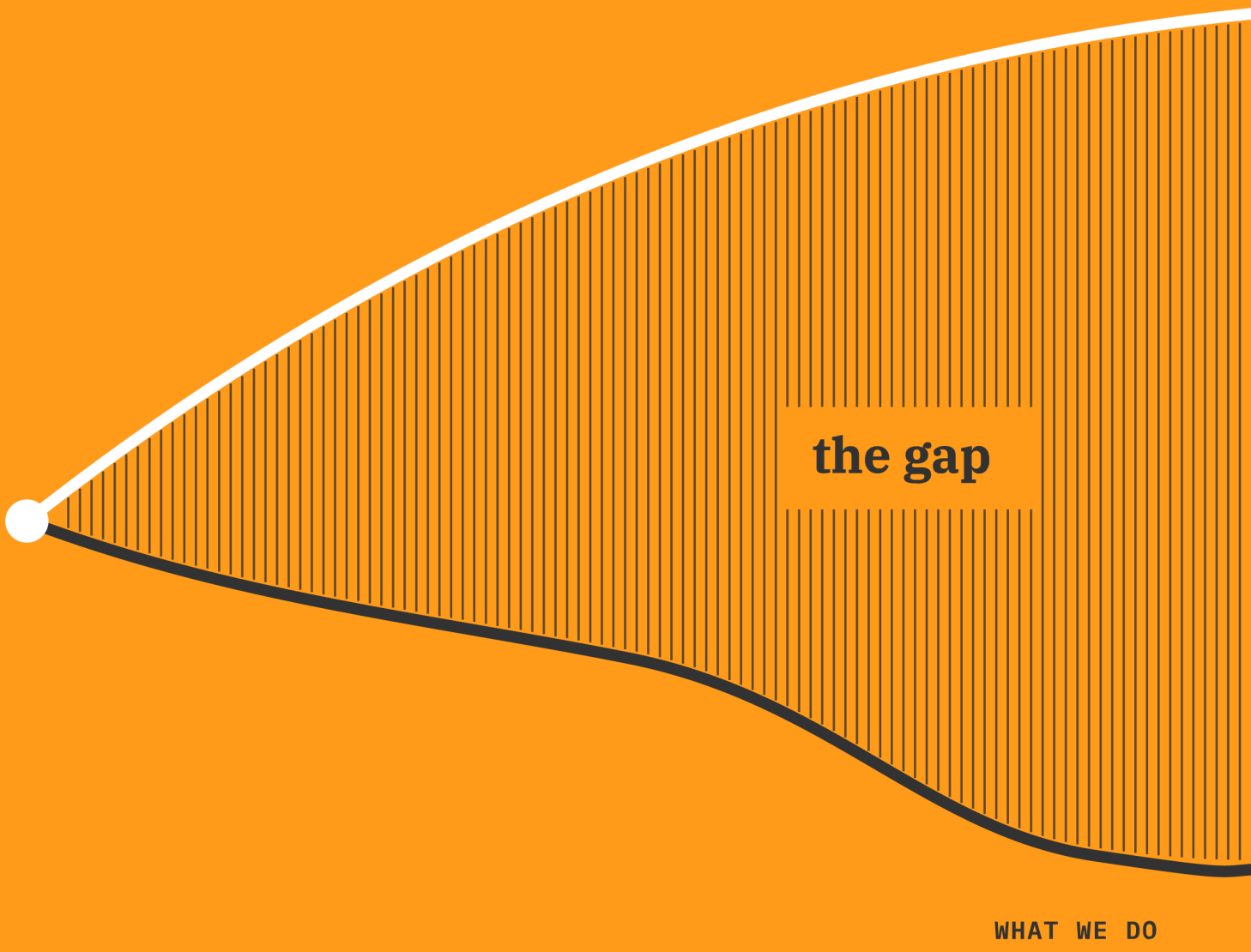
Oh, Behave!

BUSINESS EDITION

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



NATIONAL CYBERSECURITY ALLIANCE

CYBSAFE

More BS* than a résumé written by ChatGPT

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

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

Optimism in the air, chaos in the feeds

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

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

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

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

So, what's the vibe in '26?

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

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

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

**Behavioral science, of course.*

Strong egos, sticky notes

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

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

Oversharing with the bots

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

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

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

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

People. Even messier than your browser tabs

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

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

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

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

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

Oz & Lisa



Oz Alashe, MBE
CEO & Founder,
CybSafe



Lisa Plaggemier
Executive Director,
The National Cybersecurity Alliance

Business edition

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

Critical takeaways

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

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

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

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

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

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

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

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

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

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

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

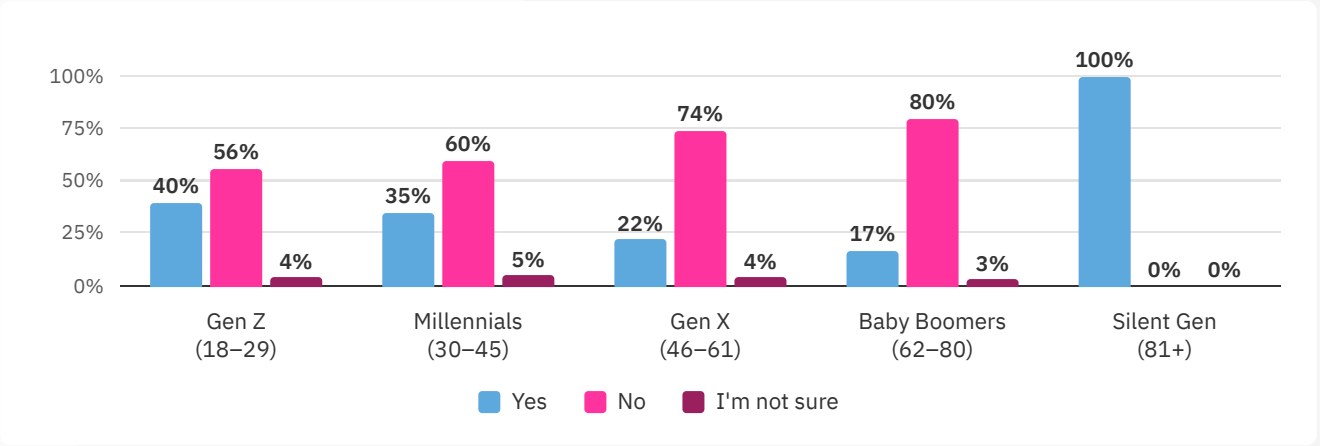
👉 **NEWS YOU CAN USE**

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

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

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

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



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

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

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

COUNTRY COMPARISONS

AI adoption & workplace use

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

Security, training and oversharing

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

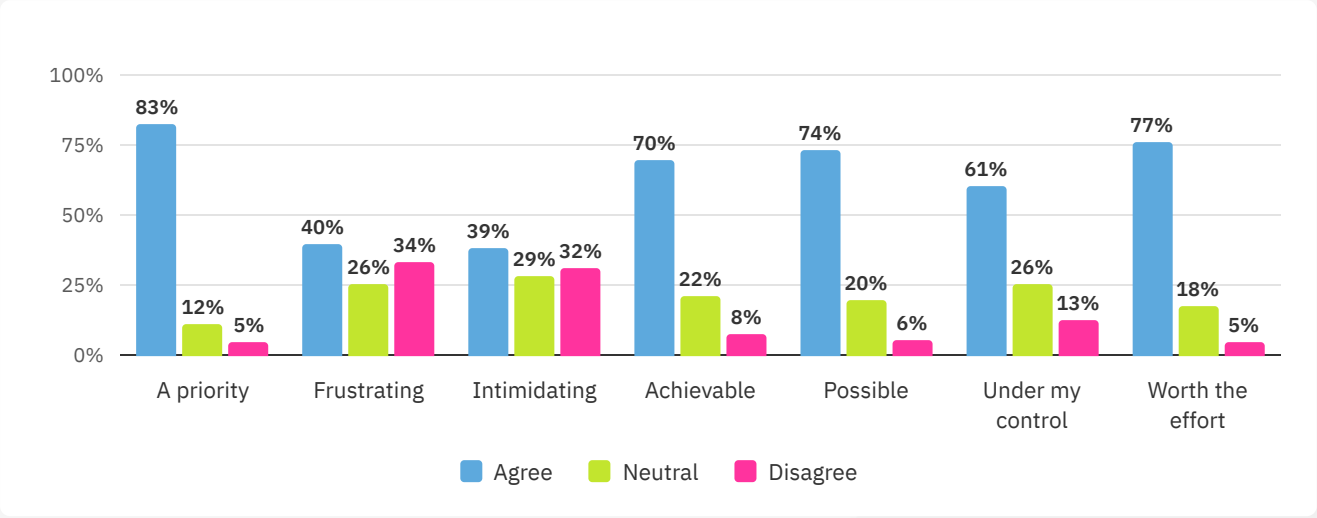
Spotting fakes & public sentiment

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

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

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

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



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

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

👉 **NEWS YOU CAN USE**

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

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

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

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

COUNTRY COMPARISONS

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

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

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

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

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

Scam-o-rama: When bad clicks happen to good people. **Cybercrime victimization & reporting**

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

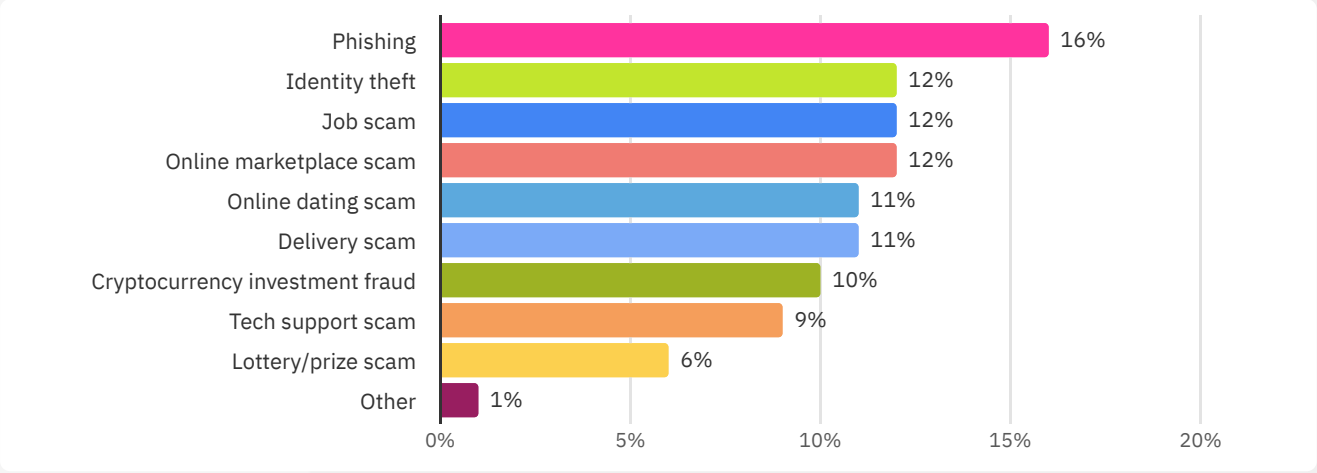
A meaningful share has also grown fatalistic: about a third consider losing money (33%) or having personal data stolen (39%) an unavoidable cost of being online. Concerns about those defending against cybercrime are widespread too: 57% doubt law enforcement has the capability and capacity to fight cybercrime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

👉 **NEWS YOU CAN USE**

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

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

Figure iii. Types of cybercrime incidents.



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

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

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

👉 NEWS YOU CAN USE

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

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

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

🌏 COUNTRY COMPARISONS

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

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

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

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

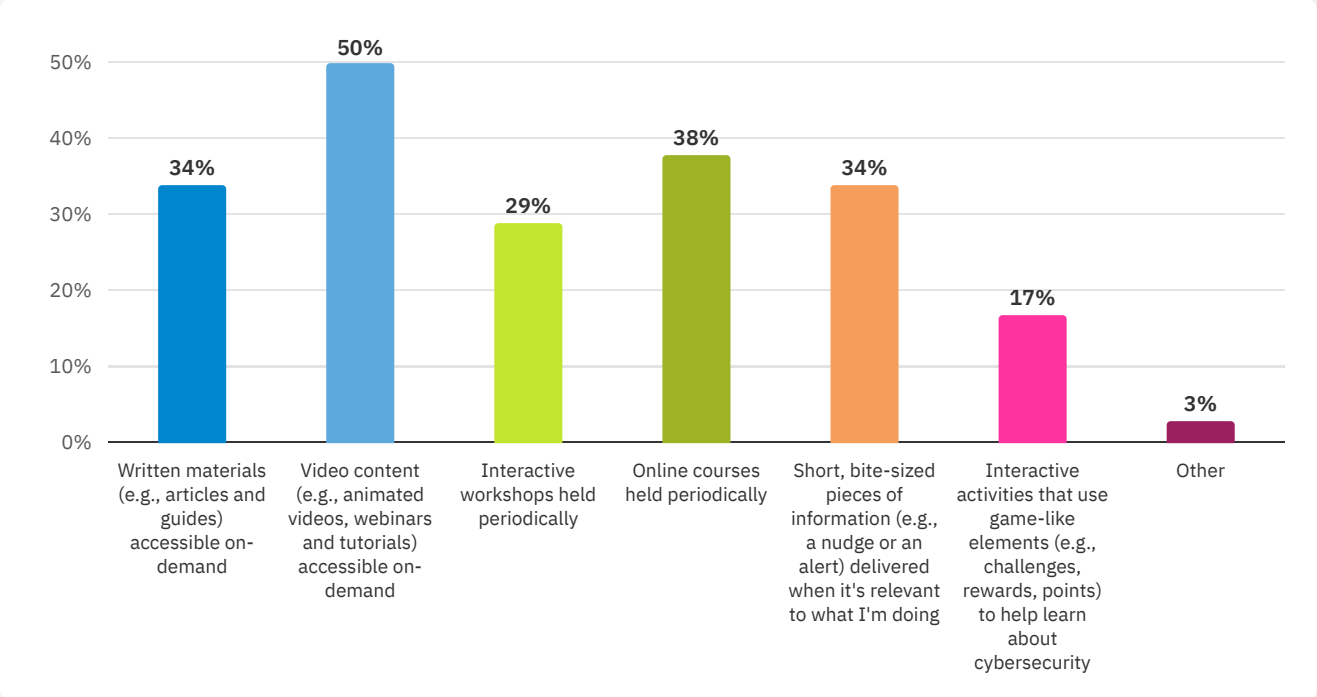
Singapore: Where the crypto pirates hang out 🏴‍☠️, or at least where they target – 25% of all crypto fraud victims are here, second only to India (30%).

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

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

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

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



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

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

👉 **NEWS YOU CAN USE**

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

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

🌏 **COUNTRY COMPARISONS**

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

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

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

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

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

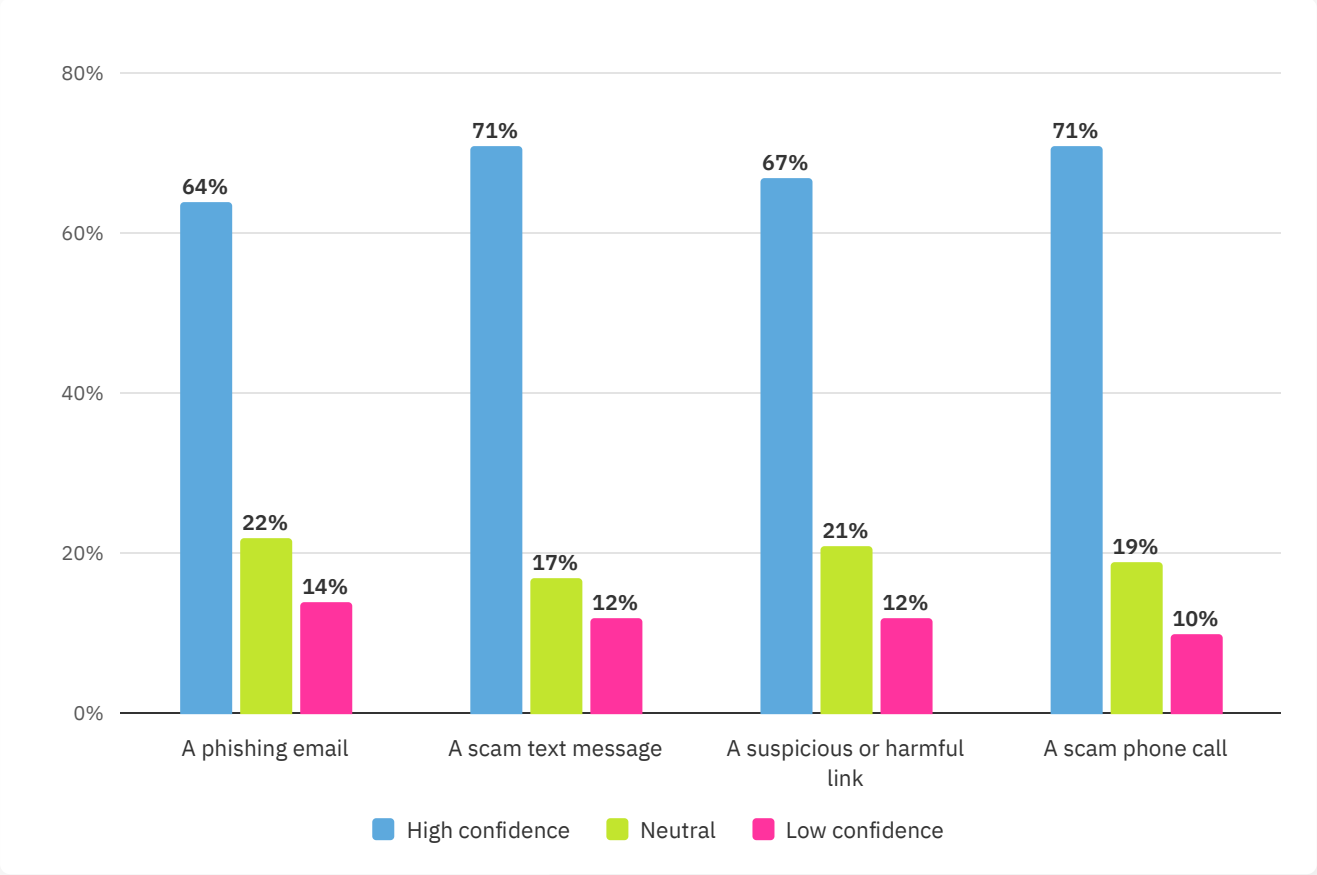
Lock it down or just sticky-note it? Cybersecurity behaviors

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

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

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

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



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

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

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

👉 NEWS YOU CAN USE

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

🌍 COUNTRY COMPARISONS

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

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

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

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

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

About

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 the AI platform that points at the workforce security behaviors most likely to cause a breach, changes them, and proves it worked, or explains why not.

It's the behavior change platform for the AI era – built on behavioral science and powered by SebDB, the world's cybersecurity behaviors database.

CyLab Carnegie Mellon University Security and Privacy Institute

Carnegie Mellon University is a private research university serving more than 16,500 students from over 130 countries. Widely regarded as the birthplace of artificial intelligence, it holds top rankings in fields such as AI, business analytics and drama, and its research spans technology, science, policy and the arts. CyLab is the university-wide security and privacy institute at CMU that coordinates security and privacy research and education across all departments. Its mission is to catalyze, support, promote, and strengthen collaborative security and privacy research and education across departments, disciplines, and geographic boundaries to achieve significant impact on research, education, public policy, and practice.

Authors

Dr. Suzie Dobrontei, CPsychol, Behavioral Scientist, CybSafe

Dr. Jason R.C. Nurse, Director of Science & Research, CybSafe and Reader in Cyber Security, University of Kent

Contact us: research@cybsafe.com

Expert contributors

Oz Alashe MBE, CEO & Founder, CybSafe

Lisa Plaggemier, Executive Director, The National Cybersecurity Alliance

Jennifer Cook, Senior Director of Marketing, The National Cybersecurity Alliance

Brian Hansford, SVP of Marketing, The National Cybersecurity Alliance

Dr. Lorrie Faith Cranor, Director and Bosch Distinguished Professor, CyLab Security & Privacy Institute; FORE Systems University Professor, Computer Science and Engineering & Public Policy, Carnegie Mellon University

Acknowledgments

Cliff Steinhauer, The National Cybersecurity Alliance

Max McKenna, The National Cybersecurity Alliance

Adam Brett, Senior Account Executive, ModOp

Patrice Gamble, Account Director, ModOp

Alice Cooke, Copywriter, CybSafe

Veronika Bondareva, Head of Creative & Design, CybSafe

Lily Klucinec, PhD student in Societal Computing, Carnegie Mellon University

Alexandra Li, PhD student in Societal Computing, Carnegie Mellon University

Ginger Smith, PhD student in Engineering & Public Policy, Carnegie Mellon University