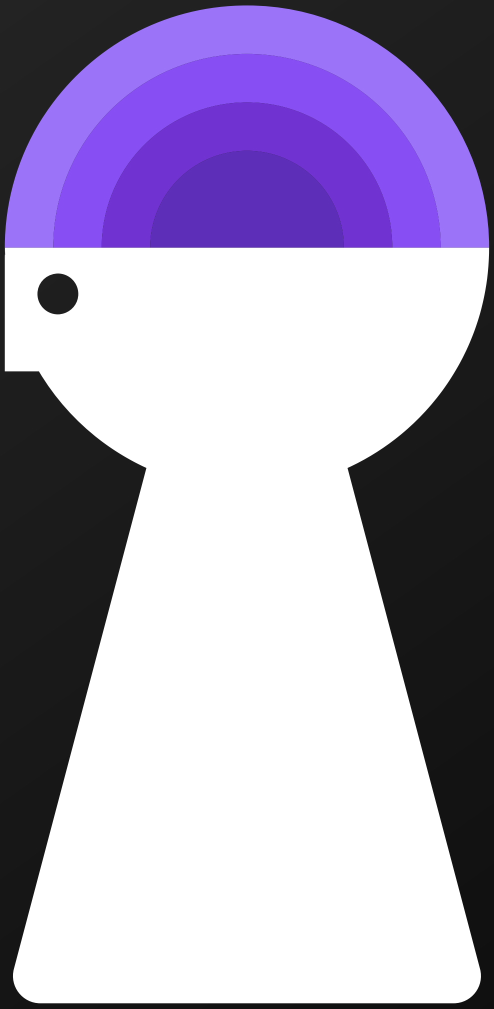
NATIONAL CYBERSECURITY ALLIANCE

CYBSAFE



Oh, Behave!

The Annual Cybersecurity Attitudes and Behaviors Report 2025-2026

Contents

More BS* than a late-night infomercial for a miracle mop

Welcome to the 2025-2026 Annual Cybersecurity Attitudes and Behaviors Report.

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

Fast, loud, full of opinions

If 2024 was the year of 'Can AI really do that?', then 2025 is the year of '*Should* AI be able to do that?'

Tools now churn out code, essays, and unsolicited opinions faster than you can say 'terms of service'. But while AI might grab the headlines, our data shows people remain the real wild card here.

Shadow AI is creeping into workplaces, with half of employees feeding sensitive data into unsanctioned tools. Meanwhile, training lumbers along miles behind adoption.

In other words, the tech might be shiny, but human behavior is still the risk frontier.

So, what's the vibe in '25?

Every year we tweak the lens to bring even more insight, but this time the picture really shifted. For the first time, we've added Brazil and Mexico to the mix, giving us a more global 7-country snapshot of human cyber behavior. That means more cultural contrasts, more fresh perspectives and, yes, more than a few surprises.

We've also doubled down on emerging risks. Last year we asked about everyone's favorite dinner party enlivener: AI. This year we've gone deeper with not just who's using it but how much sensitive data they're feeding it, what they think it means for their work, and whether they can spot AI-generated content. Spoiler: confidence is up, but so is risky behavior.

Did we stop there? Nah. Deepfake scams have joined the pack of probing questions. We captured who's been targeted, who's losing money, and which countries are bracing hardest against this new wave of impersonation fraud.

With this broader coverage and sharper focus, 2025 represents a step-change. The result is a richer story about what people know, what they do, and where they're still vulnerable.

Strong egos, weak passwords

Here's the twist we saw everywhere this year: confidence is up, behavior is down. Almost half of people feel sure they can spot AI content, phishing emails, or dodgy websites. But the same folks admit they rarely double-check, report, or take protective action.

We humans are famous for overestimating ourselves. It's like that time you were tempted to enter a marathon just because you once sprinted 100 meters to catch a bus. Yeah. Exactly.

This is the knowing–doing gap in action. And it's widening. People know what's secure. They just don't actually do it.

People. Even messier than your browser tabs

If this all sounds a little chaotic, that's because, well, it is. From MFA misunderstandings to password notebooks to the unstoppable rise of deepfake scam calls, the behavioral picture is more unhinged than ever.

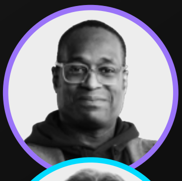
But buried in the maelstrom are real signals: how age, culture, and sector shape security decisions. Why younger generations are both the most confident and the most vulnerable. And where organizations can step in to bridge the gap.

That's why this report *really* matters. It's big, blunt, and brimming with BS*.

So settle into your seat, sip a beverage (just don't get mad if these stats make you do a spit take!), close those tabs (mental and on-screen alike), and join us as we unpack the human side of cybersecurity in 2025. We promise plenty of surprises, a few uncomfortable-but-vital truths, and a few lols along the way.

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

* Behavioral science, obvs.

Report aim & structure

Our fifth Cybersecurity Attitudes and Behaviors, *Oh, Behave! 2025-2026* report aims to give a thorough snapshot of people's cybersecurity attitudes and behaviors across representative global samples.

Building on four years of findings, we zoom in on five critical security behavior types that make or break security:

1. Ensuring password hygiene
    - Password creation habits[1] – specifically, password length, use of personal information, and single dictionary word
    - Using separate passwords[2]
    - Password management techniques[3]
2. Using multi-factor authentication (MFA)[4]
3. Installing the latest software updates[5]
4. Backing up data[6]
5. Checking messages for signs of phishing[7] and reporting[8] them

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

- How online are people, really?
- What do they think about cybersecurity, and what keeps them up at night?
- Who do they rely on for protection, and where do they place the responsibility?
- What types of scams do people experience, and do they report them?
- Who's got access to training, how do they feel about it, and does it stick?
- How do people engage with each of the five core security behaviors?
- And finally, what do people make of AI, both as a tool and as a threat, in both their personal and professional lives?

[1] SebDB behavior: [SB003] Uses a strong password or passphrase
[2] SebDB behavior: [SB016] Does not reuse passwords between accounts
[3] 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
[4] SebDB behavior: [SB001] Authenticates with MFA
[5] SebDB behaviors: [SB024] Keeps software up-to-date
[6] SebDB behaviors: [SB061] Backs up data
[7] SebDB behaviors: [SB058] Checks a website for signs of deception, [SB081] Checks a message for signs of deception
[8] SebDB behaviors: [SB087] Reports a suspicious message

Throughout, we dig deep into the attitudes and perceptions that sit behind the stats. We examine 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 cybersecurity behaviors.

The ultimate goal here? To arm cybersecurity professionals, policymakers, and educators with insight they can actually use to design smarter, more human-centered strategies.

And if you're hungry for the juicy details, the appendices serve up methodology, demographics, and country-by-country findings.

So that's the aim and structure covered. But wait! Before we floor it to the findings, let's take a sec to bust some jargon.

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 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: For this report, we narrowed down our investigation to five security behaviors (there are many more). These include: password hygiene (password creation, use, and management), applying MFA, 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, with the funds 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. 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.

KEY TERMS

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

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.

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

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).

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 are overseas.

Password hygiene: Creating unique and separate passwords for sensitive online accounts, managing passwords using browser or stand-alone apps, 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. Phishing via SMS is referred to as smishing, via phone call is referred to as vishing, and via QR code is referred to as quishing. For simplicity, we use the term 'phishing' throughout the report to refer to all deceptive messages, no matter how one receives them.

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, Apple), claiming there are issues with a device. They trick people into paying for fake repairs or granting remote access, which is then used to steal data or install malware.

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

Drumroll, please.
So here it comes.

From 7,000 people across 7 major countries, here's the big-picture view. The cyber attitudes and behaviors. The takeaways that you (and your board) can't afford to miss.
So, let's do this.

Executive summary

Bots gone wild: Artificial intelligence (AI)

Trust issues unlocked: Attitudes, beliefs & perceptions about online security

Deepfakes and deja vu: Cybercrime victimization & reporting

Gamified or game over? Cybersecurity training

Ctrl+Alt+Delusional: Cybersecurity knowledge & behaviors

Executive summary

Bots gone wild:
Artificial intelligence (AI)

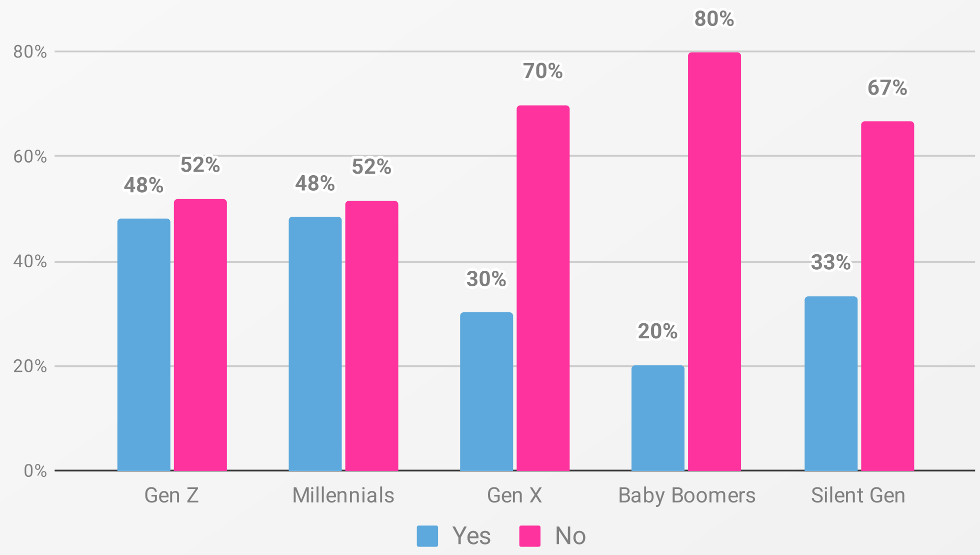
The rapid rise in AI usage is the double-edged sword to end all double-edged swords: while it boosts productivity, it also opens up new and urgent security risks, particularly as employees share sensitive data without proper oversight.

Adoption has exploded. Sixty-five percent of participants now report using AI, a complete reversal from last year's findings. This growth is sharpest among younger generations, with 89% of Gen Z and 79% of Millennials using AI.

But the safeguards aren't keeping up. More than half of employed participants (52%) say they've never received training on the security or privacy risks of AI tools.

This lack of training is feeding 'shadow AI'. Forty-three percent of workers admitted to sharing sensitive work information with AI tools without their employer's knowledge. This risky behavior is particularly common among younger demographics, with nearly half of Gen Z and Millennial employees admitting to it (Figure i), exposing confidential documents, customer data, and proprietary code.

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



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 2521 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

Confidence in spotting AI-generated content is mixed. Nearly half (48%) of participants say they feel highly confident, led by Millennials (60%) and Gen Z (58%), and particularly those in tech-focused sectors. In contrast, confidence is lowest among older generations and those in fields like healthcare and government.

Security concerns are high across all ages. Sixty-three percent of participants are worried about AI-related cybercrime and scams, and 67% believe AI will make it difficult to distinguish real from fake information. Many also believe that AI will make it easier for criminals to impersonate others (65%) and bypass security systems (67%).

Despite these concerns, trust in companies to implement AI responsibly is rising, from 36% in 2024 to 45% this year. However, skepticism remains strong, especially among older generations (27% of Baby Boomers, 19% of Silent Gen).

Perceptions of AI's impact on work are shifting, too. Forty-four percent believe it will affect their employment status, 49% think it will boost productivity. Younger generations are far more likely to believe AI will disrupt their employment status (59% of Millennials and 53% of Gen Z) but also enhance their productivity at work (63% of Millennials and 59% of Gen Z).

By sector, tech-heavy industries like IT (69%) and finance (62%) are more concerned about AI's impact on their employment status, while those in arts, entertainment, and recreation fields (36%) remain largely optimistic, believing AI won't touch them.

🌏 COUNTRY COMPARISONS

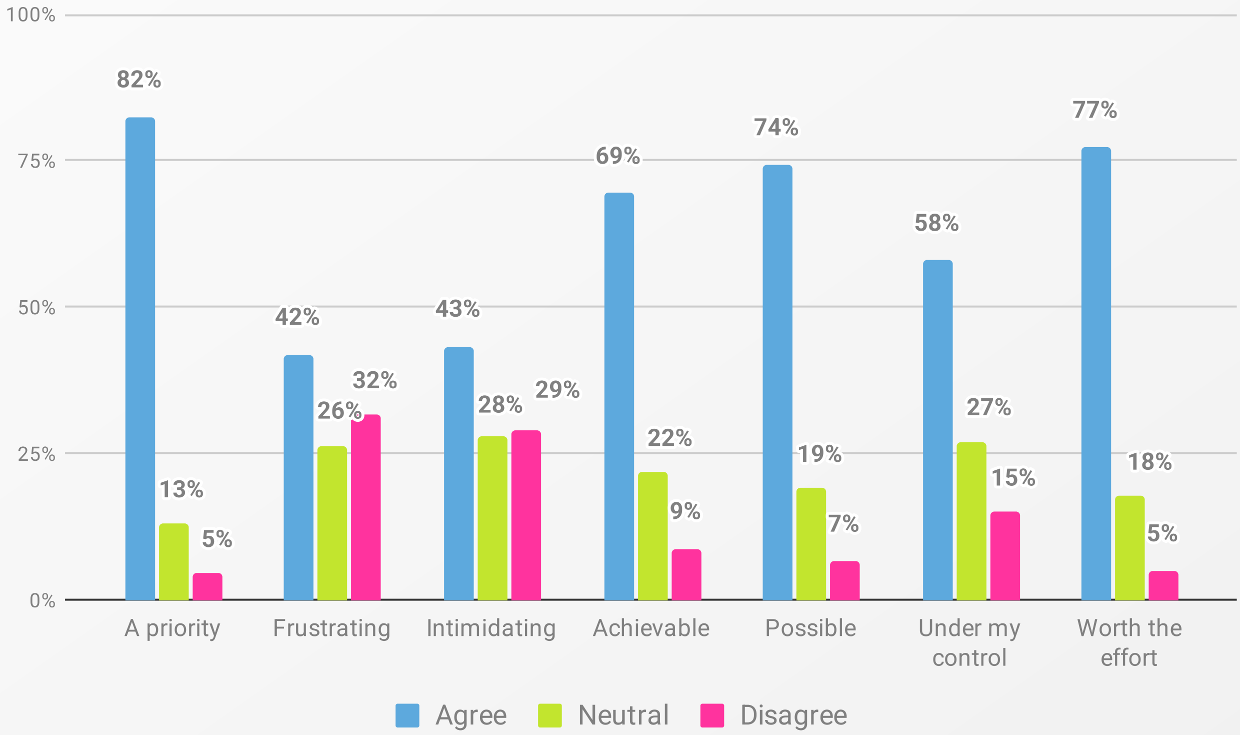
India leads in AI usage, with a hefty 87% of participants using AI and 55% of employees sharing sensitive work information with AI tools. This is in stark contrast to the UK, Australia, and Germany, where roughly half of participants report not using any AI tools at all. While Brazil and Mexico also show high adoption, it is primarily for home use. Despite these high usage rates in emerging digital economies, a low percentage of people in Brazil and Mexico have received training on AI risks (31% in both countries), highlighting a security gap.

But while AI might be rewriting the script, the plot still hinges on how people see their own role in the secure use of AI.

Trust issues unlocked: Attitudes, beliefs & perceptions about online security

Overall, participants' feelings toward online security are increasingly positive (Figure ii). A strong majority now consider staying secure online a priority (82%), believe it's worth the effort (77%, up 17% from 2024), and find it possible (74%, up 21%). Negative attitudes like frustration and intimidation have dipped slightly, but confusion (45%) and a belief that staying secure is easy (58%) have both increased since last year. Still, 43% of participants minimize online actions due to feeling overwhelmed, a 6% increase. Gen Z shows the biggest positive attitude shift, with 76% prioritizing online security (an 8% increase) and 71% believing it's possible (a 31% increase).

Figure ii. *'I feel that staying secure online is...'*



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

Yet misconceptions persist. Half of participants believe their devices are automatically secure (+7% from 2024), and 53% still consider online protection expensive. Concerns about governmental misuse of apps remain widespread, with 55% concerned about foreign states and 53% about their own governments.

Younger generations show slightly higher concern about domestic government data misuse (58% of Millennials, 53% of Gen Z) compared to older generations (44% of Baby Boomers).

Within the workplace, cybersecurity is recognized as a top priority. Sixty-nine percent say their organization prioritizes it, and 70% believe senior management is focusing on risk reduction. However, nearly half (49%) see colleagues as the biggest IT threat, either through carelessness or malice.

The media cuts both ways. It fuels fear (54%, +10%) and complexity (55%, +8%) but also informs (62%, +8%) and motivates protective actions (65%, +6%). Notably, the media's motivating impact is now highest among younger participants (Millennials and Gen X at 68%, Gen Z at 62%), a change from older generations in 2024. Media pushes action too: 51% now use stronger passwords and watch for AI-generated content.

🌏 COUNTRY COMPARISONS

India and Mexico report the highest confidence that security is achievable and under their personal control, yet they also report the highest levels of confusion and intimidation about security information.

Confusion is most common in India (56%) and Mexico (50%), while the UK consistently shows a more proactive and less fearful attitude, and a strong belief in continued self-protection. Germany stands out as the only country where a majority (55%) feel that security is not under their personal control.

In workplace culture, India, Mexico, and Brazil show strong confidence in management's prioritization of security, while the US, Germany, and Australia lag behind.

Government-related concerns vary sharply. The UK shows the lowest levels of concern about both foreign and domestic misuse, while Mexico has the highest.

Across all countries, most participants believe law enforcement lacks the capacity to address cybercrime, and an even greater number feel that cybercriminals are more advanced than those tasked with stopping them.

Of course, perceptions are only one part of the puzzle. What happens when cybersecurity hits home?

Deepfakes and deja vu: Cybercrime victimization & reporting

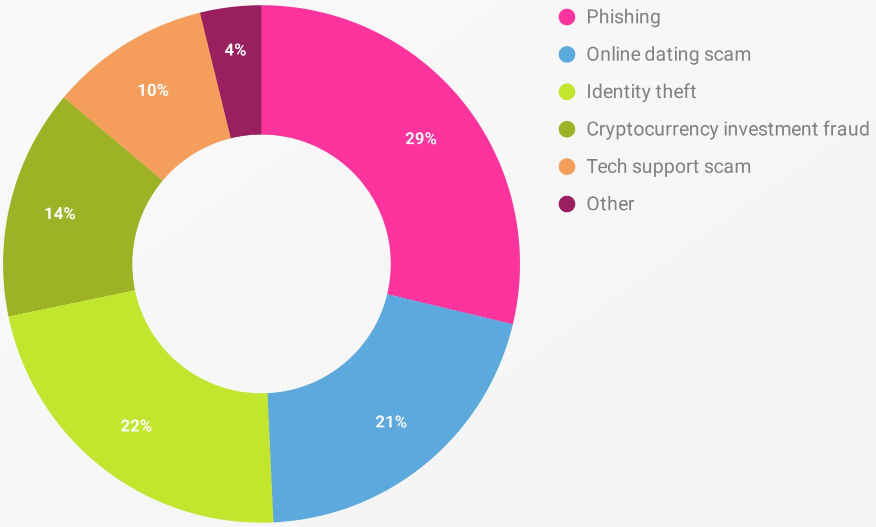
Concern about becoming a victim of scams and wider cybercrimes is widespread. Around two-thirds of participants (68%) express worry, an increase since 2024, and particularly pronounced among younger generations (70% of Millennials). Yet only 41% consider themselves likely targets. This perception has shifted away from older generations toward younger ones, suggesting a growing disconnect between risk awareness and self-perceived vulnerability.

A rising belief in the inevitability of losing money (31%) and personal details (40%) online points to a sense of helplessness. Confidence in institutions is also low. Almost two-thirds (64%) doubt law enforcement's effectiveness, and 69% believe cybercriminals outpace those meant to stop them.

As well as being a concern, victimization is increasingly a reality. Forty-four percent of participants reported being personally victimized, with a loss of money or data, in 2025 (a 9% rise from 2024), accounting for 4,745 self-reported incidents.

Phishing remains the most common type of incident (29%), followed by identity theft (22%) and online dating scams (21%) (Figure iii). Younger generations, particularly Gen Z (59%) and Millennials (56%), are disproportionately affected across various crime types.

Figure iii. Types of cybercrime incidents.



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of cybercrime incidents: 4745. Dates conducted: May 2, 2025 - May 27, 2025.

For the first time, our data shows the scale of deepfake scams. Over a third (34%) of participants have experienced deepfake scam calls, with younger age groups again being more frequently targeted.

Cybercrime victimization often causes significant emotional distress, including stress (51%), anger (49%), and anxiety (42%).

Overall reporting rates for cybercrime incidents are high (91%), with most victims turning to banks or credit card companies, followed by police or government agencies. However, underreporting persists: 25% of phishing victims didn't know who to tell, and 22% of online dating scam victims felt too ashamed. Cyberbullying victimization also saw a 5% rise this year, impacting 23% of participants, with the highest prevalence among younger age groups. While reporting cyberbullying to formal authorities has increased, reporting to other support networks (e.g., peers, family) has declined.

🌏 COUNTRY COMPARISONS

India (59%) and the US (49%) report the highest rates of overall cybercrime victimization, a trend consistent across threats such as phishing and identity theft. In contrast, the UK (33%) and Germany (37%) report the lowest rates of victimization and are least exposed to emerging threats like deepfake scams. However, Germany stands out with the highest rate of financial loss among deepfake victims (55%). Brazil shows the lowest reporting rates across all types of crime.

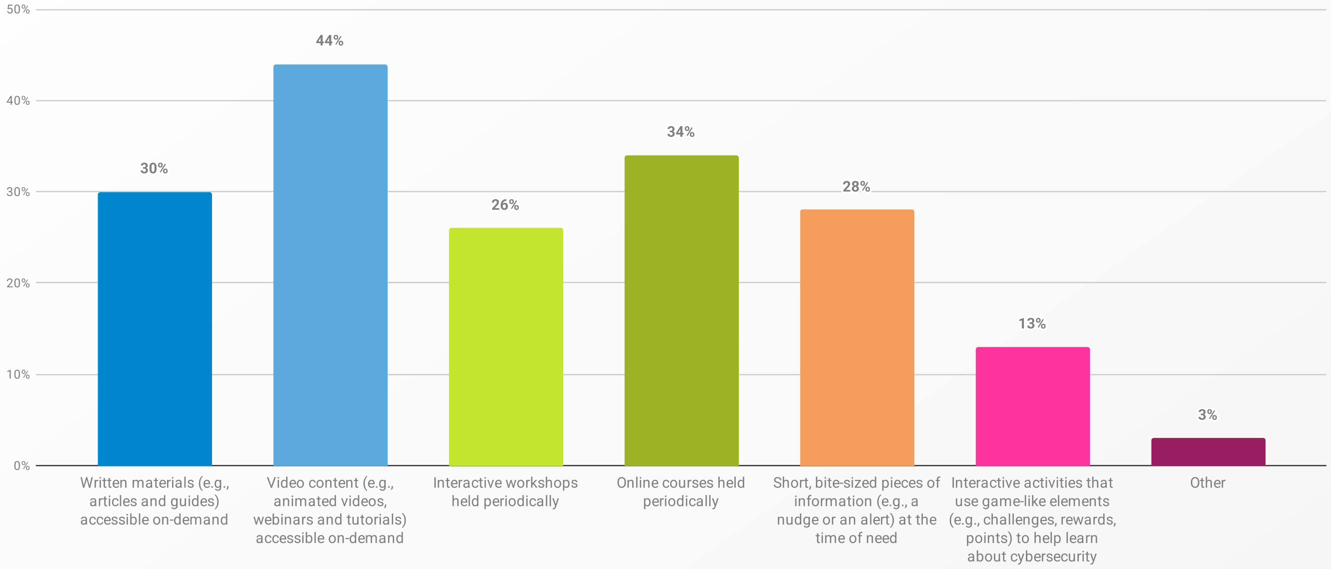
With crime on the rise, we need to think about how best to make people aware of the risk and how they can respond to it; enter... training. Let's see who gets access to it, who takes it up, and how effective it really is.

Gamified or game over? Cybersecurity training

Only 32% of participants reported having access to and using cybersecurity training, a minor decrease from last year. Access remains highly uneven. Younger generations (43% of Gen Z and 45% of Millennials) are far more likely to receive training, as are workers in tech (64%), finance (58%), and utilities (60%). In contrast, the majority in retail (56%), hospitality (58%), and arts (49%) lag behind. And more than half of all participants (55%) have no access to training at all. Among those with access who don't attend, top reasons remain lack of time (21%) and disbelief it reduces risk (20%).

Among employed participants who have mandatory training (49%), a growing number are completing it more than once a year, potentially signaling that organizations are moving toward more dynamic approaches to cybersecurity. Videos top the list; 44% prefer it, and it's also the most common format provided by employers (54%), followed by online courses (34%, Figure iv). However, preferences vary by age and employment status. Older generations and those not actively employed show a higher preference for written materials.

Figure iv. '*What format do you prefer to consume cybersecurity training information?*'



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

The bigger issue here is impact. Most attendees (83%) said training was useful, but fewer than half actually changed their behavior as a result. Only 47% said they became better at spotting phishing, 42% started using MFA, and 40% adopted strong passwords.

🌏 COUNTRY COMPARISONS

India stands out, with a majority of participants (72%) required to complete mandatory training and a high rate of actual training use (46%). In contrast, most participants in Germany (63%), Brazil (63%), the UK (60%), and Australia (60%) report having no access to training at all. When training is offered, video is the most common and preferred format in most countries. Germany is the exception, with 32% of participants preferring written materials over video.

Now, training might plant the seed, but knowledge is what grows from that seed. Sometimes. Because the thing is, we can't ignore how confident people really feel about their cybersecurity know-how.

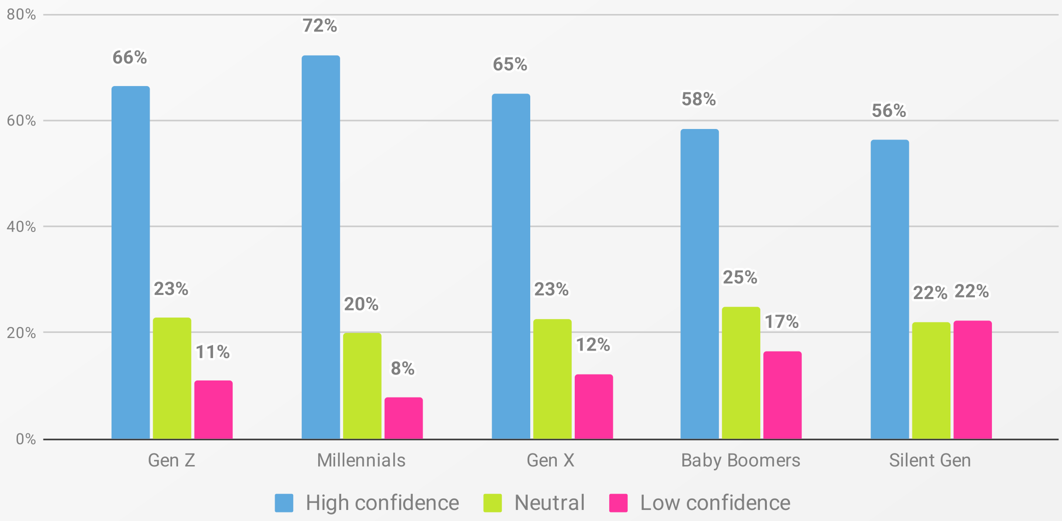
Ctrl+Alt+Delusional: Cybersecurity knowledge & behaviors

Overall, people's perceived level of cybersecurity knowledge has dropped. Only 49% of participants now rate themselves as having intermediate or advanced knowledge, an 8% drop from 2024. Younger generations and those in tech-related sectors display the highest confidence, but this confidence in their knowledge often doesn't translate into secure actions. For instance, weak password creation is on the rise, and fewer people are using unique passwords across their accounts compared to last year, with just 62% doing so frequently. On top of this, a staggering 41% have never used a password manager, most often citing a preference for personal control or a lack of trust in these tools.

Convenience continues to trump security in many cases, particularly when it comes to MFA. A concerning 23% of participants have never even heard of it, and only 41% use it regularly. Somewhat surprisingly, older generations are more diligent: 49% of Baby Boomers use MFA regularly, compared to just 17% of Gen Z, who dismiss it as unnecessary or inconvenient. Only 43% of people use biometrics to log in, with reluctance driven by concerns about companies mishandling biometric data or fears of it being hacked.

This 'knowing–doing' gap shows up elsewhere too. Software updates are slipping. Just 60% install them, down 3%, and 23% admit they know how to update but choose not to. Similarly, confidence in spotting phishing remains fairly high (66%), particularly among younger participants (Figure v), but consistent follow-through is lacking. Both checking for phishing signs and reporting suspicious messages have declined, with fewer than half of participants (45%) doing so 'always' or 'very often'.

Figure v. '*How confident are you in your ability to identify a phishing email or a malicious link?*' by generation.



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025

🌏 COUNTRY COMPARISONS

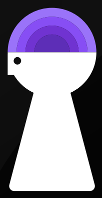
While India (65%) and Germany (56%) lead on intermediate or advanced knowledge, the majority of participants in Brazil (43%), the UK (42%), Australia (41%), the US, and Mexico (both 40%) report having only basic knowledge. This is particularly concerning in India, where despite reporting relatively solid knowledge, participants are most likely to use weak password creation techniques. The UK (54%) and Australia (53%) lead in MFA adoption, while Mexico (41%) and Brazil (28%) have the lowest awareness. The US leads in password manager usage (50%), while India, Mexico (both 21%), and Brazil (20%) have the highest rates of users who have stopped using them. The UK (60%) and Mexico (59%) are the most proactive about installing software updates, while Germany and the US (both 18%) have the highest percentages of people who rarely or never do.

Stage: set.
What comes next is the full feature, a closer look at the data, the context, and those surprising contradictions that define this year's picture.

Deep breath. Coffee refill. In we go.

Main findings

1. Scroll, stream, swipe, repeat: Online presence
2. Hope, fear, and culture: Attitudes, beliefs, and perceptions about online security
3. Are we in an accountability void? Reliance & responsibility
4. Cybercrime victimization & reporting
5. Lessons (un)learned? Cybersecurity training
6. Confidence trick? Cybersecurity knowledge & behaviors
7. Large liability model? Artificial intelligence (AI)



Main findings

So, how exactly did we reel in this almighty data haul? Excuse a little repetition from the intro, but we know some of you dataheads will have skipped the starter and got straight into the juicy bits.

When? We ran our fifth Cybersecurity Attitudes and Behaviors survey online, between May 2 and 27, 2025.

Where? Toluna collected representative samples, balanced by age and gender, from the United States, the United Kingdom, Germany, Australia, India, Brazil, and Mexico. That's 7000 people. The most international Oh Behave! yet!

Who? Our survey targeted adults (aged 18 years and older), with the average age being 45 years (SD=17.02). Sixty-five percent of respondents were in full- or part-time employment. All the demographic details are in Appendix A, for those endnote fans out there.

What? Just like past years, we broke things down by age group and employment status. We delve into country-specific differences in Appendix B.

Who wants an extra slice?

For the first time this year, we sliced the data by industry too. Why? Because we all know a healthcare worker's exposure isn't the same as someone in retail or finance. But now, for the first time, we can put actual numbers to those hunches.

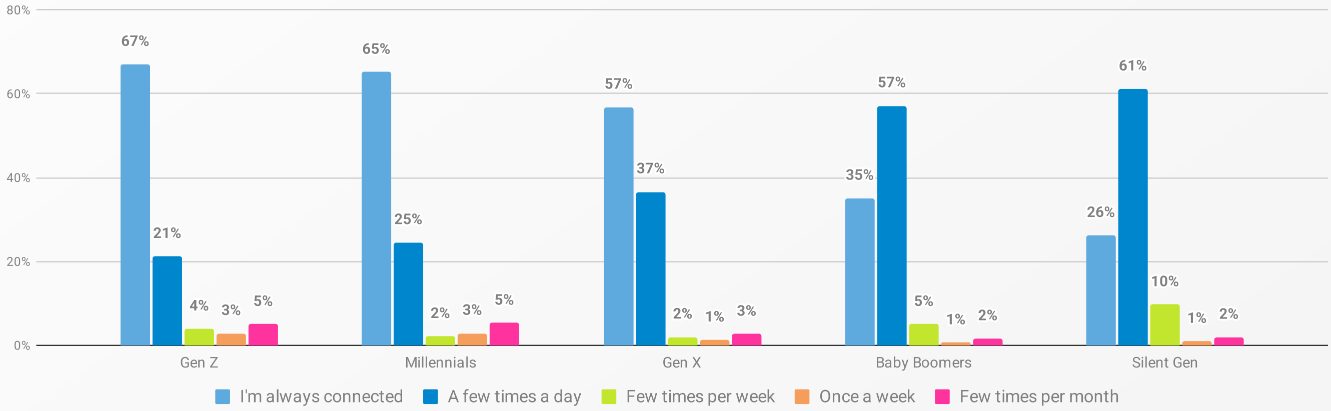
First up, how are people living their digital lives? How connected are people, *really*? And how are they handling the accounts that hold their digital lives together?

1. Scroll, stream, swipe, repeat: Online presence

In an increasingly hyper-connected world, people are spending more time online than ever before. This year, a significant 57% of participants report being ‘always connected’ to the internet, a 4% increase from last year.

This constant connectivity is still driven by younger generations (Figure 1), with 67% of Gen Z and 65% of Millennials reporting they are ‘always connected’, though the percentages have increased for all generations since 2024. Even the so-called ‘offline’ generations are sneakily creeping upward.

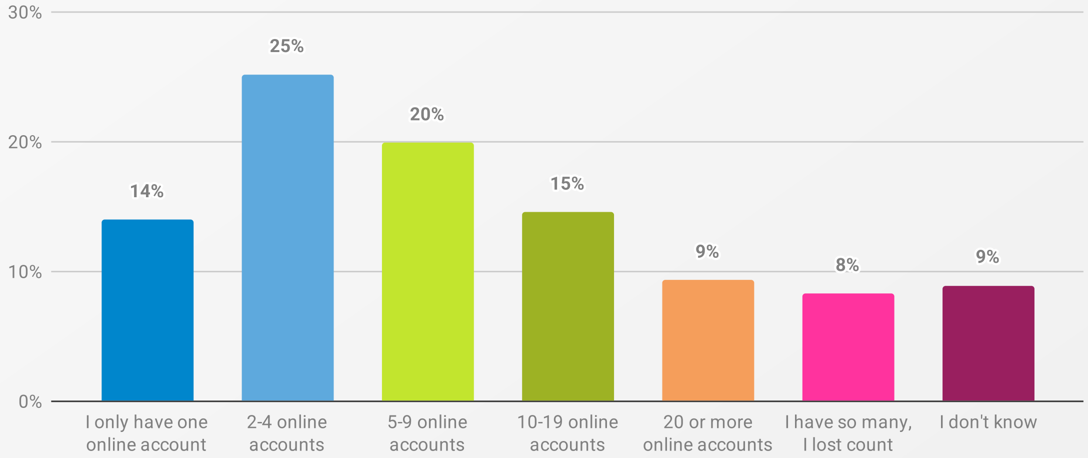
Figure 1. ‘*How frequently do you use the Internet?*’ by generation.



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

But while people are spending more time online, they may be getting more savvy about how many doors they leave open. We asked how many sensitive online accounts (that’s the ones with personal information) people held (Figure 2). And get this: only 24% admitted to more than ten accounts this year. That’s down an eyebrow-raising 9% from last year.

Figure 2. ‘*Overall, how many sensitive online accounts that hold personal information do you have?*’



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

So, the picture is a little paradoxical, really. People are more online than ever, yes. But, they're also trimming the digital fat. What we're seeing is a shift toward consolidation, maybe toward people being more intentional and discerning, saying no to digital sprawl and chaos. For anyone tracking and managing human risk, that's an encouraging sign.

That said, trimming down the number of accounts doesn't mean the ones left behind are safe. So next, let's talk about passwords and authentication. Are people *finally* ditching '123456', or is it the same old highly hackable story?

2. Hope, fear, and culture: Attitudes, beliefs, and perceptions about online security

The Knowledge-Attitude-Behavior (KAB)[9] model tells us something powerfully simple:

What people know (knowledge) shapes how they feel (attitudes), which in turn influences their actions (behaviors).

When it comes to online security, attitudes, beliefs, and perceptions are at the heart of things. They're factors that significantly affect how people engage with online security. These internal states often serve as critical precursors to action. And they're key to understanding why people choose to adopt or ignore secure practices.

In this chapter, we explore the security mindset in detail. We start by examining how people navigate their personal security, exploring their feelings about the ease, frustration, and overall possibility of staying safe online.

From there, we address common misconceptions and concerns about device security, the cost of protection, and governmental data use.

Then we shift the focus to the workplace, analyzing the prevailing cybersecurity culture within organizations. And finally, we investigate the powerful role media plays in shaping these attitudes and perceptions, and therefore on security actions too. (Spoiler: it's not always motivating the actions you'd hope for.)

[9] 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.

2.1 In our optimism era? Navigating personal security

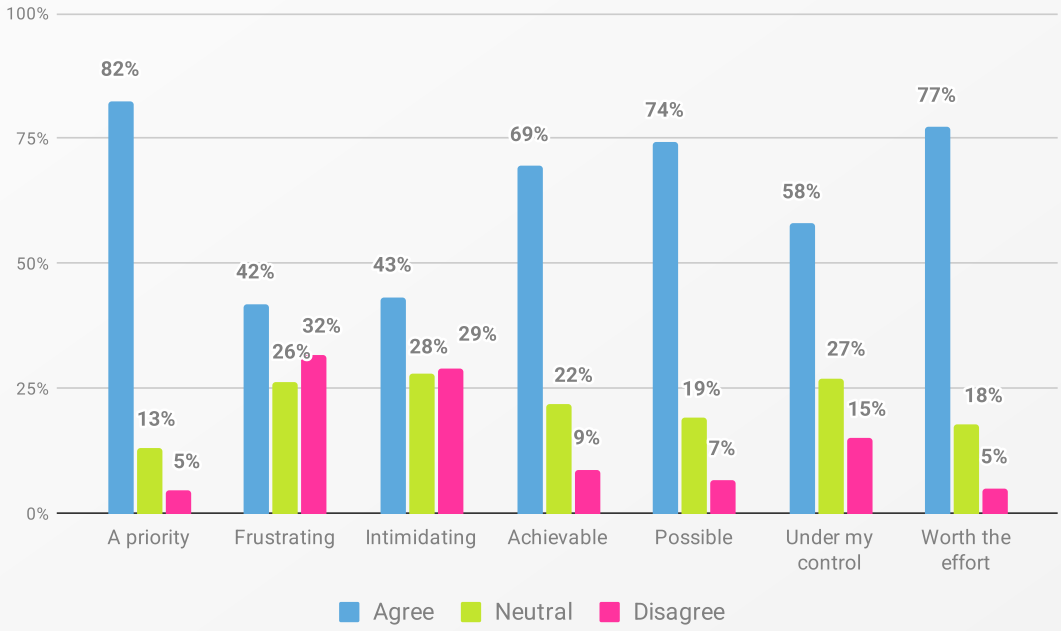
How are people navigating personal security? Good vibes about online security appear on the up this year (Figure 3), revealing some notable shifts since last year.

For instance, the majority of participants said staying secure online was a priority (82%), worth the effort (77%), and possible (74%). Those last two jumped sharply, up 17% and 21% respectively[10] since 2024.

And the gloomier takes have dipped too. This year 42% said online security is frustrating (down 4%), and 43% found it intimidating (down 1%).

Next, let's get generational and look at one big mood swing in particular. Gen Z had the biggest attitude shift: Figure 4 shows that all generations prioritize online security, a trend that seemed to increase with age, but the 76% Gen Z agreement is a standout. That's up 8% from last year.

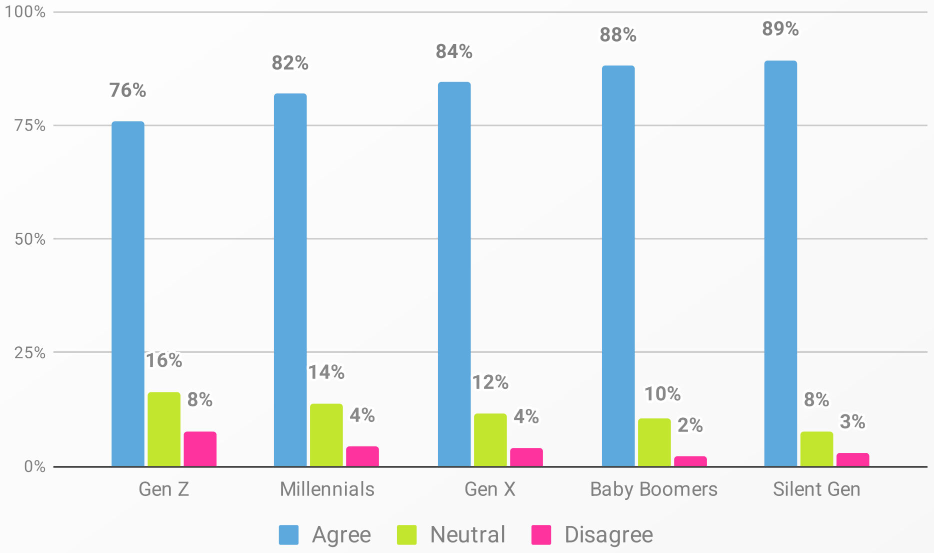
Figure 3. *'I feel that staying secure online is...'*



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

[10] This year's report used the positive phrasing 'Possible' and 'Worth the effort', whereas in previous years the options were worded negatively ('Not possible' and 'Not worth the effort'). While it's possible this has contributed to participants' responses, we believe the percentage change is too significant to be explained by the wording alone.

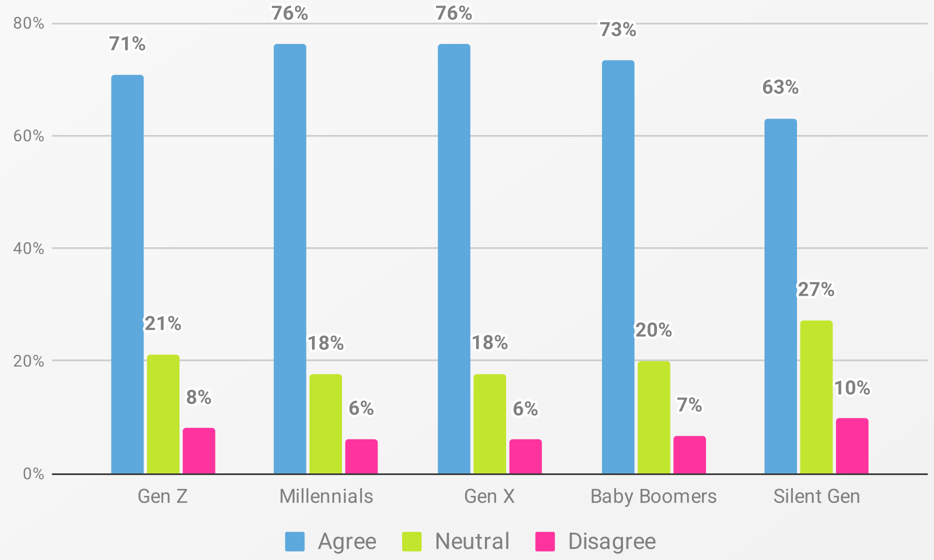
Figure 4. ‘*I feel that staying secure online is a priority*’ by generation.



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

Gen Z’s upbeat trajectory also showed up in their belief that staying secure online is possible (71%, Figure 5), with a huge 31% increase from 2024. This belief was highest among Millennials and Gen X (76%), and (no surprise) was lower for Baby Boomers (73%), and again for the Silent Gen (63%).

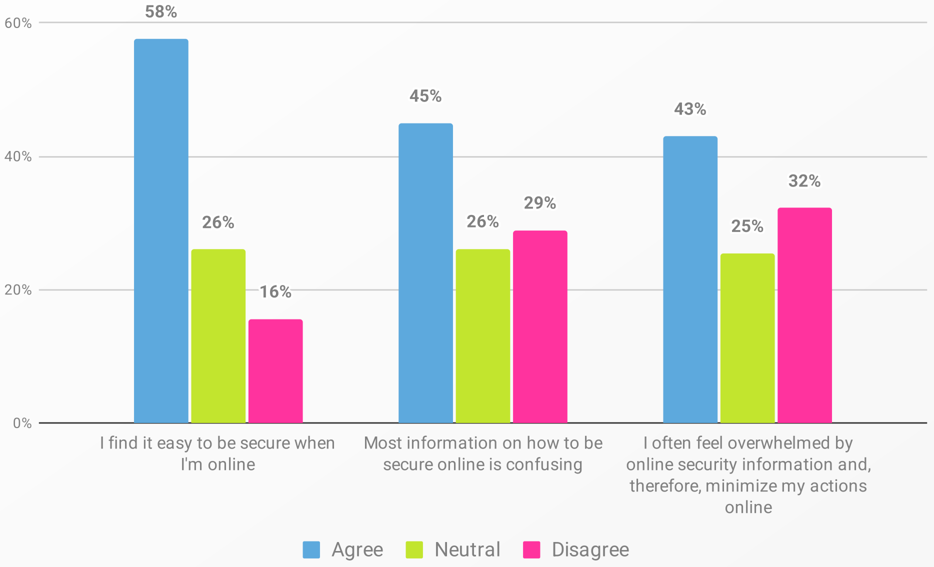
Figure 5. ‘*I feel that staying secure online is possible*’ by generation.



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

Perceptions of both ease (58%, Figure 6) and confusion about online security (45%) have risen since last year, as well as the percentage of people who minimize their online actions because they feel overwhelmed by online security information (43%), representing 4%, 5%, and 6% increases, respectively. Mixed signals, anyone?

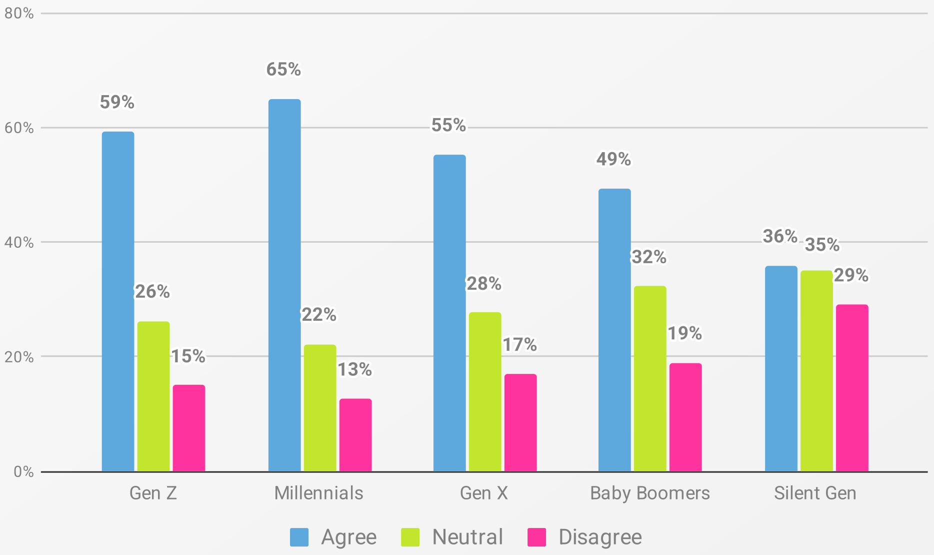
Figure 6. Participants' levels of agreement with online security ease, clarity, and overwhelm.



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

Unsurprisingly, older generations were less likely to find staying secure online easy (36% of Silent Gen, 49% of Baby Boomers) than younger generations (65% of Millennials, 59% of Gen Z, Figure 7). What's interesting, though, is the 6% increase among Gen Z, adding weight to the broader attitude shift described above.

Figure 7. '*I find it easy to be secure when I'm online.*' by generation.



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

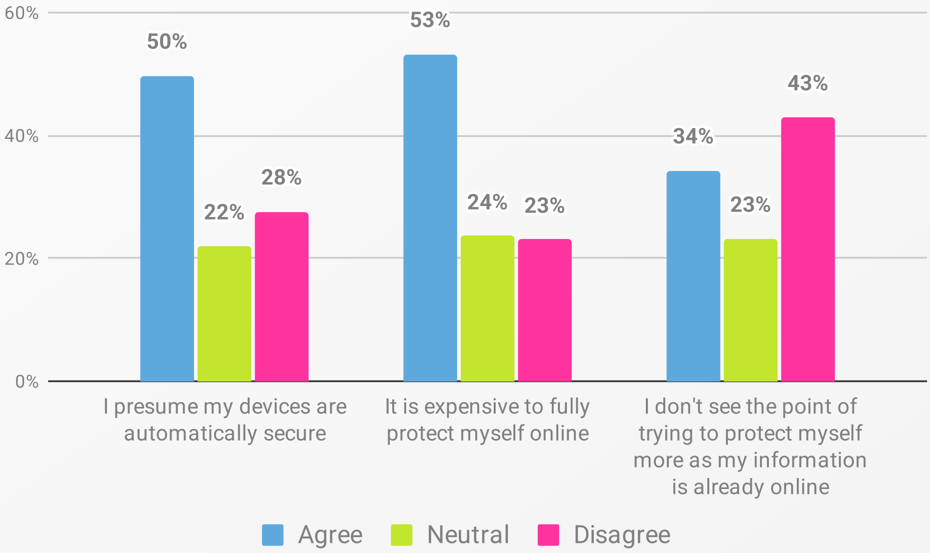
Where does that leave us? While there's a clear and encouraging trend toward more positive attitudes about the possibility and worth of online security, particularly among younger generations like Gen Z, challenges persist. Many still find security information confusing or feel overwhelmed, causing some to hold back online... Optimism = up. Myths = also up. Maybe it's time to get up close and personal with some of the myths. Ready?

2.2 Futility chic is *so* in: Misconceptions and concerns

Common misconceptions and concerns about online security have also increased since 2024. Half of participants think their devices are automatically secure (+7%), and 52% say protection is expensive (Figure 8).

What's more grim, an increasing percentage (34%, up 4%) felt there's no point protecting themselves, as their information is already out there.

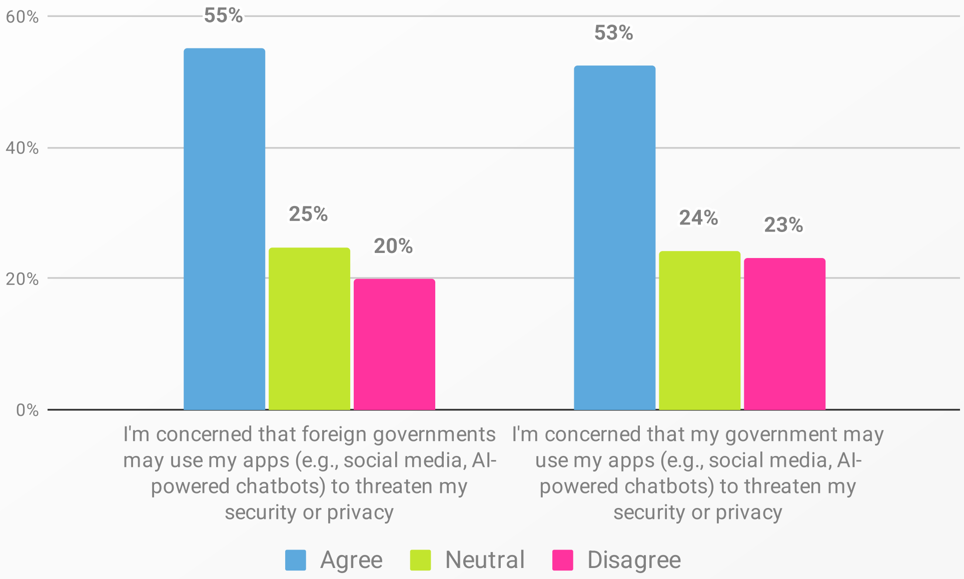
Figure 8. Perceived barriers to personal online security.



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

Government misuse worries are widespread (Figure 9). Over half fear foreign governments (55%) and their own government (53%) using apps to threaten security or privacy. These figures indicate a widespread apprehension about governmental surveillance or misuse of personal data, with foreign concerns slightly outweighing domestic.

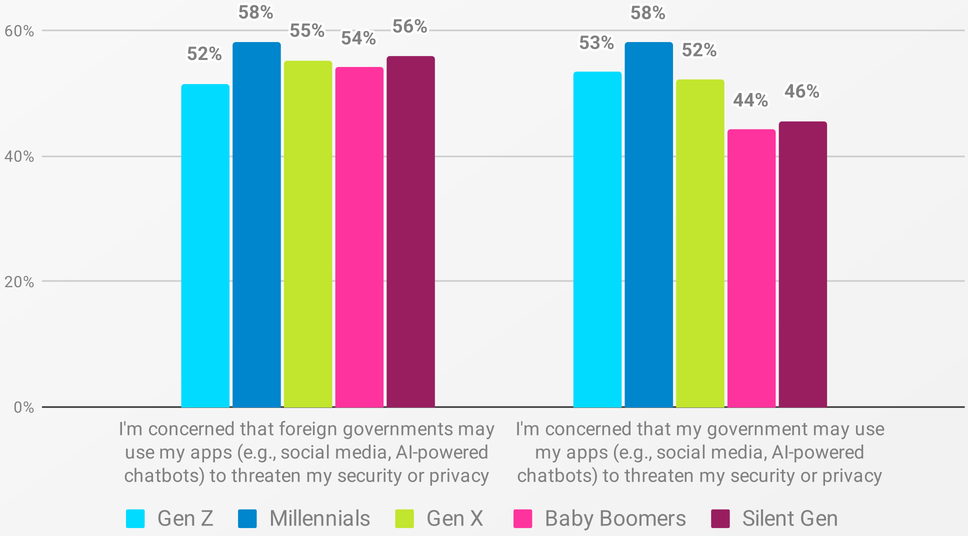
Figure 9. Concerns regarding foreign and domestic government use of apps to threaten security or privacy.



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

What happens when we slice things by generation? Well, it gets super interesting (Figure 10): Younger generations were just as concerned (Millennials, 58%; if not more, Gen Z, 53%) about their own government misusing their data. Older generations, however, saw foreign governments as a much bigger danger.

Figure 10. Concerns regarding foreign and domestic government use of apps to threaten security or privacy, by generation.



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

These findings align with broader cybersecurity research, where concerns about government surveillance and data misuse are a consistent theme. Studies[11] have shown that individuals are concerned about their personal information being collected via mobile apps, and their online activities being watched by authorities.

Furthermore, the success of government-led digital initiatives, such as contact tracing apps, often relies heavily on public trust and perceptions of privacy protection.

In conclusion, these findings highlight persistent and growing misconceptions about online security. Many still assume that devices are automatically secure, but the bigger worry is the rising sentiment of futility – that there's no point in trying to protect oneself online. This sense of helplessness, combined with distrust of both foreign and domestic governments and a skepticism about the efficacy of protective entities, points to a crisis of confidence.

Cybersecurity efforts need to go beyond simply providing information. They must directly address these deeply ingrained psychological barriers. They need to restore a sense of agency and rebuild trust in the systems and institutions leading on digital safety.

But if trust feels shaky in daily life, it's even harder to come by at work. That's where the cracks really begin to show, as we'll see next. Strap in.

2.3 Among us: Cybersecurity culture in the workplace

For the first time in the five-year history of this report, we asked our employed participants some cybersecurity culture specific questions.

We like NCSC's definition of security culture:

'*the collective understanding of what is normal and valued in the workplace with respect to cyber security. It sets expectations on behaviour and relationships, influencing people's ability for collaboration, trust, and learning.*' [12]

Understanding these cultural elements is crucial for assessing an organization's true security posture. Our findings reveal how people see their workplace's cybersecurity environment.

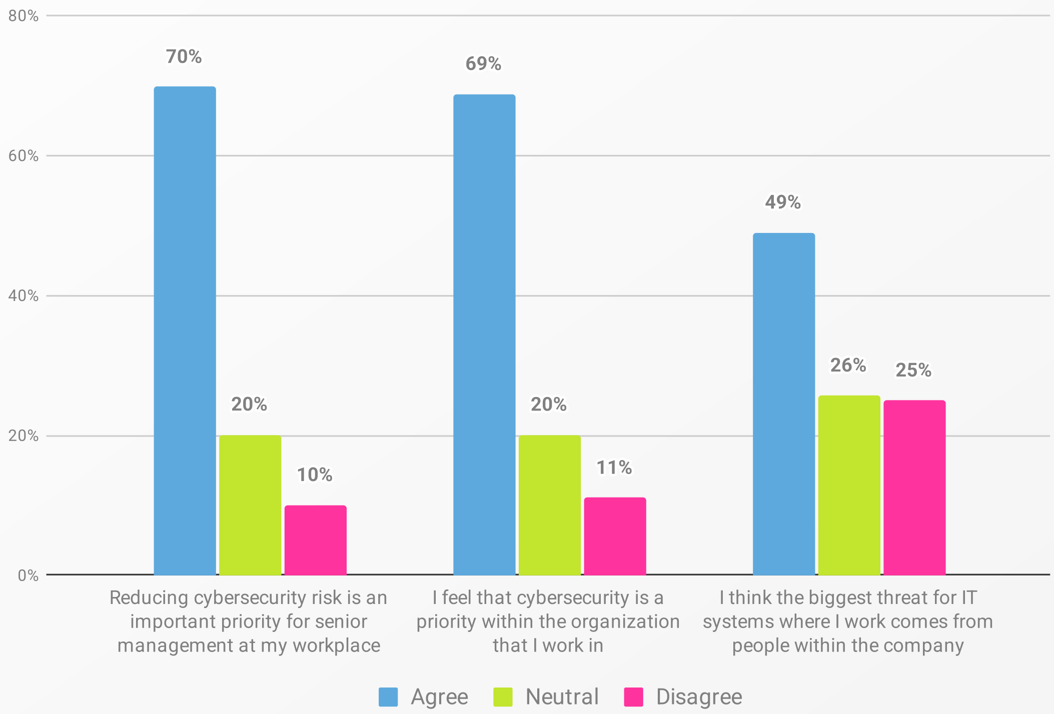
[11] Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., & Turner, E. (2019). Americans and privacy: *Concerned, confused, and feeling lack of control over their personal information*. Pew Research Center. Retrieved July 28, 2025, from https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2019/11/Pew-Research-Center_PI_2019.11.15_Privacy_FINAL.pdf;
Willems, J., Schmid, M. J., Vanderelst, D., Vogel, D., & Ebinger, F. (2023). AI-driven public services and the privacy paradox: Do citizens really care about their privacy? *Public Management Review*, 25(11), 2116–2134.

[12] National Cyber Security Centre (NCSC). (2025, June 4). *Cyber security culture principles*. NCSC.GOV.UK. Retrieved August 8, 2025, from https://www.ncsc.gov.uk/collection/cyber-security-culture-principles

The results didn't stutter: many people recognize cybersecurity's importance within their organization. Most employed participants see cybersecurity as a workplace priority (69%, Figure 11). A similar number believe senior managers saw reducing cybersecurity risk as an important priority (70%). Both figures are encouraging, but there's also room for improvement here.

On the downside, nearly half (49%) see internal personnel as the biggest IT risk. This perception of insider threat highlights a challenge that organizations ignore at their peril.

Figure 11. Attitudes toward cybersecurity in the workplace.



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

Overall, we've got a mixed bag here. Awareness is strong, and leadership buy-in is evident, but trust gaps remain. We think the real opportunity here lies in strengthening a culture of shared responsibility and continuous learning, so that good intentions translate into robust, collective security behaviors.

And, of course, culture doesn't exist in a vacuum. What people see and hear in the media also shapes how they think about security... for better or worse 👇

2.4 The press factor: Media's role in shaping attitudes

Shocker: The media and news continue to play a significant role in shaping how people think about cybersecurity and how they act online. More surprising, though, are the changes in the past year.

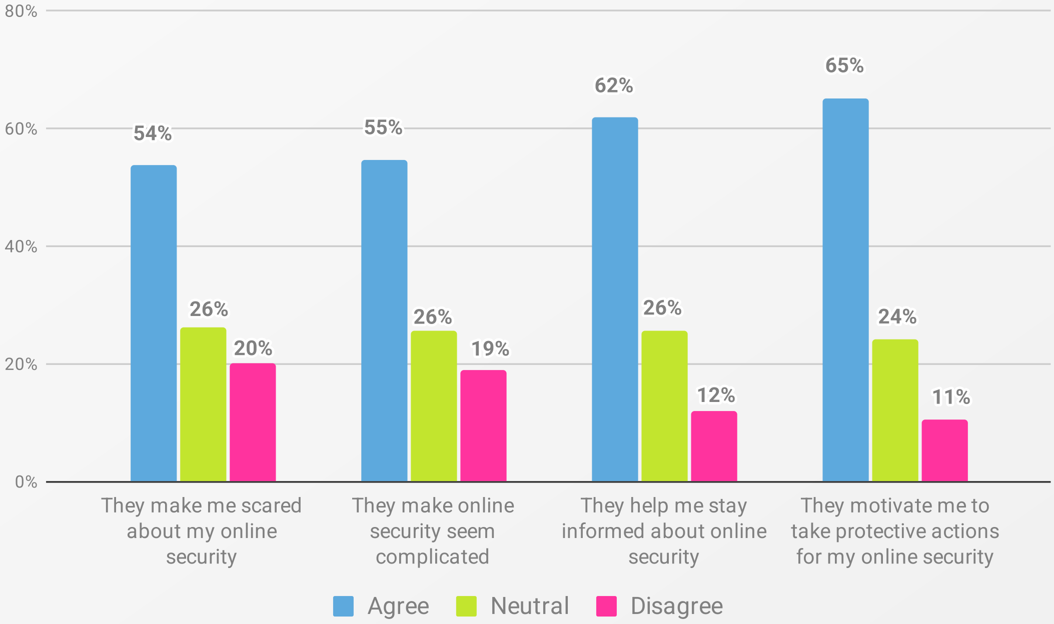
This year, 54% of participants said that the media makes them scared about their online security (Figure 12), which is a 10% increase from last year. Similarly, more than half say the media makes online security seem complicated (+8%). Headlines clearly aren't calming anyone's nerves...

> **Emails can be made to look exactly like the companies and people you regularly interact with. I check every email, from 'sender' and 'recipient/s' to spell check it. It's becoming more and more difficult and makes me fearful when I hear on media channels that people from all walks of life, regardless of their status, intelligence or wealth, are more commonly being tricked.** P2925, Australia

Despite these increases in negative perceptions, there's also a brighter side to the media story. This year, 62% said the media helps them stay informed about online security, up 8% from last year. Meanwhile, 65% said the media motivated them to act, up from 59% in 2024.

So, while media stirs up fear and complexity, its role in informing and motivating cybersecurity actions is also growing.

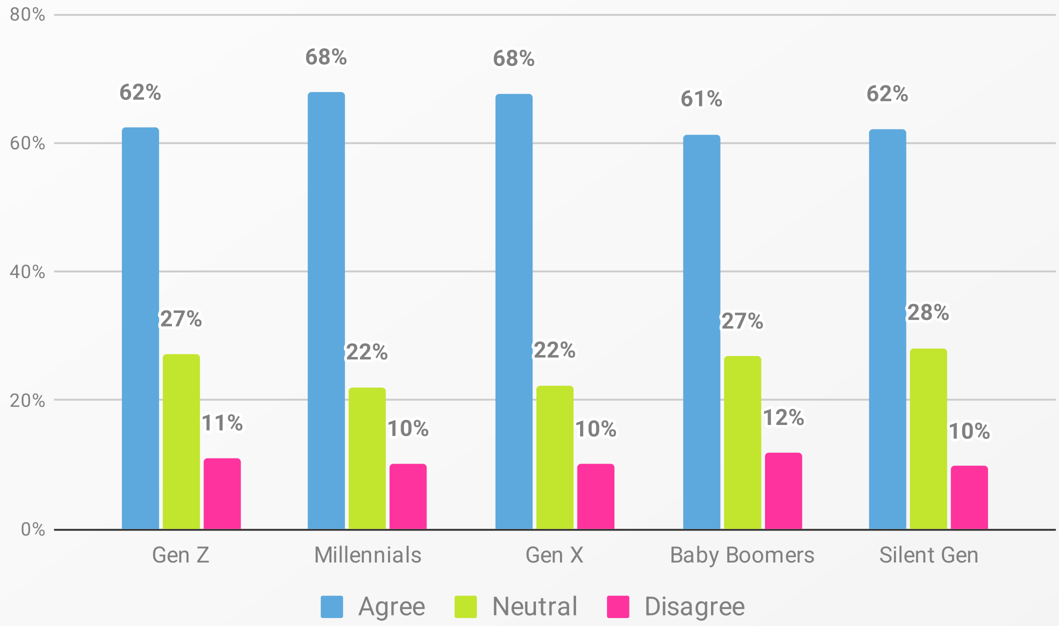
Figure 12. '*What impact does the media/news have on your views toward online security?*'



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

Looking at the generational breakdown of the media's motivating impact (Figure 13), we see a real shift. Last year, older generations reported the highest impact of media coverage on motivating protective actions. But this year, motivation was highest among Millennials and Gen X (both at 68%), and Gen Z (62%). That's a big jump in motivation from media for Millennials (+8%) and Gen X (+11%) compared to 2024, suggesting that media-driven cybersecurity campaigns are starting to resonate more with these younger demographics.

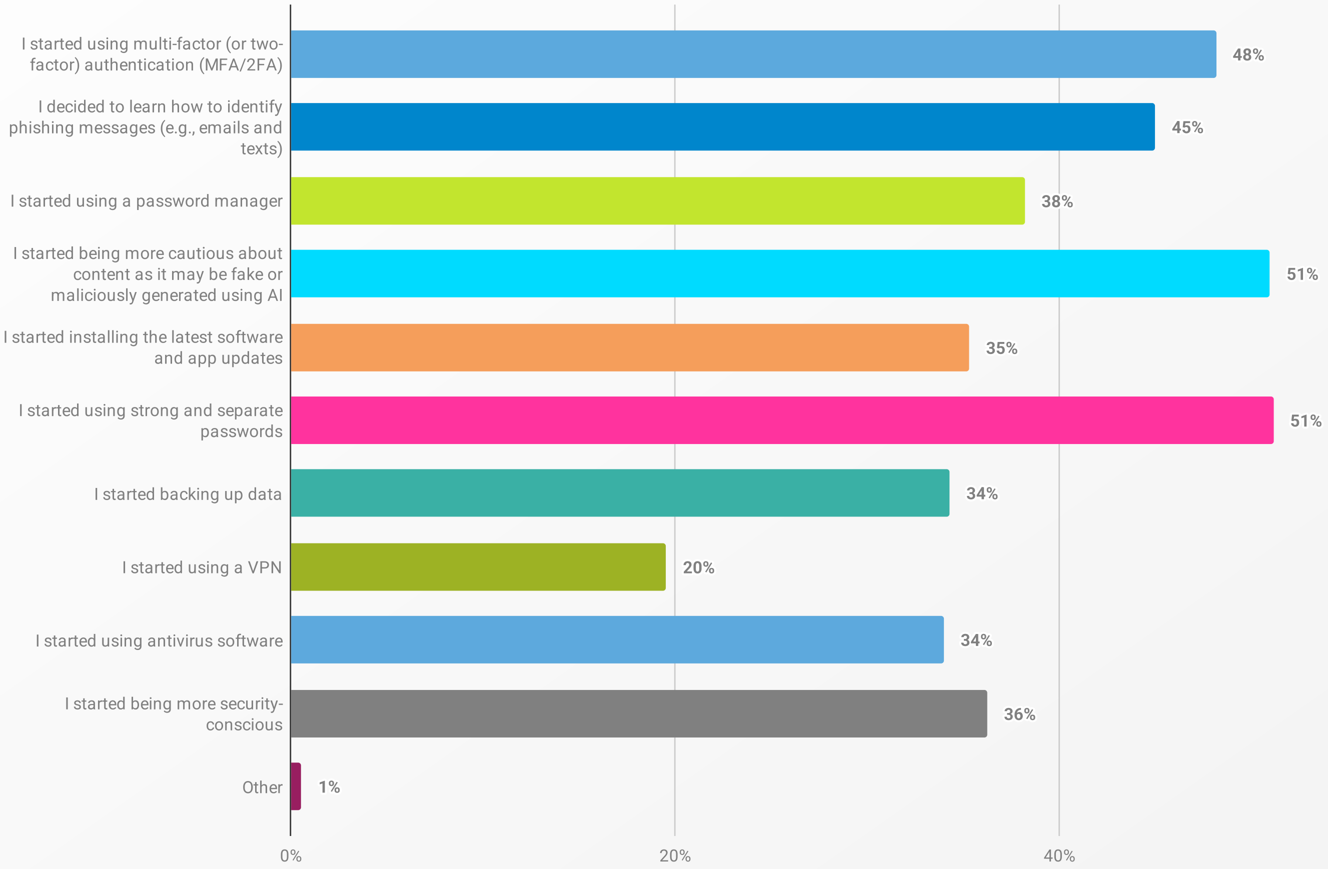
Figure 13. Impact of media coverage on motivating protective online security actions, by generation.



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

And what protective security actions do people take as a result of media coverage? Half of them reported using strong and separate passwords (51%), as well as being more cautious about content, especially with the rise of AI fakery (51%, Figure 14). Nearly as many said they'd begun using MFA (48%) and or made an effort to spot phishing messages (45%). And over a third (36%) ticked a new box we added this year: simply becoming more security-conscious overall.

Figure 14. Impact of media coverage on motivating protective online security actions.



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 5369 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

The media's influence on cybersecurity attitudes and behaviors is a mixed bag. On one hand, it fuels fear and makes security feel complex, but it also nudges people toward action. The growing impact on younger demographics is promising, as is its capacity to inform, but it continues to evoke fear and perceptions of complexity. This suggests that future awareness efforts could hit harder by tailoring media messages to resonate with these groups, encouraging practical actions like strong password use, MFA, and vigilance against AI-powered scams...

All of this leaves us with a big question though: If staying safe online isn't just about how people *feel*, who are they actually leaning on to keep them secure? Time to talk reliance and responsibility.

3. Are we in an accountability void?
Reliance & responsibility

Who do individuals turn to for help? Who relies on them? And where are the lines of accountability drawn? The answers to these questions are crucial for building effective, realistic strategies. These dynamics remind us just how interconnected digital safety can be, and how personal security often intertwines with the actions and perceptions of others.

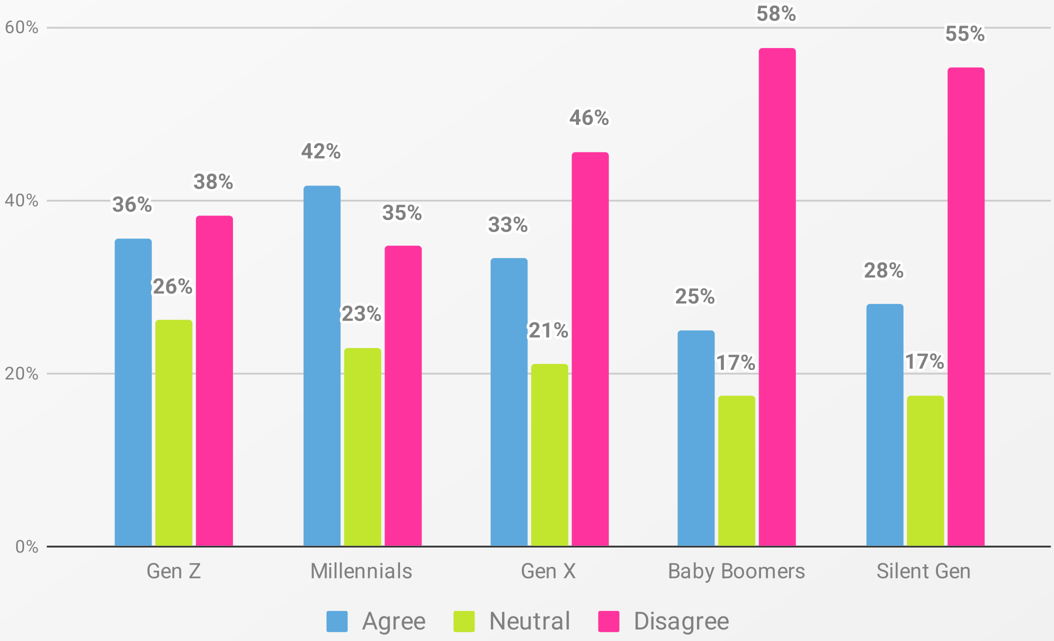
This chapter looks at the landscape of cybersecurity reliance and responsibility. We start with how people lean on others for their cybersecurity needs, and how much they are relied upon in return. Then we delve into perceptions of responsibility, dissecting who participants believe should ultimately be accountable for protecting both personal and workplace information.

3.1 'Not it!': Reliance on others for cybersecurity

Reliance on others for cybersecurity has nudged up to 35% this year (a 3% increase). This rise is sharpest among Gen X (33%, +4%) and Millennials (42%, +1%). Together with Gen Z (36%), they're the most reliant generations (Figure 15). Even so, 43% of all participants still reported not relying on anyone at all...

Among the 'reliant' group (N=3010), 45% lean on family, and 26% on IT companies.

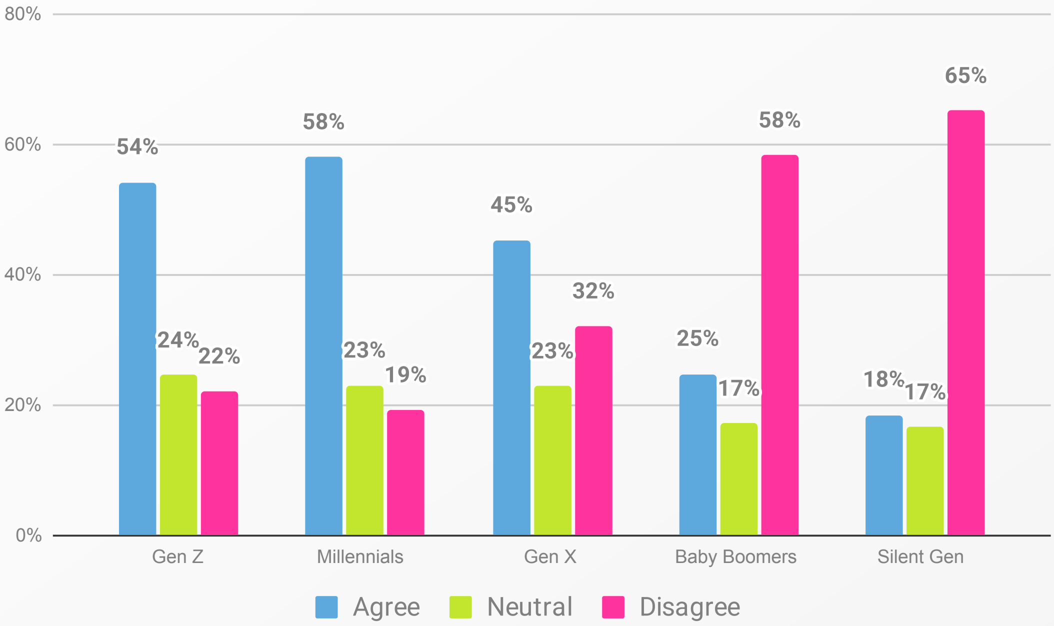
Figure 15. *'I rely on others (e.g., family, colleagues) to keep me secure online.'* by generation.



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

And it was also Millennials (58%, Figure 16) and Gen Z (54%) who reported being relied on by others for online security. Overall, reliance climbed 7% since last year, with nearly half (46%) saying others depend on them for online security.

Figure 16. '*Others (e.g., family) rely on me to keep them secure online.*' by generation.



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

In short, while more people are asking for help, the bigger story is how many are now giving help. Younger generations especially are becoming the designated cyber guru in their circles. That's a role that's rarely acknowledged but increasingly important. Future strategies should consider how to better support and empower these go-to defenders, and make sure they have the knowledge and tools to protect themselves and those who count on them.

> **I don't really know anything online. My daughter does it for me.** P21782, US

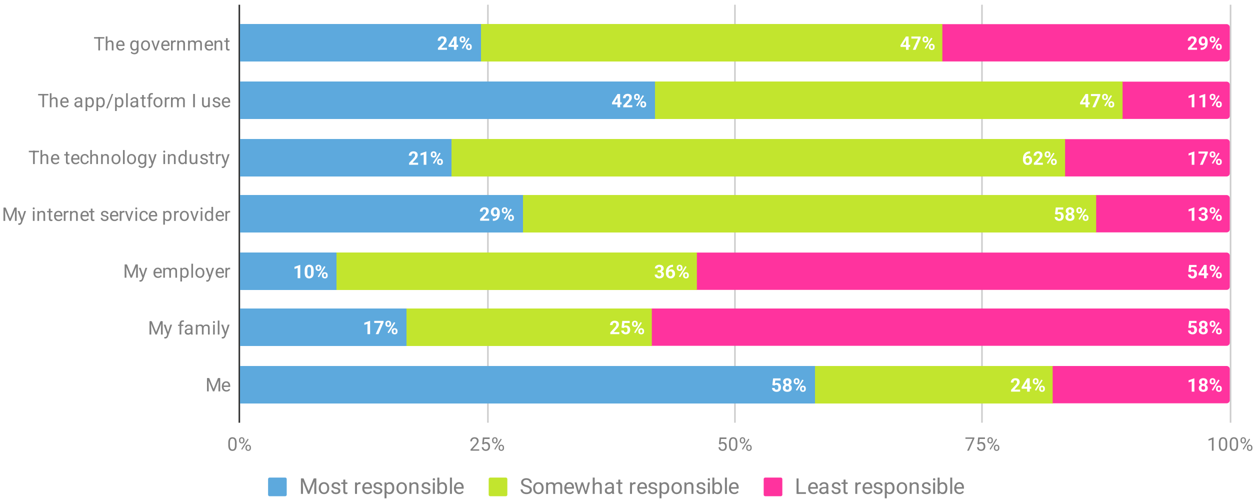
3.2 Praying to the firewall fairy: Responsibility for cybersecurity

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

As in 2024, people saw themselves as most responsible for protecting their own personal information (58%, Figure 17). But there's been a slight dip since 2024 in how responsible people feel, down 1% for personal security and 2% for workplace security (Figure 18).

Beyond themselves, people point to apps or platforms (42%) and internet service providers (29%).

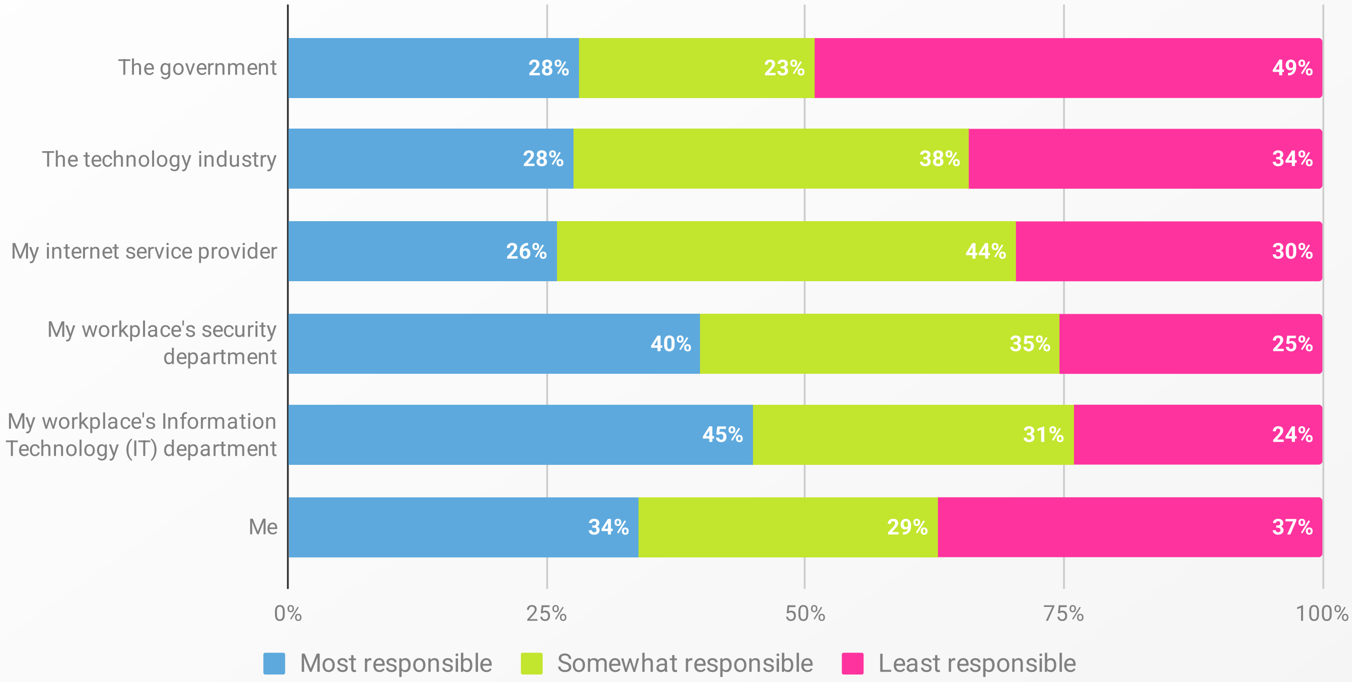
Figure 17. '*Who is most responsible for protecting your personal information?*'



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

For workplace information, people don't see themselves as the main line of defence. Instead, most point to the IT team (45%) and security department (40%). We hope you stretched before being handed that weight.

Figure 18. ***'Who is most responsible for protecting your workplace's information?'***



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 4555 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

Interestingly, perceptions of government responsibility ticked up: 24% for personal (+1%) and 28% for workplace information (+2%).

To wrap this chapter up, while individuals still see themselves as the main line of defence for their personal online security, there's a slow, steady drift into sharing the load. More people are pointing to external players, especially IT and security departments, as the real guardians in the workplace. That small rise in government responsibility points to a growing appetite for broader, systemic protection.

So if responsibility is a shared burden, what happens when the systems we lean on don't quite deliver? In chapter 4, we're going there.

4. Cybercrime victimization & reporting

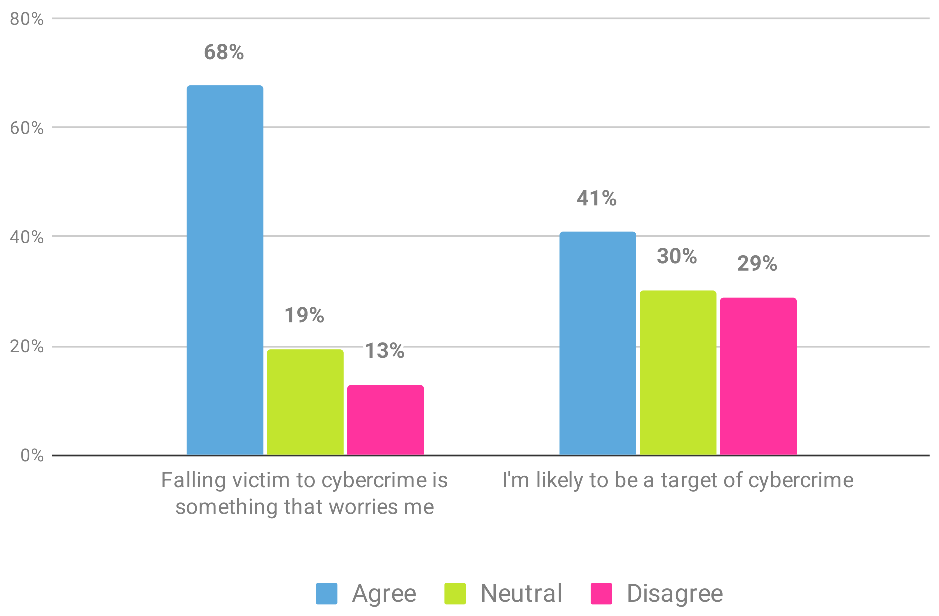
When it comes to cybercrime victimization, a crucial question arises: how do people truly perceive their risk and vulnerability? Do they see themselves as likely targets, and how much do they worry about cybercrime?

This chapter unpacks those attitudes, exploring beliefs about the inevitability of losing money or personal details online, and perceptions about the effectiveness of current cybercrime defenses. We also get into detailed victimization rates for various cybercrimes, including phishing, identity theft, and online dating scams. Plus, for the first time we've added deepfakes, cryptocurrency investment fraud, and tech support scams to the mix. On top of that, we dig into reporting rates, why many choose silence, and cyberbullying.

4.1 Is it paranoia if the stats back it up? Attitudes toward victimization

Let's start with exploring participants' attitudes toward being cybercrime victims. Around two-thirds of participants (68%) worry about becoming a cybercrime victim, up 7% from 2024 (Figure 19).

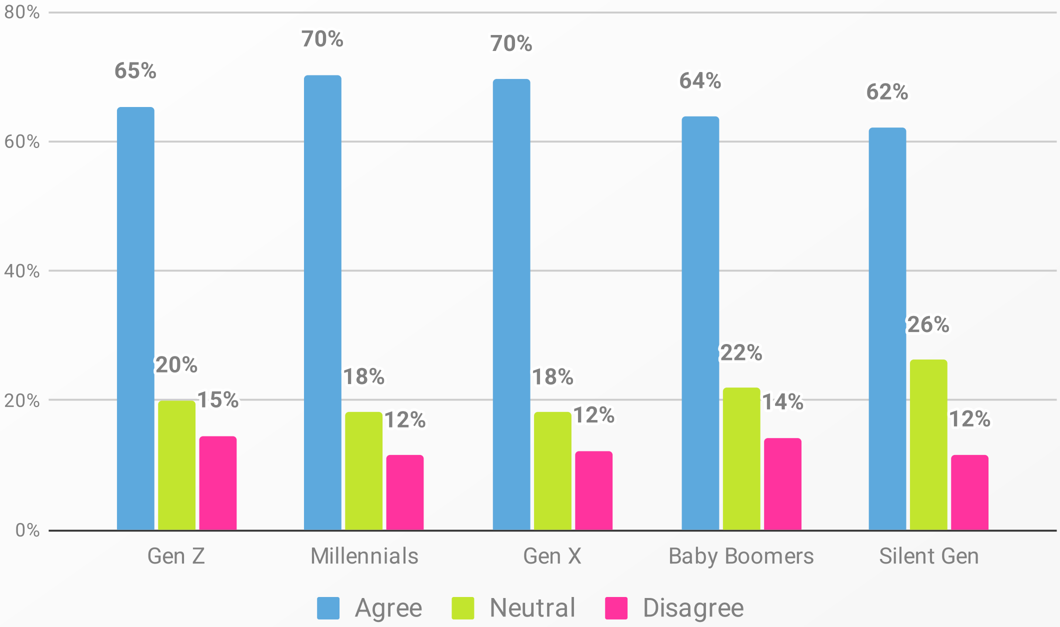
Figure 19. Attitudes toward victimization.



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

The worry cuts across all generations (Figure 20), but it's climbing fastest among the younger ones: Millennials and Gen X at 70% (up 6% and 10% respectively), and Gen Z at 65% (up 7%).

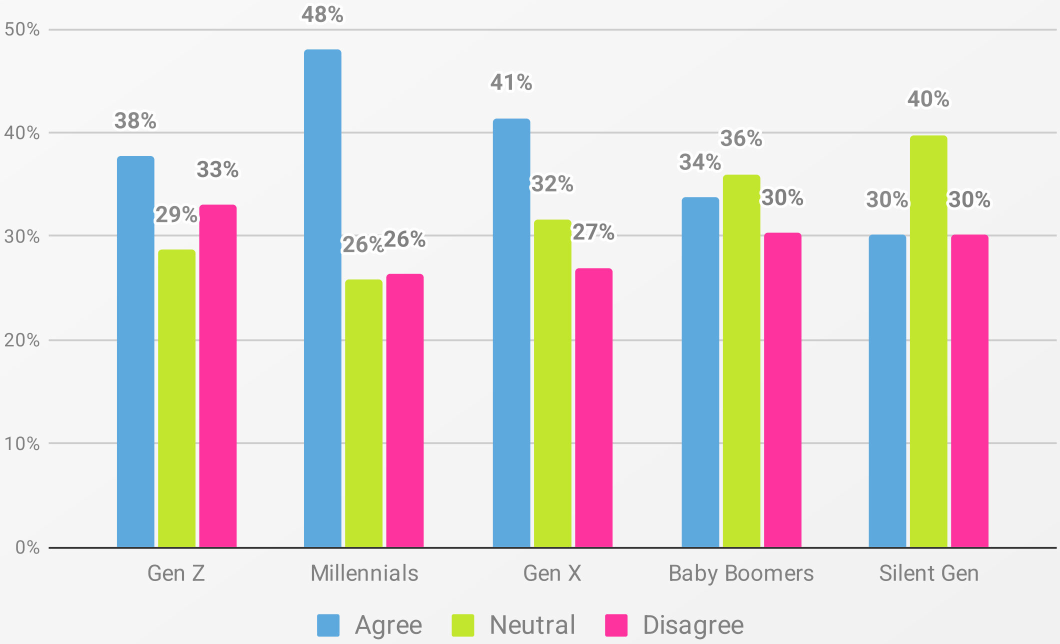
Figure 20. '*Falling victim to cybercrime is something that worries me.*' by generation.



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

In spite of the high levels of worry, only 41% considered themselves to be a likely target (-1% from 2024). What's interesting, though, is that while in 2024 the older generations topped the chart, this year it was the opposite. In 2025, Millennials are leading the pack (48%), followed by Gen X (41%) and Gen Z (38%, Figure 21).

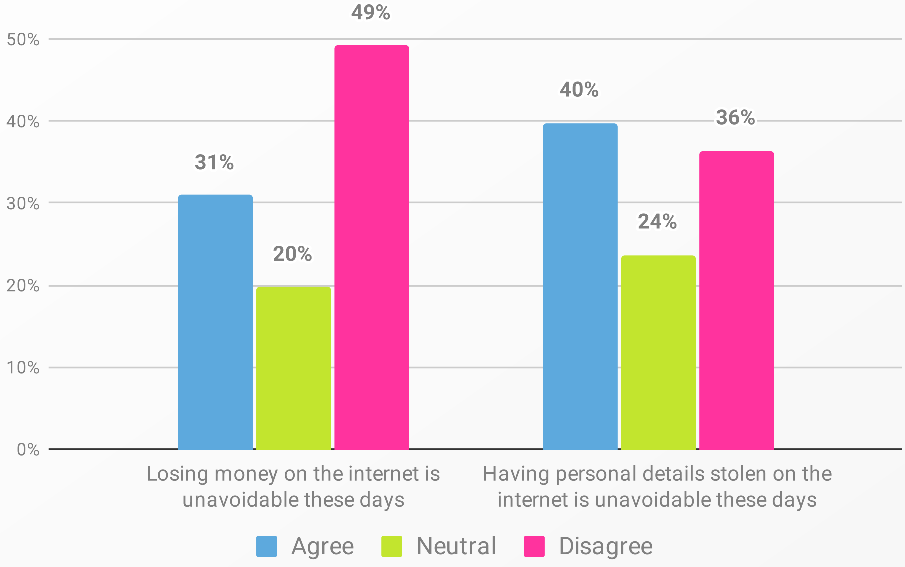
Figure 21. '*I'm likely to be a target of cybercrime.*' by generation.



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

Beliefs in inevitability are creeping up, too. The percentage of those believing that losing money (31%) and having personal details stolen (40%) on the internet is unavoidable has increased since 2024, by 3% and 2%, respectively (Figure 22).

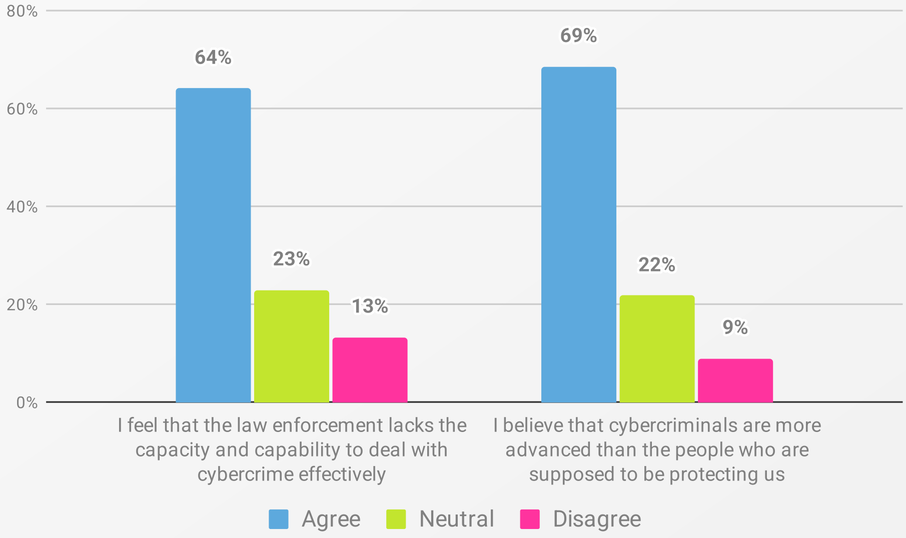
Figure 22. Perceptions on the avoidability of losing money or personal details on the internet.



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

When it comes to the perceived effectiveness of defenses against cybercrime, participants expressed skepticism (Figure 23). Sixty-four percent felt that law enforcement lacks the capacity and capability to deal with cybercrime effectively. Meanwhile, 69% believe that cybercriminals are more advanced than the cyber protector.

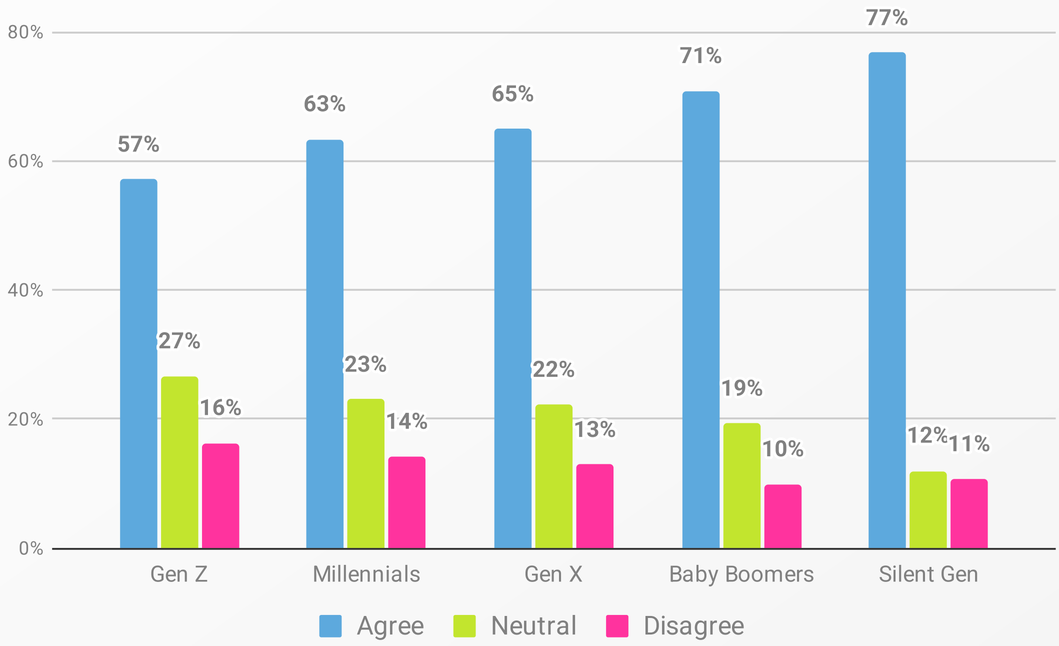
Figure 23. Perceptions of cybercrime defense effectiveness.



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

Among older participants, the sentiment was even sharper, particularly regarding the belief that law enforcement lacked the capacity and capability to effectively deal with cybercrime (Figure 24). Seventy-seven percent of the Silent Gen, and 71% of Baby Boomers felt that way, as opposed to 57% of Gen Z and 63% of Millennials.

Figure 24. '*I feel that the law enforcement lacks the capacity and capability to deal with cybercrime effectively.*' by generation.



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

> **I always feel as if scammers are one step ahead.**
> P21874, US

When it comes to cybercrime, we've found a classic 'it won't happen to me' paradox. Anxiety about cyber threats is definitely on the rise, especially for younger folks. But ask people about their own chances of being targeted, and that worry seems to disappear. Add in a growing fatalism about losses and skepticism about law enforcement, and you've got a recipe for helplessness.

What's more, if strategies are going to land, they'll need to do several things at once: raise awareness and empower people with a sense of agency, all while simultaneously building public trust in the capabilities of those tasked with combating cybercrime. Simple. 😅

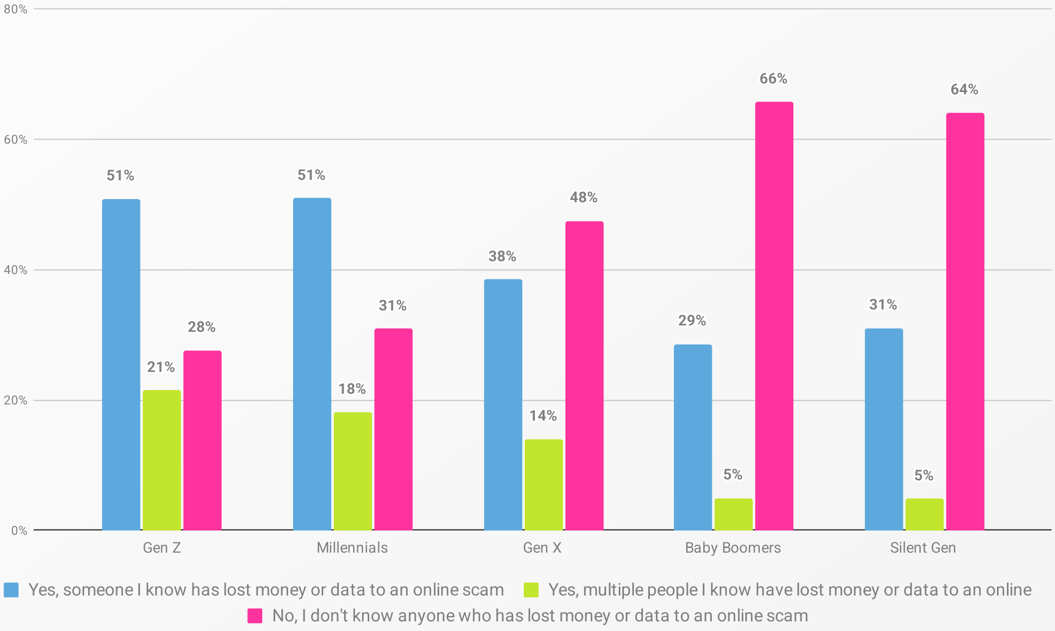
Next, let's take it from fears to facts. How often are people really getting hit?

4.2 Scams, scams, and more scams: Cybercrime prevalence

In previous reports, we tracked people's direct experiences with online scams. This year, we went a step further and asked if people knew others who'd been victims of online scamsthat led to money or data loss. Fifty-eight percent said yes, either one or multiple people in their circles had been cybercrime victims.

The generational breakdown provides a clearer picture (Figure 25). Younger generations' social circles were way more likely to be victims (72% of Gen Z, 69% of Millennials) than older ones (36% of Silent Gen, 34% of Baby Boomers).

Figure 25. '*Has anyone you know been a victim of online scams where they have lost money or data?'* by generation.



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

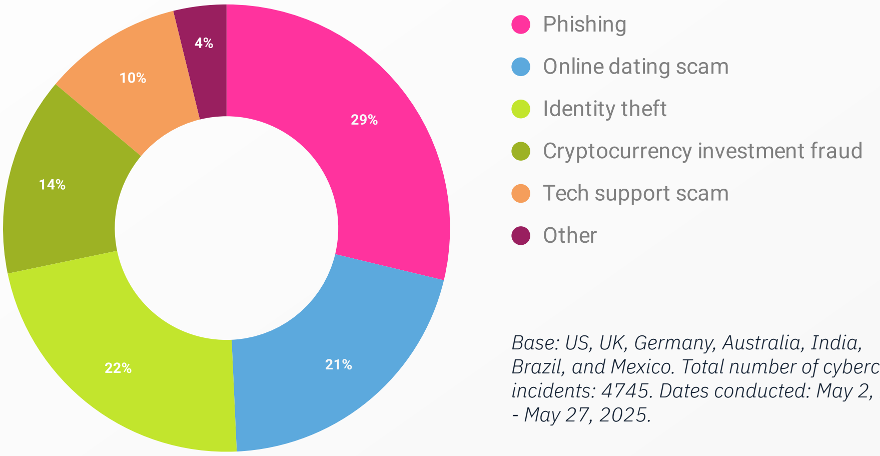
And what about the participants' victimization rates? They disclosed 4,745 cybercrime incidents[13] resulting in money or data loss, a jump of 1,399 from 2024. Overall, 44% of the participants had been victims of cybercrime, including phishing, online dating scam, identity theft, cryptocurrency investment fraud, tech support scam, and 'Other' scams. That's a 9% increase in just one year...

Phishing continues to dominate. Out of the 3,050 victims of online scams, nearly half experienced phishing crimes (45%), similar to previous years.

[13] This survey measured five specific types of cybercrime incidents: phishing scam, identity theft, online dating scam, cryptocurrency investment fraud, and tech support fraud. A free text 'Other' option was also provided to gather more insights and inform the cybercrime options provided in future *Oh, Behave!* reports.

Phishing also made up the highest share of all incidents (29%, Figure 26), followed by identity theft (22%) and online dating scams (21%). The new options – crypto investment fraud and tech support scam – accounted for 14% and 10% respectively.

Figure 26. Types of cybercrime incidents.



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of cybercrime incidents: 4745. Dates conducted: May 2, 2025 - May 27, 2025.

To dig deeper, this year we added the ‘Other’ option to the survey so people could tell us about scams not covered by the existing categories.

The responses revealed a diverse mix of online scam experiences, including unique instances such as rental fraud involving non-existent online advertisements, and fraudulent schemes related to selling goods internationally, where payment was never received.

Victims also reported encounters with extortion, deceptive fake loan offers, online survey scams, food delivery app scams, and a range of travel-related deceptions involving fake e-visas, airline tickets, and hotel reservations.

There were also mentions of shell company fraud, particular app/game scams, and even indirect data breaches stemming from real-world theft.

What does this crime buffet tell us? For one thing, it highlights the ever-expanding and specialized tactics employed by cybercriminals. But on the flipside, many of these diverse scams tie back to phishing tactics, such as deceptive emails or messages, to initiate contact and trick victims into engaging. It’s the trusty moneymaker that criminals just can’t quit, it seems.

> **I ordered a product after searching for it online. The website I used appeared legit, but when I tried to contact them after the product wasn’t delivered, I discovered the company didn’t exist and was a scam.** P2925, Australia

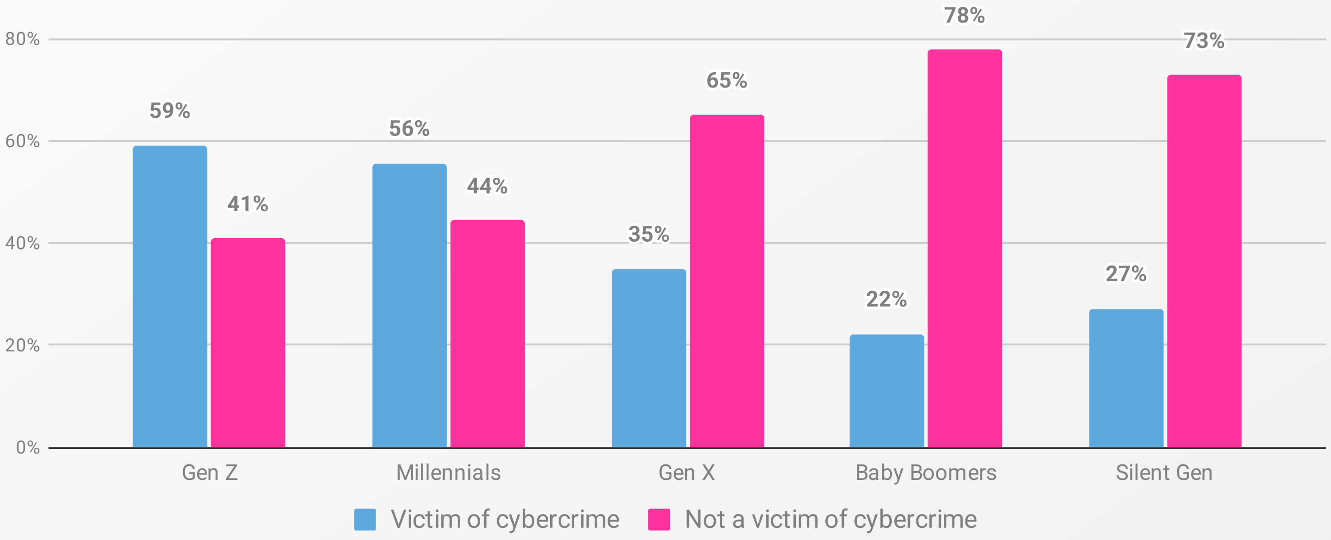
I was robbed of my Facebook account saying that I had won a prize. P16657, Mexico

After a theft at the 'Real' market and a subsequent hacker attack, my data was stolen. P18897, Germany

A PayPal payment was taken without my knowledge or consent." P2819, UK

Victimization is rising across all generations, but younger people bear the brunt (Figure 27). Fifty-nine percent of Gen Z reported having lost money or data due to online scams, followed by 56% of Millennials, which is a 7% and 10% increase from last year, respectively. Baby Boomers (22%) and the Silent Gen (27%) rates were lower, though still up 6% and 11%, respectively.

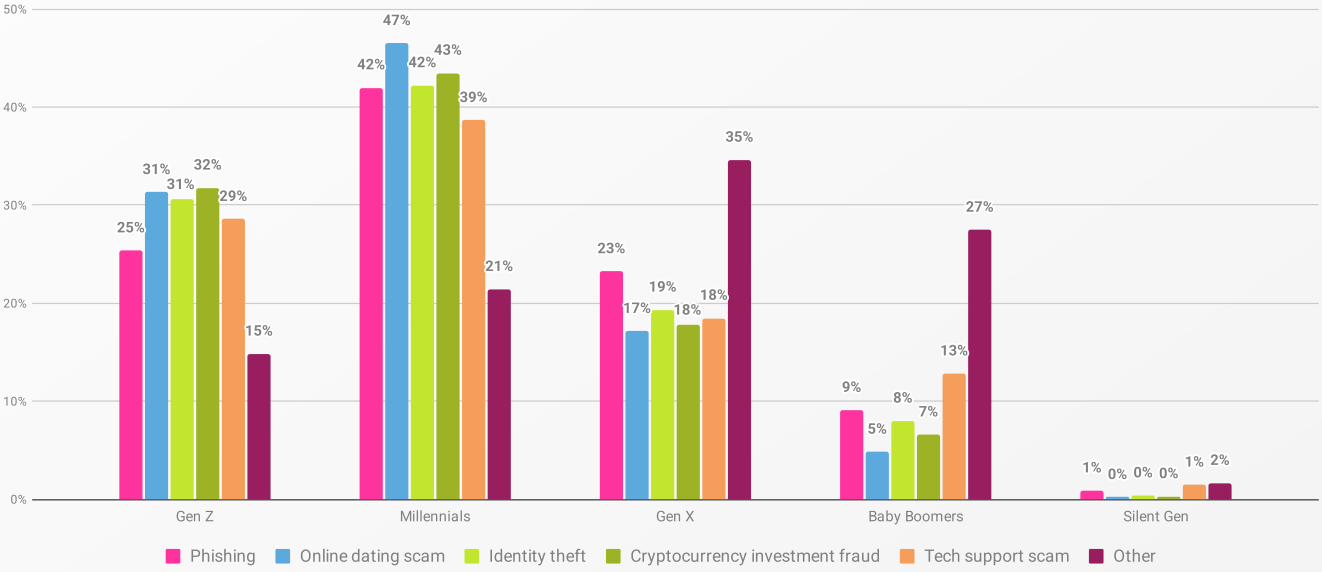
Figure 27. Victimization by generation.



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

And just like in previous years, Millennials top the charts across all five scam types that led to a loss of money or data (Figure 28), followed by Gen Z and then Gen X. To be exact, out of the total numbers of victims for each crime, Millennials accounted for 47% of online dating scam, 43% of crypto investment fraud, 42% of phishing and 39% of tech support scam victims. But hey, at least cybercrime is one industry that Millennials can't be accused of killing.

Figure 28. Cybercrime incidents by generation.



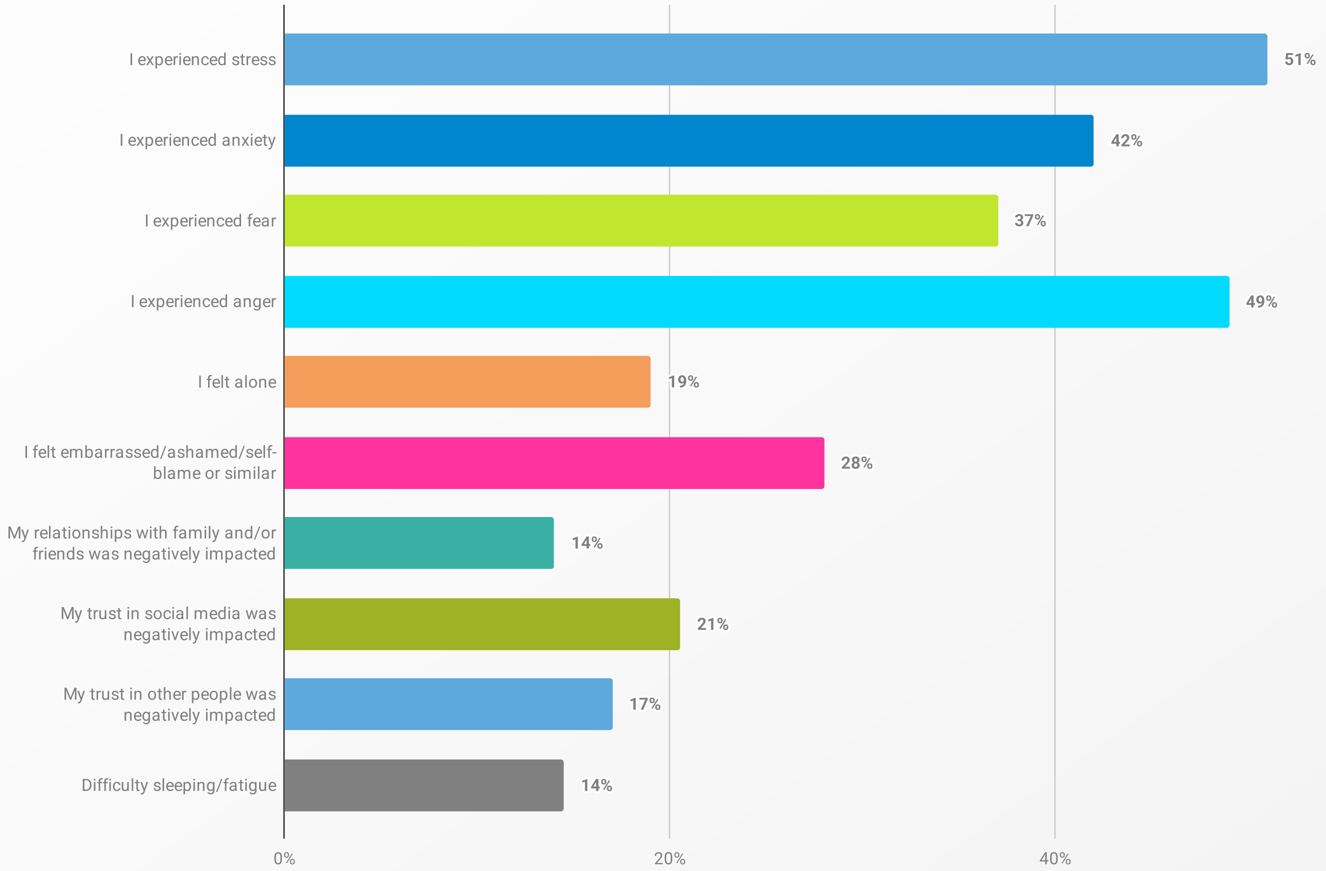
Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of cybercrime victims (age 18+): Phishing = 1364; Online dating scam = 974; Identity theft = 1066; Cryptocurrency investment fraud = 683; Tech support scam = 476; Other = 182. Dates conducted: May 2, 2025 - May 27, 2025.

For the first time this year, we asked people about the impact of their cybercrime victimization (Figure 29).

Around half of the victims reported experiencing stress (51%) and anger (49%) as a result, with a further 42% experiencing anxiety. Slightly over a third (37%) experienced fear as a result of the incident, and 28% felt embarrassed or ashamed. Twenty-one percent also admitted that their trust in social media was negatively impacted as a result of the online scam, where they had lost money or data.

These emotional aftershocks really matter to organizations, too. Their impact goes beyond the individuals, rippling into workplaces, social circles, and entire digital ecosystems.

Figure 29. '*Which, if any, of the following things happened to you as a result of the online scam where you have lost money or data?*'



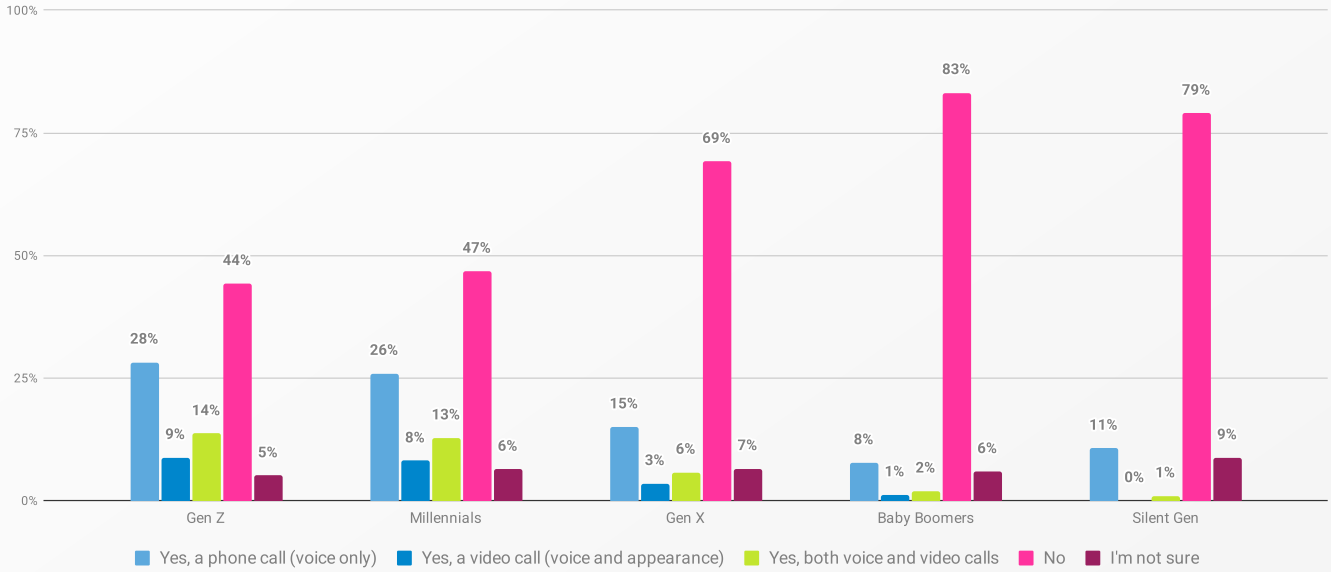
Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of cybercrime victims: 3050 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

And we didn't stop there. We also asked a few about their experiences with deepfake phone or video calls. Overall, 34% received a scam phone or video call where the caller perfectly mimicked someone they knew. Deepfake calls hit younger generations hardest (Figure 30), with 51% of Gen Z and 47% of Millennials receiving them, compared to 11% of Baby Boomers and 12% of Silent Gen.

[14] Sippy, T., Enock, F., Bright, J., & Margetts, H. (2025). *Behind the deepfake: 8% create; 90% concerned*. The Alan Turing Institute. Retrieved August 4, 2025, from https://www.turing.ac.uk/news/publications/behind-deepfake-8-create-90-concerned#:~:text=In%20terms%20of%20common%20targets,report%20being%20exposed%20to%20deepfakes

These findings on deepfake scam calls align with broader research showing just how exposed the public is to manipulated content. A report found younger people were more likely to report being exposed to deepfakes, from pornography to fraudulent scams[14]. This points to a growing challenge: telling real from fake is becoming harder every day, and AI's increasing sophistication is only sharpening the problem.

Figure 30. '*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 generation.

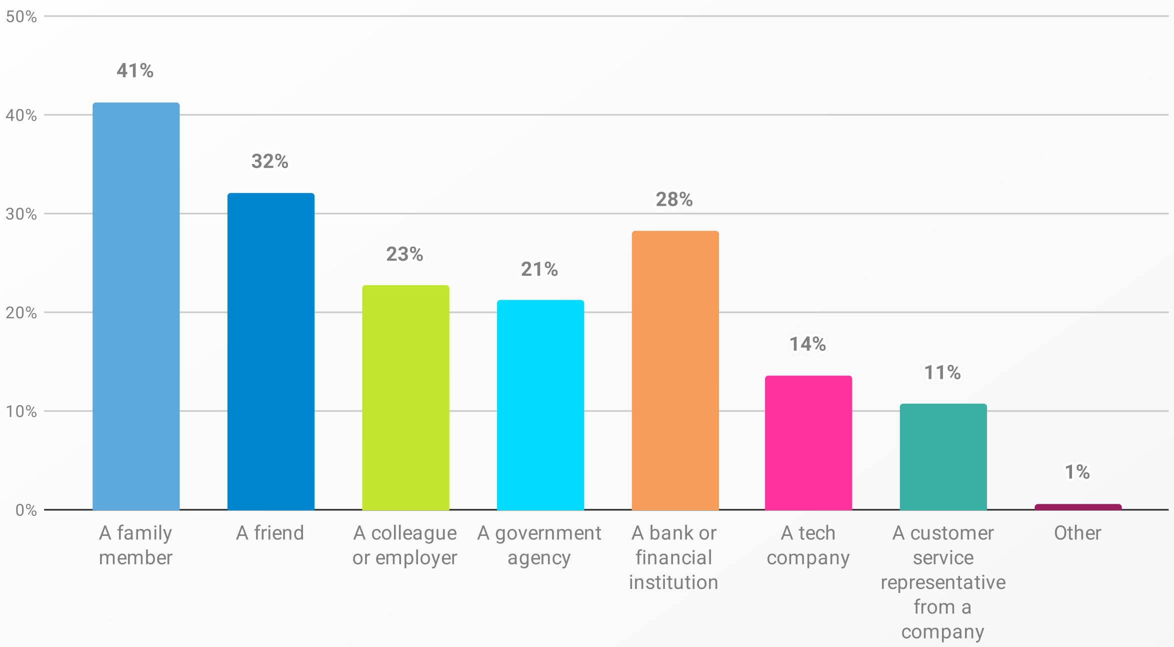


Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

And who did the caller pretend to be? Family members topped the list (41%), followed by friends (32%), and banks or financial institutions (28%, Figure 31).

> **[The caller pretended to be] my father. The call came from what seemed like the security at my parents' condo, and since they're elderly, it was especially frightening when the voice, which sounded just like my dad, said their home was being robbed.** PS12984, Brazil

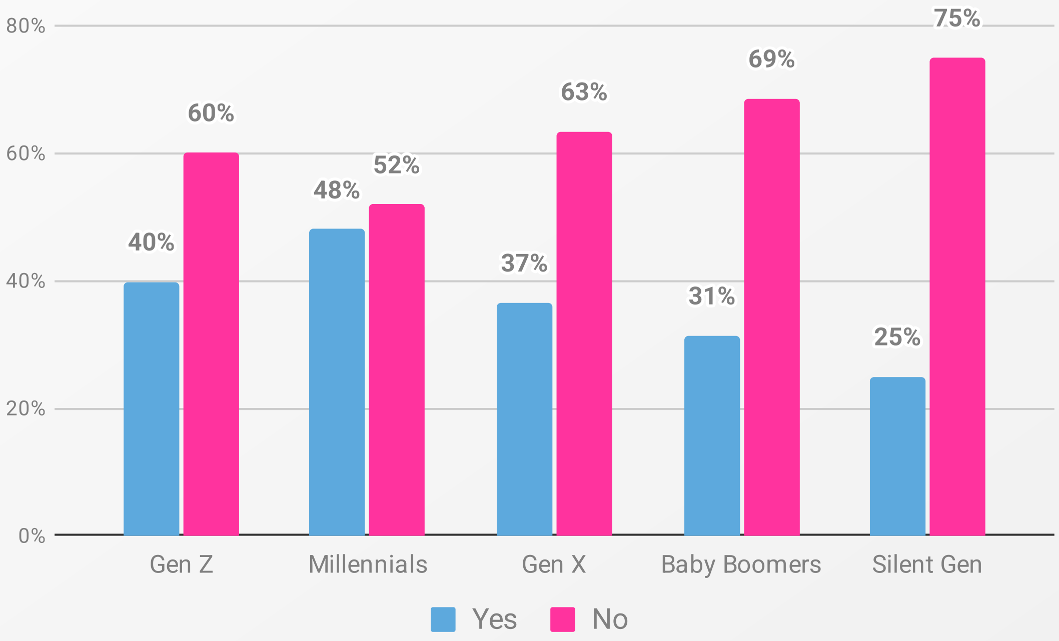
Figure 31. ‘*Who did the caller pretend to be?*’



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 2361 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

Among those who received deepfake calls (N=2361), 42% lost money or data as a result of the scam. Younger generations were hit hardest: almost half of the Millennials and 40% of Gen Z lost money in a deepfake scam (Figure 32).

Figure 32. ‘*Did you lose money or data as a result of the deepfake voice or video call you received?*’ by generation.



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 2361 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

In conclusion, the prevalence of cybercrime is still on the rise. Not only are more individuals personally falling victim to online scams, but younger generations' social circles are more likely to include cybercrime victims.

Phishing remains the biggest threat, but the rise of diverse 'other' scam types shows how fast the landscape is evolving. With younger people being targeted more often, and the heavy emotional fallout (stress, anger, anxiety) they report, the problem is impossible to ignore.

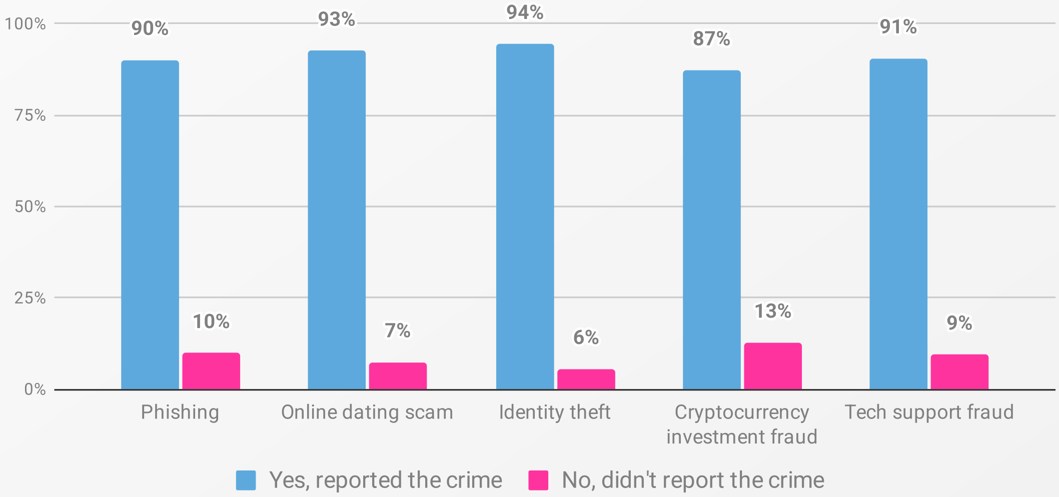
These insights suggest that future cybersecurity efforts must not only focus on broad prevention but also on equipping people with the resilience and specific knowledge to navigate increasingly personalized and emotionally impactful cyber threats.

Of course, being a victim is only half the story. The real question is: do people actually report it?

4.3 Dial M for malware: Cybercrime reporting

Overall, reporting rates were high across crime types, with 91% of cybercrime incidents being reported by victims. On average, 90% (+1% from 2024) of phishing incidents, 93% (+1% from 2023) of online dating scams, 94% (+2% from 2024) of identity theft incidents, 87% of crypto, and 91% of tech support fraud incidents were reported (Figure 33).

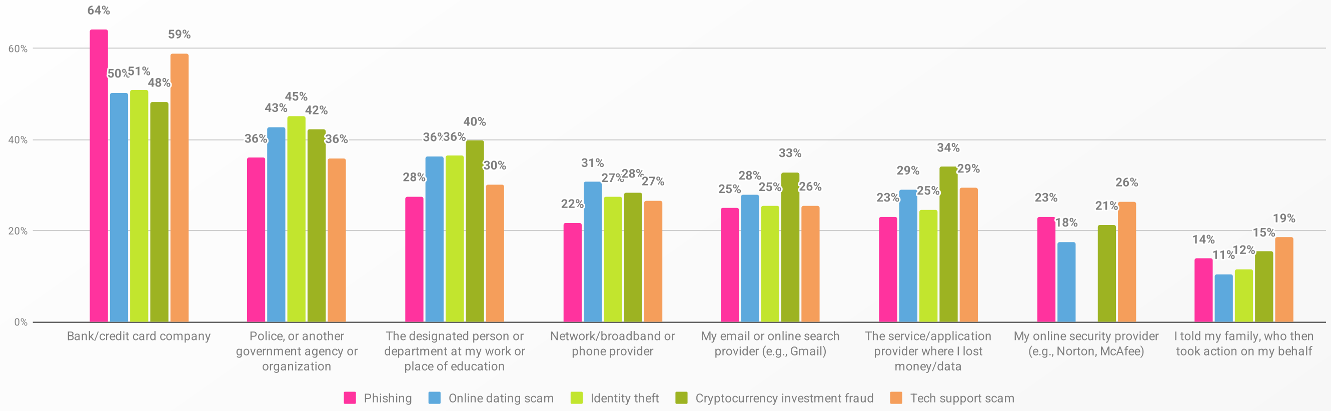
Figure 33. Crime reporting frequency by crime type.



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of cybercrime victims (age 18+): Phishing = 1364; Online dating scam = 974; Identity theft = 1066; Cryptocurrency investment fraud = 683; Tech support scam = 476. Dates conducted: May 2, 2025 - May 27, 2025.

Most victims turned to their bank or credit card company (Figure 34), followed by the police, or another government agency or organization.

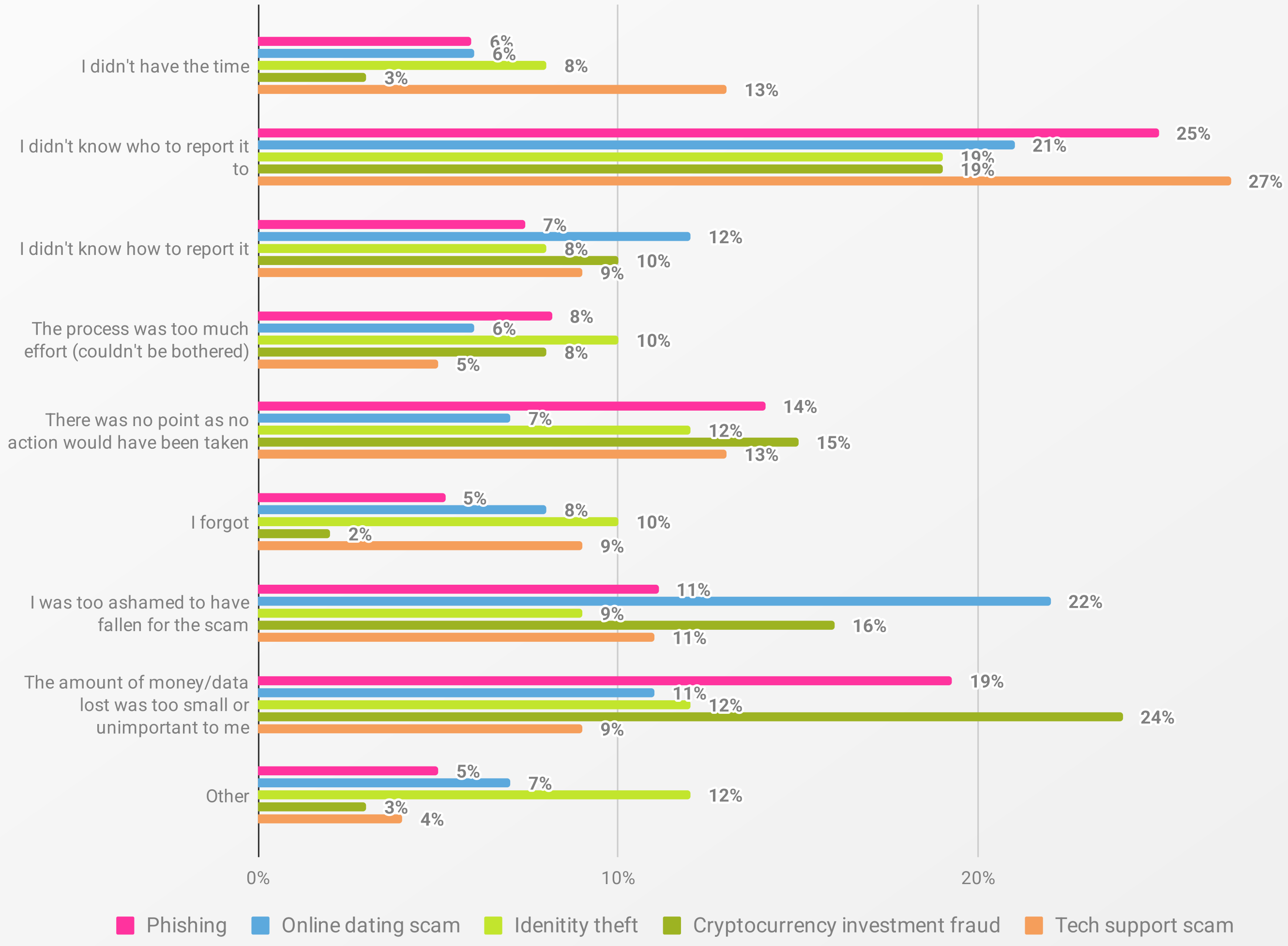
Figure 34. Who were the cybercrimes reported to?



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants (age 18+) who had reported cybercrime: Phishing = 1229; Online dating scam = 902; Identity theft = 1007; Cryptocurrency investment fraud = 596; Tech support scam = 431. Dates conducted: May 2, 2025 - May 27, 2025. Multiple-choice question. 'My online security provider' wasn't provided as a choice for victims of identity theft.

But what about the people who kept quiet (Figure 35)? The biggest reason for not reporting was simply not knowing who to report to for phishing (25%), identity theft (19%), and tech support scam victims (27%). Victims of online dating scams felt too ashamed to report (22%), and those of crypto investment fraud (24%) didn't report because the amount of money lost was too small or unimportant to them.

Figure 35. Reasons given for not reporting incidents, by crime type.



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants (age 18+) who had not reported cybercrime: Phishing = 135; Online dating scam = 72; Identity theft = 59; Cryptocurrency investment fraud = 87; Tech support scam = 45. Dates conducted: May 2, 2025 - May 27, 2025.

The following quotes, highlighted from the qualitative findings of the 'Other' response option, further illustrate the reasons for not reporting and the deep-seated frustrations with official channels:

> **I've needed various agencies/bodies multiple times. They work when they want, which is never.** P13632, Brazil

> **The authorities don't do their job as they should, and the process is too long.** P14963, Mexico

> **I'm not wasting my time asking for favors from any public agency anymore; that's just how they operate. I'm done with it. There's nothing that forces them to function. I've already called the police for various reasons many times, and they eternally claim they don't have enough staff at the moment. Now, just try delaying their salary, and you'll see.**
> P13632, Brazil

> **I don't trust many public agencies/bodies, because I've contacted several of them multiple times and none of them showed any interest.** P13632, Brazil

> **I didn't report [the scam], nor did I seek any public help, because they don't do their job.** P13632, Brazil

In conclusion, the strong and consistent willingness to report cybercrime is a bright spot in an otherwise bleak landscape. People are clearly taking action, but to encourage more, we need to address persistent barriers such as a lack of clarity on reporting channels, the emotional toll leading to shame, and the idea that small losses don't matter. (Spoiler: they do.)

But scams aren't the only way people get hurt online. Cyberbullying continues to carve deep scars. And unlike losing money, the damage can't always be refunded.

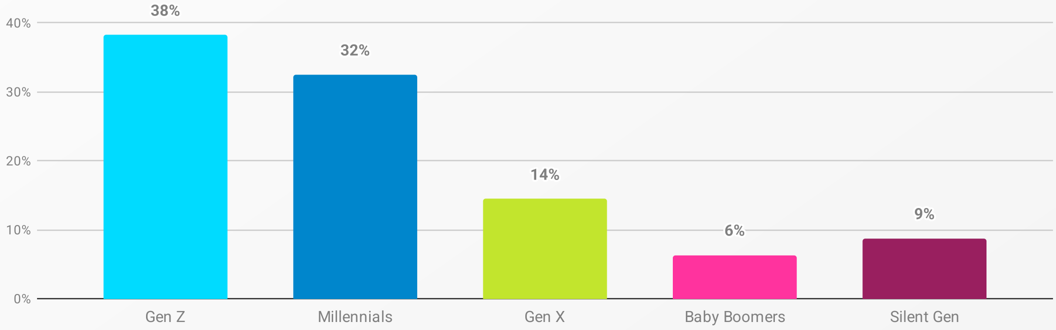
4.4 Mean tweets: Cyberbullying

Cyberbullying remains a serious concern, cutting across all age groups. This section delves into how common it is among our participants, how rates have shifted since last year, where victims turn for help, and how reporting behaviors are evolving.

Across all participants, 23% (N=1622) reported being victims of cyberbullying. That represents a 5% increase from 2024. So far, so bleak.

The highest rates were among young people, with 38% of Gen Z and 32% of Millennials reporting they have been cyberbullied (Figure 36). Overall, older age groups reported lower numbers of cyberbullying, though the percentages slightly increased for Gen X (+2% from 2024), Baby Boomers (+3% from 2024), and the Silent Gen (+5% from 2024).

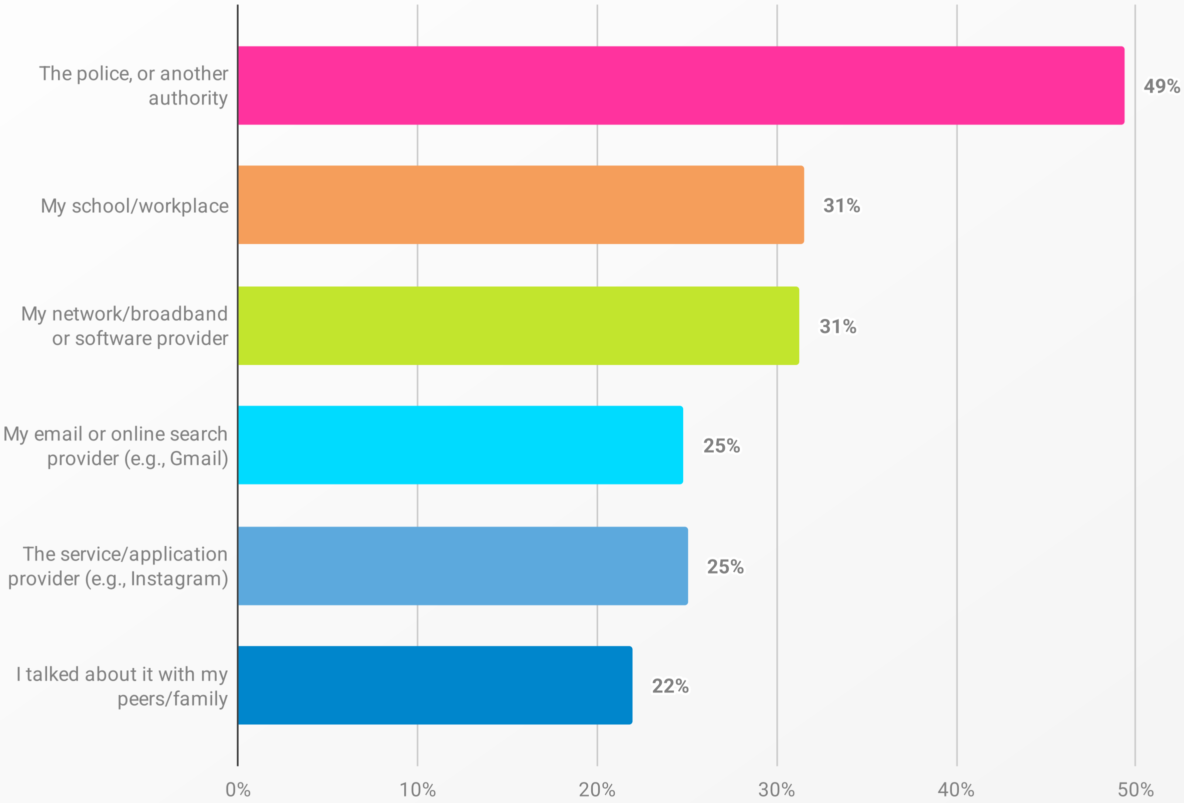
Figure 36. Victim of cyberbullying, by generation.



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of cyberbullying victims: 1622 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

When it came to reporting, just under half of victims (N=1435) reported it to the police, or another government agency or organization (49%, Figure 37). That's an 8% jump on last year. But reports to other avenues dropped: schools and workplaces are down to 31% (-6 from 2024), while family fell slightly to 22% (-1%).

Figure 37. Agencies where cyberbullying is reported to.



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of cyberbullying victims who reported the incident: 1435 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

In conclusion, cyberbullying victimization continues to rise across all generations, with younger age groups bearing the worst of it. Most victims are turning to formal authorities, which is a positive shift, but support networks like schools, workplaces, and families are seeing fewer disclosures. It's a mixed bag of progress and gaps, where people are speaking up more, but not always in the places that might provide day-to-day support.

So, yes, the trolls are thriving. In the struggle against the bad guys, training's supposed to be a golden shield... except, does anyone actually believe it works? Let's find out next.

5. Lessons (un)learned? Cybersecurity training

Back in the day, cybersecurity training was all about compliance – regurgitating stuff in policies with a focus on everybody finishing it so the auditor was happy. But today it's about access, format, and whether it actually changes behavior. In this chapter we look at who gets training, how often, what formats people prefer, and why many still skip it. We also explore whether training shifts real-world habits... or if it's just another tick-box exercise.

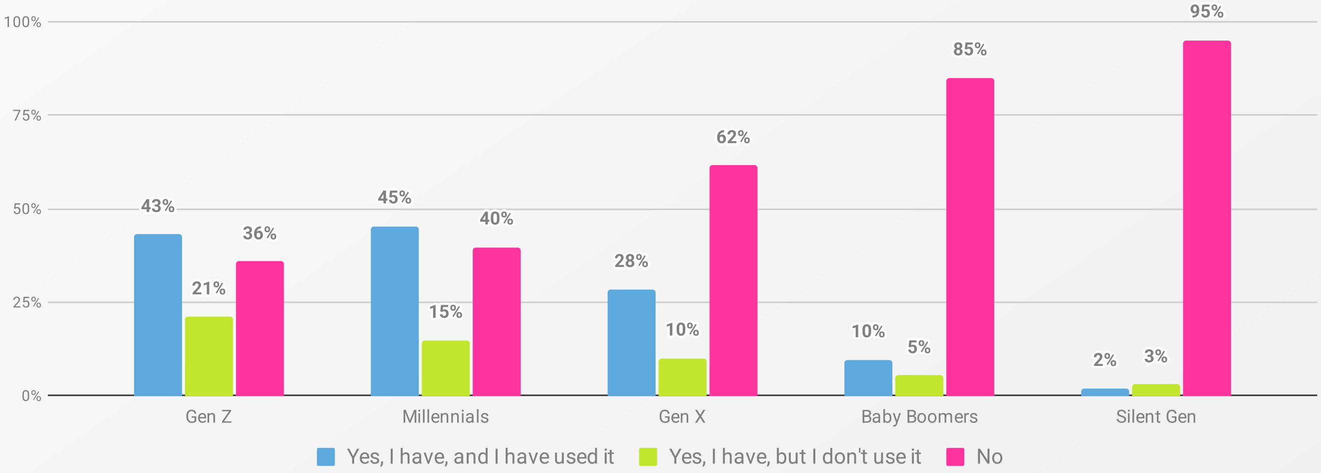
5.1 Enrolled or exposed? Access to training and prevalence of mandatory training

Only 32% reported having access to and using cybersecurity training, a minor 1% decrease from 2024. Thirteen percent said they didn't use the training they had access to (+2% from 2024). And still, slightly over half of the respondents (55%) don't have access to cyber training.

Access dipped slightly since 2024, but younger generations remain ahead (Figure 38): 48% of Millennials and 43% of Gen Z, compared to 10% of Baby Boomers and 2% of Silent Gen.

Training access and completion were also higher among employed participants, with 44% (same as 2024).

Figure 38. '*Do you have access to cybersecurity training (e.g., at work, school, or library)?*' by generation.



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

We took it a step further by examining the responses through a sector breakdown (Figure 39). Over half of the participants within the following sectors had access to and used training:

- Information technology and telecommunications (64%)
- Mining, quarrying, and utilities (60%)
- Finance and insurance (58%)
- Nonprofit and charity organizations (50%)

Sectors with the highest percentage of those without access to training were:

- Other sectors, including options not listed in the sectors provided (61%)
- Retail and wholesale trade (56%)
- Hospitality and tourism (55%)
- Arts, entertainment, and recreation (49%)

And sectors with the highest percentage of those opting not to use cyber training in spite of having access to it were marketing, advertising, and public relations (23%) and education (19%). It seems hardest to 'sell' training to sellers, and hardest to teach it to teachers. If you need us, we'll just be over here, screaming into a cushion.

But this really matters. A clear majority of participants in the retail and wholesale (56%) and hospitality and tourism (55%) sectors reported having no access to training. This lack of preparation suggests that many organizations aren't adequately equipping their employees to defend against cyber threats, potentially leaving out those who don't work in front of a computer all day.

This gap in awareness has already been exploited by threat actors in several recent high-profile breaches. UK retail giant *Marks & Spencer (M&S)*[15] was hit by a ransomware attack after criminals social-engineered a third-party vendor. Impersonating staff, they persuaded help desk workers to reset credentials, giving them direct access to M&S systems, later encrypted by the DragonForce ransomware group. *Harrods*[16] and *Co-op*[17] were also targeted in the same wave of coordinated attacks, which relied heavily on social engineering tactics.

[15] BBC News. (2025, May 1). *Marks and Spencer hit by cyber attack*. Retrieved August 5, 2025, from https://www.bbc.co.uk/news/articles/c0el31nqnpvo

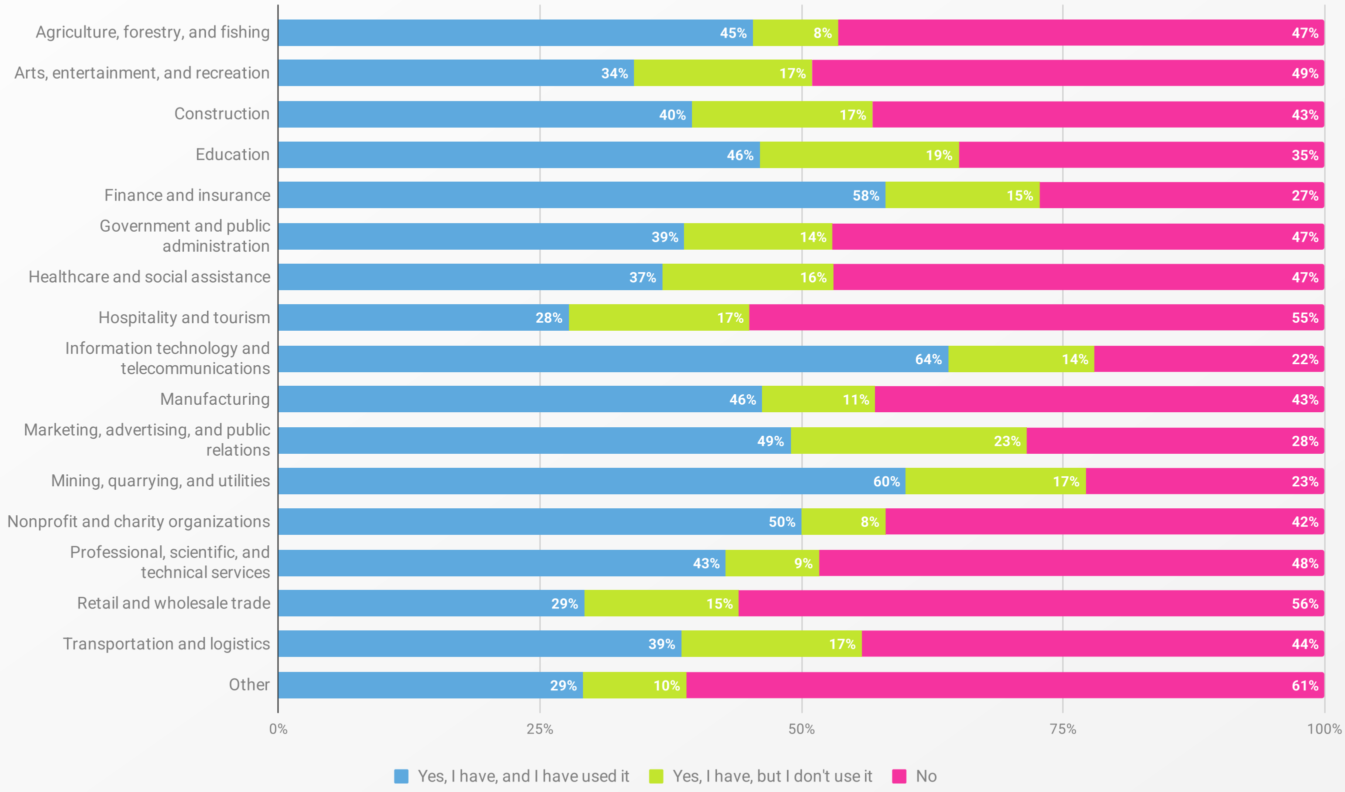
[16] BBC News. (2025, May 1). *Harrods latest retailer to be hit by cyber attack*. Retrieved August 5, 2025, from https://www.bbc.co.uk/news/articles/c62x4zxe418o

[17] BBC News. (2025, July 16). *Co-op boss confirms all 6.5m members had data stolen*. Retrieved August 5, 2025, from https://www.bbc.co.uk/news/articles/cql0ple066po

United Natural Foods (UNFI)[18], a major US food distributor, suffered a cyberattack that disrupted critical systems, and left grocery store shelves empty. Even *Adidas*[19], the international athletic apparel and footwear company, suffered a data breach via a third-party customer service provider. In this case, attackers accessed customer contact details, while payment information remained secure.

Together, these incidents show a clear pattern: neglect human risk management and you leave the door wide open to criminals. This reminds us that training and behavioral interventions aren't cute fluffy extras. When you ignore the human element, human cyber risk will come for you.

Figure 39. '*Do you have access to cybersecurity training (e.g., at work, school, or library)?*' by sector.



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

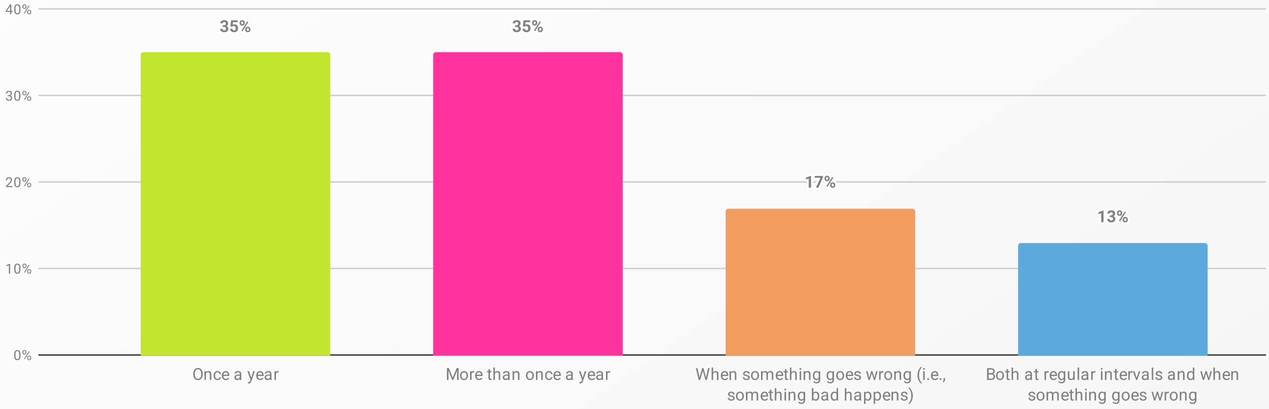
[18] Forbes. (2025, June 16). *What The Cyberattack On UNFI Reveals About The U.S. Grocery Industry*. Retrieved August 5, 2025, from https://www.forbes.com/sites/errolschweizer/2025/06/16/what-the-cyber-attack-on-unfi-reveals-about-the-us-grocery-industry/

[19] BBC News. (2025, May 27). *Adidas says customer data stolen in cyber attack*. Retrieved August 5, 2025, from https://www.bbc.co.uk/news/articles/c071m82v80po

We asked employed participants if cybersecurity training is mandatory at their workplace, and 49% said yes.

Out of those who have to complete training (N=2249), 35% are completing it more than once a year (Figure 40), which is a 9% increase from 2024. The number who only get trained when something goes wrong also rose, up 9% to 17%.

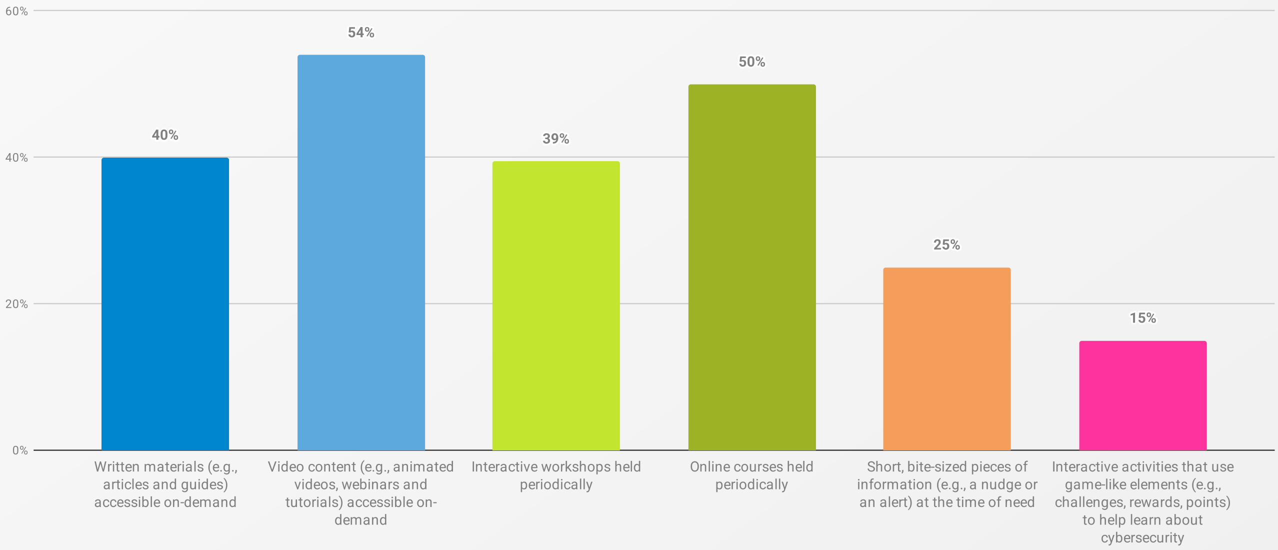
Figure 40. '*How often are you required to complete training?*'



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 2249 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

This year, we also asked those required to complete mandatory training about the formats used (Figure 41). The highest percentage received their cyber training in video content (54%), followed by periodic online courses (50%), and written materials (40%). TL;DR: Ditch the PowerPoints, load up on popcorn.

Figure 41. Cybersecurity training formats used by organizations.



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 2249 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

So, while some of the population engages with training, over half still lack access, particularly in sectors like retail and hospitality, which ironically face high-profile breaches. And although mandatory training's on the rise, the sheer number of breaches linked to human behavior shows that access and box-ticking aren't enough on their own.

The preference for dynamic formats like video content suggests that the way forward is more engaging and effective training delivery. This also emphasizes the critical need for targeted, relevant, and consistent investment in efforts to manage human cyber risk in organizations.

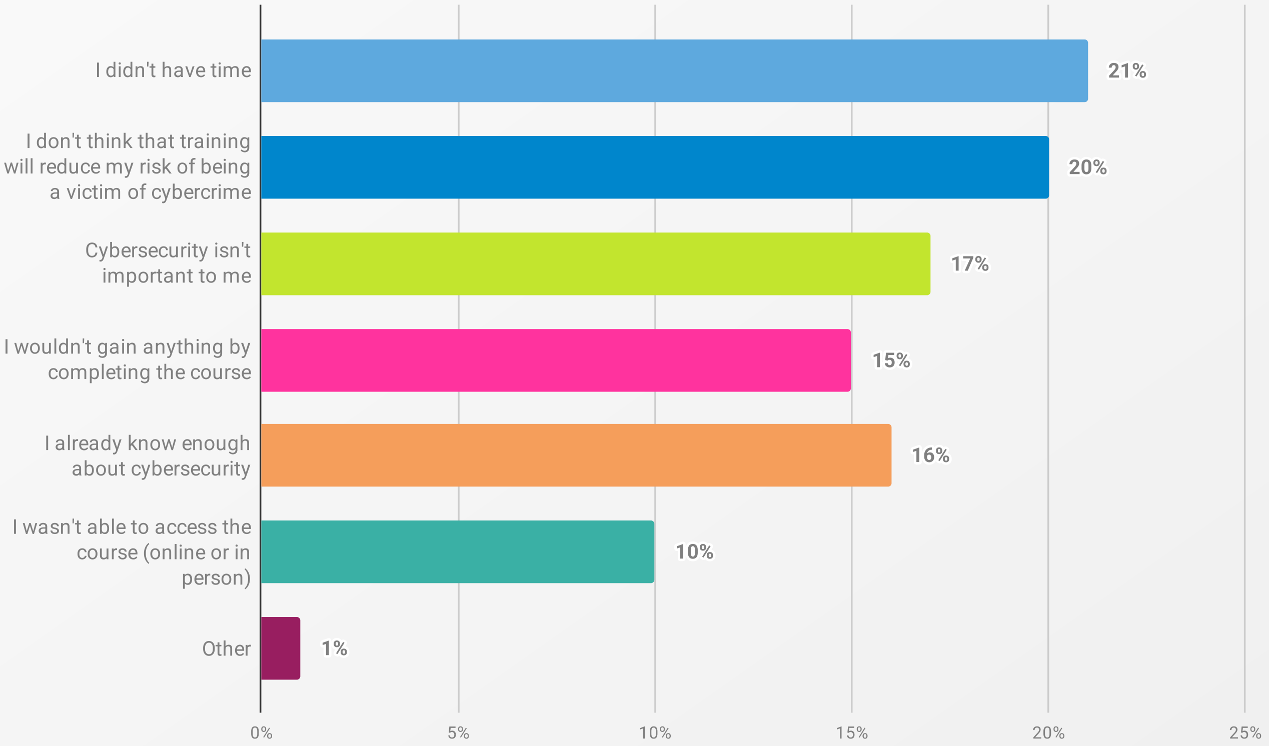
It's clear that pressing play is easy, while building resilience takes work. But even when training's on the table, plenty of people still push their plate away.

5.2 The dog ate my login: Barriers to attendance

For those with access to training but skipping it (N=893), we explored their reasons (Figure 42). In 2024, most skipped training because they felt they already knew enough. This year, only 16% gave that as a reason (down 7%).

This year, the number one reason was not having enough time (21%, -1% from 2024), closely followed by doubting that training actually lowers risk (20%, same as in 2024). Interestingly, the percentage of those not doing training because cybersecurity isn't important for them has increased by 5% to 17%.

Figure 42. '*What is the main reason you didn't use the opportunity to attend a cybersecurity training course?*'



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 893 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

The biggest barrier has shifted from 'I know enough already' to 'sorry, too busy'. But disbelief in training's impact and a growing sentiment that cybersecurity isn't important show a real need for more relevant, time-efficient, and impactful educational approaches.

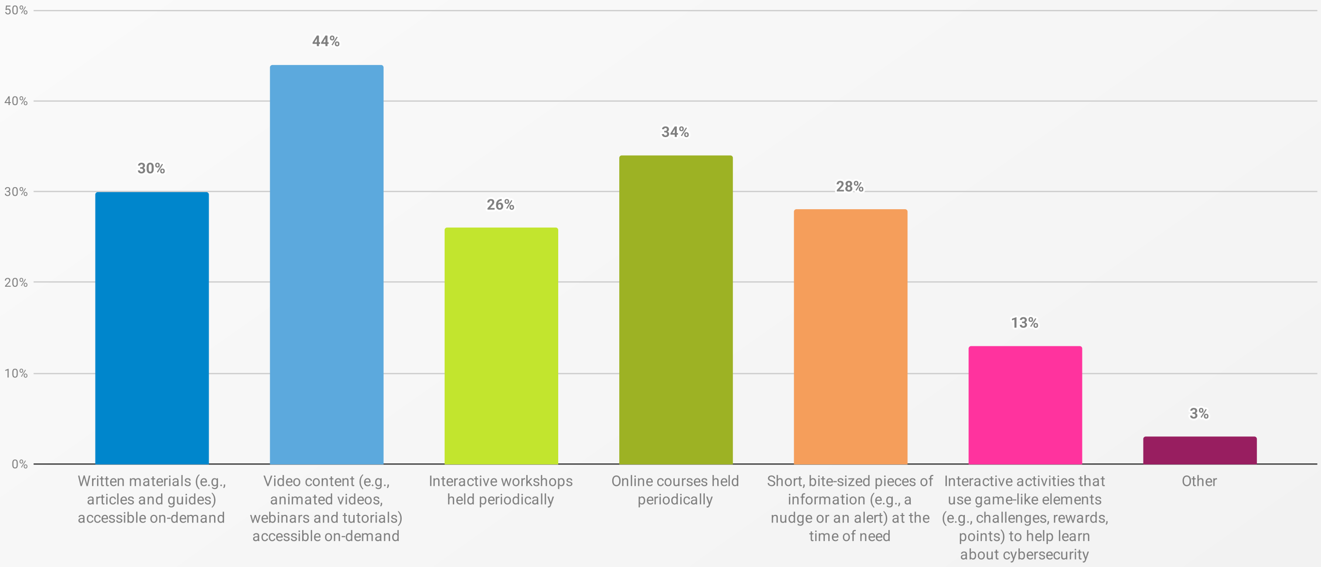
Research[20] backs this up too: lack of time is a major barrier. It also suggests training's real value may be its 'nudging effect' – reminders rather than content that is consumed in a chunk. This means it pays to deploy training that's bite-sized and time-friendly.

Which naturally brings us to the question: If people are going to engage, what training formats do they actually want?

5.3 **Binge it or bin it?** Preferred training formats

When it comes to training formats, video still leads the pack (44%), followed by periodic online courses (34%), and written materials (30%), as shown in Figure 43. That order hasn't changed since 2024. At the bottom of the list are interactive activities that use game-like elements (13%), the same as last year, despite us clarifying the wording to 'online games or gamified experiences' this year.

Figure 43. '*What format do you prefer to consume cybersecurity training information?*'



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

But does age make a difference to these preferences? Absolutely. Video is most popular among younger generations (Gen Z and Millennials at 51%) but enthusiasm drops sharply with age (e.g., Silent Gen at 15%, Figure 44). Older groups lean toward written materials, with the Silent Gen and the Baby Boomers both at 32%. Preference for short, bite-sized information appeals most to Baby Boomers (29%) and Gen X (28%). Preference for online courses was highest among Millennials (39%) and Gen X (36%).

[20] Lain, D., Jost, T., Matetic, S., Kostiainen, K., & Capkun, S. (2024, December). Content, Nudges and Incentives: A Study on the Effectiveness and Perception of Embedded Phishing Training. In *Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security* (pp. 4182-4196).

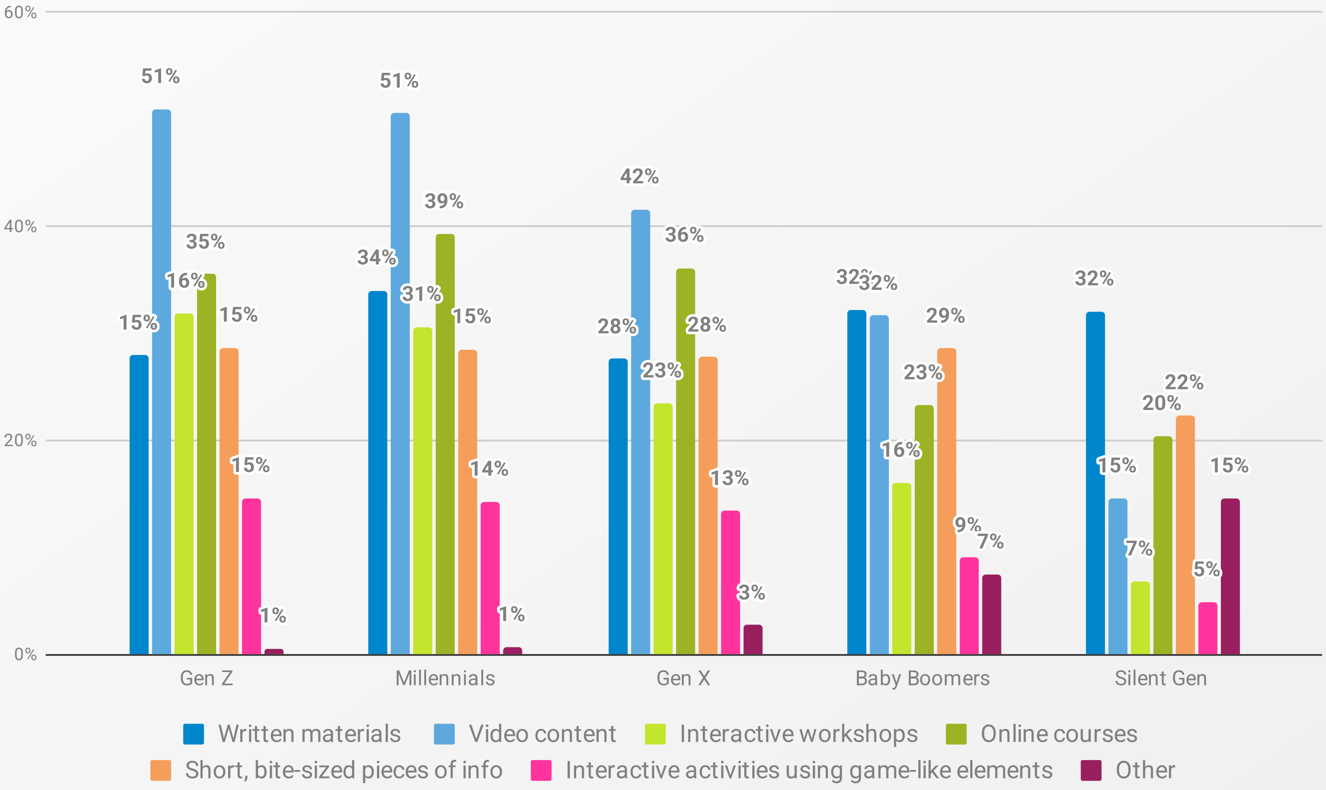
The ‘Other’ responses tell an even blunter story. A high share came from Silent Gen (15%) and Baby Boomers (7%). This data reveals a widespread lack of interest and perceived relevance, which is represented in the quotes below from a Baby Boomer and a Silent Gen participant. Other responses included: ‘None,’ ‘I don’t,’ ‘No need,’ and ‘I have no intention of doing anything about that’. It’s a clear signal that traditional formats aren’t cutting through with older demographics.

> **I won’t remember [cybersecurity training] whatever form it takes.** P2772, UK

> **Zero intent of using [cybersecurity training].**
> P2566, Australia

It’s a small data point, but it could highlight a bigger issue: training needs more tailoring. In particular, it needs to acknowledge and address the unique concerns and comfort levels of older generations. Otherwise, that’s a huge swathe of society (and your organization) who will otherwise stay unequipped to handle modern online threats.

Figure 44. ‘*What format do you prefer to consume cybersecurity training information?*’ by generation.

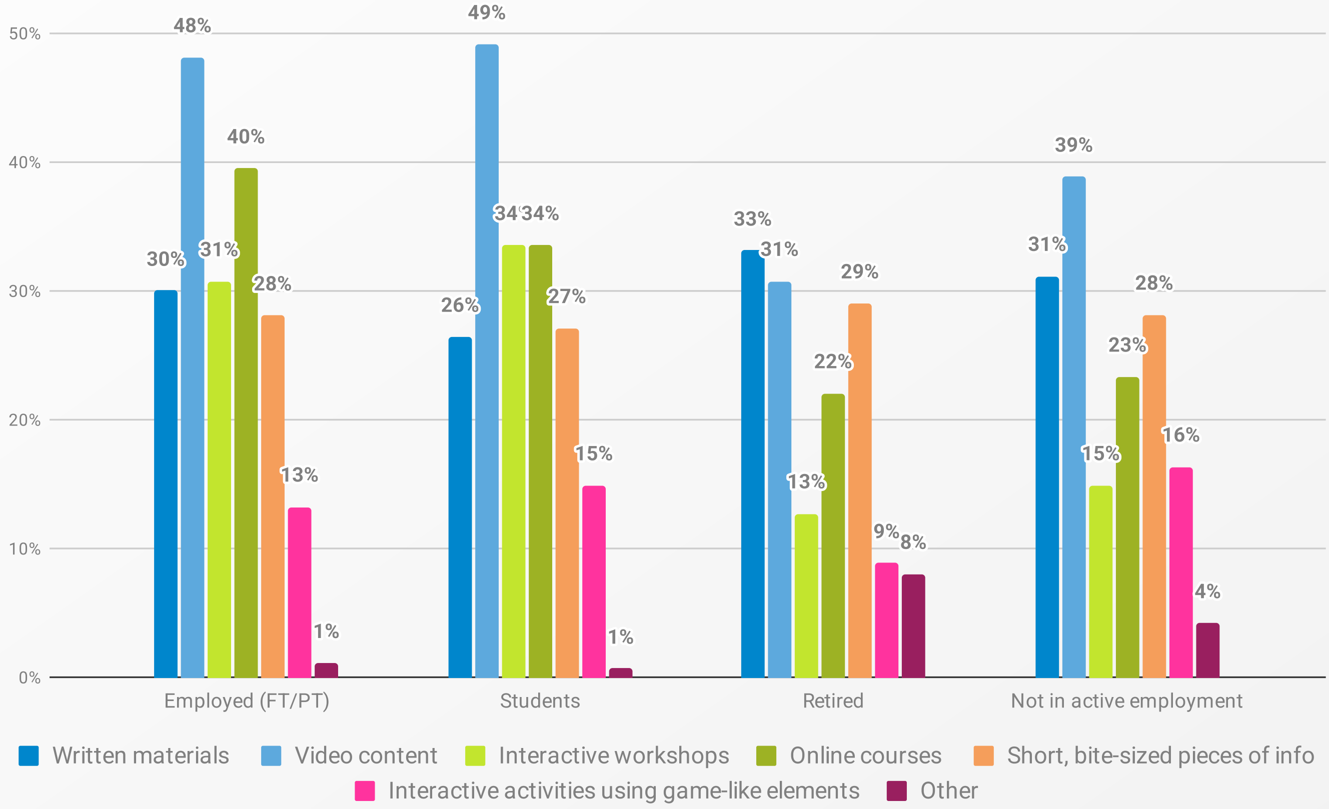


Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

The majority of employed participants preferred video content (48%), followed by online courses (40%, Figure 45). Students also leaned the same way (49%), followed by online courses and interactive workshops (both at 34%). Only retired participants had a preference for written content (33%), but that was closely followed by videos (31%). And those not in active employment also preferred video content (39%), followed by written materials (31%).

Our findings align with research[21] that found varied training preferences across different groups (in our case, different generations and employment statuses), as well as a consistent preference for video-based training[22] overall.

Figure 45. ‘*What format do you prefer to consume cybersecurity training information?*’ by employment.



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

[21] Tschakert, K. F., & Ngamsuriyaroj, S. (2019). Effectiveness of and user preferences for security awareness training methodologies. *Heliyon*, 5(6).

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

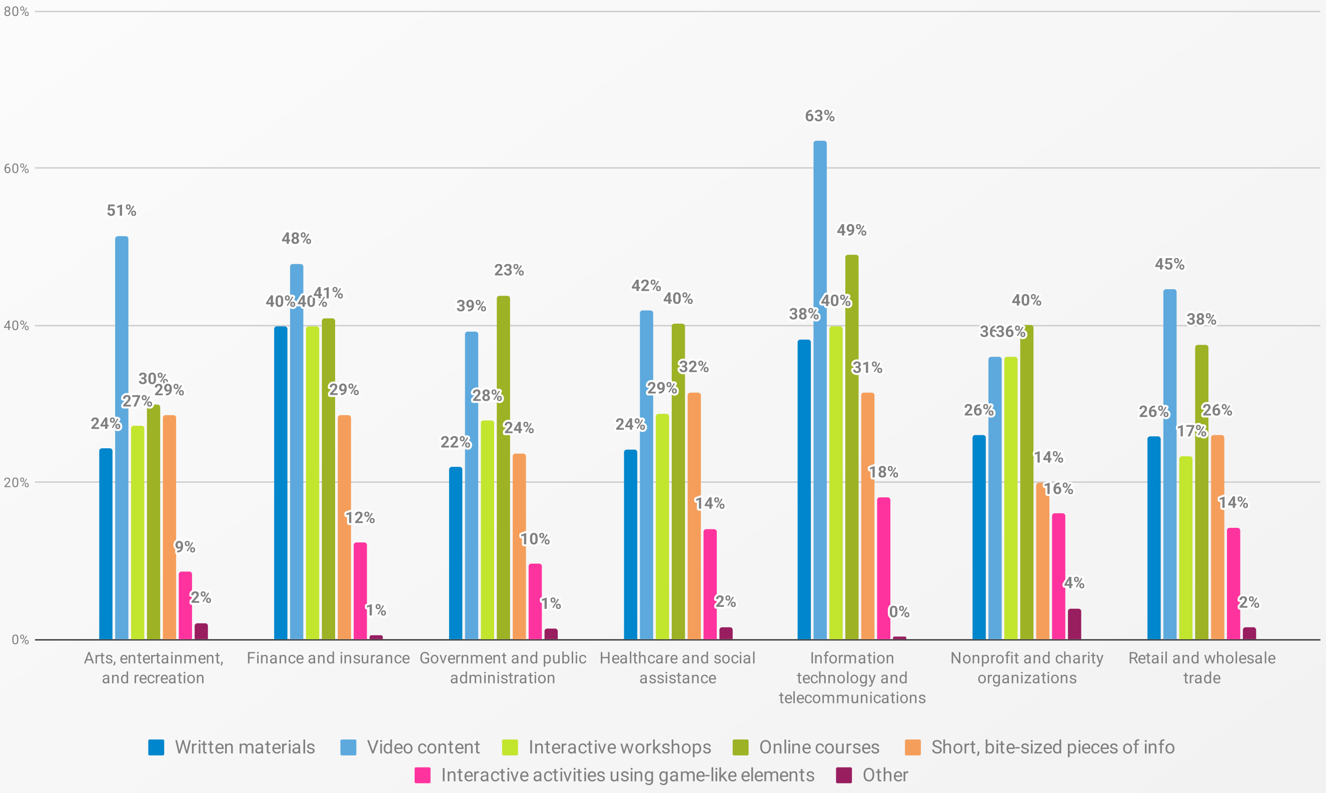
So how about the industry breakdown? The analysis of preferred training formats across different sectors[23] shows clear and consistent trends (Figure 46).

Video content came out on top in information technology and telecommunications (63%), arts, entertainment, and recreation (51%), finance and insurance (48%), retail and wholesale trade (45%), and healthcare and social assistance (42%).

Online courses were most popular among those in nonprofit and charity organizations (40%) and government and public administration (23%).

Written materials and interactive workshops still had their fans, but they didn't take the top spot in any sector, indicating a strong overall preference for screen-based, digital formats.

Figure 46. '*What format do you prefer to consume cybersecurity training information?*' by some sectors.



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants in the presented sector: 2324 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

[23] The sectors were selected based on those that stood out in certain areas, for example, either showing a strong preference for a format or a clear lack of preference for it.

In conclusion, the data on training preferences points to one clear lesson: cybersecurity education can't be one-size-fits-all. Younger, digitally native groups lean heavily toward videos and online courses, while older participants and those outside of active employment still show a pull toward written materials. When you add in the resistance from some older demographics, it's clear that the challenge is engagement, not just access.

Organizations and educators need to adapt content delivery to match the specific preferences and engagement styles of their diverse audiences[24]. That's how to meet people where they are and foster greater security resilience across all age groups and sectors.

But, one thing we can't ignore is that all the video modules in the world don't matter if nothing sticks. So, did it?

5.4 Did it stick? Impact on security behaviors

Break out the celebratory cookies, because the majority of those who attended training found it useful (83%, same as in 2024). That's a promising start, no doubt. But what about the perceived impact of cybersecurity training on people's behaviors (Figure 47)?

Almost half of the participants (47%, -5% from 2024) who completed training (N=2268) said they became better at recognizing and reporting phishing messages as a result. Forty-two percent (-3% from 2024) started using MFA, and 40% (-1% from 2024) began using strong and separate passwords after training completion.

The findings on mandatory training present a case of the glass being both half full and half empty. The fact that only 4% (unchanged from 2024) of attendees felt the training didn't change any of their online security behaviors is a positive sign, suggesting that training can be a successful first step in improving a person's security awareness.

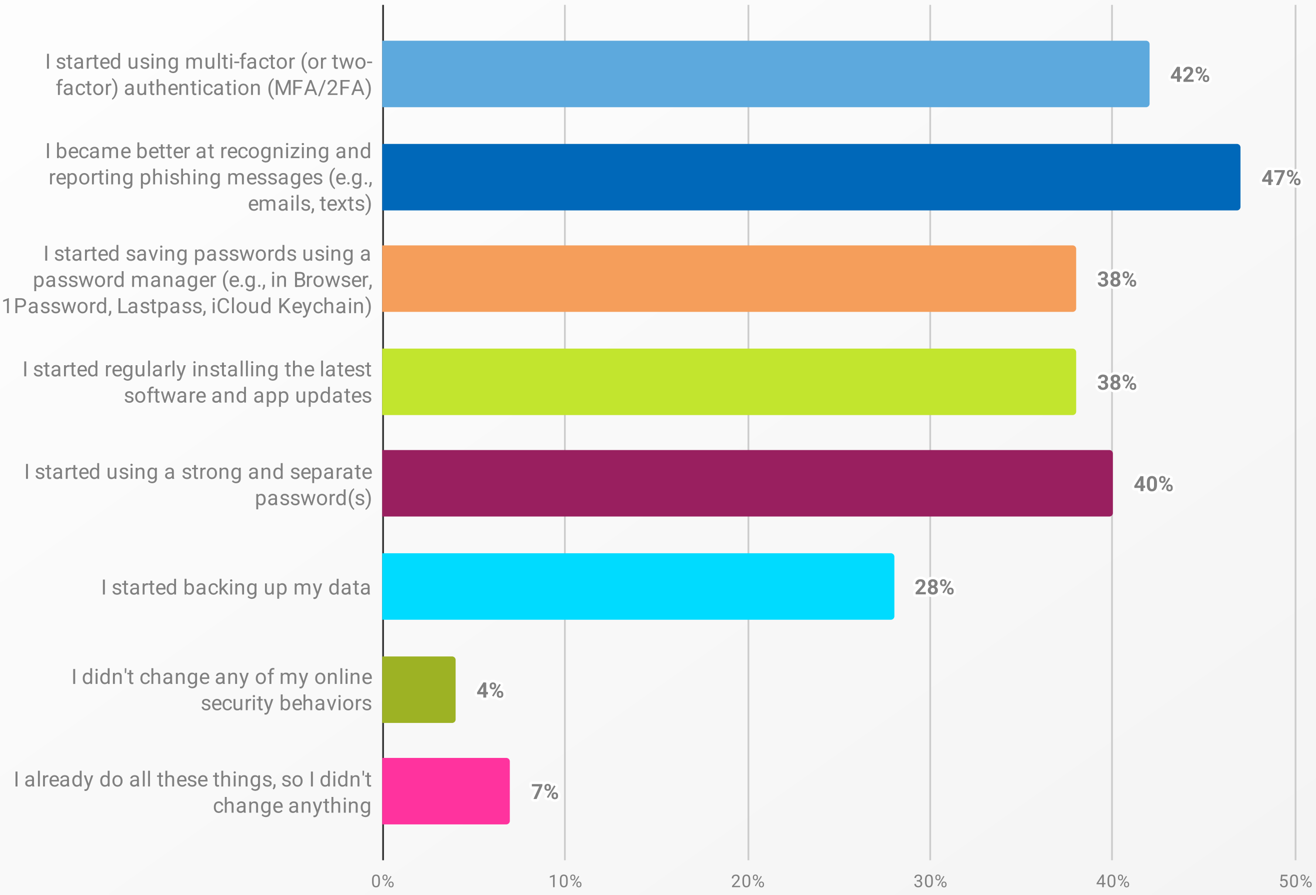
But still, we can't ignore this: less than half of the training attendees adopted truly critical security behaviors after completion. These findings align with research[25] that found only 39% of participants reported improved security behavior after training.

This highlights the gap between what people know and what they do. While training provides the necessary knowledge (the "K" in the KAB model), it doesn't guarantee a change in attitude or behavior.

[24] Furnell, S., & Vasileiou, I. (2017). Security education and awareness: just let them burn?. *Network Security*, 2017(12), 5-9.

[25] 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.

Figure 47. '*When you attended cybersecurity training, how did it influence your security behaviors?*'



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 2268 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

In summary, the perceived impact of cybersecurity training on behavior is promising, but it's far from ideal. Many reported making positive changes, such as becoming better at recognizing phishing and adopting MFA and strong passwords. But the numbers reveal plenty of room for improvement. This isn't surprising, given the mixed record[26] of Security Education, Training, and Awareness (SETA) programs in driving behavior change.

The verdict, then? Training works, just not as much as we'd like. So what really drives people's digital choices when training isn't enough? Enter decision-making. In all its messy, human glory. Brace, we're going in...

[26] Hu, S., Hsu, C., & Zhou, Z. (2022). Security education, training, and awareness programs: Literature review. *Journal of Computer Information Systems*, 62(4), 752-764.

6. Confidence trick? Cybersecurity knowledge & behaviors

With more than half of participants constantly connected and managing multiple online accounts, the question is: how cyber-savvy do people think they really are, and what do they do to keep their information, accounts, and devices secure?

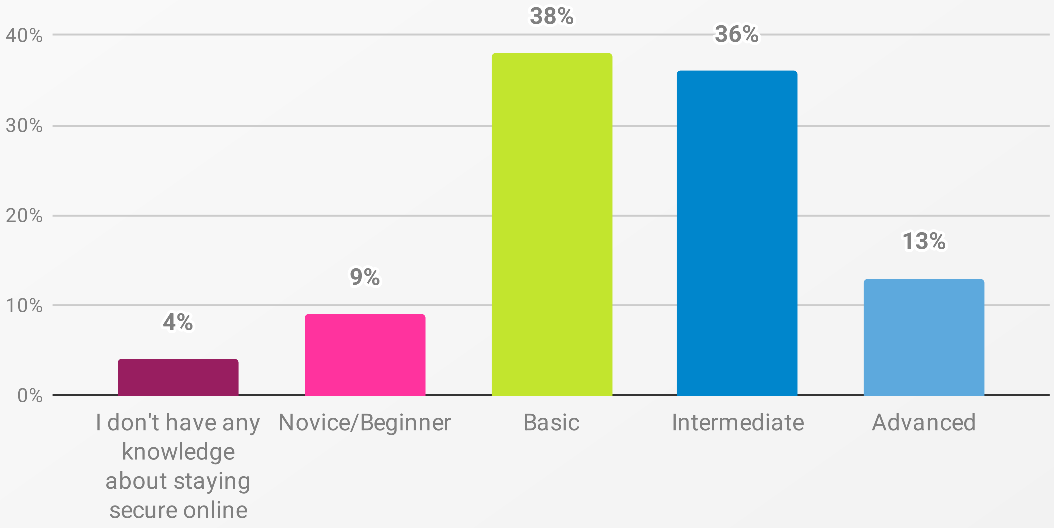
This chapter delves into the practical side of cybersecurity. We look at people's self-reported knowledge levels and examine their engagement with essential security practices. That means everything from password hygiene (including creation techniques, the use of unique passwords, and preferred management strategies), to MFA adoption, software update habits, and backup routines.

We also explore how people spot and report phishing. In short, it's a colorful snapshot of what cybersecurity looks like in practice.

6.1 Cybersecurity knowledge

Let's kick off with self-reported security knowledge. Only 49% say they have intermediate or advanced cyber knowledge (Figure 48), an 8% decrease from 2024. The biggest group (38%) rated their knowledge as basic. Meanwhile, the share of beginners (9%) and those without any knowledge (4%), both nudged up, by 3% and 1% respectively.

Figure 48. Self-reported cybersecurity knowledge.



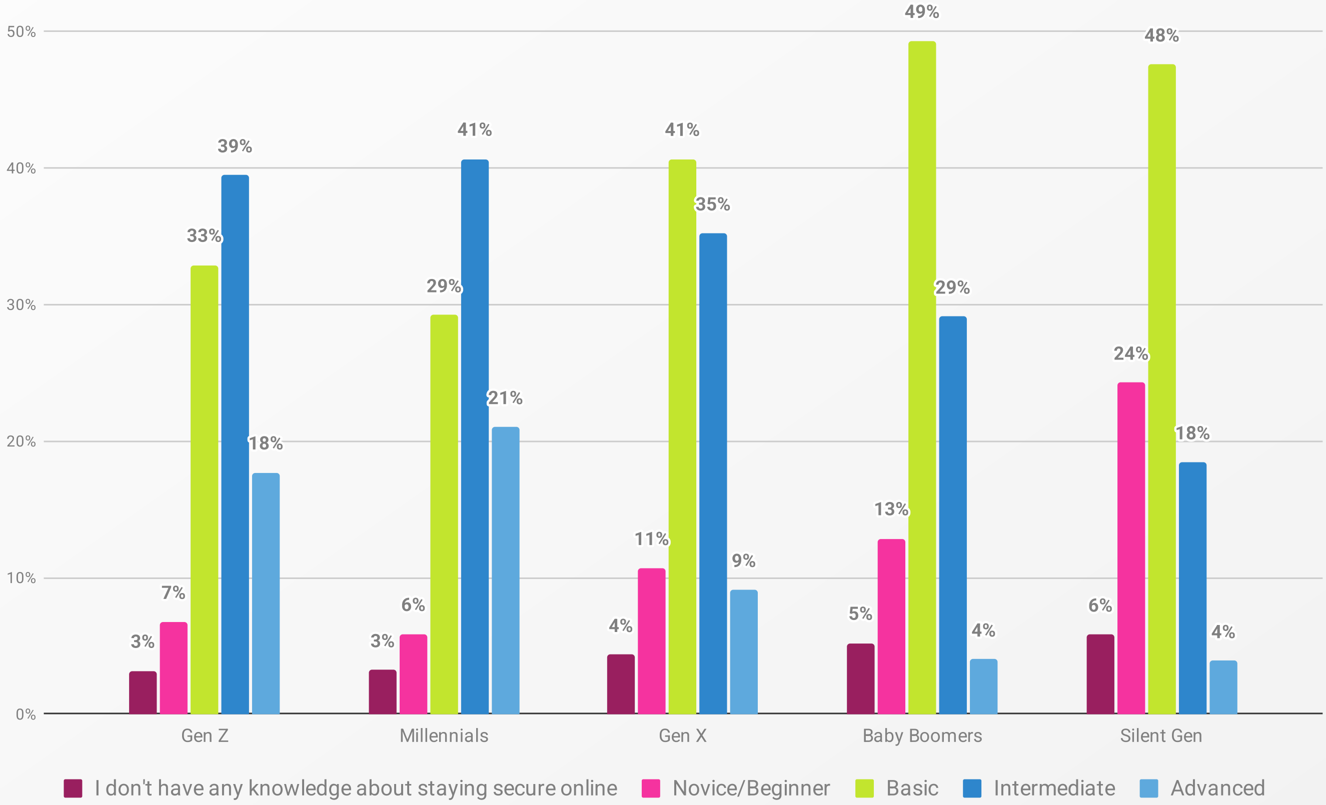
Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

Breaking this down by generation tells an interesting story (Figure 49). Younger generations still think more highly of themselves, with 62% of Millennials and 57% of Gen Z claiming intermediate or advanced knowledge, though both percentages are down since 2024, by 6% and 9%, respectively.

In contrast, the largest shares of Baby Boomers (49%) and Silent Gen (48%) describe their knowledge as 'basic', which is a rise of 3% and 5%, respectively. In fact, the 'basic knowledge' label rose across all generations: 33% of Gen Z (+8%), 29% of Millennials (+4%), and 41% of Gen X (+5%).

And unsurprisingly perhaps, older groups make up the bulk of those reporting no security knowledge at all or novice levels.

Figure 49. Self-reported cybersecurity knowledge, by generation.

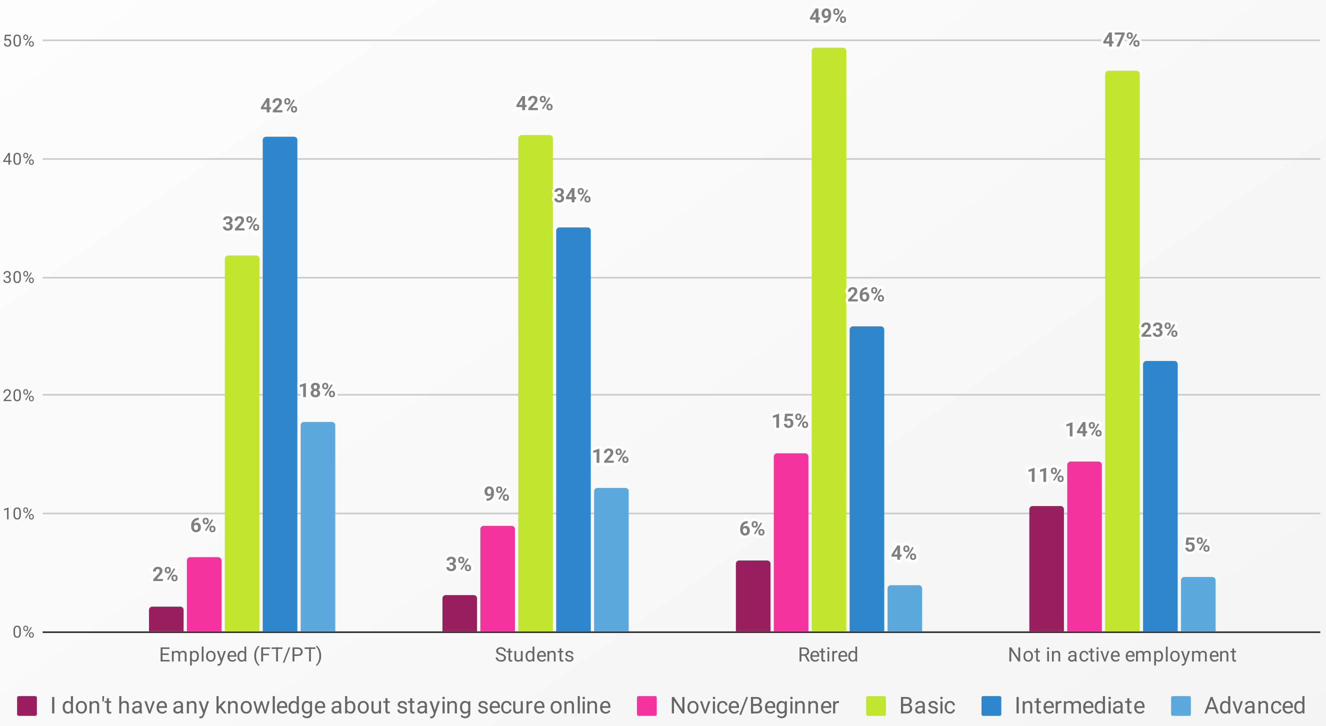


Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

> **I know a little but not a lot.** P4024, US

Employment adds another level (Figure 50). Most employed people put themselves in the 'intermediate' camp (42%, -2% from 2024). Students (42%, +11% from 2024), retirees (49%, +1% from 2024) and those not actively employed (47%, +3% from 2024) all leaned toward 'basic'.

Figure 50. Self-reported cybersecurity knowledge, by employment.



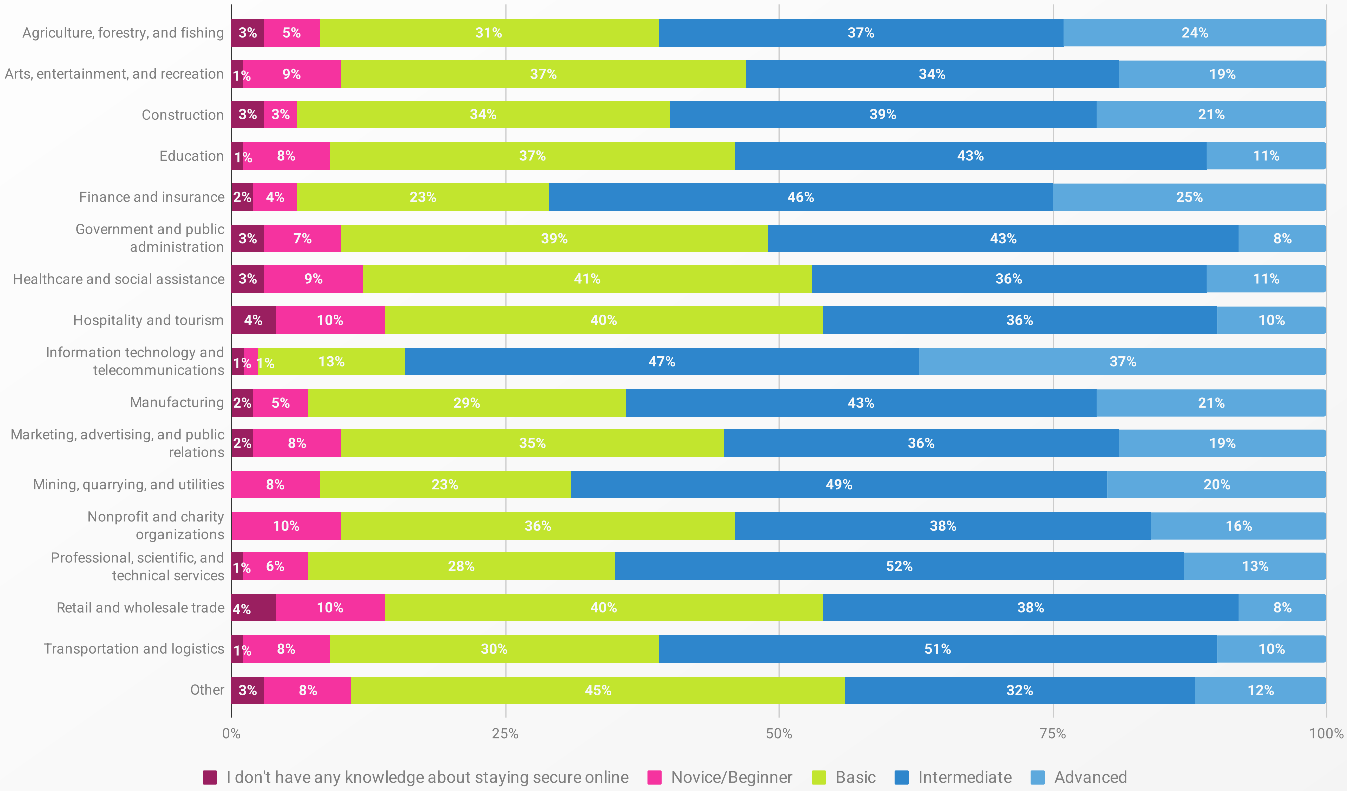
Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 4555 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

By sector, the gap is starker (Figure 51). The tech crowd lead the way: 37% of people in IT and telecoms rated themselves as advanced, followed by finance and insurance (25%) and agriculture, forestry, and fishing (24%).

Intermediate cyber knowledge was highest in professional, scientific, and technical services (52%), closely followed by transportation and logistics (51%).

The majority of those working in healthcare and social assistance (41%), hospitality and tourism (40%), and retail and wholesale trade (also 40%) reported having basic cybersecurity knowledge.

Figure 51. Self-reported cybersecurity knowledge, by sector.



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 4555 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

In summary, the trend is clear... and scary: despite a growing digital presence, the overall confidence in cybersecurity knowledge has declined since 2024, with nearly half of participants rating their knowledge as basic or below. And while younger generations and tech sectors are still ahead, they're also sliding backward. For older generations and less technical industries, the gap is even wider. It suggests that a big chunk of the population is vulnerable in an online world that gets more complex every second.

And another snag here: Knowing isn't doing. Knowledge doesn't always translate into safer behavior. So next, we'll talk about one of the real tests: passwords. Are people ditching Fluffy123 yet?

6.2 123456 reasons to worry: Password hygiene

How does self-reported knowledge stack up against actual password practices?

The National Institute of Standards and Technology (NIST) guidelines[27] for password hygiene are:

- Check passwords against breached password lists (e.g., using the 'haveibeenpwned' website).
- Avoid the use of passwords contained in password dictionaries.
- Prevent the use of repetitive or incremental passwords.
- Avoid the use of context-specific words as passwords.
- Increase the length of passwords.

These principles aren't unique to the US. Most are reflected across participating countries and/or regions, including agencies such as NCA[28], NCSC[29], BSI[30], ACSC[31], CERT-In[32], CERT.br[33], and SSPC[34].

In this section, we look at how closely people follow those guidelines by looking at:

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

And spoiler: pets and birthdays are still pulling more weight than they should.

6.2.1. Pet peeves, poor choices: Password creation techniques

Let's start with how people *say* they build strong passwords... Seventy percent (-8% from 2024) claimed they know how to create strong passwords, and that they actually do it. Meanwhile, the percentage of those who know how but choose not to create a strong password has increased by 6% to 22%.

Next, the numerical nitty-gritty. Most participants (40%, -3% from 2024) create passwords of 9-11 characters. Around a third (35%, +3% from 2024) create shorter ones. Only 25% create passwords of more than 12 characters.

[27] https://pages.nist.gov/800-63-3/sp800-63b.html

[28] https://www.staysafeonline.org/articles/passwords

[29] https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/three-random-words

[30] https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/sichere-passwoerter-erstellen_node.html

[31] https://www.cyber.gov.au/protect-yourself/securing-your-accounts/passphrases

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

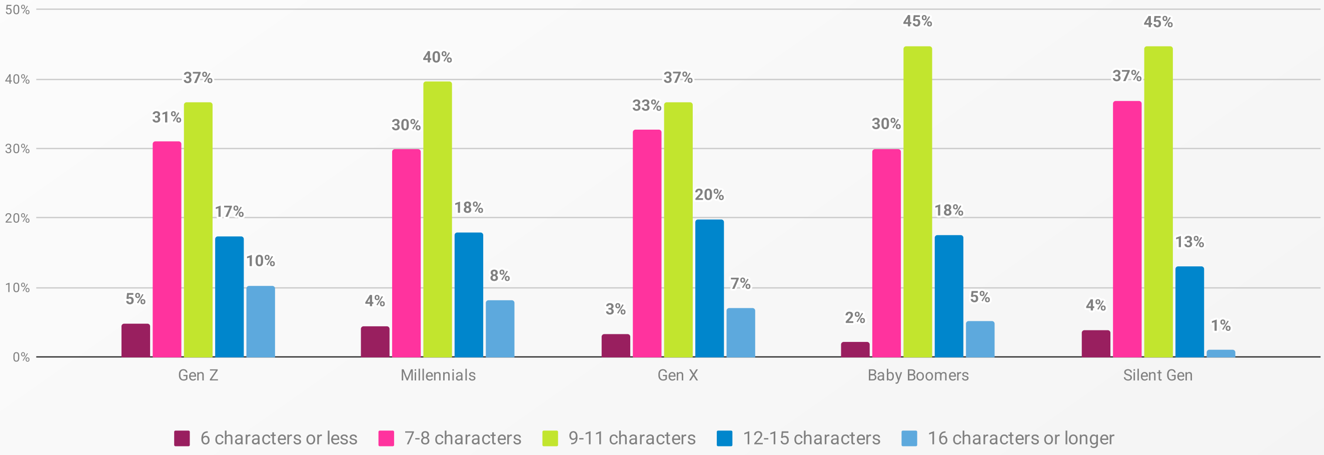
[33] https://cartilha.cert.br/dicas-rapidas/?utm_source=chatgpt.com

[34] https://www.gob.mx/sspc/prensa/sspc-emite-recomendaciones-por-el-dia-mundial-de-la-contrasena?idiom=es&utm_source=chatgpt.com

Speaking of which, those longer passwords are more common among younger generations, specifically 27% (-2% from 2024) of Gen Z, and 26% (-2% from 2024) of Millennials, who go in for longer passwords of 12+ characters. That said, the older groups are inching forward too, with 14% (+3% from 2024) of the Silent Gen and 23% (+1% from 2024) of Baby Boomers (Figure 52) now creating 12+ character passwords. We find it interesting that longer password use has slightly increased among older generations, yet slightly decreased across younger ones since 2024.

At the same time, there has been a slight increase 6-8 character passwords across most generations, for example a 9% increase among Silent Gen (to 41%) and a 6% increase among Gen Z (to 36%).

Figure 52. '*How long are the password(s) you usually create?*' by generation.



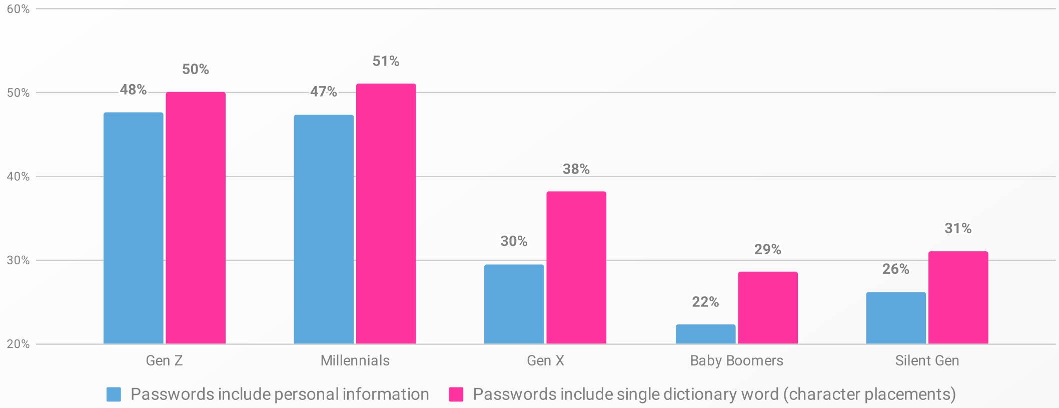
Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

Meanwhile, weak techniques aren't going anywhere. The number of people dropping their dog's name or birthday into their passwords has increased, again, for the third year in a row, by 2%, to 37%. So did the percentage of those who rely on the trusty old dictionary-word-with-symbol-swap trick, up by 2%, to 42%. (Yeah, we know. It's 2025 and yet they're still doing it. We'll pause here so you can swear under your breath.)

And similar to last year, these weaker habits are especially common across younger generations: 48% (-4% from 2024) of Gen Z and 47% (+2 from 2024) of Millennials admitted to using names of family members or pets, dates, and places when creating passwords (Figure 53), as opposed to 22% (+1% from 2024) of Baby Boomers and 26% (-3% from 2024) of Silent Gen.

Similarly, 50% (-2% from 2024) of Gen Z and 51% (+3% from 2024) of Millennials reported creating passwords using a single dictionary word or someone's name, replacing some of the characters with numbers and/or symbols (e.g., Li11y or @ wes0me).

Figure 53. Password creation techniques used by participants, by generation.



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

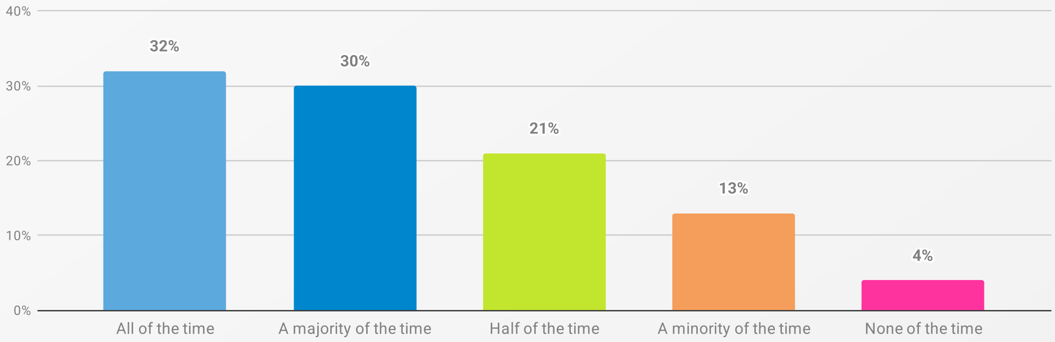
In summary, despite high self-reported knowledge, there's a glaring gap between what people know and what people do. Most participants stick with a middling length (9-11 characters) and fall back on predictable tricks like personal information or simple word-character substitutions. These behaviors are particularly common among younger, digitally native generations. Awareness is there, but the follow-through is lacking. Bridging that gap means shifting mindsets to align knowing and doing[35].

And if password length is the appetizer, next let's see how they handle the full buffet of unique logins.

6.2.2 Same old same old: Using separate passwords

Sixty-two percent of participants reported using a unique password either 'all of the time' or 'a majority of the time' (Figure 54). That's a 3% drop from 2024, continuing a downward trend that began in 2023. The remaining 38% used separate passwords less often.

Figure 54. *'How often do you use unique passwords for your important online accounts (e.g., emails, social media, payment-related sites)?'*

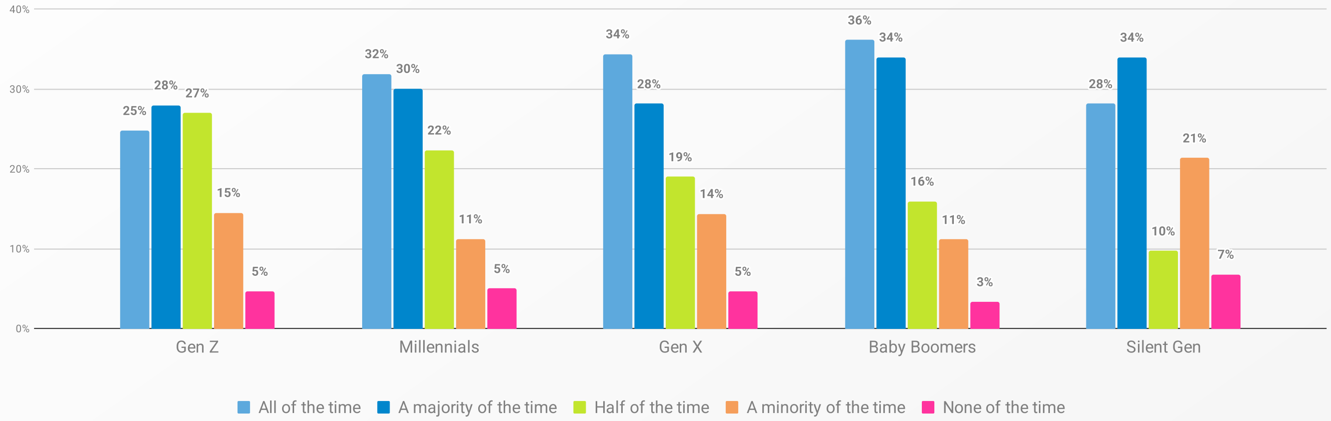


Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

[35] 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.

Baby Boomers led the way in unique password use, with 70% (-1% from 2024) saying they stick to it ‘all of the time’ or ’a majority of the time’ (Figure 55). But across almost every generation the numbers dipped again this year. The biggest drops were in the youngest (Gen Z, -5% to 53%) and oldest (Silent Gen, -8 to 62%) demographics.

Figure 55. ‘*How often do you use unique passwords for your important online accounts (e.g., emails, social media, payment-related sites)?*’ by generation.



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

When we got nosy with those who rarely use separate passwords (N=1208), the answer was clear: memory. The majority (51%, -9% from 2024) reported difficulty remembering multiple passwords, and 21% (+4% from 2024) said they only used separate passwords for accounts where they wanted increased security. Another 18% mentioned that having separate passwords was time-consuming or required extra effort.

> **I’m starting to forget things so I have to use the one [password] I’ve always used.** P21782, US

These findings echo broader research[36] on password behavior, demonstrating that the main causes for password reuse are preference for memorability over security, and misconceptions about risk. This is further supported by the concept of security fatigue, a term that describes the mental and emotional exhaustion that comes from being constantly vigilant about security and managing multiple security tasks. This mirrors our findings: many skip unique passwords because they’re hard to remember, while others have misconceptions about the inevitability of online threats.

But if failing memory is the main reason for reusing passwords, this sounds like the perfect case for password managers, right? Right??

[36] Hanamsagar, A., Woo, S., Kanich, C., & Mirkovic, J. (2016). *How users choose and reuse passwords*. (Technical Report ISI-TR-715). Information Sciences Institute, University of Southern California.

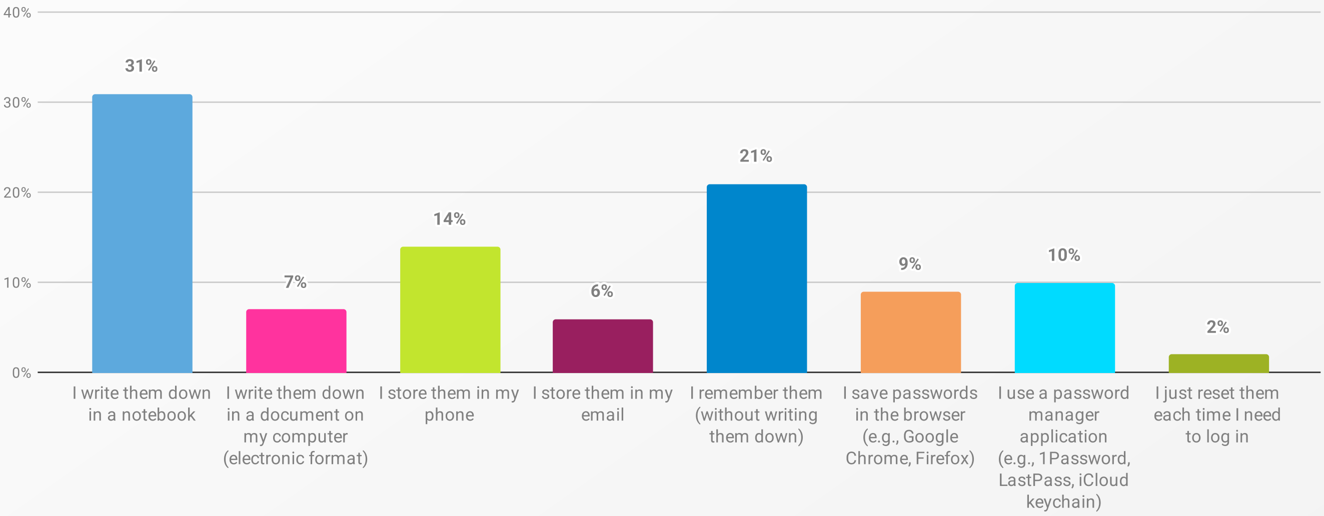
6.2.3 Sticky note sickness: Password management strategies

With 91% juggling more than one online account and 62% using unique passwords, the question is: how on earth are they keeping track of them all? So here we'll look at people's preferences for keeping track, and whether they use password managers.

6.2.3.1 Trust issues: Preferred password management strategies

The majority (31%, +2% from 2024) of participants with more than one account (N=5400) prefers writing passwords in a notebook (Figure 56). Twenty-one percent (same as in 2024) bragged that they could remember their passwords without storing or writing them down anywhere. Twenty-nine percent used other methods, anything from saving passwords in their phone or email, to documenting them in electronic files, to resetting them each time they logged in. We'll be having nightmares about that last one.

Figure 56. Preferred password management strategies.



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 5400 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

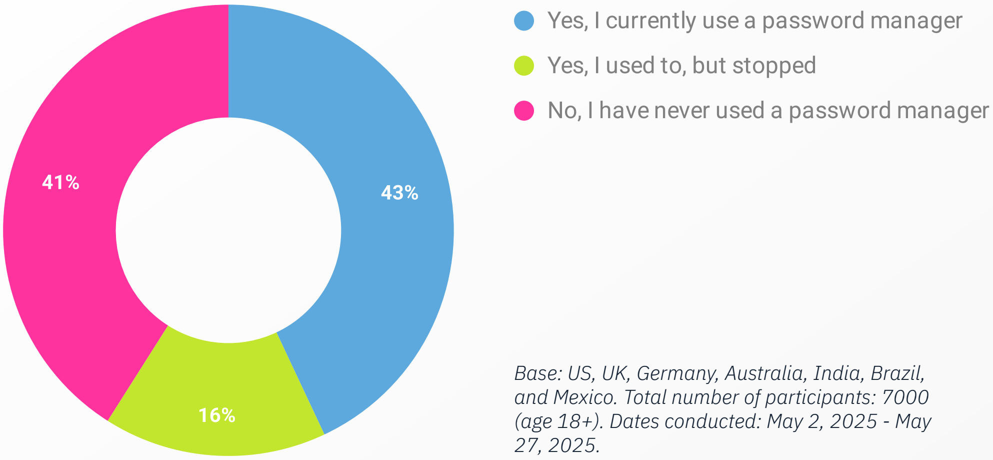
What's striking is that notebooks weren't just an older-generation thing this year. Writing passwords into notebooks was the most popular option among all generations, though it was still more common among older generations. Twenty-five percent of both Gen Z and Millennials, 34% of Gen X, 44% of Baby Boomers, and 49% of the Silent Gen use their notebook for password storage.

Which begs the question: If even digital natives are sticking to notebooks, how's the uptake on actual password managers looking?

6.2.3.2 App-rehensive? Use of password managers

Forty-one percent have never used a password manager, but at least this is a 5% decrease from 2024 (Figure 57). Of the 57% (+3% from 2024) who have used password managers, 16% (+2%) have stopped using them. We can't help but wonder what's going on there, as that's a sizable chunk of PM drop-outs.

Figure 57. ***'Have you ever used a password manager?'***



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

Of active users (N=2992), 39% rely on their browser, 37% use free stand-alone password managers, and 24% use paid stand-alone tools.

What about those avoiders? The top five reasons for not using password managers were:

1. I prefer my own password management methods because I'm more in control (66%) – this was a new option we added to the survey this year.
2. Feeling that using it won't stop cybercriminals (54%, +6% from 2024).
3. Not knowing which password manager to use (47%, -1% from 2024).
4. It is unnecessary if it isn't required (47%, +6% from 2024).
5. Not trusting password managers (41%, +2% from 2024).

So while adoption is inching up overall, hesitation remains strong. People who don't use password managers (N=4008) mentioned wanting more personal control, distrusting the tech, or simply not seeing the point.

This highlights a key challenge for security: moving beyond the simple message of using unique passwords to actively promoting safer, more modern management strategies that address user concerns around control, trust, and usability.

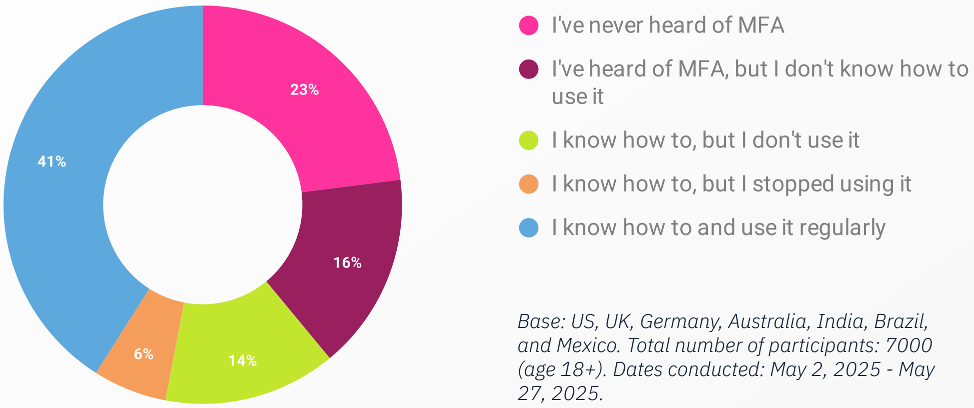
And for those still clinging to sticky notes and browser autofill, there's at least one defense they can't afford to skip. Let's talk about that extra lock that some of us put on the door: MFA.

6.3 Double or nothing: Enabling multi-factor authentication (MFA)

This section explores MFA usage, examining people's understanding of the technology, key generational differences in adoption, and the primary reasons for non-use. We also delve into where MFA is most commonly enabled and what factors, such as login methods like biometrics and preferences for second-factor verification, influence its broader adoption.

Twenty-three percent have never heard of MFA (+4% vs 2024), and 16% have heard of it but don't know how to use it (Figure 58). Only 41% said they use MFA regularly. Another 14% know how to use it but chose not to. So, while MFA is simple in theory, it continues to be bafflingly elusive in practice.

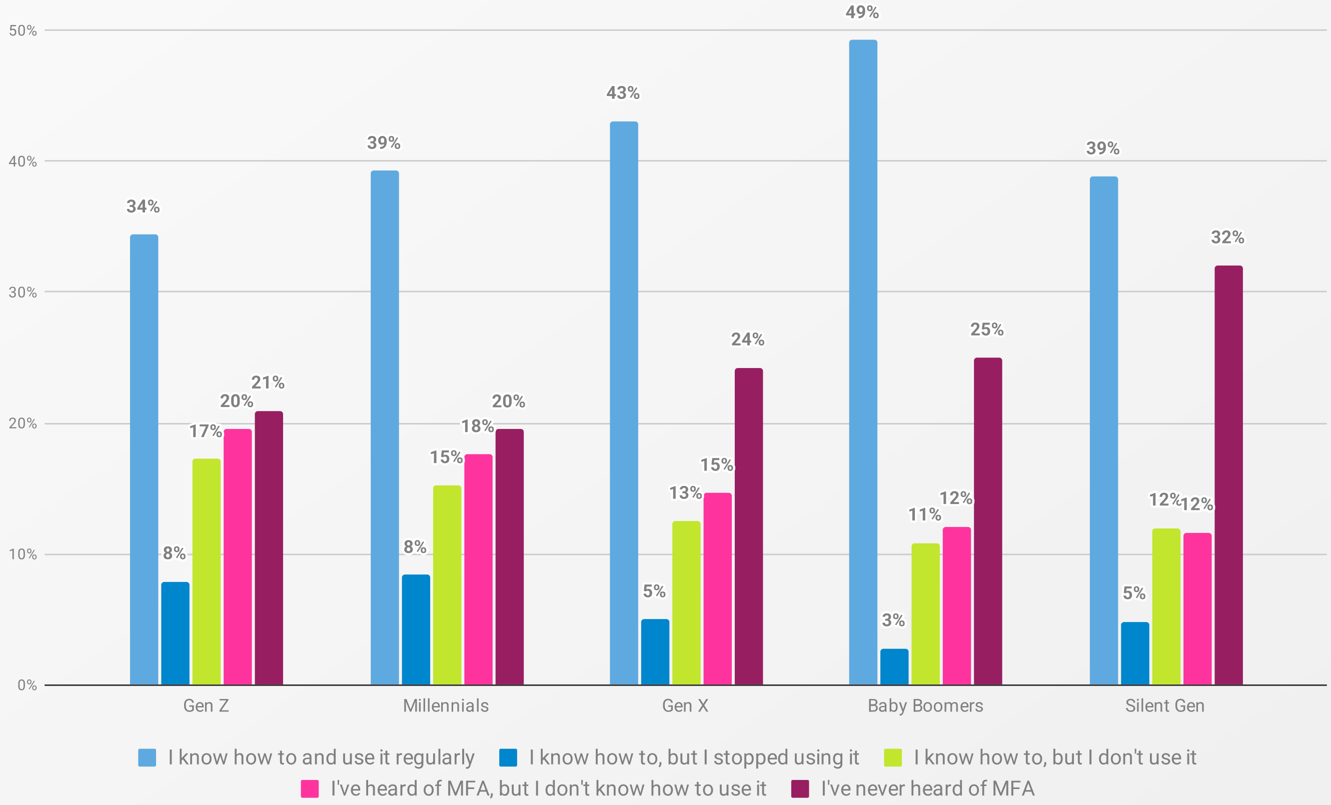
Figure 58. *'Do you know how to use multi-factor authentication (MFA)?'*



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

So, which age group is MFA's biggest fan (Figure 59)? Baby Boomers (49%), followed by Gen X (43%). Younger generations were more likely to skip or stop using it: 17% of Gen Z and 15% of Millennials reported not using MFA, and 8% of both generations decided to stop using it. The highest percentage of those who have never heard of MFA were the Silent Gen (32%).

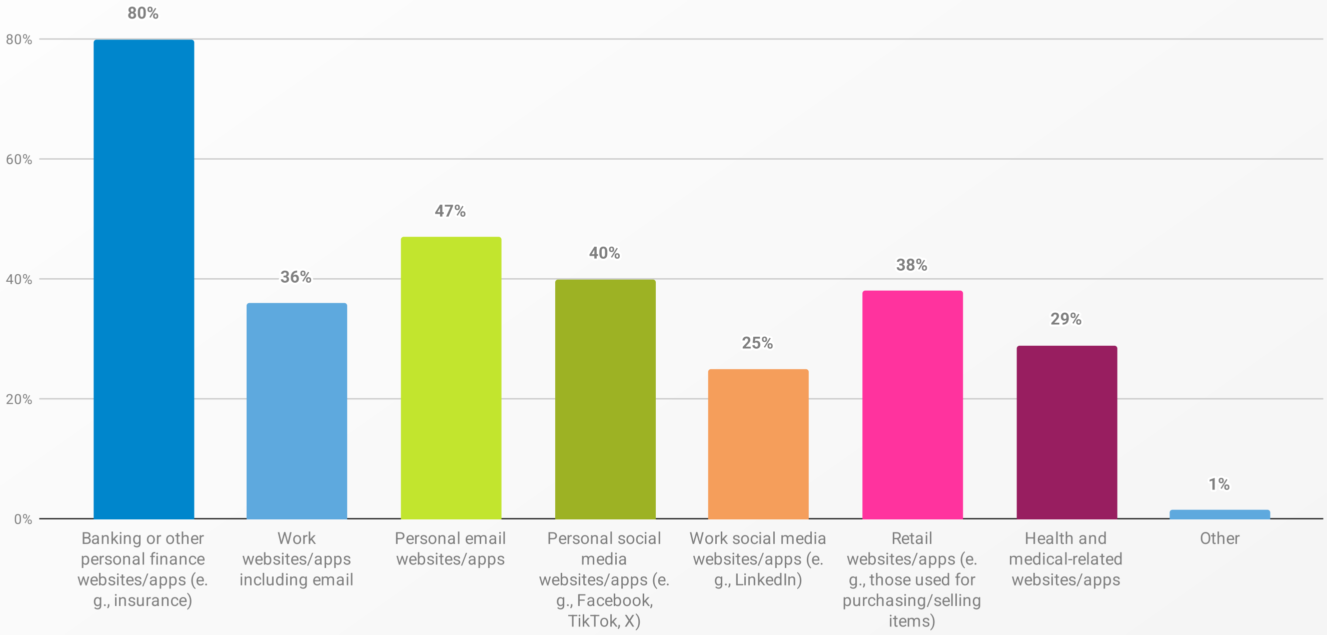
Figure 59. *'Do you know how to use multi-factor authentication (MFA)?'* by generation.



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

Among those who do use MFA (N=2890), banking and finance apps and sites predictably came top of the list (80%, Figure 60). Forty-seven percent used MFA on their personal email accounts, and only 36% enabled it on work websites/apps, including emails. Work social media websites (e.g., LinkedIn) were bottom of the ladder, at just 25%.

Figure 60. ‘*Where have you enabled MFA?*’



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants who use MFA: 2890 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

We also asked those who don’t use or have stopped using MFA (N=1422) why. The most common reason was the belief that passwords alone are strong enough (37%), followed by not seeing MFA adding any extra protection (18%). Not carrying phones all the time to verify was another popular reason (17%).

> **Facebook’s MFA, which is arbitrarily inflicted, includes a mandatory WhatsApp step. I was locked out of my Facebook account (and others) due to a one-off internet access problem, although able to get back in to other accounts, including bank, in less than a minute, I am now permanently locked out of my Facebook account as WhatsApp can not be used with all phones, including Telstra landlines which is the phone number Facebook has for me. This is impacting numerous people who have lost access to (but not limited to) all of their messages, in my case, years of work too.** P3907, Australia

> **It [MFA] is a pain in the ass to use.** P5986, Australia

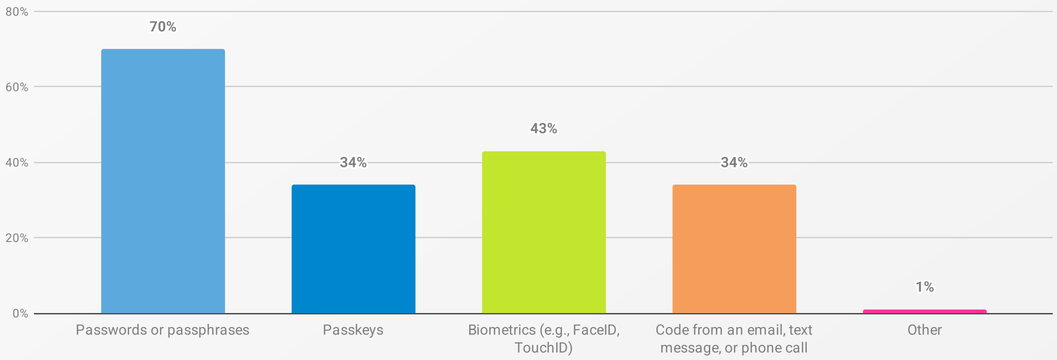
> **Cut out this method of use. I've never been hacked, so I don't think I should be expected to follow this. It's people's responsibility to protect their own privacy without safety nets being forced on to the rest of us.** P17436, Australia

These frustrations with inflexible and inconvenient MFA experiences align with research[37] showing that poor usability and negative user attitudes are key barriers to adoption.

Next let's turn to those who have never heard of MFA or don't know how to use it (N=2543). Fifty-one percent felt it won't stop cybercriminals. Forty-eight percent said they simply don't understand it, and 47% felt that MFA is unnecessary if their device works as it should. A further 45% claimed they simply don't have time for it, while 44% cited a lack of benefits, the fact that no one they knew was using it, and a lack of confidence in their own ability to use it.

And we didn't stop here. We also asked participants about what login methods they use in their online accounts. Most said password or passphrases (70%, Figure 61). The second most popular option was biometrics, though only 43% reported using them.

Figure 61. '*Which of the following methods do you use to log in to your online accounts?*'

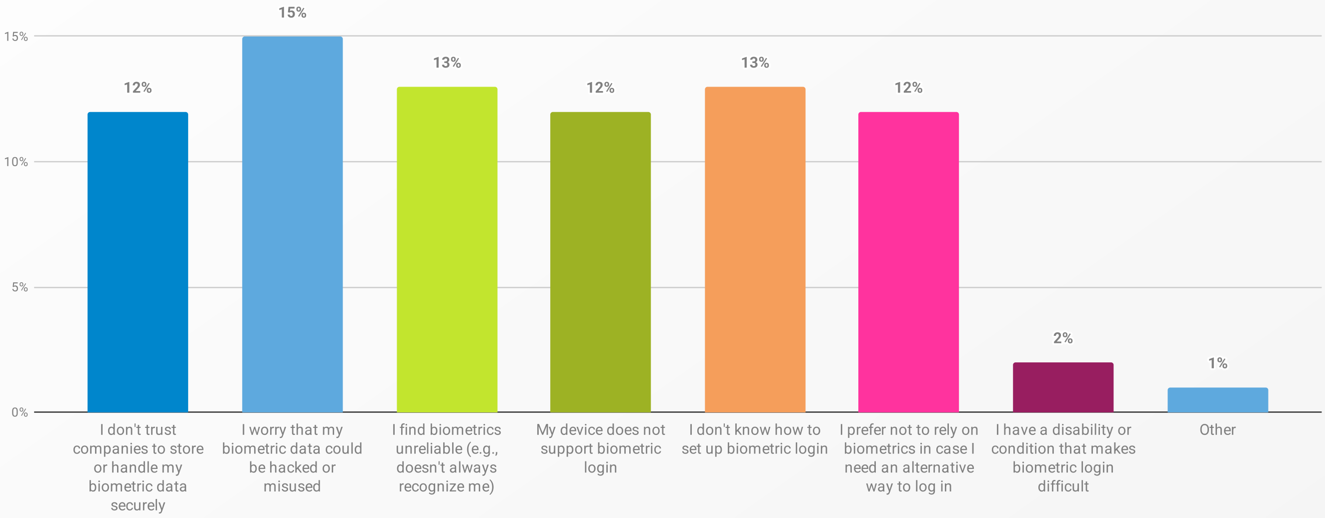


Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

[37] Das, S., Wang, B., & Camp, L. J. (2019). *MFA is a Waste of Time! Understanding Negative Connotation Towards MFA Applications via User Generated Content*. arXiv. https://arxiv.org/abs/1908.05902

Considering the increasing popularity of biometrics in tech for authentication, we asked the non-biometrics users (N=3994) why they didn't use them. The most popular reason was the worry that biometric data could be hacked or misused (15%, Figure 62). Finding biometrics unreliable and not knowing how to set them up were the next most common reason (13% each).

Figure 62. '*What's the main reason why you don't use biometrics to log in to your online accounts?'*



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants who don't use biometrics: 3994 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

Then there's the 12% who said they didn't trust companies to store or handle their biometric data securely, a sentiment that was also echoed in some of the qualitative responses (N=57), which were provided in the 'Other' option. Deep-seated security and privacy concerns were apparent, as expressed by a clear mistrust of tech companies and fears that biometric data could be misused or stolen, with some even calling it the 'ultimate way to steal identity'. Some people mentioned convenience and functionality issues, such as the technology malfunctioning or general hassle, while others felt biometrics just weren't necessary, believing that traditional security methods like passwords were 'enough'.

> **It [biometrics] could possibly make things worse if things go down.** P21739, US

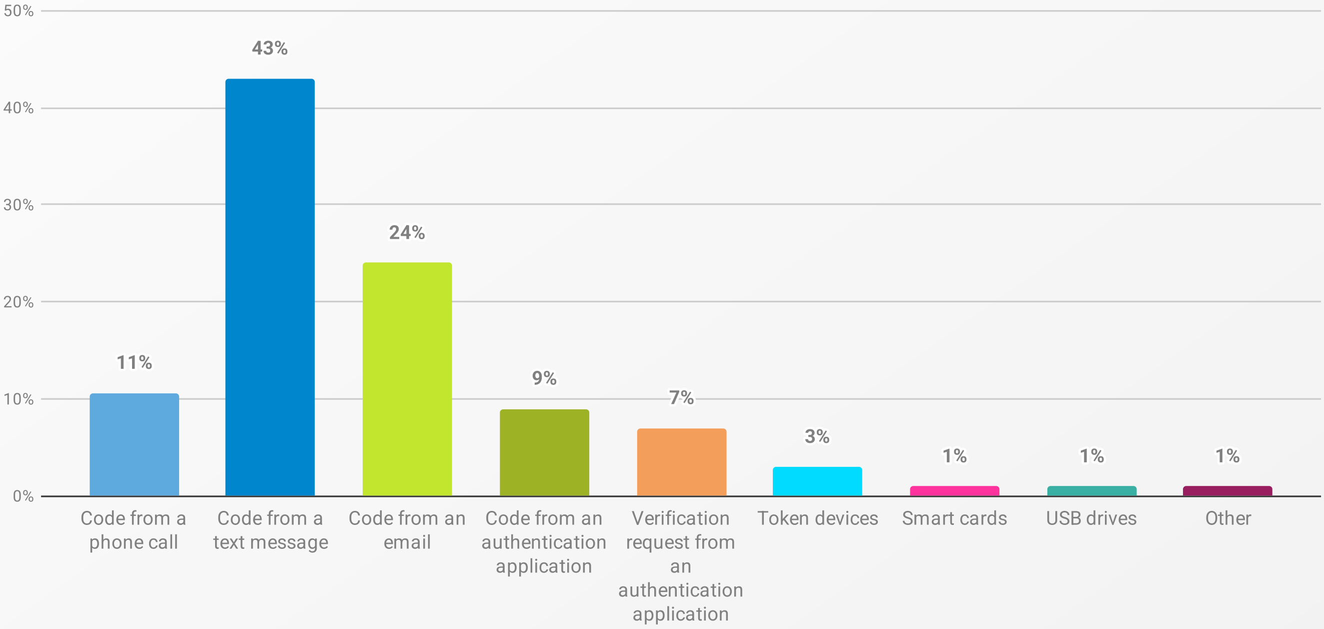
> **I don't trust biometric collections from tech companies, [it's the] ultimate way to steal identity.** P17037, Australia

> **All I've got to do is leave my glasses off and facial recognition doesn't like me.** P21950 Australia

These findings align with established research that identified similar barriers to biometric adoption, highlighting that a primary reason for non-adoption is a strong mistrust of the technology and the data collectors[38]. This is further backed up by the finding that users harbor misconceptions about biometric implementation and are also likely to abandon the technology due to usability issues.

Speaking of usability and convenience, we also asked participants which second-factor authentication methods they prefer using (Figure 63). The highest percentage of participants (43%) found code from a text message to be the most convenient, followed by code from an email (24%), and from a phone call (11%). Smart cards (1%) and USB drives (1%) were the least preferred methods. What's striking here (and kudos to the eagle-eyed among you who have spotted it already) is that SMS remains king, despite NIST having called it out because it's not considered secure[39]. So while the security community may cringe, for many people out there, convenience beats caution hands down.

Figure 63. *'After entering your password to log into a website or app, you may be asked to use another method to verify your identity. Which one of these would you find MOST convenient to use?'*



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

[38] Wolf, F., Kuber, R., & Aviv, A. J. (2019, May). 'Pretty Close to a Must-Have' Balancing Usability Desire and Security Concern in Biometric Adoption. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (pp. 1-12).

[39] Coldewey, D. (2016). *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/

The data on MFA use presents a complex landscape of awareness and behavior. Many use it regularly, but a notable portion remain uninformed or unwilling to adopt it, often because they don't see the need or don't trust the tech. Generational differences are stark, with older generations more likely to be regular users, while younger generations, who are more active online, show a higher rate of non-use.

Add to that frustration with clunky user experiences and a strong attachment to SMS codes, and the challenge becomes dazzlingly obvious: To increase MFA adoption, this community needs to do more than simply promote its existence. It's going to take some serious work to address usability concerns, build trust, and show MFA's value beyond passwords alone.

Making MFA a no-brainer

CybSafe's top five ways to get MFA use up in your organization:

1. Lose the faff
Convenience wins. Sure, apps beat texted codes on paper. But if more people actually stick with codes, that's still a net security win. Perfect is the enemy of secure.

2. Give them a nudge
Sometimes all it takes is a prompt. Don't underestimate the power of 'set this up now' at the right moment.

3. Sweeten the deal
Rewards work. A small incentive, badge, or even public praise can tip people from 'maybe later' to 'done'.

4. Tell the story
People need the 'why'. Explain how MFA keeps their money, data, and dignity intact, and what can happen without it. No scare tactics, just clear cause and effect.

5. Build the bridge
Handing over phone numbers or biometrics feels personal. Acknowledge that, be transparent about what happens next, and show you have their back. Trust makes adoption stick.

Further reading

- Check out our blog: 'Have you got multi-factor?'. It explains MFA in plain language and why adoption matters.
- Delve into the Stay Safe Online MFA guide, backed by the National Cybersecurity Alliance. It focuses on how to make MFA adoption a baseline move for organizations.

6.4 Snooze and lose: Installing software & app updates

Keeping devices secure is a continuous process that relies heavily on keeping software and applications up to date. Security updates and patches are crucial for protecting against new vulnerabilities and threats.

This section examines people's update habits (or lack thereof), exploring overall trends, generational differences in update frequency, and the timing of these actions.

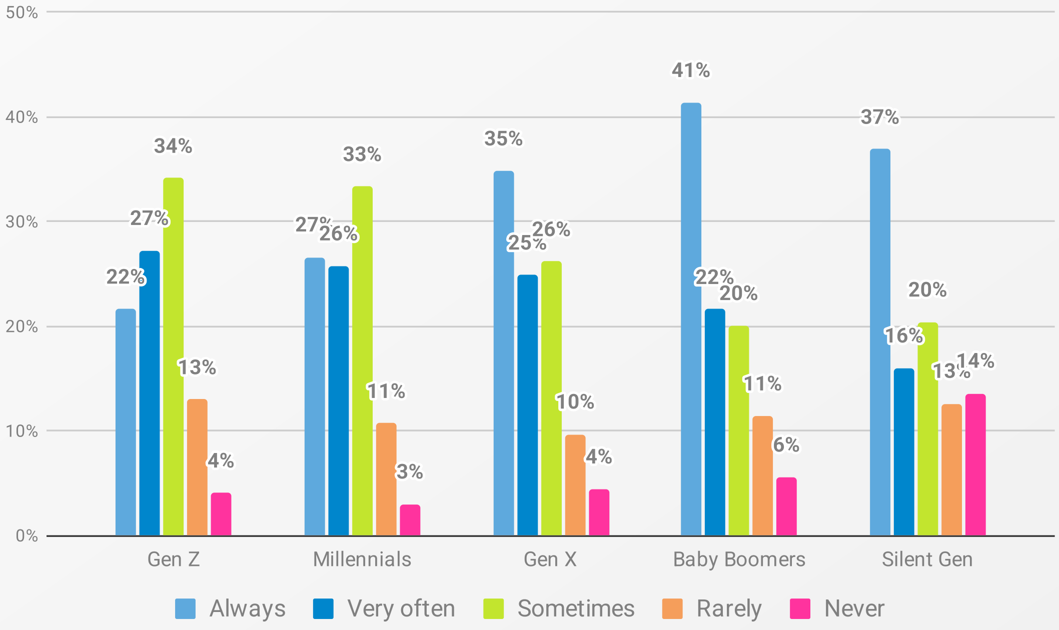
First off, 60% reported installing the latest software and app updates across their devices, down by 3% since 2024. Meanwhile, the number of those who know how to install updates but don't do it has increased by 3% to 23%.

When it came to frequency, 56% updated 'always' or 'very often' (-1% from 2024), and 4% (N=313) claimed they never updated their devices – unchanged from last year.

Older generations were more dutiful. The largest proportion of Baby Boomers (41%, -3% from 2024), Silent Gen (37%, +8% from 2024), and Gen X (35%, +1% from 2024) 'always' updated their devices when notified, as opposed to younger generations (Figure 64).

The majority of Gen Z (34%, -1% from 2024) and Millennials (33%, +2% from 2024) only 'sometimes' updated their devices.

Figure 64. '*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, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

Among those who update least sometimes (N=5911), 40% have turned on automatic updates (-5% from 2024) Additionally, 30% update as soon as the notification appears, 20% do it after clicking 'Remind me later' a few times, and only 10% when they're away from or not using their devices.

In summary, most people still update, but slightly fewer than before. More than last year don't, despite knowing how, while a stubborn minority never updates at all. Older users are proving more reliable than younger ones, and the decline in automatic updates hints at a worrying shift.

And for practitioners, this pattern is deja vu: awareness without follow-through. So, what can you do about it?

Updating devices

Getting people to stop hitting 'Remind me later' is never easy, but there are ways to tip the scales:

1. Default to auto-update
People go with the flow. If auto-update is the norm, they are more likely to stick with it. An easy win for any organization.

2. Updates people trust
If an update crashes apps or slows devices, confidence drops. Testing before roll-out keeps trust intact.

3. Work with people's time
Give flexibility. Let updates happen during lunch or at the end of the day, so security fits into routines rather than disrupting them.

Further reading

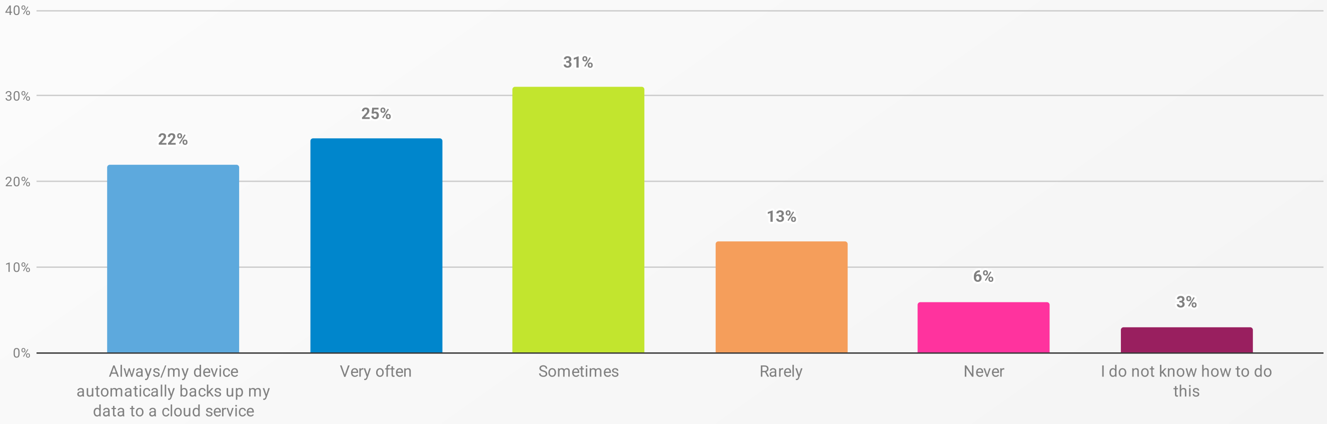
- Stay Safe Online's Why software updates matter is a practical guide on how updates protect against emerging threats.
- CybSafe's blog Why are you snoozing updates? gives a deeper look at the behavioral barriers stopping people from updating their devices.

6.5 Ctrl+S your life: Backing up data

Forty-seven percent (+2% from 2024) said they ‘always’ or ‘very often’ back up their important data (Figure 65).

A further 31% (-1% from 2024) reported backing up their data ‘sometimes’, while 19% (-1% from 2023) reported that they ‘rarely’ or ‘never’ make backups.

Figure 65. *‘How often do you back up your most important data?’*



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

On the surface this is encouraging, but context matters. In most working environments, data backup is an automated, centrally-managed process requiring little direct action from individuals.

In contrast, personal or home environments rely more heavily on individuals to manage their own backups, either through automated cloud services or manual actions.

Boosting backups

Backups are only lifesavers if they actually exist. Here are five ways to make sure they do in 2025:

1. 3-2-1 still rules
Three backups, two devices, one offsite. Make it easier by handing out encrypted flash drives or secure cloud options.

2. Automate everything
Cloud backups, scheduled syncs, system defaults. If people do not need to think about it, they are far more likely to keep their data safe.

3. Shout about the ease
People often assume backups are complicated. Show them how little effort it takes and adoption will climb.

4. Celebrate the savers
Spotlight those who back up without fail. Gentle reminders and positive nudges can pull the rest along.

5. Make it cultural
Treat backups as a normal part of organizational life, not an optional extra. It should feel as standard as locking the office door.

Further reading

- CybSafe's guide to how to make data backups a regular part of everyone's day
- Back it up: Stay Safe Online's backup guide

6.6 The bait debate: Recognizing & reporting malicious messages

Phishing remains one of the most pervasive and successful cyber threats, with attackers becoming sneakier by the day. For this report, we use the term 'phishing' as a broad term to cover all malicious and deceptive messages, whether they arrive via email, text, or social media. This part looks at the human side of the phishing problem: how confident people feel about recognizing phishing, what they actually do to check messages, and how often they bother to report them. We break it down into the specific steps people take to protect themselves, from checking for grammatical errors to proactively reaching out to senders. Finally, we analyze how often people report malicious messages, and the key barriers that stop them.

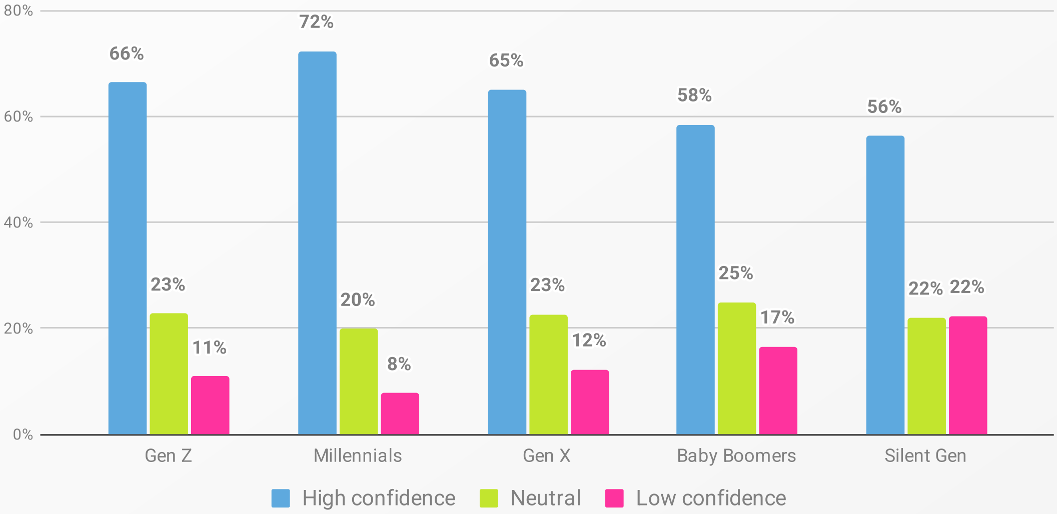
First up: recognition. Do people really know when not to click?

6.6.1 Can I click it? Recognizing phishing messages

Phishing is still one of the most effective weapons in an attacker's arsenal, and confidence alone won't stop a bad click. Overall, people reported high confidence in spotting phishing emails or malicious links (M=7.12, SD=2.3, N=7000). Specifically, 66% (a 1% drop from 2024) of participants felt confident in their abilities. Still, 12% (a 2% increase from last year) report not feeling confident in their abilities to identify malicious emails or links.

By generation, Millennials (72%, Figure 66) felt most confident in identifying malicious messages, representing a 4% decrease from 2024. This was followed by Gen Z (66%, -3% from 2024) and Gen X (65%, -1% from 2024). The older cohorts were far less sure. Confidence dropped to 22% in Silent Gen and 17% among Baby Boomers, down 5% and 3% respectively from 2024.

Figure 66. '*How confident are you in your ability to identify a phishing email or a malicious link?*' by generation.



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

But what about the 12% who lack confidence? A primary theme is the rapidly increasing sophistication of scams. Many participants noted that phishing emails and links are 'very clever,' 'extremely deceptive,' and 'look so genuine' that even a wary user can be fooled. This is compounded by the belief that cybercriminals are 'too advanced' and that the sheer volume of scam emails makes vigilance overwhelming, not to mention the advancements with AI.

Another notable reason is a lack of formal training or knowledge. Many people said they 'don't know enough about them,' 'have never been shown,' or 'do not know what to look for.' For some, this is tied to a lack of confidence in their general tech skills, with multiple people describing themselves as 'not tech savvy' or a 'real beginner.' The emotional impact of this is clear: participants admitted to feeling 'scared stiff,' 'nervous,' and 'vulnerable,' with some feeling they would be an easy target for criminals.

> **It's very easy to be taken in by a convincing looking phishing email.** P4430, UK

> **Unfortunately many scams are becoming very sophisticated and one has to be very careful online.**
> P2566, Australia

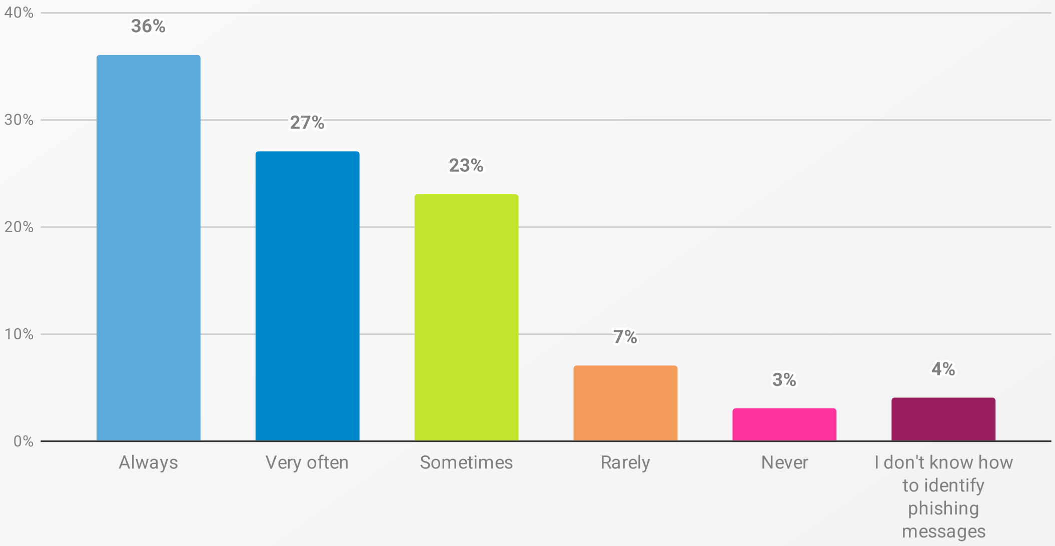
> **I am scared stiff these days. I am not happy on my computer like I used to be.** P2841, UK

> **I get so many emails that I'm scared to open them because some use the same names as companies I use.**
> P21859, US

But when it comes to behavior, how often do people inspect emails and links, and what steps do they take to verify them?

Sixty-three percent reported 'always' or 'very often' checking messages (e.g., emails, texts, or social media) for signs of phishing before clicking any links or responding to them (Figure 67), which is a 4% drop from 2024. Ten percent (same as in 2024) reported 'never' or 'rarely' doing so, and 4% (+2% from 2024) admitted not knowing how to identify phishing emails.

Figure 67. Frequency of checking messages for signs of phishing before taking action.

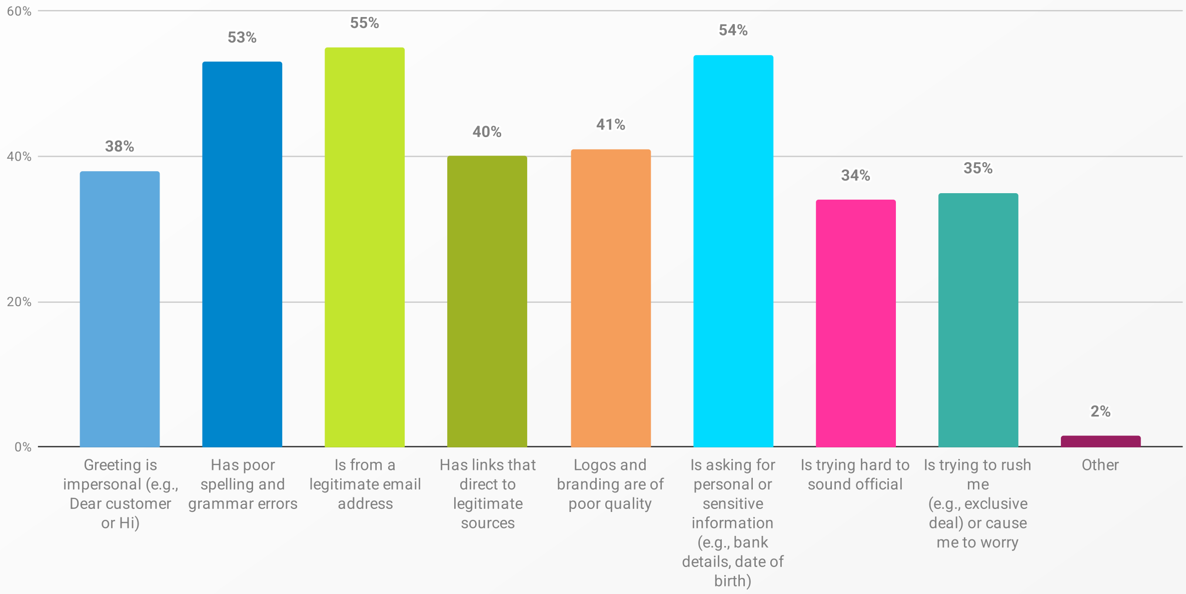


Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

Generationally, Baby Boomers (72%) and the Silent Gen (71%) are most likely to inspect messages, compared to only 55% of Gen Z. Conversely, most likely to only 'sometimes' check their messages were Gen Z (32%) and Millennials (26%). Younger generations led the way in not checking: 11% of both Gen Z and Millennials said they 'rarely' or 'never' inspect messages.

The most common verification step was checking if an email came from a legitimate address (55%, Figure 68), closely followed by checking if it asks for personal or sensitive information (54%), and for poor spelling and grammatical errors (53%).

Figure 68. Steps taken to verify email legitimacy – '*I check whether the email...*'



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

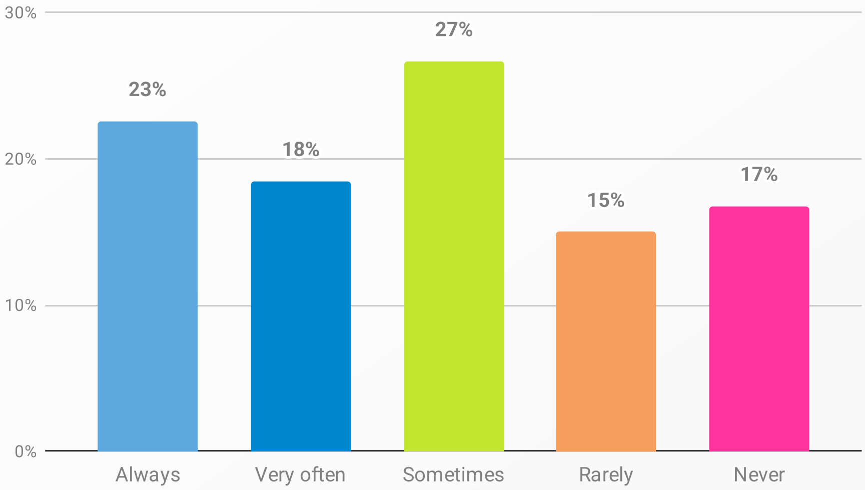
> **If something seems too good to be true, it usually is. Remember this and you won't go too far wrong.**
> P22042, UK

> **The bad people are so good it's hard to tell these days what's real.** P3281, US

But here's the catch: While 55% reported checking the sender's email address, people often stop short of double-checking with the sender. Thirty-two percent (a 5% increase from 2024) admitted to 'never' or 'rarely' doing so, while 41% (-4% from 2024) reported contacting the sender either 'very often' or 'always' to ask about a potential phishing message before clicking the link or opening the attachment (Figure 69).

Across most generations, the habit of verifying suspicious messages before acting has declined. The data shows a widespread increase in the percentage of users who 'never' or 'rarely' check with the sender, with this trend being particularly pronounced among older generations. This shift is accompanied by a mixed pattern in security-conscious behavior, as most generations either decreased or saw only minor increases in how often they 'always' or 'very often' verify messages, with the most dramatic decline in this habit also belonging to the Silent Gen.

Figure 69. *'If someone you know sends you a message you're unsure of (a potential phishing message), how often do you reach out to the person to ask about it before you click the link or open the attachment?'*

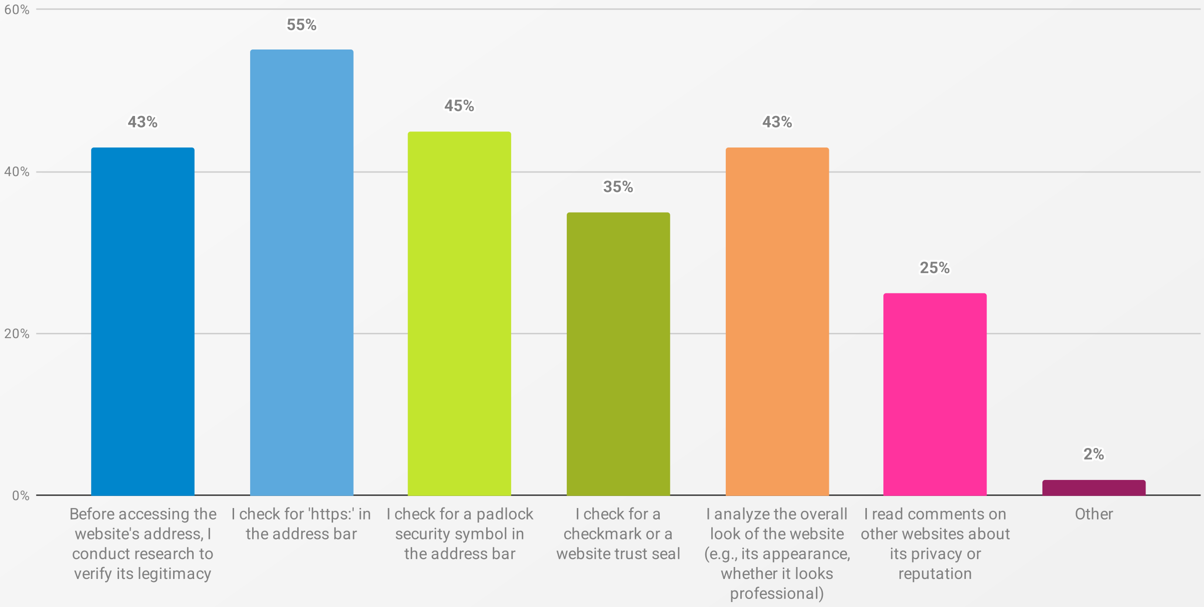


Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

What about verifying a website? What steps do people take to check their legitimacy (Figure 70)?

The top verification methods were checking for 'https:' in the address bar (55%, -3% from 2024), checking for a padlock security symbol in the address bar (45%, -2% from 2024), analyzing the overall look of the website (43%, -3% from 2024), and conducting research on the website (43%, +2% from 2024).

Figure 70. Steps taken to verify website legitimacy.



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

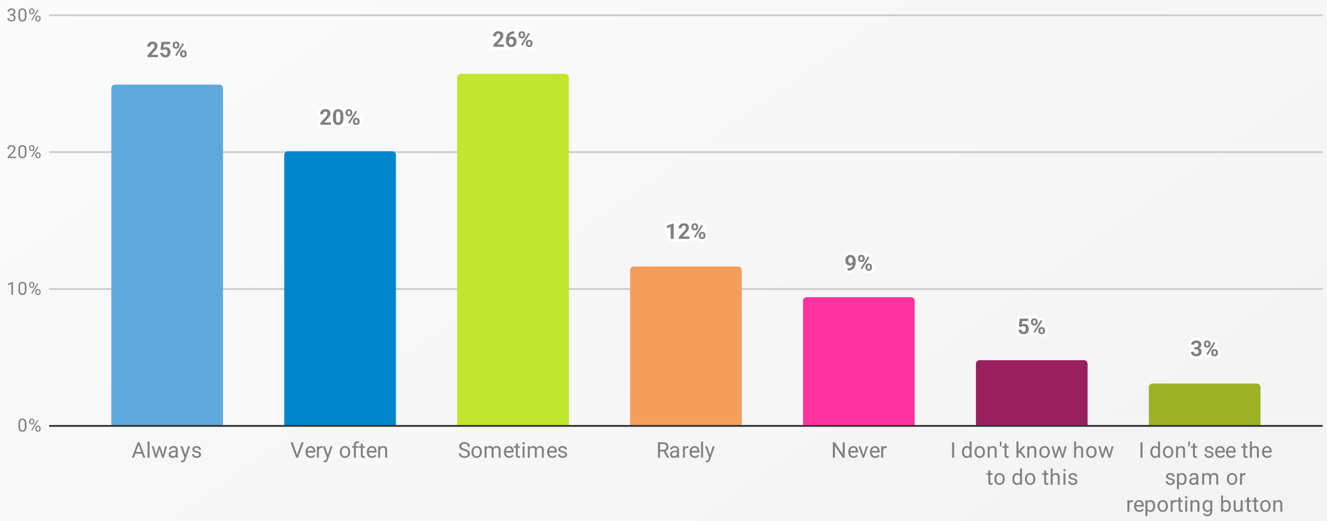
In conclusion, people say they're confident in spotting phishing, but their actions don't always back it up. The gap between perception and practice is widening, particularly when it comes to consistent verification habits. This is further complicated by a decline in the habit of proactively verifying suspicious messages with senders. To mitigate the ongoing threat of phishing, there is a clear need for strategies that not only build confidence, but also reinforce the importance of consistent verification behaviors.

But what happens when we look at reporting instead of just recognition?

6.6.2 Snitch or sink: Reporting phishing messages

Less than half (45%, Figure 71) report phishing 'always' or 'very often', a 2% drop from 2024. Less than a quarter (21%, same as last year) mentioned they 'never' or 'rarely' report it. And, just like last year, 8% of participants either didn't know how to report it, or didn't see the 'spam' or 'report' button. This means there are still 29% who are not taking action against cybercriminals, just like in 2024.

Figure 71. *'How often do you report phishing messages (e.g., email or social media) by using the 'spam' or 'report phishing' button?'*



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

So, what's stopping that 21%? Among those (N=1470) who 'never' or 'rarely' report phishing messages, 68% agreed they would do so if it helped to stop cybercriminals. A further 64% would report phishing if it would stop spam messages from getting into their inbox. Additionally, 60% claimed they would report phishing if they trusted the phishing reporting process.

We really hope you're not drinking a shot every time we say 'mixed picture', because guess what... Phishing reporting behaviors are a mixed picture. Plenty of people are doing the right thing, but the slight drop in reporting highlights a clear issue: many just don't see the point. The data suggests that a key factor in underreporting is a perceived lack of tangible benefit. But to flip that on its head, a big chunk of people could easily be influenced to report phishing if they believed it would help stop criminals or reduce spam. Clearer communication and demonstrable results are needed from reporting systems, to translate passive awareness of phishing into consistent and active reporting behavior.

These findings are consistent with research[40] showing that underreporting is influenced by people's confidence in their ability to report (self-efficacy) and their fear of negative outcomes, such as being embarrassed by a false report. The fact that most reporting portals fail to provide users with direct feedback helps explain the 'lack of tangible benefit' we see here, and it supports the need for communication and systems that reduce user dissonance and encourage active participation.

In short, people don't love shouting into the void. Show them that their reports matter, and reporting rates will rise.

Staying safe from phishing

Phishing isn't going anywhere. But its impact can be reduced if people are supported with the right tools and environment.

1. Train people to spot the signs
Keep the guidance clear and simple. Encourage people to ask themselves:

1. Do the From details match the sender details?
2. Am I being asked to do something unusual?
3. Does the message include a link or attachment I do not recognize?

2. Look deeper than click rates
It is not enough to measure how many people click on simulated phishing emails. Find out why they clicked. Use point-of-click or post-click surveys, or bake influencing techniques into simulated templates. Once you know the reason, you can provide tailored support.

3. Make reporting easy and worthwhile
Keep the process quick and intuitive. Provide immediate acknowledgment, and follow up with feedback on what action was taken. Above all, avoid blame. Punishing people for clicking discourages reporting and undermines progress.

Further reading

- Practical advice in the phishing guidance from the NCSC.
- CybSafe explains how simulated phishing adds value.
- Explore Stay Safe Online's advice on phishing.

So, human behavior: still messy in 2025. But the biggest challenge in this decade? Keeping up with the tool that never sleeps: AI. Ready or not, here it comes.

[40] Kwak, Y., Lee, S., Damiano, A., & Vishwanath, A. (2020). Why do users not report spear phishing emails?. *Telematics and Informatics*, 48, 101343.

7. Large liability model? Artificial intelligence (AI)

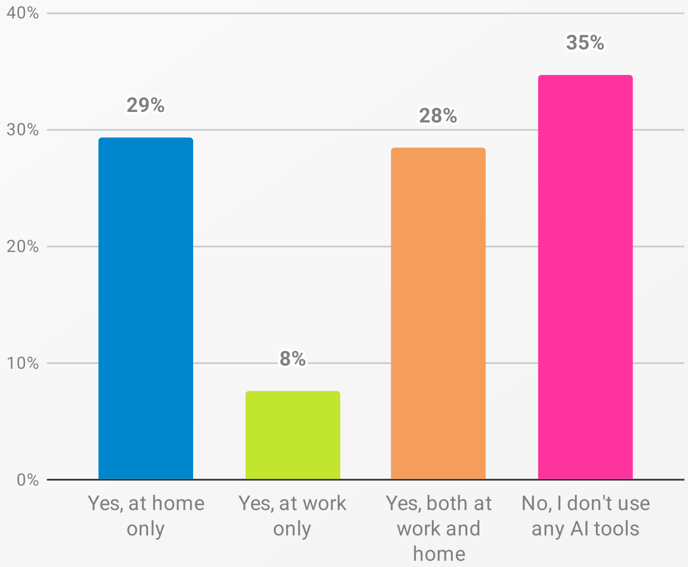
While some superpower leaders are busy using AI to turn themselves into the pope for the lols, the rest of us are already living in a world where it runs our jobs, shopping, and small talk. This chapter looks at how people are adopting AI, what they're feeding it, and whether they understand the risks. We look at how people perceive AI's impact on their work and personal security, shedding light on the critical balance between AI's benefits and its very tangible risks.

First, what are people doing out there? And what secrets are they spilling?

7.1 Bot BFFs all round: Adoption & data sharing

What a difference a year makes! The percentage of people not using any AI tools has dropped significantly from 65% last year to 35% this year (Figure 72). That's a complete flip from last year, as the 65% of participants who now use AI tools is the same percentage who reported not using them in 2024. Much of this is personal use, with 29% using AI tools exclusively at home, and 28% using them both at home and work.

Figure 72. ***'Do you use any AI tools at home or at work?'***

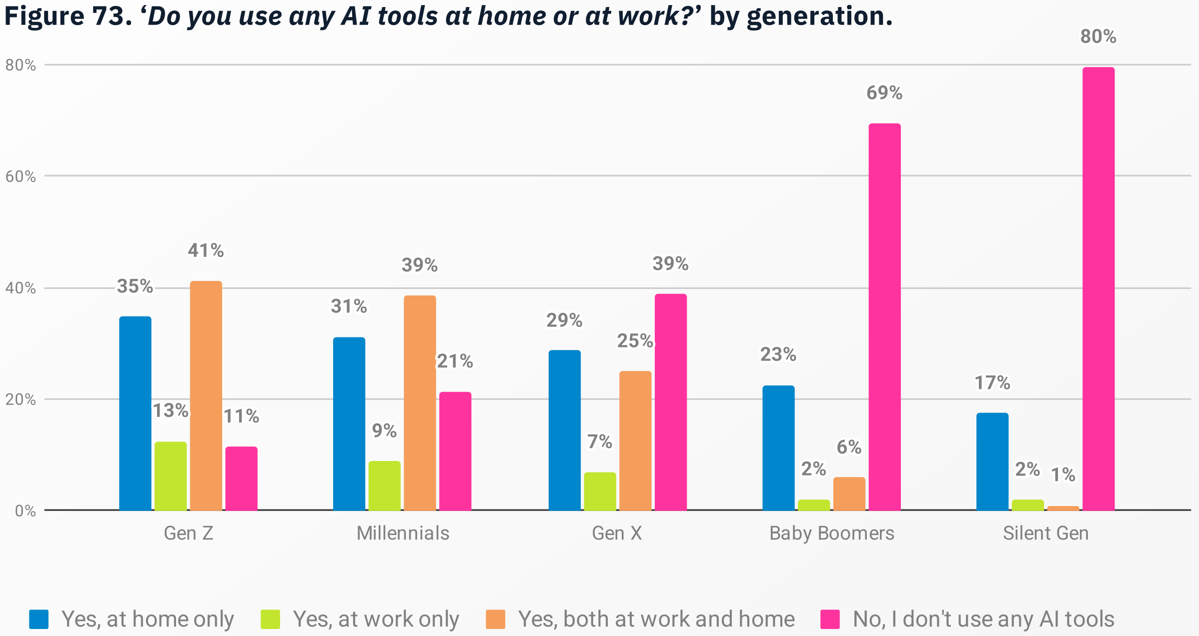


Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

AI tool usage is highest among younger participants, and drops with age. Gen Z leads the pack at 89% (+17% from 2024), followed by Millennials at 79% (+17%), Gen X at 61% (+23%), Baby Boomers at 31% (+16%), and the Silent Gen at just 20% (+13%, Figure 73). This trend is consistent across home-only, work-only, and both home and work usage.

This is further highlighted by the fact that the most active AI users are Millennials (41%) and Gen Z (39%), who use AI in both home and work contexts. Across all age groups, AI use is more prevalent at home than in the workplace. In stark contrast, a significant digital divide persists: 80% of Silent Gen and 69% of Baby Boomers report not using any AI tools.

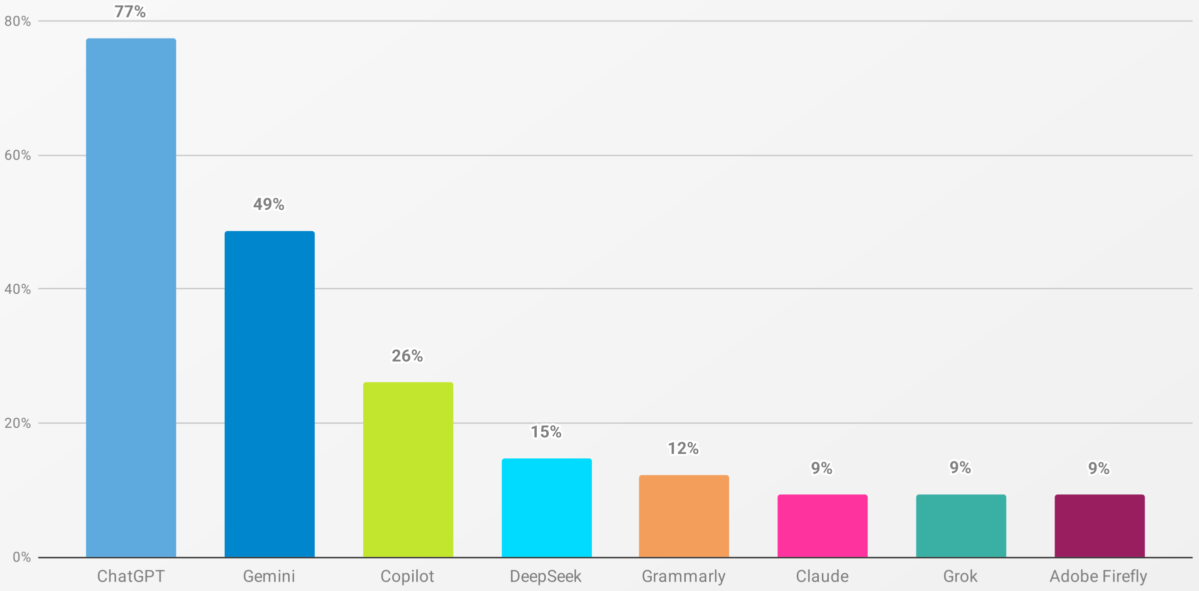
Figure 73. ‘*Do you use any AI tools at home or at work?*’ by generation.



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

Among AI users (N=4573), ChatGPT is the most popular, with 77% (+12% from 2024) reporting usage, followed by Gemini (49%, +19% from 2024), Copilot (26%, +7% from 2024), DeepSeek (15%), and Grammarly (12%, Figure 74). Other popular AI tools included Claude, Grok, and Adobe Firefly, and based on the qualitative responses, we also noted mentions of Meta AI, Siri, Alexa, and Perplexity.

Figure 74. ‘*What AI tools do you use?*’

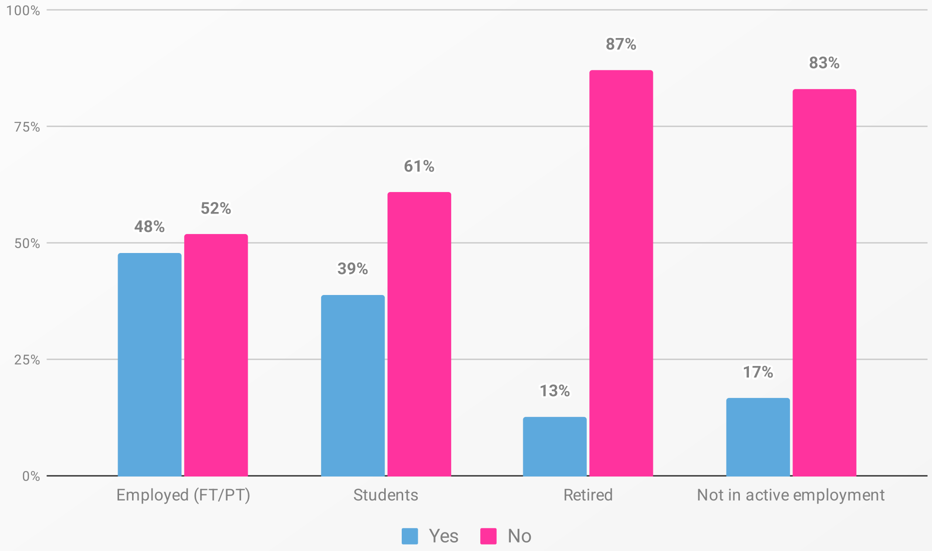


Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 4573 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

We wanted to know whether AI users (N=4573) received any training on the security and privacy risks associated with these tools. And... most hadn't. Fifty-eight percent reported they hadn't, a 3% increase from 2024. This mirrors wider findings[41] that a majority of employees believe they are not being trained properly, contributing to an 'AI adoption gap' where tools are often misused, underutilized, or generally misunderstood.

Breaking this down by employment status (Figure 75), the picture is predictable in some ways and surprising in others. The vast majority of those not actively employed (87%, +3% from 2024) and retirees (83%, same as in 2024) have not undergone AI training. But even among the employed, over half (52%) still hadn't received any, the same as last year. And students are slipping backward too, with a 3% increase in those reporting no training.

Figure 75. '*Have you received any training about the security and privacy risks of AI tools?*' by employment.



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 4573 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

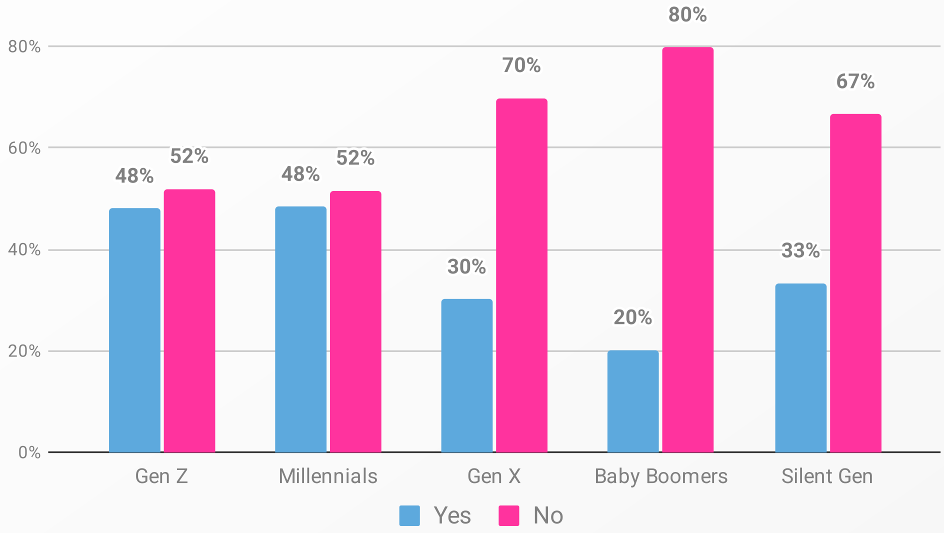
Given the high usage and low training rates among those using AI at work (N=2521), it's not surprising that there was an increase (5%) in sensitive data sharing: 43% admitted sharing sensitive work information with AI tools without their employer's knowledge.

Using unauthorized AI tools without the knowledge or approval of IT or security teams is now commonly referred to as 'shadow AI' (a close cousin of shadow IT), and it's a growing trend. It's usually driven by employees seeking to boost their productivity with tools they prefer or to bypass lengthy internal approval processes. But the risks are obvious: many of these unapproved tools use entered data for training, creating a real possibility of confidential information leaking into the wild.

[41] Employees are using AI where they know they shouldn't. (2025, June 18). *Help Net Security*. Retrieved August 11, 2025, from https://www.helpnetsecurity.com/2025/06/18/employees-ai-potential/

And the pattern is generationally skewed, just like last year. Forty-eight percent of Gen Z and Millennials shared sensitive work info with AI tools, compared to 30% of Gen X, 20% of Baby Boomers, and 33% of Silent Gen (Figure 76).

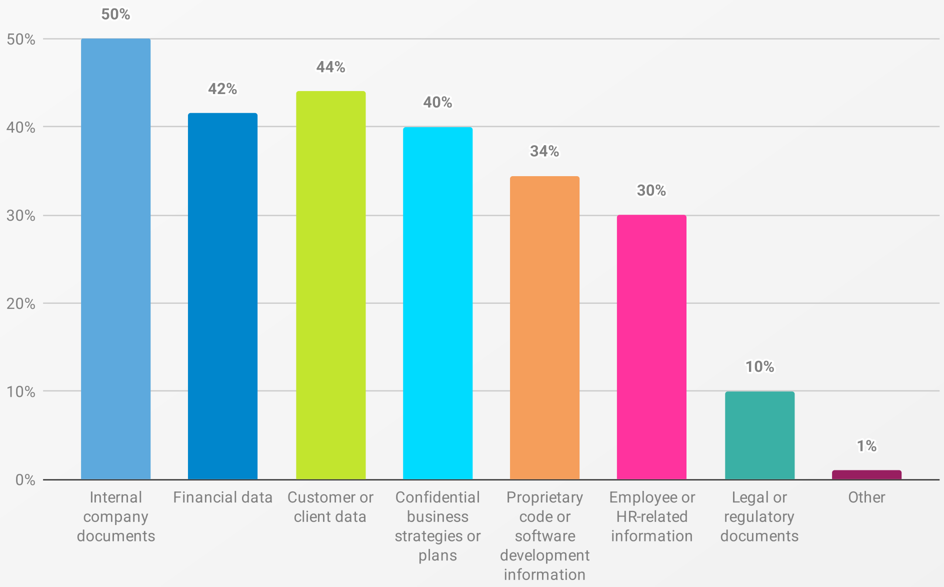
Figure 76. '*Have you ever shared sensitive work information with AI tools without your employer's knowledge?*' by generation.



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 4573 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

This year, we dug deeper into what sensitive data people are actually disclosing (Figure 77). Of the people who shared data with AI tools (N=1074), 50% reported sharing internal company documents, and 44% admitted sharing customer or client data with AI tools. Financial data (42%), confidential business strategies or plans (40%), proprietary code or software development information (34%), and employee or HR-related information (30%) were also commonly shared by AI users.

Figure 77. '*What kind of sensitive work information did you share with AI tools?*'



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 1074 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

In conclusion, the rapid adoption of AI tools in the workplace, especially among younger generations, has far outpaced formal training and safeguards. The high rate of sensitive data sharing, including internal documents, customer data and confidential business plans, underscores a critical gap between the convenience of AI and employee awareness of its risks. Organizations urgently need clear policies and training to prevent leaks and protect sensitive information in the AI-driven workplace.

Are you thinking what we're thinking? If people are this casual with what they share, how confident are they in spotting what's real and what's machine-made? Time to find out.

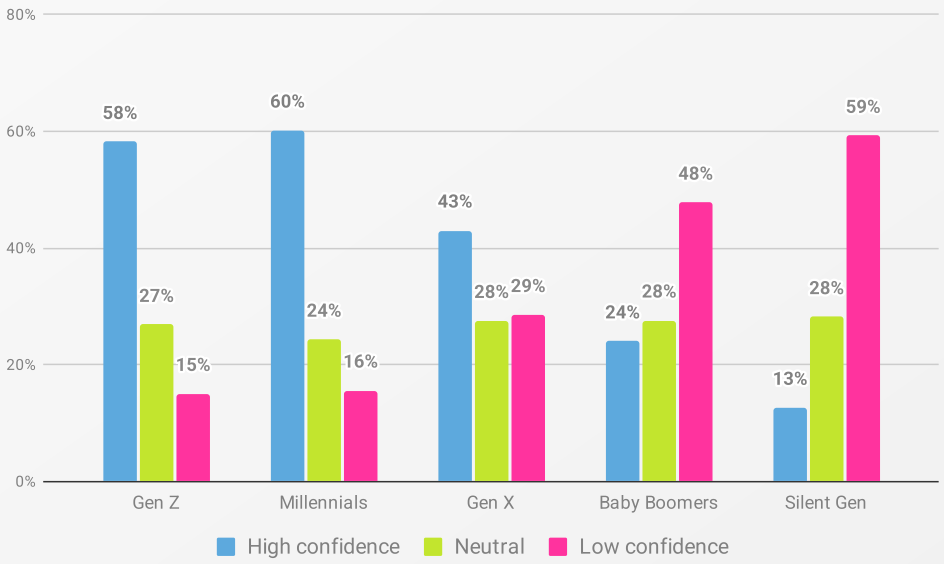
7.2 Bot the difference: Confidence in recognizing AI content

How do people rate their spotting skills, then? Overall, participants felt moderately confident in their ability to recognize AI-generated content (M=6.09, SD=2.6, N=7000).

Confidence in recognizing AI-generated content has risen by 11% since 2024, with almost half (48%) rating their confidence levels as high. Twenty-six percent expressed low confidence, and the same percentage rated their ability to be somewhere in the middle.

Once again, Millennials (60%) and Gen Z (58%) led the way (Figure 78), with their confidence levels rising by 7% and 5% respectively. In contrast, the Silent Gen remains the least assured, with 59% (-10% from 2024) reporting low confidence in recognizing AI-generated content, followed by Baby Boomers (48%, -7% from 2024). Still, confidence has risen across all generations since 2024.

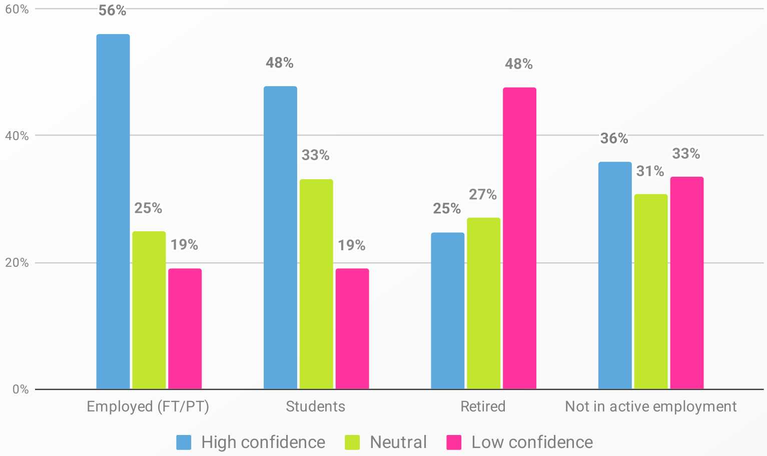
Figure 78. '*How confident are you in your ability to recognize AI-generated content?*' by generation.



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

By employment status, the pattern sharpens (Figure 79). A majority of employed participants (56%, +12% from 2024) felt confident, as did 48% of students (which actually represents a 4% drop). The highest proportion of retirees didn't feel confident (48%) in AI content recognition.

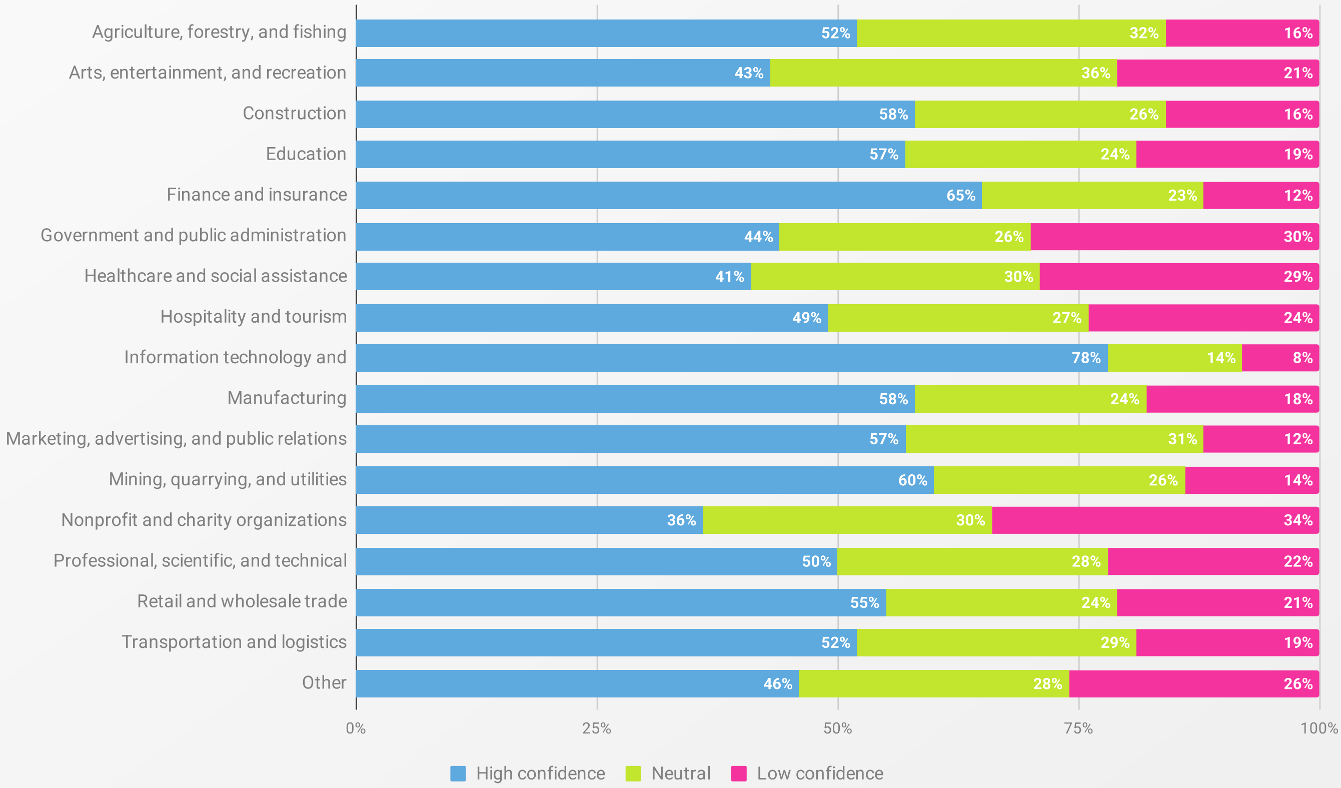
Figure 79. '*How confident are you in your ability to recognize AI-generated content?*' by employment.



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

Sector breakdowns revealed even clearer divides (Figure 80). Unsurprisingly, folks working in information technology and telecommunications had the highest level of confidence (78%), followed by finance and insurance (65%) and mining, quarrying, and utilities (60%). The lowest confidence levels were expressed among those working in nonprofit and charity organizations (34%), followed by government and public administration (30%) and healthcare and social assistance (29%).

Figure 80. '*How confident are you in your ability to recognize AI-generated content?*' by sector.



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 4555 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

> **AI can imitate legitimate sites very well.** P9492, US

> **AI makes everything seem real.** P13003, Brazil

The data reveals a notable confidence gap. Last year's data hinted at this, and the divide has only sharpened. While a large portion of the population feels sure in their ability to recognize AI-generated content, older groups and less technical sectors remain less sure. This lack of confidence may in fact be a realistic and healthy response to a complex threat. Building a more nuanced understanding of AI's capabilities and limitations across all segments of the population will be key to ensuring people remain vigilant and cautious when faced with AI-generated content.

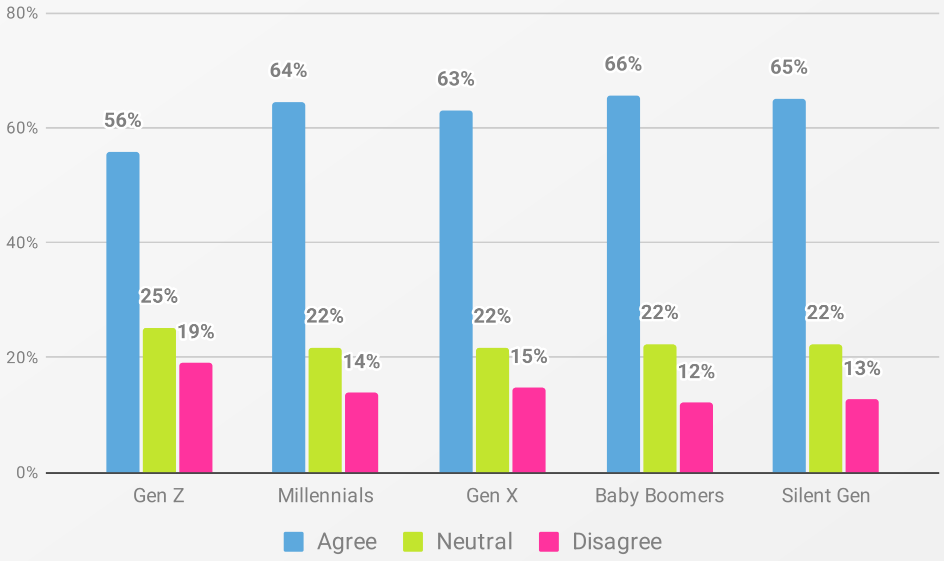
Regardless of confidence level though, there are real, tangible risks here that we can't ignore. Beyond the clever wordplay and funny filters, AI is fueling scams, fraud, and fresh security headaches.

7.3 Hype and heists: Perceived risks & concerns

Curious how people feel about the potential risks associated with AI tools? We were too. The headline here is that the majority of participants (63%) expressed concern about AI-related cybercrime, though this represents a slight 2% decrease from 2024.

Concerns were consistently high across generations (Figure 81). Baby Boomers topped the list (66%, -4% from 2024), closely followed by the Silent Gen (65%, -8% from 2024) and Millennials (64%, -2% from 2024). Gen Z seemed the least concerned (56%) about AI-related cybercrime.

Figure 81. '*I'm concerned about AI-related cybercrime.*' by generation.

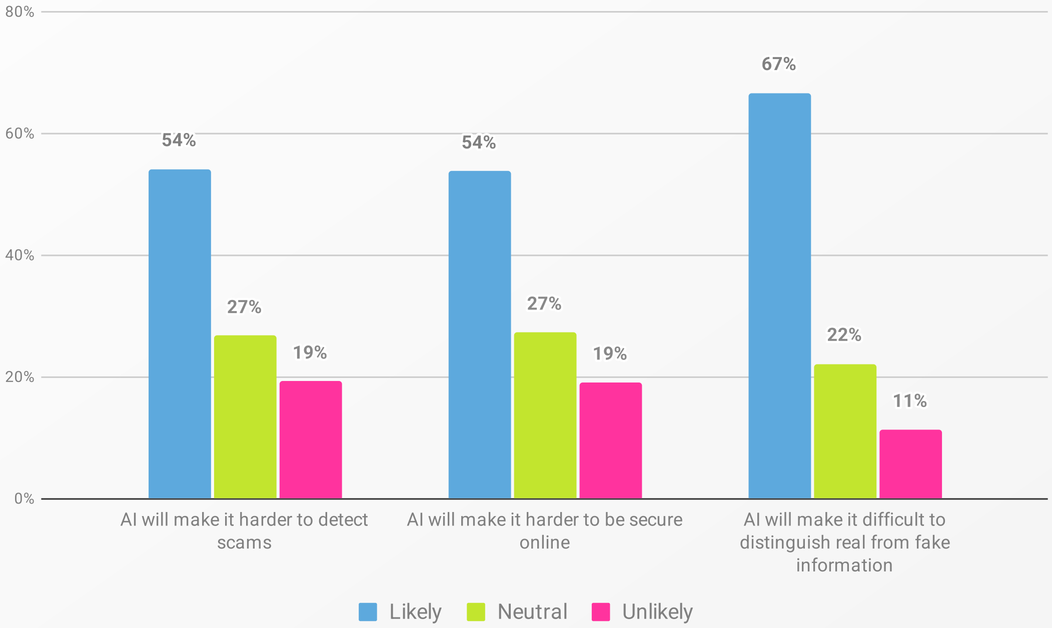


Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

Participants expressed a high level of concern about the negative security implications of AI. Slightly over half (54%) believe AI will make it harder to detect scams and to be secure online (Figure 82). The most pronounced concern is spotting manipulated content: 67% think AI will make it difficult to distinguish real from fake.

What's more, this apprehension was consistent across all generations. The perceived likelihood of AI making it harder to detect scams ranged from 48% (+7 from 2024) of the Silent Gen to 58% (same as in 2024) of Millennials. The perceived likelihood of AI making it harder to be secure online ranged from 50% (-7% from 2024) of Gen Z to 57% (-2% from 2024) of Millennials. The concern that AI will make it difficult to distinguish real from fake information ranged from 60% of Silent Gen to 70% of Baby Boomers.

Figure 82. Perceptions of AI's impact on scams and online security.



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

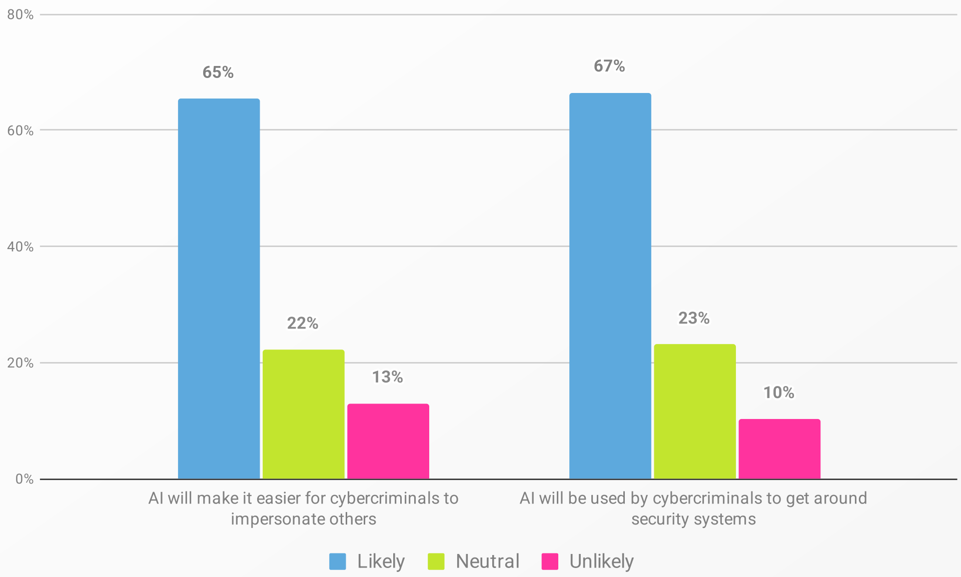
> **Up until now, I've always deleted any email that just looks wrong, but cybercriminals are getting more and more sophisticated, especially with the advance of AI.** P2933, UK

> **Scammers are getting better at scamming, especially with the help of AI.** P6527, US

Given last year's concerns about recognizing real vs fake being echoed again this year, we asked further questions. Unsurprisingly, the majority of participants felt that AI will make it easier for cybercriminals to impersonate others (65%) and that it will be used by cybercriminals to get around security systems (67%, Figure 83).

And again, both of these beliefs were consistently high across generations. The belief that AI will make impersonation easier ranged from 59% of Gen Z to 69% of Baby Boomers. The likelihood of criminals' use of AI to get around security systems was reported by 58% of Gen Z to 73% of Baby Boomers.

Figure 83. Perceptions of AI as a tool for cybercriminals.

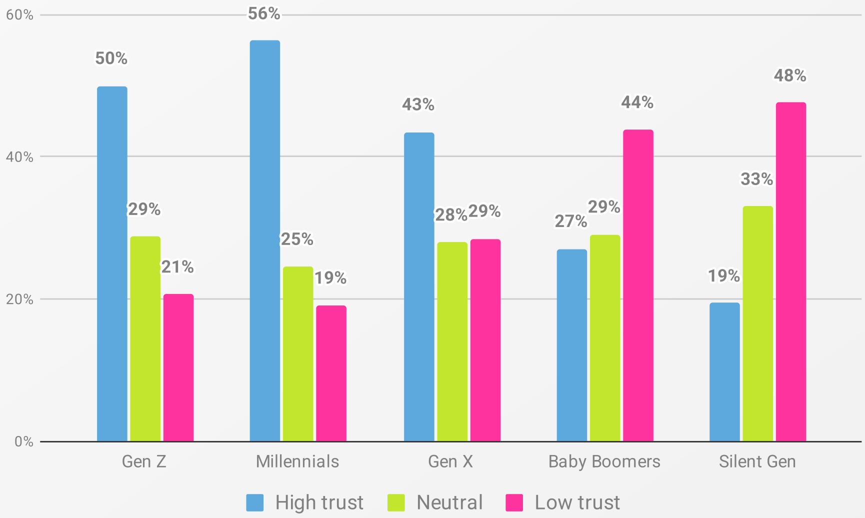


Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

And what about trust in companies implementing AI technologies responsibly? Those placing high trust rose from 36% to 45%. Those distrusting fell to 28% (-7%). The rest (27%) remained neutral.

Similar to last year, trust declines with age (Figure 84). The Silent Gen perceived companies' AI implementation to be the least trustworthy (48%, -8% from 2024), followed by Baby Boomers (44%, -9% from 2024). Millennials (56%, +3% from 2024) and Gen Z (50%, same as in 2024) expressed the highest level of trust.

Figure 84. Participants' level of trust in companies to implement AI responsibly, by generation.



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

Despite the increase, overall trust remains low. This skepticism is underscored by an open letter[42] from current and former employees of prominent AI companies like OpenAI and Google DeepMind, warning that these companies were not implementing sufficient safeguards and were resisting effective oversight. These real-world doubts likely reinforce public unease.

The data on AI-related concerns, from the rise of cybercrime to general trust in companies, reveals a troubling landscape. People broadly believe AI will supercharge cybercrime, make scams harder to spot, and blur the line between fact and fake. This apprehension is particularly strong among older generations, yet a lack of trust in companies to implement AI responsibly is a sentiment shared by all age groups. These findings suggest that as AI becomes more prevalent, building confidence will require transparent and responsible AI development and clear education on both the benefits and the tangible security risks associated with these technologies.

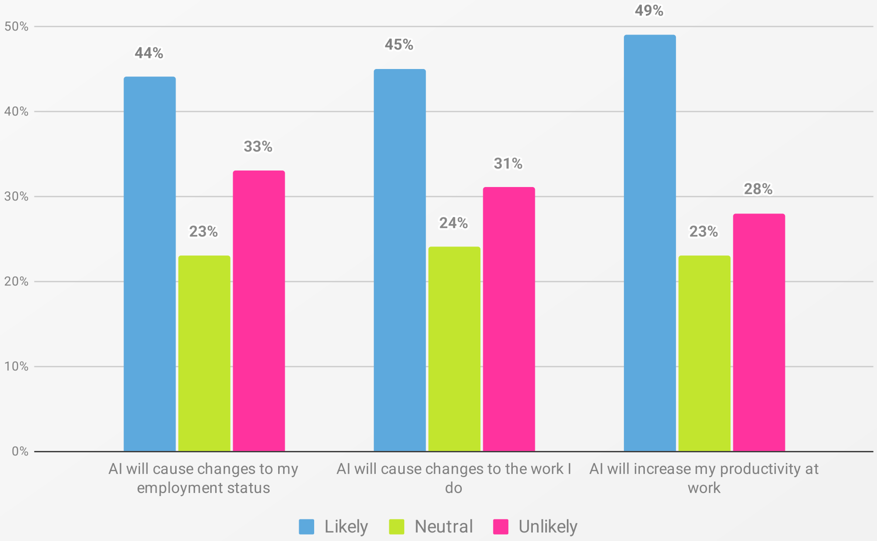
Which raises the next question: if people already worry this much about AI reshaping security, how do they feel about it reshaping work itself?

7.4 **Automation nation:** Perceived impact on work

Finally, what do people think about AI's impact on jobs and productivity (Figure 85)? Specifically, employment status, nature of one's work, and productivity at work.

Compared to 2024 – when views were fairly balanced – there's been a clear shift. This year, 44% believe AI would cause changes to their employment status (10% increase), 45% felt it would cause changes to the work they do (8% increase), and 49% thought AI would increase their productivity (11% increase). Still, a third remain unconvinced that AI will cause changes to their employment status (33%) or the work they do (31%).

Figure 85. Perceived likelihood of AI's impact on employment status, nature of work, and productivity.



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

[42] Robins-Early, N. (2024, June 4). OpenAI and Google DeepMind workers warn of AI industry risks in open letter. *The Guardian*. Retrieved August 11, 2025, from https://www.theguardian.com/technology/article/2024/jun/04/openai-google-ai-risks-letter

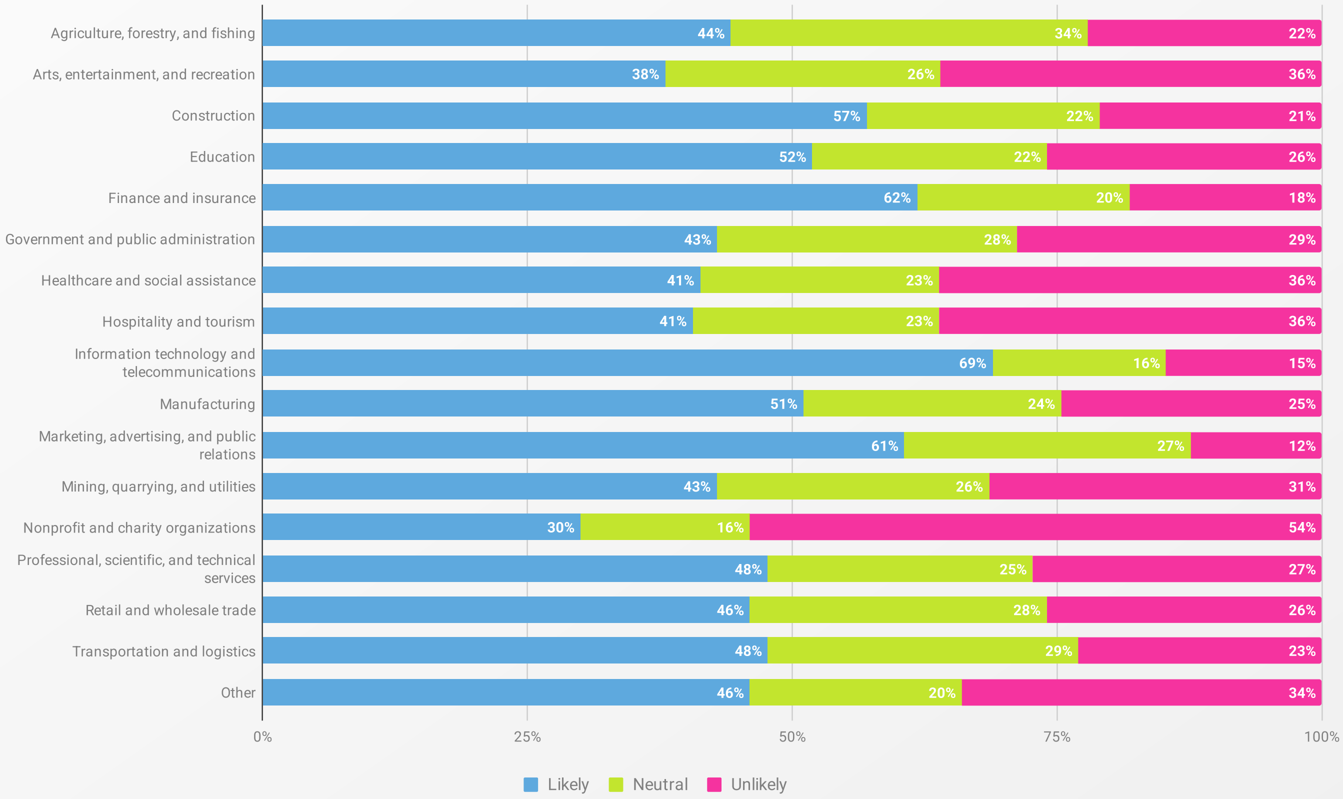
The belief that AI will reshape work is strongest among younger generations. Fifty-nine percent of Millennials and 53% of Gen Z believed AI would cause changes to their employment, as opposed to only 12% of Silent Gen and 20% of Baby Boomers. Similarly, 63% of Millennials and 59% of Gen Z reported that AI will increase their work productivity, as opposed to only 14% of Silent Gen and 22% of Baby Boomers. Our findings are in line with a recent poll[43] that found that half of UK adults (51%) are concerned that AI will take or alter their job, with this anxiety being particularly high among younger workers aged 25-34 (62%).

Across sectors, perceptions diverge (Figure 86). While the overall picture is mixed, tech-heavy sectors show the most concern, while many creative and service-oriented fields remain largely optimistic.

The highest level of concern was found in the information technology and telecommunications sector, where the majority of participants (69%) feel it's likely that AI will cause changes to their employment status. This is followed by other tech-reliant fields, finance and insurance (62%), and marketing, advertising, and PR (61%).

Conversely, some of the most optimistic sectors are typically less technologically focused. Slightly over half (54%) of the participants in nonprofit and charity organizations feel it is unlikely that AI will impact their employment, followed by arts, entertainment, and recreation, hospitality and tourism, and healthcare and social assistance (36% each).

Figure 86. Perceived likelihood of AI's impact on employment status, by sector.



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 4555 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

[43] Partridge, J. (2025, August 27). Half of UK adults worry that AI will take or alter their job, poll finds. *The Guardian*. Retrieved August 29, 2025, from https://www.theguardian.com/technology/2025/aug/27/half-of-uk-adults-worry-that-ai-will-take-or-alter-their-job-poll-finds

In conclusion, younger generations are bracing for disruption and even leaning into the idea that AI might make their jobs more productive. This stands in stark contrast to the skepticism and lower perceived impact among older generations.

Furthermore, the most technologically advanced sectors, such as information technology and finance, show the highest degree of concern that AI will change their employment status. Conversely, many creative and service-oriented fields, like nonprofit and arts, remain largely optimistic. The findings suggest that perceptions of AI's transformative effects are driven not only by age or tech-savviness, but also by the nature of one's work and AI's proximity to it.

Taken together, these generational and sectoral divides highlight the need for a nuanced approach to AI education and preparedness that addresses the unique concerns of different demographics.

Still here?

Congrats! You've survived passwords, phishing, MFA, and AI without rage-quitting. Together we've covered a lot of ground, so let's bring the main threads back together.

Conclusion

1. Shadow AI is here to stay
2. The perils of privacy fatalism
3. Tailor your training
4. Knowledge ≠ behavior
5. The Gen Z stare (of confidence)
6. Game over? Nah, next level unlocked

Conclusion

Shadow AI is here to stay

The rapid adoption of AI tools has significantly increased concerns around human risk in the workplace, and our data suggests this 'shadow AI' problem is becoming the new norm. The report reveals a dramatic shift in AI usage, with the percentage of people using AI tools jumping to 65% this year.

The problem lies in the fact that this adoption is happening without proper guidance or training, particularly in professional environments. The majority of AI users (58%) reported receiving no training on the security and privacy risks of these tools. As in none. Zero. Zilch.

This lack of training matters, because more than 40% of employed participants admitted to using AI tools to process confidential work information. This (now everyday) behavior, driven by a desire for increased productivity, creates an unmonitored flow of sensitive data into platforms with unknown security protocols. Translation: people are pasting the crown jewels into chatbots and hoping for the best 🫣

Researchers[44] have called 'shadow AI' a 'sociotechnical governance failure' that creates a 'governance drift zone'. In plain English, there are rules, but no one's following them. The study, which surveyed professionals and interviewed executives, found that while employees widely see AI as a productivity tool, organizations' governance frameworks are not keeping pace with employee practices. This lag exposes significant 'responsibility gaps' in high-risk functions, where AI-generated outputs can slip through without proper oversight.

The generational split only underscores this point: younger workers are leading the charge in feeding AI sensitive data. Gen Z and Millennials are the most frequent sharers of sensitive data with AI tools. Organizations must recognize that this isn't a fringe activity but a widespread, unmanaged risk. The solution isn't to ban AI (because the horse hasn't just bolted, it's writing your pitch decks), but to provide clear policies, secure tools, and effective training that empower employees to use AI safely, turning shadow AI into a managed and secure asset.

The same research study suggests practical fixes (AI tool registries, role-specific training, and internal audits) to help organizations shift from a posture of restriction to one of 'controlled enablement.' That's how you get the best of AI without the worst of shadow AI.

If AI is already in your workplace (and trust us, it is), solid AI governance needs to be there too.

[44] Silic, M., Silic, D., & Kind-Trüller, K. (2025). From Shadow It to Shadow AI—Threats, Risks and Opportunities for Organizations. *Strategic Change*.

The perils of privacy fatalism

Our findings show a clear and troubling trend toward privacy fatalism, the belief that a loss of personal data and security is just part of the deal when you go online. This year, more people shrugged and said that losing money or having personal details stolen online is basically inevitable. Add the fact that two-thirds of respondents don't believe law enforcement can deal with cybercrime, and you've got a recipe for resignation.

This psychological barrier is a major obstacle to improving cybersecurity. Because, as research has shown[45], when people think the game is rigged, they stop playing. So if individuals feel that a loss of privacy is inevitable, they're less likely to bother with protective actions. Our own data backs this up: yes, general security worry has increased, but feelings of personal responsibility and a sense of agency remain low.

Breaking this cycle will take more than simply raising awareness of threats. Practitioners need to focus actively on the other components core to changing behavior. These include considering how best to motivate people, ensuring that the opportunities are there to encourage good security behaviors – yes, good old COM-B[46] to the rescue!

For the day-to-day, this could mean activities such as moving beyond fear-based messaging and using creativity, storytelling, social proof (showing that others are taking protective actions), and methods such as Cialdini's[47] principles of persuasion (e.g, Authority: having a known security expert deliver the message).

Public trust and a sense of agency badly need to be restored, and fast. People need understand how security relates to them and they also need proof that individual actions and systemic protections can, in fact, make a tangible difference.

Until then, 'why bother?' will keep winning.

Tailor your training

When training competes with deadlines, inboxes, and meetings-that-should-have-been-emails, it needs to be short, relevant, and timed well.

The era of one-size-fits-all cybersecurity training is officially over. Our findings highlight a stark disconnect between the training formats provided and the preferences of different age groups and employment statuses.

[45] Penney, J. (2019). The Right to Privacy: The End of Privacy Fatalism. In Susi, M. (Ed.), *Human Rights, Digital Society and the Law* (p. 45). Routledge.

[46] Michie, S., Van Stralen, M. M., & West, R. (2011). *The behaviour change wheel: a new method for characterising and designing behaviour change interventions*. Implementation science, 6(1), 42.

[47] Cialdini, R. B. (2001). *Influence*. Allyn and Bacon.

While video content is the top choice overall (44%), older generations and retirees still prefer written materials. Meanwhile, entire industries under constant attack, such as retail and hospitality, report the lowest access to training.

This proves the obvious: a static, generic training program won't land with a diverse workforce. To be truly effective, training must be tailored to address their unique needs, habits, and preferences. This means adapting content formats, using microlearning to address time constraints, and real-world examples that actually fit the sector.

Meet people where they are, in a format they like, and you stand a chance of turning training from a box-ticking exercise into behaviors that stick.

When it comes to training, real change comes from relevance. The trick is matching the method to the person.

Knowledge ≠ behavior

Knowledge alone won't save you. Every year, our findings hammer home the same point: what people *know* about security and what they actually *do* are worlds apart.

Confidence in cybersecurity knowledge has dropped, with only half of the participants rating themselves as intermediate or advanced. But even where knowledge exists, behaviors don't follow. Unique password use is slipping, and weak password creation techniques are on the rise, particularly among younger generations. Plus MFA adoption is stagnating. Plenty of people know how to use it, but don't bother because they're convinced that basic passwords are 'good enough'.

This gap is a core challenge for the cybersecurity community. It suggests that simply providing information or mandating training isn't enough to drive lasting behavior change[49]. Behavioral science helps explain this. The COM-B model says behavior requires Capability, Opportunity, and Motivation. Traditional training only ticks the Capability box, which is why progress is so patchy.

Strategies need to go beyond traditional education and address both Opportunity and Motivation. This means designing systems that are easy to use, providing clear and immediate feedback on security actions, and creating a culture of shared responsibility that rewards positive behaviors rather than punishing mistakes. As suggested by research[50], the goal must be to make the secure choice the easiest and most intuitive choice.

[48] Aschwanden, R., Messner, C., Höchli, B., & Holenweger, G. (2024). Employee behavior: the psychological gateway for cyberattacks. *Organizational Cybersecurity Journal: Practice, Process and People*, 4(1), 32-50.

[49] 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.*

[50] Nurse, J. R., 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.

Did someone say Human Risk Management[51]? The data-driven approach that quantifies and predicts employee and organizational risk, delivers tailored real-time interventions, and builds healthier cybersecurity cultures? Start with the definitive guide to HRM. And if you're still hungry, this whitepaper is for you.

The Gen Z stare (of confidence)

For Gen Z, cybersecurity is one big paradox. They're the first true digital natives, defined by a lifelong, hyper-connected relationship with technology. Our research shows their deep-seated confidence and optimism about navigating the digital world. However, this same confidence is proving to be their greatest vulnerability.

You see, while Gen Z leads in AI adoption and are more likely to act as a 'cyber guru' for others, they are also the most frequently victimized generation. Our research found that 59% of Gen Z have lost money or data to online scams, and they are disproportionately hit by new threats like deepfake scams. Their misplaced confidence often translates into risky behaviors, as evidenced by their poor password hygiene and tendency to 'sometimes' update devices. Research[52] shows how people who overestimate their cyber skills are more vulnerable to victimization due to their false sense of security. Gen Z believe they're too savvy to be fooled, making them prime targets for criminals who exploit that very overconfidence.

The challenge, therefore, is to move beyond traditional awareness campaigns and address the root of this contradiction. The aim isn't to make Gen Z less confident, but to encourage a more realistic understanding of risk. Future efforts must channel their optimism and digital fluency into a new kind of vigilance that accepts that even the most tech-savvy can fall victim, and that secure behaviors remain the only true defence against an increasingly sophisticated threat landscape.

Gen Z might think they've seen it all already online. But even the most confident digital natives need some guardrails. Confidence is good. Overconfidence, though? It's giving 'scammer's dream'.

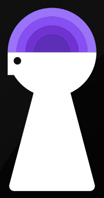
Game over?
Nah, next level unlocked

Is your boss asking you for the receipts? We've got you. Time to hit the appendices for the data, methods, country comparisons and take-it-to-the-board intel.

[51] Nurse, J. R., Milward, J., & Alashe, O. (2025, June). From Security Awareness and Training to Human Risk Management in Cybersecurity. In *International Conference on Human-Computer Interaction* (pp. 86-104). Cham: Springer Nature Switzerland.

[52] 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.

Appendices



Appendix A: Methodology

Survey design

We set out to understand not just what people do online, but what they believe, fear, and assume about security, AI, and five core cyber behaviors: maintaining good password hygiene, using multi-factor authentication (MFA), installing software updates promptly, backing up data regularly, identifying and reporting phishing attempts.

The survey mostly used multiple-choice and single-choice questions. These offered either 5- or 10-point Likert scales with descriptive options (e.g., ‘All of the time’ to ‘None of the time’) or two anchor points (e.g., ‘Strongly agree’ to ‘Strongly disagree’). For specific questions, participants also had the chance to choose ‘Other, please specify’ and give a written response in their own words.

And because numbers don’t always tell the whole story, one question on confidence in recognizing phishing attempts asked for a longer, open-ended answer. This provided richer, qualitative insight into why some people feel unsure about spotting scams.

Procedure

Participants were recruited via the Toluna[53] platform for the United States, the United Kingdom, Germany, Australia, India, Brazil, and Mexico. Everyone responded to the survey in their local language (e.g., German for Germany).

Participants were compensated for their time. They were briefed about the survey, and their informed consent was required before they could begin. They were asked not to reveal personal information and assured that their responses would be anonymized. It was stressed that participation was entirely voluntary, and respondents had the right to withdraw at any time. CybSafe’s Science and Research team collected no personally identifiable information.

Data collection ran from May 2 to May 27, 2025. The survey was designed to take less than 30 minutes, and participants completed it in 23 minutes on average.

[53] https://uk.toluna.com

Sample

A representative sample of 1,000 participants per country was recruited through the survey provider Toluna, giving a total of 7,000 participants. Sampling was balanced by gender and age, and all participants were aged 18 or older, with the average age being 45 years (SD=17.02). Detailed demographic information by country, including gender, age, and employment status, is presented in Table 1.

The generational breakdown was relatively even, with Millennials making up the largest group (30.2%), followed by Gen X (26.7%), Gen Z (21.1%), and Baby Boomers (20.5%). The Silent Gen (1.5%) was represented to a lesser degree.

The majority (65%) of participants were in employment (either full- or part-time), including students who were working (2.5%). Around a third (35.3%) reported not being employed, which included 18.8% who were retired.

Table 1. Participant demographics, by country.

Demographic		United States (N=1000)	United Kingdom (N=1000)	Germany (N=1000)	Australia (N=1000)	India (N=1000)	Brazil (N=1000)	Mexico (N=1000)	Total (N=7000)
Gender (N=7000)	Female	486 48.6%	492 49.2%	491 49.1%	492 49.2%	511 51.1%	491 49.1%	491 49.1%	3454 49.3%
	Male	514 51.4%	508 50.8%	509 50.9%	508 50.8%	489 48.9%	509 50.9%	509 50.9%	3546 50.7%
	Non-binary/ third gender	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%
	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%	0 0.0%	0 0.0%
Age (N=7000)	Gen Z (18-28)	181 18.1%	171 17.1%	142 14.2%	196 19.6%	292 29.2%	239 23.9%	259 25.9%	1480 21.1%
	Millennials (29-44)	298 29.8%	284 28.4%	242 24.2%	286 28.6%	346 34.6%	317 31.7%	339 33.9%	2112 29.8%
	Gen X (45-60)	242 24.2%	263 26.3%	278 27.8%	239 27.8%	253 25.3%	310 31.0%	284 28.4%	1869 26.7%
	Baby Boomers (61-79)	249 24.9%	257 25.7%	319 31.9%	256 25.6%	104 10.4%	134 13.4%	117 11.7%	1436 20.5%
	Silent Generation (80+)	30 3.0%	25 2.5%	19 1.9%	23 2.3%	5 0.5%	0 0.0%	1 0.1%	103 1.5%
Employment status (N=7000)	Employed	631 63.1%	637 63.7%	627 62.7%	626 62.6%	617 61.7%	624 62.4%	617 61.7%	4379 62.6%
	Full-time	506 50.6%	483 48.3%	476 47.6%	410 41.0%	518 51.8%	526 52.6%	469 46.9%	3388 48.4%
	Part-time	125 12.5%	154 15.4%	151 15.1%	216 21.6%	99 9.9%	98 9.8%	148 14.8%	991 14.2%
	Students	41 4.1%	45 4.5%	42 4.2%	40 4.0%	154 15.4%	61 6.1%	88 8.8%	471 6.7%
	Not working	21 2.1%	32 3.2%	18 1.8%	14 1.4%	120 12.0%	35 3.5%	55 5.5%	295 4.2%
	Working student	20 2.0%	13 1.3%	24 2.4%	26 2.6%	34 3.4%	26 2.6%	33 3.3%	176 2.5%
	Retired	227 22.7%	220 22.0%	263 26.3%	215 21.5%	98 9.8%	163 16.3%	133 13.3%	1319 18.8%
	Don't work or study outside home	101 10.1%	98 9.8%	68 6.8%	119 11.9%	131 13.1%	152 15.2%	162 16.2%	831 11.9%

Participants' highest level of education for each country is listed in Table 2. The most common qualification was an undergraduate degree, held by 31.8% of the total participants.

Table 2. Participants' education levels, by country.

Highest level of qualification (N=7000)	United States (N=1000)	United Kingdom (N=1000)	Germany (N=1000)	Australia (N=1000)	India (N=1000)	Brazil (N=1000)	Mexico (N=1000)	Total (N=7000)
Some school / high school credit, no diploma or qualification	82 8.2%	45 4.5%	5 0.5%	113 11.3%	58 5.8%	130 13.0%	32 3.2%	465 6.6%
Primary / secondary education	339 33.9%	285 28.5%	186 18.6%	182 18.2%	78 7.8%	208 20.8%	215 21.5%	1493 21.3%
Trade, technical, or vocational training	131 13.1%	192 19.2%	470 47.0%	264 26.4%	53 5.3%	128 12.8%	187 18.7%	1425 20.4%
Undergraduate degree	307 30.7%	284 28.4%	167 16.7%	276 27.6%	364 36.4%	348 34.8%	479 47.9%	2225 31.8%
Postgraduate degree	108 10.8%	160 16.0%	114 11.4%	142 14.2%	340 34.0%	160 16.0%	67 6.7%	1091 15.6%
Professional degree	33 3.3%	34 3.4%	58 5.8%	23 2.3%	107 10.7%	26 2.6%	20 2.0%	301 4.3%

A detailed overview of the professional sectors for the total employed sample (N=4555) is provided in Table 3. Employment spans a wide range of industries, with a few sectors demonstrating a high concentration of workers. The top three most represented industries were:

- Information technology and telecommunications (14.2%)
- Retail and wholesale trade (11.6%)
- Education (9.9%)

Table 3. Industries employed participants work In, by country.

Industry (N=4555)	United States (N=651)	United Kingdom (N=650)	Germany (N=651)	Australia (N=652)	India (N=651)	Brazil (N=650)	Mexico (N=650)	Total (N=4555)
Agriculture, forestry, and fishing	14 2.2%	7 1.1%	26 2.5%	12 1.8%	10 1.5%	14 2.2%	13 2.0%	86 1.9%
Arts, entertainment, and recreation	25 3.8%	16 2.5%	20 2.1%	26 4.0%	18 2.8%	15 2.3%	20 3.1%	140 3.1%
Construction	65 10.0%	41 6.3%	33 5.1%	52 8.0%	28 4.3%	21 3.2%	56 8.6%	296 6.5%
Education	45 6.9%	62 9.5%	76 11.7%	57 8.7%	82 12.6%	47 7.2%	82 12.6%	451 9.9%
Finance and insurance	47 7.2%	60 9.2%	61 9.4%	45 6.9%	80 12.3%	47 7.2%	34 5.2%	374 8.2%
Government and public administration	24 3.7%	30 4.6%	43 6.6%	33 5.1%	16 2.5%	39 6.0%	34 5.2%	219 4.8%
Healthcare and social assistance	71 10.9%	60 9.2%	73 11.2%	68 10.4%	31 4.8%	41 6.3%	24 3.7%	368 8.1%
Hospitality and tourism	34 5.2%	31 4.8%	23 3.5%	47 7.2%	17 2.6%	19 2.9%	31 4.8%	202 4.4%
Information technology and telecommunications	85 13.1%	101 15.5%	56 8.6%	55 8.4%	156 2.4%	154 23.7%	39 6.0%	646 14.2%
Manufacturing	44 6.8%	34 5.2%	54 8.3%	36 5.5%	77 11.8%	27 4.2%	61 9.4%	333 7.3%
Marketing, advertising, and public relations	13 2.0%	15 2.3%	11 1.7%	8 1.2%	35 5.4%	27 4.2%	28 4.3%	137 3.0%
Mining, quarrying, and utilities	6 0.9%	6 0.9%	6 0.9%	8 1.2%	4 0.6%	1 0.2%	4 0.6%	35 0.8%
Nonprofit and charity organizations	9 1.4%	11 1.7%	12 1.8%	9 1.4%	1 0.2%	2 0.3%	6 0.9%	50 1.1%
Professional, scientific, and technical services	26 4.0%	43 6.6%	39 6.0%	58 8.9%	32 4.9%	56 8.6%	50 7.7%	304 6.7%
Retail and wholesale trade	76 11.7%	80 12.3%	71 10.9%	91 14.0%	35 5.4%	78 12.0%	96 14.8%	527 11.6%
Transportation and logistics	25 3.8%	26 4.0%	34 5.2%	23 3.5%	9 1.4%	27 4.2%	30 4.6%	174 3.8%
Other	42 6.5%	27 4.2%	23 3.5%	24 3.7%	20 3.1%	35 5.4%	42 6.5%	213 4.7%

Data quality

To ensure data quality, the survey providers applied several safeguards. If a participant's response was determined to be of a 'low' quality (e.g., incomplete responses), they were excluded and replaced by another participant to meet the required sample size. The survey included two attention checks, designed to exclude potential 'bots' and participants who were just clicking through the survey without properly reading the questions.

Data analysis

Descriptive statistical analyses were conducted on all Likert-based questions, providing frequencies (N) and proportions (%). Proportions were then visualized using tables, charts, and various data visualization techniques.

All 5- and 10-point Likert scale responses (e.g., 'Strongly agree' to 'Strongly disagree') were recoded into 1-3 options (e.g,. 'Agree', 'Neutral', 'Disagree') for better understanding and clearer data visualization.

Qualitative responses were analyzed using thematic analysis. Selected quotes were included to illustrate the themes and add depth. Non-English responses were translated into US English using machine translation.

In Appendix B, we highlight comparisons with findings from the Oh, Behave! 2024-25 report. Since this is the first time we gathered data from Brazil and Mexico, no comparisons were made to last year's data for these countries.

Appendix B: Country comparisons

Spoiler: What works in London doesn’t always work in Lucknow.

This appendix provides a detailed country-by-country comparison of cybersecurity attitudes, perceptions, and behaviors among our participating countries: the United States, the United Kingdom, Germany, Australia, India, Brazil, and Mexico.

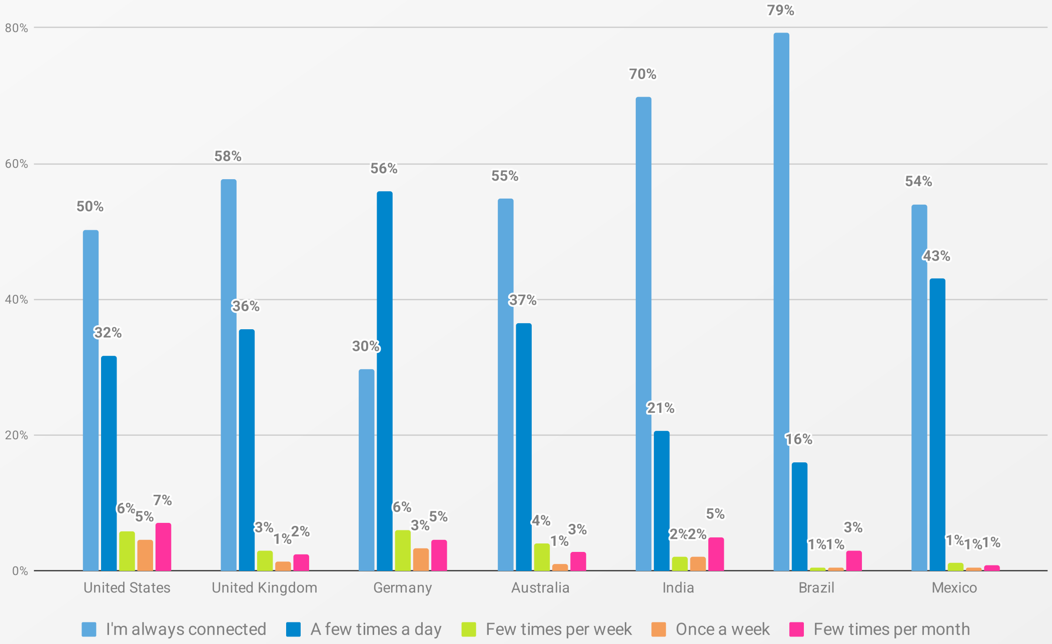
The analysis spans a wide range of topics, including online presence, attitudes and beliefs about online security, the media’s role in shaping attitudes, and cybersecurity culture in the workplace. It also explores attitudes toward victimization, cybercrime victimization itself, and behaviors related to password hygiene, MFA usage, updating software, and backups. Finally, it highlights differences in AI usage and perceptions.

While there are plenty of similarities, we were most interested in the areas of difference. They shed light on how national trends and cultural contexts influence cybersecurity attitudes, behaviors, and decision-making.

Online presence

The majority of participants from Brazil (79%) and India (70%, -1% from 2024) are ‘always’ connected, along with 58% (+2% from 2024) from the UK, 55% (same as in 2024) from Australia, 54% from Mexico, and 50% (-3% from 2024) from the US (Figure 87). In comparison, only 30% (-3% from 2024) of participants from Germany reported ‘always’ being connected.

Figure 87. ‘*How frequently do you use the internet?*’ by country.



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

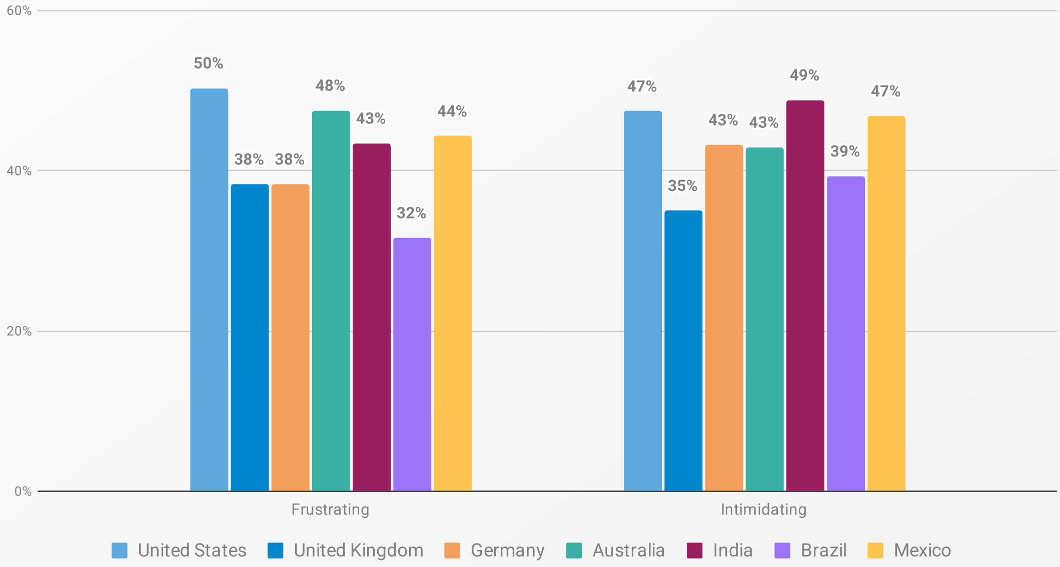
Attitudes, beliefs, & perceptions about online security

There were some striking differences between countries in terms of cybersecurity attitudes and perceptions.

The perception of security as frustrating varied notably (Figure 88). Half of participants in the United States (50%, -3% from 2024) felt that staying secure was frustrating, the highest percentage among all countries. This was closely followed by Australia (48%, +2% from 2024), Mexico (44%), and India (43%, -5% from 2024). Finding online security frustrating was the least common among participants from Brazil (32%), Germany, and the UK (both 38%).

When it came to security feeling intimidating, the picture shifted. Participants in India reported the highest agreement at 49% (+1% from 2024). The US and Mexico tied for the next highest percentage at 47%, followed by Germany and Australia, both at 43%. The lowest percentage of participants who found security intimidating was in the United Kingdom, at 35% (-4% from 2024).

Figure 88. '*I feel that staying secure is frustrating & intimidating.*' by country.

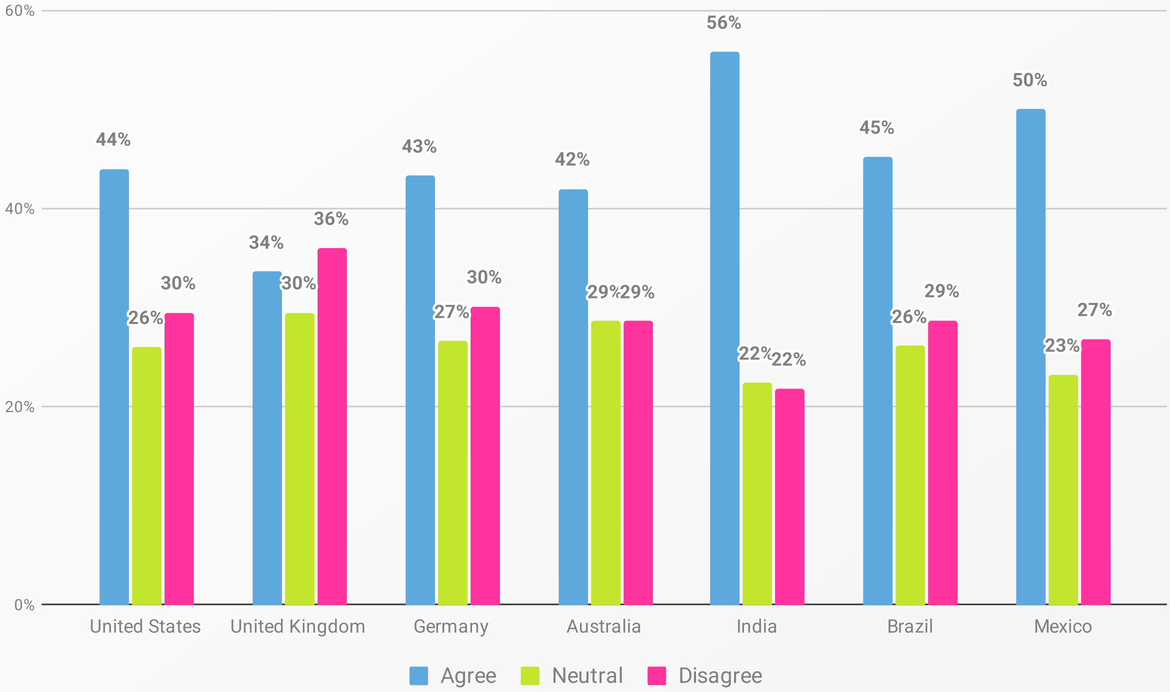


Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

A similar pattern emerged in perceptions of confusion (Figure 89).

This perception was highest in India (56%, a notable 14% increase from 2024), followed by Mexico (50%), the US (44%, +2% from 2024), Germany (43%, with another sharp increase of 13%), and Australia (42%, -2% from 2024), while the lowest percentage was found in the UK, at 34%, which represents an 8% decrease from 2024.

Figure 89. '*Most information on how to be secure online is confusing*.' by country.



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

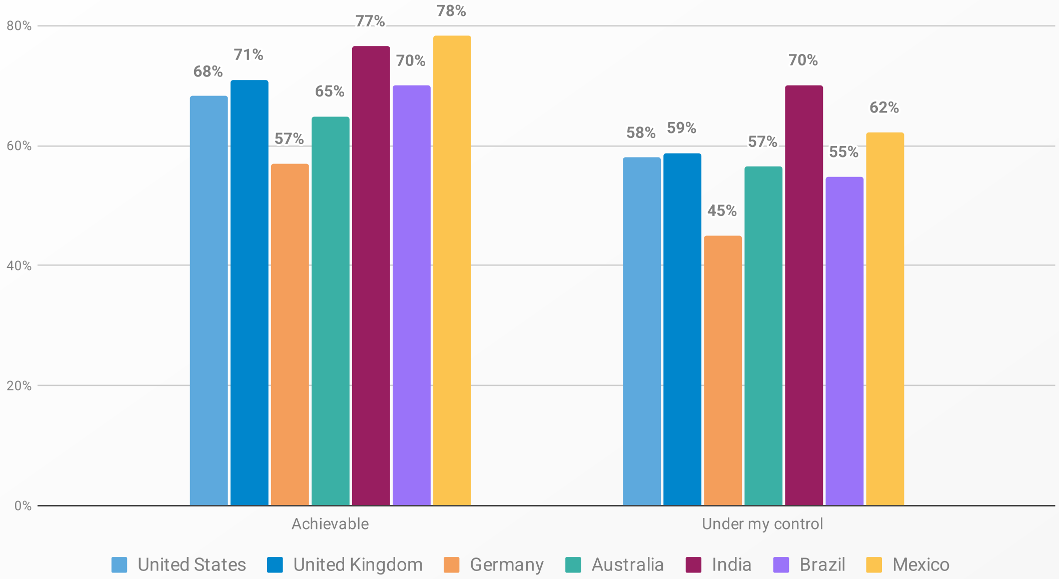
What about positive attitudes? The majority of participants from all countries felt that staying secure is achievable, ranging from 78% in Mexico, closely followed by India (77%, same as in 2024), to 57% (-3% from 2024) in Germany (Figure 90).

The perception of personal control over security was less universal than the belief that security is achievable. The percentages for feeling that security is under their control ranged from a high of 70% (+4% from 2024) in India to a low of 45% (+2% from 2024) in Germany.

Notably, Germany was the only country where a majority of participants didn't feel that staying secure was under their control.

Meanwhile, the UK (59%, +5% from 2024), the US (58%, +1% from 2024), and Australia (57%, +1% from 2024) all reported similar levels of confidence.

Figure 90. ‘*I feel that staying secure is achievable & is under my control.*’ by country.

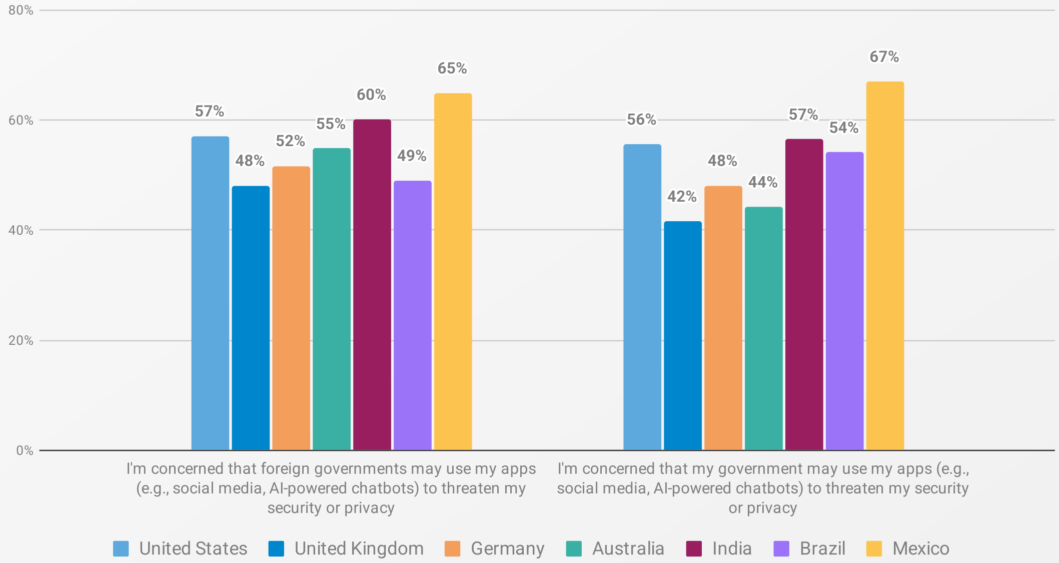


Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

Government concerns told a more complex story (Figure 91). UK participants reported the lowest percentage of worry, while Mexico reported the highest. In the UK, 48% were concerned about foreign governments and 42% about their own. In Mexico, 65% worried about foreign governments and 67% about their own.

Concern was higher for foreign than domestic governments in the US (57% vs 56%), UK (48% vs 42%), Germany (52% vs 48%), India (60% vs 57%), and especially Australia (55% vs 44%). Conversely, participants from Brazil (54% vs 49%) and Mexico (67% vs 65%) were slightly more concerned about their own government’s misuse of apps.

Figure 91. Concerns regarding foreign and domestic government use of apps to threaten security or privacy, by country.



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

In short, cybersecurity attitudes by country are full of contradictions. Mexico and India expressed the highest confidence that security is achievable and under their control, yet they also reported the highest levels of feeling that security information is confusing and intimidating. Meanwhile, Germany serves as a key outlier, being the only country where a majority of participants feel that security is not under their personal control.

Complexity also emerged in government-related concerns. The UK stands out for having the lowest level of concern regarding both foreign and domestic governments. Conversely, Mexico exhibits the highest levels of concern. While most countries are more worried about foreign governments, Brazil and Mexico are unique in that they express greater concern about their own government's use of apps to threaten individuals' security or privacy.

So, as well as organizational culture impacting people's cybersecurity beliefs, geography plays a part too. Global organizations, take note.

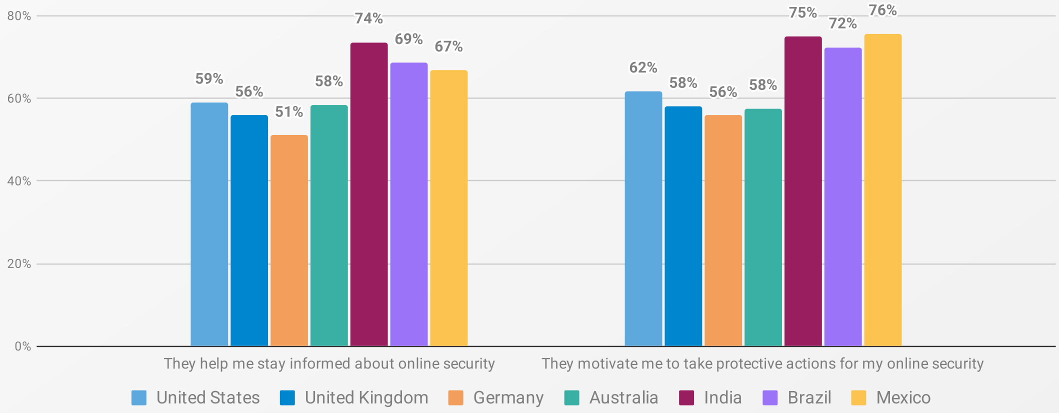
The media's role in shaping attitudes

Let's explore country differences regarding the impact of media on people's feelings toward online security. Heads up: It's pretty dramatic.

Across the board, most participants felt the media and news play a key role in keeping them informed about online security (Figure 92). This sentiment was highest in India (74%), followed by Brazil (69%), and Mexico (67%). The lowest percentage was found in Germany (51%), with the US (59%), UK (56%), and Australia (58%) clustered in the middle.

Media also motivated protective action: Majorities in Mexico (76%), India (75%), and Brazil (72%) said media coverage spurred them to take protective actions. Once again, Germany had the lowest percentage, at 56%.

Figure 92. The role of the media in informing and motivating online security actions, by country.

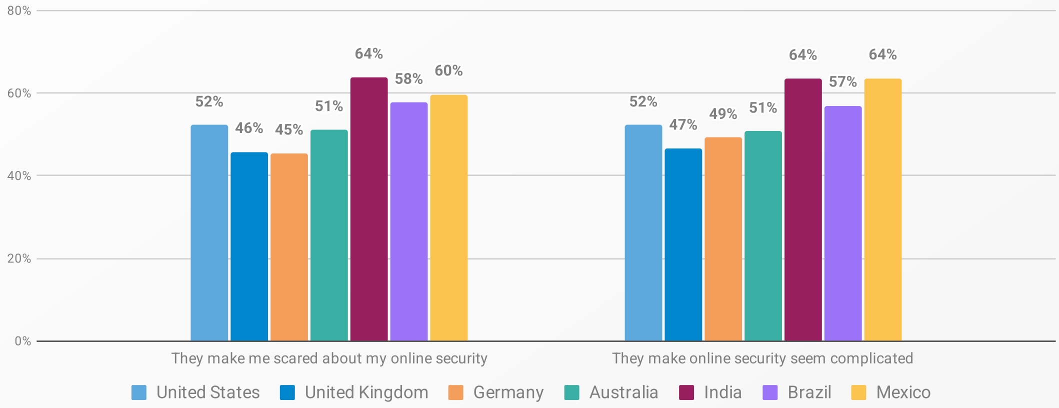


Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

But media influence cuts both ways. For many, it makes online security feel scary and complicated (Figure 93). In India (64%), Mexico (60%), and Brazil (58%) a majority reported that the media makes them scared about their online security. This perception was the lowest in Germany (45%) and in the United Kingdom (46%).

When it came to complexity, India and Mexico again topped the list (64%), followed by Brazil (57%) and the US (52%). The UK (47%) and Germany (49%) reported the lowest levels of confusion.

Figure 93. The role of the media in negative attitudes toward online security, by country.



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

So, the story isn't simple here. The media is widely seen as an effective tool for informing and motivating protective actions, particularly in India, Brazil, and Mexico, but these same countries report the highest levels of fear and confusion caused by media coverage. This suggests that the media's impact is not uniform, and it's not all positive or negative.

Overall, media coverage doesn't land the same everywhere. Its impact shifts depending on cultural and national context.

Cybersecurity culture in the workplace

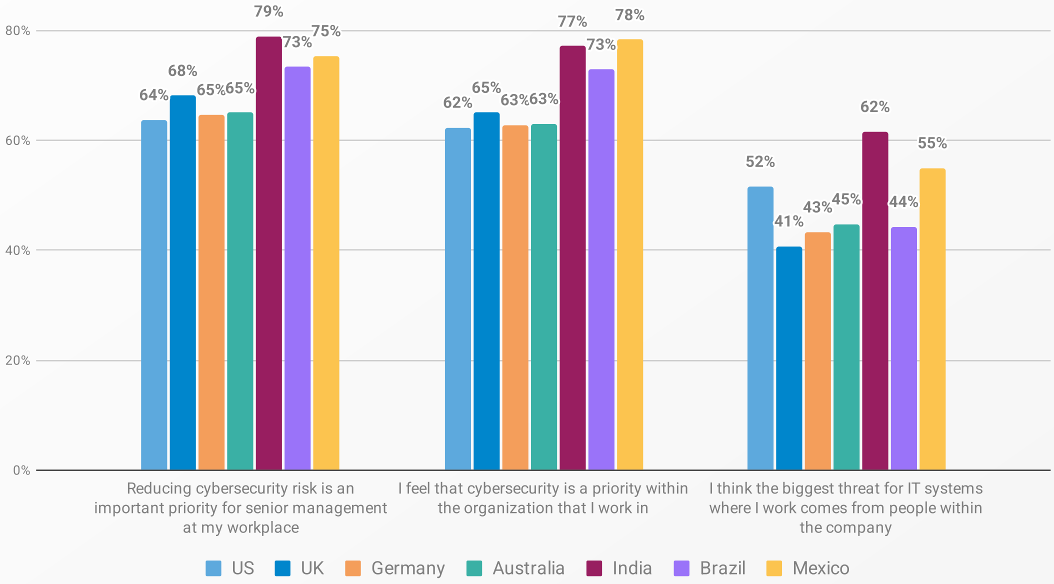
The data reveals some interesting differences in how employees from various countries view their organizations' priorities and key threats.

When asked whether reducing cybersecurity risk is an important priority for senior management, the divide was distinct (Figure 94). Employees in India (79%), Mexico (75%), and Brazil (73%) expressed the highest agreement with this sentiment, while their counterparts in the UK (64%), Germany, and Australia (both 65%) reported the lowest levels of agreement.

This pattern held for overall organizational prioritization of security. Again, Mexico (78%), India (77%), and Brazil (73%) came out on top.

Perceptions of insider threats also varied significantly. In India 62% of participants felt that the biggest threat came from people within the company. This was also a somewhat prominent belief in Mexico (55%) and the US (52%). In contrast, this perception was lowest in the UK (41%), followed by Germany (43%), Brazil (44%), and Australia (45%).

Figure 94. Attitudes toward cybersecurity in the workplace, by country.



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 4555 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

What’s considered a strong cybersecurity culture really depends on the country. In emerging digital economies like India, Mexico, and Brazil, employees generally feel confident that management is making security a top priority. In more developed nations, however, the picture isn’t so clear-cut. Views on insider threats also change significantly from one country to another. This means a one-size-fits-all security plan just won’t be effective. Organizations need to build tailored security strategies that fit the unique cultural landscape of each specific country.

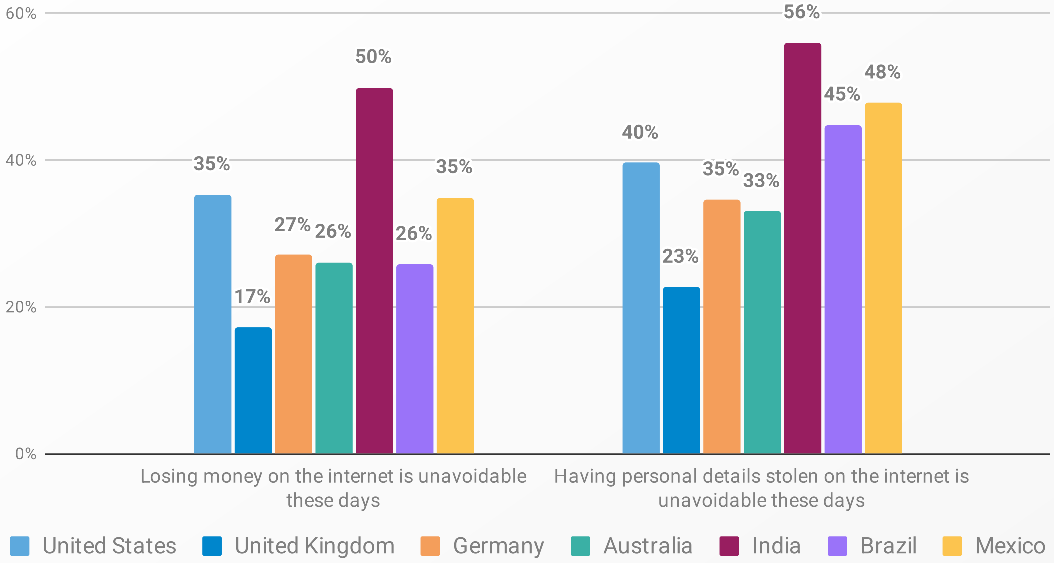
Attitudes toward victimization

When it comes to cybercrime, one theme stands out: inevitability. In India, half of the participants believe losing money online is unavoidable (50%), and even more feel the same about having personal details stolen (56%, Figure 95).

Other countries painted a very different picture. Only 17% of people in the UK think losing money is inevitable, followed by Australia and Brazil (26% each) and Germany (27%).

The UK also had the lowest proportion who believed data theft was unavoidable (23%), followed by Australia (33%) and Germany (35%).

Figure 95. Perceptions on the avoidability of losing money or personal details on the internet, by country.

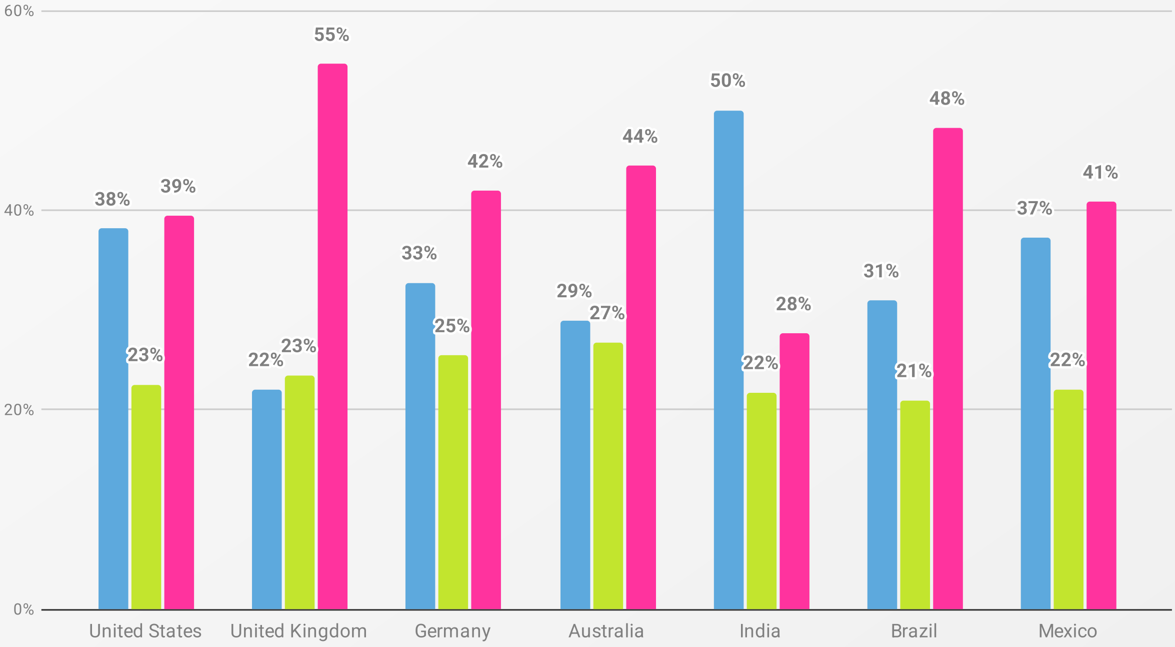


Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

A sense of resignation was most common in India (50%), where many felt there was no point in trying to protect themselves further because their information is already out there. This belief is also prevalent in the US (38%) and Mexico (37%).

By contrast, the UK once again stood out, showing a good old-fashioned stiff upper lip with 55% rejecting this fatalism and backing continued self-protection (Figure 96). Brazil (48%), Australia (44%), and Germany (42%) also showed strong resistance to giving up.

Figure 96. '*I don't see the point of trying to protect myself more as my information is already online.*' by country.



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

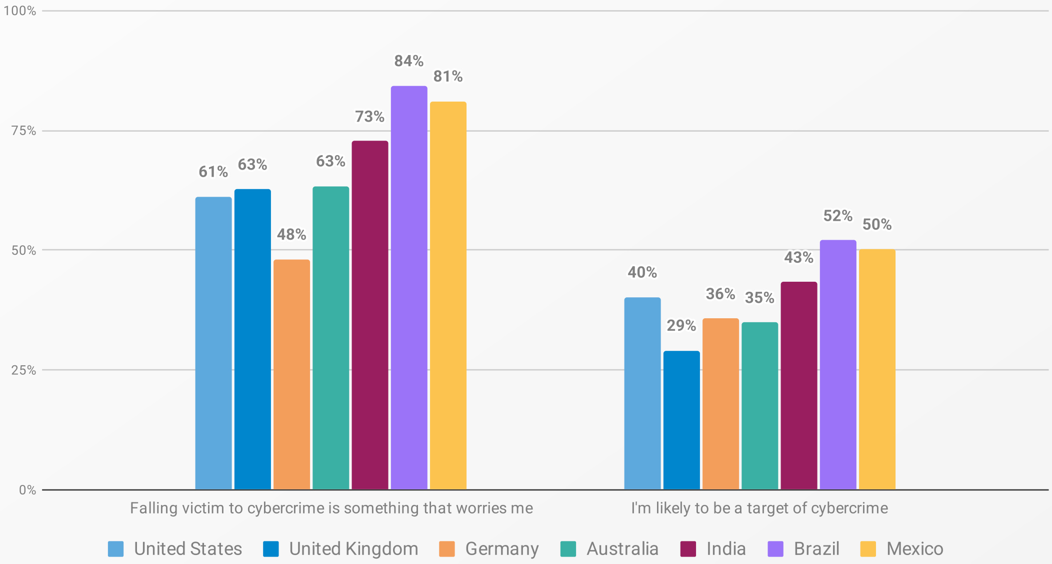
Worry about cybercrime is widespread (Figure 97). Brazil (84%) and Mexico (81%) topped the chart, but India (73%), the UK, Australia (both 63%), and the US (61%) all shared this concern too.

In contrast, Germany was the only country where a minority of participants (48%) expressed worry.

Yet belief in being an actual target was much lower. The highest percentages were once again in Brazil (52%) and Mexico (50%), where over half of the participants felt they were likely to be targeted.

Participants in the US (40%), Germany (36%), and Australia (35%) were in the middle of the range, while the United Kingdom reported the lowest percentage (29%).

Figure 97. Attitudes toward victimization, by country.



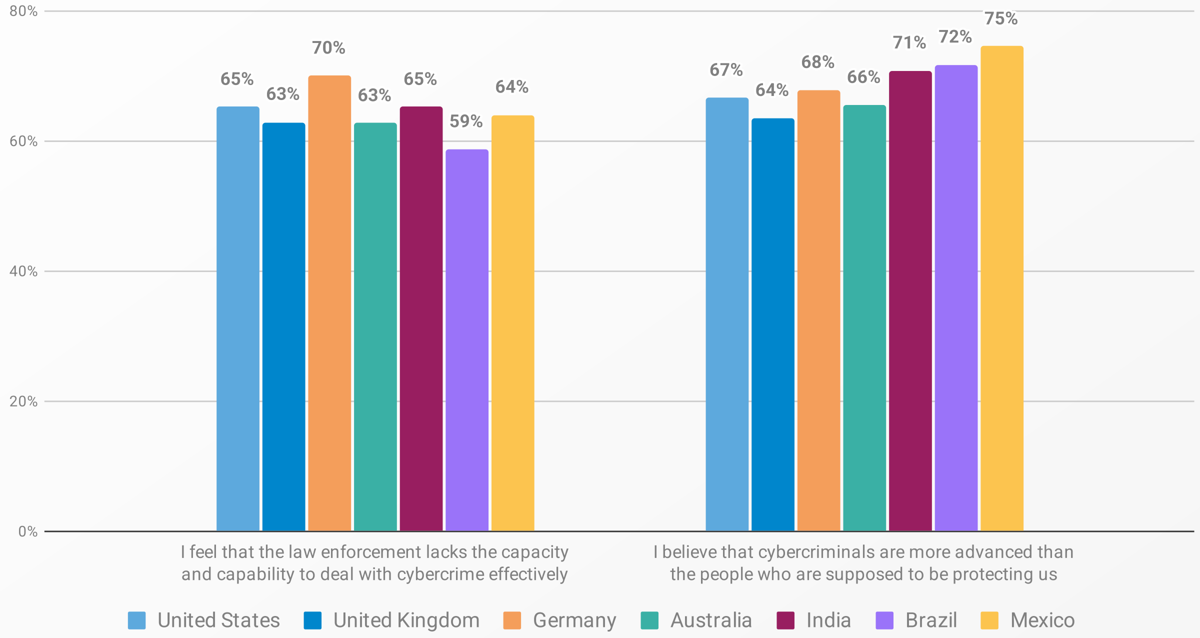
Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

Across all countries, one consistent theme was distrust in defenders (Figure 98). Most participants expressed concern that law enforcement lacks the capacity and capability to deal with cybercrime effectively.

Germany (70%) was the most skeptical, followed by the US and India (both 65%), Mexico (64%), the UK and Australia (both 63%). Even Brazil, with the lowest figure, still had a majority (59%).

And when comparing defenders to attackers, the verdict was clear: people think cybercriminals are winning. Mexico (75%), Brazil (72%), and India (71%) reported the highest agreement, but even in the UK, which came in bottom of the charts, still had 64% believing that criminals have the edge over protectors.

Figure 98. Perceptions of cybercrime defense effectiveness, by country.



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

In short, attitudes toward victimization may vary wildly by country, but the thread of global concern runs through them all. And high concern doesn't always equal high confidence in prevention. For instance, while countries like Brazil and Mexico reported the highest levels of concern about falling victim to cybercrime, they also showed the highest sense of inevitability and resignation.

This stands in contrast to the UK, which consistently reported the lowest levels of worry and also the lowest belief that cybercrime is unavoidable.

But one near-universal theme cuts through: confidence in defenders is weak, and faith in cybercriminal superiority is high. In other words, as well as a cybercrime challenge, the cybersecurity community has a confidence challenge on our hands.

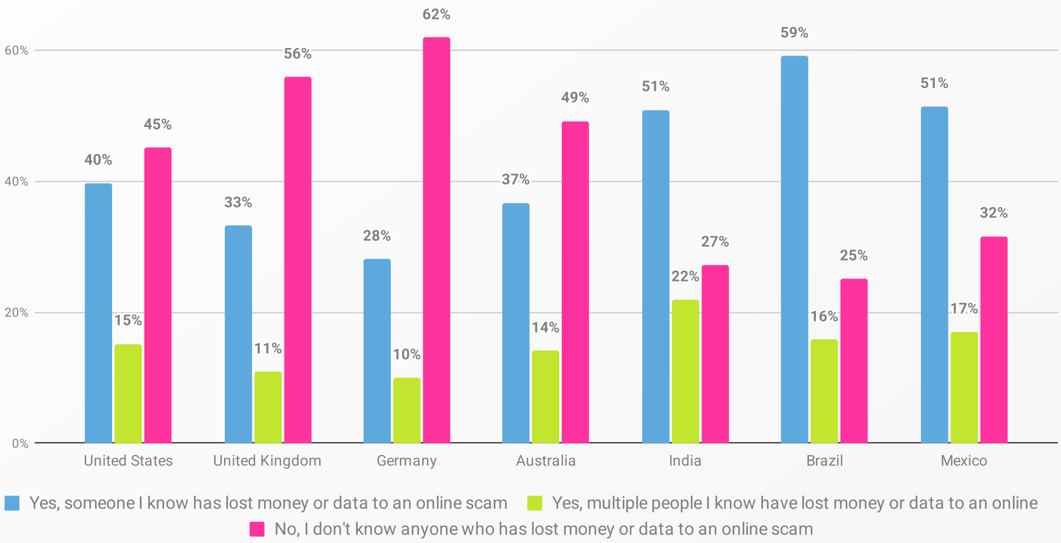
Cybercrime victimization

The data reveal some big differences in victimization across the participants' social circles (Figure 99).

A combined majority of participants in Brazil (75%) and India (73%) reported knowing at least one person who had lost money or data in an online scam, with India having the highest percentage of people who knew multiple victims (22%).

In contrast, a majority of participants in Germany (62%) and the UK (56%) reported not knowing anyone affected.

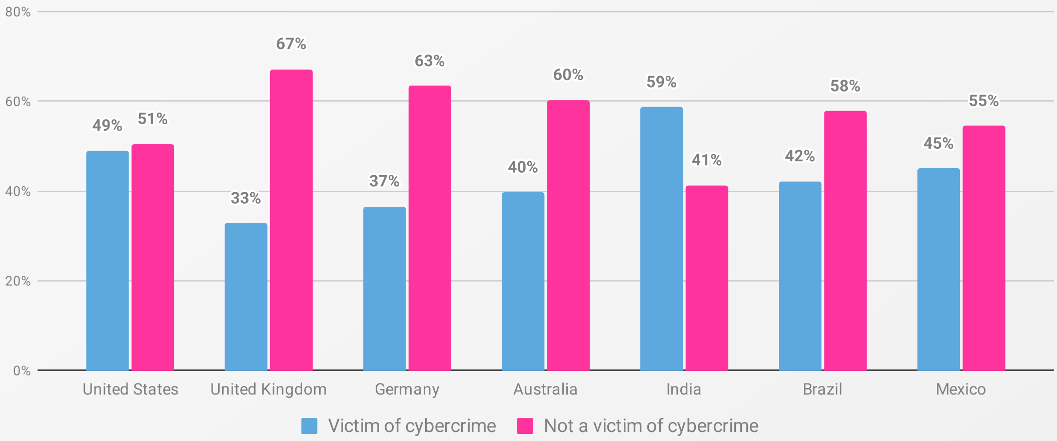
Figure 99. '*Has anyone you know been a victim of online scams where they have lost money or data?*' by country.



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

At the individual level, the UK (33%), Germany (37%), and Australia (40%) had the lowest percentages of cybercrime victims (Figure 100), while India again topped the chart just like last year, at 59%, followed by 49% in the US.

Figure 100. Victimization by country.



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

Similar to last year's report, participants in India and the US were the most likely to have been victims of all five types of cybercrime measured[54]: phishing, online dating scams, identity theft, cryptocurrency investment fraud, and tech support scams (Figure 101).

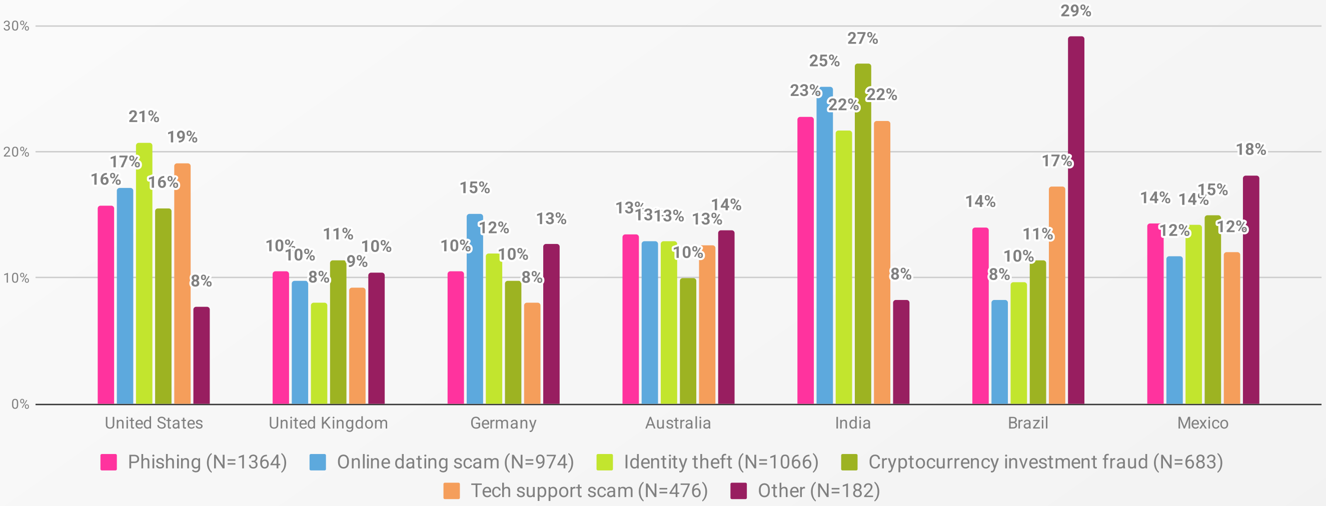
Of all phishing victims, 25% were from India, followed by 16% in the US. This trend was consistent across the other crime types:

- Online dating scams: 25% India, 17% US
- Identity theft: 22% India, 21% US
- Crypto fraud: 27% India, 16% US
- Tech support scams: 22% India, 19% US

Do different countries have different cybercrime weak spots? Absolutely. Compared to other cybercrimes, participants in India (27%), the UK (11%), and Mexico (15%) were more likely to fall victim to crypto fraud, which was the least common cybercrime incident among participants in Australia (10%).

Participants in the US (21%) were more likely to be identity theft victims, while in Germany (15%), participants were more likely to fall for online dating scams. Finally, participants from Brazil (17%) were more likely to fall for tech support scams.

Figure 101. Crime prevalence by incident type, by country.



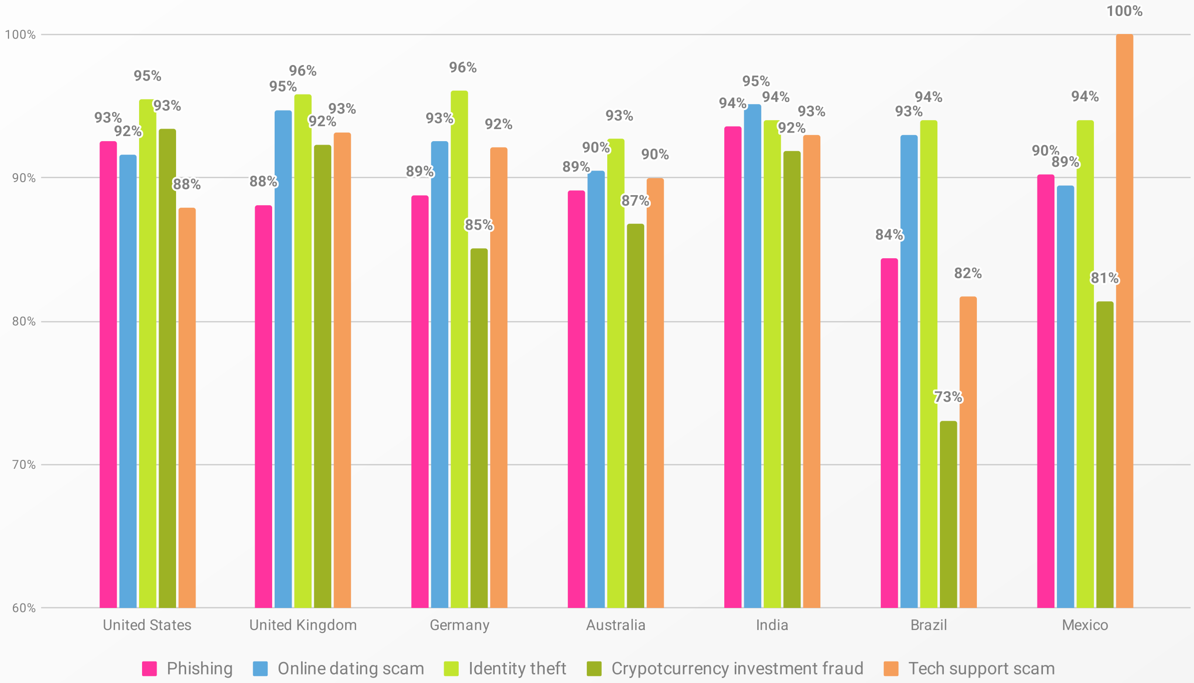
Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of cybercrime incidents: 4745. Total number of participants losing money to one or more incidents: 3050 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

Reporting rates also vary (Figure 102). India (94%) and the US (93%) had the highest phishing reporting rates. Reporting rates for online dating scams were highest in the UK and India (both 95%). Germany and the UK (both 96%) had the highest reporting rates for identity theft, closely followed by the US (95%).

[54] Participants were provided with the 'Other' option to share cybercrime victimization experiences that were not covered in the five existing categories. Whilst the 'Other' option is included in the figures in the Main findings, we omitted it in Appendix B for simplification.

Cryptocurrency investment fraud had the lowest reporting overall, ranging from 73% (Brazil) to 93% (US) And finally, tech support scam reporting rates ranged from 82% in Brazil to 100% in Mexico. Across all five categories, Brazil consistently had the lowest reporting rates.

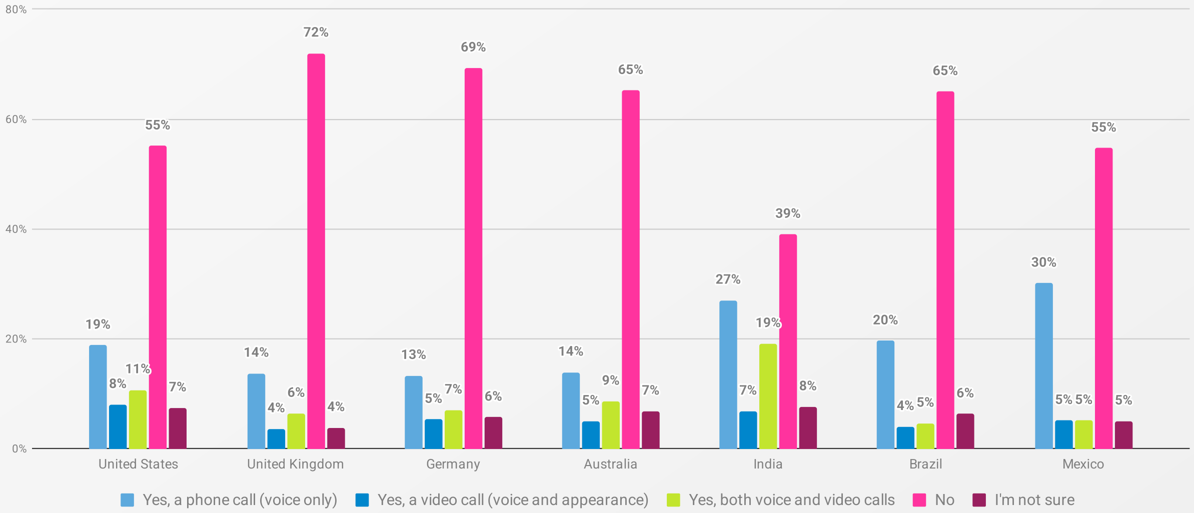
Figure 102. Percentage of cybercrimes reported to authorities, agencies, or organizations, by country.



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of reported incidents: 4165 (age 18+). Total number of incidents: 4563 (without the ones described by participants in the 'Other' category). Dates conducted: May 2, 2025 - May 27, 2025.

When it came to deepfakes, exposure varied dramatically (Figure 103). Over half of participants in India (53%) reported receiving a deepfake call, compared to 40% in Mexico and 38% in the US. In contrast, the majority of participants in the UK (72%) and Germany (69%) said they had never been targeted.

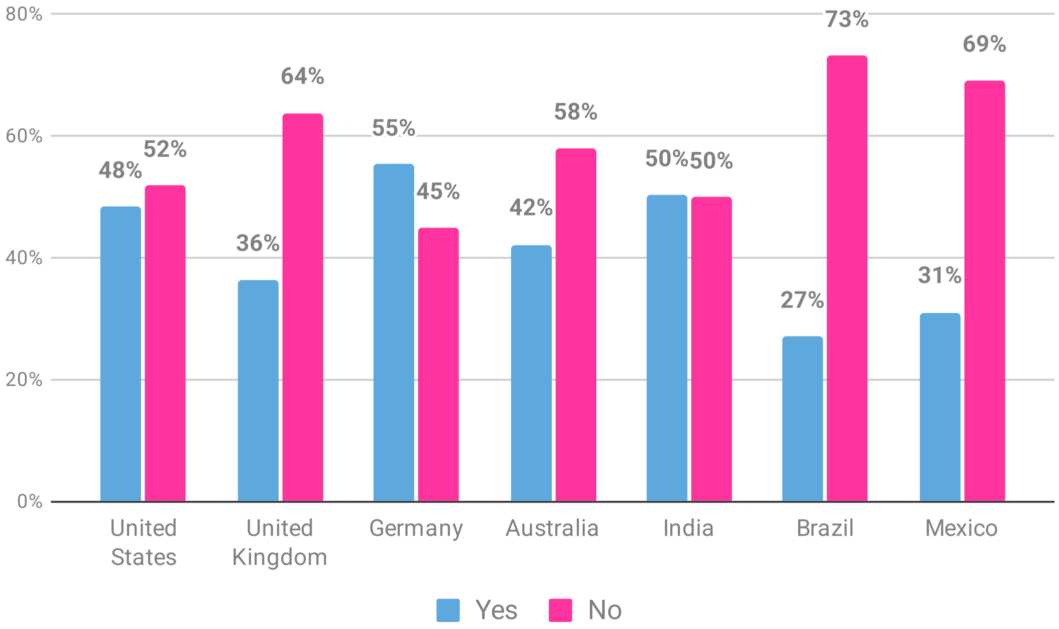
Figure 103. '*Have you ever received a phone or video call where the caller's voice or appearance exactly matched someone you know, but it turned out to be a scam?*' by country.



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of reported incidents: 4165 (age 18+). Total number of incidents: 4563 (without the ones described by participants in the 'Other' category). Dates conducted: May 2, 2025 - May 27, 2025.

But exposure doesn't always mean loss (Figure 104). The highest percentages of participants who have lost money or data are in Germany (55%), followed by India (50%) and the US (48%). The lowest percentages of victimization are found in Brazil (27%) and Mexico (31%), where a large majority of participants reported no loss of money or data as a result of a deepfake scam.

Figure 104. '*Did you lose money or data as a result of the deepfake voice or video call you received?*' by country.



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 2361 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

In conclusion, India and the US consistently show the highest rates of victimization, not only in overall numbers but also across specific threats like phishing, online dating scams, and tech support scams. This is further reflected in their high exposure to emerging threats, with India leading in reported deepfake phone calls. In contrast, participants in the UK and Germany generally reported the lowest rates of victimization and exposure to these emerging scams.

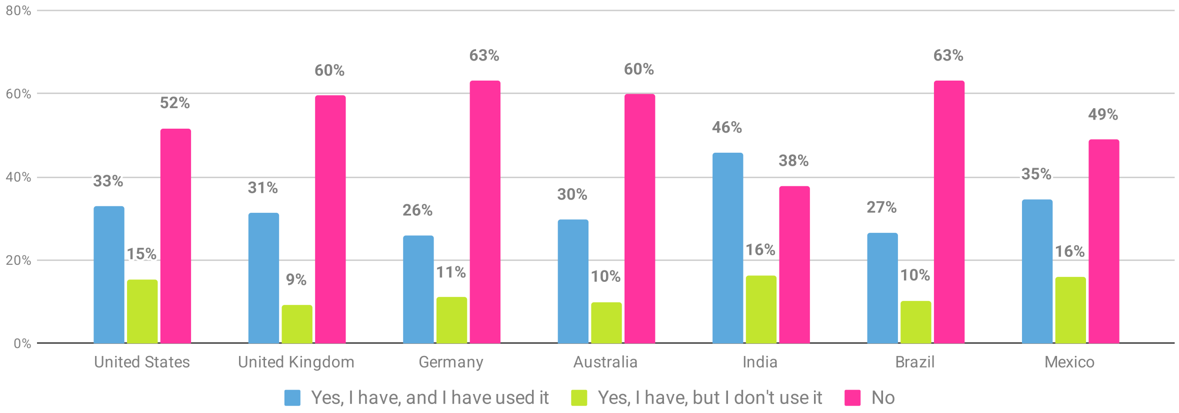
However, the data also highlights key contrasts. Germany, for instance, reported lower overall exposure to cybercrime yet recorded the highest rate of deepfake-related financial loss among those who fell victim to it. Brazil, meanwhile, had the lowest reporting rates across all crime categories while other countries demonstrated high reporting for specific crimes. Ultimately, these findings underscore that while some regions face a higher overall threat, the specific nature of cyber risk and response behaviors can vary significantly by country.

Cybersecurity training

The data reveals stark contrasts in access to cybersecurity training across countries (Figure 105). Most participants from Germany and Brazil (63% each), and the UK and Australia (60% each) had no access to cybersecurity training. In contrast, India stands out with only 38% lacking access, followed by Mexico (49%) and the United States (52%).

Among those with access, India again leads: 46% said they had actually used the training, compared to 33% in the US. In countries with high rates of no access, such as Germany, Brazil, the UK, and Australia, uptake of available training was much lower.

Figure 105. '*Do you have access to cybersecurity training (e.g., at work, school, library, or other public location)?*' by country.

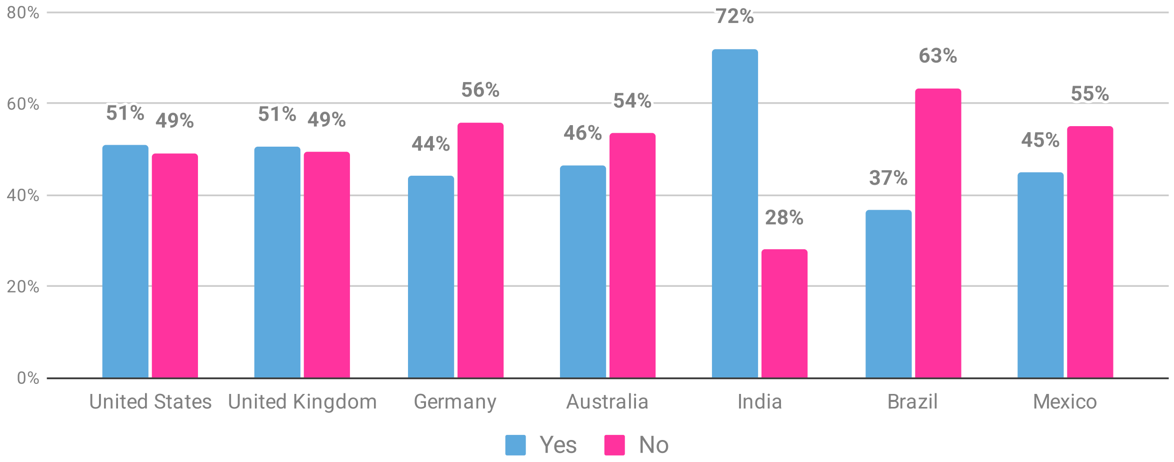


Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

Requirements for mandatory cybersecurity training also vary dramatically by country (Figure 106). India tops the list, with nearly three-quarters (72%) required to complete training, by far the highest proportion.

At the other end of the spectrum, Brazil had the lowest rate (37%), followed by Germany (44%), Mexico (45%), and Australia (46%). The US and the UK both reported an even split, with 51% of participants saying training was mandatory.

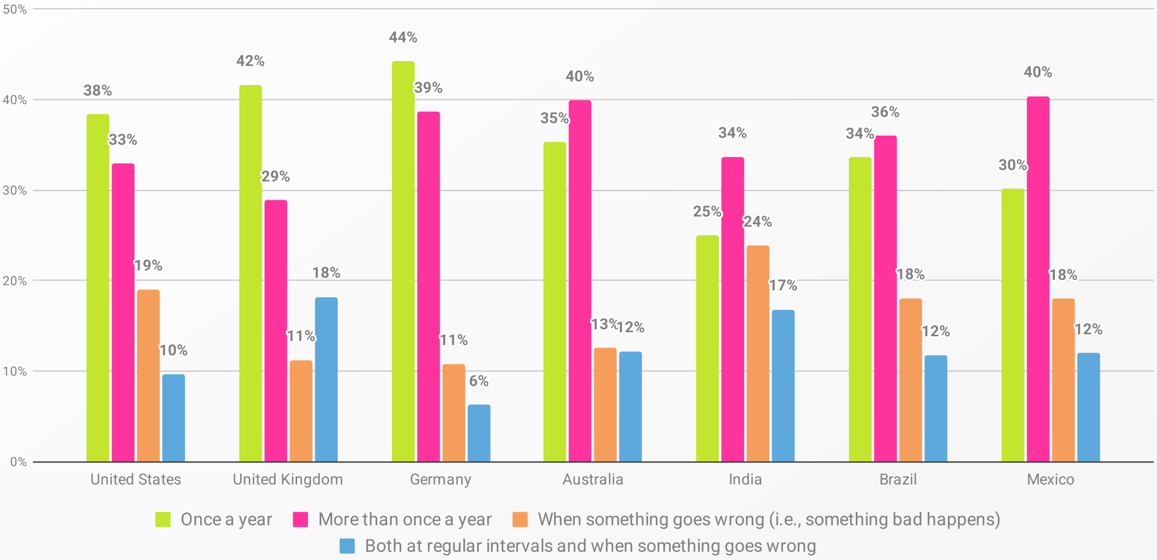
Figure 106. '*Are you required to complete mandatory cybersecurity training at work or your place of education?*' by country.



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 4555 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

The frequency of training also differs. Most working participants in Germany (44%), the UK (42%), and the US (38%) were required to train once a year (Figure 107). The majority in Mexico, Australia (both 40%), Brazil (36%), and India (34%) are required to train more than once a year. Training triggered by an incident was most common in India (24%), followed by the US (19%) and Brazil (18%). In the UK (18%) and India (17%), people were most likely to report training both at regular intervals and in response to incidents.

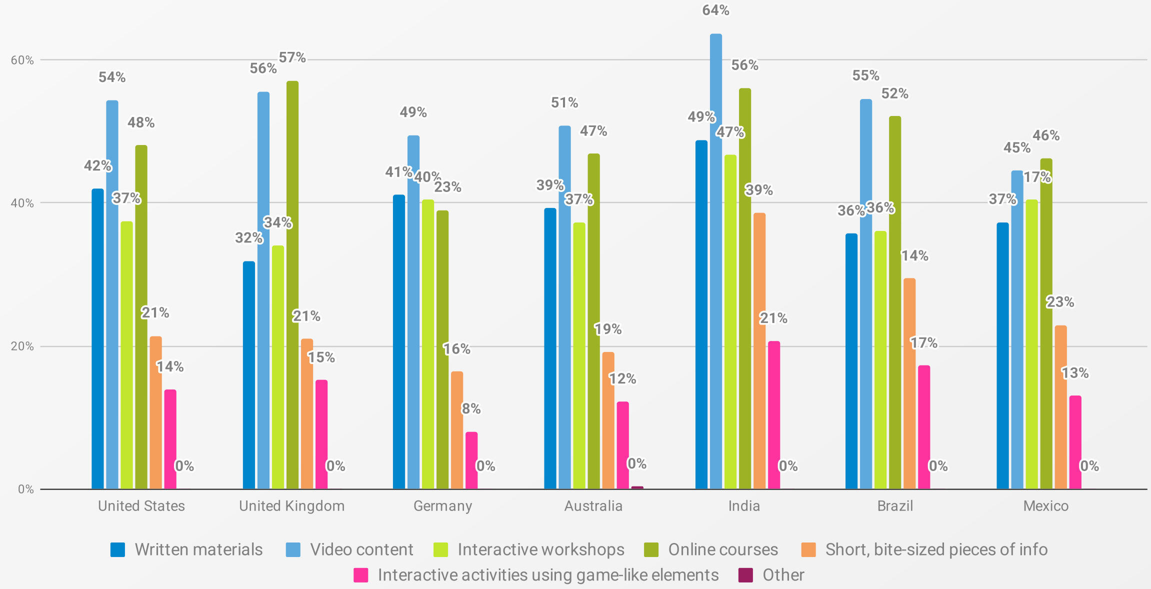
Figure 107. '*How often are you required to complete training?*' by country.



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 2249 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

Video content is the most common training format across most countries, with adoption rates of 64% in India, 55% in Brazil, 54% in the US, 51% in Australia, and 49% in Germany (Figure 108). The UK and Mexico were the only exceptions. In both countries, online courses were more common, reported by 57% in the UK and 46% in Mexico.

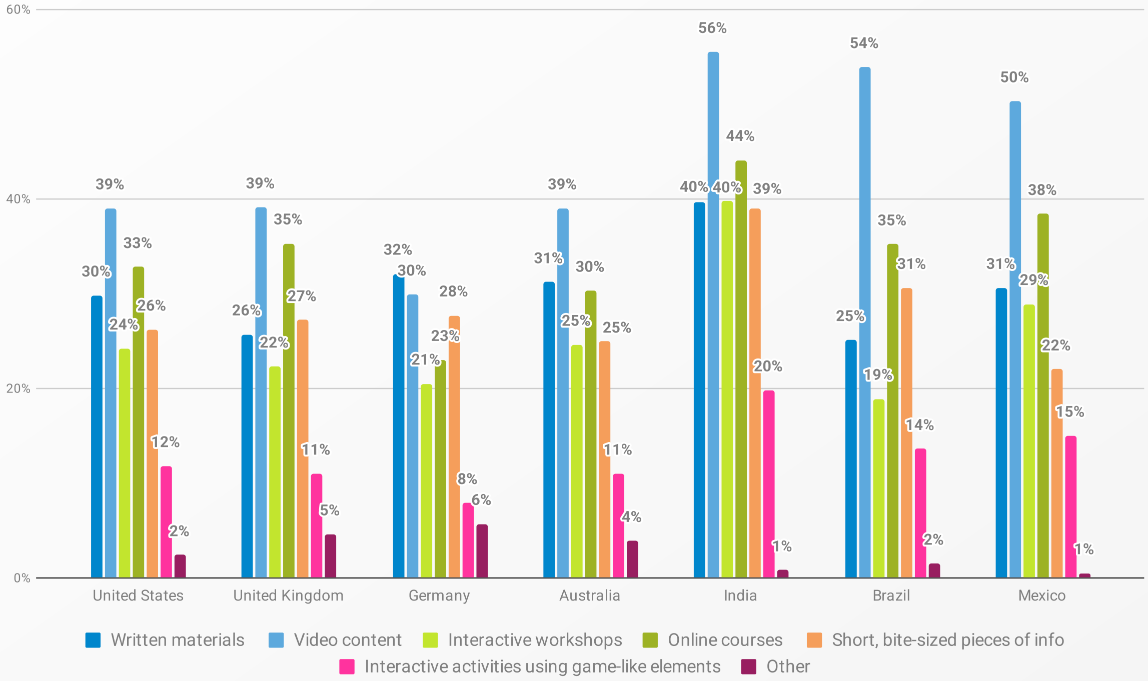
Figure 108. Cybersecurity training formats used by organizations, by country.



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 2249 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

When it comes to preferred formats (Figure 109), video content once again came out on top across most countries, just like last year. Video content was the most preferred training format across all countries, ranging from 56% in India to 39% in the US, UK, and Australia. Germany stood out as the only country where written materials were most preferred (32%). In contrast, interactive activities using game-like elements were the least preferred format in every country.

Figure 109. '*What format do you prefer to consume cybersecurity training information?*' by country.



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

So, where does that leave us? In summary, while some nations like India stand out with a high percentage of mandatory training (72%), others, such as Brazil, Germany, and the UK, have a notable portion of participants who report no access at all. Mandatory training frequency also varies: countries like Germany and the UK lean toward annual requirements, while others adopt more frequent or reactive schedules. For instance, in Brazil and Mexico training is more than once a year, and in India it is often triggered when something goes wrong.

When it comes to training formats used by organizations, video content remains the most common format in most countries. The exceptions are the UK and Mexico, where online courses are slightly more common. This preference for video content holds true even for participants' personal preferences, though Germany continues to be an outlier, preferring written materials over all other formats.

Access is one thing, but does all that training actually translate into knowledge people can use? Time to find out.

Cybersecurity knowledge

Self-reported cybersecurity knowledge looks very different depending on where you live (Figure 110). The highest proportion of participants in Brazil (43%), the UK (42%, +7% from 2024), Australia (41%, +7% from 2024), the US, and Mexico (40% both, +5% from 2024 in the US) rated themselves as having basic knowledge.

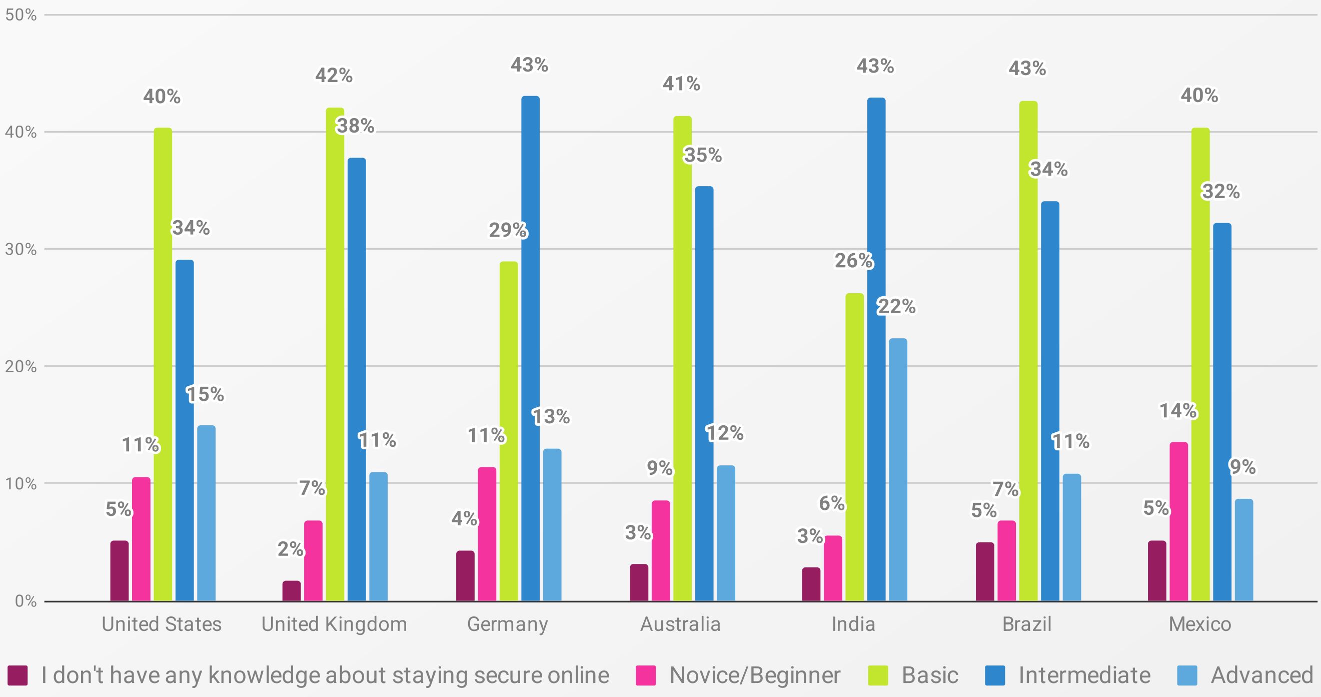
Those reporting intermediate or advanced knowledge were most common in India (65%, -7% from 2024), followed by Germany (56%, -5% from 2024). At the other end of the spectrum, Mexico had the highest number of novices (14%), followed by the US (11%, +4% from 2024) and Germany (11%, +5% from 2024).

And when it comes to people who feel like they have no cybersecurity knowledge at all, the US, Brazil, and Mexico came out on top at 5% each, with the US seeing a slight improvement since 2024, down by 1%.

So, people may say they know what they're doing online, but the numbers tell us otherwise. Confidence is patchy, gaps are growing, and plenty of folks admit to knowing next to nothing.

And here's where things get really interesting: knowledge doesn't always translate into action. So let's put theory to the test and look at what people are *actually* doing with one of the biggest weak spots of all: their passwords.

Figure 110. Self-reported cybersecurity knowledge, by country.



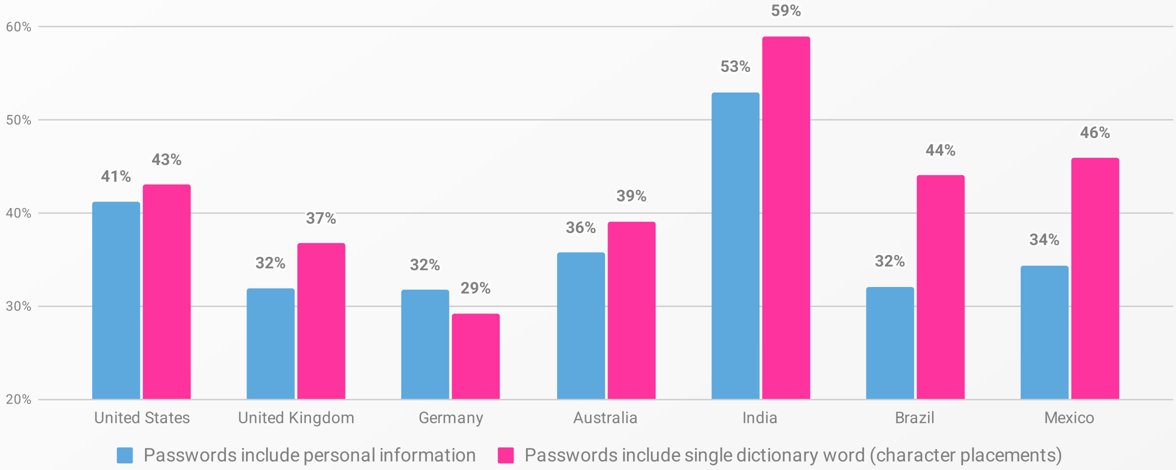
Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

Password hygiene

Weak passwords are alive and well. Across all countries, participants continue to lean on two favorites: single dictionary words with character swaps, and the use of personal information (Figure 111). Neither is a winning formula.

India is the biggest outlier, with a majority relying on both poor practices: 53% use personal information, and 59% go for the good ol' swap-a-letter technique. The US also shows high numbers for both, at 41% and 43%, respectively. Germany, on the other hand, reported the lowest percentages for both: 32% for personal information and 29% for single dictionary words.

Figure 111. Password creation techniques used by participants, by country.

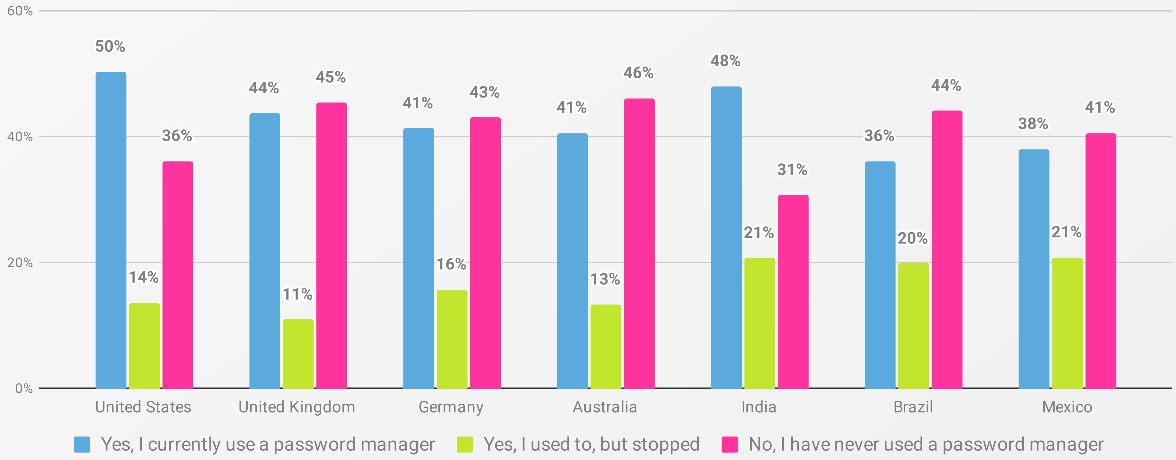


Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

Password manager adoption paints a different picture (Figure 112). The US leads, with 50% of participants currently using one. This is followed by India (48%) and Australia (41%), while Brazil (36%) has the lowest current adoption rate.

However, a big share of participants in Australia (46%) and the UK (45%) have never touched a password manager. And in India, Mexico, and Brazil, over 1 in 5 said they tried one but gave up. That suggests awareness isn't the only barrier here, but we're also contending with things like trust, usability, and sticking power.

Figure 112. '*Have you ever used a password manager?*' by country.

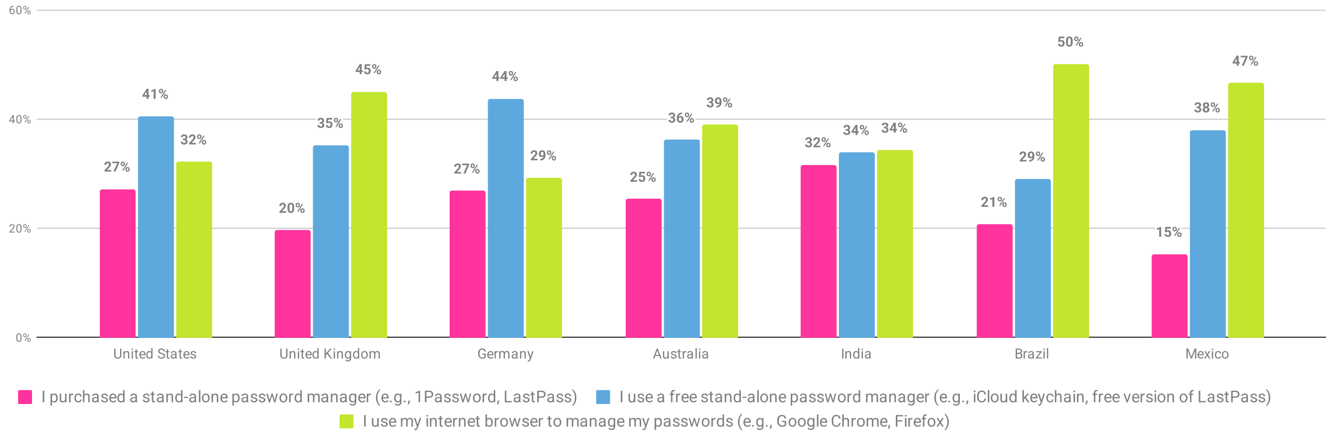


Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

Preferences also vary (Figure 113). Brazil (50%), Mexico (47%), and the UK (45%) prefer browser-built managers. Germany is the least likely to go down that road (29%).

In contrast, participants in Germany (44%) show the highest preference for a free stand-alone password manager, followed by the United States (41%). The highest proportion of paid stand-alone password manager users is in India (32%), followed by the US and Germany (27% each) and Australia (25%).

Figure 113. '*What is your preferred password manager?*' by country.



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 2992 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

In conclusion, the data on password hygiene reveals clear differences in both creation habits and tool adoption across countries. The most concerning profiles are found in India and the US, where participants are more likely to use weak password creation techniques, such as personal information or single dictionary words. This contrasts sharply with Germany, which reported the lowest percentages for these insecure practices.

While the US leads in current password manager usage, a sizable portion of participants in Australia and the UK have never adopted one. Furthermore, India, Mexico, and Brazil have the highest rates of users who tried a password manager but have since stopped. These trends suggest that while awareness is growing, consistency and sustained adoption remain major challenges.

Which leads us neatly into the next question: if passwords are shaky, what about adding a second layer of protection with MFA?

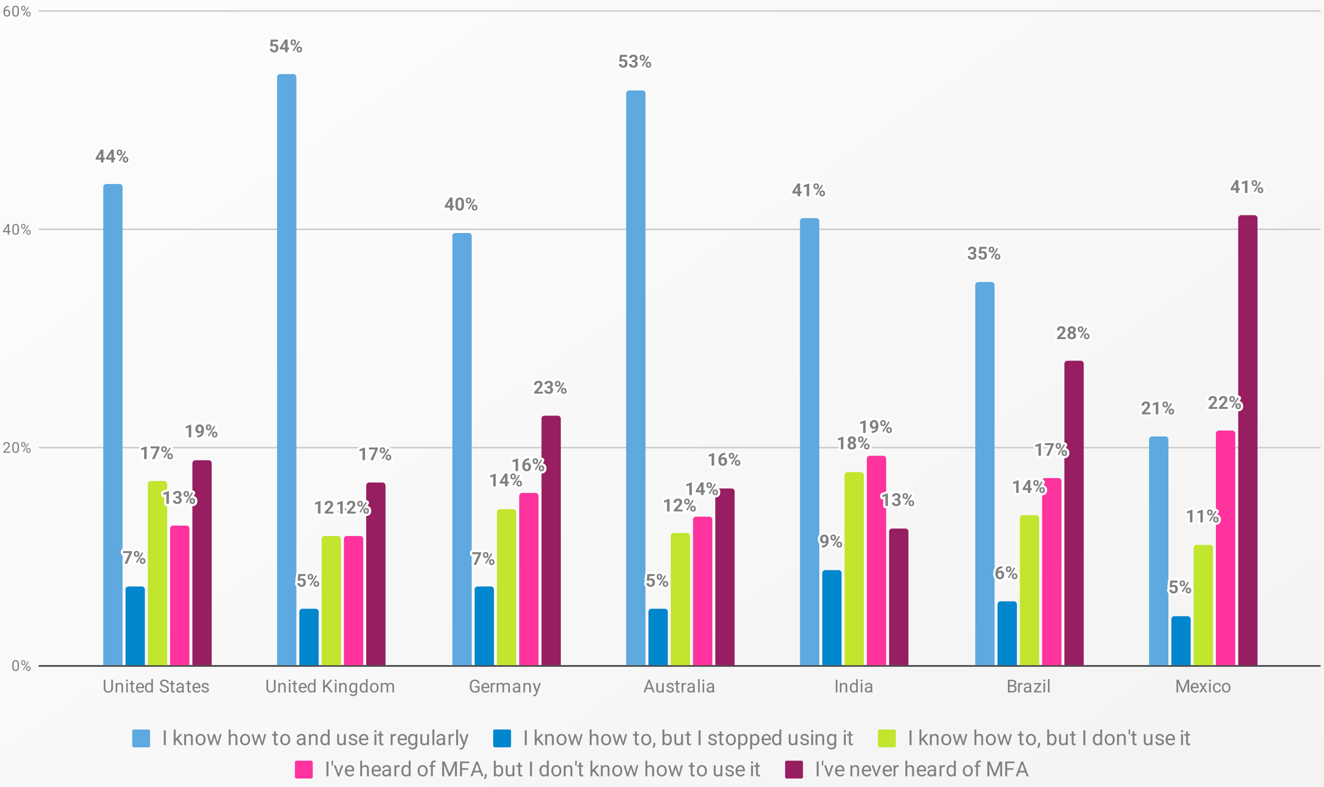
Enabling MFA

The findings reveal a striking contrast in MFA adoption and awareness across different countries (Figure 114). The UK (54%) and Australia (53%) lead the way, with over half of participants reporting that they know how to use MFA and do so regularly, followed by the US (44%), India (41%), and Germany (40%).

On the flip side, Mexico and Brazil stand out for low awareness and uptake. In Mexico, 41% of participants have never heard of MFA (the highest across all countries), while a further 22% know about it but don't know how to use it. Brazil shows a similar pattern, with 28% unaware of MFA and 17% unsure of how to use it.

India also shows an interesting wrinkle: 18% of participants report knowing how to use MFA but choosing not to. This suggests that barriers to MFA usage include attitudes as well as awareness and capability.

Figure 114. '*Do you know how to use MFA?*' by country.



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

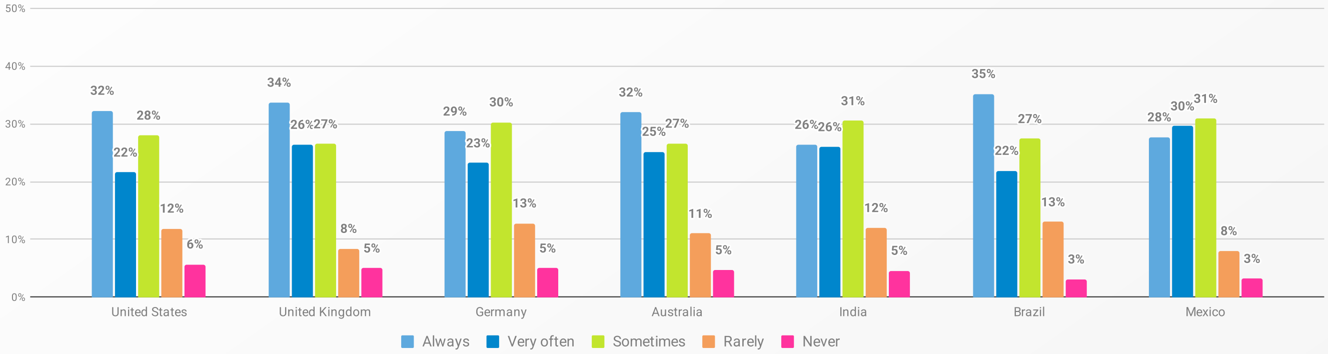
So, safe to say that MFA adoption has its ups and downs. But how are people doing with the oldest cybersecurity chore in the book, hitting 'update now'?

Installing software & app updates

Most participants across all countries are proactive about installing software and app updates (Figure 115). The combined percentages for those who 'always' or 'very often' install updates are highest in the UK (60%, +1% from 2024), followed closely by Mexico (59%), Brazil (57%), and Australia (57%, -3% from 2024).

In contrast, the US and Germany have the highest percentages of participants who ‘rarely’ or ‘never’ install updates (18% each, -2% each from 2024). Mexico was least likely to delay updates: only 11% ‘rarely’ or ‘never’ install them.

Figure 115. ‘*How often do you install the latest software or application updates to your devices when notified that they are available?*’ by country.



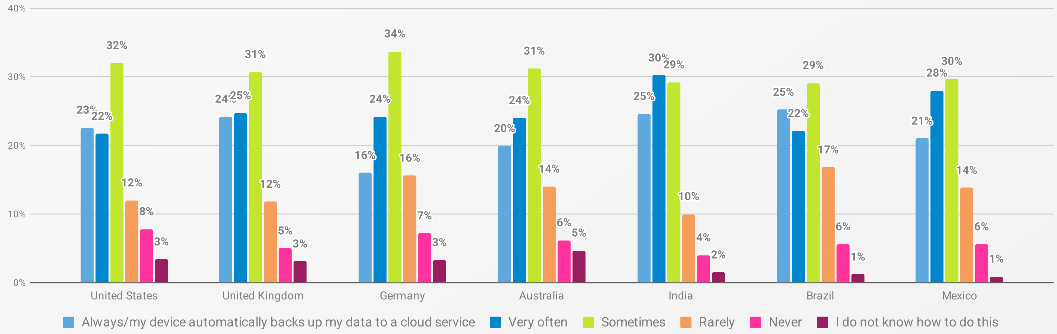
Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 2992 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

Next up: backups. Because sometimes prevention isn’t enough. You also need a parachute.

Backing up data

The frequency of data backup also varies by country (Figure 116). India once again leads the way, with 55% of participants saying they ‘always’ or ‘often’ back up their data (though that’s a 3% dip from 2024). Much of this is thanks to India having the highest rate of automated backups (30%). The UK and Mexico also show a high combined rate of frequent backups (49% each). In contrast, Germany and Brazil had the highest percentages of participants who ‘rarely’ or ‘never’ back up their data (23% each).

Figure 116. ‘*How often do you back up your most important data?*’ by country.



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

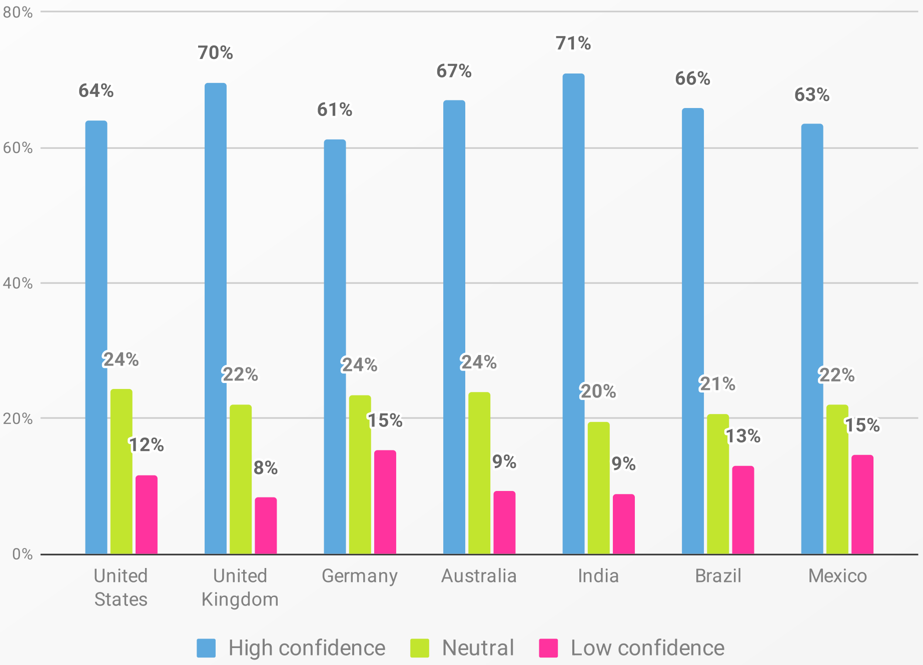
So, storage stats sorted. But what about that dodgy email in your inbox? Time to dive into phishing.

Recognizing & reporting phishing messages

A consistent cross-country trend stood out here: A moderate to high level of confidence in spotting phishing emails and malicious links (Figure 117).

Confidence is highest in India (71%, -2% from 2024), followed by the UK (70%, same as in 2024), Australia (67%, -3% from 2024), and Brazil (66%). Germany sits at the bottom of the confidence scale, though still with a decent 61%, up 9% from last year.

Figure 117. '*How confident are you in your ability to identify a phishing email or a malicious link?*' by country.



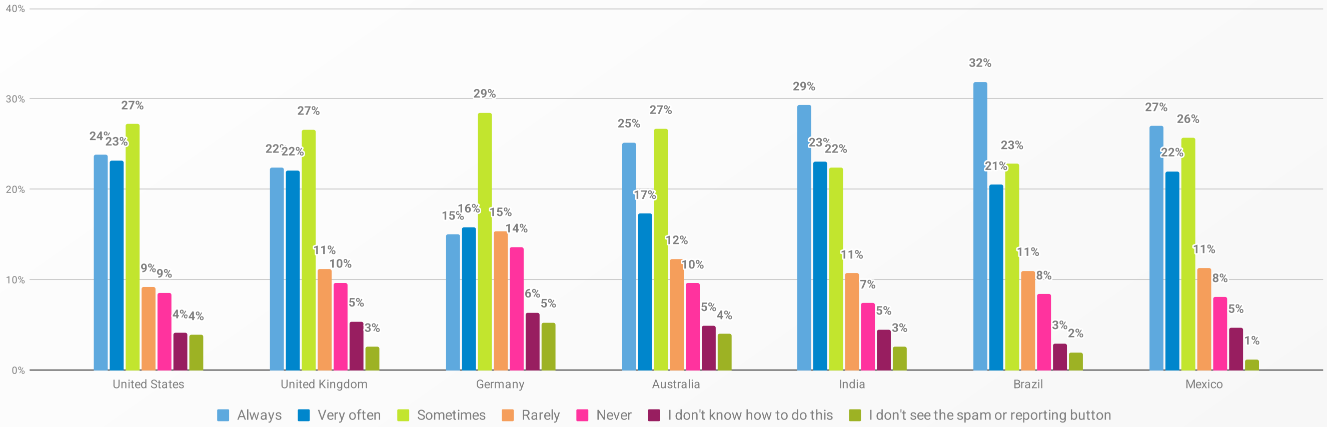
Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

Reporting rates, however, tell a different story (Figure 118). Countries with the highest rates of reporting phishing messages 'always' or 'very often' were Brazil (53%), India (52%), and Mexico (49%).

In contrast, Germany has the lowest rate of proactive reporting at 31%, and the highest rate of 'never' and 'rarely' reporting (29%). Barriers to reporting, like not knowing how to report and not seeing the button for reporting, were also highest in Germany (11%).

Furthermore, the largest percentage of participants in Germany (29%), the US, the UK, and Australia (each 27%) said they report phishing 'sometimes'.

Figure 118. ‘*How often do you report phishing messages by using the ‘spam’ or ‘report phishing’ button?*’ by country.



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+). Dates conducted: May 2, 2025 - May 27, 2025.

In conclusion, phishing recognition and reporting follow clear national patterns. Brazil and India show strong confidence in phishing recognition and proactive reporting. The UK and Australia show confidence without consistent follow-through, pointing to a gap between awareness and action. Finally, Germany shows a different picture again, with lower confidence reflected in the lowest reporting rates overall.

These varied national trends cry out for security education and tools that address a country’s specific challenges, whether that is encouraging active engagement or building foundational confidence.

And if phishing feels like a never-ending cat-and-mouse game, AI is about to hand the mouse a jetpack. Let’s see how people really feel about the rise of artificial intelligence.

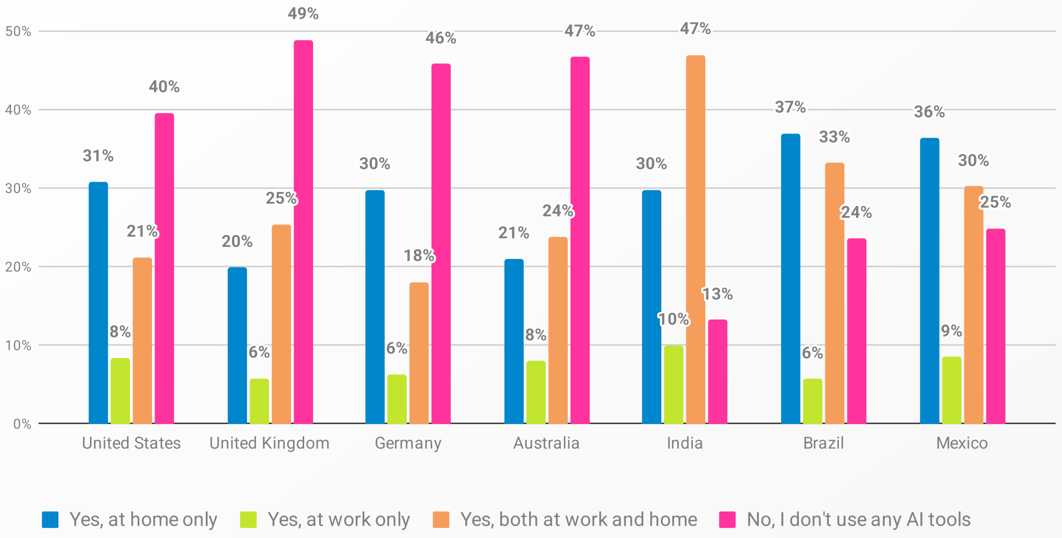
AI

The use of AI tools varies significantly by country (Figure 119). The highest overall adoption of AI tools is in India, where a whopping 87% of participants use AI either at home, at work, or both. Nearly half (47%) reported using it in both contexts. Brazil (76%) and Mexico (75%) also show high adoption, though this is driven mainly by home-only users (37% and 36%, respectively).

In contrast, non-use was highest in the UK (49%), Australia (47%), and Germany (46%).

When looking at usage patterns, the largest proportion of users in Brazil (37%), Mexico (36%), the US (31%), and Germany (30%) use AI tools at home only. Conversely, in India (47%), the UK (25%), and Australia (24%), the most common group are those using AI both at home and work.

Figure 119. ‘*Do you use any AI tools at home or work?*’ by country.

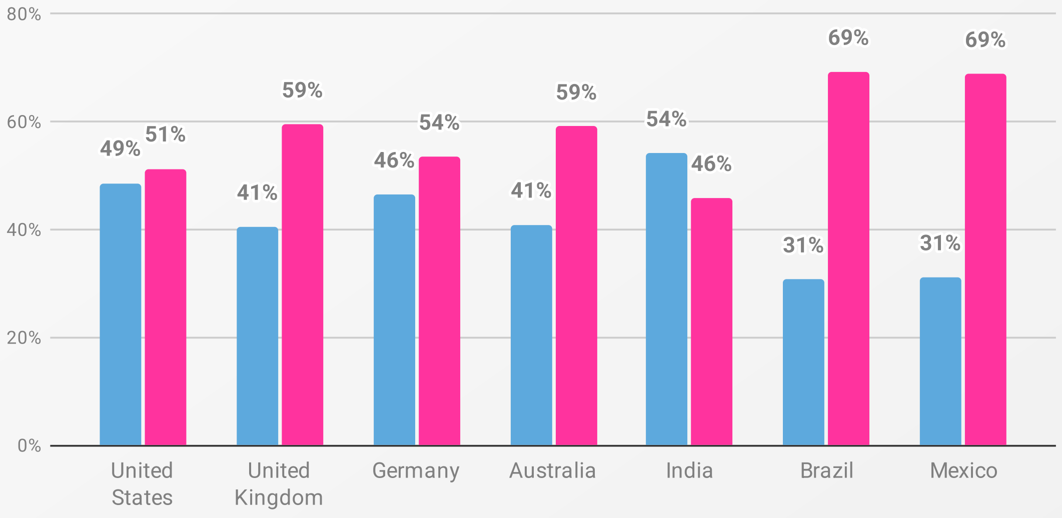


Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+).
Dates conducted: May 2, 2025 - May 27, 2025.

There’s a big contrast in the availability of training on AI security and privacy risks across different countries (Figure 120).

While over half of participants in India (54%) reported having received such training, this is not the case in most other countries. Only 31% of participants from Brazil and Mexico have received AI training, followed by 41% in the UK and Australia.

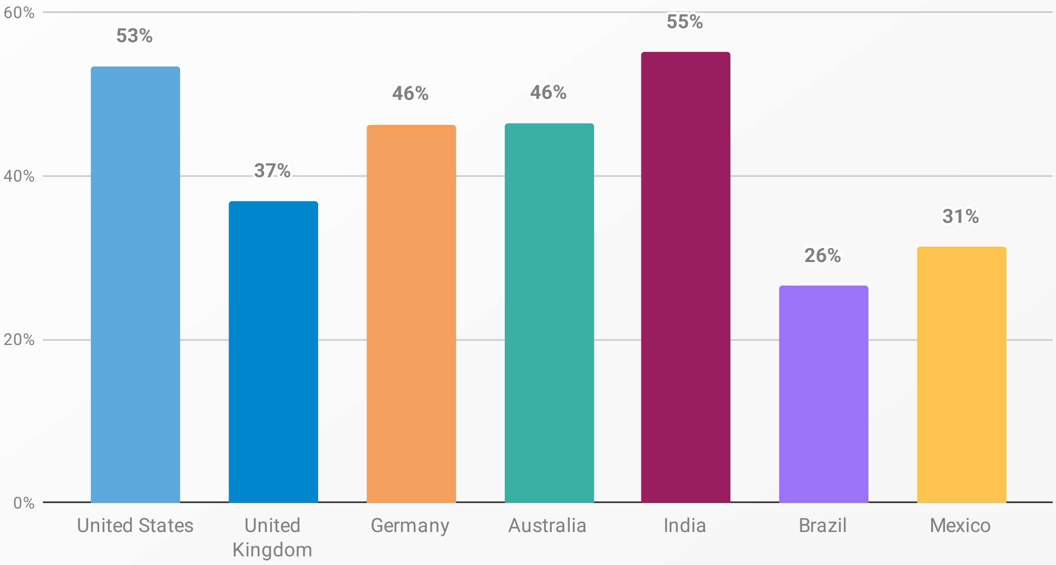
Figure 120. ‘*Have you received any training about the security and privacy risks of AI tools?*’ by country.



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 4573 (age 18+).
Dates conducted: May 2, 2025 - May 27, 2025.

Across all countries, participants admitted to sharing sensitive work information with AI tools without their employer's knowledge (Figure 121). This was most common in India (55%) and the United States (53%). Germany and Australia sit in the middle at 46%, while the UK (37%) and Mexico (31%) report lower rates. Brazil comes in lowest at 26%, but even there, more than a quarter have engaged in this risky behavior.

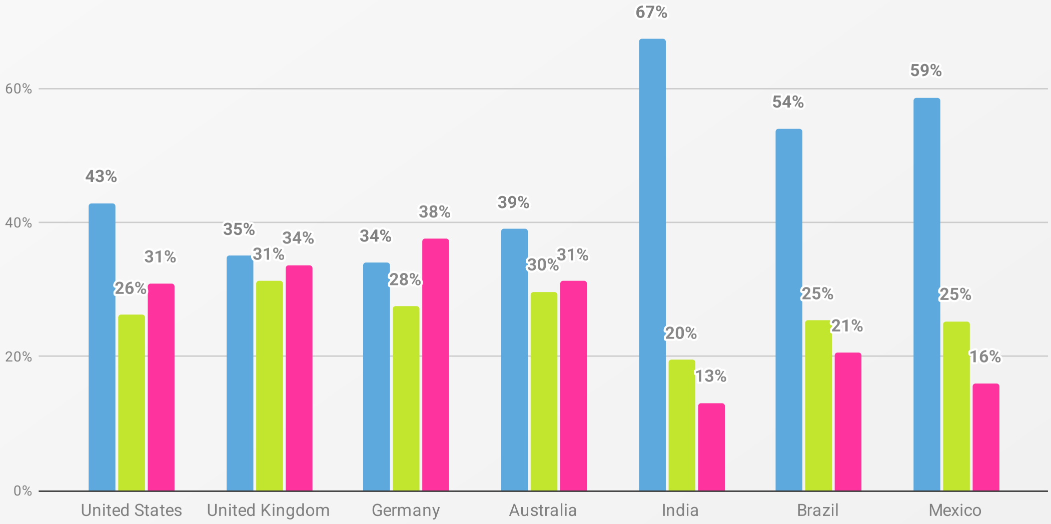
Figure 121. '*Have you ever shared sensitive work information with AI tools without your employer's knowledge?*' by country.



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 4573 (age 18+).
Dates conducted: May 2, 2025 - May 27, 2025.

Confidence in spotting AI-generated content also splits countries (Figure 122). Participants in India (67%), Mexico (59%), and Brazil (54%) reported the highest levels of confidence. The US (43%) and Australia (39%) were in the middle of the range, with slightly lower levels of confidence. In clear-cut contrast, participants from Germany (38%) had the lowest levels of confidence, followed by the UK (34%).

Figure 122. '*How confident are you in your ability to recognize AI-generated content?*' by country.



Base: US, UK, Germany, Australia, India, Brazil, and Mexico. Total number of participants: 7000 (age 18+).
Dates conducted: May 2, 2025 - May 27, 2025.

In conclusion, the data on AI usage and perceptions reveal a complex and often contradictory picture across countries. There is a clear divide between the high rates of AI adoption in India, Mexico, and Brazil and the lower rates in the United Kingdom, Germany, and Australia. This divergence is accompanied by a paradox: while participants in countries like India and Mexico are more likely to use AI and express high confidence in their ability to recognize AI-generated content, they are also less likely to have received training on AI's privacy and security risks.

This combination of high adoption, high confidence, and low training, particularly in Brazil and Mexico, presents a heightened risk profile. Conversely, participants in the UK and Germany show lower adoption and confidence, but also a lower willingness to share sensitive information with AI tools.

In other words: some countries are sprinting into the AI age without checking their laces, while others are still standing at the starting line with one sock on.

Looks like you made it 💪

Achievement unlocked: Appendix Mastery. No loot box, just a universe-brain stuffed with more cybersecurity insight than most boardrooms manage in a quarter.

There's plenty more where this came from on the Behave Hub. Are you signed up yet?

Or maybe your brain's buzzing and you're wondering 'so what now?'. We've got you. Book a chat with CybSafe and together we can plot your next steps.

Want to learn more about the intersection of people and security? Attend a Convene conference where thought leaders share their creative approaches to addressing human risk, and sign up for our Convene Current newsletter to get more resources in your inbox each month.

Check out the National Cybersecurity Alliance and join our mission to empower a more secure, interconnected world by becoming a partner or supporter, a network working across sectors to raise awareness and make a meaningful impact.

NATIONAL
CYBERSECURITY
ALLIANCE

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

CybSafe is a cybersecurity software platform transforming how organizations manage human risk in the AI era. It integrates with your existing tools and uses behavioral data and intelligent automation to surface real risk signals, deliver science-backed interventions, and track behavior change—helping reduce the likelihood and impact of cyber incidents before they disrupt the business.

At the heart of CybSafe's behavioral security platform is SebDB – the world's cybersecurity behavior database – offering insight into every security behavior capable of minimizing human cyber risk.

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

Acknowledgements

Famia Humayun

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