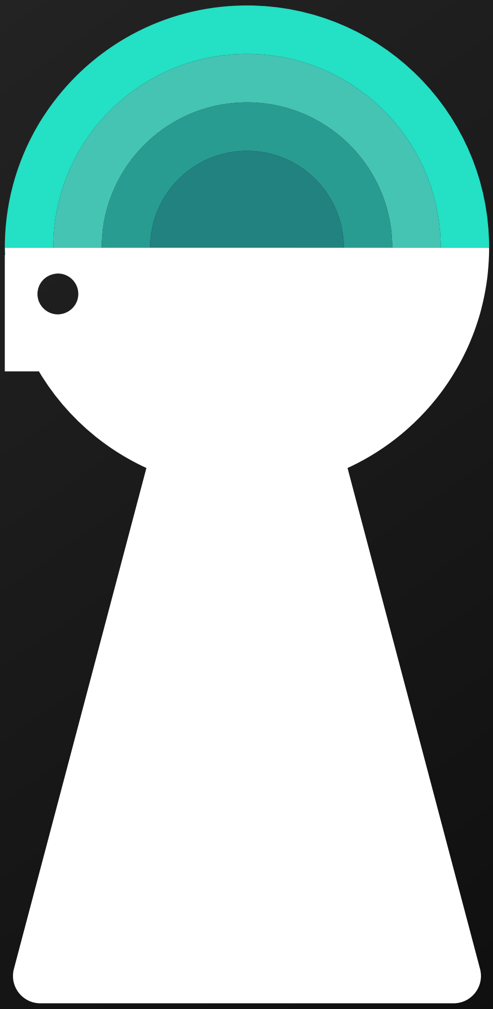
NATIONAL CYBERSECURITY ALLIANCE

CYBSAFE



Oh, Behave!

The Annual Cybersecurity Attitudes and Behaviors Report 2024-2025

Contents

More BS* than a televised debate 🎪

Welcome to the 2024-2025 Annual Cybersecurity Attitudes and Behaviors Report. Or, as it’s known round these parts, Oh, Behave!

Hold on tight. 2024 is officially a whirlwind: elections, sporting events, and enough breaking news to make your head spin. Between deciphering political mudslinging and keeping up with “Have you seen what AI can do now?!”, it feels like the year is on fast forward, with no sign of slowing.

But this year isn’t just momentous in politics and sports: Cybersecurity Awareness Month is turning 21 this year! Yet, as we raise a glass (which it could now legally do across the world) we can’t ignore that since its inception, the online threats we face have rocketed. The stakes are higher than ever.

Thankfully, y’all are a discerning bunch. More and more of this beautiful community are ditching the outdated notion that security awareness training magically transforms people into security evangelists.

More and more of you are asking: “What now?”

Well, it starts with understanding what people think, and what people do, and why they do what they do. Because (genuinely rather fascinating) behaviors and attitudes abound—from the considered clickers to the free-wheeling risk-takers—a foundation in behavioral science is now the cornerstone of strong cybersecurity.

That’s exactly what makes this report essential reading. It’s why we’re back for the fourth year running, with the big-hitting, data-driven blockbuster you’ve come to expect.

What's the score in '24?

We've come back bigger and better! We've upped our participant numbers to over 7,000 this year (7,012, to be obnoxiously precise), which means a clearer picture of security behaviors and attitudes alike.

To achieve this we partnered with some outstanding organizations: New Zealand's National Cyber Security Centre (NCSC), SAP, and the Australian Cyber Collaboration Center.

These partnerships allowed us to expand to more countries. India, Germany, the UK, US, Canada, New Zealand and Australia are all representing. This means for the first time we've surveyed the Five Eyes (a longstanding intel-sharing powerhouse of an alliance, for the uninitiated).

However, just like last year, we've kept a strong focus on the workforce, with over 65% of participants working either full time or part time. This insider knowledge is vital in helping organizations understand how employees behave online.

AI-openers ahoy

You *might* just have noticed AI is in practically every tech conversation these days (don't *even* get us started on LinkedIn influencers). So it's only natural that we dig into how people use AI tools, their understanding of AI risks, and their perception of AI companies and content. We've even snuck in a question about elections and AI, in light of 2024's political circus (we're looking at you, UK and US!).

That doesn't mean we slacked off on the fundamentals—far from it. We've spread the net wide on people's knowledge of cybersecurity threats, their security habits, and the hurdles they face online.

Some stats will brighten your day, some will leave you scratching your head, some might even make you sweat a little. But hey, just like last year, there's hope! And fret not, because this report is packed with recommendations for organizations and individuals to bridge the gap between knowledge and the thing that matters the most...action.

Slip into your Speedos!

No two ways about it, changing behavior takes effort. Plain sailing it ain't. But creating a safer digital world is worth the fight, right?

So, slip into your Speedos (or the aquatic attire if your choice, no judgment here), and let's dive into a veritable ocean of BS*. We hope you enjoy reading this as much as we enjoyed putting it together.

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

Oz & Lisa

Oz Alashe, MBE
CEO & Founder, CybSafe

Lisa Plaggemier
Executive Director, The National Cybersecurity Alliance

* Behavioral science, obvs.

Report aim & structure

Our fourth Cybersecurity Attitudes and Behaviors, Oh Behave! 2024-2025 report aims to provide a comprehensive international snapshot of people's cybersecurity attitudes and behaviors across representative global samples.

No guesswork or speculation here. Just a global pulse check on how real, actual people think and act.

Workforce. Covered.

Of the 7,000+ respondents, the majority are employees somewhere. This is important because the more we understand about employees' behaviors, the better we can help them behave safely.

We built on the last three years' findings and focused on five critical security behaviors:

1. Ensuring password hygiene[1]
    - Password creation habits—specifically, password length, use of personal information and single dictionary words
    - 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 them[8]

[1] SebDB behavior: [SB003] Uses a strong password or passphrase

[2] SebDB behavior: [SB016] Does not reuse passwords between accounts

[3] SebDB behaviors: [SB209] Uses a stand-alone password manager application, [SB210] Saves passwords of passphrases into a browser

[4] SebDB behavior: [SB001] Enables multi-factor authentication for workplace accounts

[5] SebDB behaviors: [SB024] Enables auto-updates for workplace devices (if permitted), [SB208] Ensures work devices and software are updated regularly, [SB174] Does not log in from a device running out of date operating software

[6] SebDB behavior: [SB061] Regularly backs up data

[7] SebDB behaviors: [SB081] Checks instant messages for signs of deception, [SB088] Checks emails for signs of deception

[8] SebDB behaviors: [SB013] Reports known or suspected security incidents, [SB087] Reports suspicious messages (e-mails, texts, phone calls)

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

- What is the level of people's online presence?
- What are people's general attitudes toward cybersecurity?
- Who do people rely on when it comes to cybersecurity?
- Who is responsible for our online security in the workplace and at home?
- What types of cybercrimes do people experience? Do they report them?
- Who has access to training, and do they use it?[9] If so, how do they feel about it?
- How do people engage with cybersecurity in terms of the five specific security behaviors?
- How do people feel about artificial intelligence (AI) and its impact on their personal and professional lives?

Upping the AI-nte

Yup, that's right—artificial intelligence (AKA everybody's favorite dinner party topic: 'are we all about to lose our jobs?' ...nope) is a crucial addition to the survey this year. And it's not just lip service either, AI is on the front lines of both cyber attack and cyber defense.

We looked into how people use it, their concerns, trust, confidence, and the broader implications of AI on decision-making during elections, work, and online security.

Content warning: unfiltered employee opinions ahead!

The survey combined multiple choice and open-ended questions, resulting in a combination of quantitative data and qualitative responses. With this, we aim to uncover the motivations and concerns that drive individuals' cybersecurity behaviors.

Ultimately, the goal is to bring actionable insights to cybersecurity professionals, policy makers, and educators. We believe this information will help to develop more effective strategies to enhance online security for everyone.

Finally, in the Appendices, you can find the nitty-gritty details of our research methodology, participant pool demographics, and the country-specific findings.

[9] SebDB behavior: [SB015] Completes assigned security awareness training successfully

Key terms

We're not really ones for jargon. Here are the key terms we've used throughout the report:

Artificial intelligence (AI): The application of mathematics and software code to teach computers how to understand, synthesize, and generate knowledge in ways similar to how people do it.

AI tools: This term could be debated for...a long time. To keep things simple, and for the purposes of this report "AI tools" were described to participants as 'software programs that use AI techniques to achieve specific goals. This includes Generative AI such as ChatGPT, Copilot, and DALL-E'.

AI-related cybercrime: Criminal activity that uses AI to improve the effectiveness and efficiency 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 people have towards 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 our focus 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.

Cyberbullying: Cyberbullying occurs on digital platforms. It includes sending, posting, or sharing negative, harmful, false, or mean content about someone else. It also covers sharing personal or private information about someone else, and causing embarrassment or humiliation.

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

KEY TERMS

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

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

Identity theft: The stealing of someone's personal information to assume their identity. This can involve applying for credit and loans, and filing taxes using a victim's identity, potentially damaging their credit status.

(Security) knowledge: People's knowledge and understanding about: cybersecurity risk; why risk matters to the organization and themselves; and the security behaviors required to reduce the risk.

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: The adoption of a fake online identity to create the illusion of a romantic or close relationship to manipulate and/or steal. Dating scams often use highly emotive requests for money, claiming emergency medical care, transport costs, or overseas visits should be paid for.

Password hygiene: Creating unique and separate passwords for online accounts, managing passwords using browser or standalone applications, and the approach of changing passwords.

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

Phishing: The act of getting people to provide information or install dangerous software in order to steal money or data. Phishing is often done via fake emails that appear to be from trusted senders, encouraging people to click malicious links, open malicious attachments, or supply sensitive information.

Sensitive (important) online accounts: Online accounts holding identity, location, and payment information (e.g., payment-related sites, social media accounts, and work accounts).

(Security) training: The process through which people acquire and develop skills, e.g., how to use a particular security mechanism correctly, or how to recognize and respond to a social engineering attack.

Executive summary

Our online presence: The Matrix? Completed it, mate

Artificial intelligence (AI): AI caramba!

General attitudes to online security: Relationship status = ‘It’s complicated’

Reliance on others for cybersecurity: It takes a (very patient) village

Responsibility for cybersecurity: Who’s driving this thing?

Cybercrime victimization & reporting: A growing sense of helplessness

Cybersecurity training: This ain’t a game

Cybersecurity knowledge & behaviors: Hack-proof or hapless?

B-sides: India

Executive summary

Our online presence:
The Matrix? Completed it, mate

An impressive 53% of participants are always connected online. Read that again. They are always connected online.

An additional 38% go online several times a day. Younger generations, particularly Gen Z (65%) and Millennials (64%), are the most connected. A third of the participants reported having ten or more sensitive online accounts, with younger generations again leading in multiple account ownership.

Artificial intelligence (AI):
AI caramba!

Let's talk about AI—that little-known, under-discussed topic that definitely hasn't dominated any and all IT conversations for 18+ months.

But talking about it is one thing—who's actually using it? Over half (56%) of participants report not using any AI tools. Among users of AI tools, 17% use them at home, 11% at work, and 16% in both settings. AI usage was highest among younger participants (72% of Gen Z). ChatGPT was the most popular generative AI tool, used by 65% of participants who use AI tools.

> ***38% admitted to sharing sensitive work information with AI without their employer's knowledge.***

So, there's plenty of AI adoption going on...but who has the skills and knowledge to back it up? It's not great news: More than half of employed participants (52%) and students (58%) had not received training on safe AI use. A terrifying 38% admitted to sharing sensitive work information with AI without their employer's knowledge, and this was more prominent among younger generations (46% of Gen Z, 43% of Millennials, Figure 1).

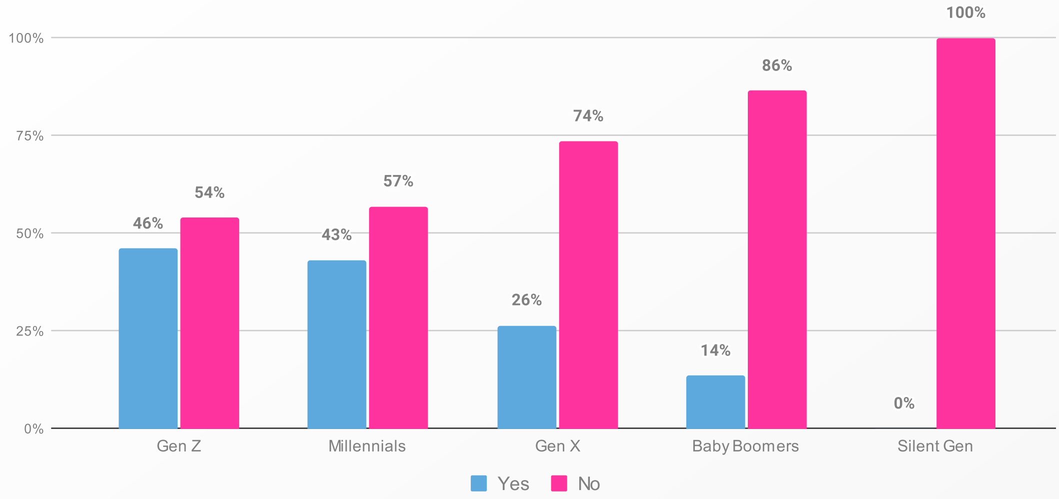


Figure 1. *"Have you ever shared sensitive work information without your employer's knowledge?"* by generation.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants with generation information who use AI tools at work: 1862 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

The majority of participants (65%) expressed concern about AI-related cybercrime, with older generations showing the highest concern (73% of the Silent Generation and 70% of Baby Boomers). Trust in companies' responsible implementation of AI seemed to decline with age, with Millennials (53%) and Gen Z (50%) expressing the highest level of trust. Explore more on perceptions of AI companies in section 8.2 Trust & perceived responsibility.

Overall, participants had a balanced level of confidence in their ability to recognize AI-generated content. And much like trust in companies' responsible AI implementation, younger generations displayed the highest confidence in recognizing AI content (53% of both Gen Z and Millennials). The largest proportion of those employed (44%) felt confident in recognizing AI content, with even higher confidence levels among students (52%).

That said, most people think AI will complicate both scam detection and online security. Millennials, in particular, are more likely to believe AI will make it harder to detect scams (58%) and maintain online security (59%) compared to older generations.

Like Ron Burgundy, this next one is kind of a big deal: 36% believed it was likely AI would influence their decisions on what is real and fake during election campaigns, and this was more pronounced among younger generations (49% of Millennials and 43% of Gen Z) compared to older ones (22% of Baby Boomers and 14% of Silent Gen).

> ***36% believed it was likely AI would influence their decisions on what is real and fake during election campaigns.***

People who were working or entering the workforce were more concerned about AI affecting their careers, specifically their employment status (41% of employed, 48% of Gen Z), the nature of their work (45% of employed, 51% of Gen Z), and its impact on work productivity (47% of employed, 52% of Gen Z).

Let's face it, most of us are still feeling our way around the AI landscape. Sure, some are diving into the water head-first and settling in on a lilo. But others are dipping a cautious toe in. Either way, AI is here to stay, and the world (or, *sigh*, the LinkedIn influencer community) isn't going to stop talking about AI any time soon.

General attitudes to online security: Relationship status = 'It's complicated'

Don't get us wrong: it's a positive picture. Participants' feelings towards online safety remain generally upbeat, but some concerning trends have emerged compared to last year's *Oh, Behave!* report.

While 81% (Figure 2) still prioritize online safety, this figure has dropped by 3%. The Silent Generation (91%) and Baby Boomers (89%) place higher importance on online security compared to Gen Z (68%). But sit down for this next one: The belief that online safety is worth the effort decreased by 9% to 60%, and only 53% believe staying safe online is possible, a 5% decline.

> ***The belief that online safety is worth the effort decreased by 9% to 60%.***

Older generations, including Baby Boomers (79%) and the Silent Generation (77%), are more likely to believe that staying secure online is worthwhile, compared to only 42% of Gen Z and 47% of Millennials (both of which dropped by 10% since 2023). Similarly, only 41% of Gen Z and 45% of Millennials believe that maintaining online safety is possible.

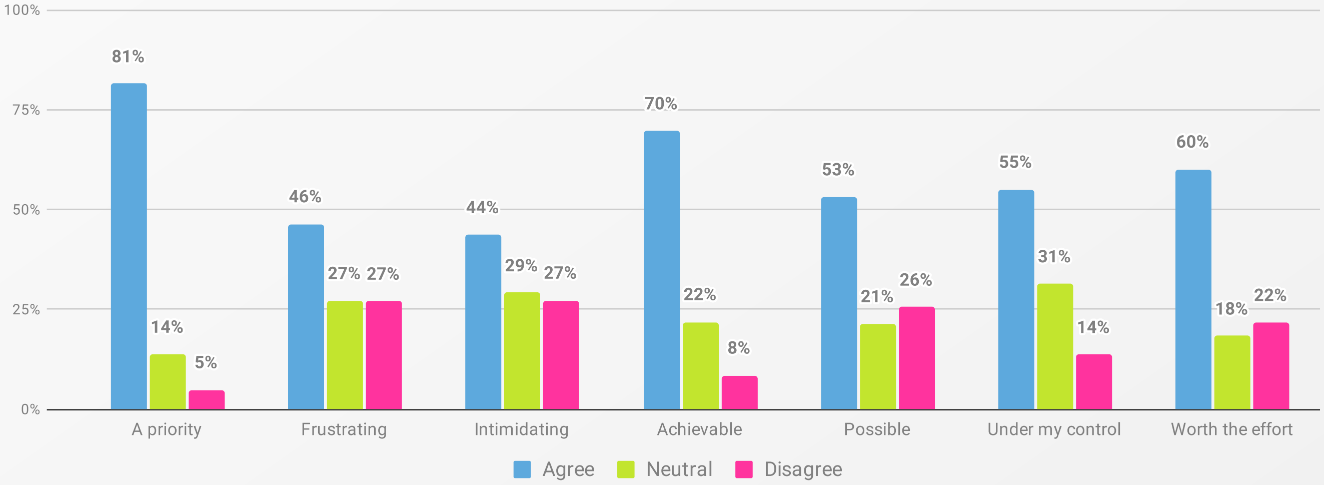


Figure 2. *"I feel that staying secure online is..."*

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants: 7012 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

Meanwhile, the frustration factor is on the rise, with the challenges of navigating online security becoming more apparent. 46% of participants reported finding staying safe online frustrating (ranging from 43% of Baby Boomers to 59% of Silent Gen), and 44% finding it intimidating (ranging from 39% of Baby Boomers to 53% of Silent Gen), both representing a 7% rise since 2023.

Seventy percent found staying safe online achievable, a slight increase from last year. Additionally, 55% felt online security is under their control (ranging from 42% of Silent Gen to 60% of Millennials), a 3% rise from 2023.

Younger generations seem to be a tad more overwhelmed by online security information—42% of Millennials and 41% of Gen Z reported minimizing their actions online as a result, compared to 30% of Baby Boomers. It was also the largest proportions of Gen Z and Millennials (both 50%) who reported going online regardless of the potential risks, in comparison to 35% of Baby Boomers.

Misconceptions about online security were common, with 43% of participants assuming their devices were automatically secure. Additionally, cost is becoming a real barrier, with more than half (52%) finding the cost of comprehensive online protection to be a burden.

The media has a mixed influence on online security attitudes. Positively, 59% of participants reported media coverage motivated them to take protective online security actions, a 3% increase from 2023, ranging from 57% of Gen X to 64% of the Silent Generation. Additionally, over half of the respondents (54%, up 3% from 2023) acknowledged media and news sources play a crucial role in keeping them informed about online security matters. However, on the not-so-good side, there is apprehension, with 44% feeling scared about their online security due to media coverage. Moreover, 47% reported the media's portrayal of online security makes it seem complicated, a 5% increase from 2023.

Reliance on others for cybersecurity: It takes a (very patient) village

We asked people about digital dependency: Who—if anyone—do they turn to for online security support? While 46% of participants rely on no one for cybersecurity, this percentage has decreased by 10% from last year. There is an increasing reliance on others, particularly among younger generations (Gen Z 38%, up 12%, Millennials 41%, up 10%). Family members and IT companies are the primary sources of help. Thirty-nine percent of participants are relied upon by their family members to ensure online security, and it turns out Millennials are the most likely generation to get called into action when Aunty Mary accidentally orders 500 Thighmasters™.

Responsibility for cybersecurity: Who's driving this thing?

People expect security as standard. According to 90% of participants, apps and platforms are at least somewhat responsible for protecting their personal information online. Though 59% still see themselves as primarily responsible, this represents a 7% decrease from 2023.

In the workplace, IT and security departments are viewed as most responsible for safeguarding information. However, their perceived responsibility has also decreased, with more responsibility now attributed to the tech industry. Personal responsibility in the workplace has also decreased by 3% to 36% from 2023.

Cybercrime victimization & reporting: A growing sense of helplessness

Overall, 61% of participants expressed worry about becoming cybercrime victims, with the Silent Generation showing the highest concern at 70%, and Gen Z being positively horizontal at 20%. Despite these worries, fewer participants feel they are likely targets compared to last year (42%).

Older generations—63% of Silent Gen and 56% of Baby Boomers—were more likely to consider themselves likely targets. Meanwhile, large proportions of Gen Z (44%) and Millennials (40%) felt they were unlikely targets.

> ***30% of participants expressed there is no point in protecting themselves as their information is already online, up 8% from 2023.***

When it came down to specific risks, about half of the participants believed losing money online is avoidable, though this percentage has dropped by 5% since 2023. The perception of the inevitability of personal information theft increased by 5% to 38%. Younger generations were more pessimistic, with notable percentages believing both financial loss and information theft online are unavoidable.

30% of participants expressed there is no point in protecting themselves as their information is already online. That's up +8% from 2023, indicating a growing sense of helplessness, which was particularly evident among Gen Z and Millennials.

Thirty-five percent of participants have encountered cybercrime, with phishing being the most common experience. Out of the 2,425 victims of cybercrime, the majority suffered phishing crimes (60%), similar to last year. Millennials were most likely to be victimized across all three types of crimes (Figure 3). While the second highest rates of online dating scams were reported by Gen Z (27%), the second highest proportions of phishing and identity theft crimes were actually reported by Gen X, with 25% and 28%, respectively.

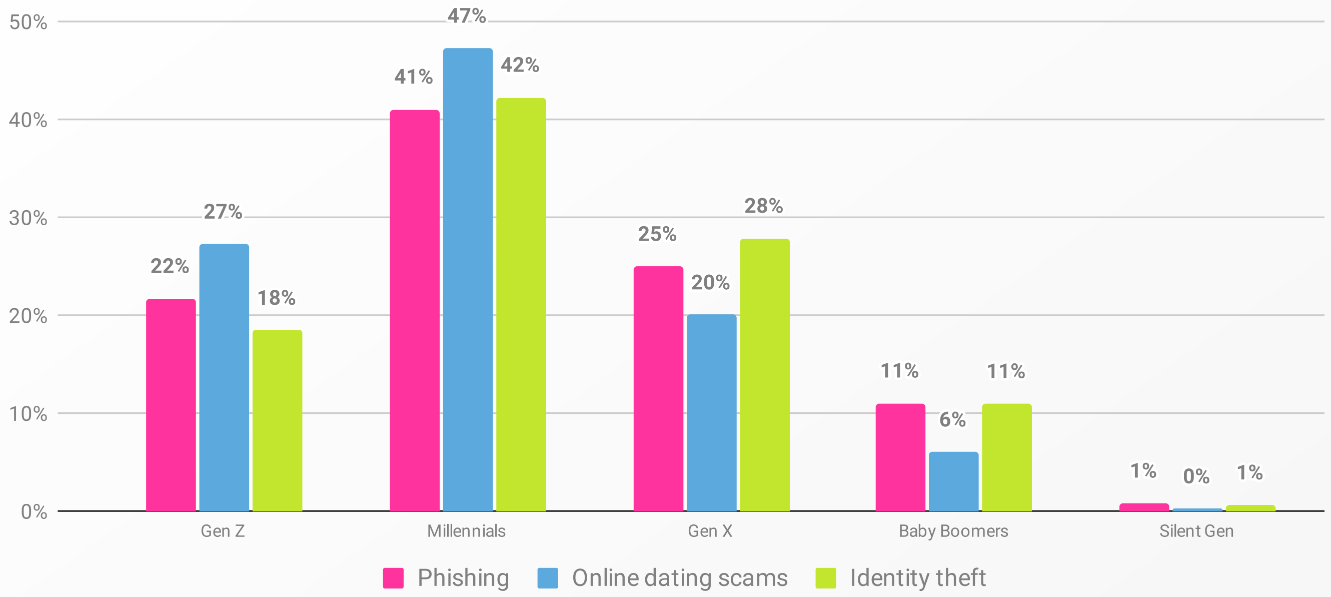


Figure 3. Cybercrime incidents by generation.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of cybercrime victims (age 18+): Phishing = 1407; Online dating scam = 1010; Identity theft = 841 (excluding any cybercrime incidents noted by 263 participants from New Zealand, who didn't provide their age). Dates conducted: March 6, 2024 - April 22, 2024.

Bullying isn't just for high school. Across all participants, 18% reported being victims of cyberbullying, representing a 3% increase from 2023. Whilst larger proportions of the younger generations reported having been cyberbullied, the percentages slightly increased for Gen X and the Silent Gen. So while the younger generations are getting the worst of it, no one's immune.

When looking ahead, 37% of participants felt unlikely they would be a victim of cybercrime in the next year, and 28% felt it was likely. Once again there seemed to be a generational trend, with younger generations—38% of Gen Z and 37% of Millennials—feeling more at risk in the future, compared to older generations, suggesting younger generations recognize their vulnerability. Those of us of a more silver-haired disposition should take note: our younger peers have more to teach us about rational skepticism than maybe we give them credit for.

Reporting rates for cybercrime were high, with 91% of phishing incidents, online dating scams, and identity thefts being reported. Additionally, 88% of cyberbullying incidents were reported. The most common reason for not reporting among victims was not knowing whom to report to.

Cybersecurity training: This ain't a game

Access to cybersecurity training has increased for the first time in four years, with 33% of participants using it and 11% having access but not utilizing it. However, 56% still lack access—a cold-sweat-inducing state of affairs. Training is most accessible to employed individuals and students, with 86% of those with access required to complete mandatory training, a 4% increase from 2023. Among those, 48% now complete it annually, a 7% decrease from 2023. Additionally, there were increases in participants completing training 'when something goes wrong' (8%) and 'both at regular intervals & when something goes wrong' (18%), by 3% and 4%, respectively.

> ***The least preferred format was online games or gamified experiences.***

The main reasons for not attending training were the classic excuses of "I already know enough" (23%) and "too busy" (22%). Video content and online courses are the preferred training formats overall (Figure 4), while older generations specifically favor written materials. The least preferred format was online games or gamified experiences, with only 11% expressing a preference for leveling up their cyber knowledge.

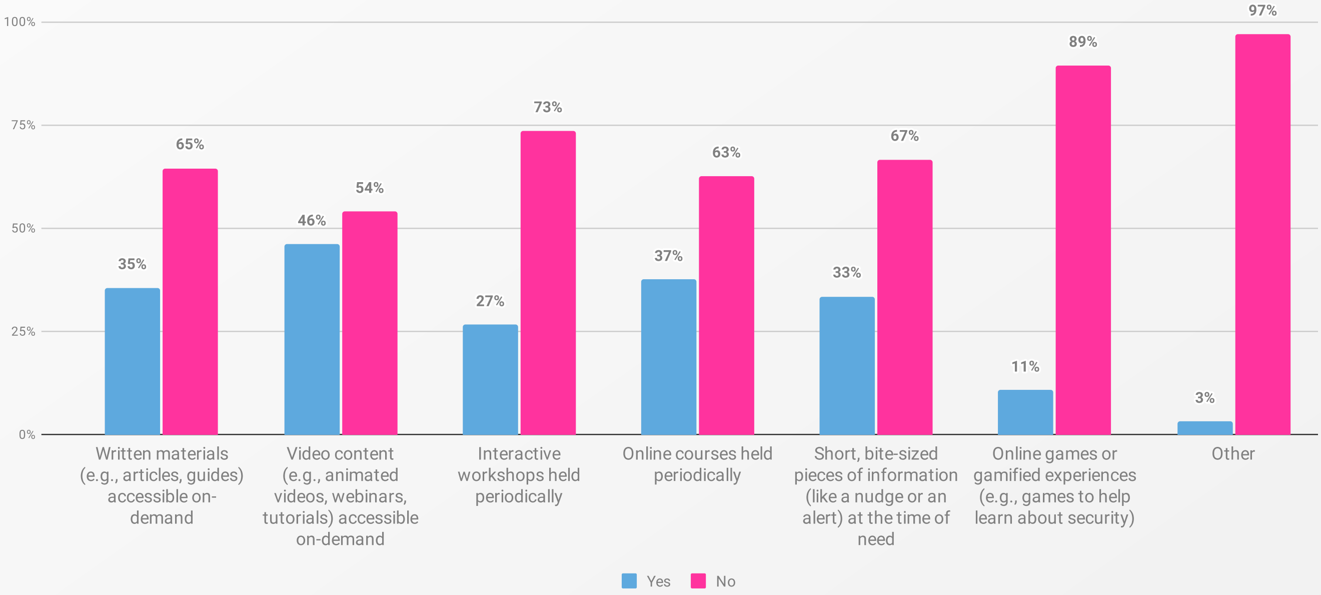


Figure 4. ***"What format do you prefer to consume cybersecurity training information?"***

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants: 7012 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

The majority (83%) of those who accessed training at their workplace or place of education found it useful. The biggest impacts reported were on recognizing and reporting phishing messages (52%) and using MFA (45%, an 11% increase from 2023). Overall, there were increases in the perceived impact of training on all security behaviors compared to 2023.

Cybersecurity knowledge & behaviors: Hack-proof or hapless?

More than half of participants (57%) reported having intermediate or advanced cybersecurity knowledge, and overall, younger generations and those with jobs put themselves higher up the know-how charts compared to other groups. Hold up though, because the data tell us a different story...

First off, password creation approaches. For the second year in a row, the percentage of participants including personal information—such as family members or pet names—in their passwords increased. Over a third (35%) of participants included personal information in their passwords, and this was more prevalent across younger generations (52% Gen Z and 45% of Millennials).

> ***Over a third (35%) of participants included personal information in their passwords.***

Forty percent of participants reported creating passwords using a single dictionary word or someone's name, an increase across all generations since 2023, with Gen Z being the highest at 52%. If we had to summarize in a word what people think they know, vs what they do, it would be this: Doh!

Sixty-five percent reported using a separate password either 'all of the time' or 'a majority of the time', but this was also less frequent across younger generations (58% of Gen Z), compared to older generations (71% of Baby Boomers).

The most preferred method for remembering multiple passwords was to write them down in a notebook (29%), and this was highest among older generations (59% of Silent Gen, and 44% of Baby Boomers). This has been a consistent finding for several years. Remembering passwords without writing them down was most common among Millennials (23%), Gen X (22%), and Gen Z (21%).

Forty-six percent of the entire participant pool had never used a password manager, but this figure is down 10% from last year. While 40% reported using one, 14% had stopped. Usage was highest among Gen Z and Millennials (both 46%), who also had the highest abandonment rates (22% and 18%). In contrast, 66% of the Silent Generation and 60% of Baby Boomers had never used a password manager.

While awareness of multi-factor authentication (MFA) has increased, with 81% of participants having heard of it (an 11% increase from 2023), actual usage remains varied across generations. Millennials and Gen Z demonstrate higher awareness but lower regular use compared to older generations, who report more consistent adoption of MFA.

Despite the known security benefits of MFA, a considerable portion of those who have heard of it either do not use it (8%) or have stopped (16%), especially among Gen Z (21% and 14%, respectively), often citing inconvenience (e.g., it takes too long, or the phone needed as a second factor is not always available) and the perceived sufficiency of passwords as reasons why. The most favored MFA method is receiving a code via text message, while USB devices are deemed the least convenient.

Notably, most regular MFA users employ it for banking and financial sites, but far fewer use it for work-related or social media accounts. This is likely linked to financial sites (rightly) mandating 2FA—workplaces take note! ←

There is a persistent gap between the awareness of the importance of software updates and the actual behavior of installing them. While the majority know how to install updates (62%), a notable number either delay (16%) or avoid doing so (20%). This discrepancy is particularly pronounced among younger generations, such as Gen Z. Despite the convenience of automatic updates, only 45% have enabled them.

Forty-five percent (a 3% increase from 2023) of participants report they 'always' or 'very often' back up their important data. Performing backups 'sometimes' was most common across generations (ranging from 31% of the Silent Gen to 36% of Gen Z), except for Baby Boomers, where the majority (27%) back up 'very often'.

Overall, confidence in recognizing phishing emails and malicious links remained high among most participants (67%), with Millennials (76%, Figure 5) and Gen Z (69%) reporting the highest levels of confidence—an increase of 6% and 10%, respectively—can we get a 'woohoo!'? However, less cheer-worthy was the fact that older generations exhibited decreased confidence compared to last year.

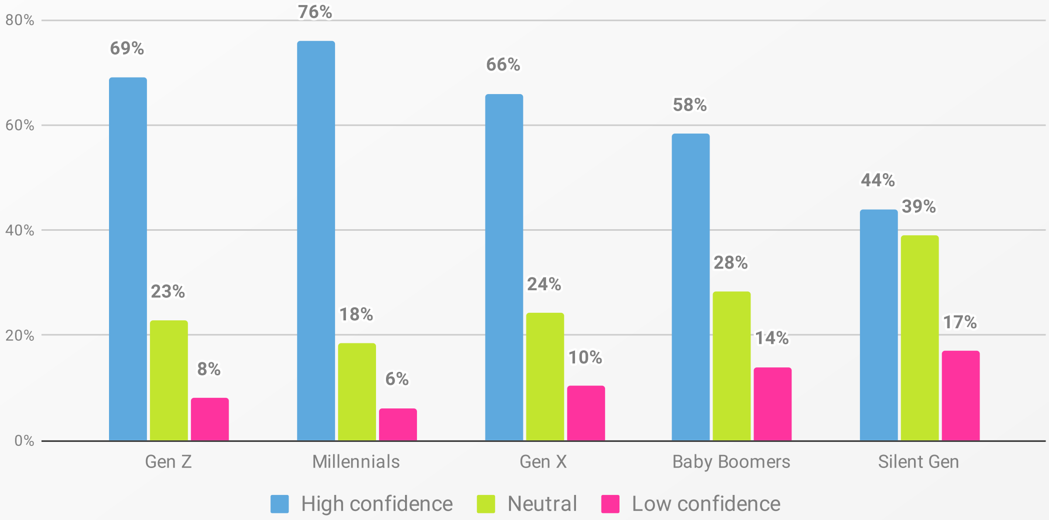


Figure 5. *"How confident are you in your ability to identify a phishing email or a malicious link?"* by generation.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants with generation information: 6749 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

Common reasons behind the lack of confidence in recognizing phishing emails included the increasing sophistication of phishing attempts, often driven by artificial intelligence, and the constant evolution of those pesky, persistent criminal tactics.

> ***The primary reasons for not reporting phishing messages include skepticism about whether reporting can effectively stop cybercriminals***

67% of participants reported 'always' or 'very often' checking their messages for phishing signs before clicking links or responding, with Baby Boomers (78%) being the most vigilant compared to just 55% of Gen Z. Younger generations were more likely to check whether an email is from a legitimate address (with 56% of Gen Z and 59% of Millennials doing so), while the majority of older generations tended to focus on detecting poor spelling and grermmatikal errors (with 75% of Baby Boomers and 79% of Silent Gen using this approach). (Head to the end of section 7.5.1 Recognizing phishing messages of the report for a deep dive into steps taken to identify legitimacy of emails and websites.)

Whilst there has been an increase in the frequency of reporting phishing messages since 2023, a notable portion (29%) still refrain from taking action, in spite of convenient reporting tools like 'Spam' or 'Report phishing' buttons. The primary reasons for not reporting phishing messages include skepticism about whether reporting can effectively stop cybercriminals, the belief that reporting would be more worthwhile if it also prevented spam from getting through to their inboxes, and the desire for tangible outcomes from their reporting efforts.

B-sides: India

India stands out in the global landscape of cybersecurity attitudes and behaviors, often showing more pronounced trends compared to other countries. We're going to dwell on this for a hot moment, because many multinational companies have *significant* operations there.

Running a global Security awareness or Human risk management program from abroad (US, Europe, etc.), and expecting to replicate the actions for the same results in the East simply won't work. The cultural differences are too pronounced. Check out Appendix B: Country comparisons for the full details.

Speaking of in-depth discussions, snap on those goggles. Now you've had the headlines, it's time to dive deep into the data...

Main findings

1. Our online presence
2. General attitudes to online security
3. Reliance on others for cybersecurity
4. Responsibility for cybersecurity
5. Cybercrime victimization & reporting
6. Cybersecurity training
7. Cybersecurity knowledge & behaviors
8. Artificial intelligence (AI)

Main findings

So, how did we snag this goldmine of intel? Forgive some repetition from the intro, but we want to catch any data-hungry folk who skipped straight to the good stuff.

The fourth Cybersecurity Attitudes and Behaviors survey was conducted online between March 6 and April 22, 2024. We collected representative samples, based on age and gender, from the United States, Canada, the United Kingdom, Germany, Australia, New Zealand, and India. Toluna[10] ran the survey in all countries except New Zealand, where the National Cyber Security Centre (NCSC)[11] managed the data collection. In total, 7,012 participants bared their souls.

Our survey targeted adults (aged 18 years and older). Two-thirds (67%) of respondents reported being in full- or part-time employment. As with previous years, we analyzed the sample population and examined differences between age groups. (Spoiler: the generational findings are famously juicy.)

Age group % within country of residence	**United States** (N=1000)	**Canada** (N=1000)	**United Kingdom** (N=1000)	**Germany** (N=1000)	**Australia** (N=1000)	**New Zealand** (N=1012)	**India** (N=1000)	**Total** (N=7012)
Gen Z (18-27)	169 16.9%	137 13.7%	142 14.2%	116 11.6%	164 16.4%	72 7.1%	264 26.4%	1064 15.2%
Millennials (28-43)	300 30.0%	268 26.8%	289 28.9%	243 24.3%	300 30.0%	236 23.3%	375 37.5%	2011 28.7%
Gen X (44-59)	266 26.6%	294 29.4%	313 31.3%	283 28.3%	261 26.1%	238 23.5%	256 25.6%	1911 27.3%
Baby Boomers (60-78)	250 25.0%	276 27.6%	242 24.2%	338 33.8%	250 25.0%	203 20.1%	104 10.4%	1663 23.7%
Silent Gen (79+)	15 1.5%	25 2.5%	15 1.5%	20 2.0%	25 2.5%	0 0%	1 0.1%	100 1.4%
Inconclusive (age not provided)	0 0%	0 0%	0 0%	0 0%	0 0%	263[12] 0%	0 0%	263 3.7%

Table 1. Number of participants per country and age group.

We also kept an eye out for any employment status-related quirks, and naturally we analyzed country-specific differences separately in Appendix B. The number of participants by age group and employment status are shown in Table 1 and Figure 6, respectively, and you can delve into the delicious demographic details in their full glory in Appendix A.

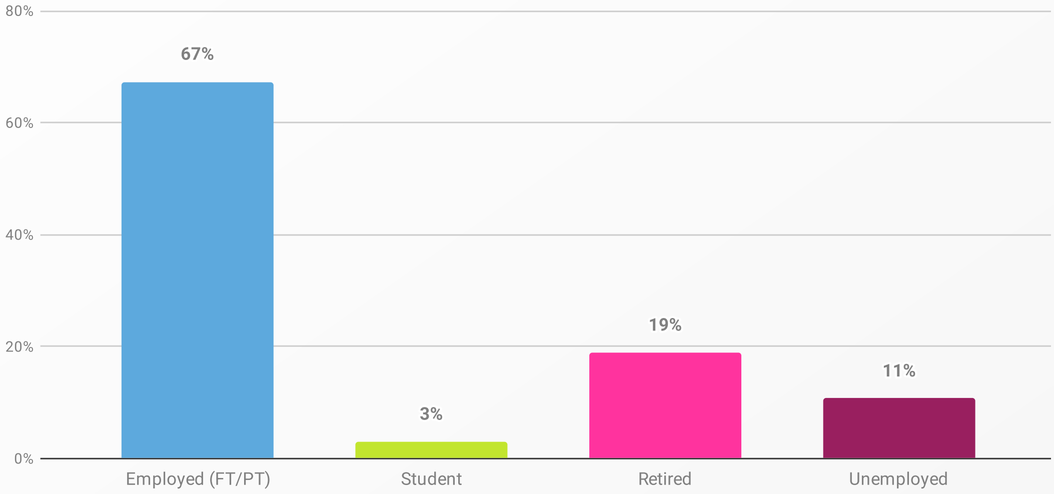


Figure 6. Participants' employment status.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants: 7012 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

1. Our online presence

We live in a hyper-connected world, where half of us have essentially entered The Matrix. 53% of participants say they're permanently plugged in, while another 38 percent go online a few times a day. Only nine percent connect less than once a day, though it has increased by two percent from 2023.

It'll come as no surprise that the younger generations lead the way in online connectivity. An impressive 65% of Gen Z and 64% of Millennials report being always connected (Figure 7). However, more surprising is although the percentage for Millennials remains unchanged, Gen Z's "always on" status has dipped by 4% compared to last year. Have the hardcore digital natives reached screen saturation point?

[10] https://uk.toluna.com
[11] https://www.ncsc.govt.nz/
[12] Participants in New Zealand, who had overlapping age grouping categories, were excluded from the generational analysis. Where generational differences are reported in the Main findings section, these participants are excluded.

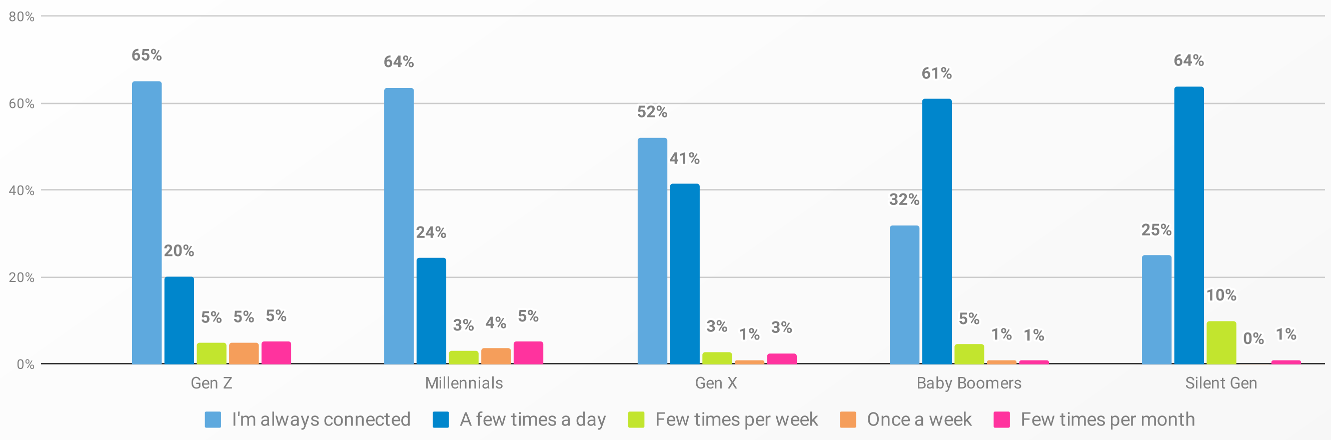


Figure 7. *"How frequently do you use the internet?"* by generation.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants with generation information: 6749 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

We also asked participants about the number of sensitive online accounts they have. Thirty-three percent of them reported having ten or more accounts. Nineteen percent confessed to losing track and being unsure of the exact number (Figure 8). Should this be this alarming, or is it becoming the norm?

There are strong generational trends here. Younger generations are more likely to have multiple online accounts, with 38% of Gen Z and 36% of Millennials reporting holding 10 or more. In contrast, older generations, such as the Silent Generation, have fewer accounts, with only 23% reporting holding 10 or more. Additionally, single account ownership was highest among older generations, with 17% of the Silent Generation and 12% of Baby Boomers having just one account.

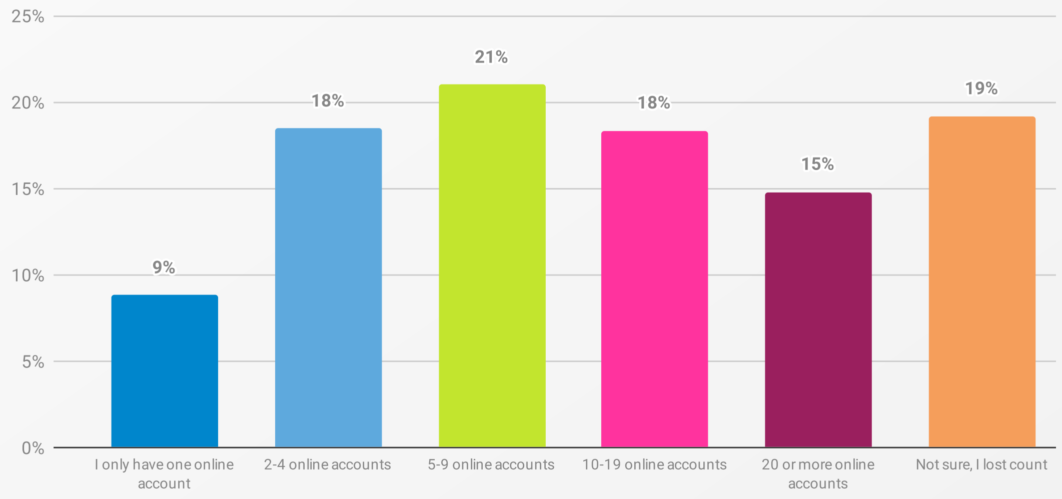


Figure 8. *"Overall, how many sensitive online accounts that hold personal information do you have?"*

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants: 7012 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

2. General attitudes to online security

Why are we so focused on attitudes? Well, to put it bluntly, they matter. A lot.

It's the difference between someone acting safely because they feel it's the right thing to do, and someone acting safely (only) if they're being watched.

Understanding attitudes allows us to design effective interventions. The Knowledge–Attitude–Behaviour (KAB)[13] model suggests people's behaviors are influenced by their knowledge and attitudes. In the context of cybersecurity, one's understanding of threats (knowledge) shapes their beliefs and perceptions (attitudes), which in turn influence their online actions (behavior).

Research[14] has shown that better knowledge of policies and procedures is associated with more positive attitudes towards them. Moreover, better knowledge and attitudes are both linked to self-reported behavior that is more risk-averse.

Participants' feelings towards online safety are generally positive (Figure 9), but there are a few intriguing (and a little worrying) changes compared to last year. While 81% still consider online safety a priority, that's 3% down from last year. Similarly, the percentage of those who believe it's worth the effort has dropped by 9%, now standing at just 60%, and only 53% think staying safe online is possible, a decrease of 5%.

Meanwhile, the frustration factor is on the rise, with the challenges of navigating online security becoming more apparent. 46% of participants reported finding staying safe online frustrating, and 44% finding it intimidating, both representing a 7% rise since 2023.

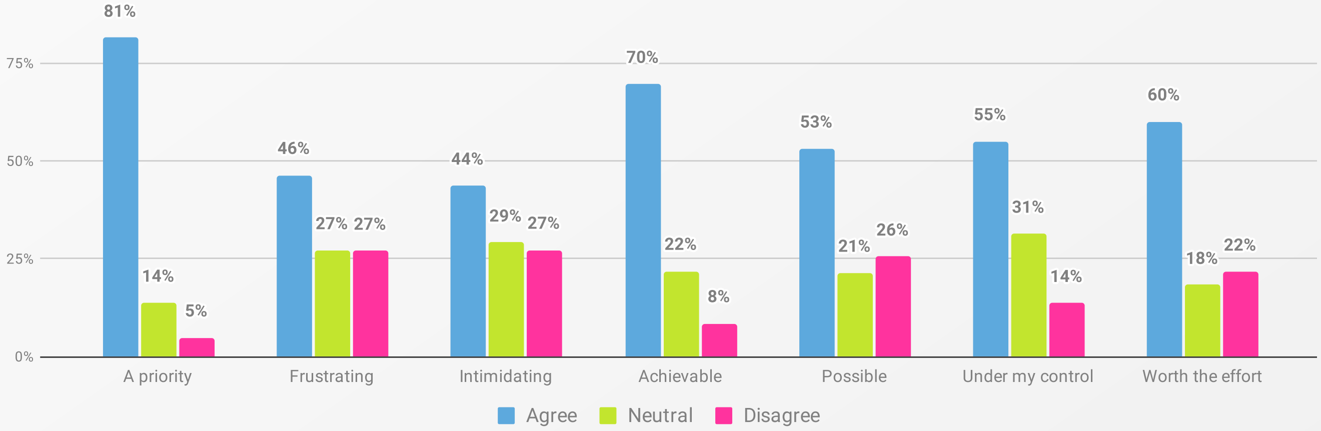


Figure 9. *"I feel that staying secure online is..."*

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants: 7012 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

[13] Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & Security, 25*(4), 289-296.

[14] 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.

Seventy percent of participants find staying safe online achievable, a slight increase from last year. Additionally, 55% feel that online security is under their control, showing a 3% rise.

It seems people's feelings about online security are more mixed up than a six-year-old's sock drawer. The importance and perceived achievability are stacked up against growing frustration and intimidation.

And how about the people feeling both confident and confused? Just over half of participants (54%) found it easy to be secure online (Figure 10), up 4% from 2023. However, 40% felt that information on how to stay secure is confusing, indicating that despite their confidence, clarity is still lacking for many.

This confusion is undoubtedly linked to the security guidance information overload. In fact, the sense of being overwhelmed by online security information led 37% of participants to minimize their online activities. Yet, despite these challenges, 44% reported that they continue to go online regardless of the potential risks and feelings of being overwhelmed.

These findings reveal a nuanced perspective on online security: while many feel capable of staying secure, it can also be daunting. As a result, some limit their online presence, while others continue to engage online despite the associated risks. The internet—can't live with it, can't live without it.

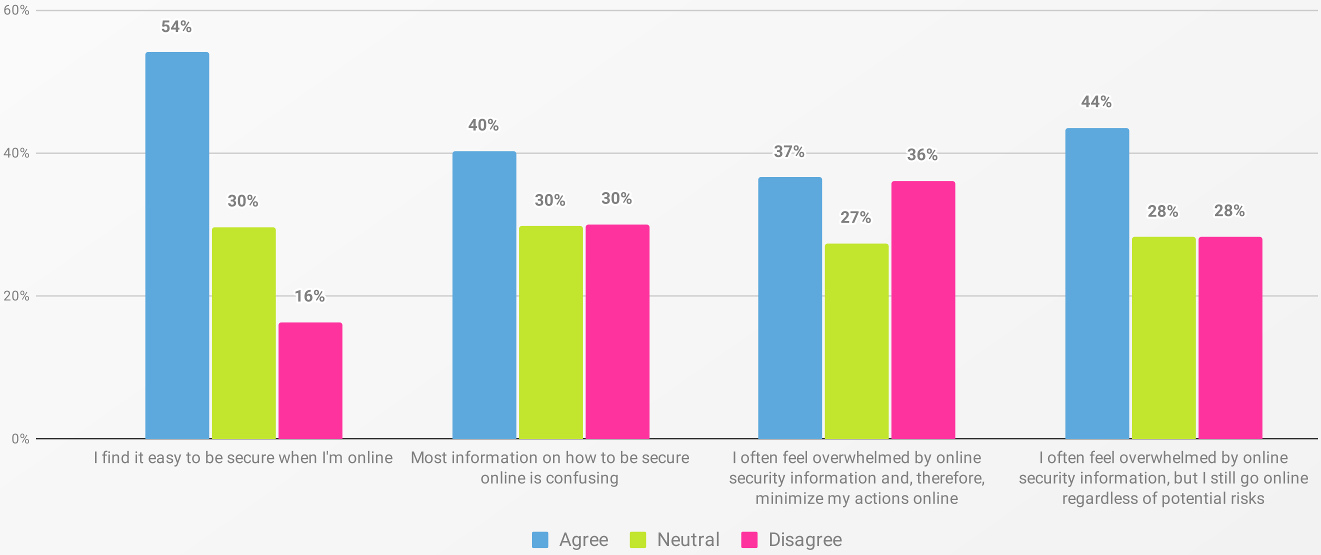


Figure 10. Participants' levels of agreement with online security ease, clarity, and overwhelm.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants: 7012 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

> ***Cost is a barrier, with more than half (52%) finding the cost of comprehensive online protection to be a burden.***

Many participants hold misconceptions and concerns about online security. Forty-three percent presume their devices are automatically secure (Figure 11), meaning they likely underestimate the need for proactive security measures. Additionally, cost is a barrier, with more than half (52%) finding the cost of comprehensive online protection to be a burden.

The mistaken perception that devices are automatically secure is not uncommon in the field of cybersecurity. For example, research[15] has shown people often purchase IoT devices without verifying the presence of adequate security controls, despite expressing concern for their security and privacy.

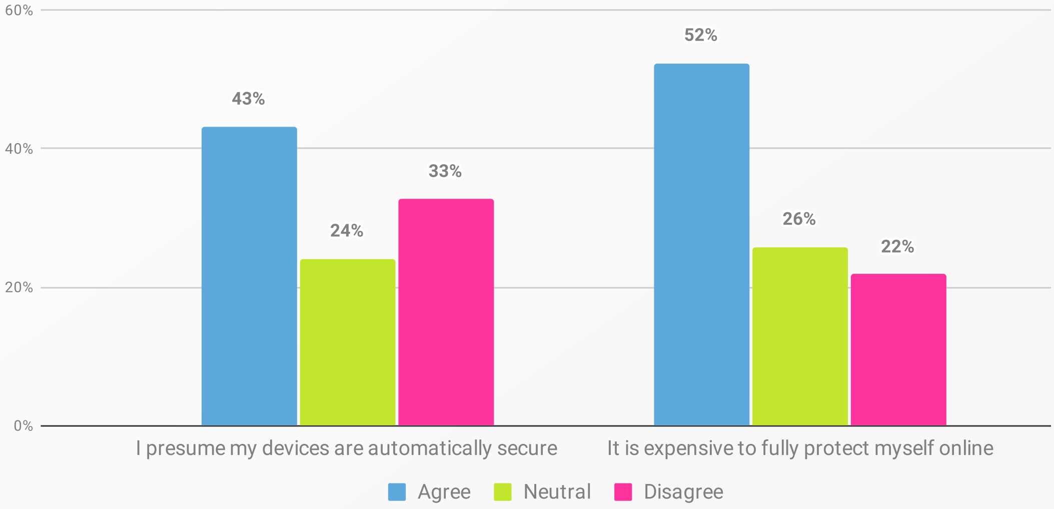


Figure 11. Perceptions of device security and cost of online protection.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants: 7012 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

2.1 Generational differences in attitudes

Age is a big hitter when it comes to shaping cybersecurity attitudes. Brace yourself. This year’s findings reveal intriguing generational differences.

One area with generational cut-through is prioritizing cybersecurity. Participants across all generations generally felt staying secure online is a priority (Figure 12) and worth the effort (Figure 13). But, there’s a twist: The older you are, the more you care. Higher percentages of the Silent Gen (91%) and Baby Boomers (89%) prioritize online security, as opposed to only 68% of Gen Z.

Still, we can’t ignore an ominous overall trend: the percentage of those who agree that online security is a priority has decreased across all generations since 2023.

[15] Williams, M., Nurse, J. R. C., & Creese, S. (2017, August). Privacy is the boring bit: User perceptions and behaviour in the internet-of-things. In *15th Annual Conference on Privacy, Security and Trust* (PST) (pp. 181-189). IEEE.

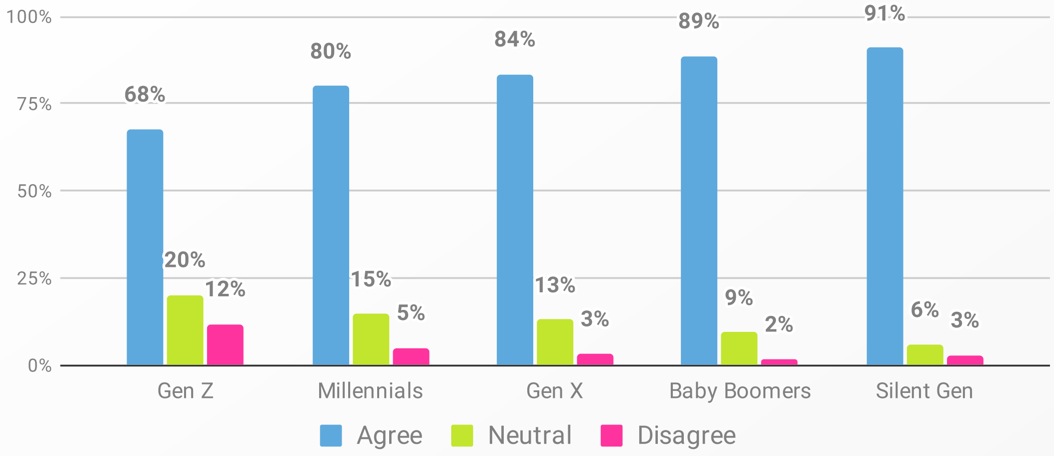


Figure 12. ***"I feel that staying secure online is a priority"*** **by generation.**

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants with generation information: 6749 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

Is staying secure online worth the effort? Depends on who you ask. A substantial proportion of Baby Boomers (79%), Silent Gen (77%), and even Gen X (65%) believed that staying secure online is worthwhile. In contrast, whilst most Gen Z and Millennials believed the same, their views were more divided, with 35% of Gen Z and 33% of Millennials reporting that online security is not worth the effort.

Similarly to the priority question, the numbers of those believing that staying secure online is "worth it" has dropped across all generations since 2023, with a noteworthy 10% dip among Gen Z, Millennials, and Gen X alike.

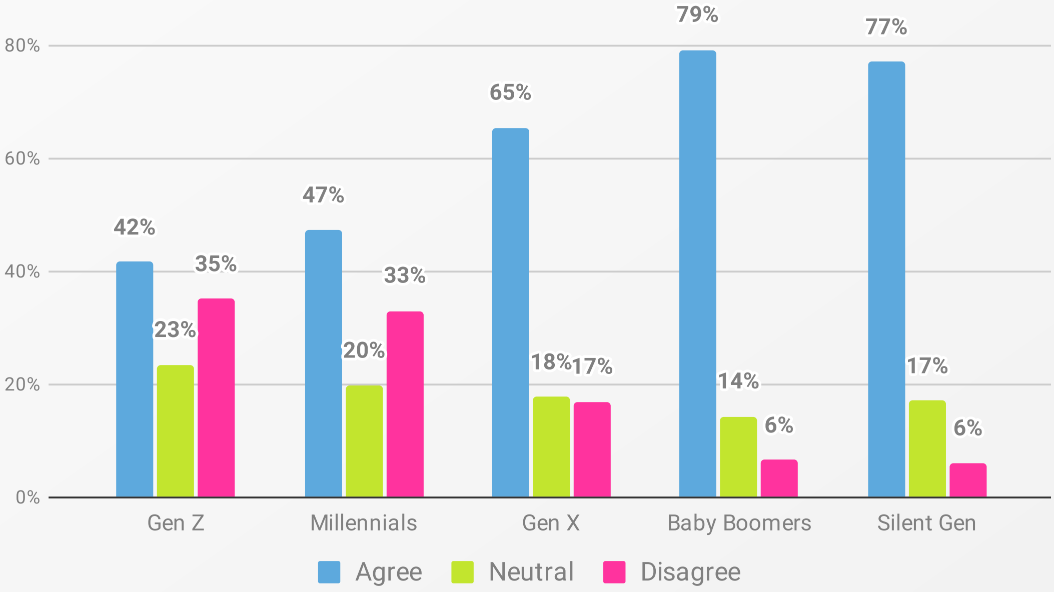


Figure 13. ***"I feel that staying secure online is worth the effort"*** **by generation.**

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants with generation information: 6749 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

Time for a vibe check. Participants across all age groups generally had a positive attitude towards staying secure online, with the majority feeling it is possible (Figure 14) and in their control (Figure 15). Gen Z and Millennials were the least optimistic of the bunch, with only 41% and 45% feeling it's possible to stay secure online.

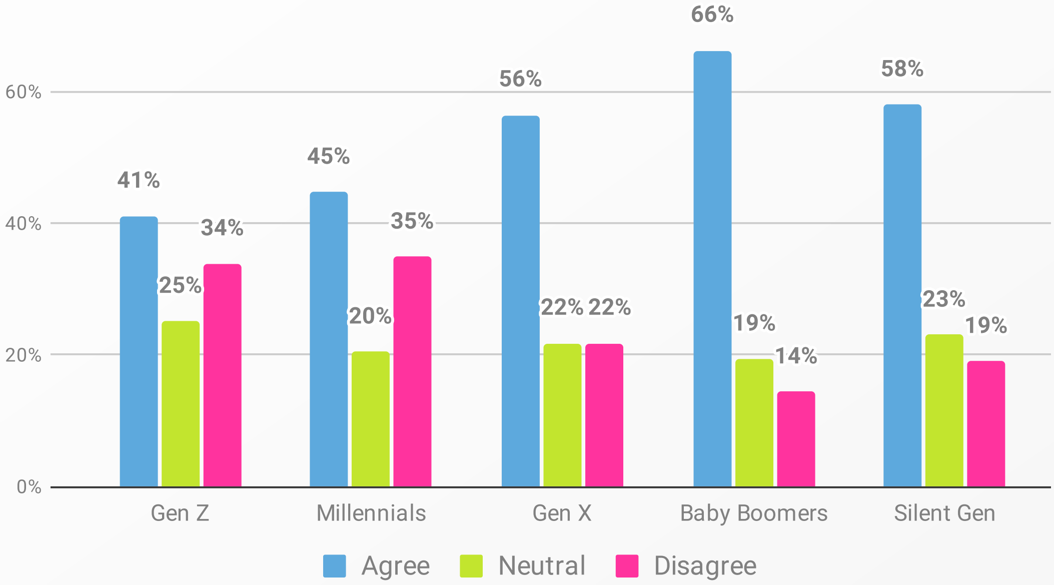


Figure 14. ***"I feel that staying secure online is possible"*** **by generation.**

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants with generation information: 6749 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

In spite of that, the majority of Millennials (60%) still felt online security is under their control, which was least agreed with by the Silent Gen (42%). Interestingly, the perception of personal control has increased in almost all generations since 2023, most notably by 9% for Gen Z and 7% for Millennials. For the Silent Gen, this perception has decreased by 11%. (Maybe their Millennial grandkids have taken away their admin privileges?)

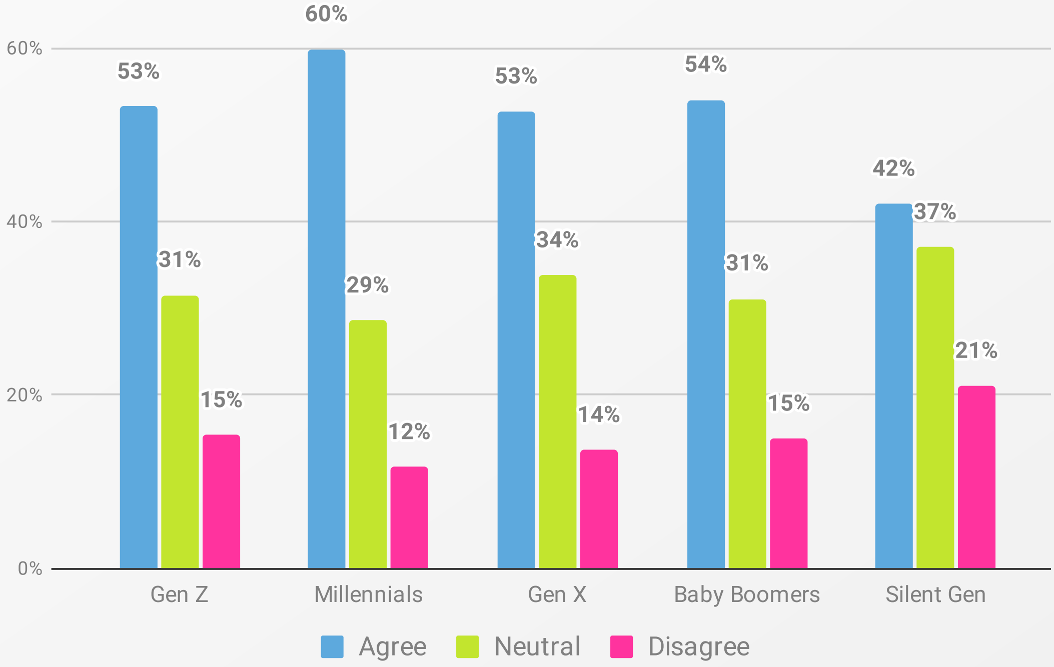


Figure 15. ***"I feel that staying secure online is under my control"*** **by generation.**

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants with generation information: 6749 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

We're united by frustration! We found most participants in all generations found staying secure online frustrating, ranging from 43% of Baby Boomers to 59% of Silent Gen. The majority of participants across all generations also feel it's intimidating (Figure 16). Silent Gen takes the cake, with 59% and 53% respectively. Furthermore, the percentages of those finding online security intimidating have increased across all generations since 2023, with the biggest jumps in Gen Z (12%) and the Silent Gen (10%).

Interestingly, Baby Boomers were most balanced in their answers, similar to last year, topping the chart with a sizable 30% who did not find online security intimidating. That said, this still represents a 6% decrease from 2023.

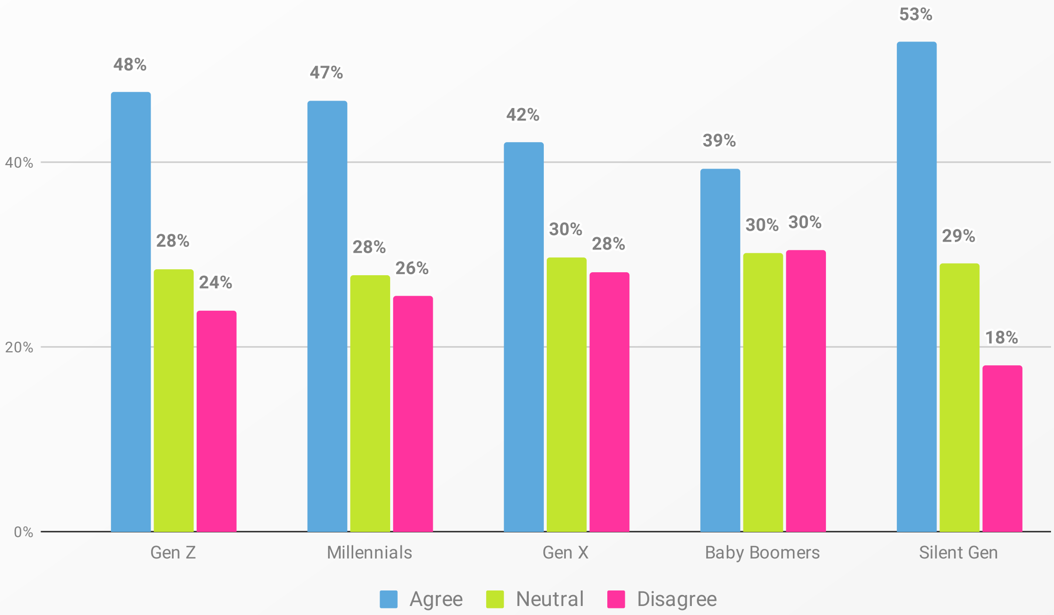


Figure 16. *"I feel that staying secure online is intimidating"* by generation.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants with generation information: 6749 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

Who's most likely to stay offline as much as possible because of overwhelm? It might not be who you think...

Younger generations are slightly more impacted—42% of Millennials and 41% of Gen Z reported minimizing their actions online because of overwhelming online information, compared to 30% of Baby Boomers (Figure 17). Furthermore, the only two generations where the majority disagreed that their online actions were minimized as a result of information overwhelm were Gen X (38%) and Baby Boomers (41%).

> ***Younger generations are more likely to minimize their online actions due to feeling overwhelmed.***

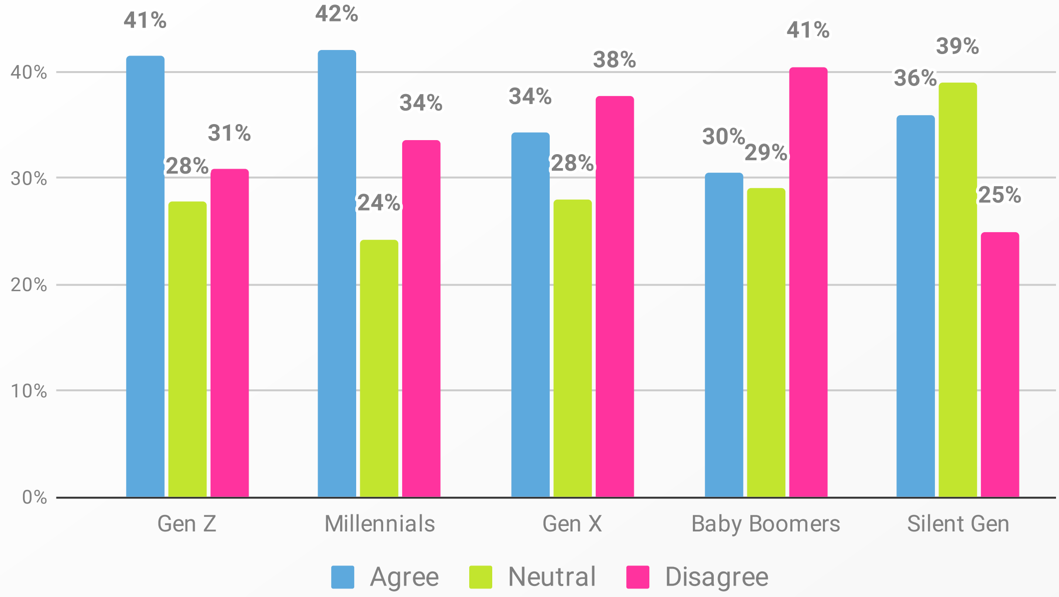


Figure 17. *"I often feel overwhelmed by online security information and, therefore, I minimize my actions online."* by generation.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants with generation information: 6749 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

On the other hand, it was also the majority of Gen Z and Millennials (both 50%) who reported going online regardless of the potential risks, in comparison to 35% of Baby Boomers (Figure 18).

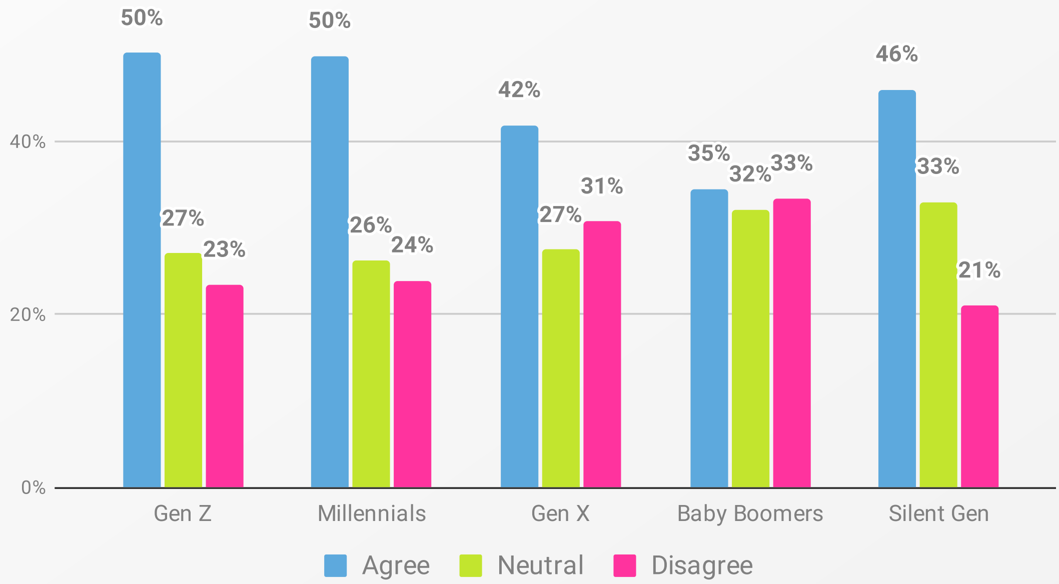


Figure 18. *"I often feel overwhelmed by online security information, but I still go online regardless of potential risks."* by generation.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants with generation information: 6749 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

What's the takeaway here? One key message is that younger generations are more likely to minimize their online actions due to feeling overwhelmed, yet they also tend to take risks and go online regardless of potential threats. Meanwhile, older generations tend to prioritize security, but feel less in control.

2.2 Media impact on attitudes & behaviors

The media's influence on attitudes towards online security is a mixed bag. On the bright side, 59% of participants reported media coverage motivated them to take protective online security actions, a 3% increase from 2023 (Figure 19). Plus, over half of the respondents (54%, +3% from 2023) acknowledged media and news sources play a crucial role in keeping them informed about online security matters.

However, there is also apprehension, with 44% left feeling scared about their online security due to media coverage. Additionally, 47% reported media portrayal of online security makes it seem complicated, 5% up from 2023. These findings highlight the need for balance. Media plays a role in raising awareness, but it needs to do this without stirring up undue panic and confusion.

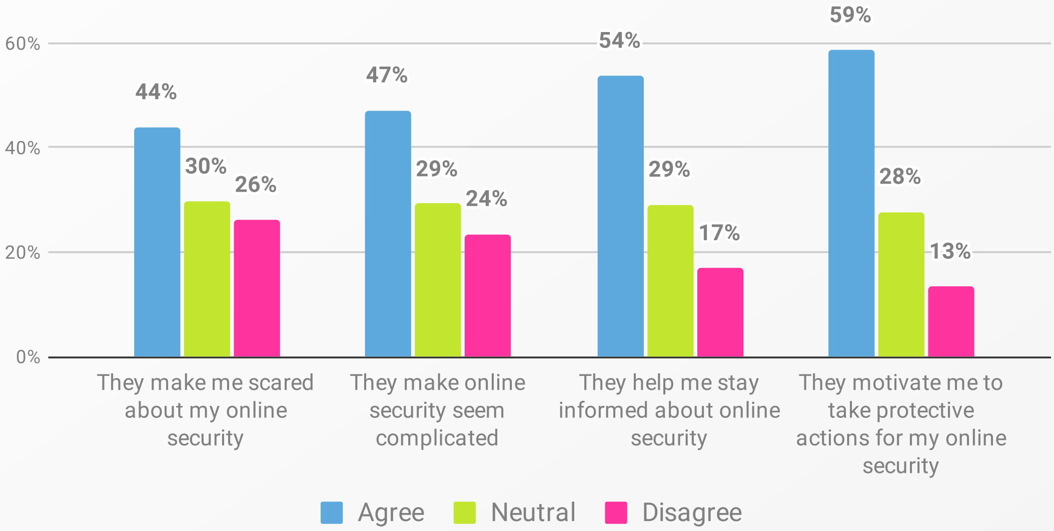


Figure 19. *"What impact does the media/news have on your views towards online security?"*

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants: 7012 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

Let's talk about motivation next. The Silent Gen is the most receptive age bracket, reporting the highest impact of media coverage on motivating their protective online security actions at 64% (Figure 20), no major change since 2003 (+1%). However, for all other generations, the impact has increased notably since 2023, with Gen Z showing the largest rise at 11%.

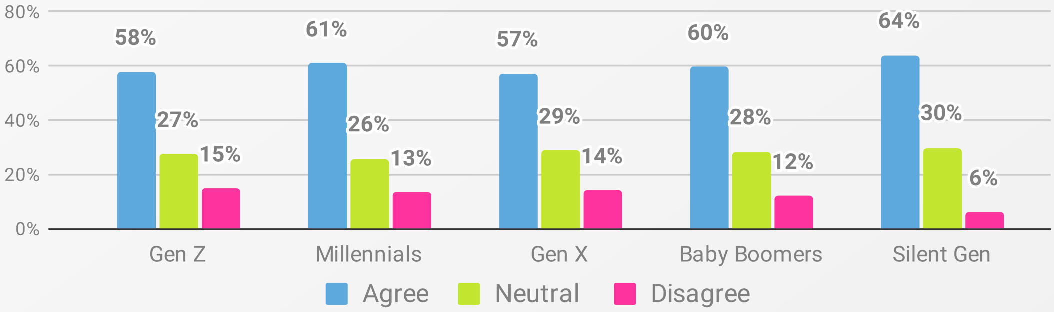


Figure 20. Impact of media coverage on motivating protective online security actions, by generation.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants with generation information: 6749 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

So, for those participants who said they were influenced by the media (5,109 to be exact), what kinds of actions had they been motivated to take (Figure 21)?

Over half of them (56%) began being more cautious about online content as it may be fake or maliciously generated using artificial intelligence (AI). Additionally, 54% started using MFA, and an equal percentage adopted strong and separate passwords, all as a result of media influence.

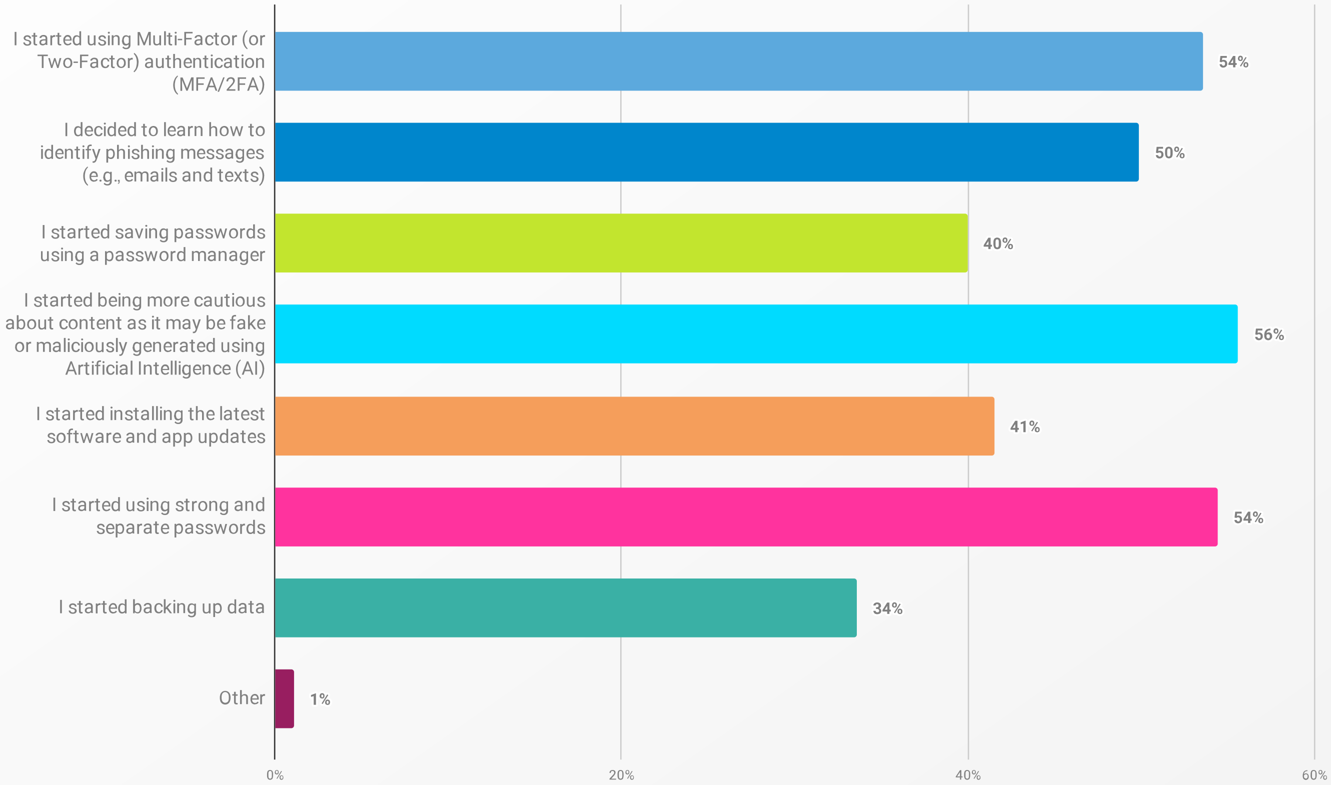


Figure 21. Impact of media on online security actions.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants: 5109 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

Drawing from qualitative responses, we found participants invested in various cybersecurity measures like VPNs and antivirus software. Interestingly, an increased sense of vigilance and awareness towards potential scams and breaches were common themes in the media's impact on protective actions.

What's apparent from the responses is our relationship with the media is complicated, influencing people in helpful and unhelpful ways. Though there's no denying the media holds a lot of power, and can be a potent tool in furthering security awareness and confidence.

> **I remain vigilant - if it's too good to be true, it probably is.** P433, New Zealand

3. Reliance on others for cybersecurity

Lean on somebody, or go lone wolf? We had to know who (if anyone) people turn to for online security support.

Survey says: it's complicated. Plenty (46%) of participants reported relying on no one to keep them secure online, but this represents a 10% decrease from 2023. Similarly to last year, generations the least reliant on others' help appeared to be the Baby Boomers (57%), and Gen X (49%), however, these proportions have decreased by 8% and 11%, respectively (Figure 22).

The findings indicate that reliance on others for cybersecurity has increased across all generations since 2023, with the biggest shift being among younger generations: a 12% increase in Gen Z (38%), and a 10% increase in Millennials (41%).

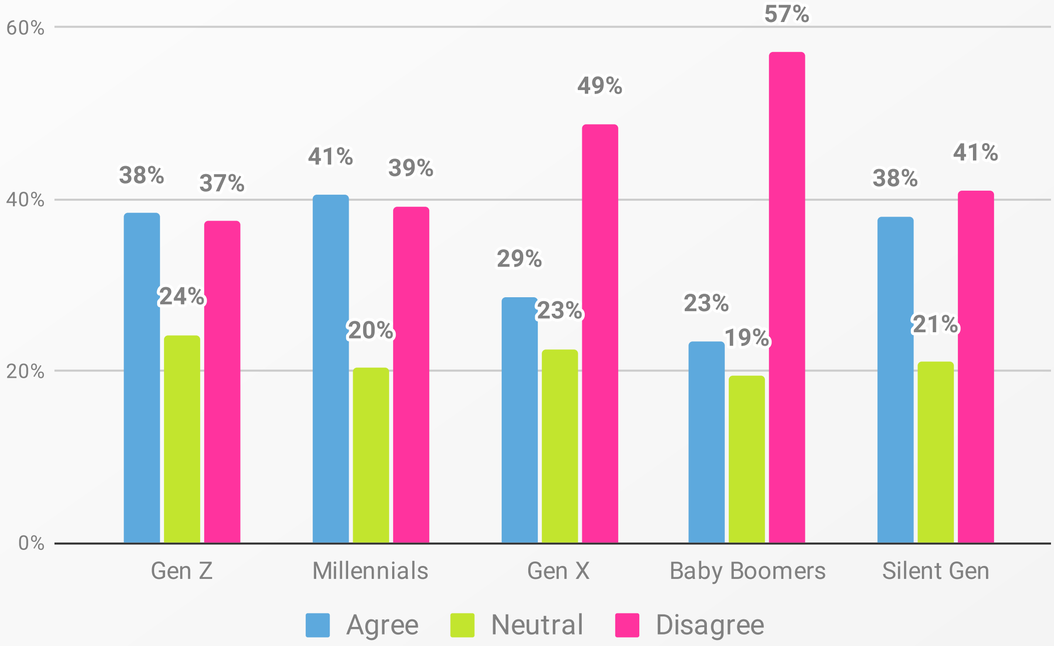


Figure 22. *"I rely on others (e.g., my family, my colleagues) to keep me secure online."* by generation.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants with generation information: 6749 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

We didn't stop at a self-reliance roll-call. We followed up by asking those who reported relying on others (32%, N=2887), about who they specifically relied on. Forty-four percent mentioned relying on their family, and a further 23% depend on IT companies.

> ***Dependence [for help] has notably increased across all security behaviors.***

Still not content, we asked next about which security behaviors people sought help for. The eye-opening result is that dependence has notably increased across all security behaviors we asked them about when compared to last year. Specifically, 70% rely on others for advice and information on staying secure online, up 9% since last year. Similarly, 67% (+7% from 2023) depend on others for checking, updating, or installing the latest software, and again 67% (+8% from 2023) rely on others for backing up data.

In addition, people often seek help with spotting scams (65%), managing security settings (64%), password recovery (63%), and managing online accounts (61%).

We also asked people about being a security support to others. A chunky 39% reported family members relied on them for help—an increase of 5% since 2023. Millennials (53%) reported the highest level of reliance from family members, followed by Gen Z (48%), showing 7% and 9% increases from last year, respectively (Figure 23). On the other hand, only 22% of Baby Boomers and 16% of Silent Gen reported that their family members rely on them for online security.

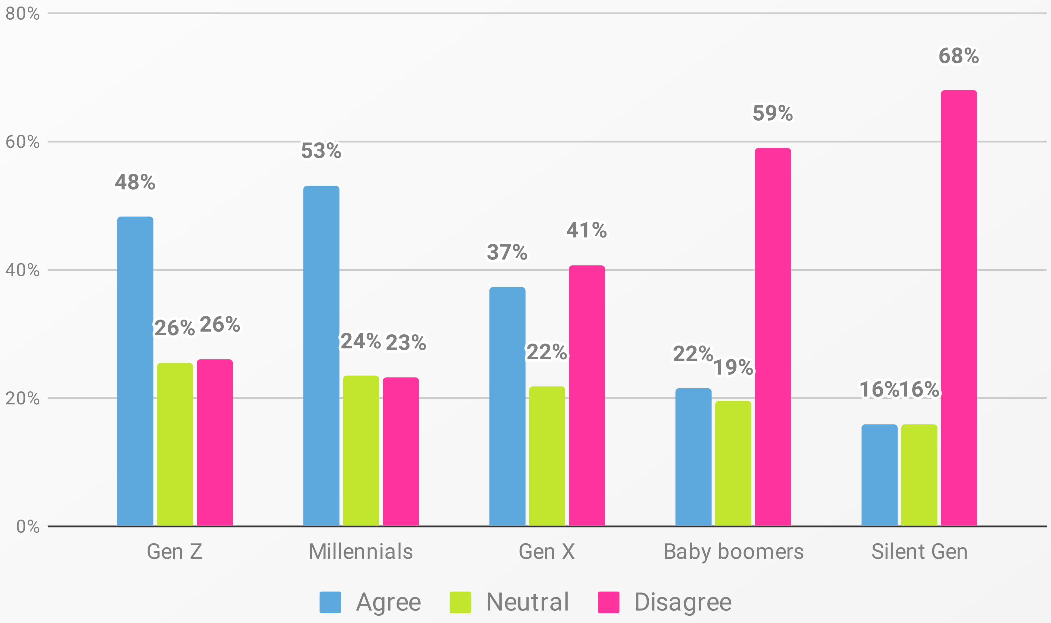


Figure 23. *"Family members rely on me to keep them secure online"* by generation.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants with generation information: 6749 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

In conclusion, while self-reliance is still a thing, people are increasingly turning to others for security support. This is especially true of younger generations–specifically, Millennials–who are also the most relied upon by their family members. As tech gets more complex, is collaboration set to become the new normal?

4. Responsibility for cybersecurity

There's an important distinction between reliance and responsibility, and we wanted to explore both.

We asked people about the responsibility for protecting their personal information online. While 59% of participants identified themselves as the most responsible party (Figure 24), this represents a 7% decrease from last year's survey, reverting to 2022 levels.

> ***People expect security as standard. Apps and platforms were deemed the most accountable by 90% of respondents.***

Beyond personal responsibility, who else do people consider accountable? Consistent with last year, a modest 41% attributed the highest responsibility to the app or platform they use. However, when considering both 'most responsible' and 'somewhat responsible' categories, apps and platforms were deemed the most accountable by 90% of respondents.

We see this as an important finding, suggesting people expect security as standard. They are unlikely to pay extra for it.

Which other parties are seen as responsible for cybersecurity? This year, 23% of participants attributed responsibility to the government, a 7% increase from last year. The tech industry's perceived responsibility also rose to 21%.

Family members (59%) and employers (55%), were viewed as the least responsible for protecting participants' personal online information. Though that's not to say employers can take their foot off the gas.

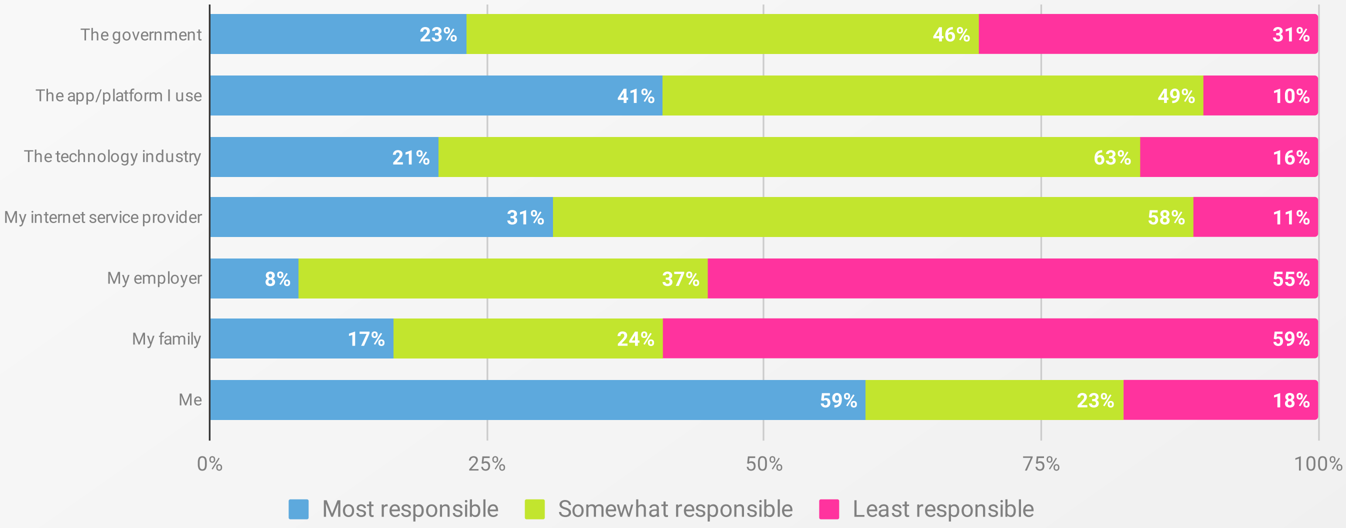


Figure 24. *"Who is most responsible for protecting your online information?"*

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants: 7012 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

Let's now shift the focus away from personal information, to workplace information (Figure 25). The employer remains the most responsible party, as in 2023—specifically, the organization's IT department (44%) and security department (42%), though it's worth noting both percentages have decreased by 4%. On the other hand, there's a growing recognition of the tech industry's potential role, with perceived responsibility rising slightly from 21% to 25%.

Once again, the government was seen as the least responsible agency, with 51% attributing responsibility to it, down from 59% in 2023. And interestingly, personal responsibility also saw a slight decline this year, dropping from 39% to 36%. Again, this seems to hint at the mindshift from security being a one-person show.

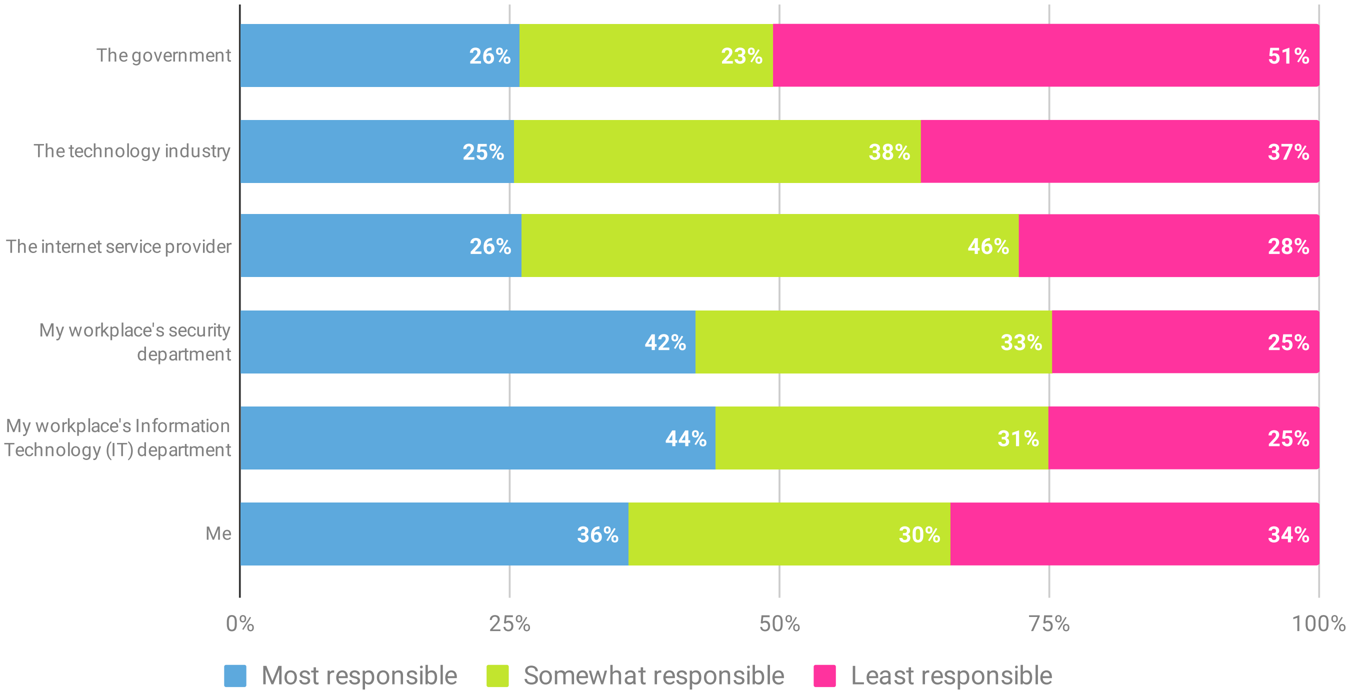


Figure 25. *"Who is most responsible for protecting your workplace's information?"*

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants: 7012 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

These findings suggest people's thoughts on who's responsible for online security are evolving. Employers' tech departments remain central, but there's increasing recognition of shared responsibility across individuals, tech companies, and government agencies.

Lastly, we can't ignore that slight drop in personal responsibility. Could it be that individuals are feeling less empowered or capable of managing workplace security on their own? More evidence (if it were even needed) to retire the tripe phrase, "Security is everyone's responsibility". Vom.

5. Cybercrime victimization & reporting

It’s time to unpack how people feel about the possibility—and reality—of becoming victims of cyber attacks. We’ll be shining a light on who’s experienced phishing scams, identity theft, and online dating scams.

We’ll also be reporting on the unreported: we’ll dive into why cybercrime is often underreported, and explore what the data suggest about why that might be. And, vitally, we’ll take a look at cyberbullying, because while it might not involve theft of data or money, the fallout can be beyond brutal.

5.1 Attitudes towards victimization

Let’s start with exploring participants’ attitudes towards being cybercrime victims. Sixty-one percent felt worried about becoming a victim of cybercrime, a 3% increase from 2023 (Figure 26).

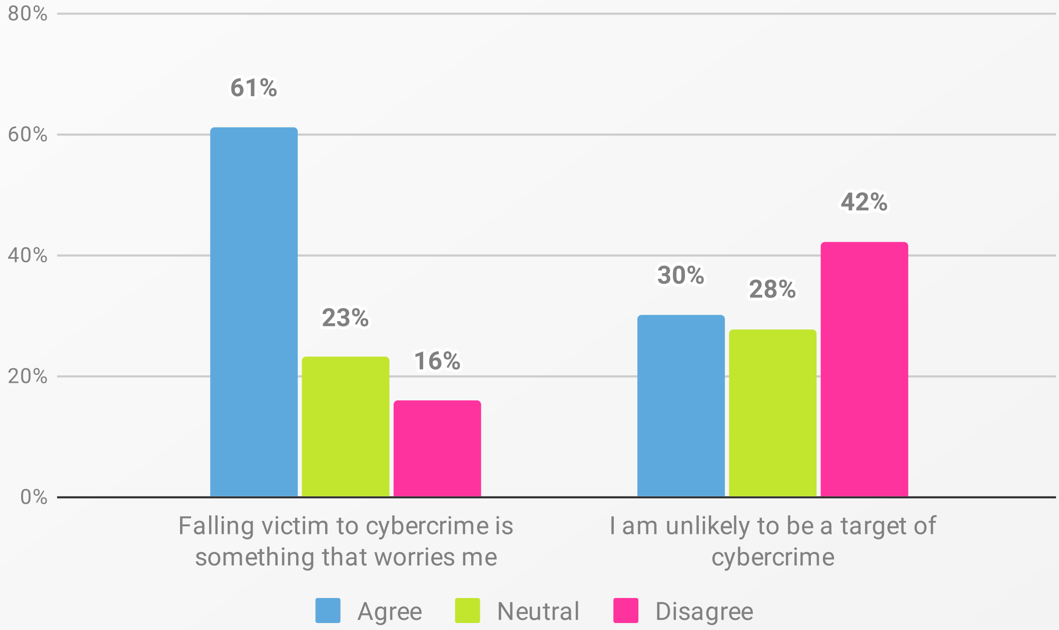


Figure 26. Attitudes towards victimization.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants: 7012 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

This concern was most pronounced from participants in the Silent Generation, with a whopping 70% expressing worry (Figure 27). In contrast, Gen Z seems the least fazed, with 1 in 5 (20%) reporting that falling victim to cybercrime is not a worry for them.

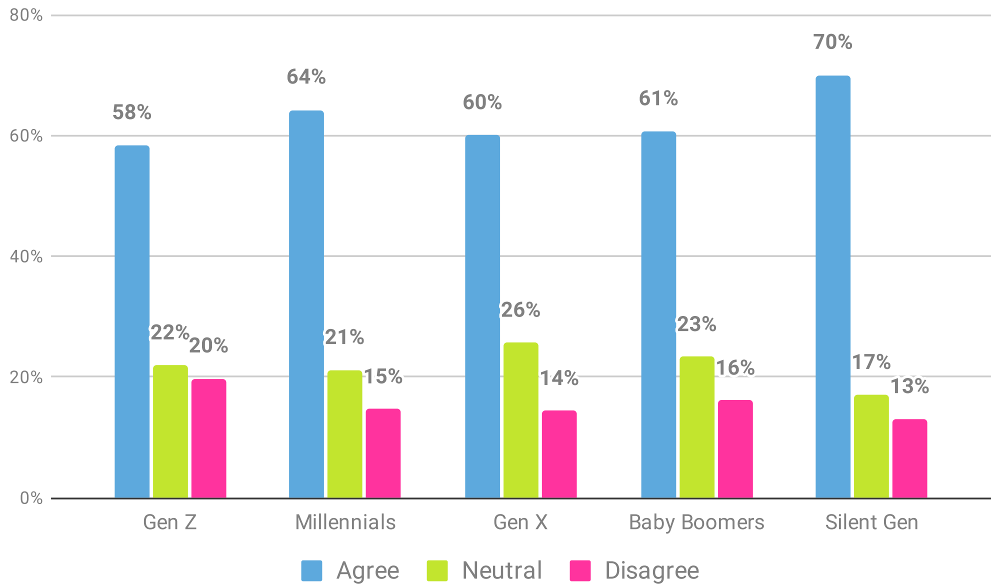


Figure 27. *"Falling victim to cybercrime is something that worries me."* by generation.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants with generation information: 6749 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

In spite of the high percentage of worry about becoming a cybercrime victim, "only" 42% felt they were likely to be targeted (Figure 26), an 8% drop from 2023. In last year's report, the 50% who felt they're likely cybercrime targets represented a 7% increase from 2022. It's also worth noting the percentage of those who don't think of themselves as potential cybercrime targets has increased to 30% (from 22% in 2023).

Older generations felt more likely to be in cybercrime's crosshairs (Figure 28), with 63% of Silent Gen and 56% of Baby Boomers considering themselves likely targets. Meanwhile, the largest proportions of Gen Z (44%) and Millennials (40%) felt they were unlikely targets.

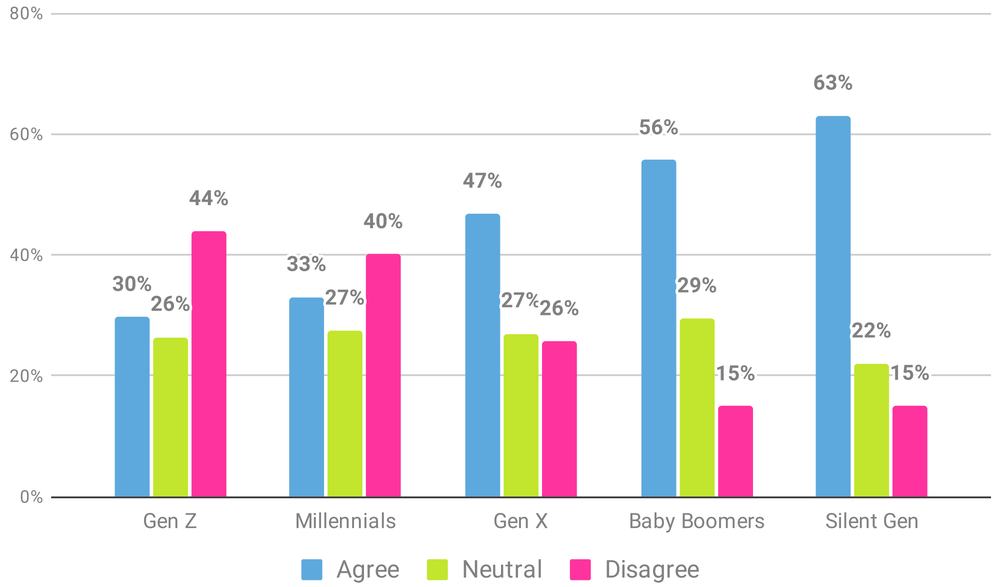


Figure 28. *"I am likely to be a target of cybercrime."* by generation.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants with generation information: 6749 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

Around half of the participants believe losing money on the internet is avoidable (Figure 29), a percentage that has dropped by 5% since 2023. Unsurprisingly, the percentage of those feeling that having personal details stolen is unavoidable also increased by 5% from 2023, reaching 38% this year. However, an almost equal percentage (37%) felt that they could dodge the data-theft bullet.

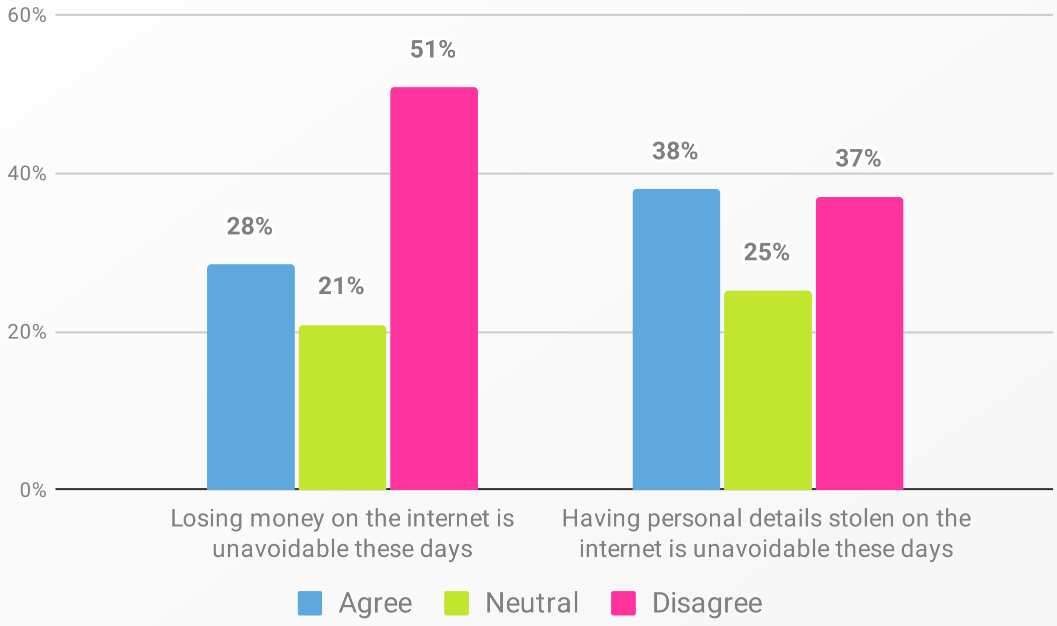


Figure 29. Perceptions on the avoidability of losing money or personal details on the internet.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants: 7012 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

The least optimistic generations were Gen Z and Millenials, where 41% of each generation felt losing money on the internet was unavoidable (Figure 30). However, Millennials represent the most balanced, with 39% believing the losing money is avoidable. Older generations—68% of Baby Boomers, 64% of Silent Gen, and 55% of Gen X—believe losing money on the internet can be avoided.

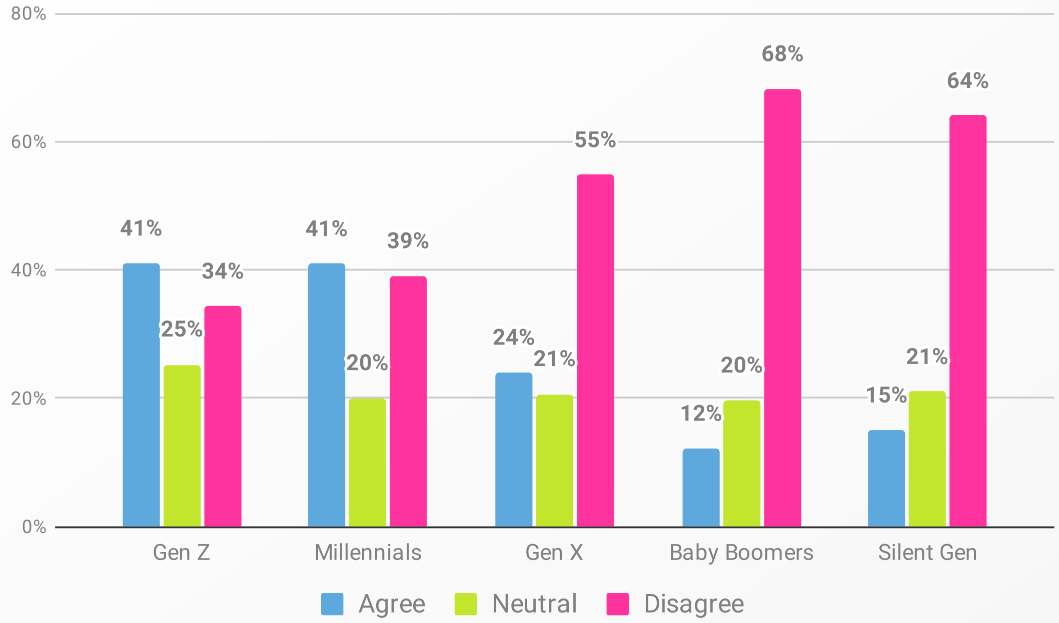


Figure 30. *"Losing money on the internet is unavoidable these days."* by generation.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants with generation information: 6749 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

It's a similar story for personal data theft. Again, Gen Z (51%) and Millennials (49%) were the most pessimistic, believing having data stolen is out of their control (Figure 31). The majority of Baby Boomers (49%), Gen X (43%), and Silent Gen (39%) felt they could play a part in keeping their data safe.

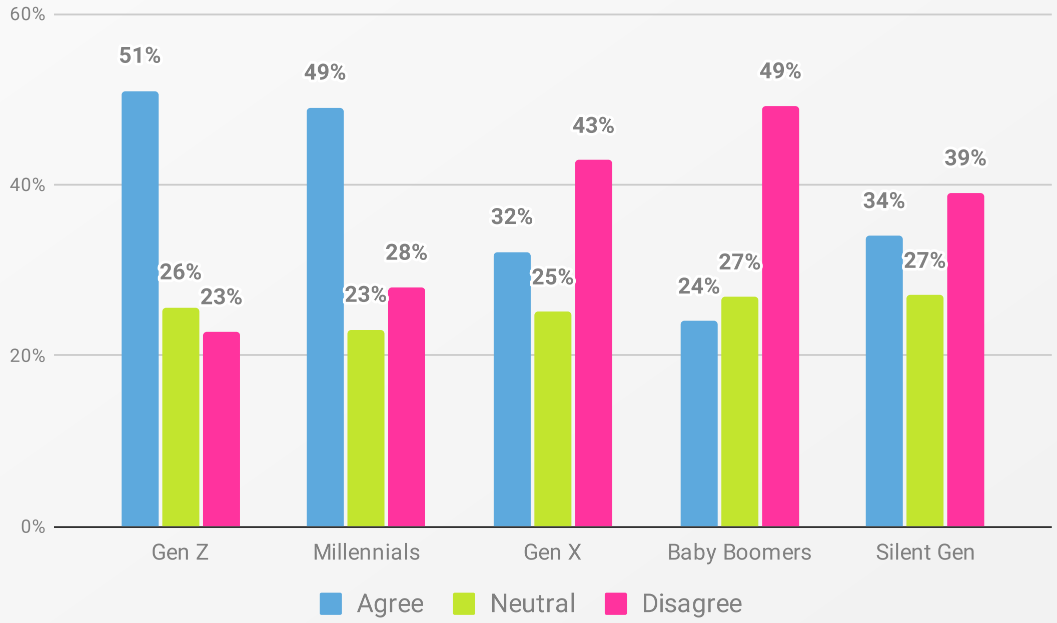


Figure 31. *"Having personal details stolen on the internet is unavoidable these days."* by generation.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants with generation information: 6749 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

Get this: Many people know that no one is an island when it comes to online safety. Over half (55%, a 3% increase from 2023) of all participants agreed that staying secure online helps to protect others from cyber attacks (Figure 32). But on a less positive note, 30% expressed there is no point in protecting themselves as their information is already online. That's up +8% from 2023, indicating a growing sense of helplessness.

> ***30% expressed there is no point in protecting themselves as their information is already online.***

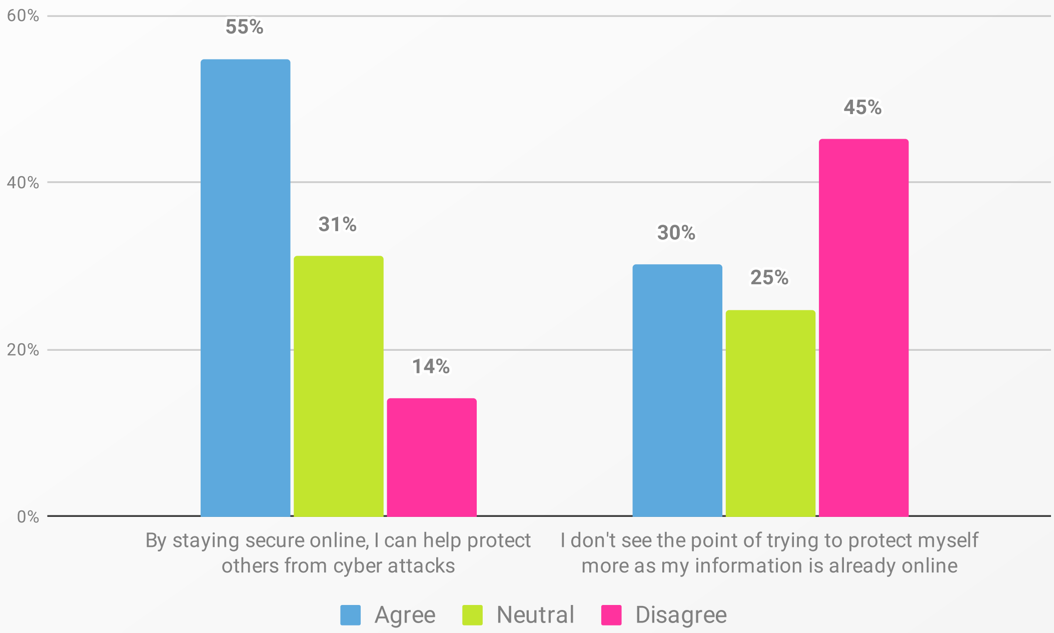


Figure 32. Perceptions of personal and collective online security.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants: 7012 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

This growing sense of helplessness was particularly evident among Gen Z and Millennials, as they were, yet again, the only two generations where the majority (40%) believed there is no point in trying to protect themselves further, as their information is already online (Figure 33). Older generations had more positive attitudes—for example, 56% of Baby Boomers disagree with the statement.

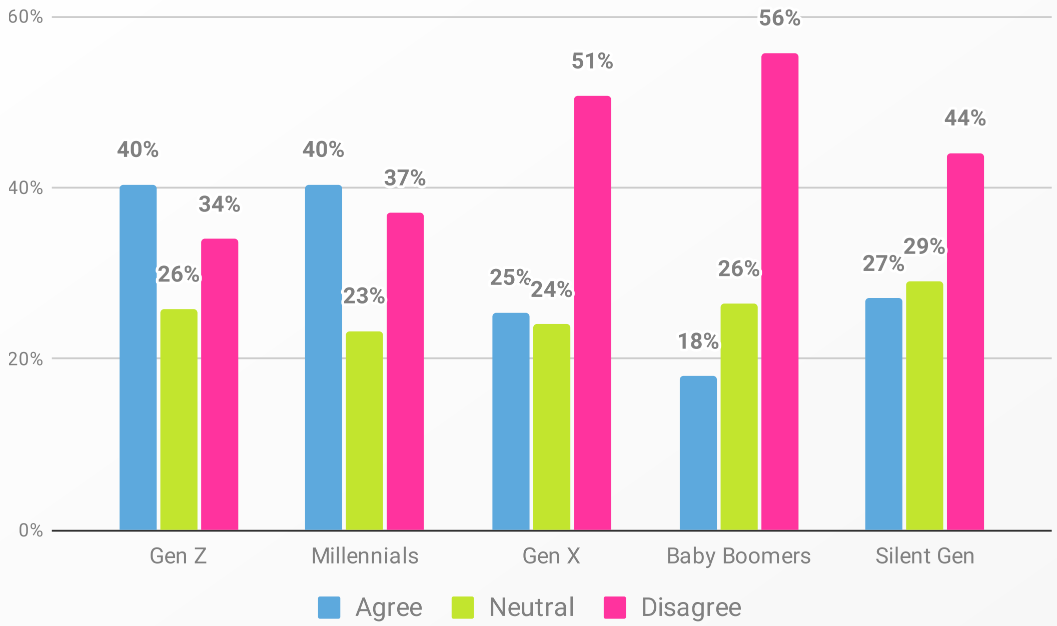


Figure 33. *"I don't see the point of trying to protect myself more as my information is already online."* by generation.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants with generation information: 6749 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

These findings reveal a complex picture of attitudes towards cybercrime victimization, especially across different generations. While there is a general worry about becoming victims of cybercrime, fewer participants feel they are likely targets compared to last year. This suggests a mix of increasing awareness and a potential underestimation of personal risk.

There appears to be a generational divide when it comes to how avoidable falling foul of cybercrime is. Younger generations hold more pessimistic views, with a sense of helplessness that's further compounded by their belief that personal information is already compromised, despite acknowledging online security's importance for protecting others. Yet, on top of all of this, they also tend to think of themselves as unlikely targets.

5.2 Cybercrime prevalence

Next, let's turn from the attitudes around cybercrime to the actualities. Participants disclosed 3,346 cybercrime incidents[16] resulting in money or data loss. This marks a colossal increase of 1,299 from 2023. Overall, 35% of the participants had been victims of cybercrime, including phishing, online dating scams, and identity theft. This represents an 8% increase from 2023, following a 7% drop the previous year.

What form of crime was the most common culprit? Phishing scams. Out of the 2,425 victims of cybercrime, the majority experienced phishing crimes (60%), similar to last year.

[16] This survey measured three specific types of cybercrime incidents: phishing scams, identity theft, and online dating scams.

What form of crime was the most common culprit? Phishing scams.

Phishing incidents accounted for the highest proportion of total incidents (44%, Figure 34), though actually this is down from 2023's figures. Identity theft (25%) is also down from last year, but online dating scams became more prevalent, accounting for 31% of total incidents, up 4% from last year. Who said romance is dead?

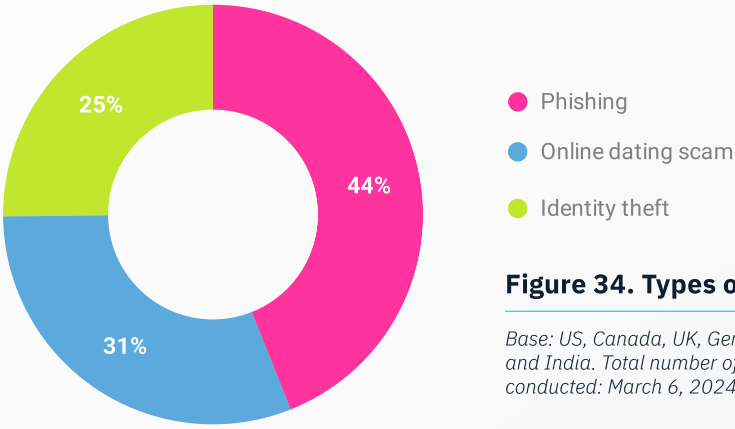


Figure 34. Types of cybercrime incidents.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of cybercrime incidents: 3346. Dates conducted: March 6, 2024 - April 22, 2024.

Generationally, the youngsters appear to be most victimized (Figure 35). Fifty-two percent of Gen Z reported having lost money or data due to online scams, followed by 46% of Millennials, representing 9% and 10% increases from last year, respectively. Baby Boomers and the Silent Gen reported the lowest numbers of victimization, both at 16% (+1% and -4% from 2023, respectively).

Interestingly, this finding aligns with research[17] from a decade ago, which showed individuals aged 18 to 35 were more susceptible to phishing than other age groups.

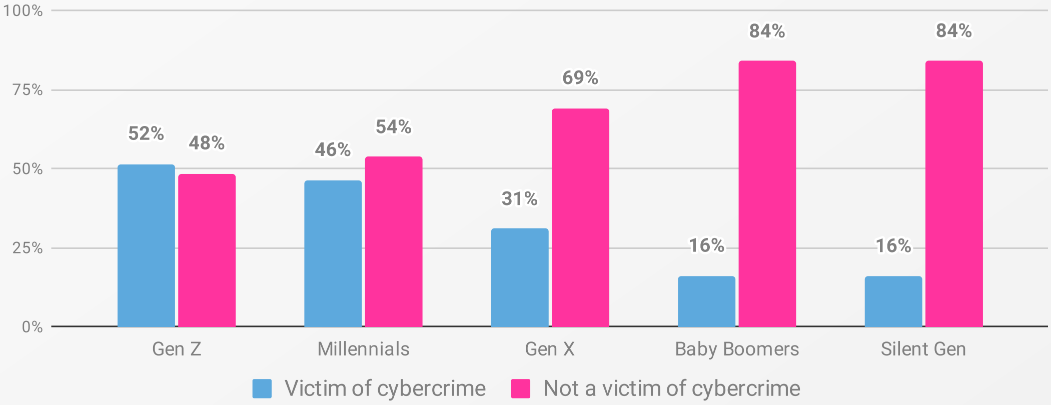


Figure 35. Victimization by generation.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants with generation information: 6749 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

[17] Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010, April). Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 373-382).

Just as in last year's report, Millennials were most likely to be victimized across all three types of crimes that led to a loss of money or data (Figure 36). If we break that down by crime type, we see 47% (+3% from 2023) of victims of online dating scams were Millennials, compared to 20% of Gen X and 6% of Baby Boomers. Millennials also accounted for the majority of identity theft (42%) and phishing (41%) crimes, both representing a five percent increase from 2023.

> ***Millennials were most likely to be victimized across all three types of crimes that led to a loss of money or data.***

While the second highest rates of online dating scams were reported by Gen Z (27%), the second highest proportions of phishing and identity theft crimes were actually reported by Gen X, with 25% and 28%, respectively.

All three types of cybercrimes were lowest among the Silent Gen (1%, 0%, 1%) and Baby Boomers (11%, 6%, 11%), with a decrease from 2023 for Baby Boomers in phishing incidents (-8%), online dating scams (-1%), and identity theft (-6%).

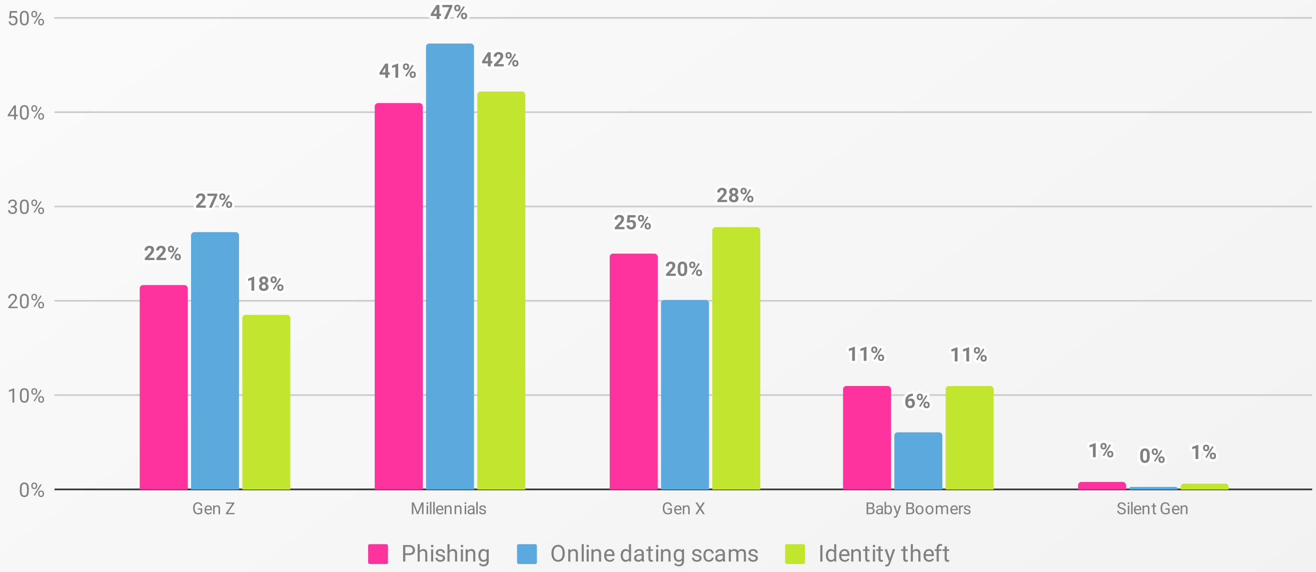


Figure 36. Cybercrime incidents by generation.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of cybercrime victims (age 18+): Phishing = 1407; Online dating scam = 1010; Identity theft = 841 (excluding any cybercrime incidents noted by 263 participants from New Zealand, who didn't provide their age). Dates conducted: March 6, 2024 - April 22, 2024.

Next we asked people to look ahead. Did participants feel they would be a victim of cybercrime in the next year? There was an even divide here, with 37% of participants feeling it was unlikely, and 28% feeling it was likely.

Once again there seemed to be a generational trend, with younger generations feeling more at risk (Figure 37). Specifically, the majority of Gen Z (38%) and Millennials (37%) saw themselves as likely victims in the next year, compared to only 14% of Baby Boomers. The Silent Gen seemed to have the most neutral (48%) view on the matter, followed by Baby Boomers (45%) and Gen X (39%).

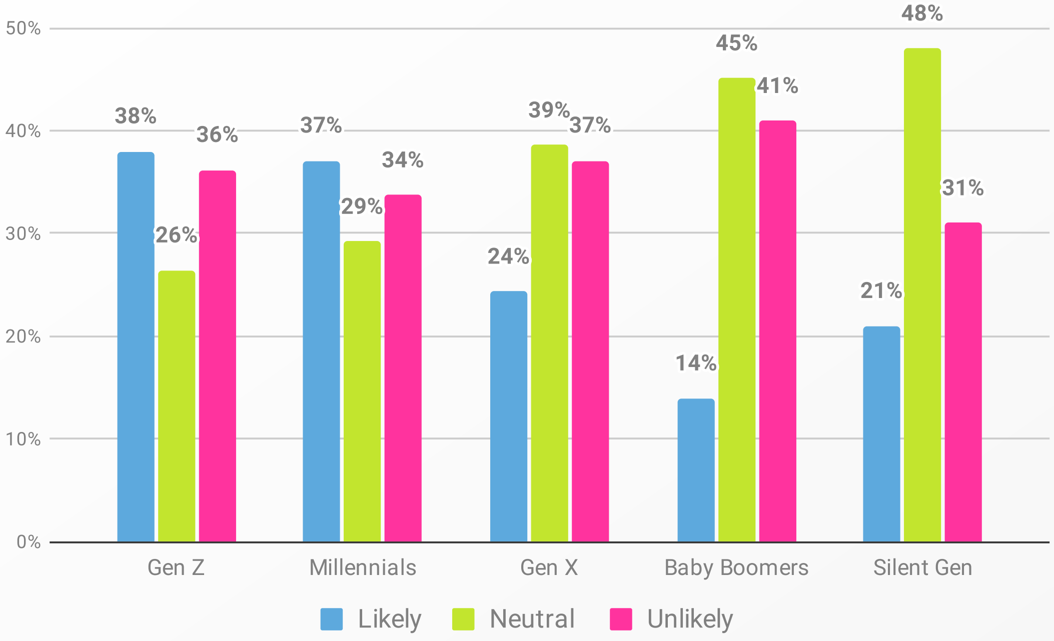


Figure 37. *"In the next year, how likely do you feel that you will become a victim of cybercrime?"* by generation.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants with generation information: 6749 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

Overall, the younger generations, particularly Millennials, and Gen Z, are experiencing the highest rates of victimization. This is likely linked to their higher online engagement—but at least they're not in denial about being targeted. Interestingly, though, they recognize their vulnerability, as they're more likely to see themselves as potential future victims compared to older generations. Self-awareness for the win!

Though scary, risk perceptions play a crucial role in cybersecurity. For instance, a study found that employees who do not perceive their organization as being at risk of a cyberattack are more likely to be complacent about information security measures.[18]

[18] Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly, 34*(3), 523-548.

5.3 Cybercrime reporting

Of course, experiencing cybercrime and reporting it are not one and the same. So, how did report rates stack up for our participants?

Good news! Overall, reporting rates were high across crime types, with 91% (+3% from 2023) of cybercrime incidents being reported by victims. On average, 89% (+3% from 2023) of phishing incidents, 92% (+8% from 2023) of online dating scams, and 92% (same as in 2023) of identity theft incidents were reported (Figure 38). We love to see it.

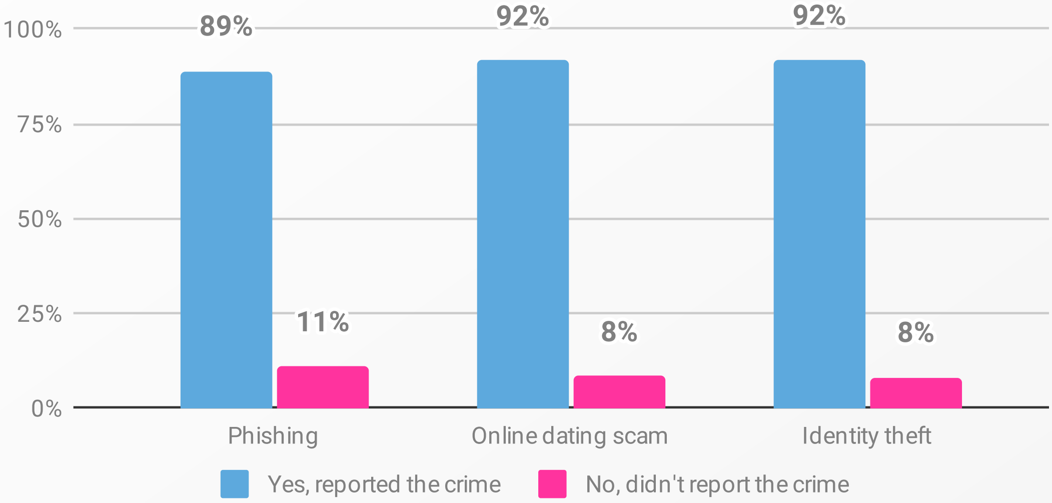


Figure 38. Crime reporting frequency by crime type.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of cybercrime victims (age 18+): Phishing = 1463; Online dating scam, 1028; Identity theft = 855. Dates conducted: March 6, 2024 - April 22, 2024.

It seems people are getting ever more comfortable reporting cybercrime, regardless of age. Reporting rates ranged from 87% for Gen X (+5% from 2023) and Baby Boomers (-1% from 2023) to 94% for the Silent Gen (-2% from 2023). The lowest report rates occurred in Gen X and Baby Boomers, with 13% of each group opting to take the hit in silence.

Reporting rates were lowest for phishing and identity theft amongst Gen X (83% and 91%, respectively), and for online dating scams amongst Baby Boomers (70%).

Who do people turn to after an attack? It all depends on the crime and the victim. The majority of those who have been victims of phishing (61%) or identity theft (59%) reported them to their bank or credit card company (Figure 39). Interestingly, victims of online dating scams (41%) opted to report the incident to the designated person or department at their place of work or education, closely followed by credit card companies and the police or any government agency (39%).

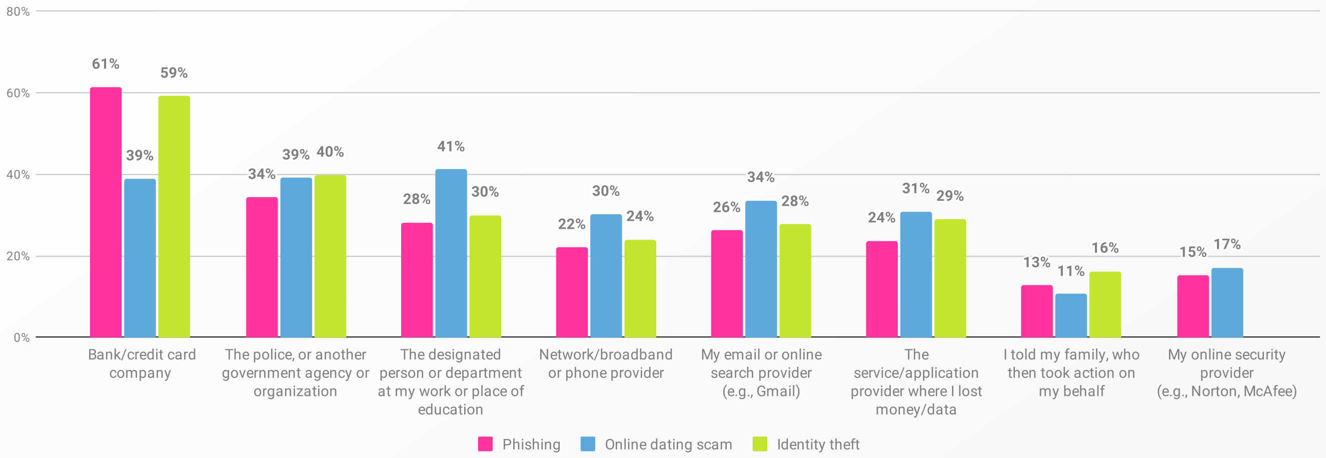


Figure 39. Who were the cybercrimes reported to?

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants (age 18+) who had reported cybercrime: Phishing = 1302; Online dating scam = 942; Identity theft = 785. Dates conducted: March 6, 2024 - April 22, 2024. Multiple-choice question. 'My online security provider' wasn't provided as a choice for victims of identity theft.

And what about motivation for reporting? Like last year, most victims of phishing (53%) and online dating scams (43%) reported the incident to relevant authorities because they wanted to prevent it from happening again to themselves or others. Getting their money back was the second biggest reason for phishing victims to take action (34%). Meanwhile 32% of online dating scam victims reported the incident to stop it from happening again. A desire to catch crims came in third place, for 12% of phishing and 18% of online dating scam reporters.

What about the people who didn't report their cybercrime incidents (Figure 40)? The most common reason for not reporting an incident was not knowing who to report it to (25% of phishing victims and 26% of identity theft victims, up 12% from 2023). Considering the amount of money lost too small was the second most common reason for not reporting phishing (16%) and identity theft (19%).

The picture's a little different for dating scams. Not knowing who to report the incident to still played a significant role (19%, up a substantial 11% from 2023), but shame is the biggest factor in the decision to keep quiet, cited by 23% of victims.

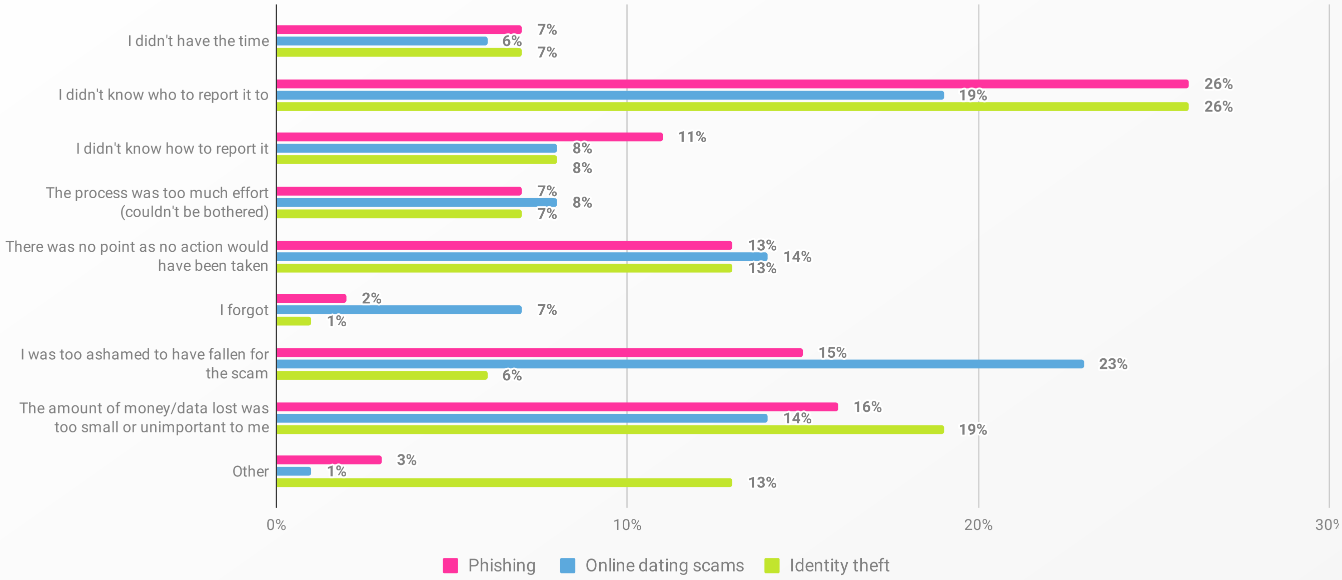


Figure 40. Reasons given for not reporting incidents, by crime type.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants (age 18+) who had not reported cybercrime: Phishing = 161; Online dating scam = 86; Identity theft = 70. Dates conducted: March 6, 2024 - April 22, 2024.

To sum this part up, there are definitely some reasons to be positive. More people are reporting cybercrime, and things are moving in the right direction. However, it's clear a knowledge gap still exists, with many not knowing where to turn. Plus, shame silences those who were simply looking for love, highlighting the importance of creating more supportive environments for victims.

5.4 Cyberbullying

Whatever your mind conjures up when you read the word, cyberbullying isn't just for misguided teenagers. It's a broad definition—using electronics to cause people distress—and people of every age use it, and are affected by it.

> ***Mental distress impacts people's wellbeing, which means it can disrupt security behaviors too, and by extension an employer's security posture.***

It's a growing threat for individuals and organizations alike, and here's why: Mental distress impacts people's wellbeing, which means it can disrupt security behaviors too, and by extension an employer's security posture. So, it was only natural we include it in our research.

Across all participants, 18% (N=1268) reported being victims of cyberbullying. That represents a 3% increase from 2023.

38% of Gen Z and 28% of Millennials reported having been cyberbullied (Figure 41). Overall, older age groups reported lower numbers of cyberbullying, though the percentages slightly increased for Gen X (+3 from 2023) and the Silent Gen (+1% from 2023).

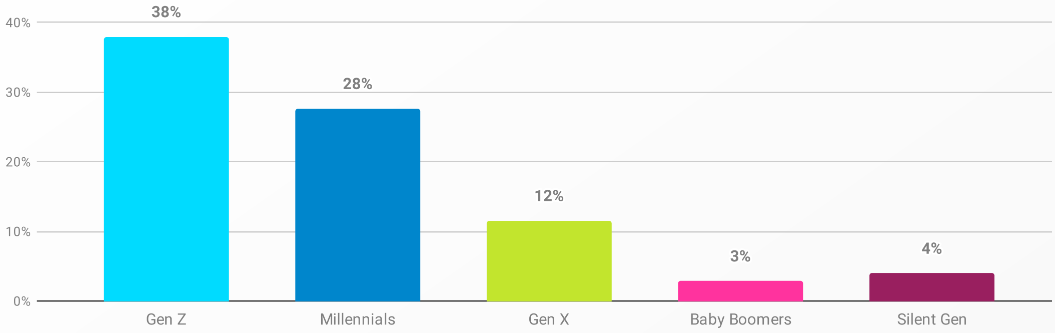


Figure 41. Victim of cyberbullying, by generation.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of cyberbullying victims with generation information: 1233 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

And more good news: only 12% of victims did not report or mention cyberbullying to anyone. (Sure, we'd like to see that figure at 0%, but that's an 8% drop from last year, so we'll take it.)

Those 88% who reported the cyberbullying (N=1115) reported it to various places (Figure 42). The top three places people reported to were the police, or another government agency or organization (41%, +8% from 2023), the school or workplace (37%, +8% from 2023), and the network provider (37%, +13% from 2023). Interestingly, fewer cyberbullying victims talked to their peers or family about it this year (23%, -8% from 2023).

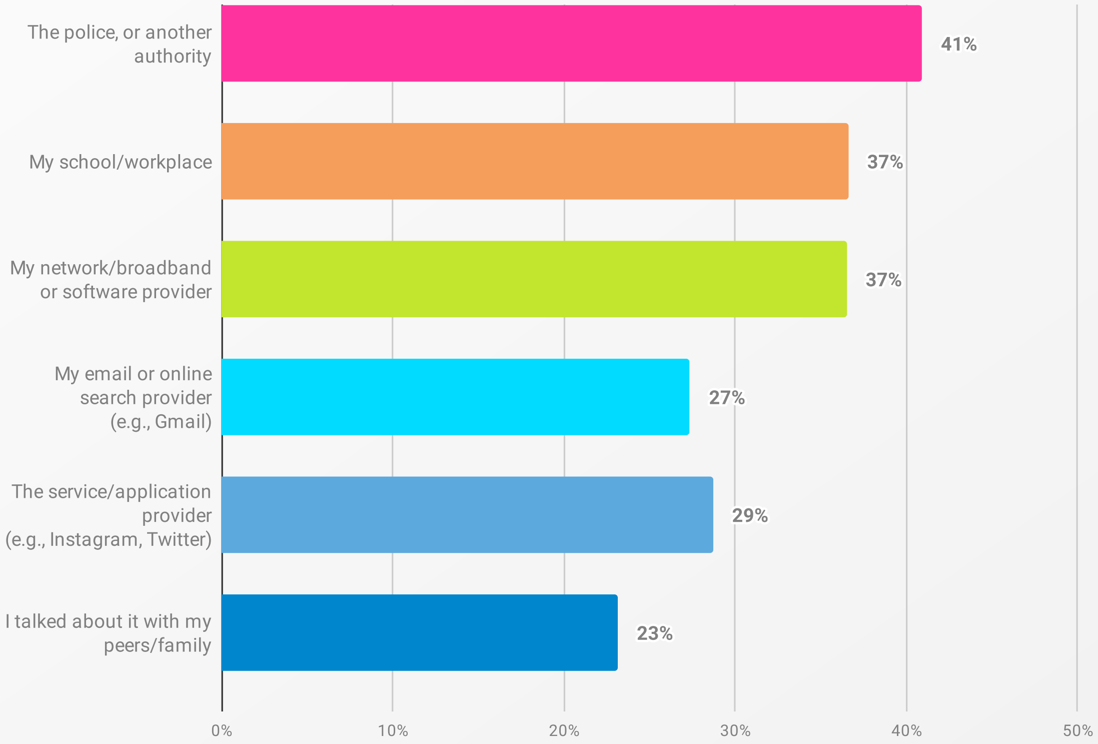


Figure 42. Agencies where cyberbullying is reported to.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of cyberbullying victims who reported the incident: 1115 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

Though incidents of cyberbullying increased from 2023, there is a positive trend: a higher percentage of victims are now reporting these incidents to relevant agencies. And whilst cyberbullying remains more prevalent across younger generations, the fact that older generations are increasingly likely to report incidents reinforces a vital message: cyberbullying can affect anyone.

6. Cybersecurity training

Are you ready to talk training? Because this is where we peel back the layers of that tricky giant onion that is educating people on all things cybersecurity.

We're getting down to brass tacks on it all: Who's getting trained, and who isn't? What training formats are a hit, and which are bottom of people's list?

And...was it all worth it? Tender hearts beware, as we asked people if they, you know, actually learnt anything from it.

Just like that battered old laptop bag you keep swearing to replace, this section ain't always pretty, but it's beyond essential.

6.1 Access to training

Break out the bunting! For the first time in four years, access to training has increased, with 33% reporting to have used it, and 11% having access but not using it (Figure 43). Baby steps, people. Baby steps.

The less-great news? Over half (56%) of the participants *still* don't have access to cybersecurity training (or are unaware they have access).

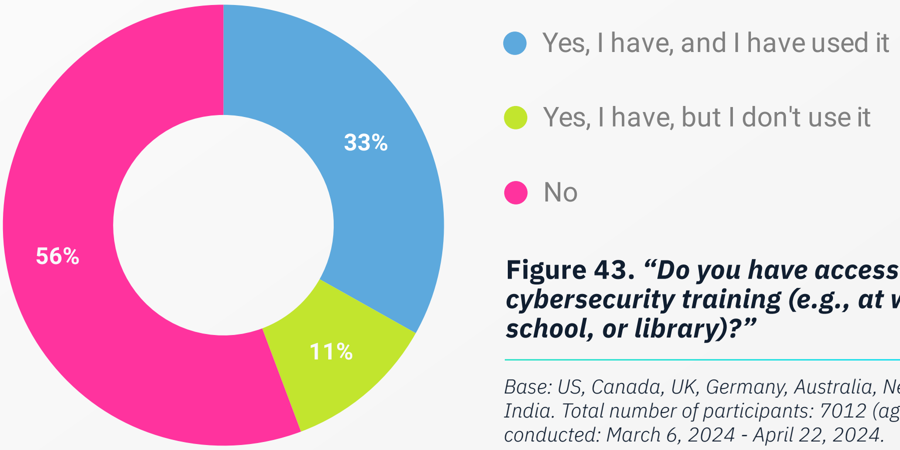


Figure 43. *"Do you have access to cybersecurity training (e.g., at work, school, or library)?"*

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants: 7012 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

There's a distinct divide in training accessibility. Participants who are employed or who are students have markedly better access to training (57% and 55% respectively) than retirees and those not actively working or studying (11% and 19% respectively) (Figure 44).

But while access has increased notably for employed individuals and students since 2023 (by 10% and 6%, respectively), 43% of working individuals and 45% of students still lack access to training. It remains very much a game of chance.

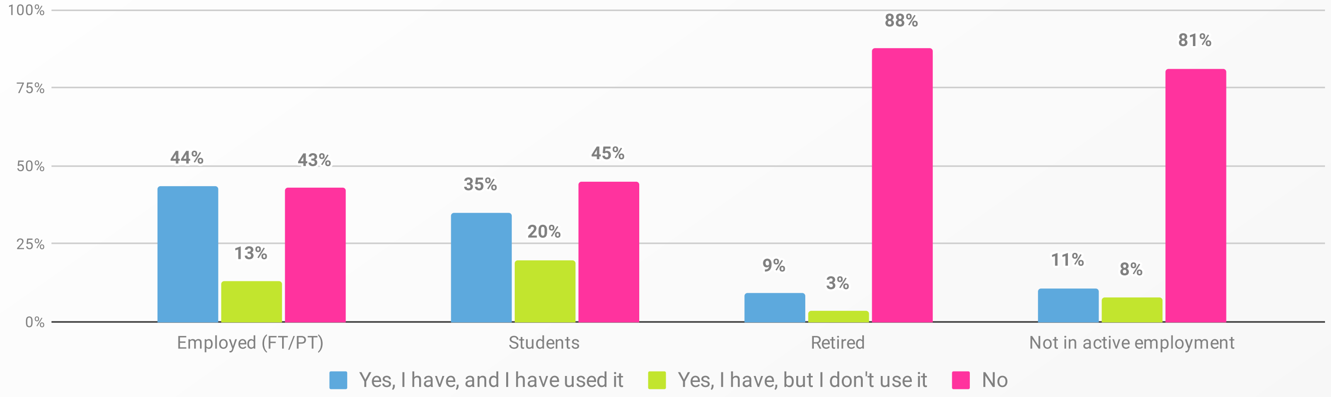


Figure 44. ***"Do you have access to cybersecurity training (e.g., at work, school, or library)?"*** **by employment.**

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants: 7012 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

Next, the generational trends. It turns out the majority of Millennials (47%) and Gen Z (44%) have access to and have used training, reflecting increases of 9% and 10% from last year (Figure 45). Overall, fewer people across all generations reported a lack of access to training compared to 2023, most notably 35% (-9%) of Gen Z, and 39% (-11%) of Millennials.

But don't roll out the confetti cannons just yet: Despite the positive trend in increased access to training, a substantial number of older participants still do not have access to cybersecurity training, with 92% of the Silent Generation, 80% of Baby Boomers, and 59% of Gen X in cyberskills purgatory. This certainly raises a king-size red flag, because when it comes to online safety, ignorance is categorically *not* bliss.

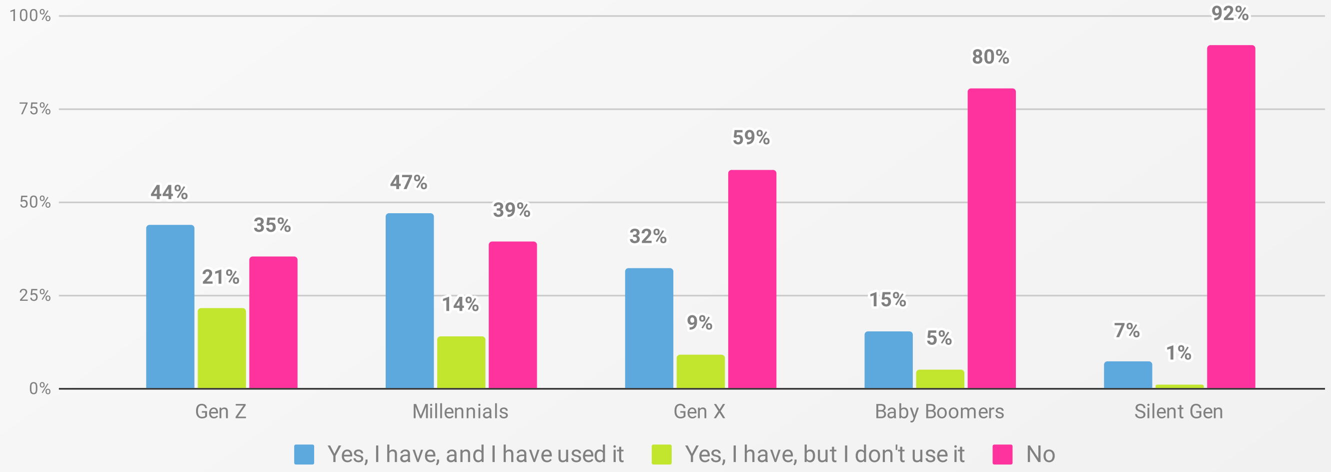


Figure 45. ***"Do you have access to cybersecurity training (e.g., at work, school, or library)?"*** **by generation.**

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants with generation information: 6749 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

Switching our focus from the have-nots to the haves. We asked those who were using the training they had access to (2,336 of them, if we're being pedantic) a bunch of questions to gain further insights.

Where exactly does the training happen? The majority (66%, down 3% from 2023) said that they accessed cybersecurity training at their workplace. There was a slight uptick in those accessing training at home (42%, a 5% increase from 2023). Additionally, 12% of participants accessed training at their educational institutions.

> ***Only 1 in 3 people are being equipped to stay secure against evolving threats.***

Furthermore, 71% of those who completed training reported that it was a one-off session, whether it was individual or group, online or in person. Only 29% reported continuous training over a period of time, whether individually or in groups. In other words, fewer than 1 in 3 people are being equipped to stay secure against evolving threats.

6.2 Mandatory training

Of those with access to cybersecurity training at their workplace or place of education (N=1661), 86% reported being required to complete mandatory training, representing a 4% increase from 2023.

Among those required to complete training (N=1432), 48% (-7% from 2023) do so at an annual one-and-done event (Figure 46). Additionally, there were increases in participants completing training 'when something goes wrong' (8%) and 'both at regular intervals & when something goes wrong' (18%), by 3% and 4%, respectively.

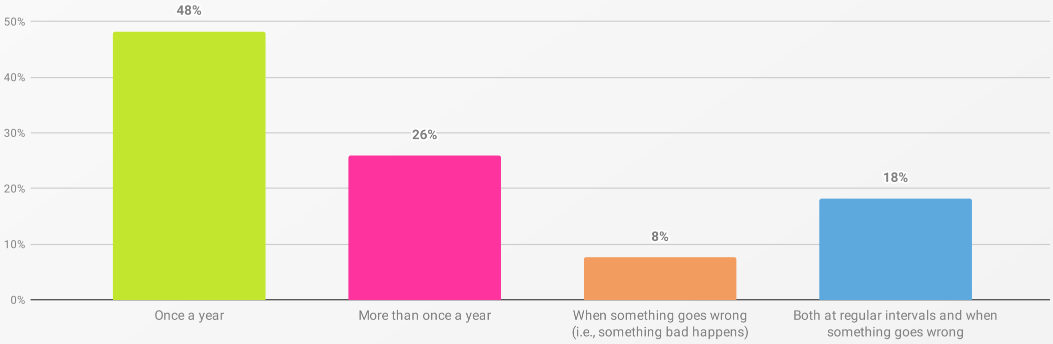


Figure 46. ***"How often are you required to complete training?"***

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants required to complete mandatory cybersecurity training at work or their place of education: 1432 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

Careful with excessive training! A study[19] found that frequent information security training at work was associated with lower awareness regarding email security. This could be due to overconfidence, mismatched training styles, or training overload, which can lead to fatigue and decreased compliance.

[19] Reeves, A., Parsons, K., & Calic, D. (2020, July). Whose risk is it anyway: How do risk perception and organisational commitment affect employee information security awareness? *International Conference on Human-Computer Interaction* (pp. 232-249). Cham: Springer International Publishing.

6.3 Barriers to attendance

Remember the 11% (N=785) who, despite having access to training, decided not to utilize the opportunity? We asked them why.

The most common reason for not attending training was people feeling they already knew enough about cybersecurity (23%, Figure 47), which increased by 5% from 2023. Lack of time (22%) was a close second, representing a 7% drop. Indeed, these two reasons switched places since 2023.

> ***20% opted out of training because they didn't believe it would reduce their risk of being a victim of cybercrime.***

The third most popular response in the "reasons to skip" list? Twenty percent (+4% from 2023) opted out of training because they didn't believe it would reduce their risk of being a victim of cybercrime. Furthermore, a small percentage (1%, N=10) of qualitative responses also suggested that people's belief in their cybersecurity knowledge was a barrier to attending training.

> **Informing oneself is more effective [than attending a cybersecurity training course].** PS7967, Germany

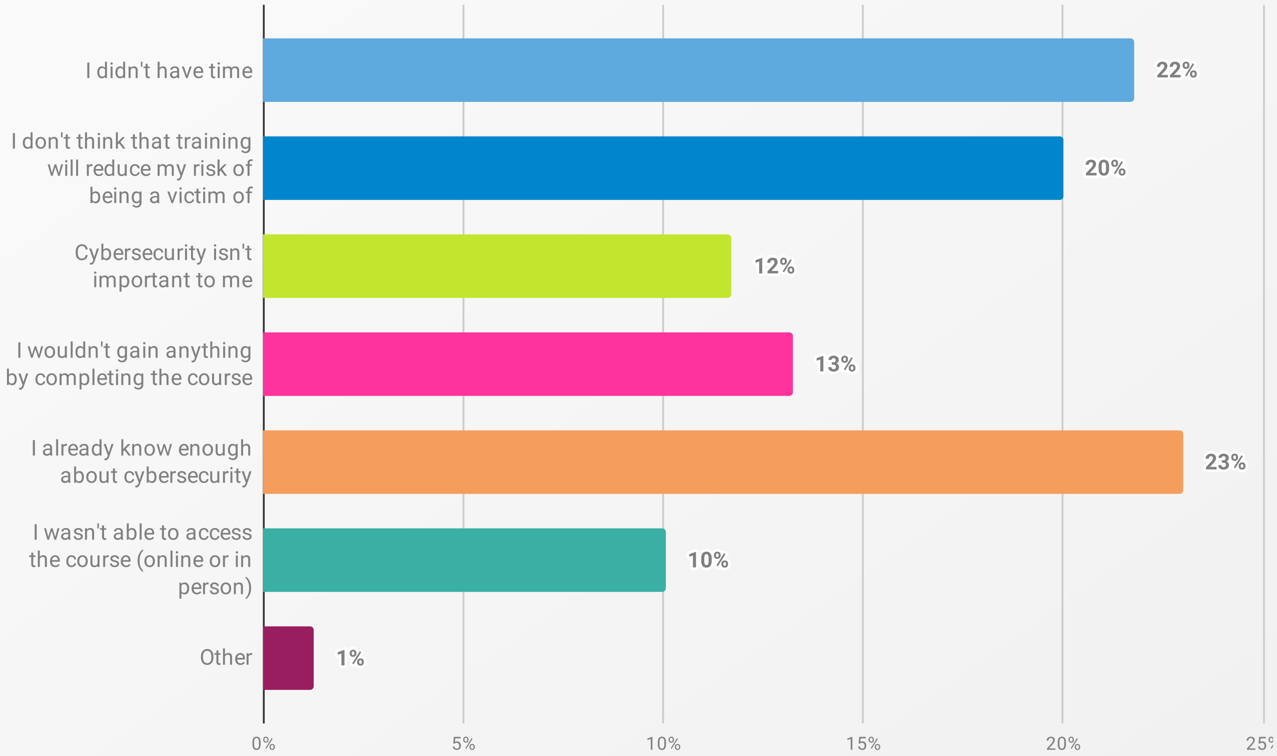


Figure 47. *"What is the main reason you didn't use the opportunity to attend a cybersecurity training course?"*

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants who have access to cybersecurity training but don't use it: 785 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

6.4 Preferred format

We were keen to shine a light on people's preferred training formats—something that organizations are keen to pin down too. For many, it's all about video content (46%, Figure 48). In second place, 37% of participants preferred online courses held periodically, closely followed by written materials (35%). Short, bite-sized pieces of information delivered at the time of need (like nudges) were only preferred by a third (33%) of the participants. The least preferred format was online games or gamified experiences, with only 11% expressing a preference. This may come as a surprise to some, given how widespread gamification is across a host of industries.

Some respondents believe they do not need formal training as they rely on their own knowledge and common sense. Responses such as "I know what I am doing," "common sense," and "I am extremely proficient with IT" reflect this sentiment.

> **I know what I am doing.** PS83, USA

> **I don't need training. This is ridiculous.** PS8363, Canada

> **I don't do any cybersecurity training, just use my own commonsense.** PS290, New Zealand

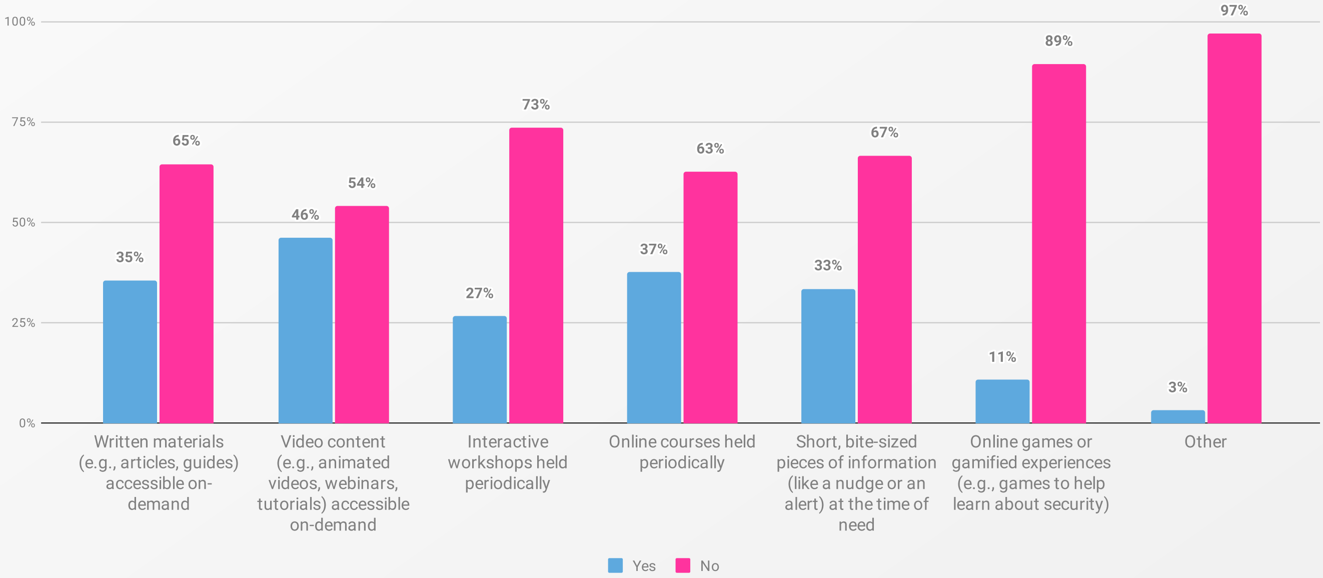


Figure 48. *"What format do you prefer to consume cybersecurity training information?"*

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants: 7012 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

Written materials accessible on-demand were preferred by older generations (Figure 49), with 36% of Silent Gen and 25% of Baby Boomers favoring them. Conversely, written content was the least preferred format for Gen Z participants, with only 15% expressing this preference.

The winner for younger generations was video content, with 27% of Gen Z, 26% of Millennials, and 24% of Gen X preferring them. Perhaps not surprising in the TikTok age. Online courses appeared to be the second preference for younger generations, with 19% of Gen Z, 20% of Millennials, and 22% of Gen X favoring them.

The preference for interactive workshops decreased across generations, from 16% of Gen Z to 9% of Silent Gen. A similar trend occurred in online games or gamified experiences, which were the least preferred training format across all generations. Again, here there was a slight drop in preference seen with age—from 8% for Gen Z to from 0% for Silent Gen.

If you'll allow us a short, sweet sidebar, it's important to note previous research[20] has shown the effectiveness of gamification in security awareness training. Gamification[21] is a broad concept, referring to using game-like elements in non-game contexts to raise awareness and, ideally, change behavior.

It's often more implicit than explicit, and users may not recognize the use of game elements in their experience. For example, leaderboards are a simple form of gamification that might go unnoticed. So, while the findings clearly point to a preference against online games for cybersecurity training, there is still lots of value in exploring the gamification approach.

Anyway, back to our regularly scheduled programming...

Overall, the data suggest younger generations prefer consuming cybersecurity training via online resources like videos and courses, while older generations prefer reading written cyber content. Alright, no shockers here, but always good to have the data confirm what we might have suspected.

[20] Abu-Amara, F., Almansoori, R., Alharbi, S., Alharbi, M., & Alshehhi, A. (2021). A novel SETA-based gamification framework to raise cybersecurity awareness. *International Journal of Information Technology, 13*(6), 2371-2380.

[21] Deterding, S., Dixon, D., Khaled, R., & Nacke, L. (2011, September). From Game Design Elements to Gamefulness: Defining Gamification. In *Proceedings of the 15th International Academic MindTrek Conference: Envisioning Future Media Environments* (pp. 9-15).

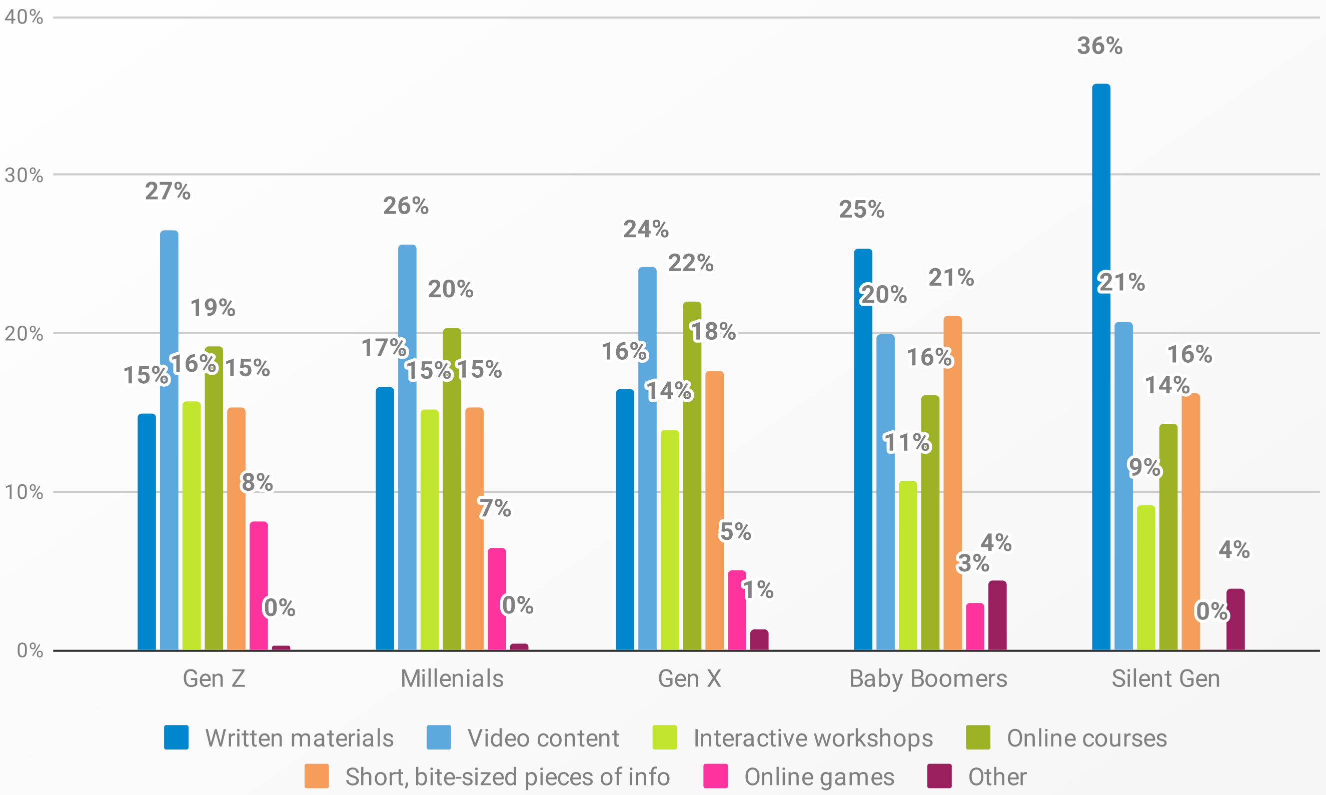


Figure 49. *"What format do you prefer to consume cybersecurity training information?"* by generation.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants with generation information: 6749 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

Think this training lark is just about age? Think again! Things get even more intriguing when we examine preferences for cybersecurity training across different employment statuses (Figure 50).

Employed participants favor video content (25%), closely followed by online courses (21%). An equal percentage (16%) preferred written materials and bite-sized information. The picture for online games didn't get any better—only 6% preferred this format.

> ***Employed participants favor video content (25%), closely followed by online courses (21%).***

Looking at preferences based on employment status revealed written cybersecurity training content is mostly preferred by retirees (28%), followed by those not in employment (19%). Similarly, 22% of retirees and 20% of those not in active employment prefer short, bite-sized information.

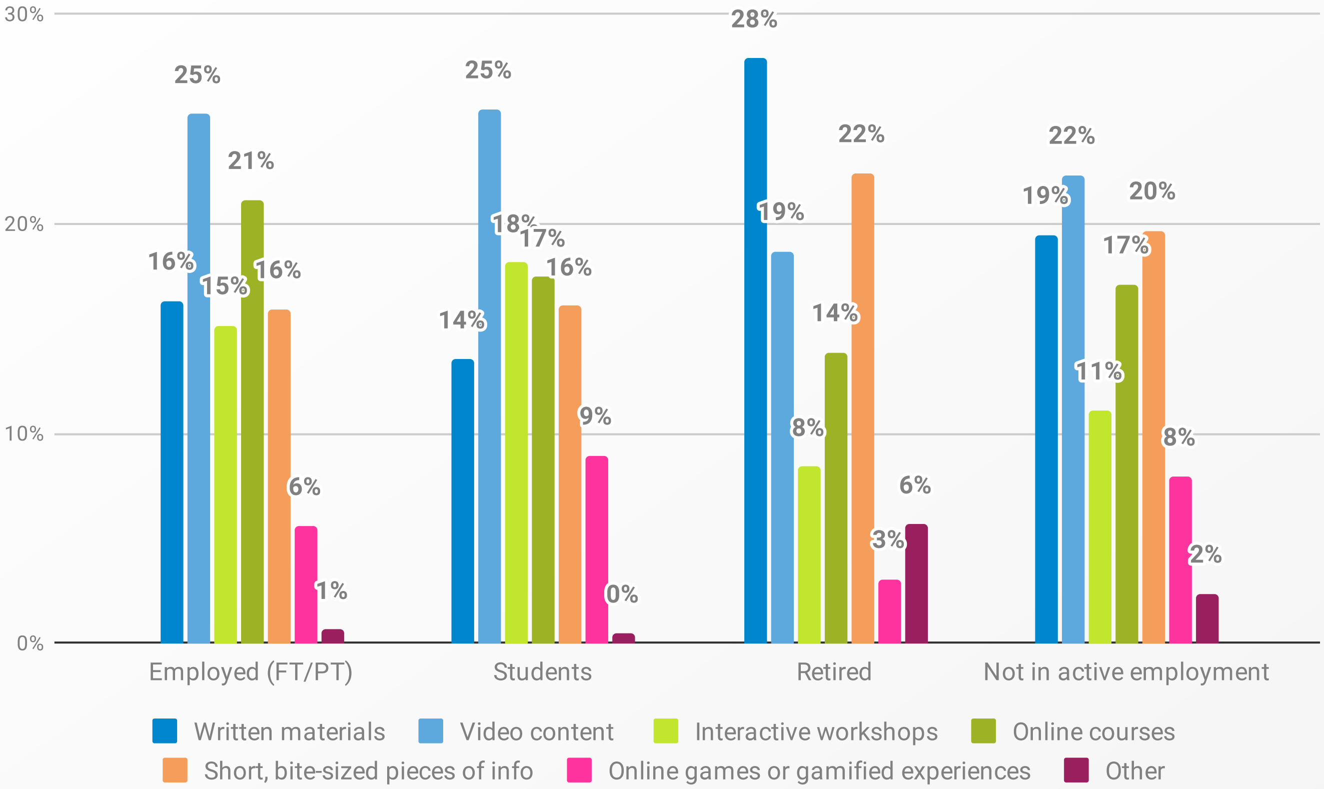


Figure 50. *"What format do you prefer to consume cybersecurity training information?"* by employment.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants: 7012 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

The findings make it clear. There is no one-size-fits-all approach when it comes to cybersecurity training. The diversity in preferences across age groups and employment statuses emphasizes organizations should offer a mix of training formats to accommodate different learning styles and preferences.

6.5 Impact on security behaviors

As we get to the business end of this section, we wanted to know what perceived impact does training have, and how do people feel about it? We asked those who completed their cybersecurity training (N=2336) about how it influenced their security behaviors (Figure 51).

Overall, there were increases in the perceived impact of training on all security behaviors compared to 2023. The biggest impact of training was on people's ability to recognize and report phishing messages, with 52% (+2% from 2023) reporting improvement. Notably, 45% reported starting to use multi-factor authentication (MFA) as a result of cybersecurity training, an increase of 11% from 2023.

> ***45% reported starting to use multi-factor authentication (MFA) as a result of cybersecurity training.***

But not everybody had their world rocked by security training. A nonplussed 4% (-2% from 2023) said training had no impact on their cybersecurity behaviors. Furthermore, 11% reported they did not change anything as a result of attending a cybersecurity training course, because they already performed the security behaviors measured.

How about the overall perceived usefulness of the training? A heartening 83% of participants who accessed training at their workplace or place of education (N=1661) found it useful. And only 4% reported it not being useful. So, whilst training is far from people's favorite things to do, it does seem to be having a positive effect.

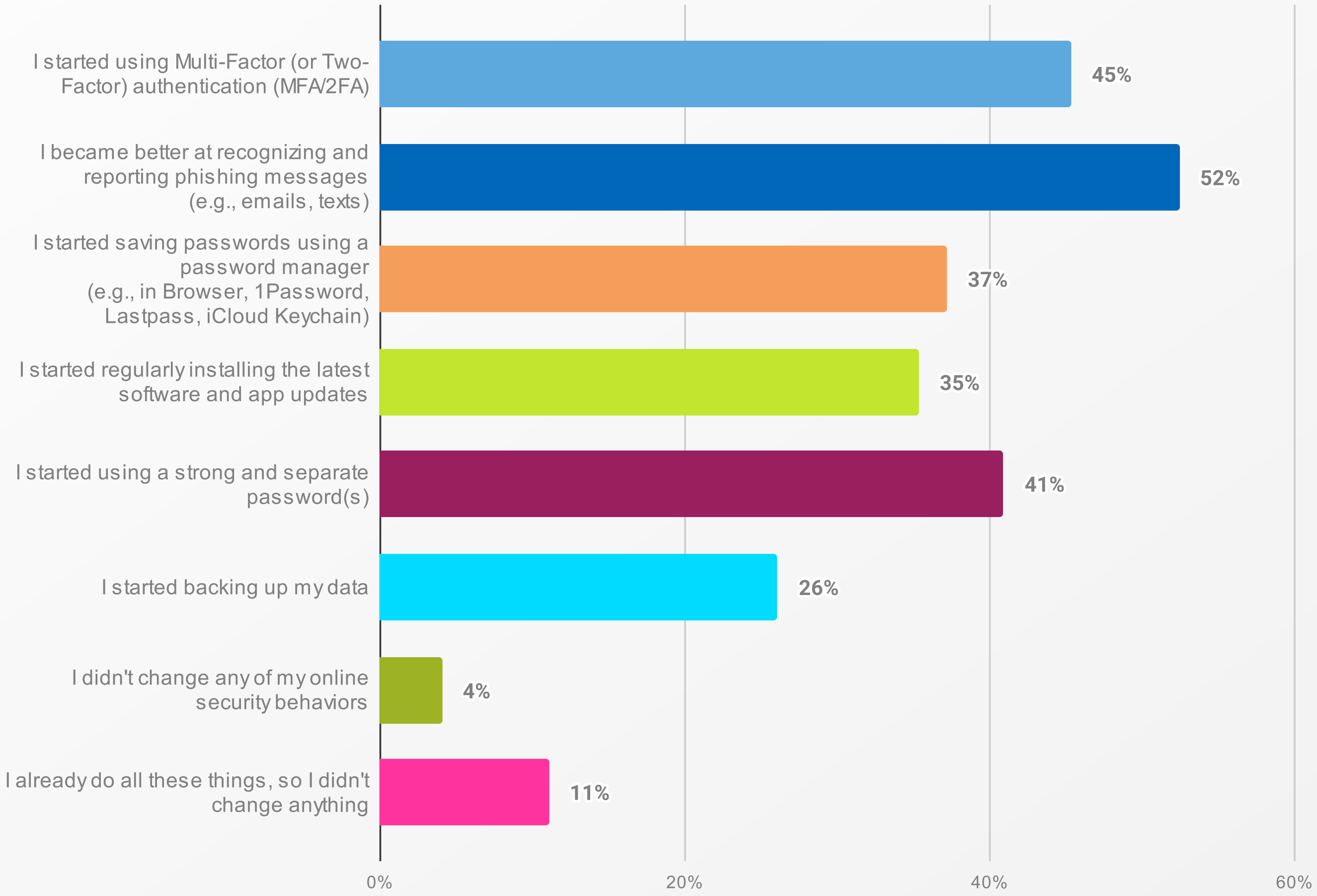


Figure 51. *"When you attended training course(s), how did it influence your security behaviors?"*

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants who have access to cybersecurity training and used it: 2336 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

While these results are promising, they're not yet ideal. This is not surprising, given that existing literature[22] has shown the limited success of Security Education, Training, and Awareness (SETA) programs in improving employees' ability to mitigate cybersecurity threats.

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

7. Cybersecurity knowledge & behaviors

With more than half of participants constantly connected and managing multiple online accounts, the million dollar question here is: how cyber-savvy do people think they are?

This is a new dimension for 2024's survey, and we didn't stop there: We asked them about the actions they take to keep their information, accounts, and devices safe from cybercriminals.

In this section, we examine five key cybersecurity behaviors:

- Ensuring good password hygiene
- Using MFA
- Installing the latest software updates
- Backing up data
- Spotting and reporting phishing

Before diving into the behavioral nitty-gritty, how do our participants think they stack up in the knowledge department?

More than half of participants (57%, Figure 52) consider themselves to have either intermediate or advanced cybersecurity knowledge. About a third said they had basic knowledge, while a mere 6% rated themselves as novices. Additionally, a tiny (yet admirably honest) 3% claimed they don't have any knowledge about staying secure online.

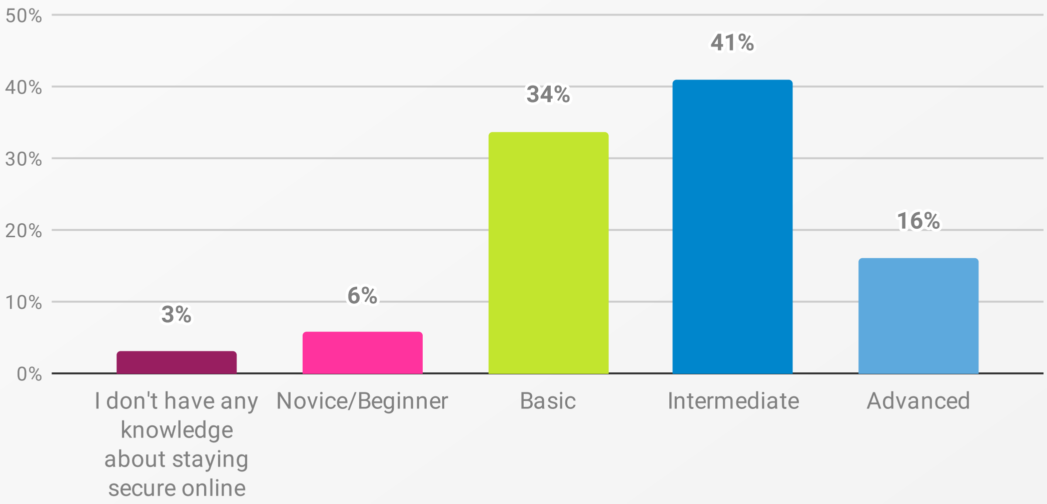


Figure 52. Self-reported cybersecurity knowledge.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants: 7012 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

Breaking this down by generations reveals notable differences (Figure 53). Younger are the most confident in their knowledge, with 68% of Millennials and 66% of Gen Z claiming intermediate or advanced.

In contrast, the largest proportions of Baby Boomers (46%) and Silent Generation (43%) rated their knowledge as basic. Moreover, older generations show higher percentages of novices, with 15% of the Silent Generation and 8% of Baby Boomers falling into this category. Additionally, 11% of the Silent Generation and 3% of Baby Boomers reported having no cyber knowledge at all.

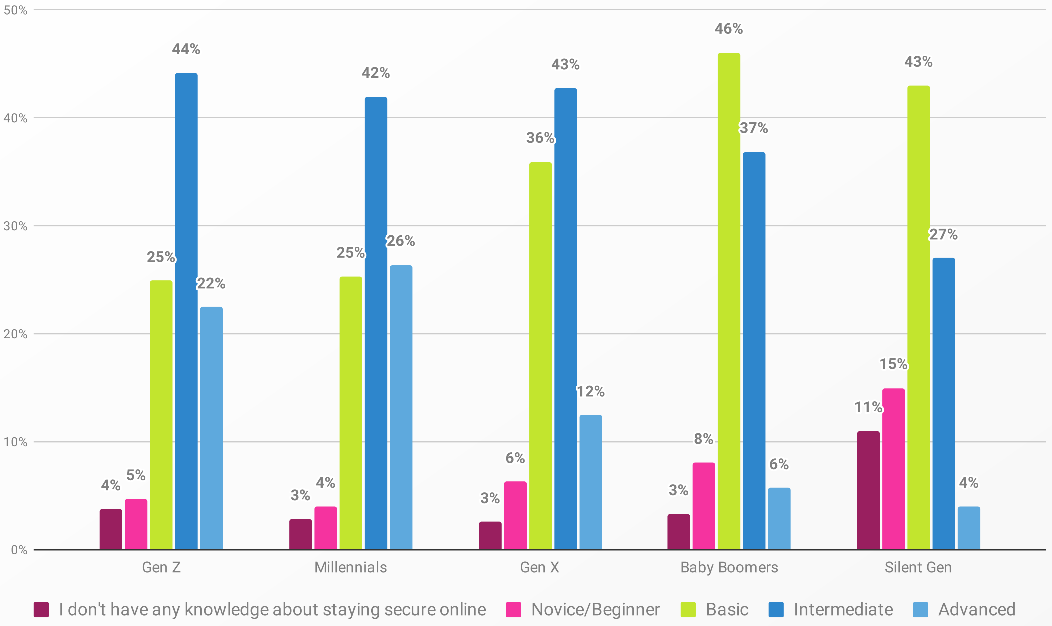


Figure 53. Self-reported cybersecurity knowledge, by generation.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants with generation information: 6749 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

Wondering how employment status relates to knowledge level? The majority of those employed (44%) and students (43%) reported having intermediate cybersecurity knowledge (Figure 54). The highest percentage of participants with advanced security knowledge are those who are employed (21%), followed by students (16%).

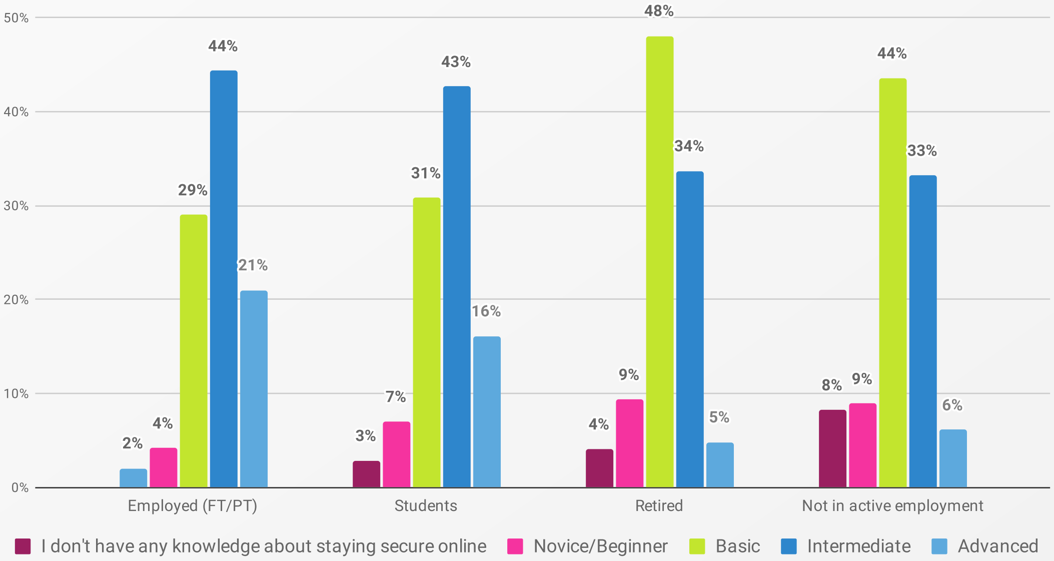


Figure 54. Self-reported cybersecurity knowledge, by employment.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants: 7012 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

Overall, younger generations and those with jobs tend to have higher levels of security knowledge compared to other groups, while retired individuals and those not in active employment generally have lower levels of security knowledge.

Now it's time to shift the focus from knowing to doing—but before we do, a reminder that the data here is based on people's self-reported behaviors. Inevitably, perceptions and reality rarely line up perfectly, but that doesn't mean that the data aren't hugely valuable.

With that said, let's turn to one of the OG cybersecurity topics—passwords.

7.1 Password hygiene

Over half of the participant pool felt knowledgeable about cybersecurity, but how do their password behaviors compare?

People's password habits are, in general, liable to send security teams' blood pressure skywards. On the whole, risky practices—like reusing weak passwords—are rife. This dials up the chances of account compromise.

The National Institute of Standards and Technology (NIST) lays out guidelines[23] for password hygiene:

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

Most of these have been reflected in all participating countries and/or regions: NCA[24], NCSC[25], Get Cyber Safe[26], Own Your Online[27], ACSC[28], CERT-In[29], BSI[30] and ENISA[31] guidelines for password hygiene.

In this report, we examine participants' password hygiene by looking at:

- Password creation tactics (e.g., length, use of personal info, and single dictionary words)
- Use of separate passwords
- Password management strategies[32]

[23] https://pages.nist.gov/800-63-3/sp800-63b.html
[24] https://staysafeonline.org/online-safety-privacy-basics/passwords-securing-accounts/
[25] https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/three-random-words
[26] https://www.getcybersafe.gc.ca/en/secure-your-accounts/passphrases-passwords-and-pins
[27] https://www.ownyouronline.govt.nz/personal/get-protected/guides/how-to-create-good-passwords/
[28] https://www.cyber.gov.au/protect-yourself/securing-your-accounts/passphrases
[29] https://www.cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES02&VLCODE=CIAD-2022-0026
[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.enisa.europa.eu/topics/incident-response/glossary/authentication-methods
[32] SebDB behaviors: SB209 Uses a stand-alone password manager application, SB210 Saves passwords of passphrases into a browser

7.1.1. Password creation tactics

Let's start by exploring participants' self-reported knowledge on how to create strong passwords. Seventy-eight percent (+2% from 2023) of participants reported knowing how to create strong passwords and actually doing so.

> ***For some, there's a disconnect between knowledge and behavior.***

This was fairly consistent across generations, with rates ranging from 70% for Gen Z to 84% for Baby Boomers. But for some, there's a disconnect between knowledge and behavior: 16% said they knew how to create strong passwords but didn't actually do so. This scenario was highest among Gen Z (23%) and Millennials (19%), compared to 10% of the Silent Generation and 11% of Baby Boomers.

The large proportion of people putting their knowledge into practice is reassuring for sure. Yet the data highlight a common issue in cybersecurity: the disparity between knowledge and behavior. It's a reminder to look beyond only imparting knowledge (read: training), and to include behavior change interventions as part of a holistic strategy. Did someone say Human risk management?

7.1.1.1 Password length

Next, how do people's password lengths 'measure' up? These puns hit hard, we know.

Most participants (43%, -3% from 2023) create passwords of 9-11 characters. Around a third (32%, +2% from 2023) create shorter ones. Only 25% create passwords of more than 12 characters, but at least that's up by 1% since 2023.

The younger generations are leading the charge with longer passwords, with 29% (same as in 2023) of Gen Z, and 28% (+1% from 2023) of Millennials sporting 12+ character passwords, compared to 11% (-5% from 2023) of the Silent Generation and 22% (+4% from 2023) of Baby Boomers (Figure 55).

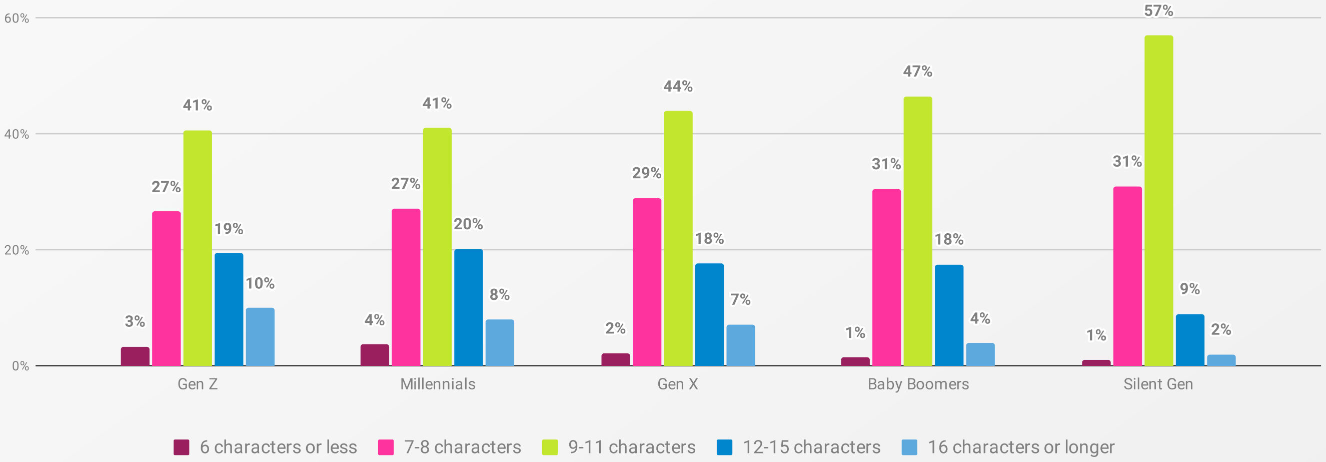


Figure 55. *"How long are the password(s) you usually create?"* by generation.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants with generation information: 6749 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

While a notable portion of participants create moderately long passwords, there is still a substantial number opting for shorter, less secure passwords. Younger generations tend to adopt longer, more secure passwords more frequently than older generations.

7.1.1.2 Use of personal information

For the second year in a row, the percentage of participants including personal information in passwords increased—such as family members or pet names. This year, over a third (35%) of participants included personal information in their passwords.

> ***Over a third (35%) of participants included personal information in their passwords. Perhaps we should be advising people to change their pets?***

Just like last year, this tendency was more prevalent across younger generations. Fifty-two percent (+2 from 2023) of Gen Z and 45% (+4% from 2023) of Millennials admitted using names of family members or pets, dates, and places when creating passwords (Figure 56).

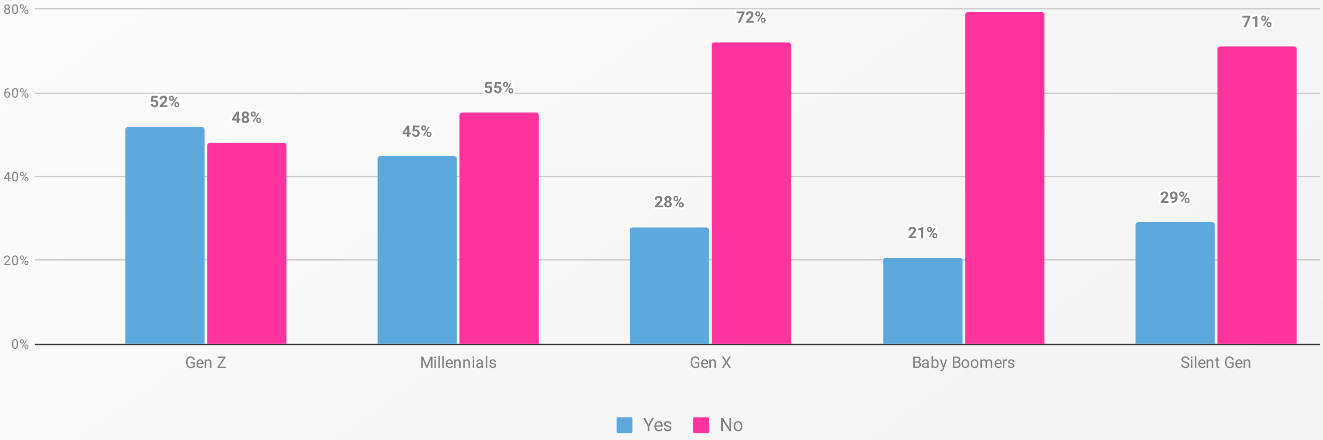


Figure 56. *"Do you tend to create password(s) that include references to personal information?"* by generation.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants with generation information: 6749 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

This persistent vulnerability in password creation practices is concerning, especially considering that the most aware groups are also most likely to use easily guessable passwords. Perhaps we should be advising people to change their pets?

7.1.1.3 Using a single dictionary word

Brace for more less-than-thrilling news: A hefty 40% of the participants 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). What's more, this represents a 6% increase from 2023, which itself was a 5% rise from 2022. Is the increasing number of accounts people are having to manage trumping the security advice on passwords?

> ***40% of the participants reported creating passwords using a single dictionary word or someone's name.***

Once again, we need to put the spotlight on the younger generations. A tad over half (52%, Figure 57) of Gen Z participants reported using single dictionary word passwords, showing a 9% increase from 2023. While the use of single dictionary word passwords has increased across all generations since 2023, it still remains the lowest among older generations, with 28% of the Silent Generation and 29% of Baby Boomers reporting using this approach.

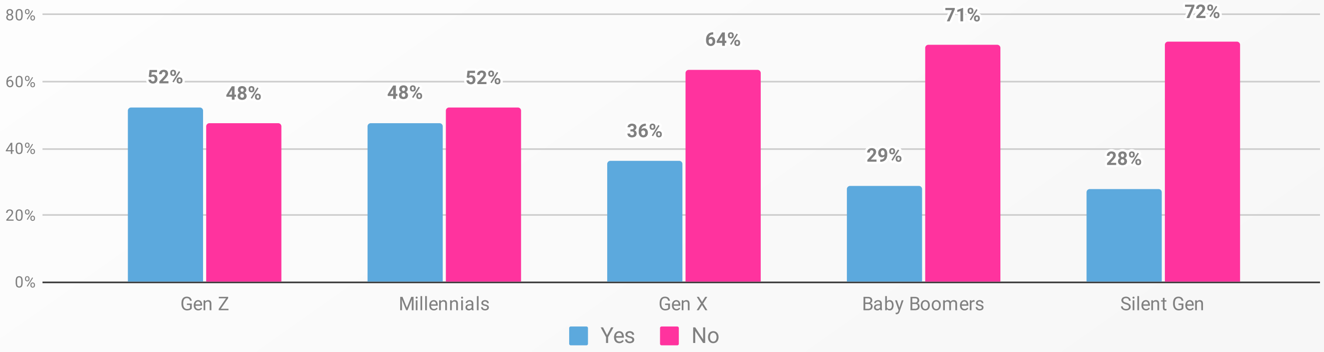


Figure 57. *"Do you tend to create password(s) that are made up of a single dictionary word or name, and you replace some characters with numbers or symbols?"* by generation.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants with generation information: 6749 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

In summary, younger generations, particularly Gen Z and Millennials, are more likely to create passwords based on a single dictionary word or name with character replacements. In contrast, older generations, especially Baby Boomers and the Silent Generation, are less likely to use this method, indicating potentially more diverse and secure password practices among the older participants.

7.1.2 Using separate passwords

Next, who's keeping it fresh...and who's shamelessly double dipping? It turns out 65% (a decrease of 2% from 2023) reported using a separate password either 'all of the time' or 'a majority of the time'. Not bad, but meanwhile, the remaining 35% were less rigorous with their use of unique passwords (Figure 58).

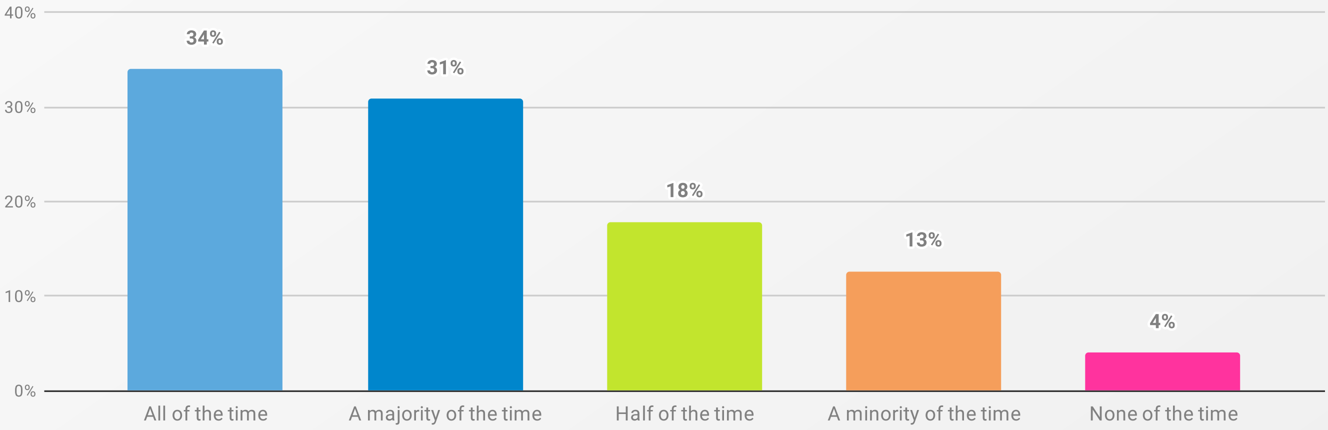


Figure 58. *"How often do you use unique passwords for your important online accounts (e.g., emails, social media, payment-related sites)?"*

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants: 7012 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

The data indicate older generations, particularly Baby Boomers and the Silent Generation, are more consistent in using unique passwords for their important online accounts (Figure 59). Specifically, Baby Boomers (71%) and the Silent Gen (70%) reported the highest frequency of using unique passwords either ‘all of the time’ or ‘a majority of the time’.

Conversely, younger generations, like Gen Z, are less consistent, with only 27% always using separate passwords and 31% doing so ‘a majority of the time’. In fact, a notable portion of Gen Z (23%) and Millennials (21%) use unique passwords only ‘half of the time’.

These figures suggest that while all generations have a generally good level of password hygiene awareness, younger generations are less likely to put this knowledge into practice. We know younger generations are juggling more accounts, perhaps this could be contributing?

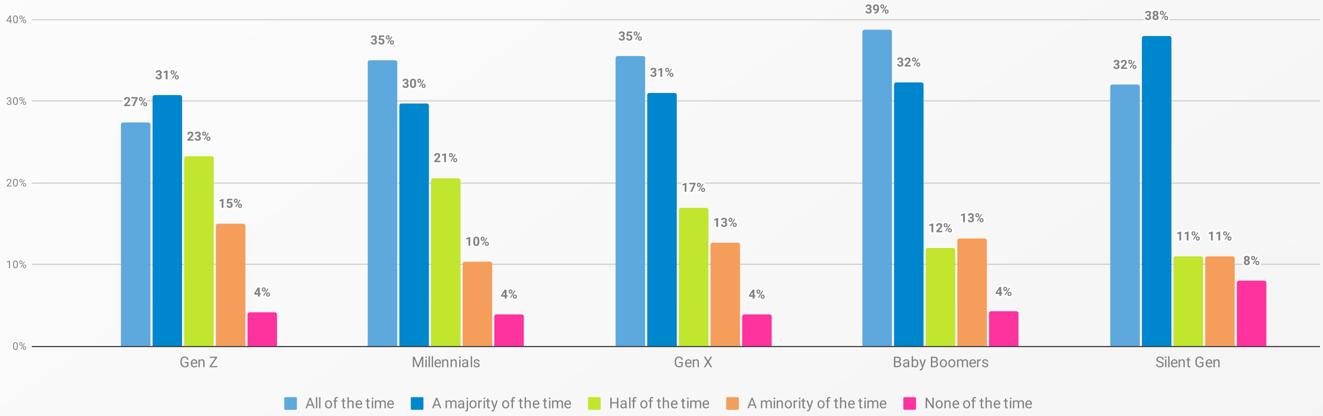


Figure 59. *“How often do you use unique passwords for your important online accounts?”* by generation.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants with generation information: 6749 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

We were super curious about our serial reusers (N=1168). Why did they rarely, if ever, use separate passwords for their online accounts? We asked!

The majority (60%, an increase of 4% from 2023) cited difficulty remembering multiple passwords. Additionally, 17% (-4% from 2023) claimed they only used separate passwords for accounts where they wanted increased security. Furthermore, 15% mentioned that having separate passwords was time-consuming or required extra effort.

> **My existing passwords have proved reliable for over 25 years!** PS1000, New Zealand

7.1.3 Password management strategies

With 91% of participants managing more than one online account, and 65% reporting they use unique passwords, we wanted to shine a light on their preferred strategies for managing and remembering these precious particulars.

7.1.3.1 Preferred password management strategies

It seems plenty of us are wedded to our old-school ways when it comes to managing multiple passwords. The most preferred method (29%) among those with more than one online account (N=6394) was to remember multiple passwords by writing them down in a notebook (Figure 60). This is not necessarily a bad tactic (as long as the book is stored safely). So maybe think twice before taking to LinkedIn decrying the “stupidity” of people using this trusty method.

Meanwhile, a mighty 21% (a 3% drop from 2023) reported remembering their passwords without storing or writing them down anywhere. Just over a quarter (27%) used other methods, such as documenting passwords in an electronic format, storing them on a phone or email, or...just resetting them every single time they logged in—ideal if you love a daily dose of frustration.

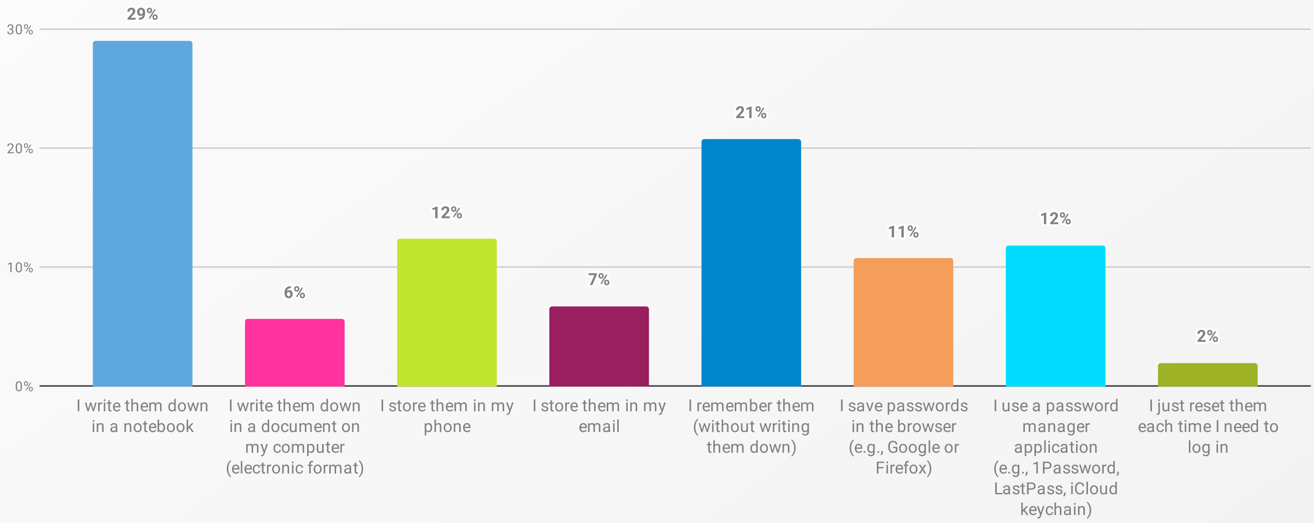


Figure 60. Preferred password management strategies.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants with more than one online account: 6394 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

The older generations were the main pen-and-paper patrons here, with 59% of the Silent Generation and 44% of Baby Boomers choosing the good ol’ notebook method. Remembering passwords without writing them down was most common among Millennials (23%), Gen X (22%), and Gen Z (21%). Quite the flex.

> ***“But what about password managers?!” you scream at your screen!***

Overall, despite a slight decline since 2023—and the laudable memory mastery from the fresher-of-face—the notebook method remains the most common approach for managing multiple passwords, especially among older generations.

“But what about password managers?!” you scream at your screen, like you’re watching a horror movie where the heroine’s investigating a dark corridor despite the ominous music. We hear you. We’re somewhat puzzled too. And in the next section we’ll get into the why, the who, and the what-the-heck of password manager usage.

7.1.3.2 Use of password managers

Let’s rip off the band aid: A grimace-inducing 46% of the entire participant pool had never used a password manager. But the better news is that this figure is down 10% from last year (Figure 61). On the flip side, whilst a promising 40% said they use a password manager, a further 14% noted that they’d given it a go, but stopped.

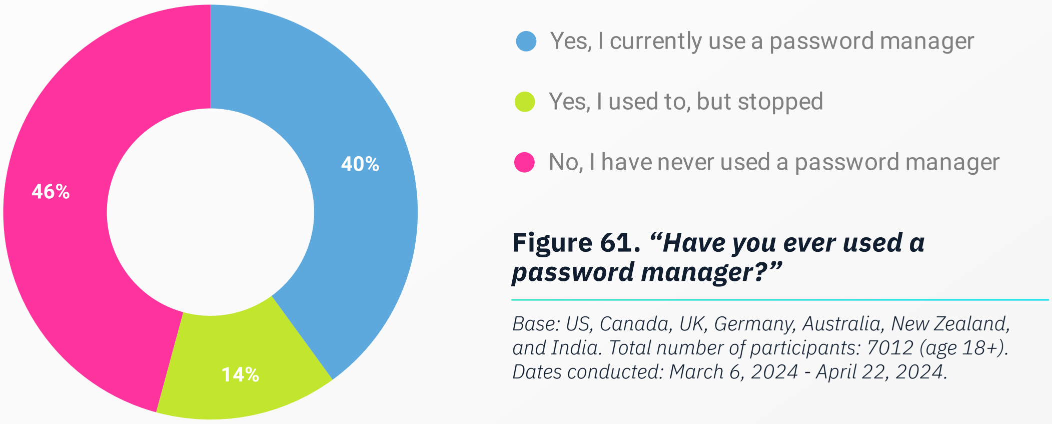


Figure 61. *“Have you ever used a password manager?”*

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants: 7012 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

Of those actively using password managers (N=2803), 40% preferred to use their internet browser option. This was followed by 37% who used free stand-alone password managers, with only 23% having purchased a stand-alone one.

The use of password managers seemed to decrease with age, as the highest percentage of usage was reported by Gen Z and Millennials (both 46%). But these generations also reported the highest rates of abandoning their password manager, with 22% of Gen Z and 18% of Millennials ditching the tool like a faulty Tamagotchi. In contrast, 66% of the Silent Generation and 60% of Baby Boomers have never even dipped a toe into the password manager pond.

The top reasons why people split or never even got started (N=4209) are pretty interesting:

> 1. Feeling that using it won’t stop cybercriminals (48%, -1 from 2023).
> 2. Not knowing which password manager to use (48%, +2 from 2023).
> 3. It is unnecessary to use a password manager if it isn’t required (41%, +1 from 2023).
> 4. Not trusting password managers (39%, same as in 2023).
> 5. Not understanding how to use it (38%, +3 from 2023).

What about those “lack of trust” responses, eh? We were curious too. We asked those people to tell us, in their own words, why the suspicion? The primary concern was the fear of the password manager getting hacked, which they perceive would give cybercriminals access to all their passwords.

Many preferred traditional methods (shout out to the trusty notebook), believing these to be more secure. Some found password managers too complex or cumbersome, while others distrusted third-party services or technology they didn’t pay for. Centralization of passwords, mistrust in cloud-based security, and a preference for personal control were also common themes.

Want to go deeper into the distrust? Here’s a selection of insightful, unfiltered comments from our participants themselves:

> **Don’t need to use one, passwords all in my head, can manage my own, another expense not needed with rising costs of living and no payrise.** PS1203, United Kingdom 😳

> **I’ve seen how cloud based apps often have poor security practices. I do not trust cloud based apps at all. May as well leave my passwords in a shoebox outside.**
> PS2812, United States

> **Because scammers are now so intelligent that they might crack the password manager and thus get to my passwords.** PS7909, Germany

> **If it gets cracked for any reason, it would be like hitting the lottery for cybercriminals.** PS8193, Germany

> **I only trust my notebook. I have no trust in using any other method. My notebook is quickly accessible.** PS8714, Germany

> **I can’t handle a password manager. Therefore, I don’t trust it because I fear my data might be accessible to criminals due to my own mistakes. Additionally, password managers (e.g., Firefox) are extremely complicated and cumbersome.**
> PS8730 Germany

> **I don’t trust technology that I don’t have to pay for, but I don’t want to spend money on it either.** PS8880, Germany

> **I think it has the potential to be hacked and a safer alternative is to write them down in a notebook at home.**
> PS9451, Canada

> **There will always be a 'bad actor' who eventually manages to exploit these vulnerabilities.** PS9258, Canada

> **If hackers can get into online systems, what stops them from hacking password managers. The chances of someone breaking into my home, finding my list of passwords and then using them is much lower than someone hacking into an online system and getting them.**
> PS9743, Canada

> **Memorised passwords mean one person (me) who can access an account; a password manager puts an unnecessary layer in the process, and adding layers adds vulnerability.** PS190, New Zealand

So there you have it. An array of arguments against password managers, but it mainly comes down to complexity, control, and safety.

We wandered pretty far down the password path, and rightly so, as it's a key aspect. But it's not the only one.

Next, let's leap from one login topic to another: multi-factor authentication, or MFA: How are people using it, and what do they think about it?

7.2 Enabling multi-factor authentication (MFA)

Multi-factor authentication (MFA) is a security measure that adds an extra layer of protection to online accounts. In this section, we explore participants' usage and perceptions of MFA, as well as the authentication methods they prefer.

> ***An epic 81% of participants have heard of MFA. That's 11% more than last year!***

First off, some encouraging news: An epic 81% of participants have heard of MFA (Figure 62). That's 11% more than last year! (Excuse us while we break out the fancy coffee and do a victory lap around the break room.)

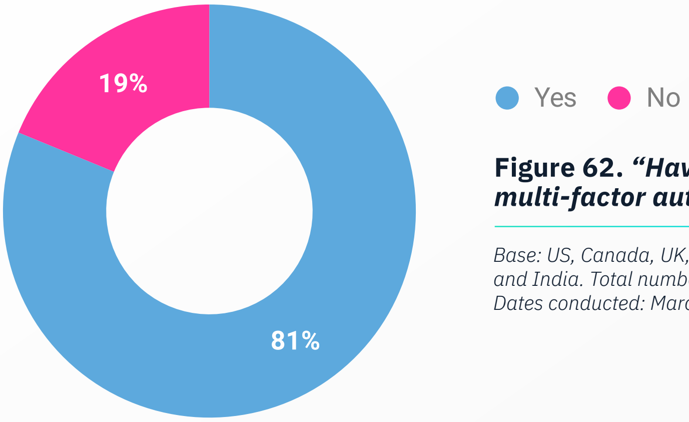


Figure 62. *"Have you ever heard of multi-factor authentication (MFA)?"*

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants: 7012 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

Ready to slice and dice by age bracket? The majority of Millennials (87%) and Gen Z (86%) have heard of MFA, compared to 51% of the Silent Generation (Figure 63). Aside from a drop in awareness within the Silent Gen (down 8% from 2023), all ages saw an increase in awareness of MFA. This uptick was between 8% and 11% for all groups, with the highest increase for Gen X.

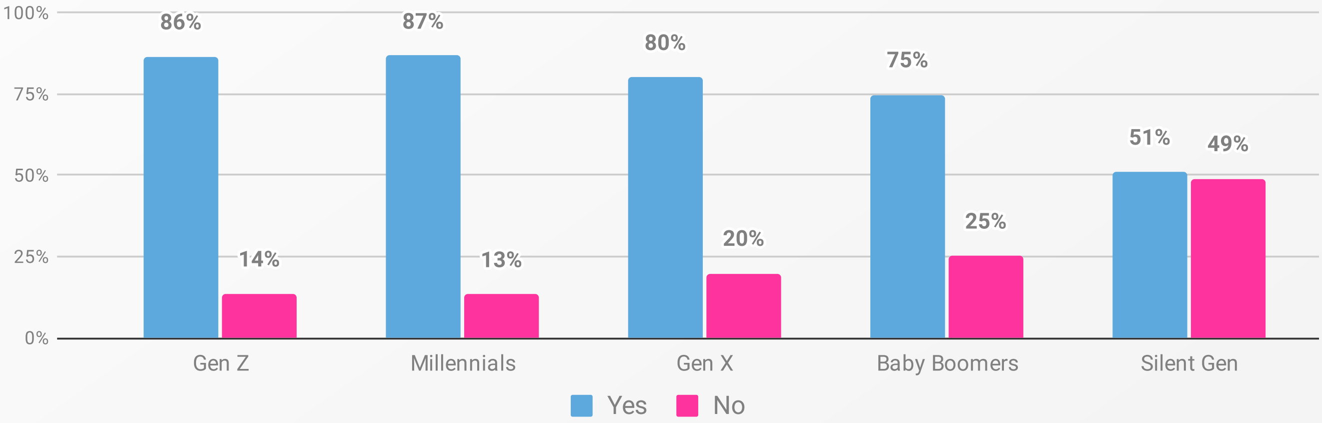


Figure 63. *"Have you ever heard of multi-factor authentication (MFA)?"* by generation.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants with generation information: 6749 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

But beyond awareness, what about adoption? Well, among those who had heard of MFA, 66% knew how to use it and were doing so, while 24% (a 9% increase from 2023) either don't use MFA or stopped using it despite knowing how to (Figure 64).

Boomers and Gen X are the ultimate MFA usage champions (71%, and 70%, respectively), followed by the Silent Gen (68%), Millennials (65%), and finally, Gen Z (56%). The highest percentage of those either not using MFA or stopped using it despite knowing how to were also from Gen Z, with 21% and 14% respectively. Not knowing how to use MFA was highest among the Silent Gen (16%), and lowest among Millennials (8%).

Interestingly, the percentage of people who've given up on MFA after using it has more than doubled since last year (16%). This suggests the issue might not be a lack of awareness or knowledge but rather other factors driving users away from a technology that's supposed to keep them safe. We will absolutely come back to this later.

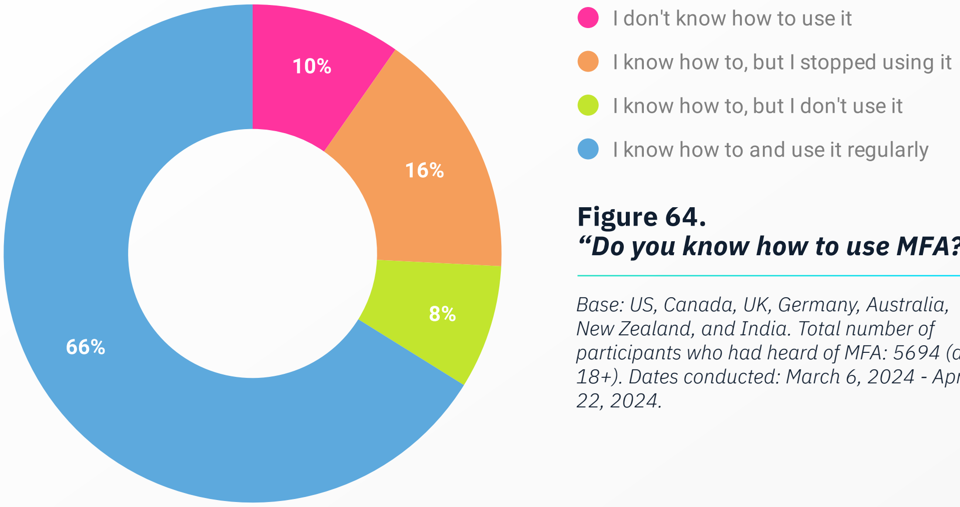


Figure 64.
"Do you know how to use MFA?"

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants who had heard of MFA: 5694 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

This year, we delved deeper-than-deep into participants' login methods and preferences by asking a few more MFA-related questions. We listed thirteen different methods (for primary and secondary verification) and asked participants which ones they use (Figure 65). No shockers here: the classic passwords/passphrases option is the most popular (79%), followed by PINs (60%), codes from text messages (57%), codes from emails (50%), fingerprints (37%), and facial recognition (31%). The least common methods were USB devices (3%), smart cards (4%), and token devices (5%).

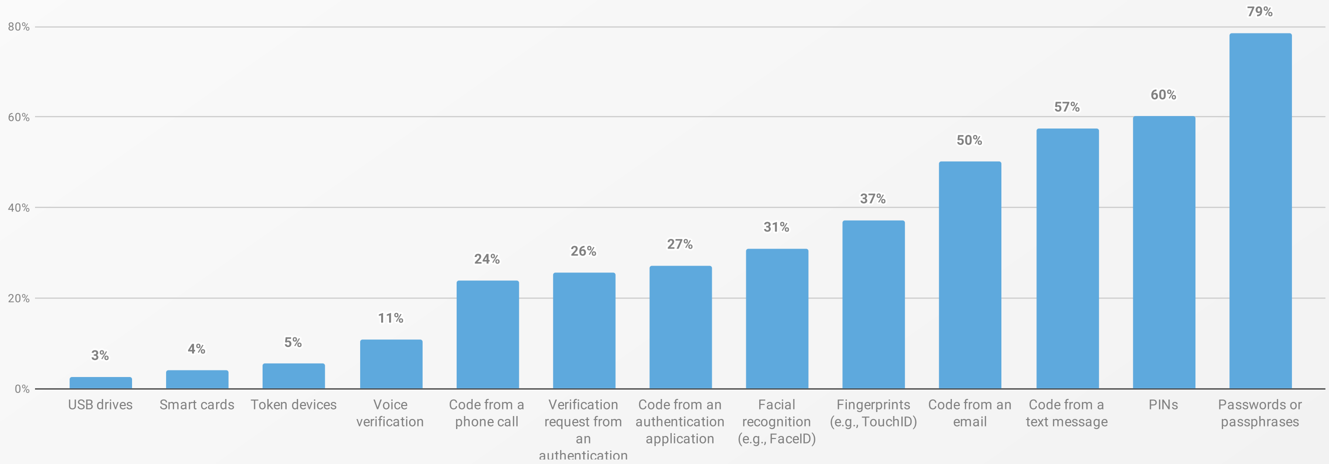


Figure 65. *"Which of the following methods do you use to log in to your online accounts?"*

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants: 7012 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

Unsurprisingly, passwords were the most common login method used across all generations, with usage increasing with age, from 68% of Gen Z to 94% of Silent Gen. Younger generations are, it seems, more open to less traditional login methods. For example, 43% of Gen Z used facial recognition, compared to only 19% of Baby Boomers and 16% of the Silent Generation. Although the percentage is small, younger generations were more likely to use token devices (8% of Millennials and 7% of Gen Z, compared to 2% of Baby Boomers and 1% of Silent Gen) and smart cards (7% of Millennials and 5% of Gen Z, compared to 2% of Baby Boomers and 1% of Silent Gen).

The rate of adoption of code-based MFA methods—such as those delivered via text messages and emails—is worth noting. This is likely (at least in part) down to how easy they are to set up, as well as their integration with existing communication channels. Additionally, younger generations show a greater propensity for adopting newer, less traditional login methods. Does this signify a trend towards more diverse practices in the future?

Let’s dig deeper into the second authentication factor: which methods are the most convenient to use?

Over half of the participants (54%) said using a code from a text message was their top method for convenience (Figure 66). This was followed by code from an email (19%), and code from a phone call or authentication apps (both at 8%).

The trend held true across the generations, with text message codes holding the top spot for all ages. Specifically, 47% of Millennials to 59% of Baby Boomers preferred text message codes. However, the Silent Gen found phone call and email codes equally convenient, with 17% selecting either option.

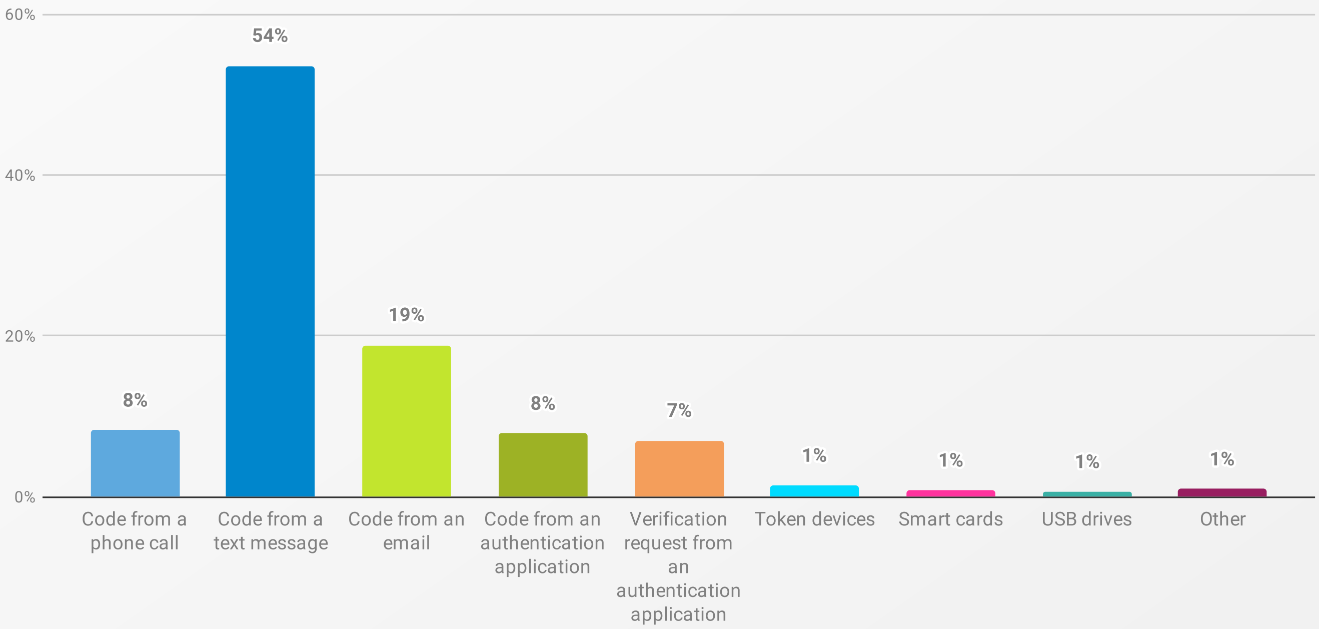


Figure 66. *“After entering your password/passphrase to log into a website or app, you may be asked to use another method to verify your identity. Which one of these would you find MOST convenient to use?”*

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants: 7012 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

On the flip side, which methods are the LEAST convenient? USB devices had the dubious honor of coming out on top (22%), followed by code from a phone call (19%), code from a text message (13%), token devices (12%), and code from an email (11%). All generations were united in their aversion to USB devices, ranging from 18% of both Gen Z and Millennials to 25% of Baby Boomers. This was followed by code from phone call and code from text message (both 17%).

Younger generations, specifically Gen Z, found codes from a phone call and from a text message the least convenient (both 17%). Elsewhere there were notable differences in the percentages across all other generations. For example, 16% of Baby Boomers would find phone calls the most inconvenient authentication method, whilst 8% said they felt the same about text messages.

To further investigate, we also asked regular MFA users (N=3766) where they have enabled MFA (Figure 67). Understandably, banking and finance apps and sites came top of the list (81%). Forty-six percent used MFA on their personal email accounts, and only 39% enabled it on work websites/apps including emails. Work social media websites (e.g., LinkedIn) were the least popular for enabling MFA, with only 22% doing so.

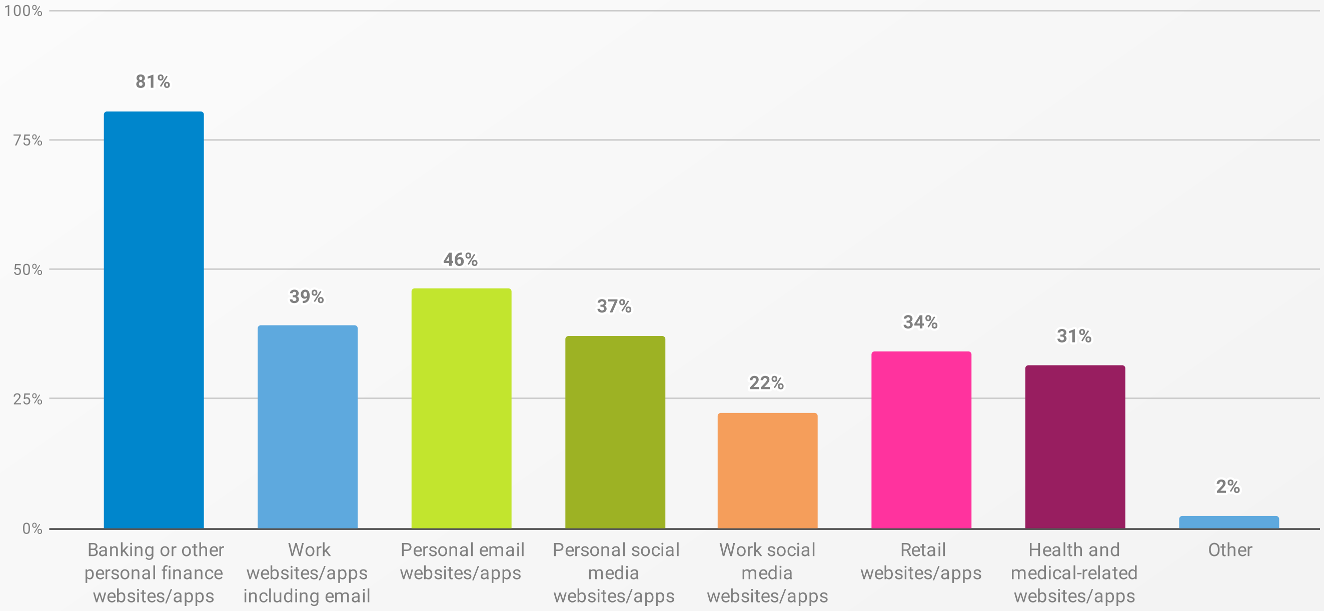


Figure 67. *"Where have you enabled MFA?"*

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants who use MFA: 3766 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

And how about those MFA-free folks? Of the 1374 participants who had stopped using MFA or never started, 28% felt their password was strong enough and 21% said they don't carry their phone with them all the time to be able to verify. A further 19% felt MFA takes too long, and 17% didn't see MFA adding any extra protection.

Common qualitative responses, based on the 3% (N=42) who provided them, included annoyance, it being a "pain to use," laziness, and previous negative experiences deterring usage.

> **It [MFA] annoys the heck out of me!!** PS8424, Canada

Additionally, of those not using, stopped using, or not knowing how to use MFA (N=1928), 42% said they would, but using it won't stop cybercriminals, while a further 37% would use MFA, but they don't understand how. Thirty-five percent of participants said they lacked confidence in their ability to use MFA, don't have the time for it, or believe it is unnecessary if their device functions properly.

The verdict? While awareness of MFA has increased, we're not popping the champagne corks just yet. Actual usage of MFA remains varied across generations. Millennials and Gen Z are the most aware of it, but the older generations are actually using it more.

> ***A considerable portion of participants either do not use it or have stopped, often citing inconvenience.***

Despite the known security benefits of MFA, a considerable portion of participants either do not use it or have stopped, often citing inconvenience, the belief that their password is good enough on its own, or a lack of understanding. Text messages are a clear winner in MFA methods, with USB the least loved. And MFA is used most for financial and banking functions over work and socials. All useful things to bear in mind when considering deploying MFA in your neck of the woods.

The security community still has a long way to go to encourage the widespread adoption of what is likely the most effective way to prevent account compromise.

Increasing MFA adoption

Our top five ways to boost MFA adoption are:

Prompting packs a punch: Simply prompting people to set up MFA will get the job done for at least some people. Don't overlook this as a first step.

Fight the friction: People hate hold-ups, so minimizing hassle is key to making MFA adoption stick. Yes, yes, we know apps are more secure than texted codes, but 70% of a workforce using texted codes is more secure than 40% of a workforce using an app. MFA perfection doesn't exist.

Sell the idea: Unless people understand the 'why' behind something, they won't be interested. Sell the benefits, sell the "why" (how does it help me) ... and point out what might happen if they don't use MFA.

Offer incentives: Who doesn't love being rewarded? Consider some small perks you can hand out to recognize those who choose to activate MFA.

Build trust: Setting up MFA can mean parting with personal data. That's why trust is a crucial part of the picture. It's okay to recognize this natural discomfort and to support people through it.

www.cybsafe.com/blog/spotlight-have-you-got-multi-factor/

https://staysafeonline.org/resources/mandate-mfa-take-a-bold-step/

7.3 Installing software & app updates

Change is the name of the game. New software rocks up, bugs pop up and get swatted, and inevitably vulnerabilities arise. It's these vulnerabilities that make enabling auto-updates so important—but that doesn't mean everyone does—(WannaCry ransomware attack, anyone?).

Anyway, what's up with updates in 2024? While 63% (-2% from last year) of participants said they know how to install the latest software and application updates across their devices (Figure 68), 17% said they don't. Then there's the 20% who said they knew how to, but tended not to install the updates, representing a 3% increase from 2023. The gap between awareness and action is widening, it seems. Yikes.

Also under the 'yikes' tab is a continuing trend of participants being less proactive about installing software and app updates, with a 3% decrease from last year, resulting in only 57% of participants reporting they 'always' or 'very often' install updates when notified. And, same as last year, 4% (N=307) claimed they never updated their devices.

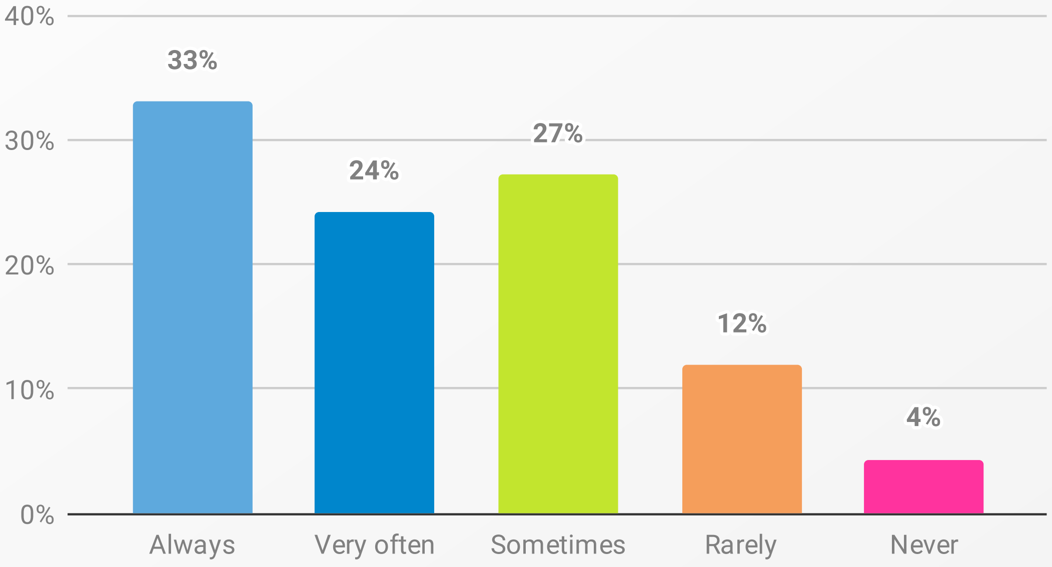


Figure 68 ***"How often do you install the latest software or application updates to your devices when notified that they are available?"***

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants: 7012 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

Leading the update charge are the Baby Boomers, with 66% of them performing the 'always' and 'very often', followed by 59% of Gen X. Compared to them, Gen Z seems less bothered about updates (44%). The Silent Generation has the highest proportion of rare updaters (19%).

> ***People know software updates are important, but they stop short of actually installing them, or put it off.***

Among those who update their devices at least sometimes (N=5871), 45% have turned on automatic updates, consistent with last year's data. Additionally, 8% perform updates when they are away from or not using their devices, and 16% tend to click 'Remind me later,' which is a slight decrease of 1% from 2023—hey, we'll take it.

So what's the bottom line here? There appears to be a persistent disconnect: People know software updates are important, but they stop short of actually installing them, or put it off. This discrepancy is particularly pronounced among younger generations, such as Gen Z. And, perhaps most baffling of all, despite the convenience of automatic updates, only 45% have enabled them.

Updating devices

So, how to encourage people away from the temptation of 'I'll do it later/never'?

Make auto-update the default: We naturally "go with the flow", so if auto-updates are presented as the default option, people are more likely to enable them. It's a quick, easy win no matter your organization's size or style.

Tireless testing: There's nothing more frustrating than a bug-riddled update. Rigorously test updates before roll-out to avoid denting people's trust in updates.

Flexibility is your friend: Give people some control. Allowing updates to take place over lunch or at the end of the day means people retain control of their workday without sacrificing security.

https://staysafeonline.org/resources/software-updates/

www.cybsafe.com/blog/why-are-you-snoozing-updates/

7.4 Backing up data

Backing up data. A simple concept that can save us from the misery of file corruption, hardware failures, ransomware, and soften the blow of physical disasters like fires and flooding. What did our participants have to say about it?

The good news? Forty-five percent (a 3% increase from 2023) of participants reported they 'always' or 'very often' back up their important data (Figure 69). A further 32% (same as in 2023) reported backing up their data 'sometimes'. Twenty percent (-2% from 2023) reported that they 'rarely' or 'never' make backups.

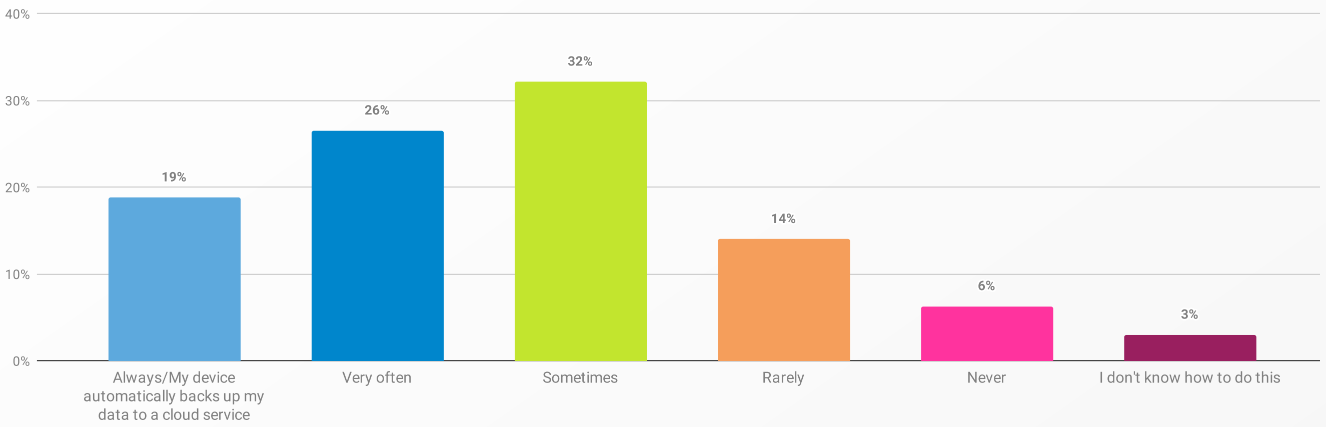


Figure 69. *"How often do you back up your most important data?"*

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants: 7012 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

Performing backups 'sometimes' was the most common response across generations (ranging from 31% of the Silent Gen to 36% of Gen Z), except for Baby Boomers, where the majority (27%) back up 'very often'. Following this trend, Baby Boomers also had the highest proportion who always back up (21%), followed by 19% of Gen X, and 18% of Millennials and Gen Z. Never backing up, or not knowing how to do so, was highest among the Silent Gen (with 13% and 9%, respectively).

Boosting backups

Backups can be super helpful in protecting data...but only if they're actually done. Here are some ways to bring better backup practices to your organization:

Automate it: Embrace solutions that automatically back up. Cloud services are extra convenient, meaning higher adoption rates.

Sell the simplicity: Just because something is easy, it doesn't mean people know it's easy. Shout about how smooth and simple the process is. Help people to understand.

3-2-1, back up!: We like the 3-2-1 rule for sensitive data: Make three backups, over two devices, and keep one offsite. Remove a barrier to this approach by handing out encrypted flash drives.

Build a backup culture: Make auto-backup part of your organization's DNA. A no-brainer security essential. Something you can't afford not to do.

Praise the backup champions: Recognize those who are on top of their backup game, and nudge those who aren't. It's as simple as regular monthly email reminders.

www.cybsafe.com/blog/how-to-make-data-backups-a-regular-part-of-everyones-day/

https://staysafeonline.org/resources/back-it-up

7.5 Recognizing & reporting phishing messages

Phishing attacks are a menace—and they're still on the rise. And while the classic phishing email still manages to pull in a decent number of victims, cybercriminals continue to up their game and evolve their tactics to land hauls. How are people holding up against this multifaceted threat?

7.5.1 Recognizing phishing messages

Let's face it, some phishing attacks are laughably conspicuous. A typo here, a blurry logo there, a sender name that sounds like AI made it up (probably because it did). But not all attempts stick out like sore thumbs.

Confidence check time. Overall, participants reported high confidence in their ability to recognize phishing emails or malicious links (M=7.12, SD=2.1, N=7012). Specifically, 67% (a 1% increase from 2023[33]) of participants felt confident in their abilities. Still, 10% (a 3% drop from last year) report not feeling confident in their abilities to identify malicious emails or links.

Millennials (76%, Figure 70) felt most confident in identifying malicious messages, representing a 6% increase from 2023. This was followed by Gen Z (69%, +10% from 2023) and Gen X (66%, -2% from 2023). Older generations—Silent Gen with 17% and Baby Boomers with 14%—reported the lowest confidence levels and felt less confident than last year, with 3% and 4% decreases respectively from 2023.

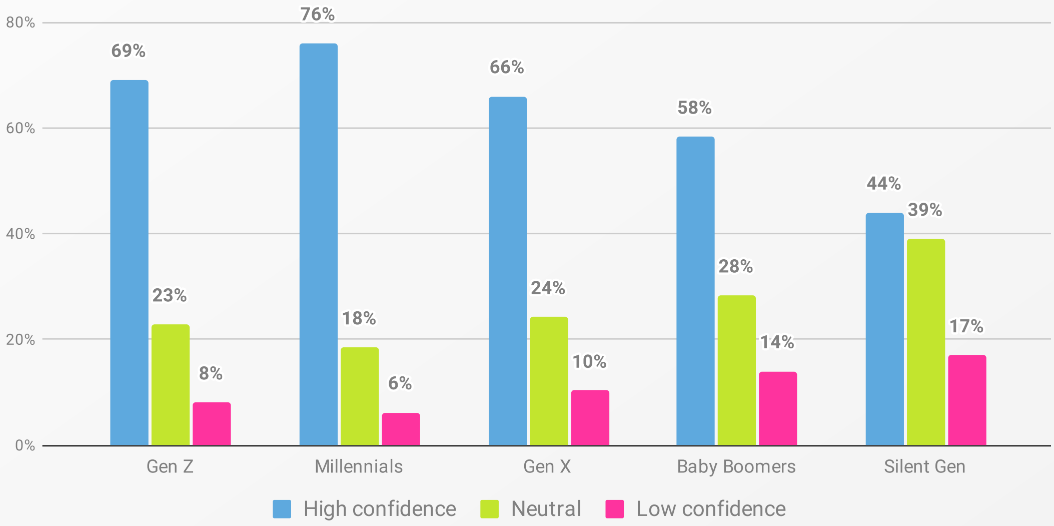


Figure 70. *"How confident are you in your ability to identify a phishing email or a malicious link?"* by generation.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants with generation information: 6749 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

[33] In the *Oh, Behave! 2023* report, participants' levels of confidence were categorized into five categories. For simplification, effective reporting, and consistency, the same confidence scale has been consolidated into three categories in this year's report.

We asked participants with lower confidence (N=1412)[34] to explain in their own words why they feel that way. The analysis of this rich qualitative data revealed many participants struggle with the increasing sophistication of phishing attempts, possibly due to the use of artificial intelligence (AI). Many pointed to the difficulty distinguishing legitimate emails from cleverly designed scams. They acknowledged their lack of confidence stems from constantly changing phishing tactics, with scammers using ever-increasing complexity and new methods, making it difficult to keep up with the latest tricks.

> ***Many participants struggle with the increasing sophistication of phishing attempts, possibly due to the use of artificial intelligence (AI).***

The perception that cybercriminals are a step ahead, constantly innovating their methods, is alive and well. This feeling of helplessness discourages some from even trying to identify phishing attempts. Then there's the FOMO factor, with some people tempted to click on suspicious links due to fear of missing out on a legitimate offer or deal. Others acknowledged their own shortcomings—in computer skills and lack of knowledge or experience—that make it difficult for them to pick up on the subtle clues that differentiate a real email from a cleverly crafted phishing attempt.

Behind this low confidence are various feelings, beliefs, and attitudes, as illustrated by participants' quotes below.

> **I get so many emails per day, it's hard to be on alert. Also, it seems as though ways to identify change all too frequently.**
> PS273, United States

> **Because every time I think I might be secure there's a new type of scam or hack that I hadn't thought of.**
> PS1498, United States

> **There are always new ways that hackers are adding to their arsenal and new ways they are trying to trick us. They keep making it harder and harder to differentiate between fake and real emails and links.** PS8629, Canada

> **AI is unpredictable.** PS9005, Germany

[34] This question was asked of those who rated their confidence level 1-5 on a 10-point scale.

I know the drill, but the tactics are always changing. I hear of intelligent, industry-aware people getting conned all the time. PS2754, United States

I receive spam and fraud emails at least once a week. I've learned to never open these emails and just delete them. Sometimes I report them but I don't know if anyone does anything about them. PS8811, Canada

So far, I've always recognized something like this, but there's always something new, so I'm not 100% sure I always recognize everything. PS7909, Germany

Sometimes the timing of phishing emails is very coincidental, such as phishing emails from a fake post service asking for details when I have ordered something through post a few hours/days ago. This makes it confusing and difficult to know what is fake and what's real sometimes. PS7353, Australia

Other than obvious characteristics in the email, I wouldn't be able to pick them out from my emails. Some can be really tricky. PS651, New Zealand

Scammers are pretty good at hiding these types of links. Although I would never click any odd link, I am still not confident in identifying phishing links. PS762, New Zealand

Because I don't even know what phishing means and I do sometimes get nervous when I open an email and not sure how to know if it is malicious. PS1214, New Zealand

Every day scammers learn how to copy real company texts and emails to a shocking degree. Anybody can fall victim to an absent minded click. PS920, New Zealand

Because I presume that fraudsters are always one step ahead of us and they have an infinite number of chances but we just have to lose guards once to fall down. PS687, India

Let's look at specific actions and behaviors—how often do participants inspect emails and links, and what steps do they take to verify them?

Similar to 2023, 67% reported 'always' or 'very often' checking their messages (e.g., emails, texts, or social media) for signs of phishing before clicking any links or responding to them (Figure 71). Ten percent (-4% from 2023) reported 'never' or 'rarely' doing so, and 2% admitted not knowing how to identify phishing emails.

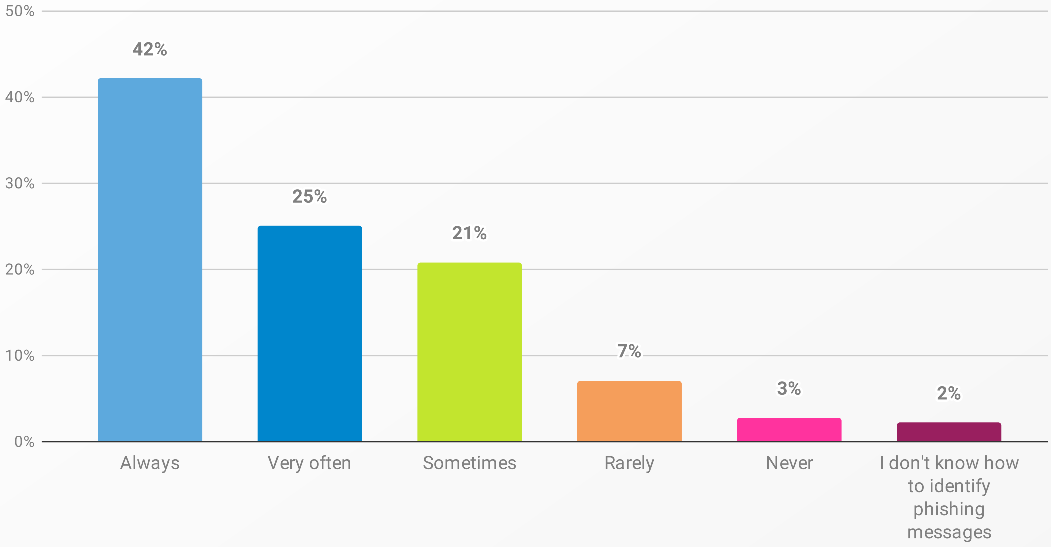


Figure 71. Frequency of checking messages for signs of phishing before taking action.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants: 7012 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

The picture is more intriguing if we look at the results by generation. The majority of Baby Boomers (78%) and Silent Gen (70%) reported 'always' or 'very often' inspecting their messages, in comparison to only 55% of Gen Z.

Conversely, most likely to only 'sometimes' check their messages were Gen Z (30%) and Millennials (25%). The highest percentage of those never or rarely checking messages or don't know how to do it were from the Silent Gen (16%, and 5%, respectively).

This year, we got our big magnifying glass out to uncover more intel on the steps people take to verify the legitimacy of emails and websites. Let's start with emails.

The most popular steps taken to verify the legitimacy of emails were checking for poor spelling and grammar errors (63%), verifying the email is from a legitimate email address (61%), and identifying if the email requests personal or sensitive information, like bank details (59%, Figure 72). Among the 2% (N=124) of 'Other' responses, some participants mentioned using intuition-based methods, often described as a 'gut feeling,' to detect suspicious emails.

Younger generations were more likely to check whether an email is from a legitimate address (with 56% of Gen Z and 59% of Millennials doing so), while the majority of older generations tended to focus on detecting poor spelling and grammatical errors (with 75% of Baby Boomers and 79% of Silent Gen using this approach). Additionally, a larger percentage of younger generations checked whether the email contained links directing to legitimate sources, with 44% of Millennials and 43% of Gen Z engaging in this practice, compared to 34% of Baby Boomers and 26% of Silent Gen.

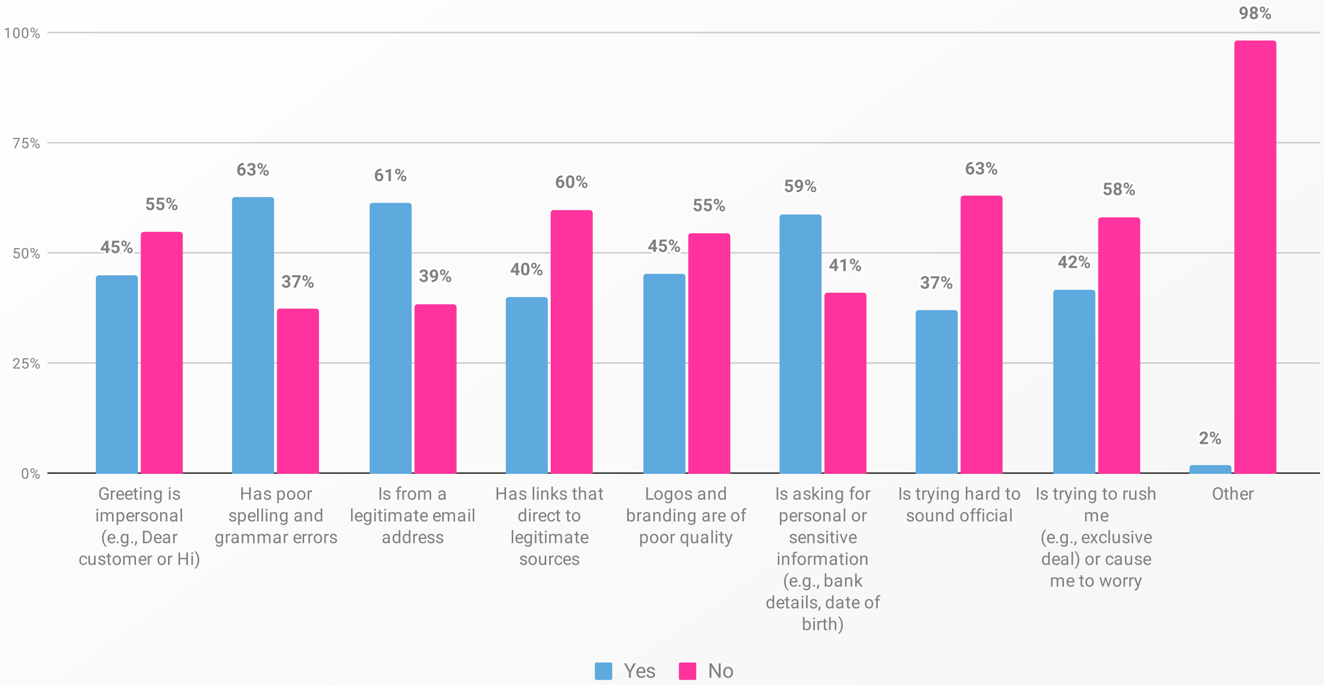


Figure 72. Steps taken to identify email legitimacy – *"I check whether the email…"*

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants: 7012 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

While 61% reported checking the sender's email address, how frequently do they reach out to the sender for verification if unsure?

Twenty-seven percent (a 5% decrease from 2023) admitted to 'never' or 'rarely' doing so, whilst 45% (-1% from 2023) reported contacting the sender either 'very often' or 'always' to ask about a potential phishing message before click the link or opening the attachment (Figure 73).

What's more, older generations are more likely to reach out to the sender, with 52% of Baby Boomers and 48% of Silent Gen reporting that they do so 'very often' or 'always', compared to 39% of Gen Z. On the other hand, 'never' or 'rarely' contacting the sender is most common among the Silent Gen (34%), followed by Gen X (28%) and Gen Z (27%). Interestingly, Gen Z leads in 'sometimes' reaching out at 33%, with this tendency decreasing across older generations.

Overall, while a notable portion of participants check the legitimacy of the sender's email address, alternative verification steps are potentially underutilized, especially among younger participants.

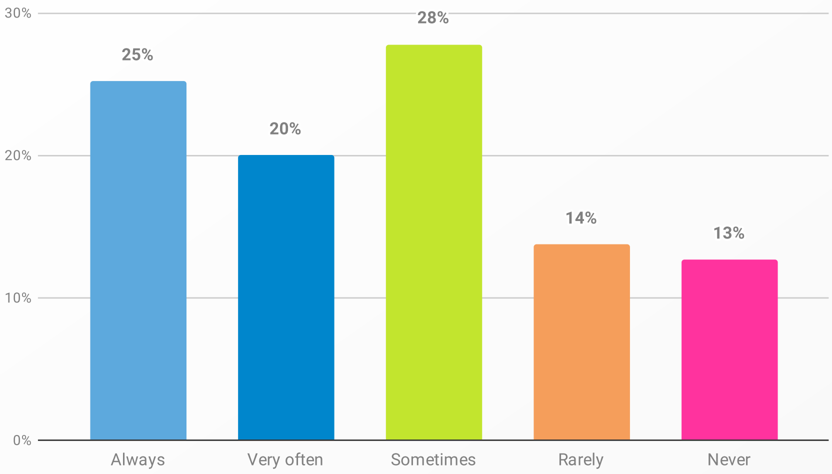


Figure 73. *"If someone you know sends you a message you're unsure of (a potential phishing message), how often do you reach out to the person to ask about it before you click the link or open the attachment?"*

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants: 7012 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

Websites next (the fake variety). What steps do people take to identify them (Figure 74)? The top verification methods for websites were checking for "https:" in the address bar (58%), checking for a padlock security symbol in the address bar (47%), and analyzing the overall look of the website (46%).

While checking for "https:" in the address bar was the most common step across all generations (ranging from 52% of Gen Z to 64% of Silent Gen), the second most popular method varied by generation. For younger generations, analyzing the overall look of the website was the second most common verification method (45% of Gen Z, and 47% of Millennials), while for older generations, it was checking for a padlock security symbol in the address bar (42% of Silent Gen, 50% of Baby Boomers, and 48% of Gen X).

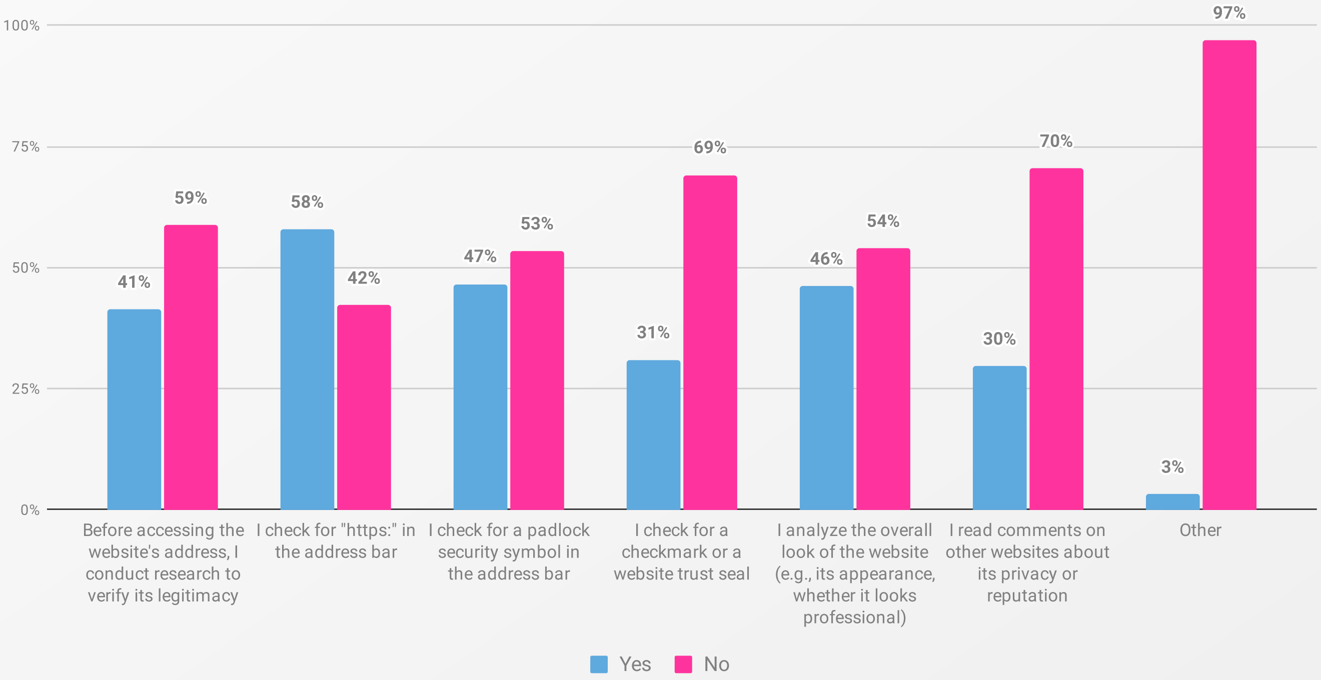


Figure 74. Steps taken to identify website legitimacy.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants: 7012 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

If you're reading this, chances are you don't need us to point out these indicators are far from foolproof. Malicious websites can also display these signs. But while researching the website is a more effective and comprehensive approach to verification (as it involves checking for detailed information about the site's ownership, reviews, and reputation), the data reveal this method is less commonly used, especially among older generations.

Let's end on a positive note though: Research[35] from a decade ago revealed people often ignore browser-based cues when identifying maliciousness, leading to higher susceptibility. Although some indicators, like HTTPS, have become less relevant over time, our findings show at least some participants are now paying attention to these cues.

7.5.2 Reporting phishing messages

What happens when people spot a phishing email? Do they use the 'spam' or 'report phishing' buttons to report it? Or do they do...nada?

Despite a 3% increase from 2023, still less than half of the participants (47%, Figure 75) said they 'always' or 'very often' report phishing. Less than a quarter (21%, down by 4% from 2023) mentioned they 'never' or 'rarely' report it. The same as 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 is still 29% (down by 4% from last year) who are not taking action against cybercriminals. Not exactly ideal.

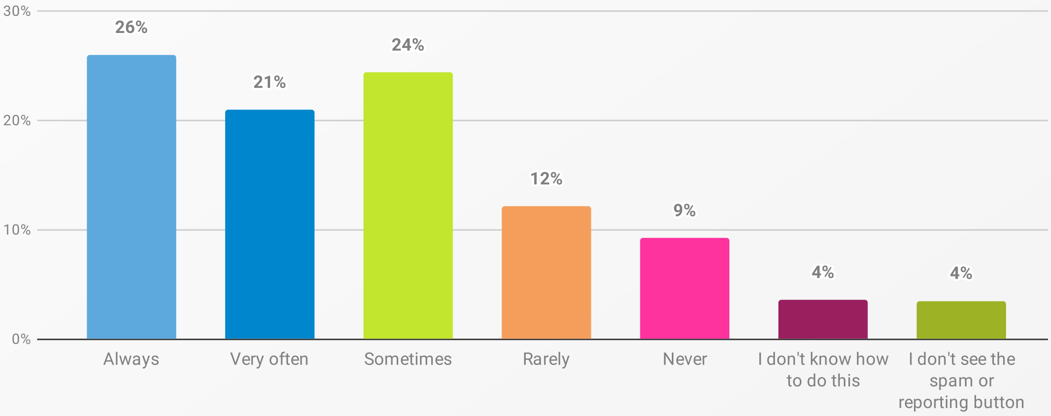


Figure 75. *"How often do you report phishing messages by using the 'spam' or 'report phishing' button?"*

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants: 7012 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

The 30%...why aren't they reporting phishing attempts? Among those (N=1500) who 'never' or 'rarely' report phishing messages, 71% agreed they would do so if it helped to stop cybercriminals. A further 68% would report phishing if it would stop spam messages from getting into their inbox. Additionally, 60% claimed they would report phishing if something would happen as a result.

[35] Iuga, C., Nurse, J. R. C., & Erola, A. (2016). Baiting the hook: factors impacting susceptibility to phishing attacks. *Human-centric Computing and Information Sciences, 6*, 1-20.

> ***The belief that reporting [phishing] doesn't stop cybercriminals was most common among Millennials (71%), Gen X (69%), and Baby Boomers (74%).***

But how does that motivation break down across the generations? There's an unusual pattern here: The belief that reporting doesn't stop cybercriminals was most common among Millennials (71%), Gen X (69%), and Baby Boomers (74%). Sidequest: why?

Meanwhile, the youngest and oldest age groups were united by their quest for Inbox Zero, with a huge 78% of the Silent Gen and 69% of Gen Z willing to report phishing if it would stop spam messages from reaching their inbox.

So while progress rolls on slowly, there's plenty more work to be done, and many people choose inaction in the face of phishing, in spite of convenient reporting tools like the 'spam' or 'report phishing' buttons. A widespread skepticism still remains about whether reporting can effectively stop cybercriminals, and a desire for more tangible outcomes arising from their reporting efforts - like recognition!

Staying safe from phishing

Like that person in the supermarket who wants to talk to you about the price of eggs, phishing is set to continue to bother us all for years to come. But we can reduce its impact with some straightforward actions:

Train people to spot the signs of phishing: Keep the messaging simple, encouraging people to ask themselves:
1. Do the 'From:' details match the sending details?
2. Does it ask you to carry out an action you wouldn't usually do?
3. Does it include a link or attachment you don't recognize?

Go beyond click rates...find out why people click: Measure why people click on simulated phishing emails. This can be done with point-of-click or post-click surveys, or by baking influencing techniques into simulated phishing templates. Once you know why, you can tailor support to address it.

Create an environment that encourages reporting: Make your reporting process quick and frustration-free. Quickly provide acknowledgement of the report. Follow up with feedback on what action is taken. And keep it positive, avoiding a blame culture (e.g., assigning training to people who click on simulates).

https://staysafeonline.org/theft-fraud-cybercrime/phishing

www.cybsafe.com/value/simulated-phishing

www.ncsc.gov.uk/guidance/phishing

8. Artificial intelligence (AI)

Certainly, here's an introduction for the AI section of the *Oh, Behave!* report...kidding! Just checking you're all still paying attention.

Also, if you skipped straight here, no judgment (as long as you go back and read the rest, obvs). We get it. AI's rapid advancement and integration into our daily lives has sparked significant discussions about its impact on cybersecurity attitudes and behaviors.

This section, brand new for 24/25, delves into the multifaceted relationship between AI and cybersecurity, examining how individuals use AI, their concerns, and levels of trust in AI-driven systems. It also explores participants' confidence in recognizing AI-generated content and the broader implications of AI on decision-making during elections, work productivity, and online security. By understanding these dimensions, we aim to shed light on AI's evolving role in enhancing and disrupting cybersecurity practices.

8.1 Usage & concerns

Over half (56%) of the participants don't use any AI tools (Figure 76). Of those who use it, 17% do so at home, 11% do so at work, and 16% use it in both settings. This discrepancy might be because people are more comfortable and open to trying new things and exploring its capabilities for personal tasks. Additionally, workplaces might have security protocols or concerns that limit people's access to AI tools...🤞

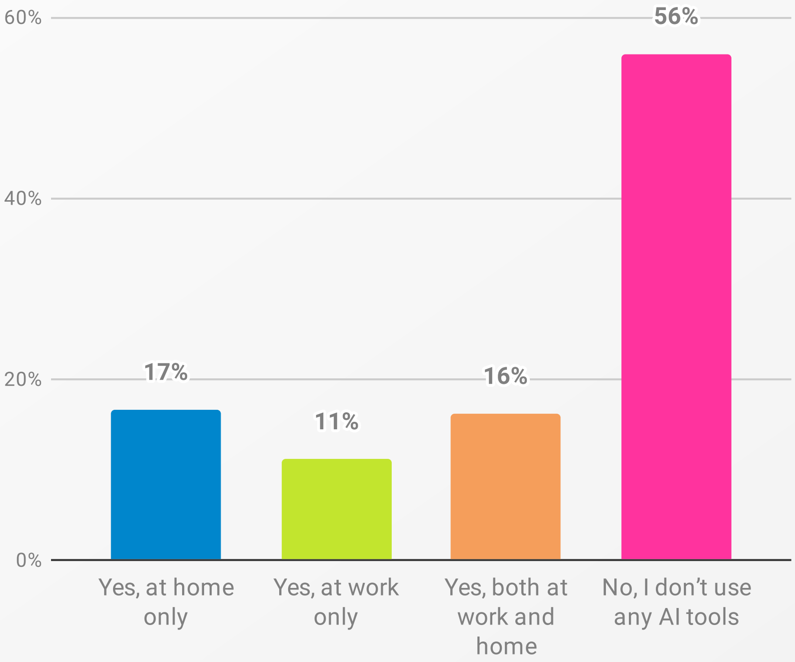


Figure 76. *"Do you use any AI tools at home or at work?"*

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants: 7012 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

The data show (Figure 77) AI tool usage is highest among younger participants, with 72% of Gen Z participants using it at work, home, or both. AI usage declines strongly as age advances: 62% of Millennials, 38% of Gen X, 15% of Baby Boomers, and only 7% of the Silent Generation report using AI tools.

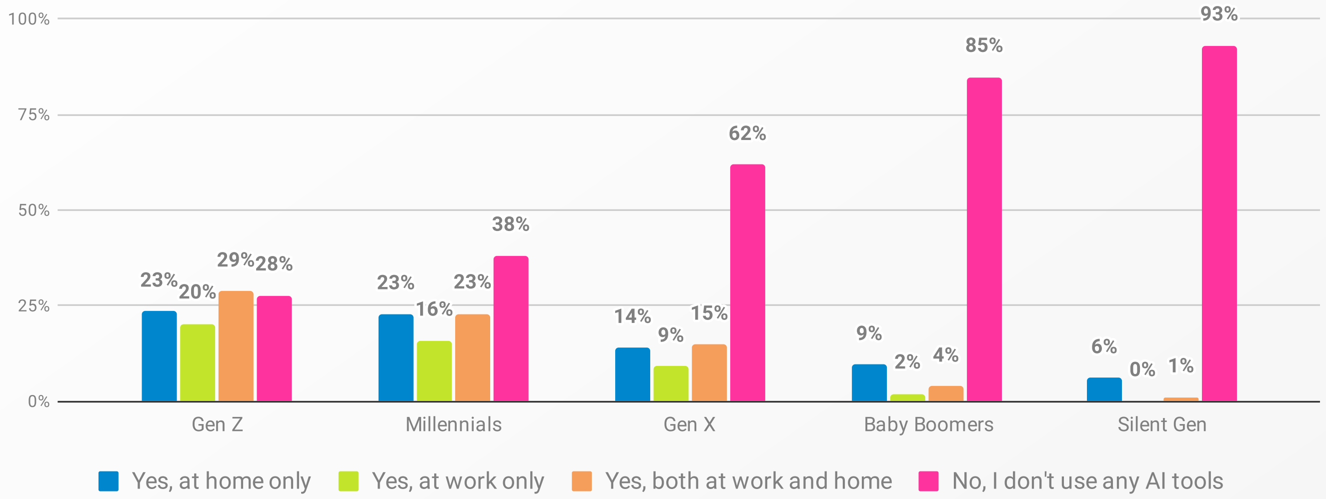


Figure 77. *"Do you use any AI tools at home or at work?"* by generation.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants with generation information: 6749 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

Overall, only 27% (Figure 76) reported using AI tools at work. As with overall AI usage, AI usage in the workplace also decreases with age. The highest percentage of workplace AI usage was reported by Gen Z (49%), followed by Millennials (39%), Gen X (24%), and only 6% of Baby Boomers (Figure 77). One possible explanation for this is that younger generations are more familiar with tech, and perhaps more open to trying emerging tools, as well as having very full online lives compared to their more mature counterparts.

Among those using AI tools (44%, N=3087), ChatGPT is the most popular, with 65% of participants reporting usage (Figure 78). Google Gemini (formerly Bard) follows with 30% usage, and Copilot with 19%.

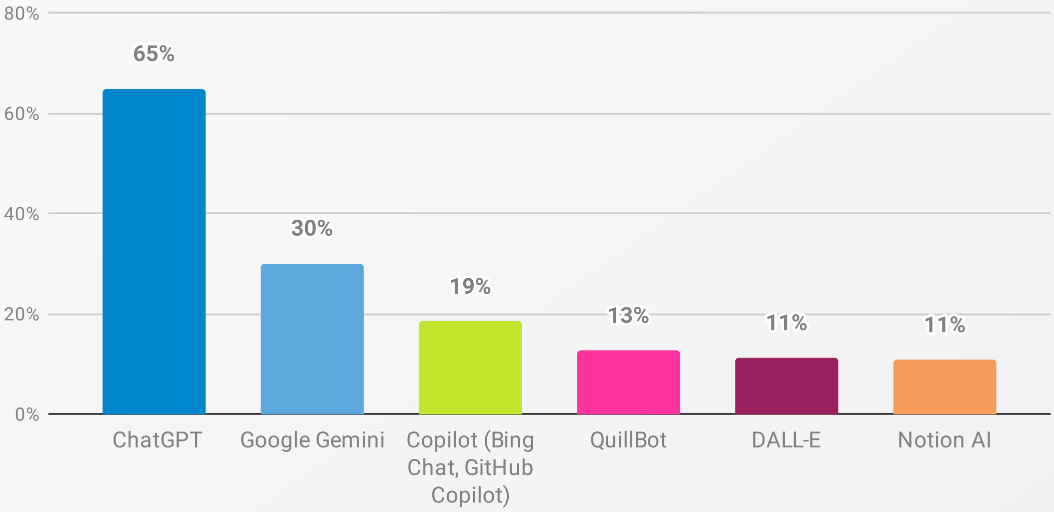


Figure 78. *"What AI tools do you use?"*

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants using AI tools: 3087 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

Alright, time to zero in on the security and privacy aspects of AI, because that's this report's focus, after all. We were particularly interested in exploring whether AI users (N=3087) received any training on the security and privacy risks associated with these tools. Fifty-five percent reported they had not. Breaking this down by employment status (Figure 79), the majority of those not actively employed (84%) and retirees (83%) have not undergone AI training, compared to 58% of students and 52% of employed participants.

> ***More than half of the employed participants and students have yet to receive any training on safe AI use.***

These findings suggest some workplaces and academic institutions are taking early steps to raise awareness of AI risk. However, there is a long way to go, as more than half of the employed participants and students have yet to receive any training on safe AI use.

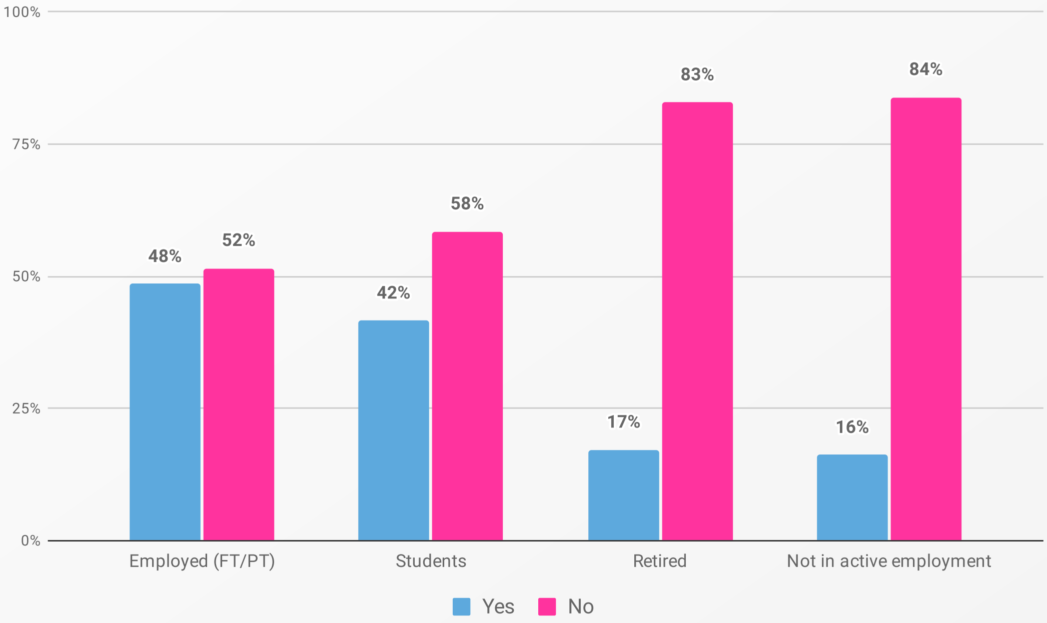


Figure 79. *"Have you received any training about the security and privacy risks of AI tools?"* by employment.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants using AI tools: 3087 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

Here's a big juicy (terrifying) stat. Among those using AI tools for work (N=1920), 38% have shared sensitive work information without their employer's knowledge.

> ***38% have shared sensitive work information [with AI] without their employer's knowledge.***

Perhaps not surprisingly, this was more prominent among younger generations (Figure 80). Specifically, 46% of Gen Z and 43% of Millennials admitted to sharing sensitive work information with AI tools without their employer's knowledge.

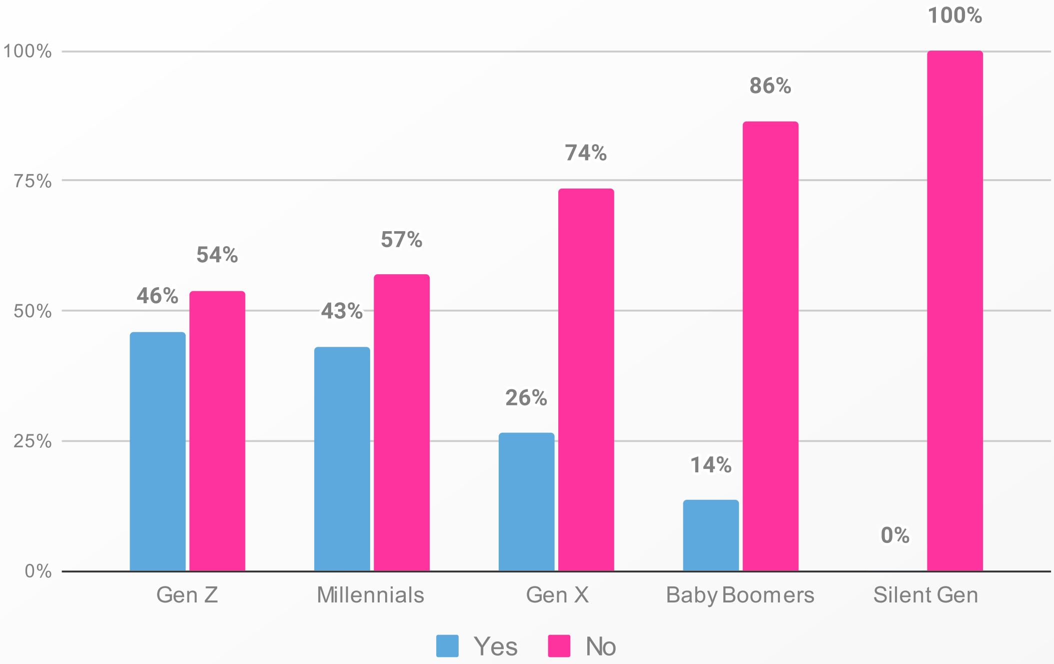


Figure 80. *"Have you ever shared sensitive work information with AI tools without your employer's knowledge?"* by generation.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants with generation information who use AI tools at work: 1862 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

How can this discrepancy be explained? Perhaps the training did not adequately cover security and privacy risks. Or participants chose not to follow the training guidelines, deciding the benefits were worth the risks. We know awareness doesn't guarantee action (i.e., doctors who smoke), and the scenario is playing out loud and clear with AI use.

Beyond AI usage and training, we also wanted to understand how participants felt about the potential risks associated with these tools. The majority of participants (65%) expressed concern about AI-related cybercrime (Figure 81). This aligns with our findings about the growing sophistication of phishing attempts, leveraging AI capabilities to make fake communications more convincing and harder to spot, as described by our participants.

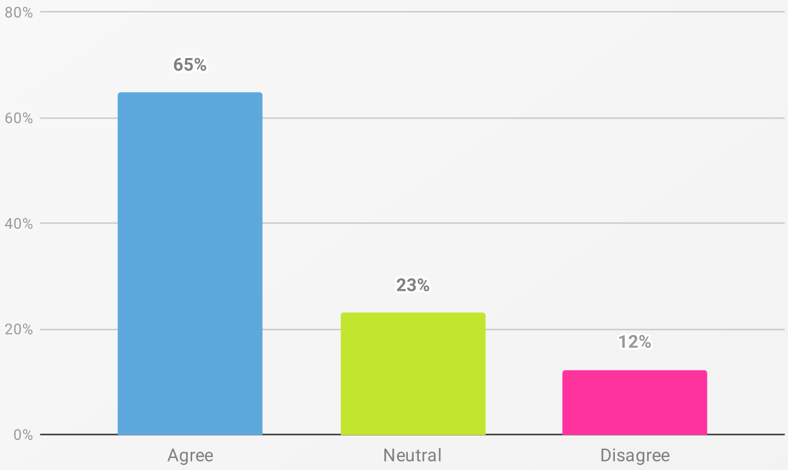


Figure 81. *"I'm concerned about AI-related cybercrime."*

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants: 7012 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

While concerns remained consistently high across generations (Figure 82), with the Silent Generation (73%) and Baby Boomers (70%) expressing the highest concern, Gen X seems the least concerned (61%) about AI-related cybercrime.

This generational gap might be down to younger generations' greater familiarity and comfort with technology, which gives them more confidence in managing and mitigating risks. Additionally, they may perceive the benefits of AI to outweigh the potential risks (as above), or feel they have a better understanding of how to protect themselves against the risks.

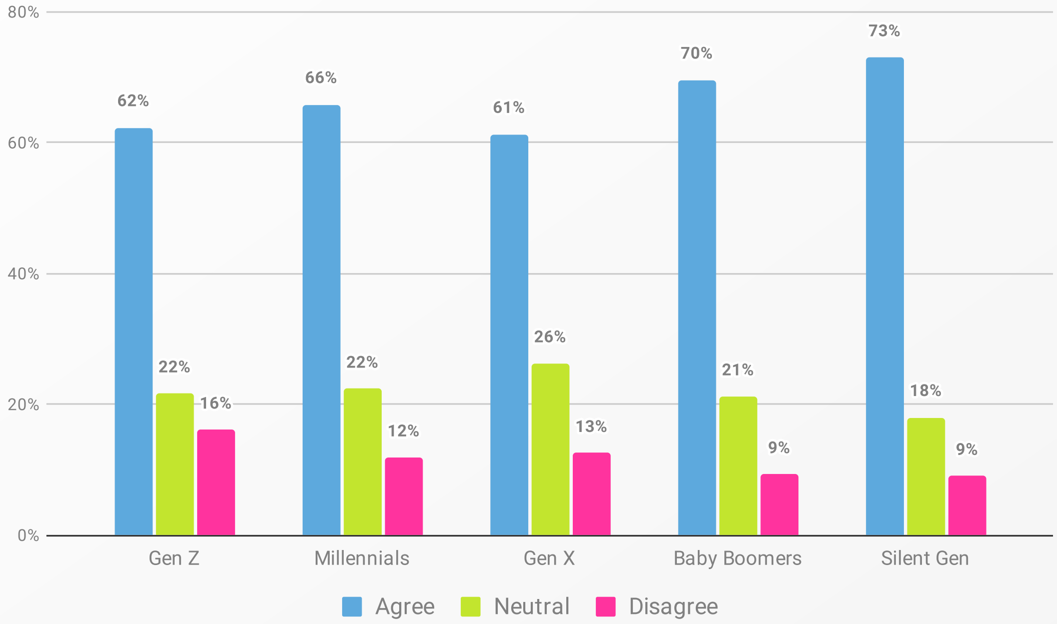


Figure 82. *"I'm concerned about AI-related cybercrime."* by generation.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants with generation information: 6749 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

The figures paint a nuanced picture of AI adoption, training, and security concerns among different demographic groups. While there is a notable uptake of AI tools, especially among younger generations and those employed or studying, there is also a gap in training about the security and privacy risks associated with these tools.

The high levels of concern about AI-related cybercrime, coupled with the finding that many participants have shared sensitive work information without their employer's knowledge, highlight a need for further interventions.

8.2 Trust & perceived responsibility

As we've touched upon, many people have some degree of unease about AI's rapid ascent. Particularly, will companies develop and implement these technologies responsibly? This section unpacks people's trust (or lack thereof) and perceived responsibility around companies implementing AI.

A trust divide appears to be developing, with 36% of participants expressing high trust and 35% expressing low trust. The remaining 29% are on the fence, expressing a neutral stance—maybe waiting to see what happens next.

Trust in companies' responsible implementation of AI looks to decline with age (Figure 83). The Silent Gen perceived companies' AI implementation to be the least trustworthy (56%), followed by Baby Boomers (53%). Millennials (53%) and Gen Z (50%) expressed the highest level of trust. Claiming its central position in both age and feelings, Gen X (32%) appeared the most neutral across generations.

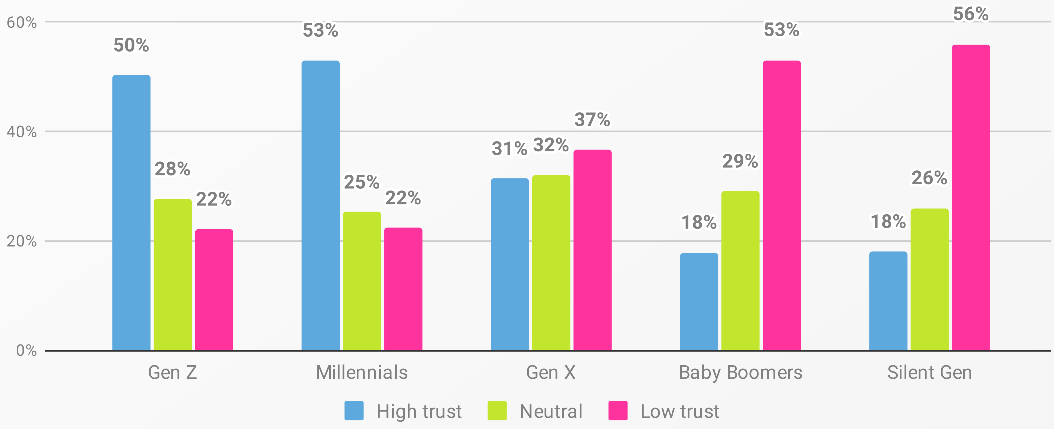


Figure 83. Participants' level of trust in companies to implement AI responsibly, by generation.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants with generation information: 6749 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

There is a similar pattern in how people feel about security and bias in AI-wielding companies (Figure 84). While 37% of participants believe companies integrate security from the start, 27% do not. When it comes to ensuring AI technologies are free of bias, 36% believe companies are achieving it, while 30% remain unconvinced.

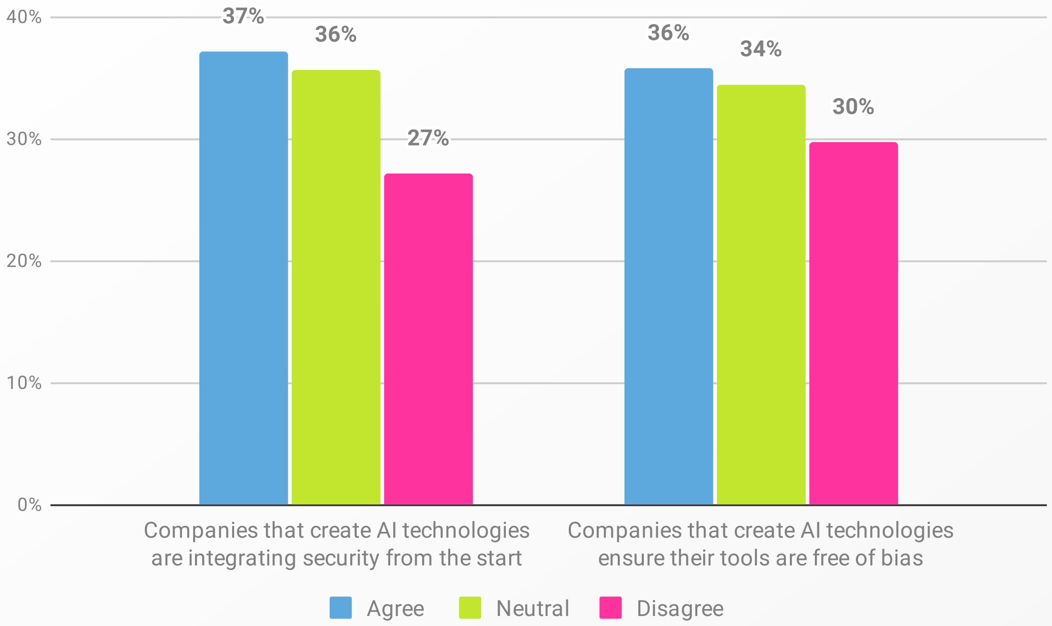


Figure 84. Participants' perceptions of companies that create AI technologies.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants: 7012 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

How about *who* should be responsible for overseeing and regulating the use of generative AI? We asked participants to rate how responsible each of the four key players should be: the government, international organizations (e.g., non-governmental organizations), technology giants (e.g., Google), and national regulators.

A beefy 77% of participants believe that tech giants should hold most responsibility for overseeing and regulating the use of generative AI (Figure 85) – which is surprising because you'd thought we would have learnt by now. Following closely behind are national regulators (73%) and the government (70%). Only 61% of participants think international organizations should hold significant responsibility in this arena.

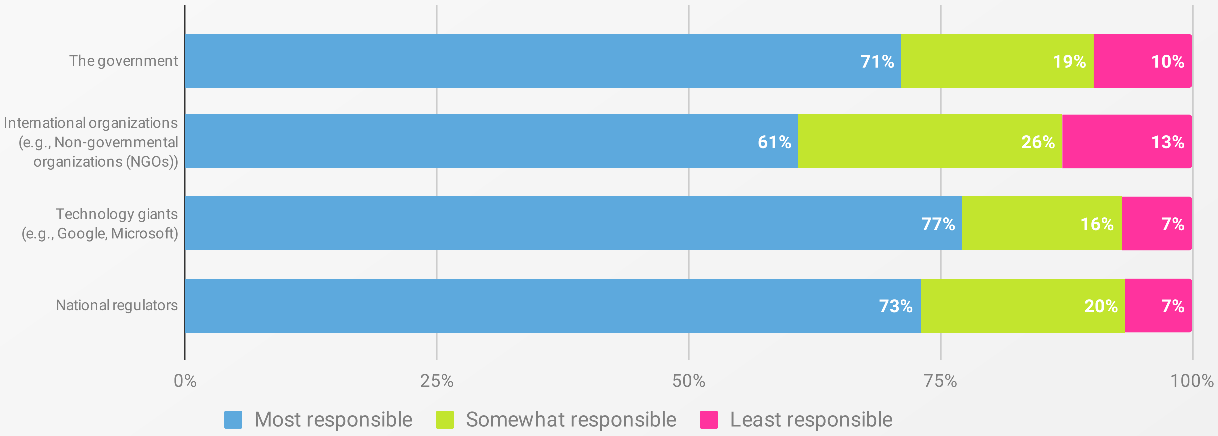


Figure 85. *"To what extent do you believe each of the following should be responsible for overseeing and regulating the use of generative AI?"*

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants: 7012 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

In conclusion, trust in AI implementation is a mixed bag. While trust in companies to implement AI responsibly is fairly balanced overall, it declines with age. Younger generations, particularly Millennials and Gen Z, exhibit higher trust levels compared to older generations. Participants also indicate tech giants, national regulators, and the government should bear the primary responsibility for overseeing and regulating AI, reflecting a strong preference for accountability within the technology industry and national governance frameworks.

8.3 Confidence in recognizing AI-gen content

As AI-generated content becomes increasingly sophisticated, an essential question arises: How confident are people in their abilities to spot such content? This section delves into participants' self-assessed ability to distinguish AI-generated material from human-created content.

Overall, participants had a balanced level of confidence in their ability to recognize AI-generated content (M=5.46, SD=2.6, N=7012). Much like AI trust levels, there is an even balance of high and low levels of confidence in recognizing AI content, with 36% expressing high confidence and 35% expressing low confidence. It should be noted, though, that the balance is holistic only when looking at the full dataset. There were differences between generations.

Once again, Gen Z (53%) and Millennials (53%) display the highest confidence in recognizing AI content (Figure 86). In contrast, the Silent Gen exhibits the lowest confidence, with 69% reporting low confidence in recognizing AI-generated content, followed by Baby Boomers (55%).

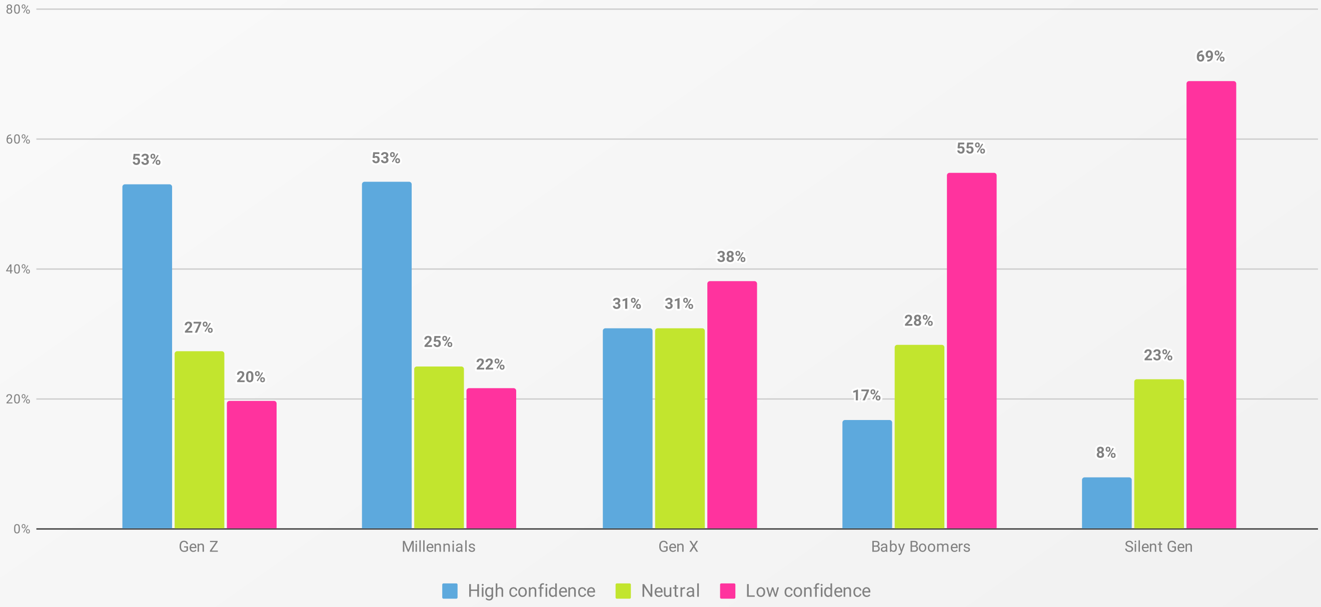


Figure 86. Participants' level of confidence in their ability to recognize AI-generated content, by employment.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants: 7012 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

The findings are even more pronounced when broken down by employment status (Figure 87). The largest proportion of those employed (44%) felt confident in recognizing

AI content, and confidence levels were even higher among students (52%). In comparison, the majority of retirees expressed low confidence (59%), as did those not in employment (39%).

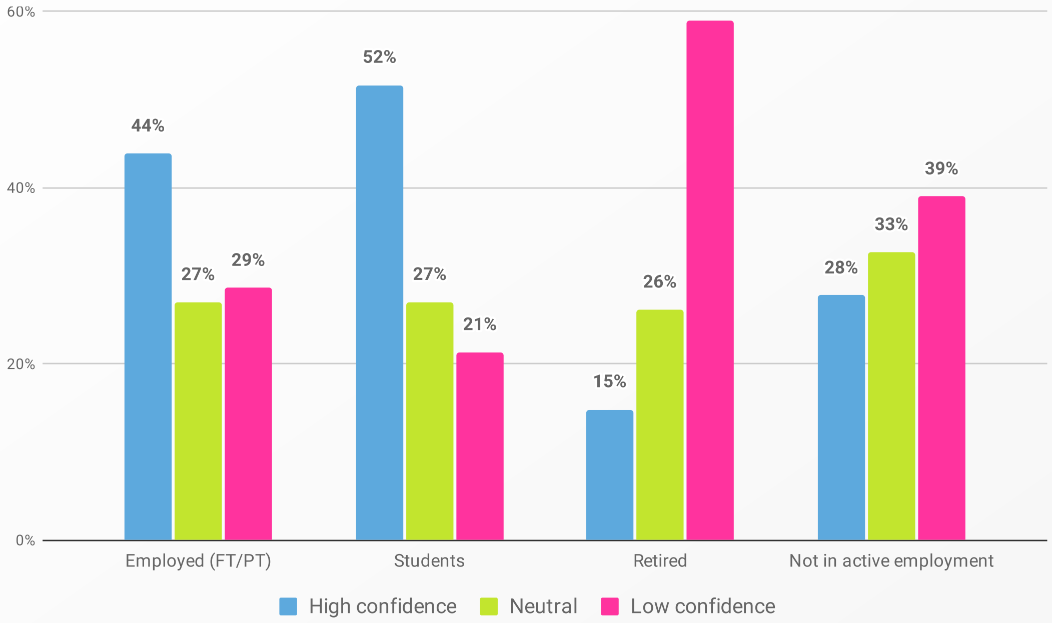


Figure 87. Participants' level of confidence in their ability to recognize AI-generated content, by employment.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants: 7012 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

So confidence in recognizing AI-generated content varies across different demographic groups. Younger generations and those actively engaged in work or study are more confident in their ability to identify AI-generated content, likely due to their more frequent use of AI tools, exposure to AI training, and overall higher confidence levels. In contrast, older generations and retirees are less sure of their AI detection skills.

8.4 Impact

This is where we get up close with participants' perceptions of AI's influence on their personal and professional lives. More specifically, do they think it'll shape their decision-making during election campaigns, affect their employment status, change the nature of their work, enhance their productivity, and impact their ability to detect scams and maintain online security?

8.4.1 Online scams & security

Do people think that AI technologies might make it harder to detect scams and maintain online security? Remember how the qualitative responses (as described in 7.5.1 Recognizing phishing messages) often pointed to advancements in AI as a reason for a lack of confidence in spotting phishing attempts? We aimed to quantify these views across our entire participant pool to gain a clearer picture of these perceptions.

The perceptions of AI's impact on online security were clear-cut. Over half of participants believed it is likely AI will make it harder to detect scams (52%) and to be secure online (55%). Interestingly, Millennials were the most likely to believe that AI will make it harder to detect scams (58%, Figure 88) and to be secure online (59%, Figure 89). The Silent Generation, on the other hand, were more chilled, with only 41% and 46% believing that AI will make it harder to detect scams and maintain online security, respectively.

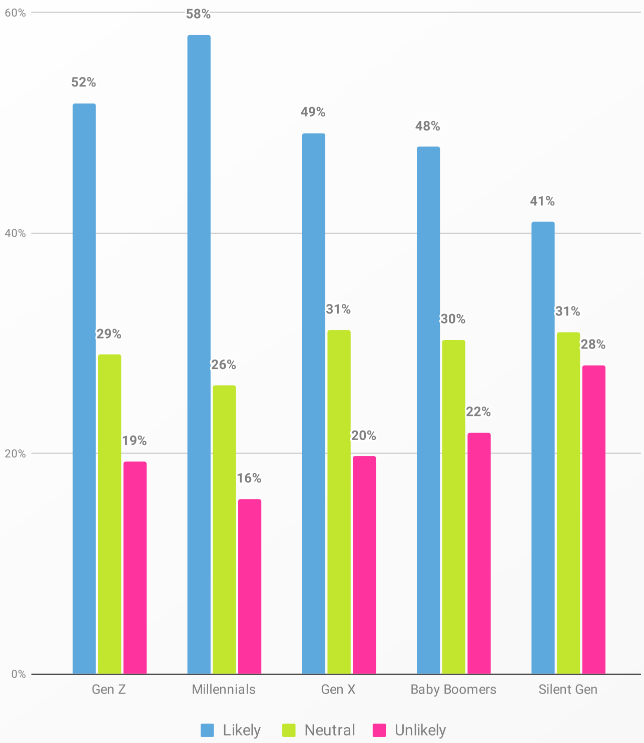


Figure 88. Perceived likelihood of AI making it harder to detect scams, by generation.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants with generation information: 6749 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

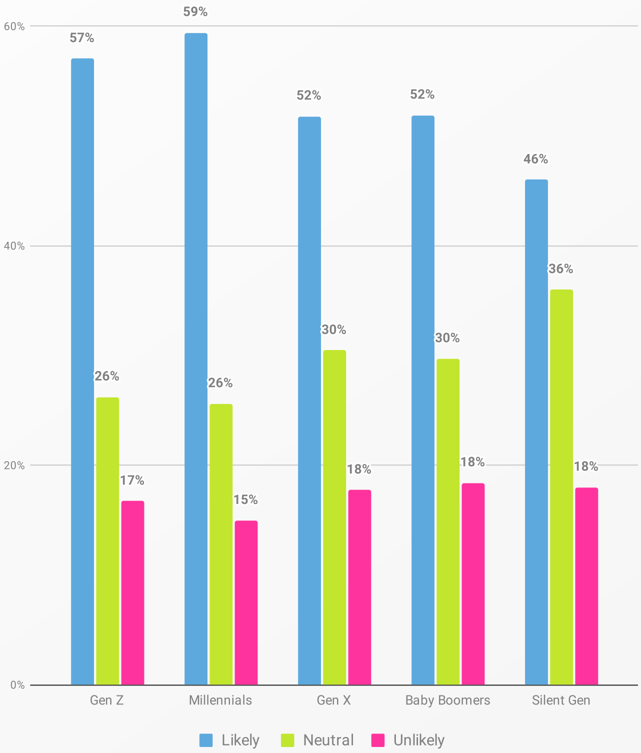


Figure 89. Perceived likelihood of AI making it harder to be secure online, by generation.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants with generation information: 6749 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

> **You can never be certain now that AI is on the scene.** PS233, United Kingdom

> **Everything looks so real. AI has made it difficult to fact from fiction.** PS2744, United States

> **They are becoming very difficult to identify because of AI.** PS6679, Australia

> **Anything AI is questionable.** PS7074, Australia

> **Crime is always evolving, and AI represents another unpredictable risk.** PS9726, Germany

> **I don’t trust AI in general.** PS8314, Canada

8.4.2 Decision making during elections

We doubt it escaped your attention that this year is home to two high-profile (and, for many, high-stakes) elections—the US and the UK. AI technologies can be, and have been, used to create and spread misinformation and deepfakes, which can mislead voters.

False information or manipulated content can sway public opinion, create confusion, and impact voters' decisions based on inaccurateness or deceptiveness. Due to the ever-growing capabilities of these technologies, it is becoming increasingly difficult to differentiate between real and fake.

It's not surprising, then, that 36% of participants believe it's likely AI will influence their decisions on what is real and fake during election campaigns. Still, 30% reported it to be unlikely they'd have the digital wool pulled over their eyes.

The majority within younger generations—49% of Millennials and 43% of Gen Z—said they expected AI will influence their decisions (Figure 90). This concern appeared to decrease with age, with older generations—Baby Boomers (43%) and the Silent Generation (49%)—believing they would avoid being influenced by AI.

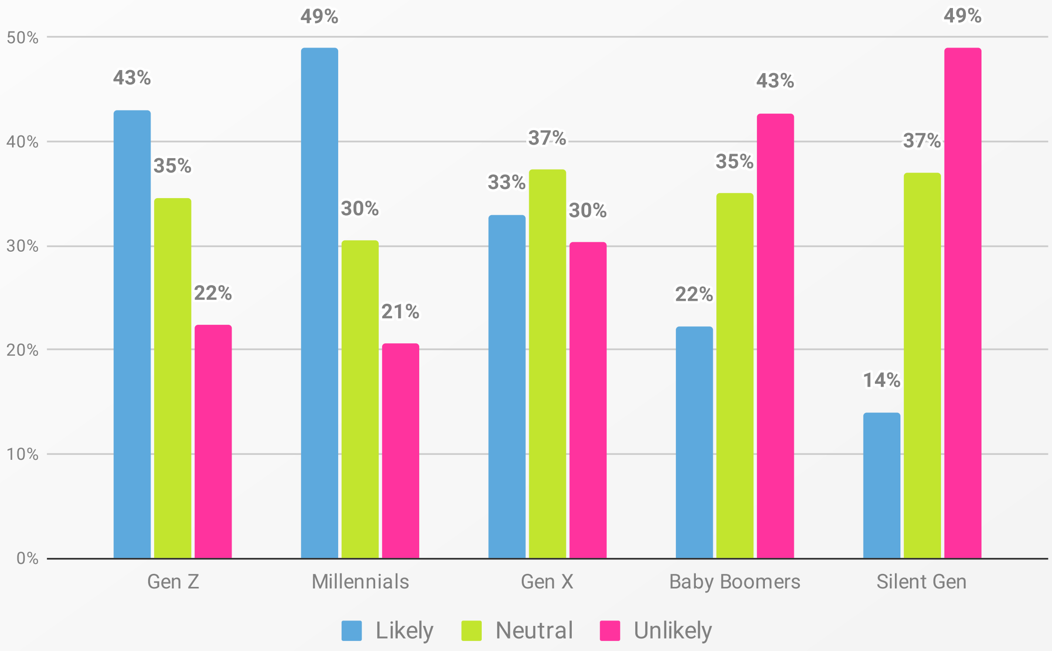


Figure 90. Perceived likelihood of AI's influence on decisions regarding what is real and fake during election campaigns, by generation.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants with generation information: 6749 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

The findings reveal a fascinating generational divide in the perception of AI's impact on decision-making during election campaigns. Younger generations, who are more tech-savvy and more exposed to digital media, are more concerned about AI influencing their ability to discern real from fake information. In contrast, older generations show more skepticism about AI's potential to sway their decisions.

8.4.3 Work & productivity

Finally, what do people think about AI's impact on jobs and productivity? We're talking employment status, nature of one's work, and productivity at work—the whole nine yards.

Overall, views are fairly balanced (Figure 91). Forty percent thought it is likely AI will cause changes to their employment status, but 37% felt this was unlikely. Opinions were split on whether AI would increase their work productivity, with 38% saying it was likely, and 36% saying it was unlikely.

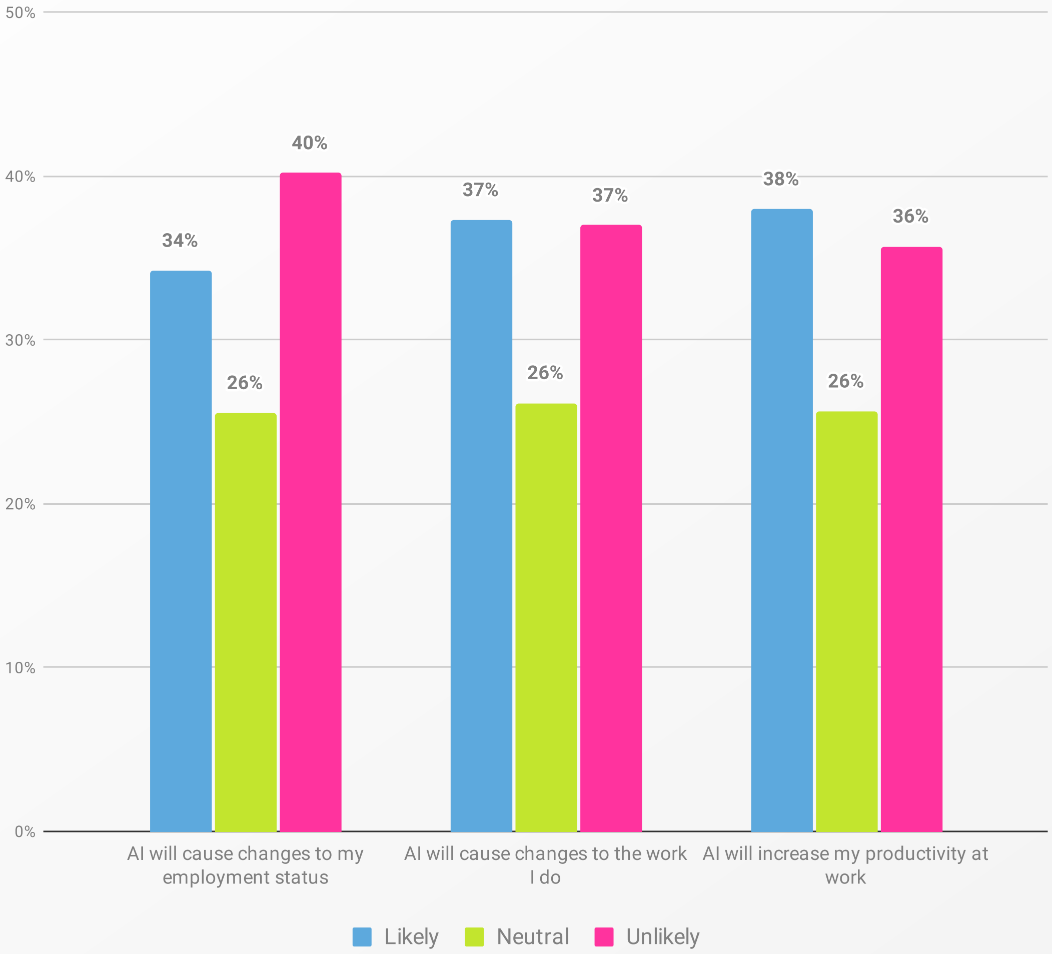


Figure 91. Perceived likelihood of AI's impact on employment status, nature of work and productivity.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants: 7012 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

Burrowing into the differences between generations, the views are a lot less balanced, and a clear trend has emerged. AI's impact on all three work-related beliefs was perceived to be more likely by younger generations (Figure 92). For example, whilst almost half of Gen Z (48%) and Millennials (49%) felt it likely AI will cause changes to their employment status, this belief was less common amongst Baby Boomers (13%) and Silent Gen (11%).

Furthermore, a smidge over half of Gen Z (51%) and Millennials (52%) felt it likely AI will cause changes to the work they do, in comparison to 16% of Baby Boomers and 13% of Silent Gen. With regards to AI's impact on work productivity, the majority of Millennials (55%) and Gen Z (52%) said an impact was likely, while 60% of Baby Boomers felt it to be unlikely, along with 71% of the Silent Gen.

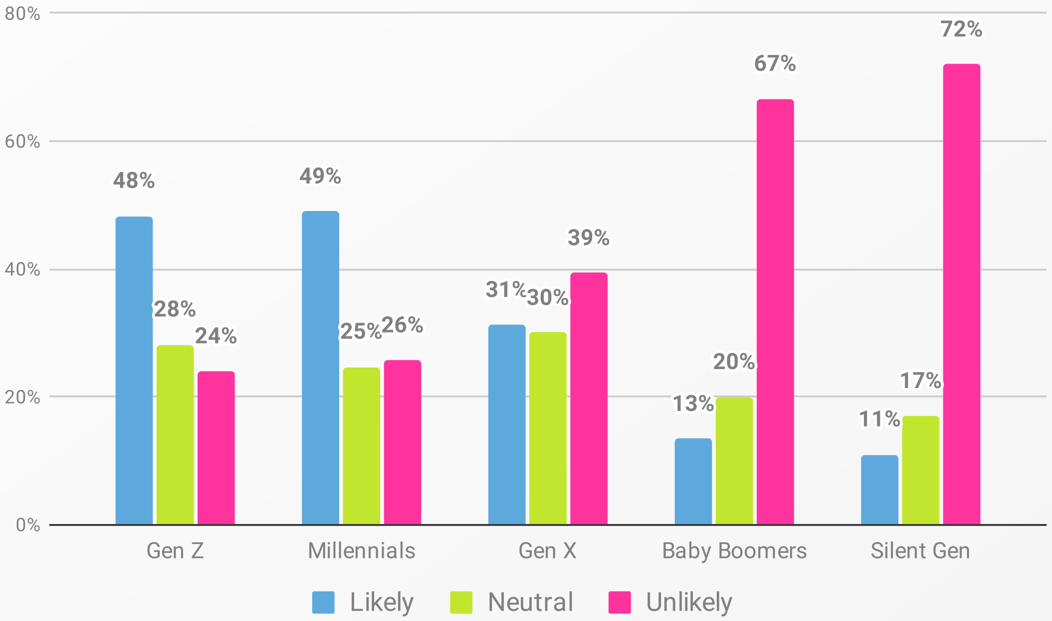


Figure 92. Perceived likelihood of AI's impact on employment status, by generation.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants with generation information: 6749 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

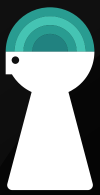
Breaking these findings down by employment status shed light on something interesting, though unsurprising—the majority of the employed found it likely AI will cause changes to their employment status (41%), the work they do (45%), and increase their work productivity (47%). While retirees and those not in employment felt all these work-related AI impacts to be unlikely, students were the most likely of all groups to believe in AI's impact (46%, 52%, and 51%, respectively).

What's the bottom line here? Understandably, people who are working or who are entering the workforce are more concerned about AI affecting their careers. People not in work and people in older generations appear to be less worried, possibly due to a perception that these changes will not significantly affect their current life stage.

Conclusion

1. People share waaay more sensitive information with GenAI tools than organizations realize
2. Knowledge ≠ behavior
3. Are we facing an overconfidence epidemic?
4. Security frustration is leading people to take less responsibility for their safety

   Boom! Behavior change!



Conclusion

We know, we know. That's some serious insight. It paints a complicated picture, where, despite many things moving slowly in the right direction, there are some worrying gaps and (rather baffling) setbacks.

As this wild ride rolls to a stop, you're probably catching your breath, gathering your thoughts, and wondering "What next?"

Here are the most pressing takeaways, along with what we believe it's going to take to tackle the various, persistent challenges this report has explored.

1) People share waaay more sensitive information with GenAI tools than organizations realize

38% have shared sensitive work information with AI tools without their employer's knowledge. Think of this another way: Imagine the public outcry if this information was being posted on social media. Just because we can't see it happening, doesn't mean we should ignore it.

No two ways about it, organizations need to get over AI governance—quickly. Simply dropping a brick of information (training) on people and wagging a finger isn't going to achieve anything.

Instead, focus should be applied to two areas. One: accept people will use GenAI, particularly in the workplace, due to the efficiency it promises—help them to use it safely. Two: understand people (generally) want to behave safely, but they need help understanding the risks of using GenAI—what may happen if they share sensitive corporate information? How could this be bad for their employer, and for them?

We can't ignore just how many participants think AI will influence elections in 2024 and beyond, as we set out in Section 8.4.2. Perhaps most galvanizing is the fact that 1 in 3 participants (36%) believe it's likely AI will influence their decisions on what is real and fake during election campaigns.

As for the other two thirds, just because they don't think they'll be fooled, it doesn't mean they won't.

This isn't about getting ahead and being smug. AI is here. You need watertight AI governance, and you need it yesterday.

2) Knowledge ≠ behavior

Hardly a new concept, but old habits die hard, and plenty of security teams continue to throw training at people expecting them to become cybersecurity ninjas.

More training won't change behavior. Funnier training won't fix it. 'Hollywood style' training won't fix it. Interactive training won't fix it. People knowing what to do doesn't mean they are doing it. Just ask the surprisingly large number of doctors who smoke.

Because this is such a tough nut to crack, we gathered more evidence this year, across a number of behaviors. Do the data make for an uplifting read? Nope. Will it prove useful in furthering behavior change? We sure hope so.

It's much easier if you think of knowledge as only part of the picture. The COM-B model for behavior change comes in clutch here. It proposes that for Behavior change (B) to take place, three factors need to be present: Capability (C), Opportunity (O), and Motivation (M).

So, instead of focusing only on capability (i.e., training to increase people's knowledge[36] about how to behave in a better way), pay attention also to increasing people's motivation, and similarly the opportunities they have to engage in the targeted behavior.

Motivation can move the needle on security behaviors. For instance, a six-month field study[37] in 2020 with 420 participants found fulfilling users' motivations and coping needs can result in statistically significant positive behavioral changes.

Here is, ideally, the state of mind people should be adopting:

- I understand my behavior can make a genuine difference in reducing risk (M)
- I have the knowledge to carry out the right behaviors (C)
- And my environment makes it easy to exhibit those behaviors over other, less secure, behaviors (O)

Wait…what if you're in a knowledge-or-nothing situation? What if training is all you've got—at least for now? We're realists. We know not every organization is in a position to focus on creating the opportunities and motivation for safer behaviors.

[36] 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

[37] Silic, M., & Lowry, P. B. (2020). Using design-science based gamification to improve organizational security training and compliance. *Journal of Management Information Systems, 37(1),* 129-161.

If all you can do is provide knowledge to people, tailoring[38] it as much as it can be tailored brings significant benefits. Some personalization (country, department, region) is better than no personalization. As this report's findings reveal, different generations and countries express different preferences for training delivery. One size fits...none!

When it comes to training, personalization is power. Give people what they need, when they need it, the way they need it.

3) Are we facing an overconfidence epidemic?

As you might have discerned, there's a paradoxical theme at play in the data: Generations exhibiting higher confidence in their ability to recognize cyber threats (like phishing attempts, and AI-generated content) also report higher rates of cybercrime victimization, specifically Gen Z and Millennials.

That's right: Younger generations are more confident...and more likely to be victims. It's like the good old "who thinks they're an above than average driver?" question. This paradox highlights a common bias (clearly not only in cybersecurity) – overconfidence.

Overconfidence leads people to overestimate their abilities and knowledge, resulting in poor decision making. In the context of cybersecurity, it means people may believe they are less susceptible to threats than they actually are—leading to a false sense of security. This can result in riskier online behaviors, increasing their vulnerability to cyberattacks.

Research[39] consistently highlights how people who overestimate their cyber skills, or even their organization's technological security measures, are more vulnerable to victimization, due to their false sense of security.

Misjudging ambition and ability isn't the only issue, though. There's the not-so-small matters of cyber complacency[40], that describes the loss of motivation to be diligent. Behind the concept is the mindset that the systems and tools we use are impenetrable and invincible. Ergo, why bother with secure behaviors? Corners were made for cutting, right?

[38] Aschwanden, R., Messner, C., Höchli, B., & Holenweger, G. (2024). Employee behavior: the psychological gateway for cyberattacks. *Organizational Cybersecurity Journal: Practice, Process and People.* Vol. ahead-of-print No. ahead-of-print.

[39] Greene, K. K., Steves, M., Theofanos, M., & Kostick, J. (2018). User context: an explanatory variable in phishing susceptibility. In *Proc. 2018 Workshop Usable Security.*
Rhee, H. S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security, 28*(8), 816-826.

[40] Stafford, T., Deitz, G., & Li, Y. (2018). The role of internal audit and user training in information security policy compliance. *Managerial Auditing Journal, 33*(4), 410-424.

Overconfidence often arises from a discrepancy between perceived and actual skills. Making people aware of the difference between what they think they know and what they actually know can reduce overconfidence. This relates to the C (Capability) of COM-B, as we discussed a few paragraphs up.

How about the O, Opportunity? Providing the right tools and environments that encourage and enable secure behaviors can address external factors contributing to overconfidence. When people have easy access to secure systems and are less able to bypass security measures, they are less likely to take risks based on a false sense of security.

Overconfidence can also be driven by psychological factors, such as a belief in personal invulnerability or a misunderstanding of threats. Addressing these through education on cognitive biases, promoting a culture of continuous improvement, and rewarding and recognizing secure behavior helps align people's motivations with safe practices.

4) Security frustration is leading people to take less responsibility for their safety

We're relying on the internet for tasks and activities that previously provided a natural respite from screen time. The burden of staying safe is weighing more heavily.

People still generally hold positive attitudes towards cybersecurity, but these sentiments are declining, and negative feelings are on the rise. This is especially true for younger generations (otherwise known as "the workforce") who appear to be growing pessimistic about cybersecurity.

The barrage of confusing and contradictory security advice is creating "advice fatigue"[41], leading to a sense of disillusionment and apathy.

At the same time, people are pushing back against the notion that security is "everyone's responsibility", because it just...isn't. People have a responsibility to behave safely, sure. But they are not responsible for creating easy-to-act-safely-in work environments, writing usable workplace security policies, or building secure tech.

Evidenced by the fact that many of us are unwilling to fork out our hard earned dollars for security features or tools (password managers and VPNs being a couple of the exceptions—and even their use is in decline), there is a growing expectation that technology and workplaces should be secured by their makers.

[41] Reeves, A., Delfabbro, P., & Calic, D. (2021). Encouraging employee engagement with cybersecurity: How to tackle cyber fatigue. *SAGE Open, 11*(1), 1-18.)

Attends voir! We're not suggesting all is lost, by any means. People *want* to be secure. Indeed, a whopping seventy percent feel staying safe online is still achievable. That said, now is not the time for complacency.

Technology makers, governments, regulators, media houses, and workplaces, listen up. People are amazing. But please don't take them for granted, because they seem to be reaching their limits.

This is a call for collective effort. Let us focus on building technology and environments that are safe to use and work in. Making security more accessible will help alleviate frustration, keep people engaged and, ultimately, lead to sustainable safer behavior.

Boom! Behavior change!

Steady. We know behavior doesn't often *change* with a boom. But we think it appropriate to take a couple of moments to celebrate.

This report represents a significant effort to develop our collective understanding on what's required to change behavior. We could not be where we are now without the support of everyone who's contributed.

So, thank you to all the participants who provided their time and insights. And thank you, curious reader, for engaging with the findings.

As we wrap up for another year, it'd be awesome if you could share and promote this report on social media using the hashtag, **#OhBehave**.

Until then, from the team here at CybSafe, the NCA, and our partners, keep inquisitive, continue to embrace the science, and keep blazin' that trail.

Adios!

CybSafe

Appendices

Appendix A: Methodology

This is how we do (okay, did) it ♫

We asked a bunch of people to fill in a survey because we were curious about what they thought about cybersecurity and how they acted online. You already know that part.

But...how exactly did it go down? Rather than rudely leave you in the dark, here's the play-by-play.

Survey design

The survey explored people's feelings on a range of cybersecurity matters, including AI, and five specific cybersecurity behaviors: maintaining good password hygiene, using multi-factor authentication (MFA), installing software updates promptly, identifying and reporting phishing attempts, and backing up data.

The survey primarily used multiple-choice and single-choice questions. These questions 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 were given an "Other, please specify" option where they could write in their own words. We went one further for the all-important topics of participants' lack of confidence in recognizing phishing attempts, and reasons for not trusting password managers, using an essay text box, inviting people to share their thoughts—thereby giving us valuable qualitative data.

One more thing: Participants from New Zealand (N=1012) were not asked to fill in their exact age, but were given age brackets as options. This meant that we had to exclude some New Zealanders (263 to be exact) from generational analyses where their age bracket did not align with a generational age bracket.

Procedure

We recruited our New Zealand participants via the support of New Zealand's National Cyber Security Centre (NCSC), and elsewhere using the Toluna platform. To accommodate everyone, the survey was available in multiple languages.

Participants who completed the survey were compensated for their time. Everyone was briefed beforehand, and gave their informed consent before they could begin. They were told not to reveal any personal information in their responses and that their responses would be anonymized. We stressed participation was entirely voluntary, and people had the right to withdraw at any point. The Science and Research (S&R) team at CybSafe did not collect any personally identifiable information.

All data collection took place between March 6, 2024 and April 22, 2024.

The survey was designed to be completed in under 30 minutes. The average completion time was approximately 25 minutes.[42]

Sample

A representative sample, based on gender and age, was recruited in all regions. As a result, we secured our biggest sample yet: 7,012 participants aged 18+, with the average age being 46 years (SD=16.79).

Table 2 shows the demographics for the survey sample. Those countries sampled by Toluna had 1000 participants per country, and New Zealand had a sample size of 1012, which brings the total survey sample size to 7012 participants.

As mentioned above regarding the New Zealand sample, we excluded 263 participants whose ages didn't align with the defined generation brackets. This included 93 individuals aged 25-29, 90 participants aged 40-44, and 80 participants above 75.

Despite this exclusion, the remaining data show a relatively even distribution across generations, with Millennials (29.8%), Gen X (28.3%), and Baby Boomers (24.6%) comprising the majority. Gen Z (15.8%) and the Silent Generation (1.5%) are represented to a lesser degree.

The majority (67.4%) of participants were in employment (either full- or part-time), including students who were working. Around a third (32.6%) reported not being employed (including 18.9% of retired participants).

[42] This excludes New Zealand whose survey provider did not provide duration of survey completion.

Demographic		United States (N=1000) % within country of residence	Canada (N=1000) % within country of residence	United Kingdom (N=1000) % within country of residence	Germany (N=1000) % within country of residence	Australia (N=1000) % within country of residence	New Zealand (N=1012, except age N=749) % within country of residence	India (N=1000) % within country of residence	Total (N=7012) % within country of residence
Gender (N=7012)	Female	514 51.4%	508 50.8%	508 50.8%	509 50.9%	508 50.8%	540 53.4%	414 41.4%	3501 49.9%
	Male	486 48.6%	492 49.2%	492 49.2%	491 49.1%	492 49.2%	470 46.4%	586 58.6%	3509 50.0%
	Non-binary/ third gender	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	2 0.2%	0 0.0%	2 0.1%
	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=6749)	Gen Z (18-27)	169 16.9%	137 13.7%	142 14.2%	116 11.6%	164 16.4%	72 9.6%	264 26.4%	1064 15.8%
	Millennials (28-43)	300 30.0%	268 26.8%	289 28.9%	243 24.3%	300 30.0%	236 31.5%	375 37.5%	2011 29.8%
	Gen X (44-59)	266 26.6%	294 29.4%	313 31.3%	283 28.3%	261 26.1%	238 31.8%	256 25.6%	1911 28.3%
	Baby Boomers (60-78)	250 25.0%	276 27.6%	242 24.2%	338 33.8%	250 25.0%	203 27.1%	104 10.4%	1663 24.6%
	Silent Generation (79+)	15 1.5%	25 2.5%	14 1.4%	20 2.0%	25 2.5%	0 0.0%	1 0.1%	100 1.5%
Employment status (N=7012)	Employed (%)	650 65.0%	651 65.1%	662 66.2%	650 65.0%	650 65.0%	643 63.5%	680 68.0%	4586 65.4%
	Full-time	513 51.3%	514 51.4%	510 51.0%	496 49.6%	456 45.6%	474 46.8%	559 55.9%	3522 50.2%
	Part-time	137 13.7%	137 13.7%	152 15.2%	154 15.4%	194 19.4%	169 16.6%	121 12.1%	1064 15.2%
	Students (%)	41 4.1%	37 3.7%	52 5.2%	15 1.5%	39 3.9%	33 3.2%	129 12.9%	346 5.0%
	Not working	22 2.2%	20 2.0%	33 3.3%	8 0.8%	18 1.8%	23 2.3%	87 8.7%	211 3.0%
	Working student	19 1.9%	17 1.7%	19 1.9%	7 0.7%	21 2.1%	10 1.0%	42 4.2%	135 2.0%
	Retired (%)	201 20.1%	206 20.6%	174 17.4%	294 29.4%	206 20.6%	188 18.5%	58 5.8%	1327 18.9%
	Don't work or study outside home	108 10.8%	106 10.6%	112 11.2%	41 4.1%	105 10.5%	148 14.6%	133 13.3%	753 10.7%

Table 2. Participant demographics, by country.

Almost half of the participants (49.2%) didn't hold a university degree (Table 3). The most common qualification to hold was an undergraduate degree with 31.6% of participants having one.

Demographic	United States (N=1000) % within country of residence	Canada (N=1000) % within country of residence	United Kingdom (N=1000) % within country of residence	Germany (N=1000) % within country of residence	Australia (N=1000) % within country of residence	New Zealand (N=1012) % within country of residence	India (N=1000) % within country of residence	Total (N=7012) % within country of residence
Some school/ High school credit, no diploma or qualification	65 6.5%	54 5.4%	51 5.1%	6 0.6%	123 12.3%	6 0.6%	48 4.8%	353 5.0%
Primary/secondary education (e.g., GCSEs/A-levels/High School Diploma/GED)	288 28.8%	242 24.2%	308 30.8%	182 18.2%	195 19.5%	292 28.9%	79 7.9%	1586 22.6%
Trade, technical or vocational training (e.g., BTEC/HND/ NVQ Diploma/CTE qualification)	99 9.9%	277 27.7%	196 19.6%	472 47.2%	264 26.4%	153 15.1%	47 4.7%	1508 21.5%
Undergraduate degree (e.g., Associates/ Bachelors)	385 38.5%	298 29.8%	295 29.5%	182 18.2%	278 27.8%	385 38.0%	392 39.2%	2215 31.6%
Postgraduate degree (e.g., Masters/PhD)	128 12.8%	107 10.7%	130 13.0%	109 10.9%	121 12.1%	166 16.4%	356 35.6%	1117 16.0%
Professional degree (e.g., MD/DDS/JD)	35 3.5%	22 2.2%	20 2.0%	49 4.9%	19 1.9%	0 0%	78 7.8%	223 3.2%
Prefer not to say	0 0%	0 0%	0 0%	0 0%	0 0%	10 1.0%	0 0%	10 0.1%

Table 3. Participants' education levels, by country.

In Appendix B, where notable, we highlighted comparisons to *Oh, Behave! 2023*. Since this is the first time we gathered data from Australia and India, no comparisons were made to last year's data for these countries.

Data quality

No number nonsense here. The survey providers know their stuff, so they were sure to throw in some measures to ensure data quality. For instance, if a participant's response was determined to be of a 'low' quality (e.g., incomplete responses), they were replaced by another participant to meet the required sample size. The survey included two attention checks to filter out any potential 'bots' and participants who were just clicking through the survey without reading the questions.

Data analysis

Finally, we crunched those numbers like a Doberman eats Doritos. We conducted descriptive statistical analyses on all Likert-based questions, providing frequencies (N) and proportions (%). To make it all easier to grasp, we employed the latest data visualization techniques—a fancy way of saying we created pretty tables and charts.

We re-coded all 5- and 10-point Likert scale responses (e.g., "Strongly agree" to "Strongly disagree") into 1-3 options (e.g., "Agree", "Neutral", "Disagree") for better understanding and effective data visualization.

We analyzed the qualitative data to find common themes and ideas, selecting the most interesting quotes to illustrate the themes and depth of responses, significantly enriching (if we do say so ourselves) the report. We also translated any non-English language comments using top-notch translation tech.

Appendix B: Country comparisons

This section examines country-wise differences in attitudes and behaviors towards cybersecurity, access to training, and cybercrime victimization. Naturally, we're comparing all our participating countries: the United States, Canada, the United Kingdom, Germany, Australia, New Zealand, and India[43]. While there are plenty of similarities, we were most interested in the areas of difference between the seven countries. For one, we were curious about whether cultural differences influenced values and decision-making capabilities.

Online presence

The majority of participants from India (71%) are 'always connected', along with 56% from the UK, 56% from Canada, 55% from Australia, and 53% from the USA (Figure 93). In comparison, just 33% of participants from Germany reported always being connected.

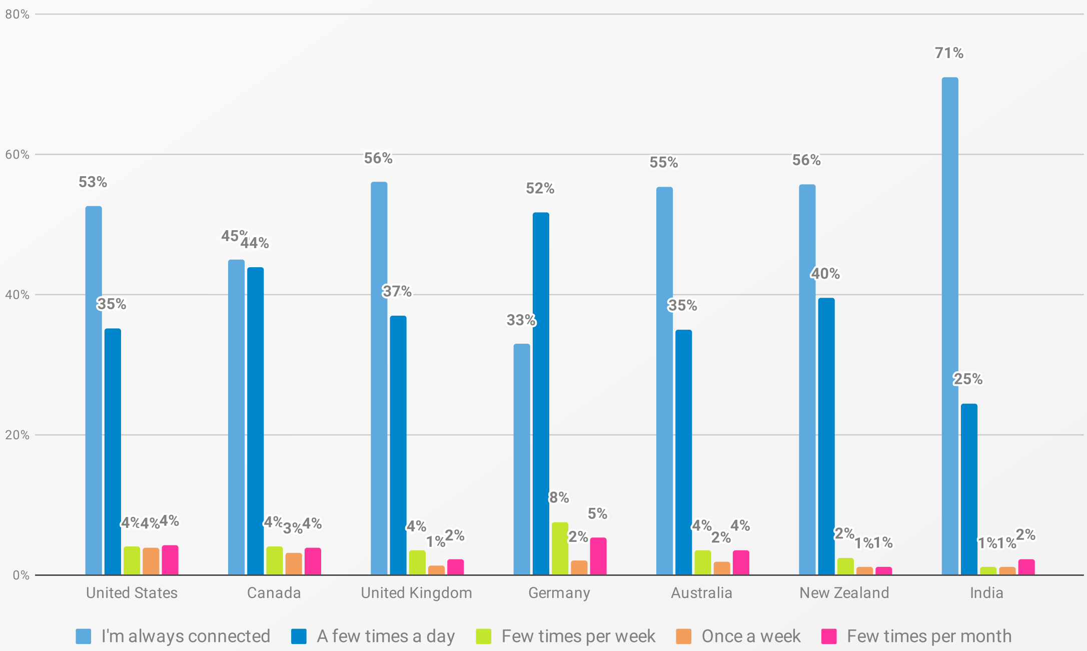


Figure 93. *"How frequently do you use the internet?"* by country.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants: 7012 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

[43] Participants from the United States are referred to as 'Americans', from Canada as 'Canadians', from India as 'Indians', and from New Zealand as 'New Zealanders'.

The largest proportion of participants from all countries reported having 2-9 sensitive online accounts, ranging from 30% in Germany to 53% in India (Figure 94). The second largest proportion of participants in Canada (20%), the UK, Germany, and New Zealand (all 23%) admitted having lost count of the number of sensitive online accounts they possess. Compared to other countries, the highest percentage of those with more than twenty accounts were from the UK and Germany (both with 17%). The highest proportion of those with only one account was in India (14%).

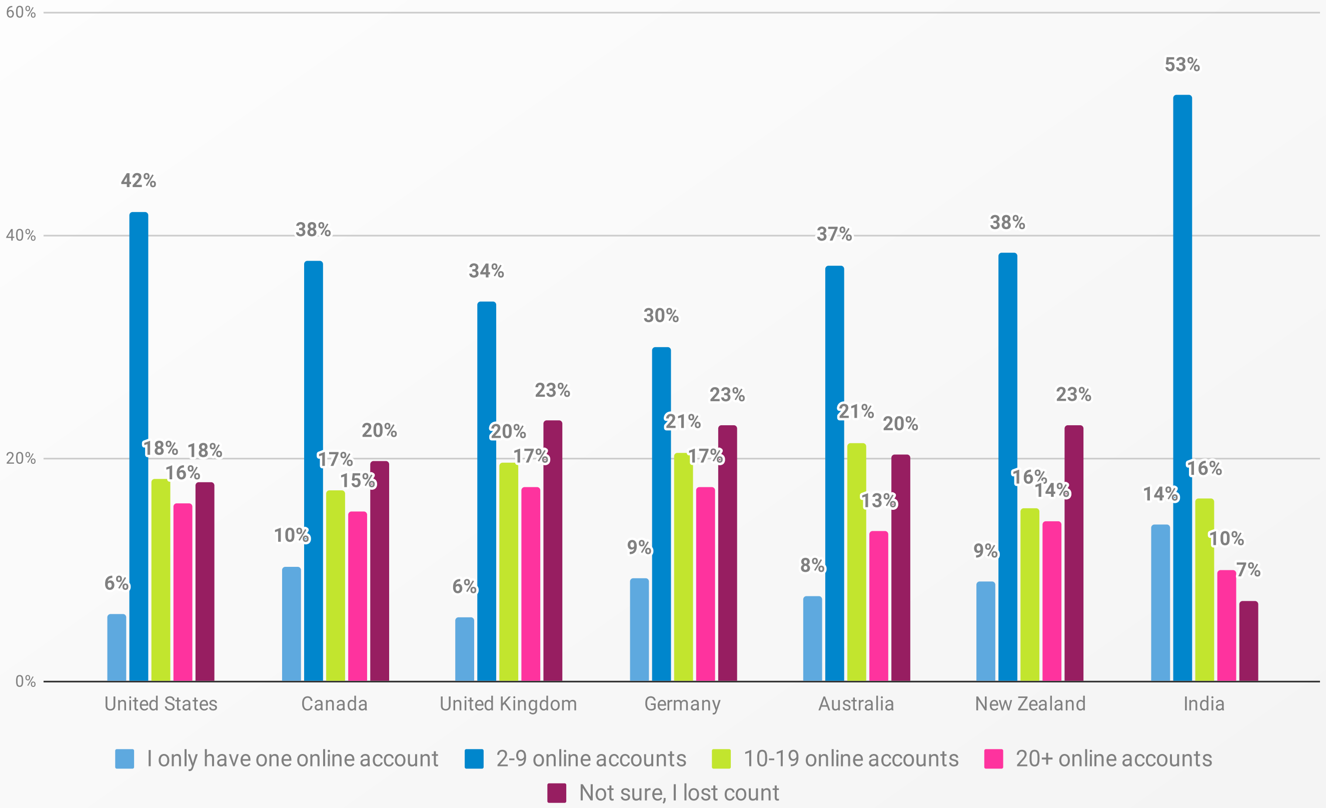


Figure 94. *"Overall, how many sensitive online accounts that hold personal information do you have?"* by country.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants: 7012 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

Cybersecurity attitudes

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

Our findings showed over half of the participant pool found it easy to stay secure online. When comparing the data across countries, the majority in almost all countries agreed, and this was highest in India (62%, Figure 95). However, only 48% of participants from Canada felt the same.

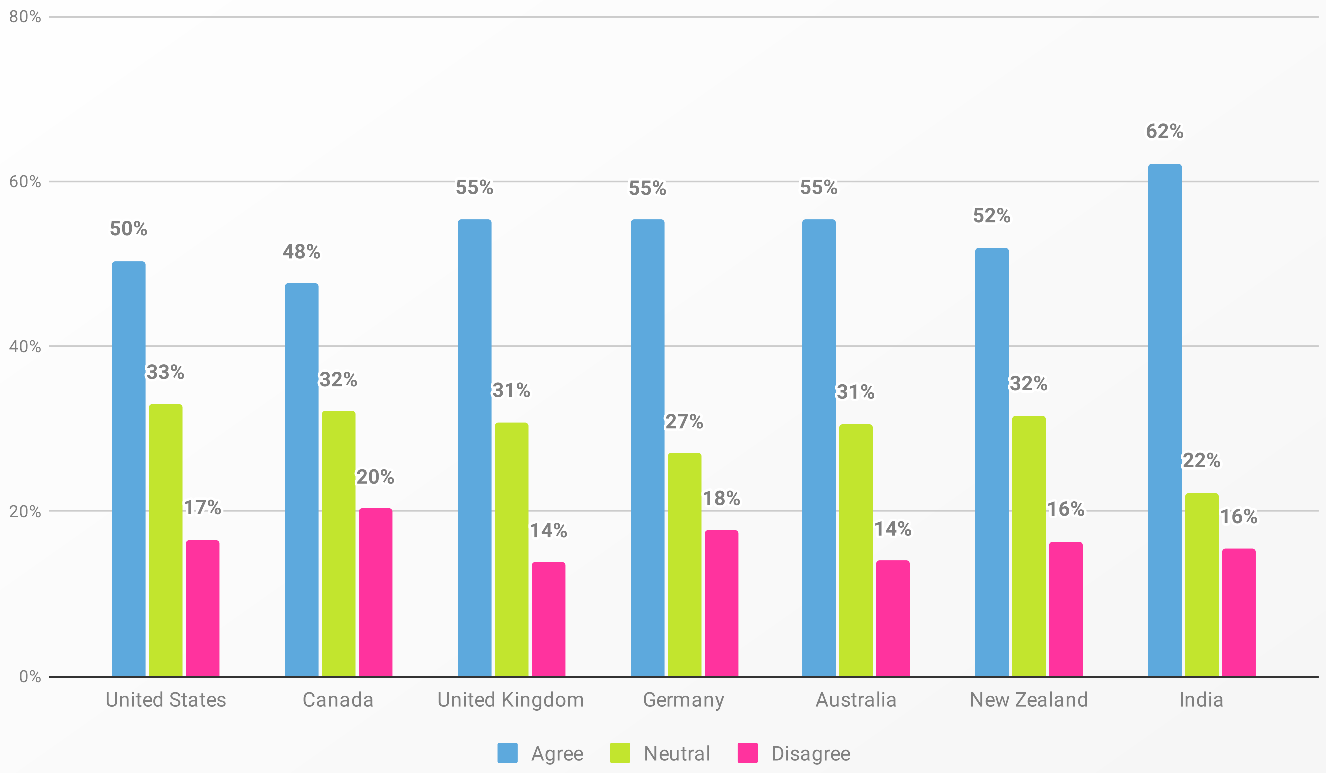


Figure 95. *"I find it easy to be secure when I'm online."* by country.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants: 7012 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

As identified above, levels of frustration around the challenges of navigating online security have increased since 2023. How does this break down by country?

The largest proportion of participants finding staying secure online intimidating (Figure 96) were from Canada (49%), followed by India (48%) and the US (47%). Conversely, 'only' 35% of New Zealanders felt the same. Slightly more than half of the participants in the USA (53%, +11% from 2023), Canada, and Australia (both 52%) found online security to be frustrating. In comparison, only 37% of Germans agreed with this, though this still represents a 6% increase from 2023. It seems the online world is increasingly becoming a real-life stress test.

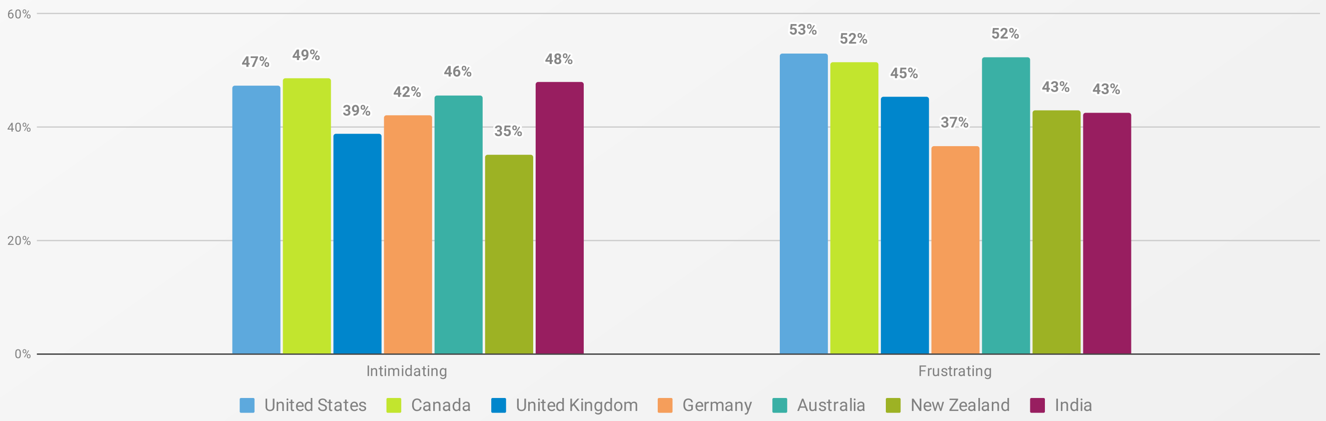


Figure 96. *"I feel that staying secure online is intimidating & frustrating."* by country.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants: 7012 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

Turns out plenty of us are scratching our heads about cybersecurity. In fact, Germany was the only surveyed country where the largest proportion of participants did not find information on how to be secure online confusing (38%, Figure 97). Participants from Canada appeared to have a neutral view (36%), but a similar proportion (35%) believed online information to be confusing, just like the majority in the rest of the countries.

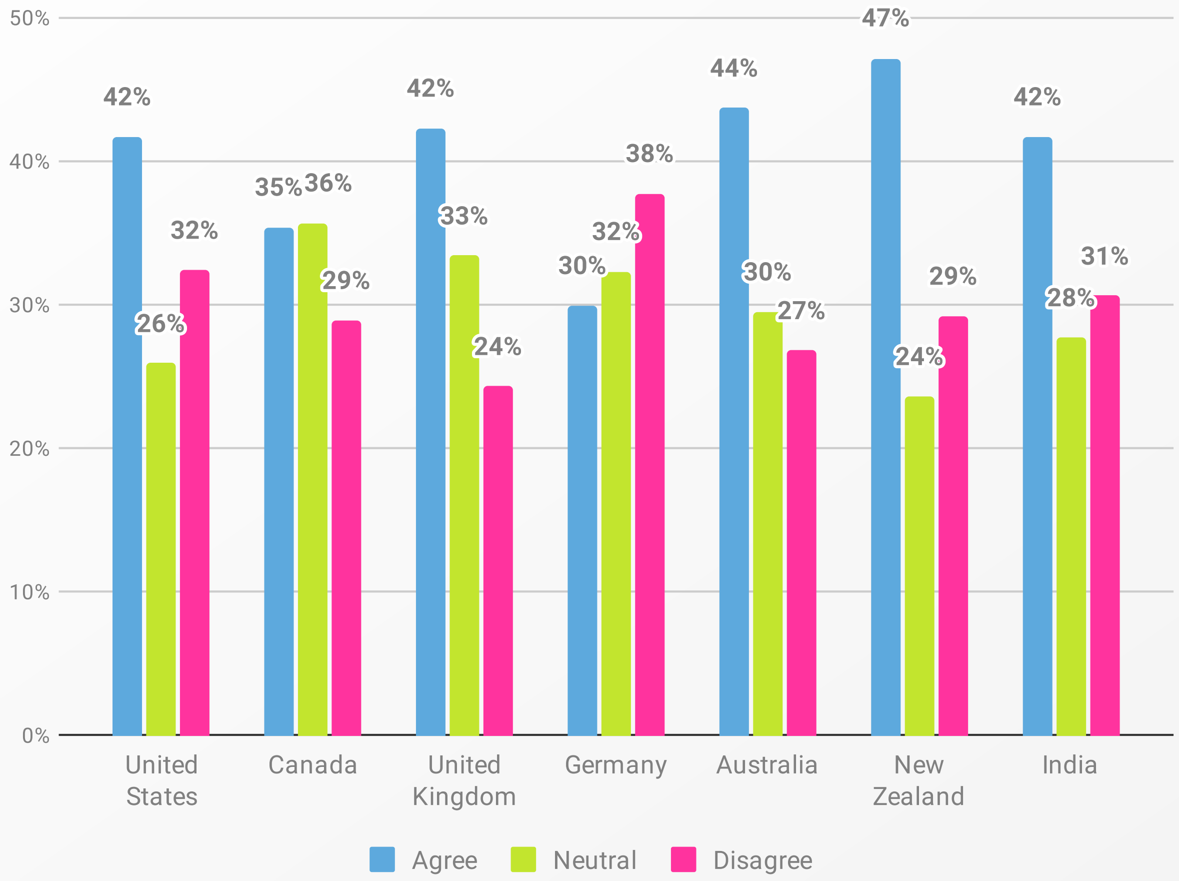


Figure 97. *"Most information on how to be secure online is confusing."* by country.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants: 7012 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

Next, online optimism. The majority of participants in all countries felt it possible to stay secure online, with the UK and New Zealand being the highest at 61% (Figure 98). In comparison, only 45% of participants in Germany felt the same.

The really weird bit? Despite aforementioned low levels of confusion and frustration, the lowest proportion of those feeling that staying secure is under their control were also from Germany (43%), while over half of the participants in the other countries thought it was under their control. This belief was most prominent among Indian participants (66%).

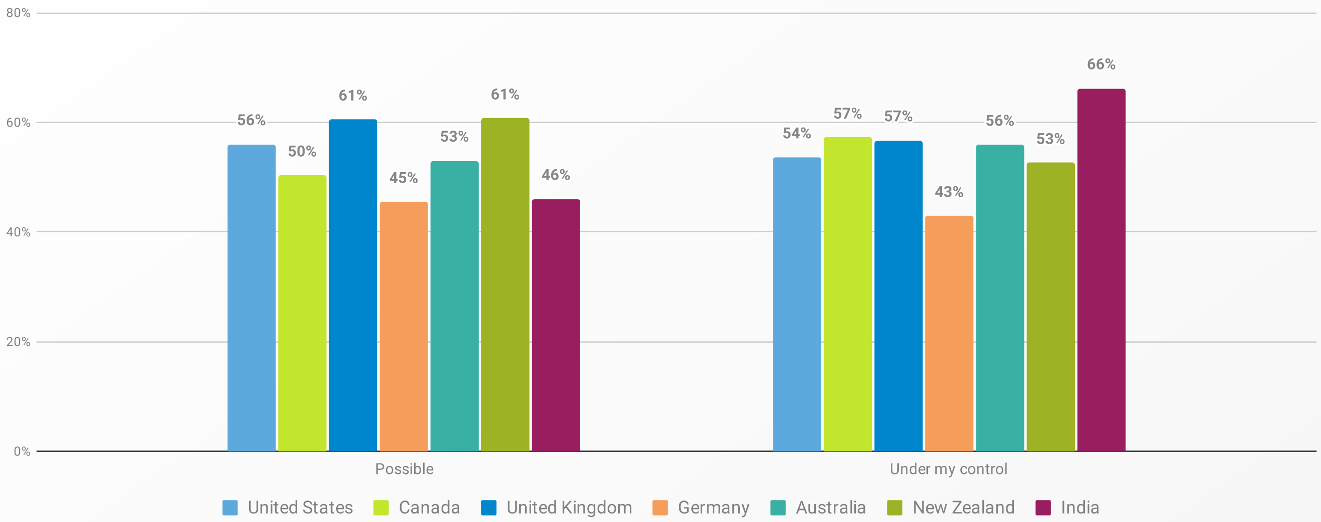


Figure 98. *"I feel that staying secure online is possible & under my control."* by country.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants: 7012 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

Now, get this: One of the most notable differences in cybersecurity attitudes was regarding whether staying secure online was worth the effort (Figure 99). While the majority in all countries agreed it was (ranging from 59% in the USA to 68% in New Zealand), only 40% of participants in India felt it was worth the fight.

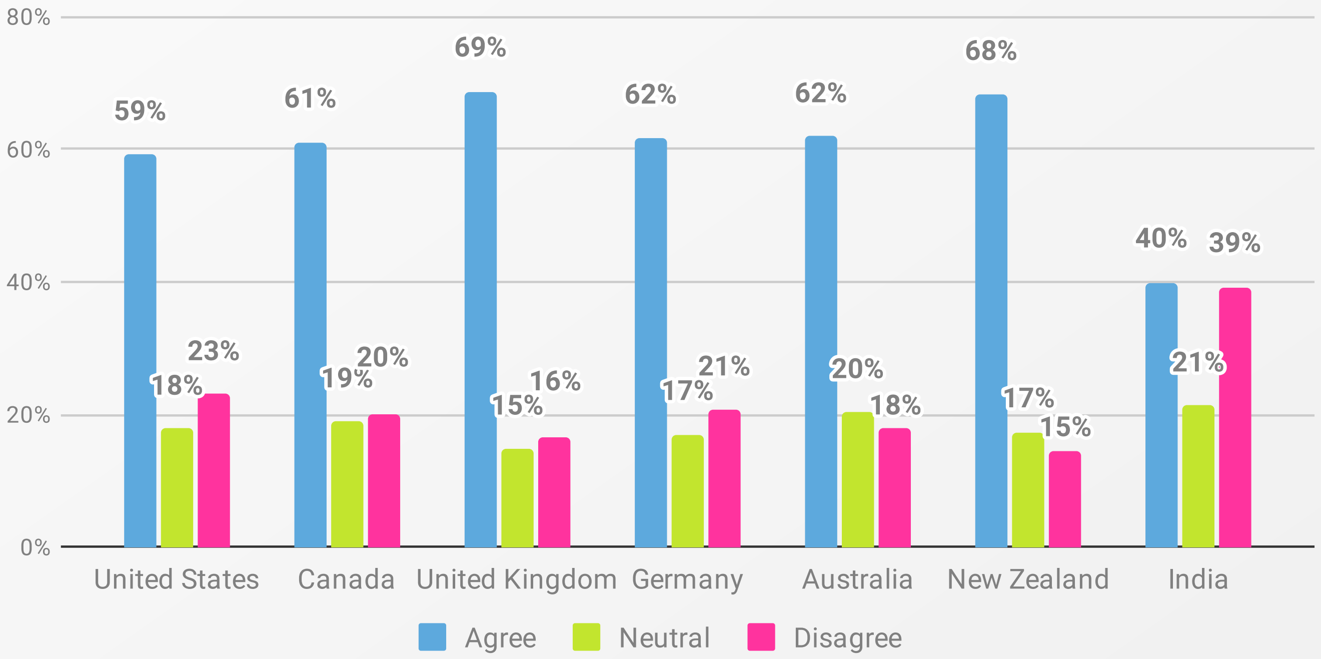


Figure 99. *"I feel that staying secure online is worth the effort."* by country.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants: 7012 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

Generally, participants from most countries are drowning in a sea of overwhelming online security information, but being unable to resist the siren song of all things online despite the risks (Figure 100). This is most pronounced among participants from India (57%), followed by Canada (48%) and Australia (46%). An equal percentage of German participants agreed and disagreed with this statement (36% each).

At the same time, cyber advice overload has made hermits of some. The highest percentage of individuals who minimize their online actions due to information overwhelm (Figure 101) are from India (51%), followed by Australia and the USA (37% each). New Zealanders claim the “feel-the-fear-and-do-it-anyway” crown, with only 27% of them downscaling their digital lives because of overwhelm.

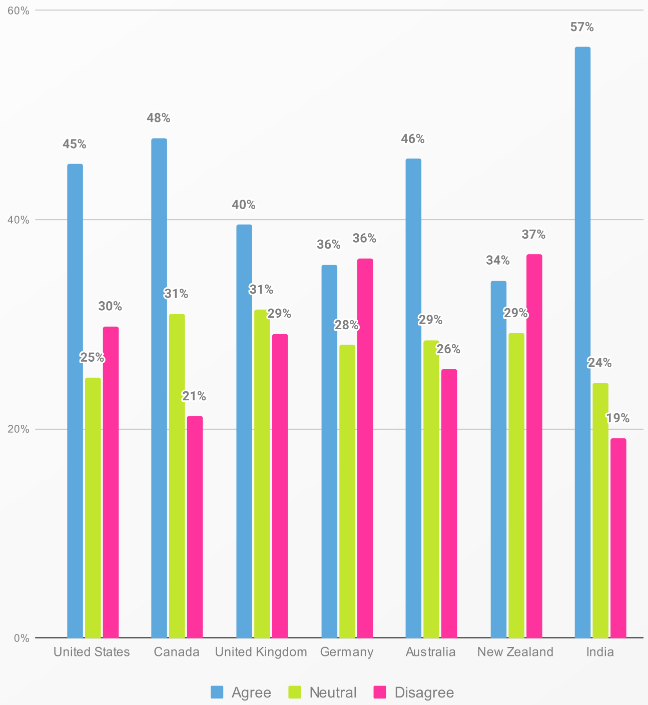


Figure 100. *“I often feel overwhelmed by online security information, but I still go online regardless of potential risks.”* by country.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants: 7012 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

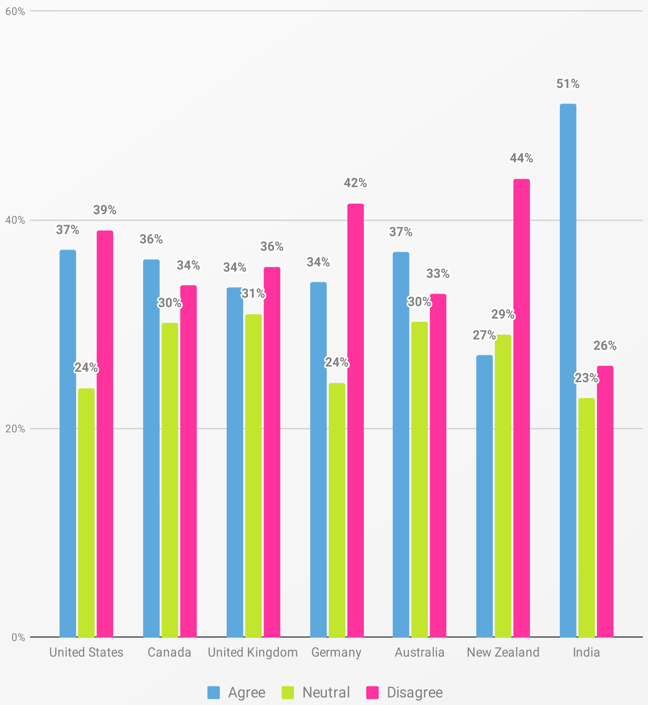


Figure 101. *“I often feel overwhelmed by online security information, and therefore, minimize my actions online.”* by country.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants: 7012 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

What about country differences in device security perceptions? Well, good news for those of you who love people living in blissful device security ignorance: Generally, the largest proportion of participants in almost every country presumed their devices are automatically secure (Figure 102), with this belief being notably high amongst Indian participants, where 61% made the presumption.

On the other hand, the only country where the largest proportion of participants did not think their devices were automatically secure was Germany, with 43% of participants disagreeing with this statement.

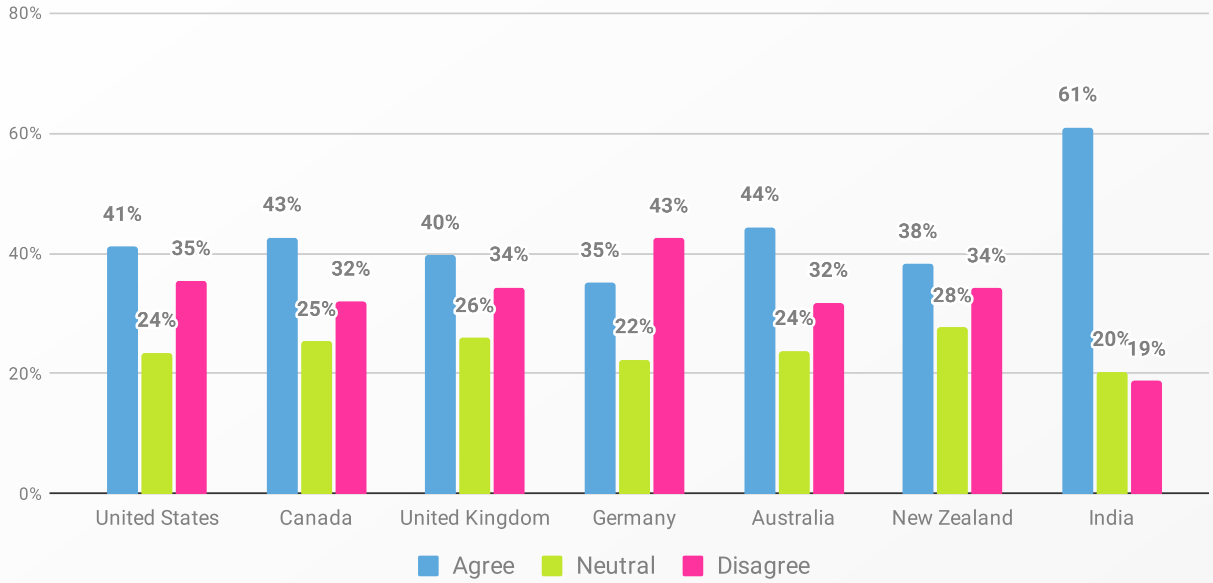


Figure 102. *"I presume my devices are automatically secure."* by country.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants: 7012 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

Media impact on attitudes & behaviors

Let's explore country differences regarding the impact of media on people's feelings towards online security.

The majority of participants from India (72%)—by far the highest proportion across all countries—said they rely on the media or news to help them stay informed about online security. While around half of the participants across the other countries felt the same, only 43% of New Zealanders report the media help them stay informed about online security (Figure 103).

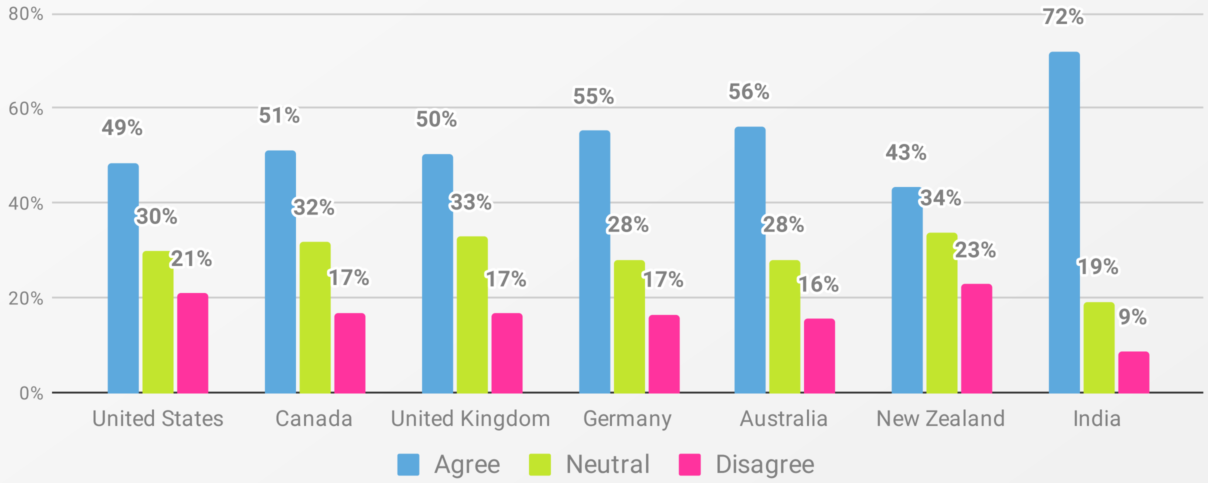


Figure 103. *"The media/news help me stay informed about online security."* by country.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants: 7012 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

Guidance is one thing. What about motivation? The findings showed the majority of participants were motivated by the media to take protective actions for their online security. Specifically, Figure 104 shows over half of the participants from nearly all countries are influenced by the media to take online security measures, with the highest proportion being in India (75%). However, less than half (47%) of New Zealanders felt the same, with 20% indicating they do not take such measures due to media coverage.

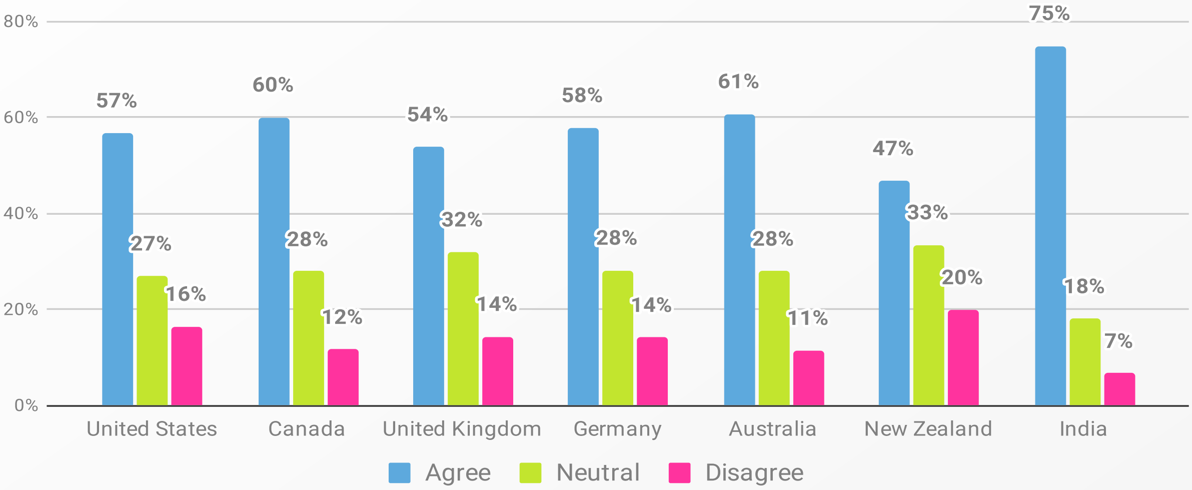


Figure 104. ***"The media/news motivate me to take protective actions for my online security."*** **by country.**

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants: 7012 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

Whilst overall, 44% of participants reported feeling scared about their online security due to media coverage, Figure 105 demonstrates this was notably stronger among participants from India, where the majority (57%) agreed with this statement. In contrast, New Zealanders were the least spooked by media coverage, with only 35% reporting that news scares them about their online security. Should the phrase have been 'cool as a Kiwi' all along?

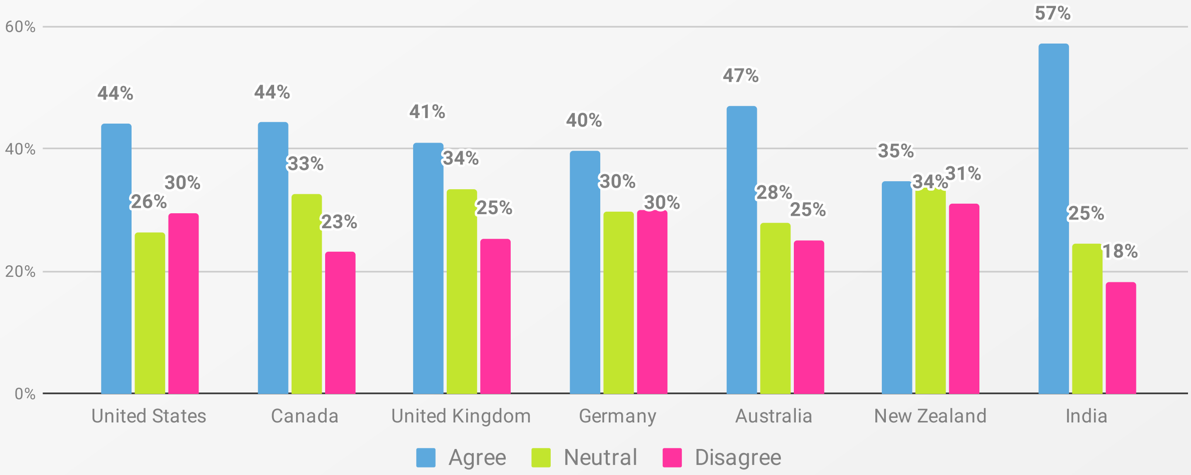


Figure 105. ***"The media/news make me scared about my online security."*** **by country.**

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants: 7012 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

Overall, the impact of media on online security perceptions reveals fascinating variations between countries. While Indian participants are highly influenced by the media both in terms of motivation for protective actions and feelings of fear about online security, New Zealanders exhibit lower levels of media-induced motivation and fear. Meanwhile, countries such as the US and UK trundle along in the media-moderate middle of the pack.

These findings highlight how media coverage can differently affect online security behaviors and attitudes depending on where you hang your hat (or plug in your router).

Victimization & reporting

Forget fear mongering about cybercrises. What about country differences in attitudes towards victimization, actual experiences of being a victim, and the reporting of cybercrime? Let’s have a look.

Attitudes towards victimization

The majority of participants in all countries were sweating bullets about becoming a victim of cybercrime (Figure 106), with the highest percentage in India (72%), followed by Australia (62%) and Canada (65%). In comparison, less than half of the German respondents (47%) and just over half of the New Zealanders (54%) reported feeling worried about falling victim to cybercrime.

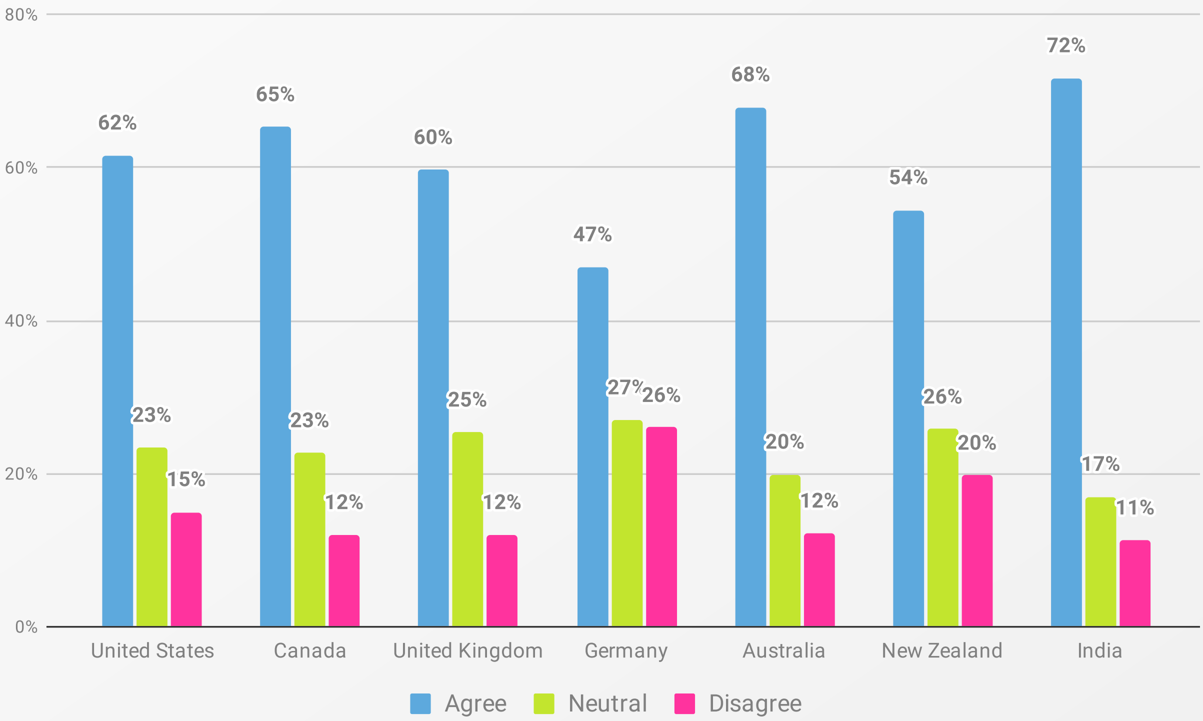


Figure 106. *“Falling victim to cybercrime is something that worries me.”* by country.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants: 7012 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

Remember how, in spite of the high levels of worry, “only” 42% felt they are likely to be a target of cybercrime? Figure 107 shows the largest proportion of participants in almost every country thought of themselves as likely targets of cybercrime, especially in the UK (47%), Australia (47%), and New Zealand (46%). However, the only country where almost half of the participants felt they were unlikely to be targets of cybercrime was India, where 48% were confident that they’d never find themselves in the cyber-crosshairs.

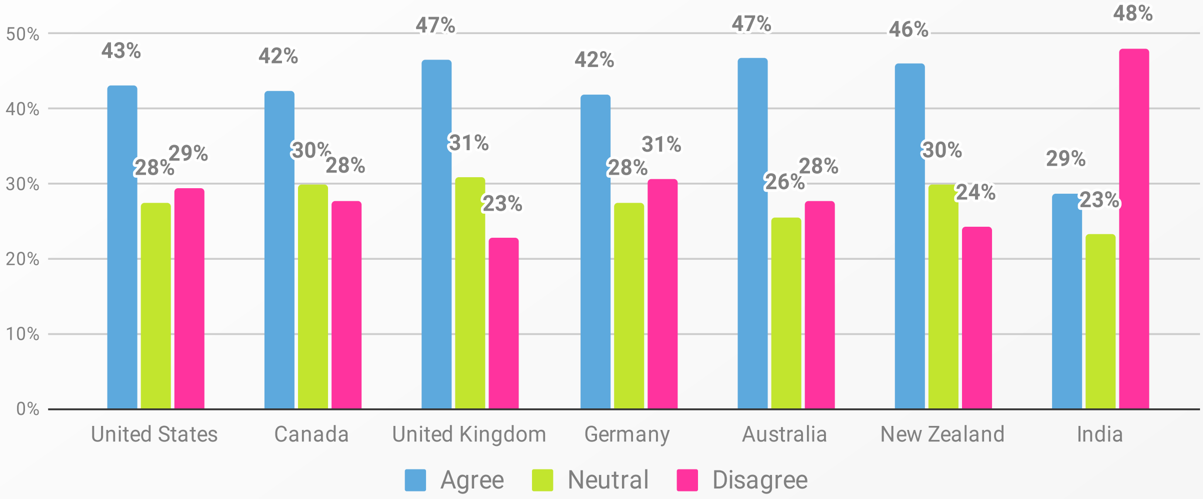


Figure 107. *“I am likely to be a target of cybercrime.”* by country.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants: 7012 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

The majority of participants from India (47%, Figure 108) expressed there is no point in protecting themselves as their information is already online—making India the only country where the majority holds this view. On the flip side, half of the respondents from the UK and New Zealand believed that all was not lost…yet.

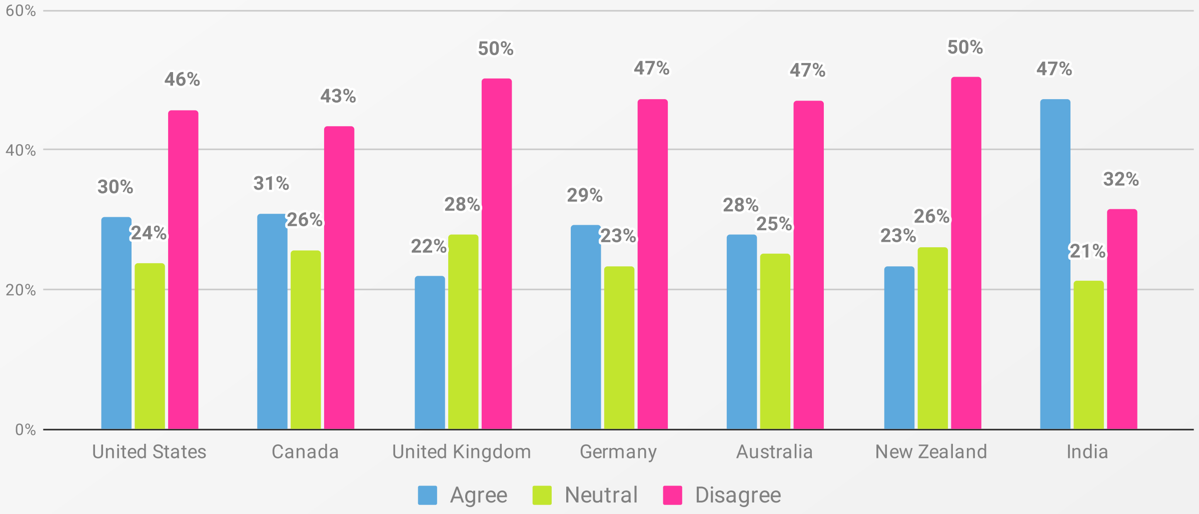


Figure 108. *“I don’t see the point of trying to protect myself more as my information is already online.”* by country.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants: 7012 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

This perceived helplessness amongst Indian participants was further demonstrated by the fact that the majority of them also felt it is unavoidable to lose money (51%) or having personal details stolen (60%) on the internet nowadays (Figure 109), and these were the highest across all countries. In comparison, only 19% of Australians believed it unavoidable to lose money on the internet, and the UK and New Zealand are also holding on to hope, with only 27% each feeling destined for digital doom.

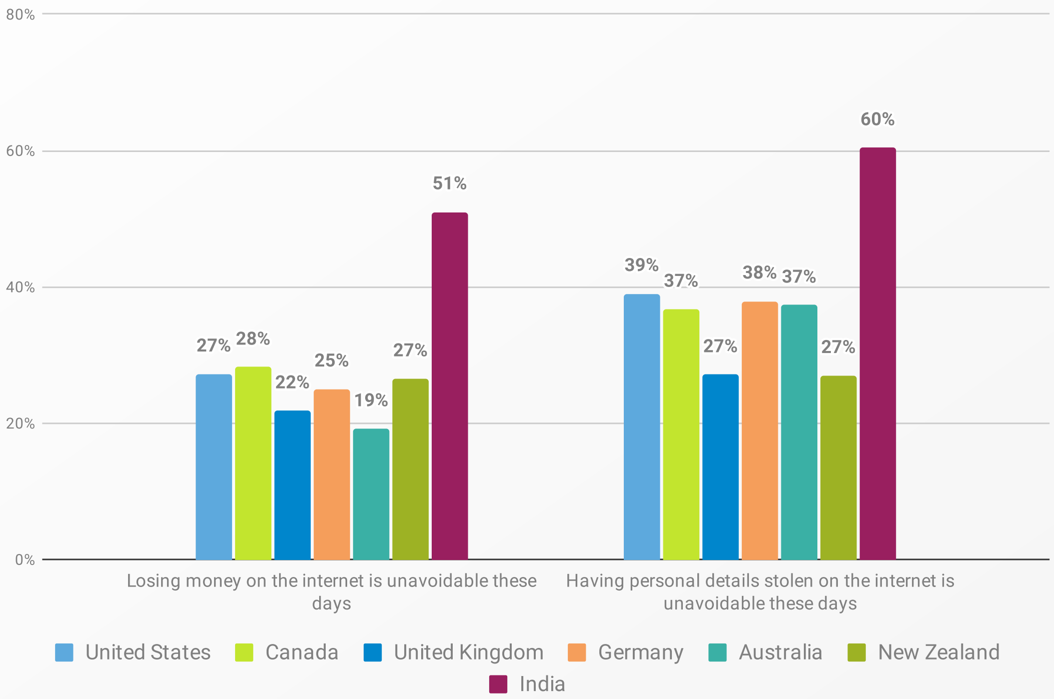


Figure 109. Perceptions on the avoidability of losing money or personal details on the internet, by country.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants: 7012 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

To wrap things up, there are some hefty differences in attitudes towards cybercrime across countries. Indian participants exhibit the highest levels of worry and perceived helplessness regarding cybercrime, with a notable portion feeling protecting themselves is futile due to their information already being online. In contrast, participants from countries like the UK, Australia, and New Zealand are hopeful that victimization isn't a done deal just yet.

Cybercrime prevalence

New Zealand (25%), the UK (30%), and Germany (30%) had the lowest numbers of cybercrime victims (Figure 110). Despite 48% of Indian participants not thinking of themselves as likely targets of cybercrime (Figure 107), India had the highest percentage of cybercrime victims at 47%, followed by 44% of Americans.

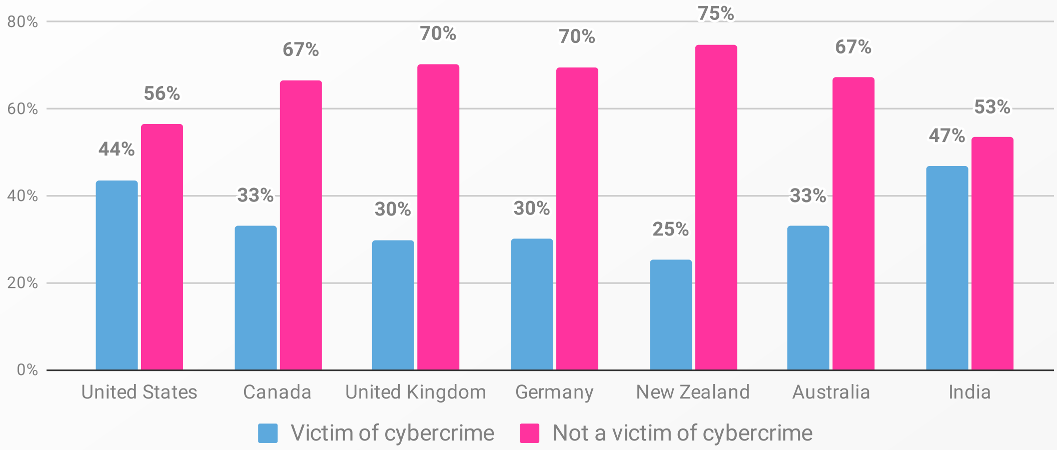


Figure 110. Percentage of cybercrime victims, by country.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants: 7012 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

Participants in the US and India were the most likely to have been victims of all three types of cybercrime measured—phishing, online dating scams, and identity theft (Figure 111).

Of all phishing victims, 20% were from India, followed by 17% in the USA. This trend was consistent across other cybercrimes: 24% of online dating scam victims were in India, followed by 19% in the USA, and 22% of identity theft cases were reported by Indians, followed by 21% in the USA.

It's important to highlight that in the past two years' reports, the USA had the highest percentage of victims and had been more likely to be victims of all cybercrime, but survey newcomer India has knocked it off the top spot—despite the percentage of victims in the USA having increased by 8% across all three crimes since 2023 (phishing by 7%, online dating scams by 5%, and identity theft by 6%).

Do different countries have different cybercrime weak spots? Compared to other cybercrimes, British (12%), Australian (14%), and New Zealander (12%) participants were more likely to fall victim to phishing. German (15%) and Indian (24%) participants were more likely to fall victim to online dating scams, while Americans were more likely to be identity theft victims. In Canada, an equal percentage of participants were victims of phishing and identity theft (14% each).

Likewise, some countries are seemingly more likely to fend off certain flavors of cybercrime. The lowest numbers of phishing incidents were in Germany (11%), while the lowest numbers of online dating scams and identity thefts were in New Zealand (8% each).

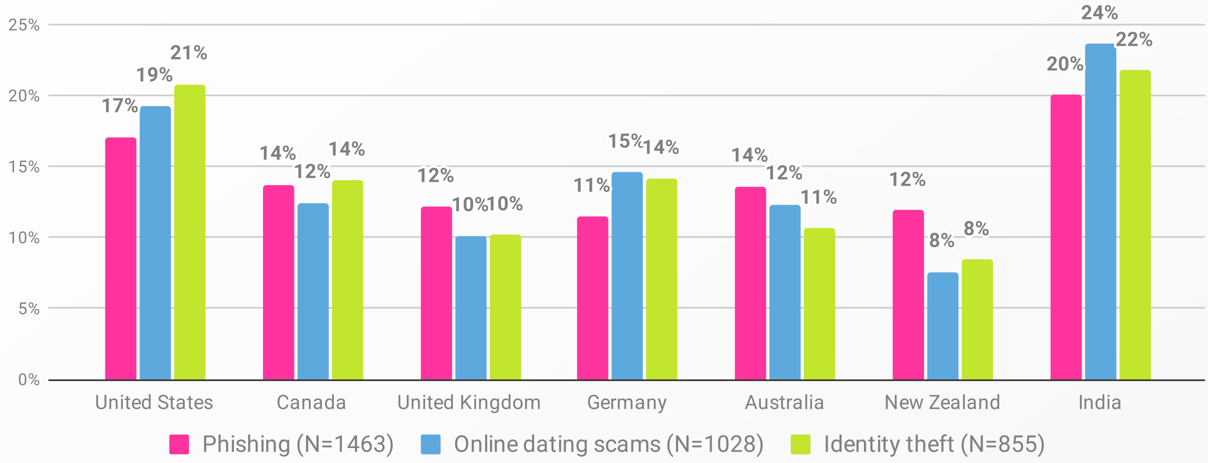


Figure 111. Crime prevalence by incident type, by country.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of cybercrime incidents: 3346. Total number of participants losing money to one or more incidents: 2425 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

We put our participants through their predictive paces, asking them if they thought they'd be targeted in the next year. Despite having the highest rates of 'I'm not likely to be a target' responses, 39% of participants from India said they felt they were likely to become victims of cybercrime in the next year, the highest among all countries surveyed (Figure 112). This is followed by the USA (31%), Australia (28%), and Canada (27%). The perceived likelihood of victimization in other countries ranged from 20% to 24%. New Zealanders appear the most optimistic, with 44% feeling they were unlikely to be victimized.

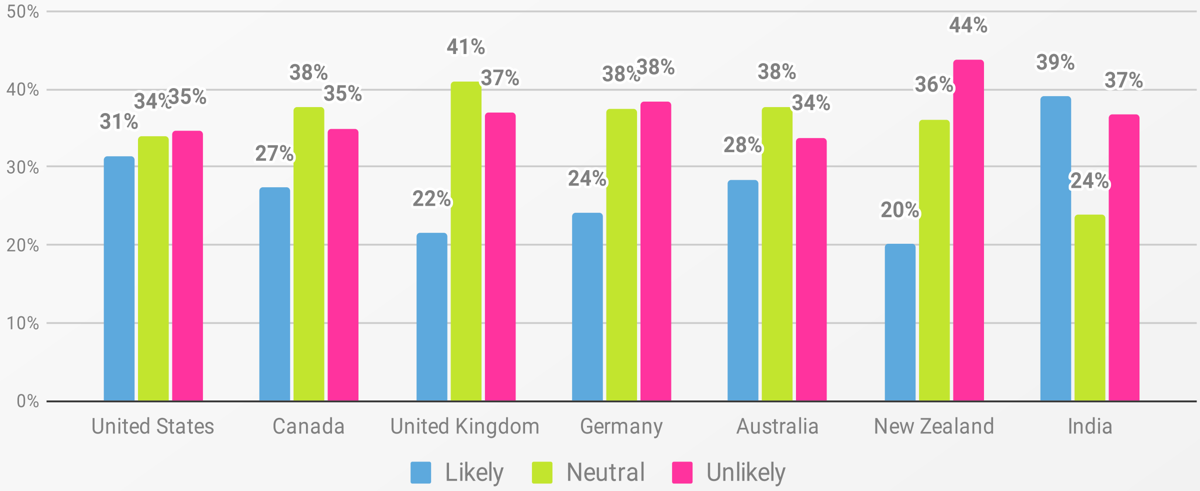


Figure 112. *"In the next year, how likely do you feel that you will become a victim of cybercrime?"* by country.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants: 7012 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

These findings tell us the cybercrime global playing field is anything but level. There are notable disparities in cybercrime victimization and perceptions across countries.

The USA stands out with high rates of identity theft, while New Zealand boasts the lowest victimization rates and the most optimism about being able to avoid falling prey to the bad guys. Meanwhile, the UK seems more likely to get reeled in by phishing scams. India is particularly intriguing here: Despite low perceived risk, India reported the highest victimization rates across all three types of cybercrime, closely followed by the USA.

Cybercrime reporting

Figure 113 shows us the percentages of phishing, online dating scams, and identity theft reported across different countries. The USA leads with identity theft reporting, with a stellar 96% (up 2% from 2023). Other reporting champions are India, where 95% of participants reported online dating scams, and Germany, where 91% reported phishing incidents.

Lagging behind in the reporting rankings were New Zealand. They came last for reporting both identity theft at 86% (up 3% on 2023), and online dating scams at 83%, though this was an impressive 14% increase from 2023.

Speaking of reporting #gainz, online dating scam reporting also increased by 10% in the USA and 16% in Germany. Reporting rates for phishing increased from last year in North America—by 1% in the USA and 4% in Canada—as well as in the UK (3%) and in New Zealand (5%).

However, it's not all good news: Identity theft reporting rates have dropped slightly from 2023 in European countries—by 1% in the UK and 2% in Germany—as well as in Canada, by 2%.

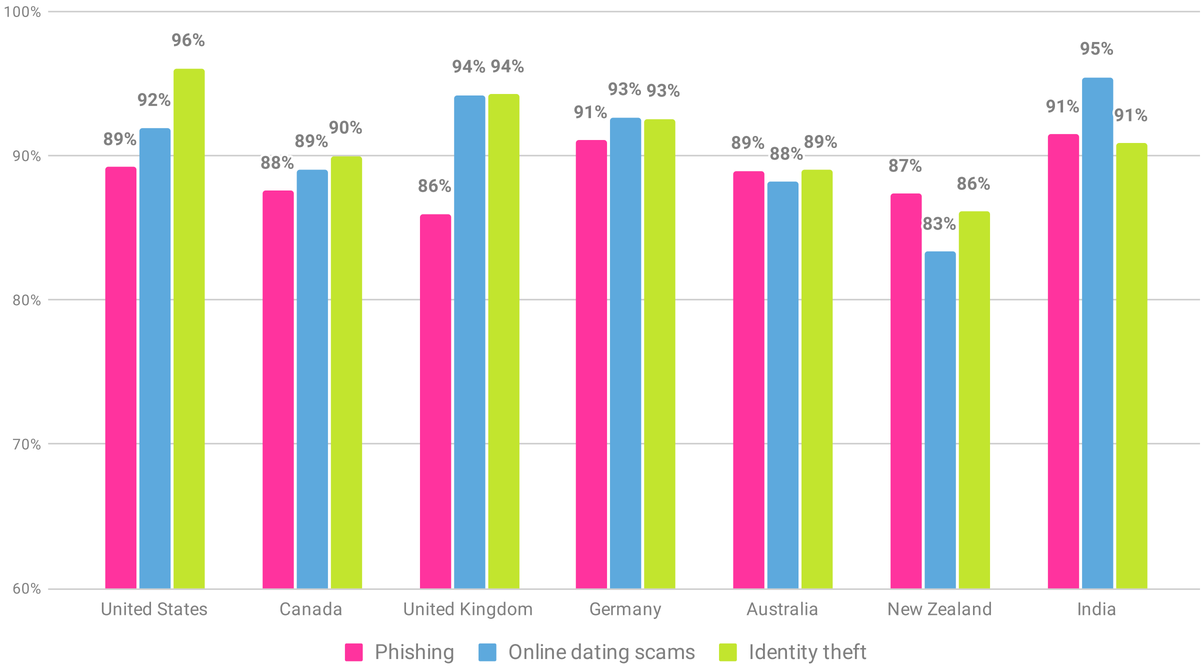


Figure 113. Percentage of cybercrimes reported to authorities, agencies, or organizations, by country.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants: 7012 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

So, where does that leave us? Overall, reporting rates for different types of cybercrime vary between countries. The US and India take the 'most likely to report' trophy, but we can't ignore the increases in reporting rates for online dating scams and phishing in several countries, including New Zealand, the USA, and Germany.

Cybersecurity training

Overall, access to cybersecurity training has increased in all countries since 2023, with notable increases of 7% in Germany and 6% in the USA, Canada, and the UK. But don't get too excited yet: Despite this growth, 66% of New Zealanders still do not have access to training (Figure 114), a stat that stubbornly refuses to budge from 2023. While access has improved, it remains generally low. India, on the other hand, leads the pack with 57% reporting having access, followed by the USA at 50%.

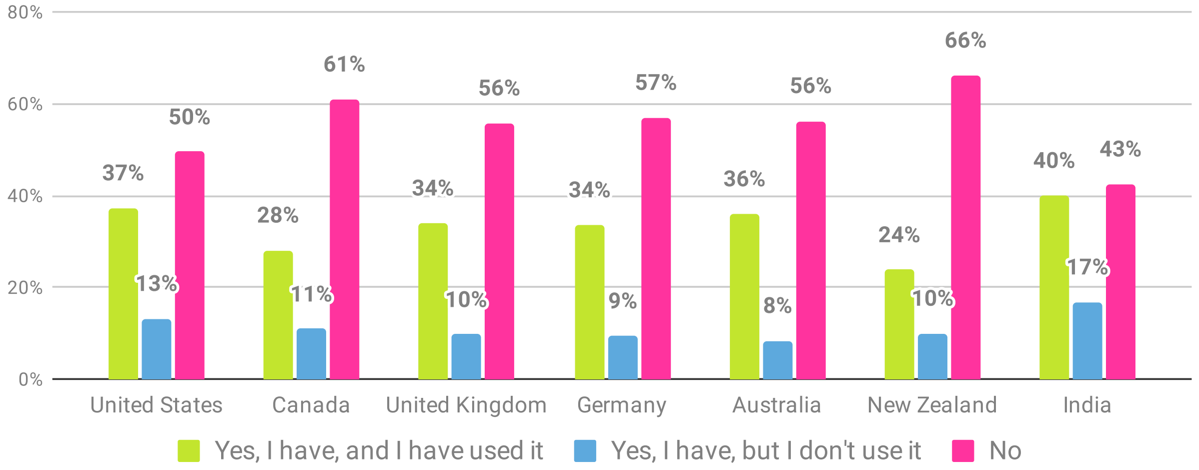


Figure 114. *"Do you have access to cybersecurity training (e.g., at work, school, or library)?"* by country.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants: 7012 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

For most countries, the workplace is the best spot for cyber-schooling, particularly among people in the UK (58%) and New Zealand (57%, Figure 115). Slightly more than a third (35%) of Americans accessed training at home. Accessing training at a participant's place of education was relatively low across all countries, with the highest proportion reported in India (14%).

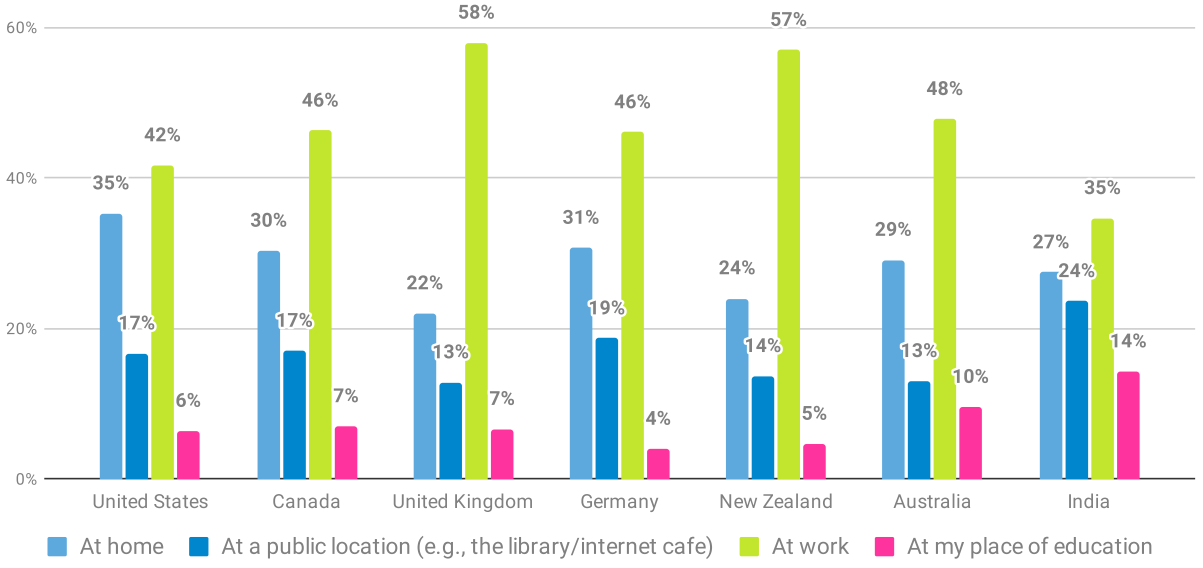


Figure 115. *"Where do you access the training?"* by country.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants who have access to training: 2336 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

Mandatory training completion was required amongst the majority of participants with access to cybersecurity training (N=1661) in all countries, ranging from 83% in Canada to 90% in Australia (Figure 116). Germany and New Zealand have both seen increases in mandatory training requirements, up by 6% and 5%, respectively.

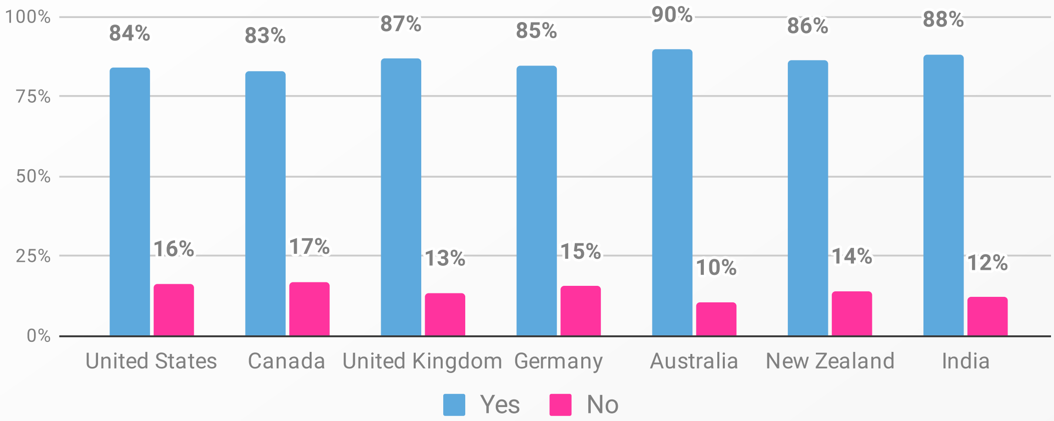


Figure 116. *"Are you required to complete mandatory cybersecurity training at work or your place of education?"* by country.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants with access to cybersecurity training at their place of work or education, and have used it: 1661 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

Annual mandatory training is the most common option across almost all countries (Figure 117), with the UK topping the charts at 61% (up 6% from 2023). The USA, meanwhile, is slippin', with 45%, down 5% from 2023. The lowest percentage of participants required to complete mandatory training once a year was from India (29%). Indian participants also reported the highest percentages for completing training 'when something goes wrong' (14%) and 'both at regular intervals & when something goes wrong' (30%).

Compared to last year (2023), the percentage of participants completing training both regularly and when something goes wrong increased in North America and Europe: by 6% in the USA, by 3% in Canada, by 2% in the UK, by 1% in Germany.

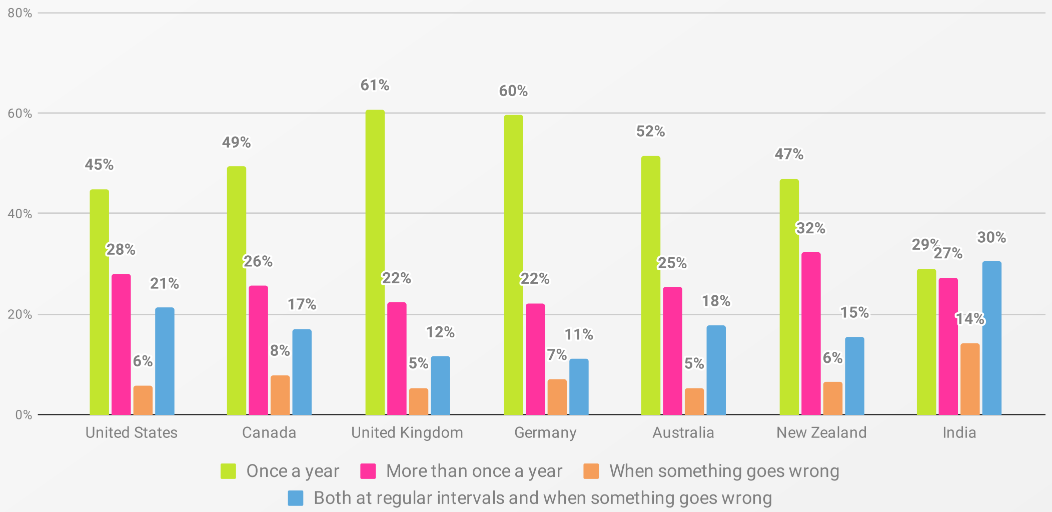


Figure 117. *"How often are you required to complete training?"* by country.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants who are required to complete mandatory training at their place of work or education: 1432 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

Video was the most preferred format across all countries for consuming cybersecurity training information, with the highest preference in the USA (26%, Figure 118). Germany, however, was decidedly more old-school, as the largest proportion of Germans preferred written training materials (24%). Short, bite-sized pieces of information were also popular in Germany (21%).

Online courses are popular in India (19%) and the UK (23%), though Brits seem to like video content just as much (23% also).

Online games were the least preferred format across all countries, with the highest preference being only 7% among Indian participants. *Cue sad electronic jingle.*

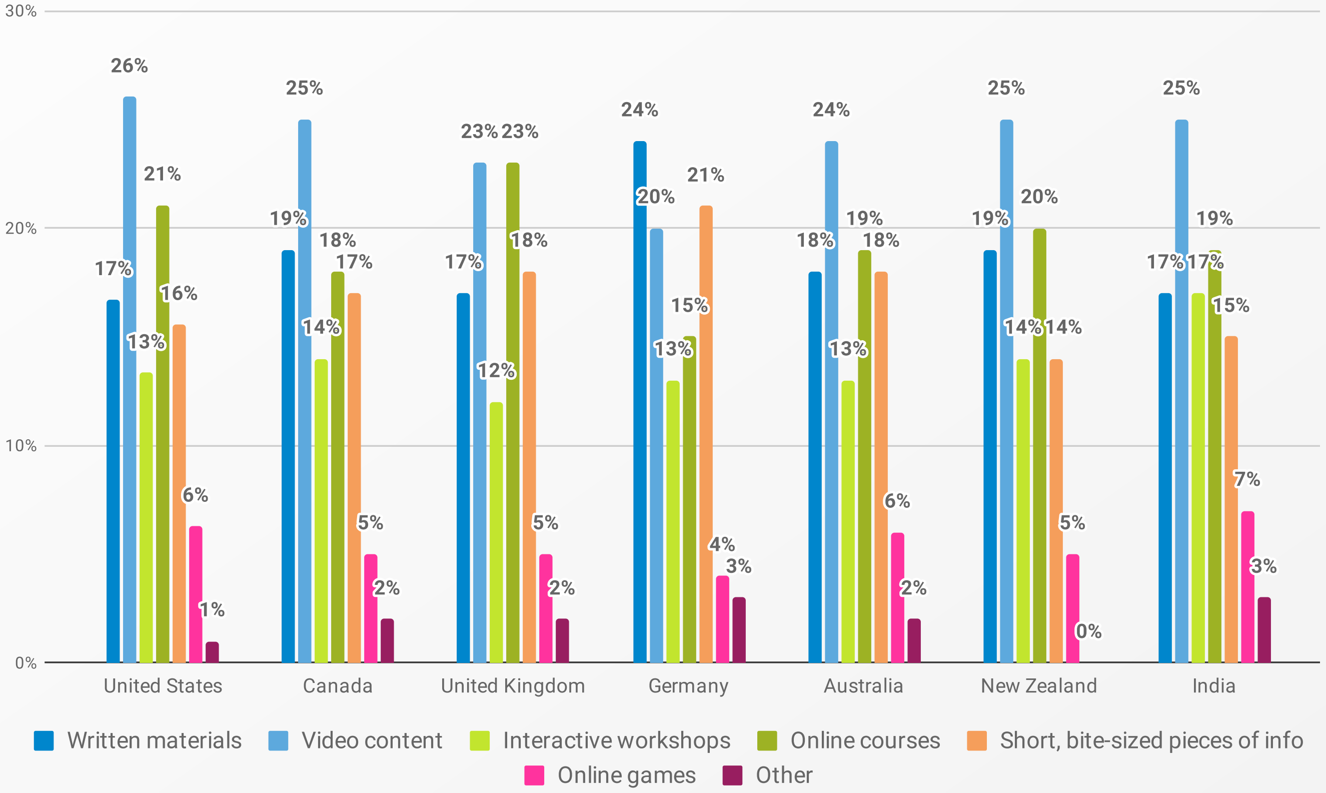


Figure 118. *"What format do you prefer to consume cybersecurity training information?"* by country.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants: 7012 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

Overall then, access to cybersecurity training has increased since 2023 across all surveyed countries, most notably in Germany, the USA, Canada, and the UK. Despite this, access remains low, especially in New Zealand.

Most training occurs at workplaces, particularly in the UK and New Zealand. Mandatory training requirements are prevalent in all countries, especially in Australia. The trend towards combining regular and incident-based training is growing (not a good idea FYI, as it associates training with the sensation of punishment), with notable increases in North America and Europe. Participants predominantly prefer video content for training, except in Germany, where written materials are favored, and online games are getting the global side-eye.

Cybersecurity knowledge & behaviors

It's time to break down the state of cyber smarts and habits across the globe. Who's ahead of the curve...and who's googling 'Is MFA contagious?'

In North America, the largest proportion of participants reported having 'basic' cybersecurity knowledge (40% Canadians and 35% Americans), followed by those with intermediate knowledge (36% Canadians and 35% Americans, Figure 119).

Elsewhere, the UK's on top with 46% of its participants having intermediate knowledge. But India is the standout star here, with 72% of Indian participants reporting either advanced or intermediate knowledge. When it comes to those completely in the dark about cybersecurity, the USA and the UK ranked highest, with 6% and 4% respectively saying they knew zilch.

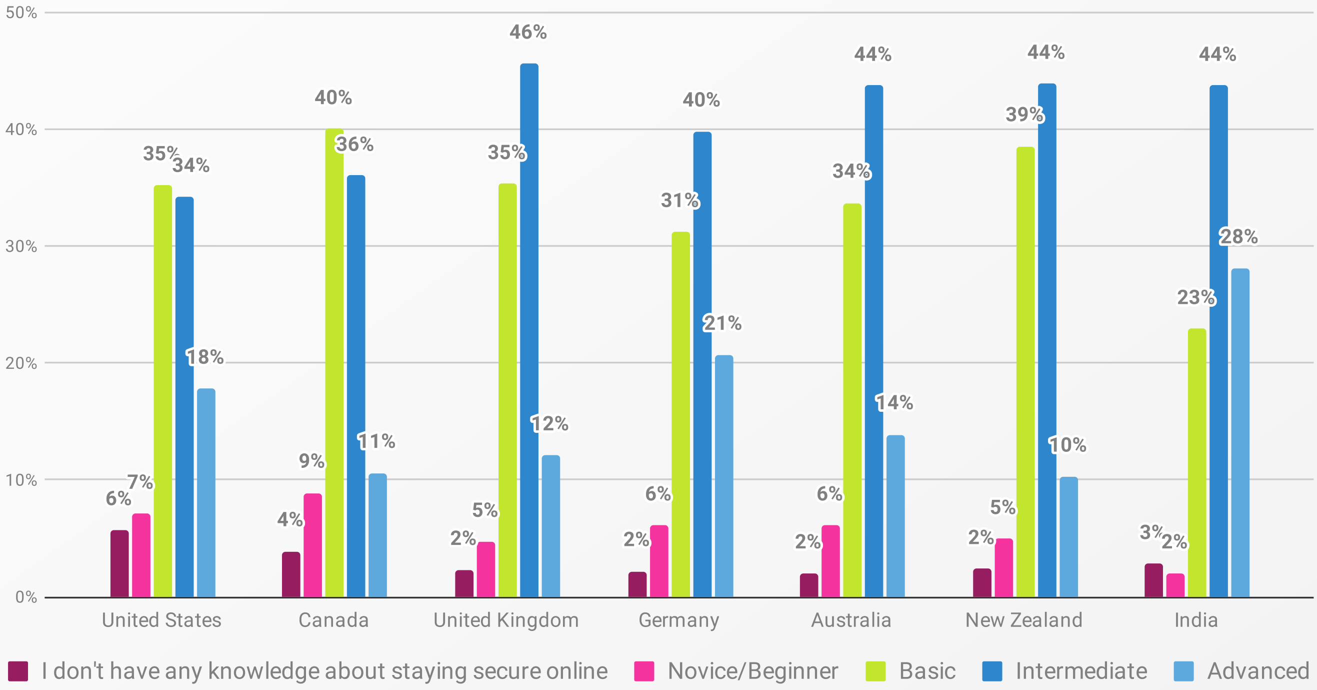


Figure 119. Self-reported cybersecurity knowledge, by country.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants: 7012 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

Password hygiene

Password practices are more varied than the ice cream flavors at a busy beach. The US and India are top of the password proactivity list, with 40% and 41% respectively using separate passwords for sensitive online accounts all of the time (Figure 120). All countries reflected this preference, except Germany, where the largest proportion used separate passwords the majority of the time (35%).

New Zealand participants (28% indicating ‘all of the time’ and 27% ‘the majority of the time’) tended not to use unique passwords as often as other countries. The highest percentage of those not using separate passwords were in the UK and New Zealand (5% each), and so were those using them ‘some of the time’ (19% of New Zealanders and 14% of British).

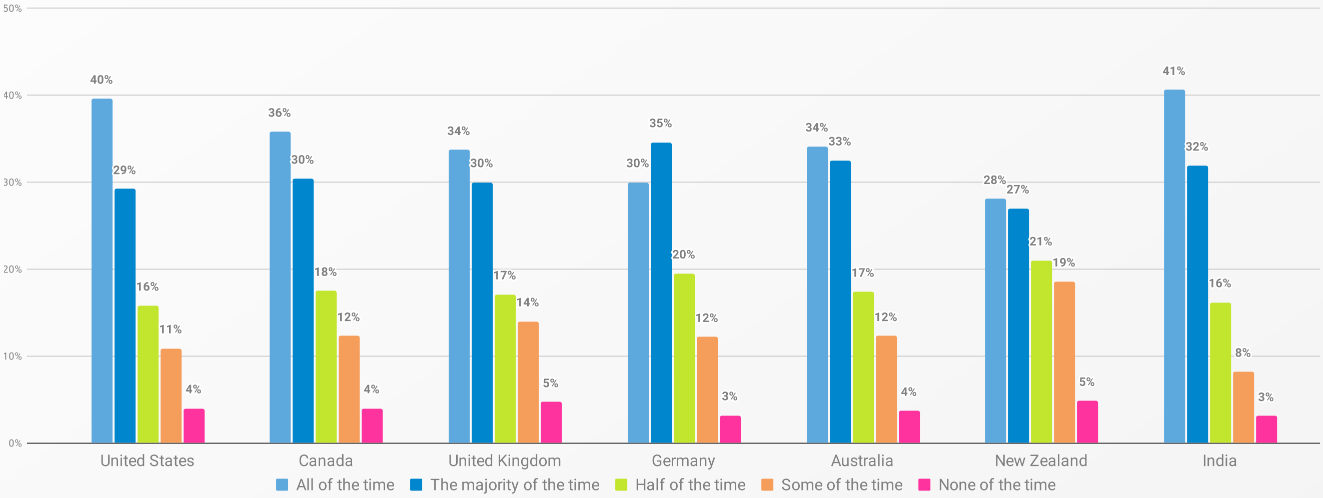


Figure 120. *“How often do you use unique passwords for your important online accounts (e.g., emails, social media, payment-related sites)?”* by country.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants: 7012 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

How about password creativity? We asked people if they used references to personal information (e.g., names and dates of birth), or if their passwords included a single dictionary word or name in which they had replaced some characters with numbers or symbols (Figure 121).

Indians admitted to doing so the most (50% and 59%, respectively), followed by Americans (36% and 43%). Happily, these percentages are on the decline—at least in the USA, where they dropped by 2% for personal info and 3% for a single dictionary word, respectively. As this is India’s first *Oh, Behave!* rodeo, we don’t have past data to compare with, but here’s hoping for progress in 2025.

Zooming out again, around a third of participants in other countries reported using personal information in their passwords. This practice has increased since 2023 in Germany by 5% and in Canada by 3%, but dropped in New Zealand by 3%.

The percentage of those creating passwords consisting of only a single dictionary word or a name with character replacements has increased in Canada by 7%, but dropped among British participants by 3%, Germans by 1%, and New Zealanders by 2% since 2023. So, no monumental sea-change in sight for the most part, just a fair bit of shuffling pet names and football teams.

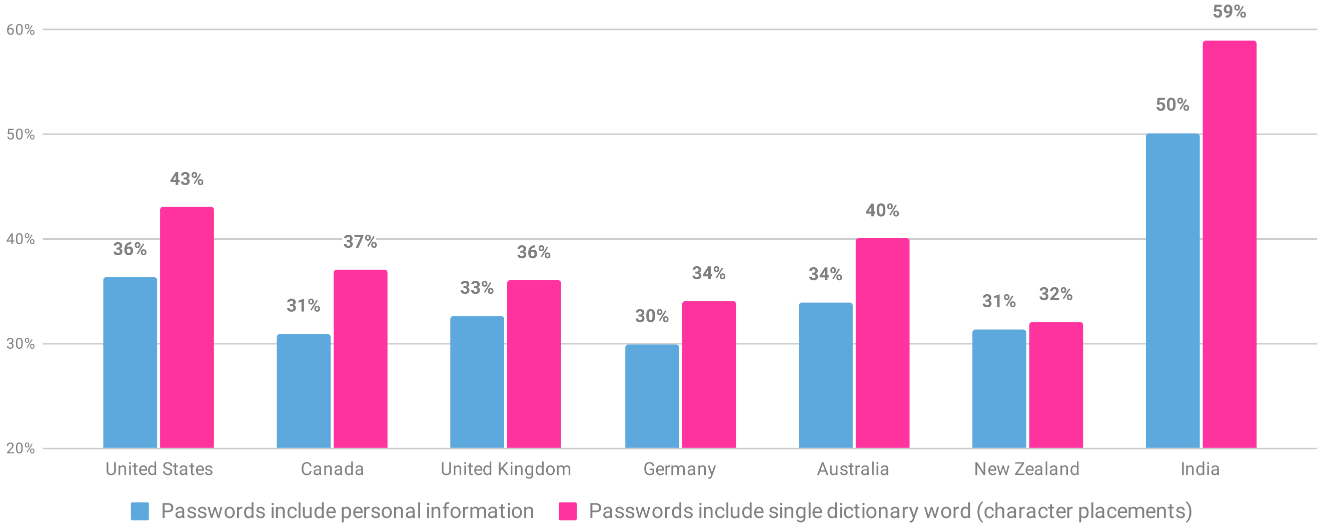


Figure 121. Password creation techniques used by participants, by country.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants: 7012 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

What about country differences in storing passwords? Indians (49%) reported using a password manager the most, followed by the Americans (43%, Figure 122), where this has increased by 5% since 2023. But these two nations are also most likely to stop using the tech (17% in India and 15% in the USA), along with Germany (also 15%).

The lowest uptake of password managers was in New Zealand (52%), though this represents an 8% jump from last year. Use of password managers increased amongst Canadians by 3%, the British by 4%, Germans by 5%, and New Zealanders by 8%.

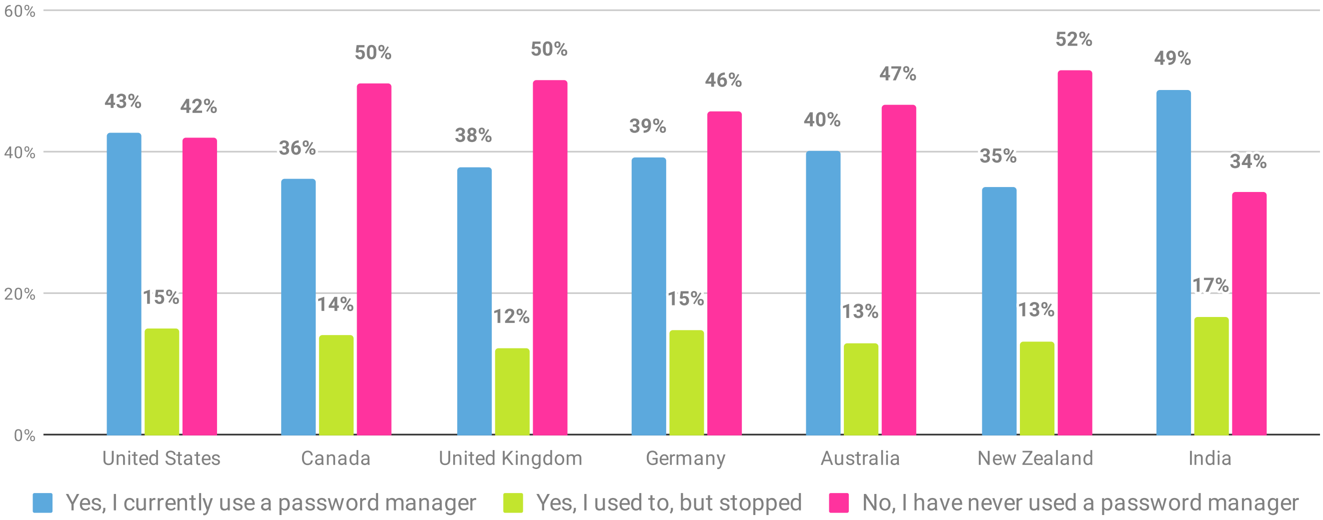


Figure 122. *"Have you ever used a password manager?"* by country.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants: 7012 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

Germany tops the charts for paid password manager use, with 33% shelling out for protection, which is the same as 2023 (Figure 123). Participants in New Zealand (50%), Australia (43%), India (41%) and the USA (40%) preferred saving their passwords in their internet browser, while British (44%), Canadian (43%), and German (38%) participants preferred free stand-alone password managers. It looks like there's a tie in the splurge vs freebie game.

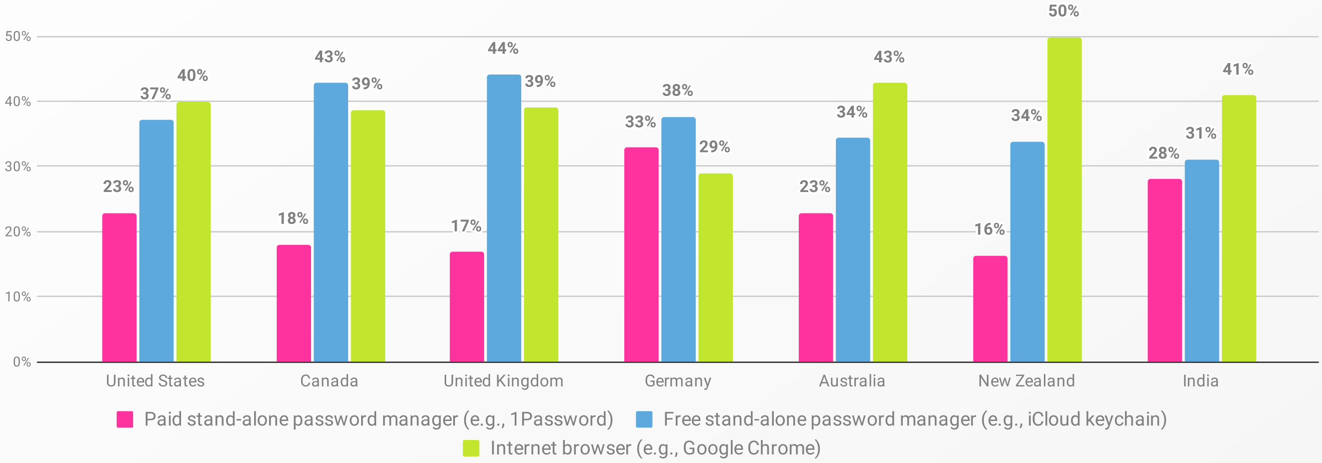


Figure 123. ***"What is your preferred password manager?"*** **by country.**

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants using password managers: 2803 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

Enabling MFA

The majority of participants in all countries have heard of MFA, ranging from 75% in Germany to 86% in India. But how about, y'know, using it?

In the lead are the Australians, where 74% of those who'd heard of MFA were using it regularly (Figure 124). At the bottom of the charts, 58% of German participants who had heard of MFA reported regular usage, on the heels of India (61%). Germany also had the highest proportion of participants not knowing how to use MFA (16%), followed by New Zealand (12%).

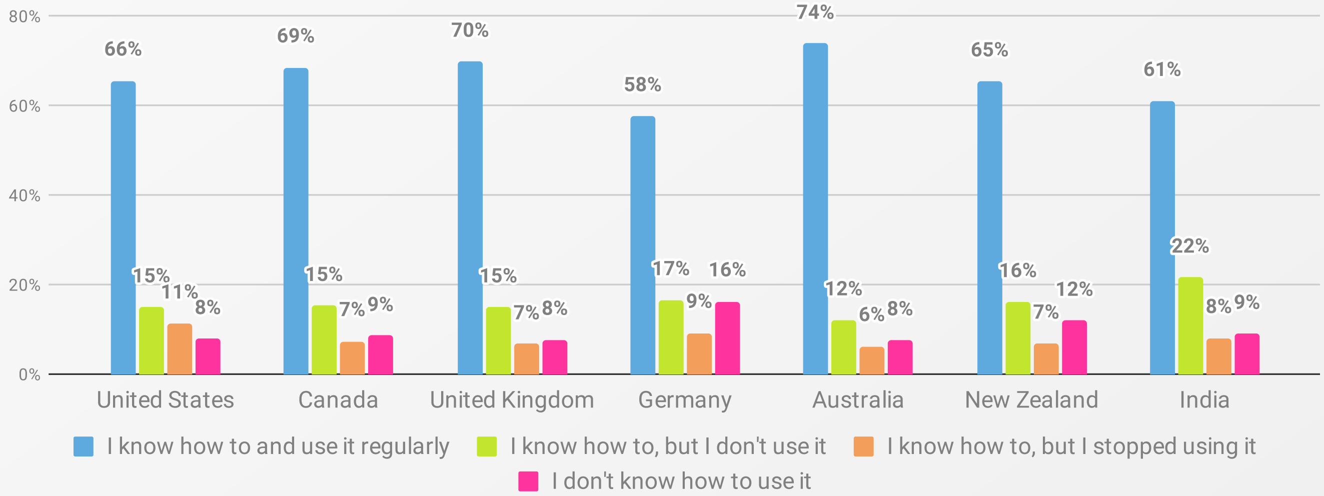


Figure 124. ***"Do you know how to use MFA?"*** **by country.**

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants who have heard of MFA: 5694 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

Installing software & app updates

Who's up on their updates? New Zealand has the highest proportion of people that make sure their devices run with the latest version of software and/or applications, with 60% of people selecting either 'always' or 'very often' (Figure 125), Australia and the UK are hot on New Zealand's heels (both 59%). On the flip side, 18% of Canadians and 17% of American and German participants admitted to 'rarely' or 'never' installing the latest versions of updates.

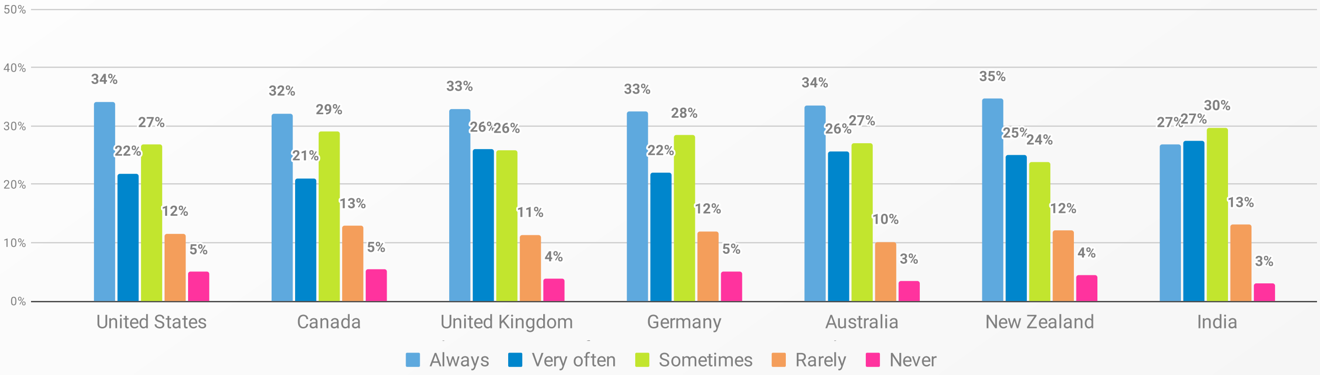


Figure 125. *"How often do you install the latest software or application updates to your devices when notified that they are available?"* by country.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants: 7012 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

Backing up data

We're trying not to overuse 'mixed bag'… yet here we are again. But when it comes to backups, a healthy chunk of folks in most countries said they backed up 'sometimes', ranging from 30% in the USA to 36% in Germany.

The exception was India, where the largest percentage (35%) reported 'very often' backing up their data (Figure 126). If we turn our attention to the regular backup crew (i.e., combining the 'always' and 'very often' responses), India is leading (59%), followed by the USA and UK (both 46%). While New Zealand had the highest proportion of those 'never' and 'rarely' backing up (26%), this represents a 7% increase from 2023.

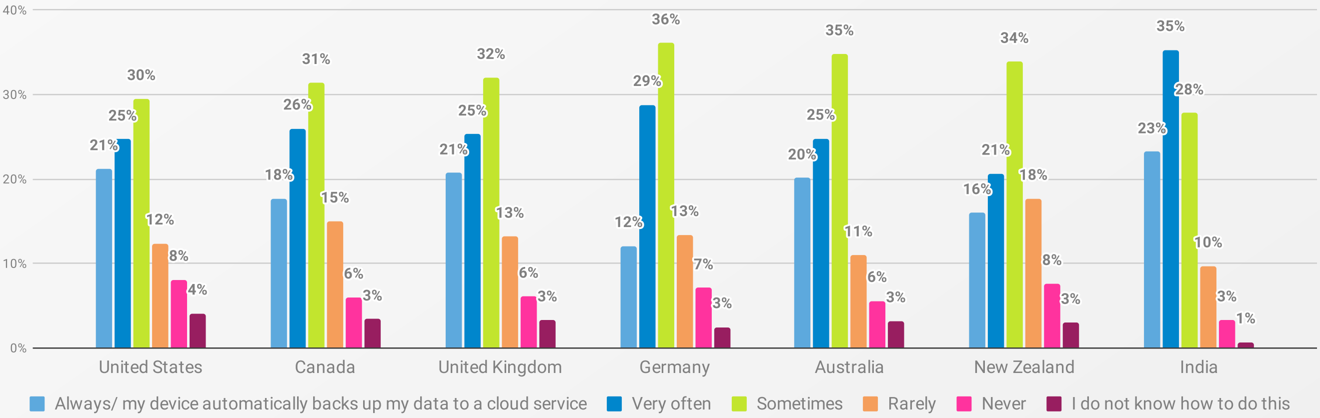


Figure 126. *"How often do you back up your most important data?"* by country.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants: 7012 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

Recognizing & reporting phishing messages

When it comes to spotting phishing messages and malicious links, Indians (73%), British and Australians (70%) felt the most confident (Figure 127). However, as in last year's report, Germans are floundering (sorry), with just 52% feeling buoyant (sorry again)—though this is up 2% since 2023.

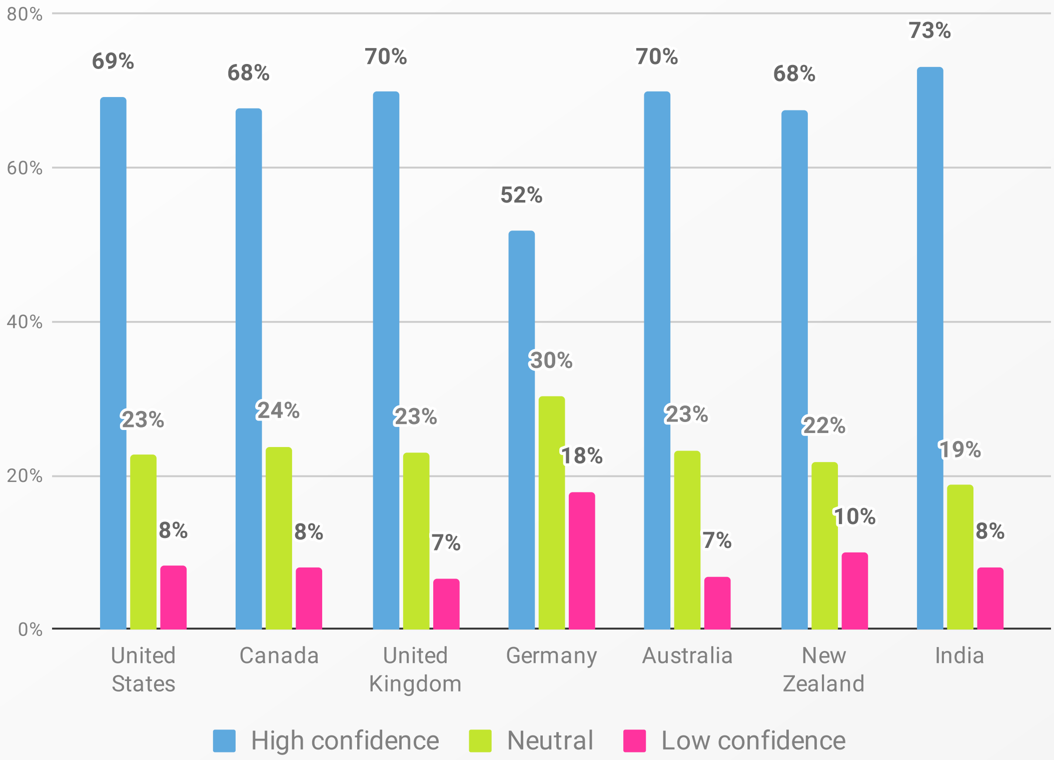


Figure 127. *"How confident are you in your ability to identify a phishing email or a malicious link?"* by country.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants: 7012 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

Checking messages for signs of phishing was similar across the seven countries. The highest proportion of those checking messages 'always' or 'very often' were in Australia (72%), while the lowest was in Germany (63%). Never checking messages or not knowing how to identify them were also highest among Germans (5% and 4%, respectively).

Reporting phishing messages 'always' or 'very often' was highest among Americans (55%, Figure 128), followed by 51% of Indians, and lowest amongst Germans (39%). Furthermore, the percentage of those 'never' or 'rarely' reporting phishing was highest amongst participants from Germany (27%), as was those not seeing a spam or reporting button (5%).

So, the gist is plenty of people are confident that they can identify a phishing email, but reporting is a bit hit-or-miss.

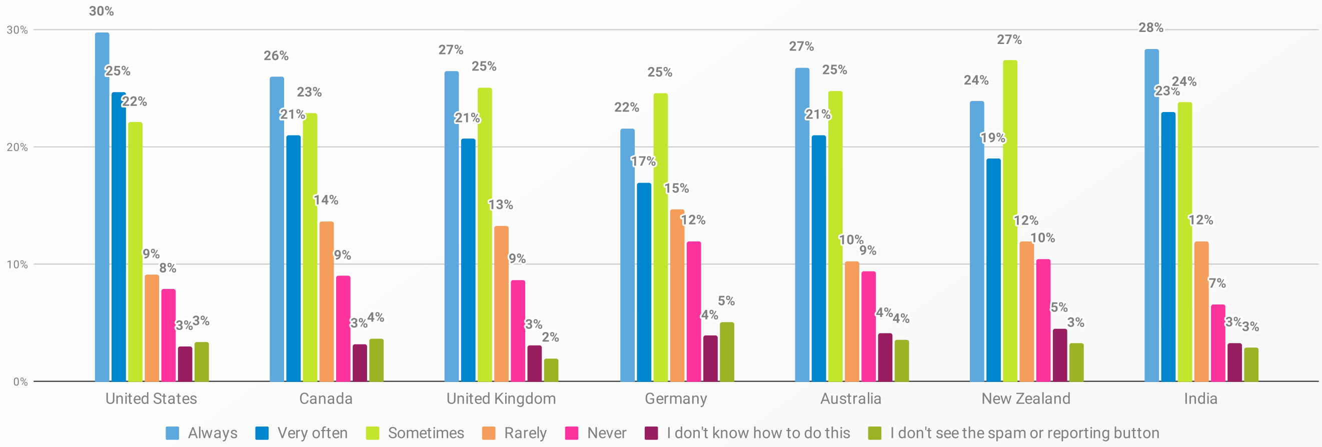


Figure 128. *"How often do you report phishing messages by using the 'spam' or 'report phishing' button?"* by country.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants: 7012 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

Artificial intelligence (AI)

The time has come—how are different countries navigating AI's rapid advancement? We've got the whirlwind tour right here, with a few surprises and eye-opening stats. Buckle up!

AI use is big in India, with a huge 74% reporting using AI tools (Figure 129). The USA follows with 45%, closely followed by participants from other countries, ranging from 42% (Australia) to 32% (New Zealand).

As you'd expect from that last stat, New Zealanders were least likely to use AI tools, with 68% reporting they did not utilize them.

When it came to where people used AI tools, twice as many Indian respondents used them at both home and work than in the UK and Australia (both 16%).

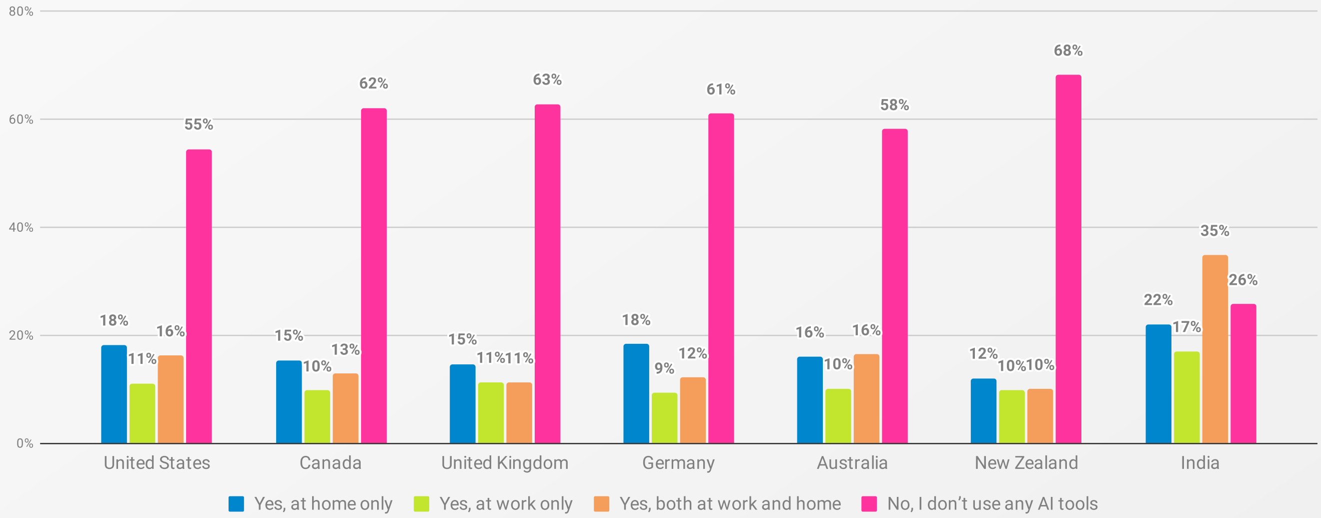


Figure 129. *"Do you use any AI tools at home or at work?"* by country.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants: 7012 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

In Germany, 52% of those using AI tools have received training (Figure 130). Training rates were somewhat similar in the US and India, with 49% of users receiving training. But other countries seem to be skipping class: The majority from New Zealand (65%), the UK (62%), and Canada (61%) report not receiving any training on AI security and privacy risks.

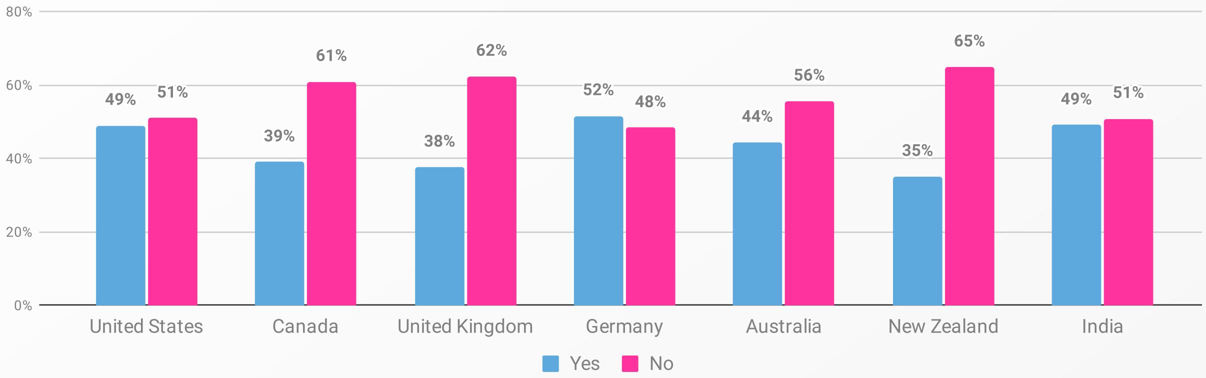


Figure 130. *"Have you received any training about the security and privacy risks of AI tools?"* by country.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants who use AI at home only, at work only, or both at home and at work: 3087 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

Notably, a little less than half (48%) of the participants from Germany, who are using AI tools, reported sharing sensitive information without their employer's knowledge (Figure 131). This was closely followed by 47% of US participants and 41% of respondents from India.

We need to pause here for a sec. In case you missed it, the very countries who've had more AI training are the ones who are more likely to share sensitive info with AI. It's a classic case of that often overlooked fact that training **does not** magically help people develop flawless security behaviors.

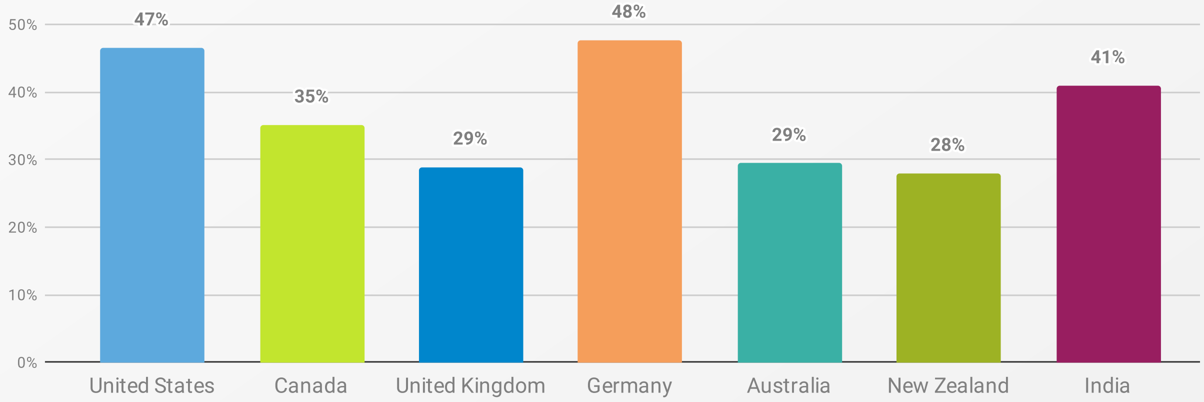


Figure 131. *"Have you ever shared sensitive work information with AI tools without your employer's knowledge?"* by country.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants who use AI tools for work and at home and work: 2042 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

AI's got plenty of people on edge: The majority of all participants (65%) were concerned about AI-related cybercrime, with consistent levels observed across countries, ranging from 58% in New Zealand to 71% in India (Figure 132).

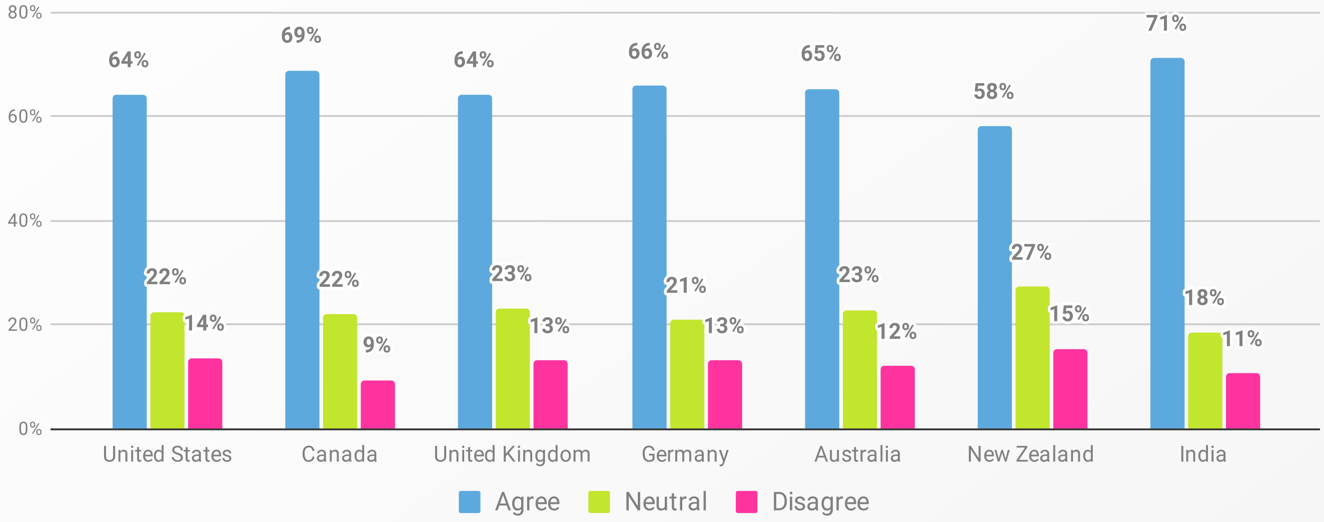


Figure 132. *"I'm concerned about AI-related cybercrime."* by country.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants: 7012 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

Trust in AI companies was more mixed, however. The majority (71%) of participants from India expressed high levels of trust in companies responsibly implementing AI (Figure 133). Conversely, the rest of the countries expressed lower levels of trust, ranging from 47% in New Zealand to 35% in Australia.

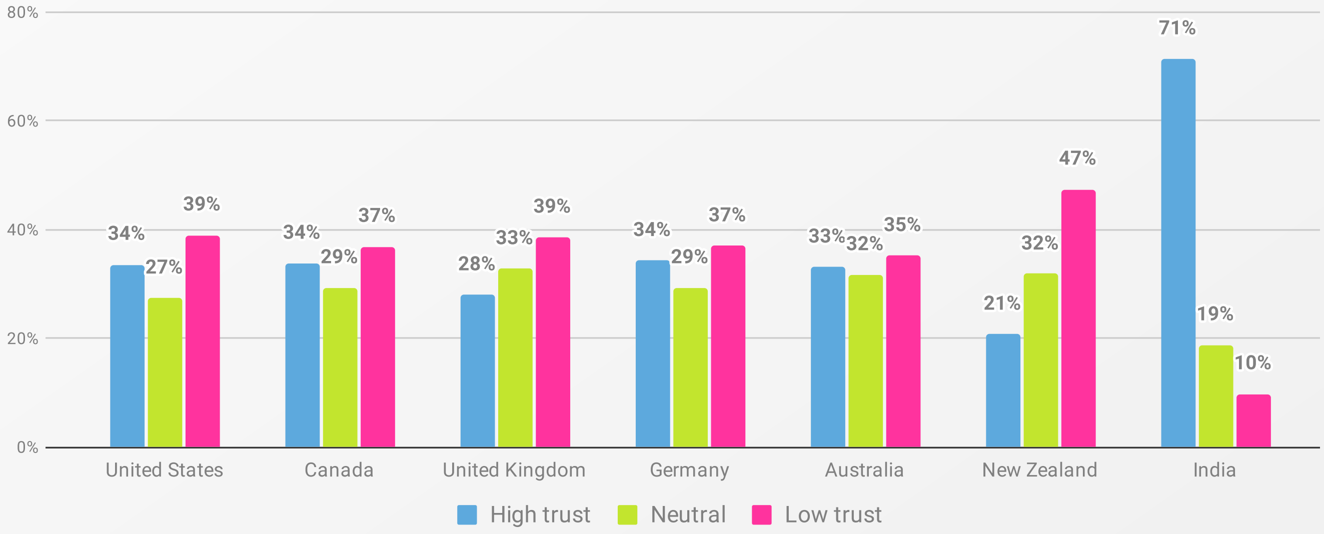


Figure 133. Participants' level of trust in companies to implement AI responsibly, by country.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants: 7012 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

The majority of participants from India also believed companies creating AI technologies are integrating security from the start (66%) and ensuring their tools are free of bias (68%). This is in contrast to participants from other countries who were more (dare we say, rightly) skeptical. The proportions of those agreeing that security is integrated from the start ranged from 24% in New Zealand to 36% in Australia, while the belief that companies ensure their AI tools are free of bias ranged from 21% in New Zealand to 34% in Canada.

Being a tech company who gives a shi*t about this kind of thing, we'll use this as an opportunity to promote the acclaimed, award-winning documentary, Coded Bias: https://www.codedbias.com/

Participants from New Zealand had the highest rates of low confidence (48%), followed closely by those from Germany (46%). Conversely, 68% of participants from India felt confident in their abilities to recognize AI content, far surpassing respondents from other countries (Figure 134).

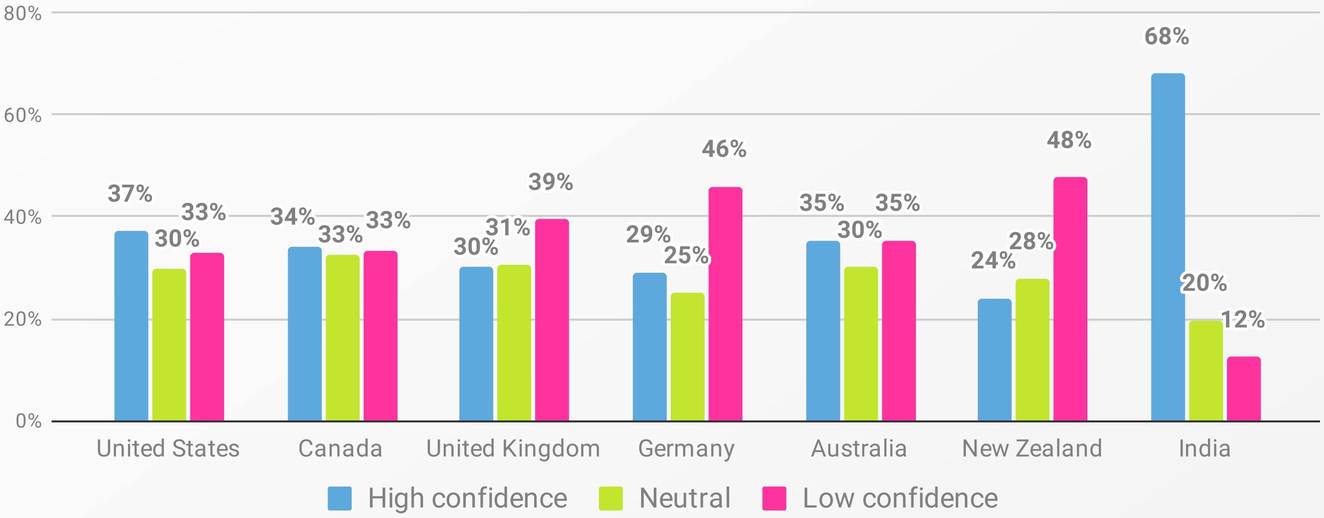


Figure 134. Participants' level of confidence in their ability to recognize AI-generated content, by country.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants: 7012 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

Across the board, people think AI will make it harder to detect scams. This view was held by the largest proportion of participants from every country, ranging from 50% in Germany to 58% in India. Similarly, most participants thought it likely AI would make it harder to stay secure online, ranging from 49% in New Zealand to 60% in India.

And last but not least: elections. A key issue in 2024 in some parts of the world, and making an appearance in our survey for the first time this year.

The only country where the notable majority felt it likely AI would influence their decision on what is real and fake during election campaigns was India (57%, Figure 135). This was followed by 37% in the USA, though 33% felt it to be unlikely.

In the remainder of the countries, the largest proportions held a neutral view on the matter, highest among British participants at 39%. In some countries, these views were fairly balanced: 34% of Germans were neutral, with the same percentage reporting likely AI influence; 36% of Australians were neutral, with the same percentage reporting likely AI influence.

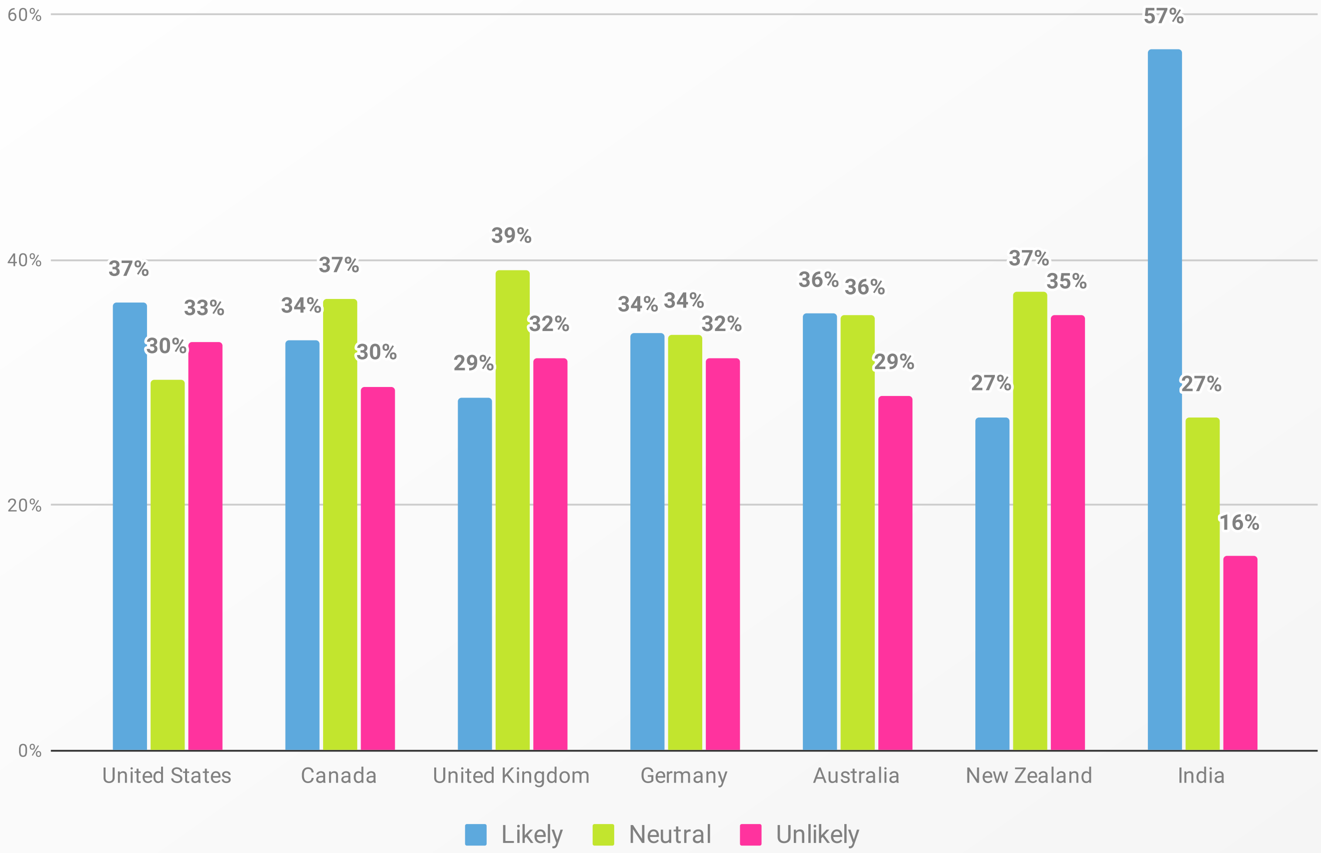


Figure 135. Perceived likelihood of AI's influence on decisions regarding what is real and fake during election campaigns, by country.

Base: US, Canada, UK, Germany, Australia, New Zealand, and India. Total number of participants: 7012 (age 18+). Dates conducted: March 6, 2024 - April 22, 2024.

It's clear there are big differences in how countries use, train on, and think about AI. India stands out as having the highest adoption rates of AI tools, both in personal and professional settings. They also reported a strong confidence in companies' responsible implementation of AI, as well as in their own ability to recognize AI-generated content.

Conversely, participants from New Zealand exhibited the lowest adoption rates and confidence levels in AI-related matters, alongside notable skepticism about companies' efforts in AI security and bias prevention. Germany and Australia aren't far behind.

Training on AI tools and security varied widely, and was not a reliable indicator of safer working with AI. A notable portion of participants from Germany, the US, and India reported formal training, while the majority from New Zealand, the UK, and Canada did not receive such training. Additionally, sharing sensitive information without employers' knowledge was a common concern, particularly in Germany and the US.

The survey also revealed widespread concern about AI-related cybercrime and its potential to complicate online security and scam detection. This concern was most pronounced among participants from India, who also felt strongly about AI's influence on their decision-making during election campaigns.

NATIONAL
CYBERSECURITY
ALLIANCE

A leading non-profit 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 human risk management platform designed to reduce human cyber risk in the modern, remote, and hybrid work environment, by measuring and influencing specific security behaviors.

CybSafe is powered by **SebDB**—The world's security behaviors database—and built by the industry's largest in-house team of psychologists, behavioral scientists, analysts, and security experts. An award-winning, fully scalable, and customizable solution, it's the smart choice for any organization.

- 91% Reduction in high-risk phishing behavior
- 55% Improvement in security behaviors
- 4x More likely to engage in cybersecurity initiatives

Authors

Dr. Suzie Dobrontei, CPsychol, Behavioral Scientist, CybSafe
Dr. Jason R.C. Nurse, Director of Science & Research, CybSafe
Toby Tracey, Research Analyst, CybSafe

Contact us: research@cybsafe.com

Expert contributors

Lisa Plaggemier, Executive Director, The National Cybersecurity Alliance
Oz Alashe MBE, CEO & Founder, CybSafe
Jennifer Cook, Senior Director of Marketing, The National Cybersecurity Alliance

Acknowledgements

Rebecca Ambler, Senior Communications and Engagement Advisor, New Zealand's National Cyber Security Centre (NCSC)
Matthew Salier, CEO, Australian Cyber Collaboration Center
Adam Brett, Senior Account Executive, Crenshaw Communications
Patrice Gamble, Account Director, Crenshaw Communications
Colleen O'Connor, Senior Account Executive, Crenshaw Communications
Michelle Barrett-Chang, Global Head of Customer Engagement, SAP Global Security & Cloud Compliance
Michael Baxter, Head of Security Communications, SAP Global Security & Cloud Compliance
Joe Giddens, Director of Content & Communication, CybSafe
Alice Cooke, Copywriter, CybSafe
Marina Soto, Visual Designer, CybSafe
Dr. Inka Karppinen, CPsychol
Dr. Ana Levordashka, User Researcher, CybSafe