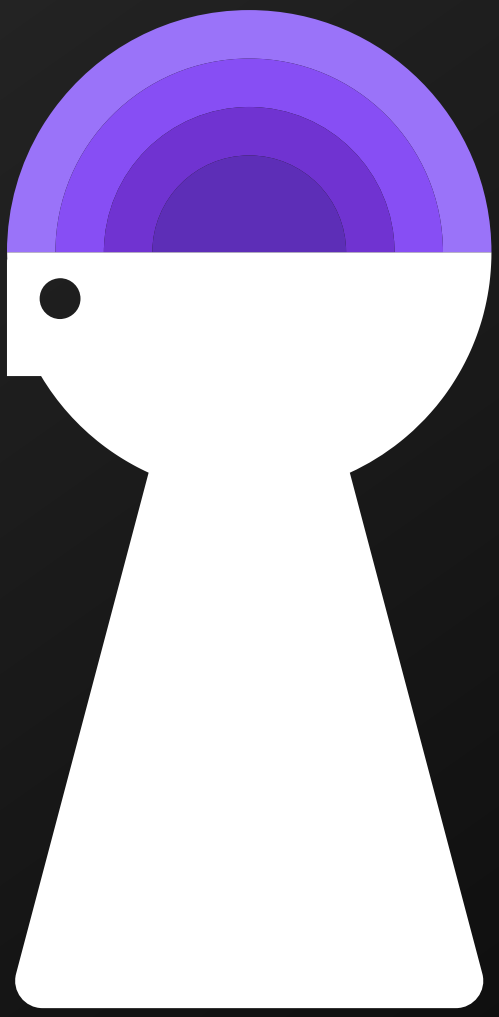
NATIONAL CYBERSECURITY ALLIANCE

CYBSAFE



Oh, Behave!

The Annual Cybersecurity Attitudes and Behaviors Report 2025-2026

EXECUTIVE SUMMARY

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.

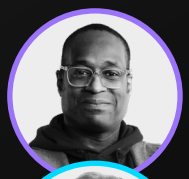
But buried in the maelstrom are real signals: how age, culture, and sector shape security decisions. Why younger generations are both the most confident and the most vulnerable. And where organizations can step in to bridge the gap.

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.

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)

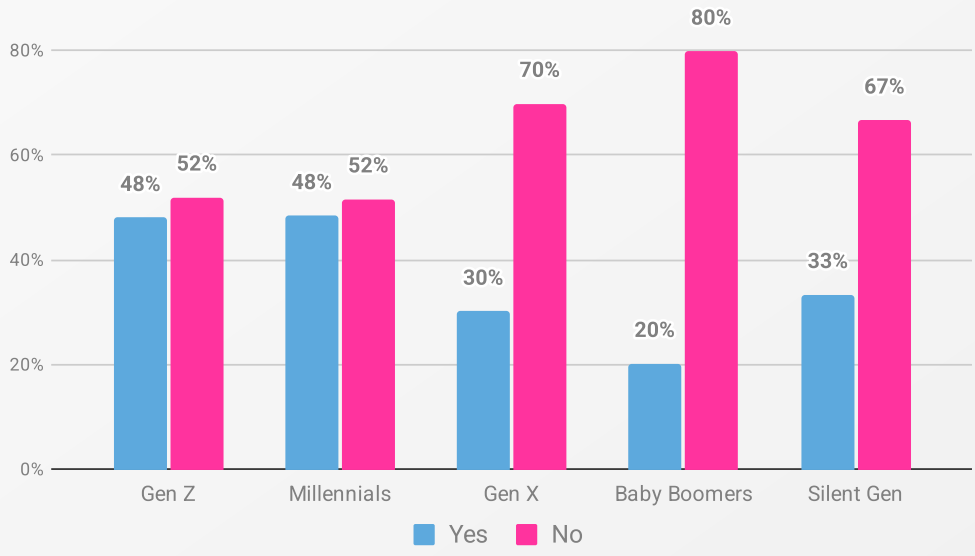
The rapid rise in AI usage is the double-edged sword to end all double-edged swords: while it boosts productivity, it also opens up new and urgent security risks, particularly as employees share sensitive data without proper oversight.

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

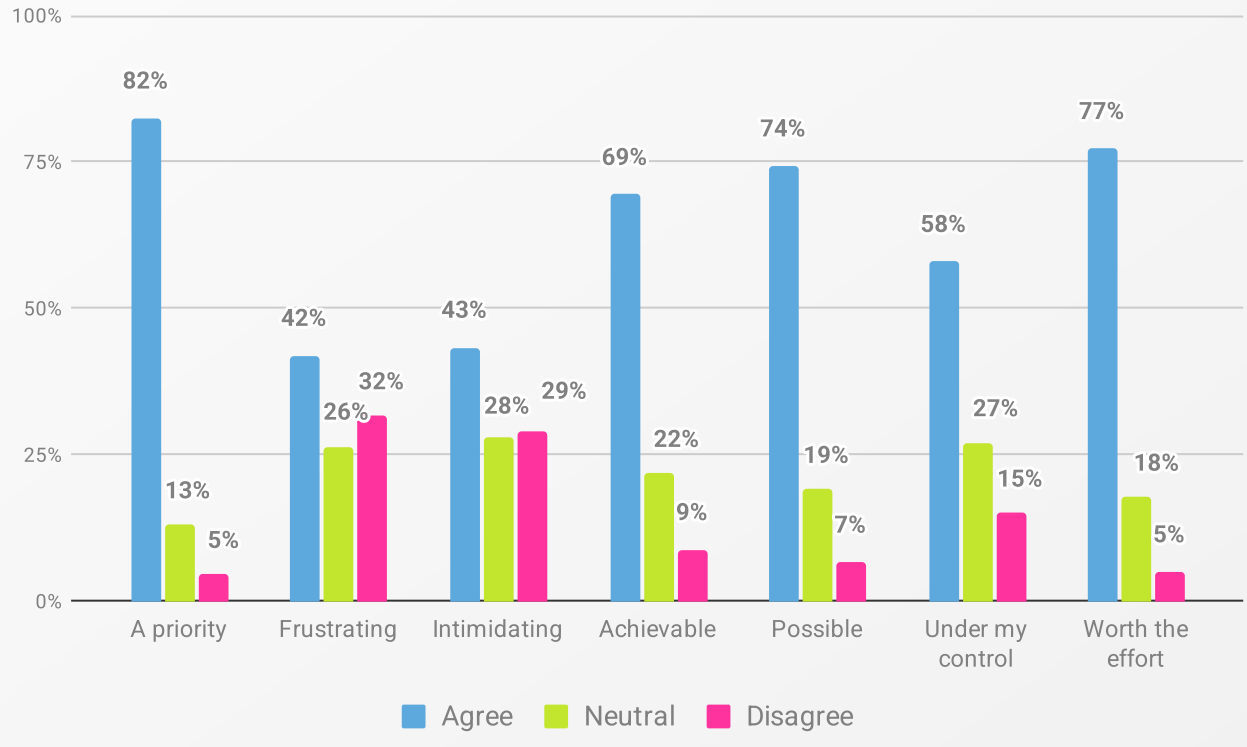
India leads in AI usage, with a hefty 87% of participants using AI and 55% of employees sharing sensitive work information with AI tools. This is in stark contrast to the UK, Australia, and Germany, where roughly half of participants report not using any AI tools at all. While Brazil and Mexico also 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

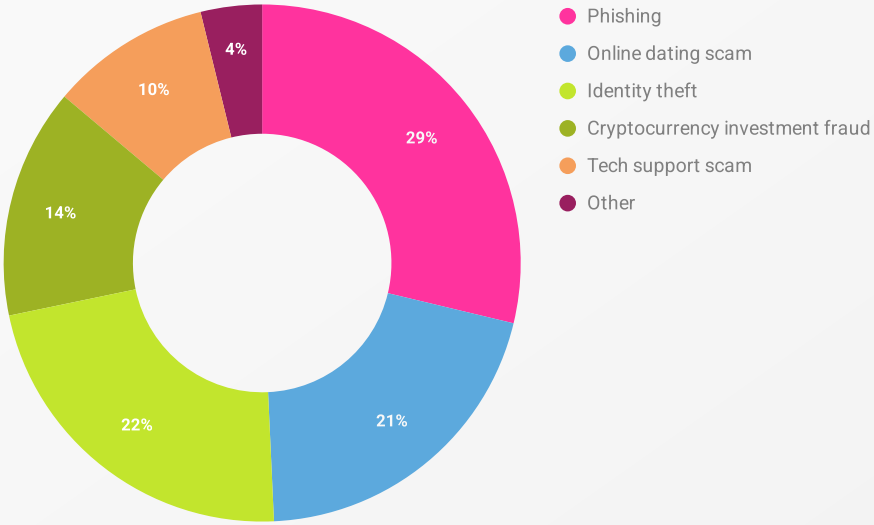
Concern about becoming a victim of scams and wider cybercrimes is widespread. Around two-thirds of participants (68%) express worry, an increase since 2024, and particularly pronounced among younger generations (70% of Millennials). Yet only 41% consider themselves likely targets. This perception has 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.

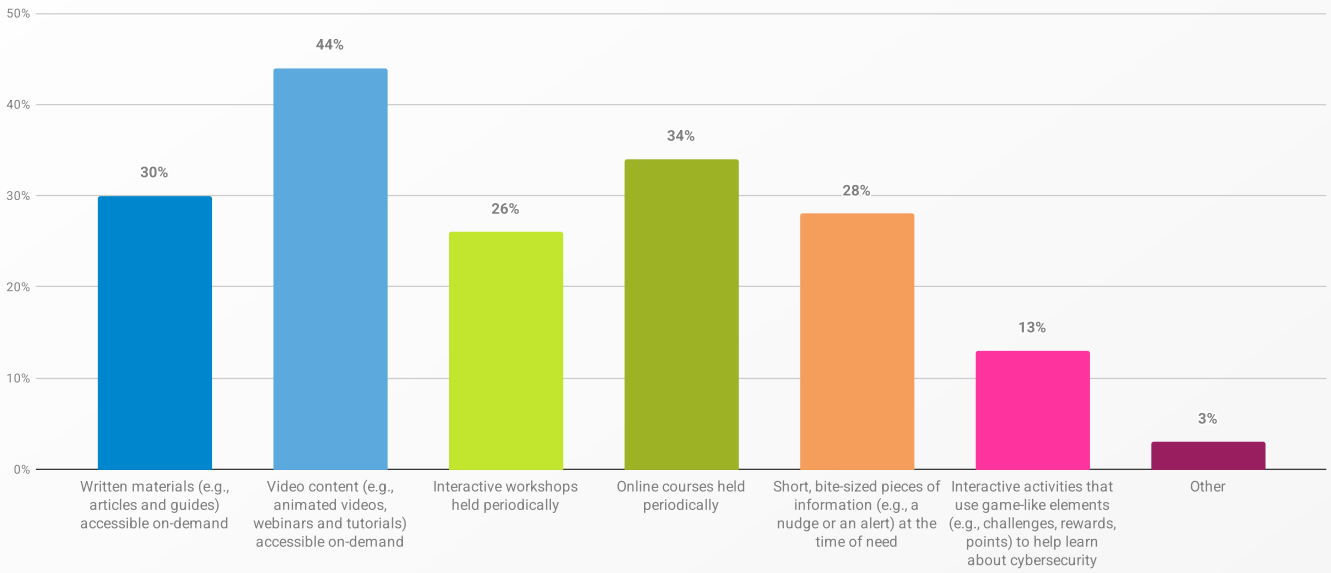
With crime on the rise, we need to think about how best to make people aware of the risk and how they can respond to it; enter... training. Let's see who gets access to it, who takes it up, and how effective it really is.

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.

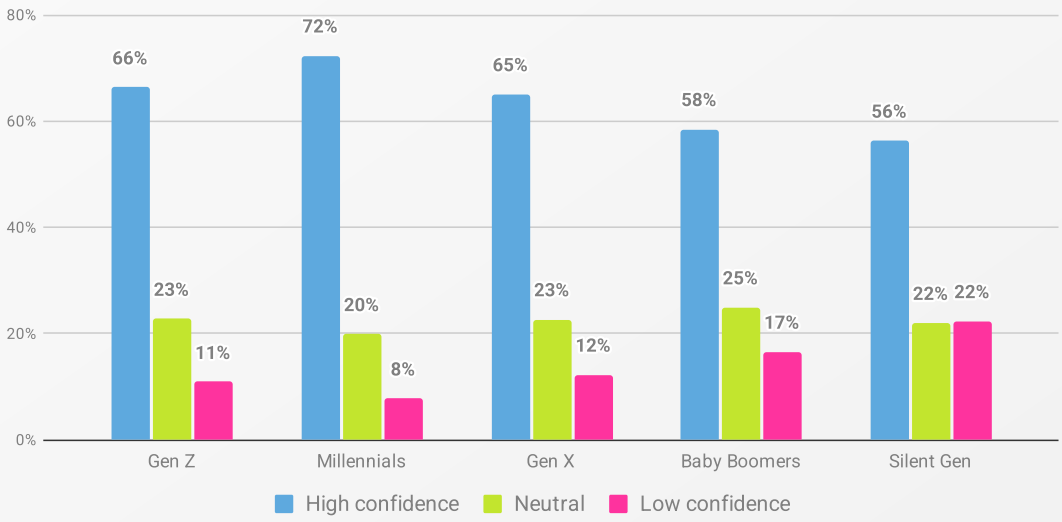
Ctrl+Alt+Delusional: Cybersecurity knowledge & behaviors

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.

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