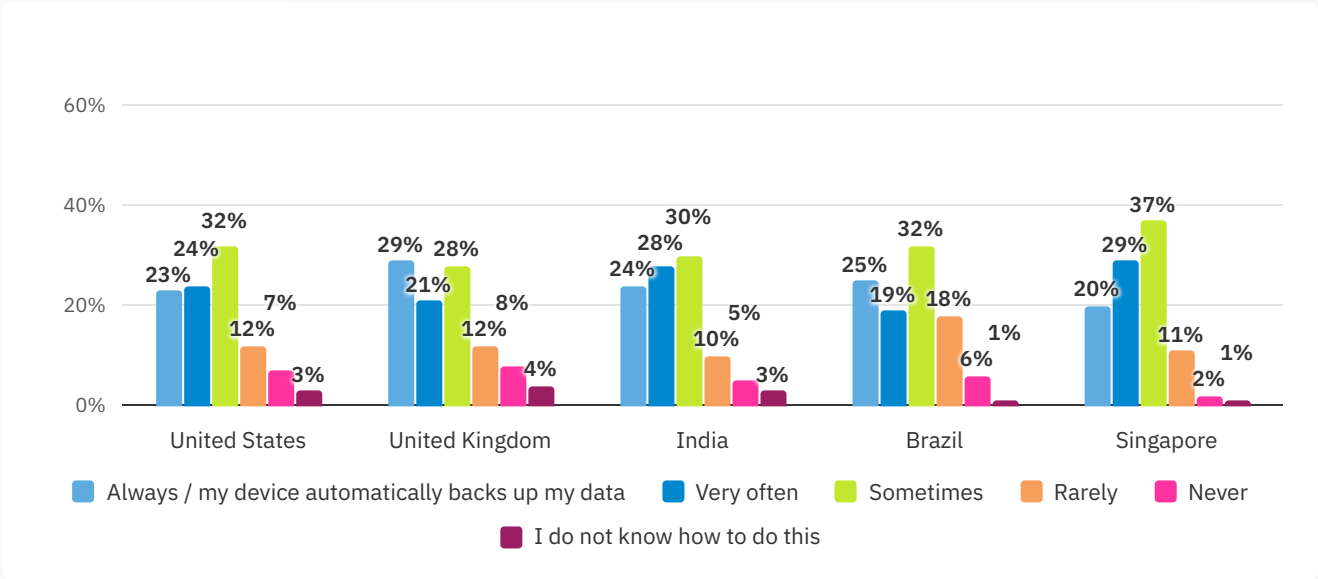
Figure 107. ‘How often do you install the latest software or application updates to your devices when notified that they are available?’ by country.

Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

Frequency of data backups also swung noticeably across different countries (Figure 108). India had the highest percentage who backed up their data always or very often (52%, -5% from 2025), followed by the UK (50%, +1% from 2025) and Singapore (49%). In comparison, Brazil had the lowest percentage who backed up their data always or very often (44%, -3% from 2025) and also the highest share who rarely did so (18%, +1% from 2025).

Completely skipping data backups or not knowing how to perform them was relatively rare across all five nations, though it was somewhat more prevalent in the UK (12% combined) than in Singapore, which had the absolute lowest figure at just 3%.

Figure 108. ‘How often do you back up your most important data?’ by country.



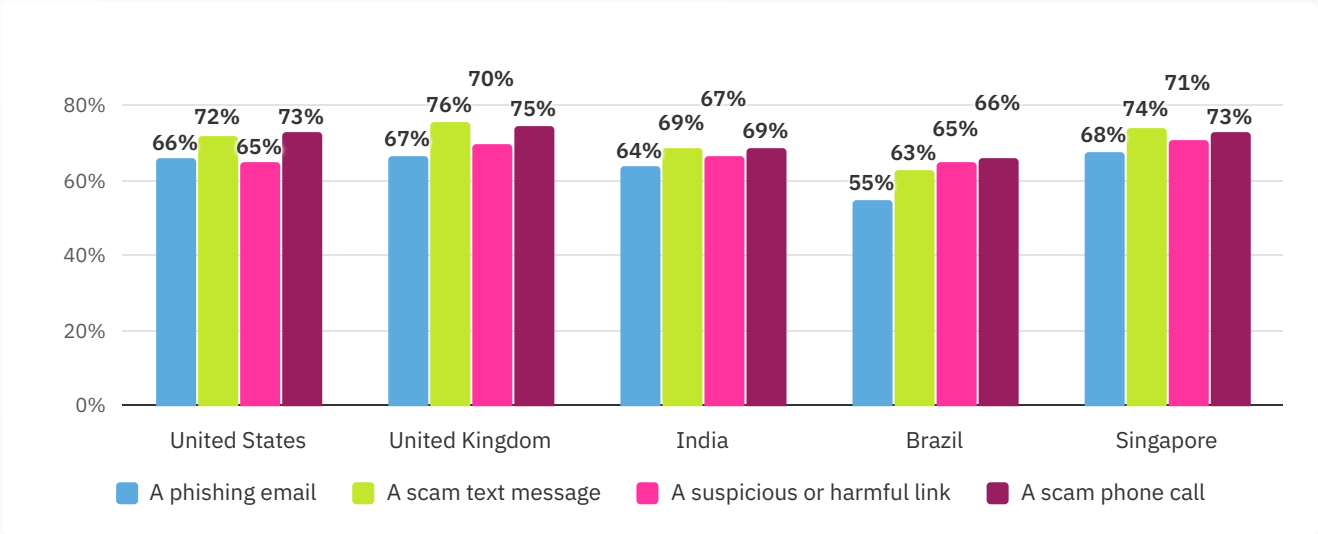
Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

Let’s break down how confident participants feel when it comes to spotting different forms of phishing attacks across each country (Figure 109). Across almost every nation, confidence in identifying phishing emails was the lowest among the four scam formats evaluated, ranging from a low of 55% in Brazil to a high of 68% in Singapore. The US was the sole exception here, where confidence in spotting suspicious links was the lowest overall (65%).

Participants had the highest confidence in recognizing scam phone calls in Brazil (66%), in the USA (73%), where confidence in recognizing fake text messages was very similar (72%), and in India, where confidence in recognizing both types of phishing content was the same (69% both). In the UK and Singapore, confidence in scam text recognition was slightly higher (76% and 74%) than for fraudulent audio calls (75% and 73%).

Looking at the big picture, Brazilian respondents reported the lowest confidence in recognizing all four types of phishing scams, while participants in the UK and Singapore posted the highest confidence overall.

Figure 109. ‘How confident are you in your ability to identify each of the following?’ by country.



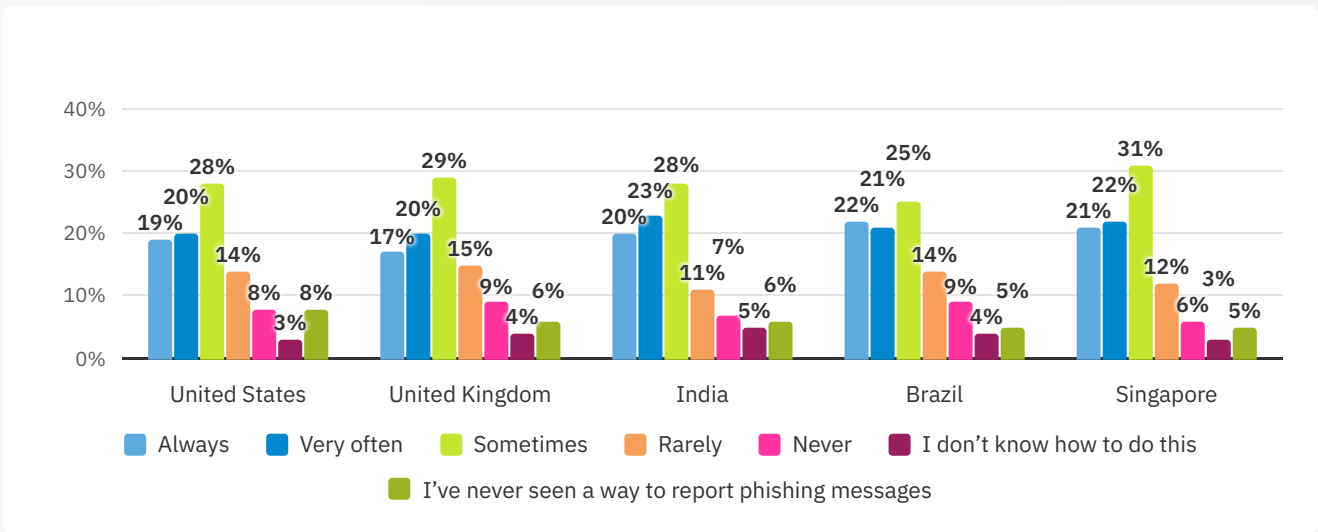
Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

Reporting behavior (Figure 110) deviated from the behavioral trends seen throughout the rest of this section. The UK, which led on regular software updates and MFA use, had the lowest combined share who ‘always’ or ‘very often’ report phishing messages (37%), and the highest share who ‘rarely’ or ‘never’ do so (24%).

India, Brazil, and Singapore had the highest regular reporting rates, with 43% in all three countries reporting phishing messages ‘always’ or ‘very often’.

The US stood out for a different reason entirely: it had the highest share who said they'd never seen a way to report phishing messages (8%), compared to 5 to 6% in all other countries.

Figure 110. ‘How often do you report phishing messages (e.g., email or social media) by using the ‘spam’ or ‘report phishing’ button?’ by country.



Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.



Summary cheat-sheet

COUNTRY COMPARISONS: CYBERSECURITY BEHAVIORS

India was the biggest outlier in password creation, relying far more on weak practices like using personal details (50%) or single dictionary words (60%). The UK recorded the lowest percentage using these risky methods, with 31% using personal info and 36% using dictionary words.

Password management styles varied widely: Jotting passwords down in notebooks was the top method in the US (35%), Brazil (33%), and the UK (28%). India split evenly between notebooks (25%) and relying on memory (25%). Memory was #1 in Singapore (22%), followed by phone storage (20%), then writing them in a notebook (19%). Password manager apps/browser tools were most popular in the UK (26%) and Singapore (23%), but lowest in Brazil (13%).

MFA adoption peaked in the UK (59%) and Singapore (58%), dropping to 33% in Brazil, where 28% had never even heard of it. Only 8% had never heard of it or its magical ways in Singapore – they're clued up. Regular use in the US (48%) and India (39%) fell in between. India had the highest rate of people who know how to use MFA but choose not to or stopped (28% combined).

Software updates: The UK led on installing updates immediately when prompted (38%), well ahead of all other nations (25% in India – 31% in Brazil). Brazil recorded the highest share of people who rarely or never update devices (18%).

Data backups: India led in regular backups (52% always/very often), followed by the UK (50%) and Singapore (49%). Participants in Brazil had the lowest regular backups (44%) and highest rare backups (18%).

Confidence in recognizing phishing attempts was lowest in Brazil and highest in the UK and Singapore. Email phishing was the hardest type to spot almost everywhere (55% in Brazil – 68% in Singapore confidence), except the US, where spotting suspicious links was the lowest (65%).

Reporting phishing: The UK had the lowest regular reporting rate (37%) and highest rate of those who said they 'never' or 'rarely' report phishing (24%). India, Brazil, and Singapore led regular reporting at 43% each. The US had the highest share of people who never noticed a reporting tool option (8%).

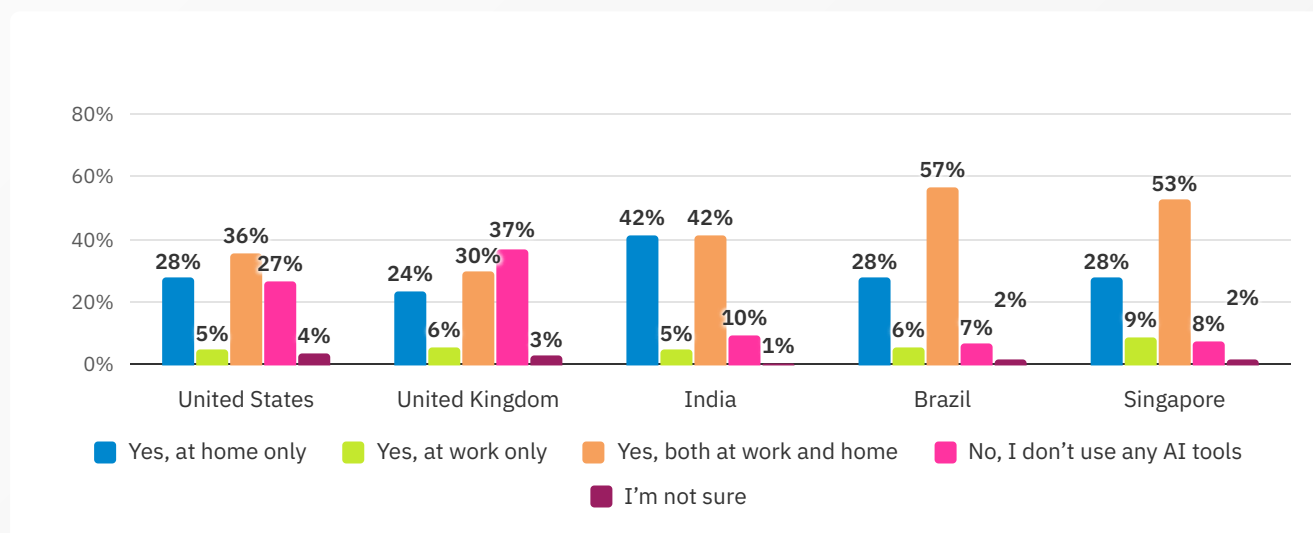
AI

Let's dive into international variations regarding artificial intelligence – looking at adoption rates, sharing sensitive data with AI platforms, confidence in spotting AI-generated content, and general attitudes toward AI technologies.

AI tool adoption varied sharply by country (Figure 111). Brazil (91%), Singapore (90%), and India (89%) reported the highest overall use of AI tools at home, work, and both. In comparison, only 69% in the US and just 60% in the UK used AI tools.

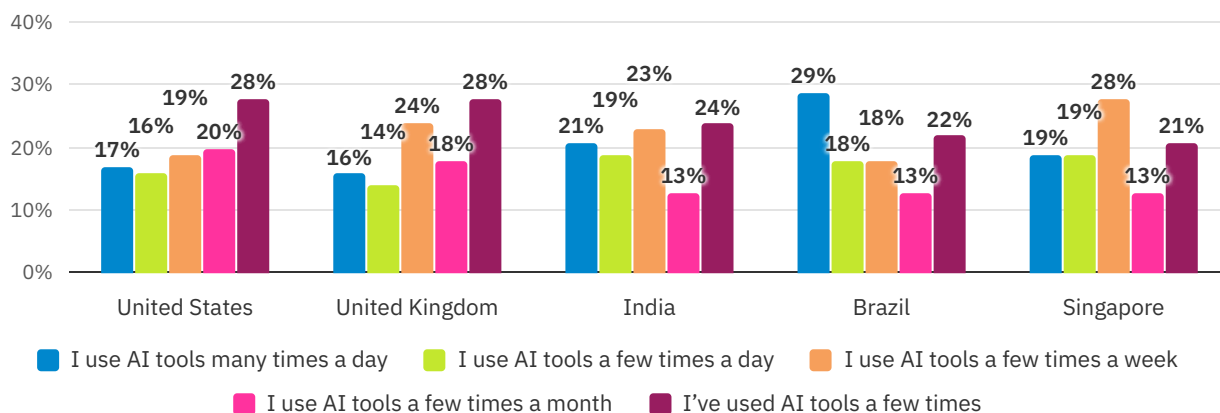
Using AI tools at work was highest in Brazil (63%) and Singapore (62%), and again lowest in the US (41%) and the UK (36%).

Figure 111. ‘Do you use any AI tools at home or at work?’ by country.



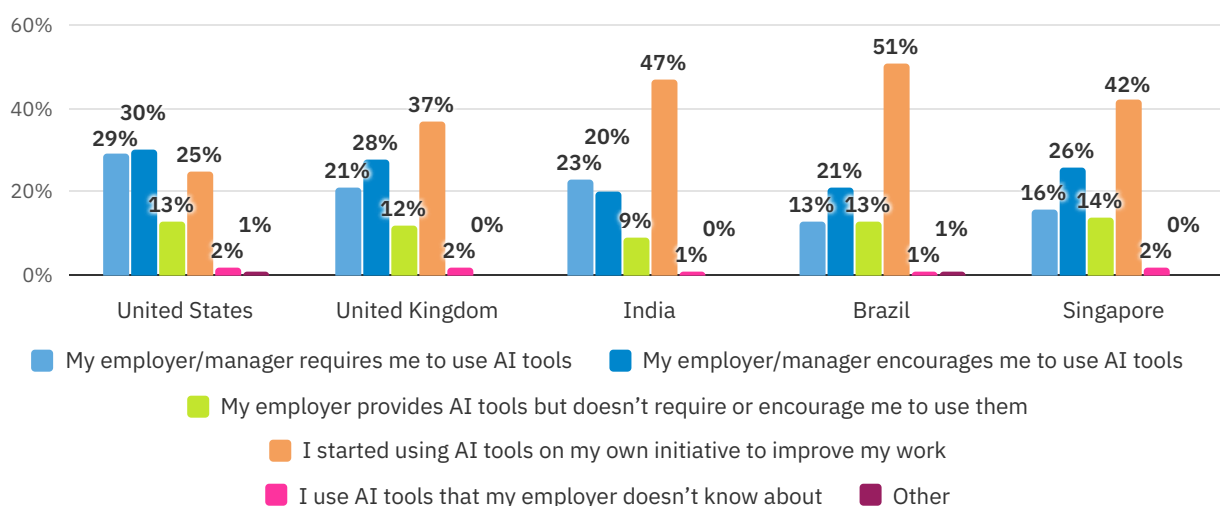
Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

Frequency of AI tool use among adopters also varied by country (Figure 112). Combining daily use (a few times a day or many times a day), Brazil reported the highest rate at 47%, driven largely by the highest proportion of any country using AI tools many times a day (29%). Singapore (38%) and India (40%) also reported higher combined daily use than the US (33%) or UK (30%). The USA and UK also had the highest percentage of those who've only tried AI a few times (28% in both).

Figure 112. ‘How often do you use AI tools?’ by country.

Base: US, UK, India, Brazil, Singapore. Total number of participants: 3,981 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

How people started using AI tools at work also varied notably by country (Figure 113). Taking personal initiative was the most common way participants adopted AI at work in Brazil (51%) and India (47%). In the US and UK, it was far more common for AI use to be employer-driven: 59% in the US and 49% in the UK started using AI at work because their employer required or encouraged them to do so. In Singapore, employee- and employer-driven AI adoption was equally common (both 42%).

Figure 113. ‘How did you start using AI tools for work?’ by country.

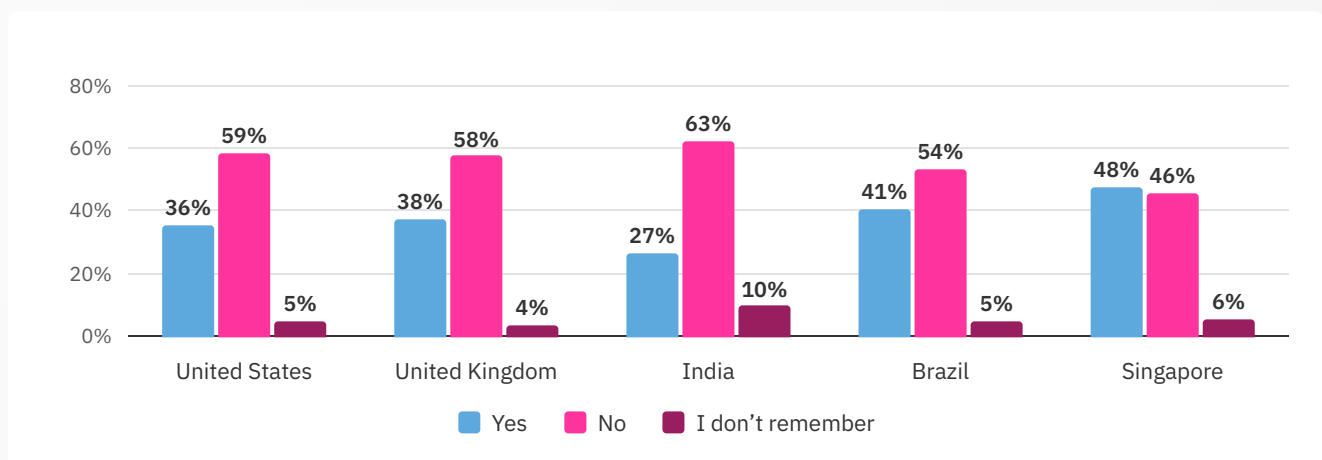
Base: US, UK, India, Brazil, Singapore. Total number of participants: 2,481 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

APPENDIX B: COUNTRY COMPARISONS

When it comes to receiving formal training on the cybersecurity and privacy risks associated with AI (Figure 114), Singapore topped the charts with 48% having received training, followed by Brazil at 41%. In contrast, only 27% in India had received AI risk training, despite India recording one of the highest overall AI adoption rates in the entire survey. India also had the highest share of respondents who simply couldn't recall whether they had taken training or not (10%).

Training numbers weren't particularly impressive in Western countries either, with only 36% in the US and 38% in the UK saying they'd received *any* formal training on AI risks.

Figure 114. 'Have you received any training about the security and privacy risks of AI tools?' by country.

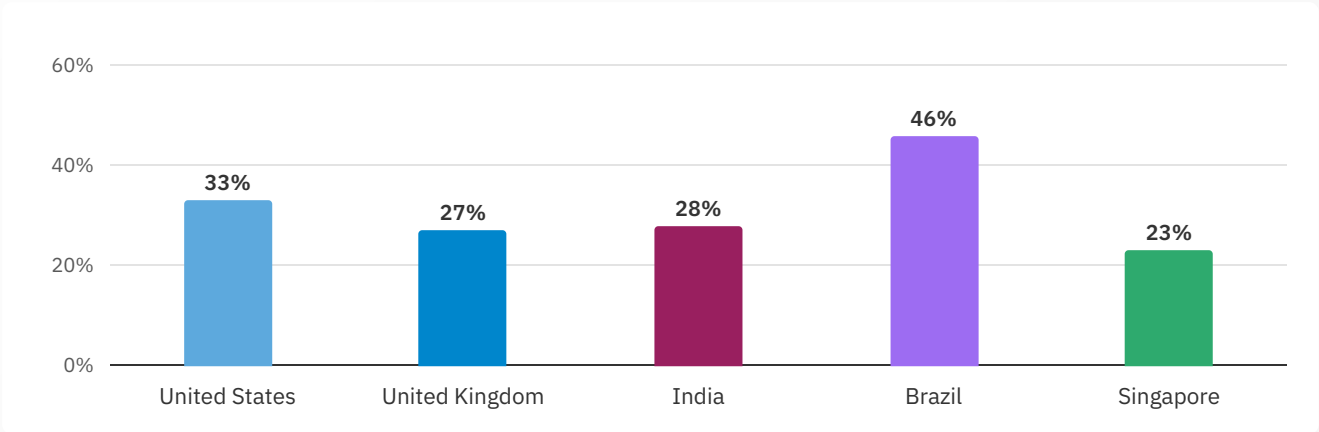


Base: US, UK, India, Brazil, Singapore. Total number of participants: 3,981 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

Sharing confidential or sensitive work information with AI tools without an employer's knowledge was most common in Brazil at 46% ...nearly double the rate recorded in Singapore (23%), which had the lowest rate of unauthorized sharing (Figure 115). The US (33%), India (28%), and the UK (27%) settled into the middle ground.

Interestingly, the highest AI training was reported in Singapore (48%), which is also where the smallest proportion of people shared sensitive info (23%). Brazil reported higher training rates than the remaining countries (41%), yet it still had by far the largest percentage of those sharing info.

Figure 115. ‘Have you ever shared sensitive work information with AI tools without your employer’s knowledge?’ by country.

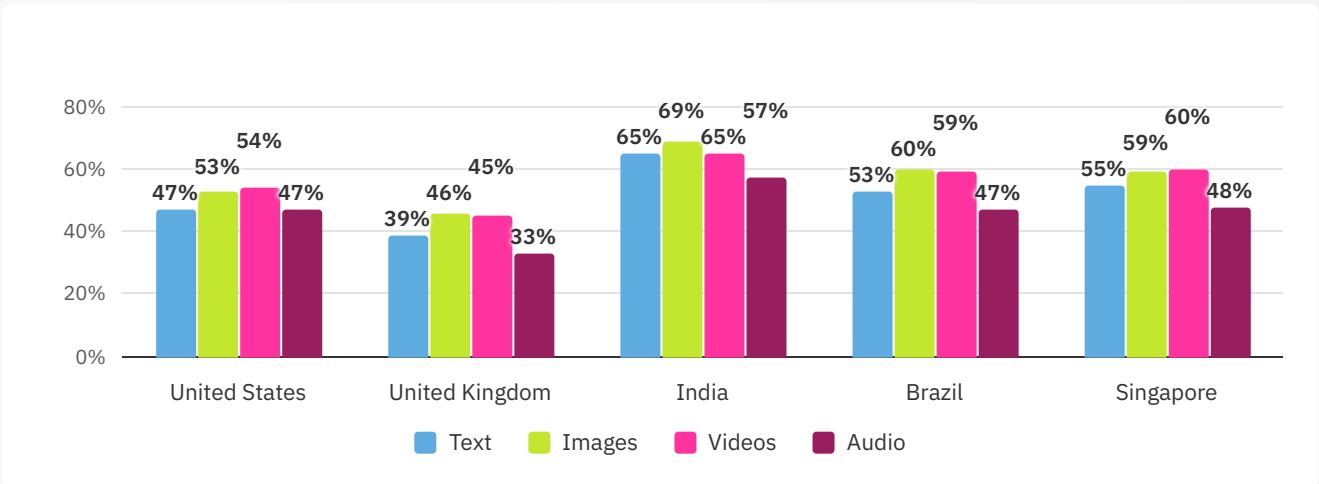


Base: US, UK, India, Brazil, Singapore. Total number of participants: 2,481 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

Confidence in recognizing AI-generated content also varied by content type as well as by country (Figure 116). Confidence in recognizing AI-generated audio, such as cloned voices, was the lowest of the four content types in every country, except the US, where it tied with text (47% each), ranging from 33% in the UK to 57% in India.

India recorded the highest confidence in spotting all four types of AI-generated content (ranging from 57% for audio up to 69% for images). Conversely, confidence was lowest in the UK (ranging from 33% for audio to 46% for images), followed by the US (ranging from 47% for text and audio up to 54% for videos).

Figure 116. ‘How confident are you in your ability to recognize AI-generated content?’ by country.

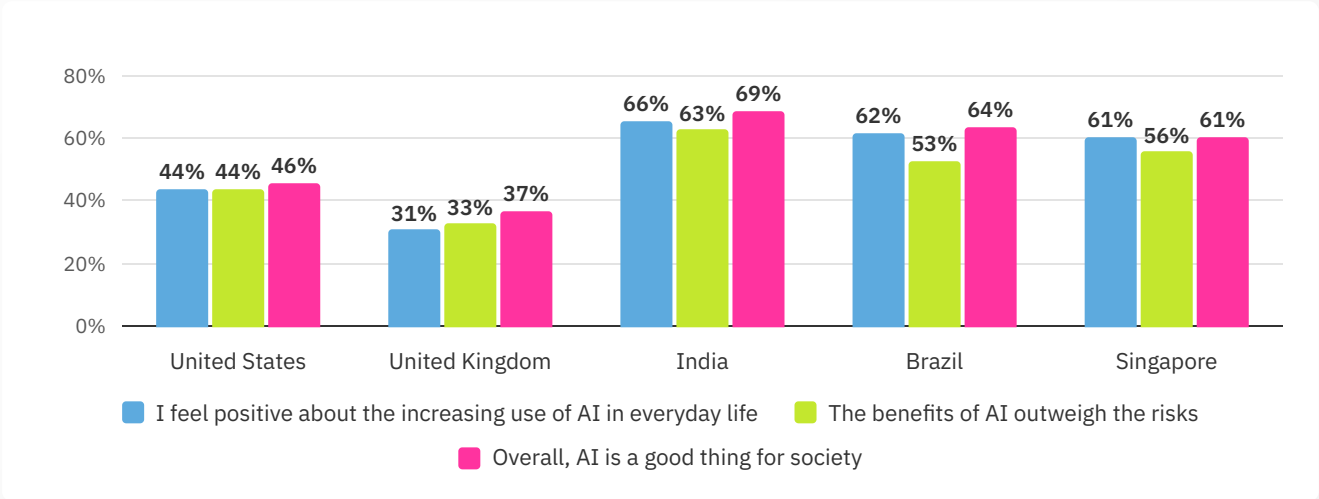


Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.

APPENDIX B: COUNTRY COMPARISONS

Attitudes toward AI also varied notably by country (Figure 117). India reported the most positive attitudes across all three measures, agreeing most that AI is a good thing for society (69%), that its benefits outweigh its risks (63%), and that they feel positive about its increasing use in everyday life (66%). The UK reported the least positive attitudes on every measure, ranging from 31% to 37%, with the US only slightly higher (44% to 46%).

Figure 117. Attitudes toward AI, by country.



Base: US, UK, India, Brazil, Singapore. Total number of participants: 5,000 (age 18+). Dates conducted: April 28, 2026 - May 19, 2026.



Summary cheat-sheet

COUNTRY COMPARISONS: AI

AI adoption is vastly higher in Brazil (91%), Singapore (90%), and India (89%) than in the US (69%) or the UK (60%). Workplace AI usage followed this exact same trend, peaking in Brazil (63%) and hitting its lowest point in the UK (36%).

AI security training varies wildly: Singapore recorded the highest training rate (48%), followed by Brazil (41%). India reported the lowest training rate (27%), despite its massive adoption figures. The US (36%) and UK (38%) sat in the middle.

Sharing sensitive work data with AI without an employer's permission was most common in Brazil (46%) and least common in Singapore (23%), with the US (33%), India (28%), and the UK (27%) falling in between. This is especially interesting given that Brazil and Singapore also had the highest percentage of those having received training on the risks of AI.

Spotting AI content: Confidence was highest in India across all formats (57%–69%) and lowest in the UK (33%–46%). The gap between them reached 20 points for AI video (65% vs 45%) and 26 points for AI text (65% vs 39%).

General attitudes toward AI were overwhelmingly positive in India (69% called it good for society, 66% felt positive about its increasing use in everyday life) and most skeptical in the UK (where only 37% and 31% agreed with those statements).

About



A leading nonprofit organization, the National Cybersecurity Alliance (NCA) is dedicated to creating a more secure, interconnected world. Advocating for the safe use of all technology, the NCA aims to educate everyone on how best to protect themselves, their families, and their organizations from cybercrime. The organization also creates strong partnerships between governments and corporations to foster a greater 'digital' good and amplify the message that only together can we realize a more secure, interconnected world.



CybSafe is the AI platform that points at the workforce security behaviors most likely to cause a breach, changes them, and proves it worked, or explains why not.

It's the behavior change platform for the AI era – built on behavioral science and powered by [SebDB](#), the world's cybersecurity behaviors database.



Carnegie Mellon University is a private research university serving more than 16,500 students from over 130 countries. Widely regarded as the birthplace of artificial intelligence, it holds top rankings in fields such as AI, business analytics and drama, and its research spans technology, science, policy and the arts. CyLab is the university-wide security and privacy institute at CMU that coordinates security and privacy research and education across all departments. Its mission is to catalyze, support, promote, and strengthen collaborative security and privacy research and education across departments, disciplines, and geographic boundaries to achieve significant impact on research, education, public policy, and practice.

Authors

Dr. Suzie Dobrontei, CPsychol, Behavioral Scientist, CybSafe

Dr. Jason R.C. Nurse, Director of Science & Research, CybSafe and Reader in Cyber Security, University of Kent

Contact us: research@cybsafe.com

Expert contributors

Oz Alashe MBE, CEO & Founder, CybSafe

Lisa Plaggemier, Executive Director, The National Cybersecurity Alliance

Jennifer Cook, Senior Director of Marketing,
The National Cybersecurity Alliance

Brian Hansford, SVP of Marketing, The National Cybersecurity Alliance

Dr. Lorrie Faith Cranor, Director and Bosch Distinguished Professor, CyLab Security & Privacy Institute; FORE Systems University Professor, Computer Science and Engineering & Public Policy, Carnegie Mellon University

Acknowledgments

Cliff Steinhauer, The National Cybersecurity Alliance

Max McKenna, The National Cybersecurity Alliance

Adam Brett, Senior Account Executive, ModOp

Patrice Gamble, Account Director, ModOp

Alice Cooke, Copywriter, CybSafe

Veronika Bondareva, Head of Creative & Design, CybSafe

Lily Klucinec, PhD student in Societal Computing, Carnegie Mellon University

Alexandra Li, PhD student in Societal Computing, Carnegie Mellon University

Ginger Smith, PhD student in Engineering & Public Policy,
Carnegie Mellon University