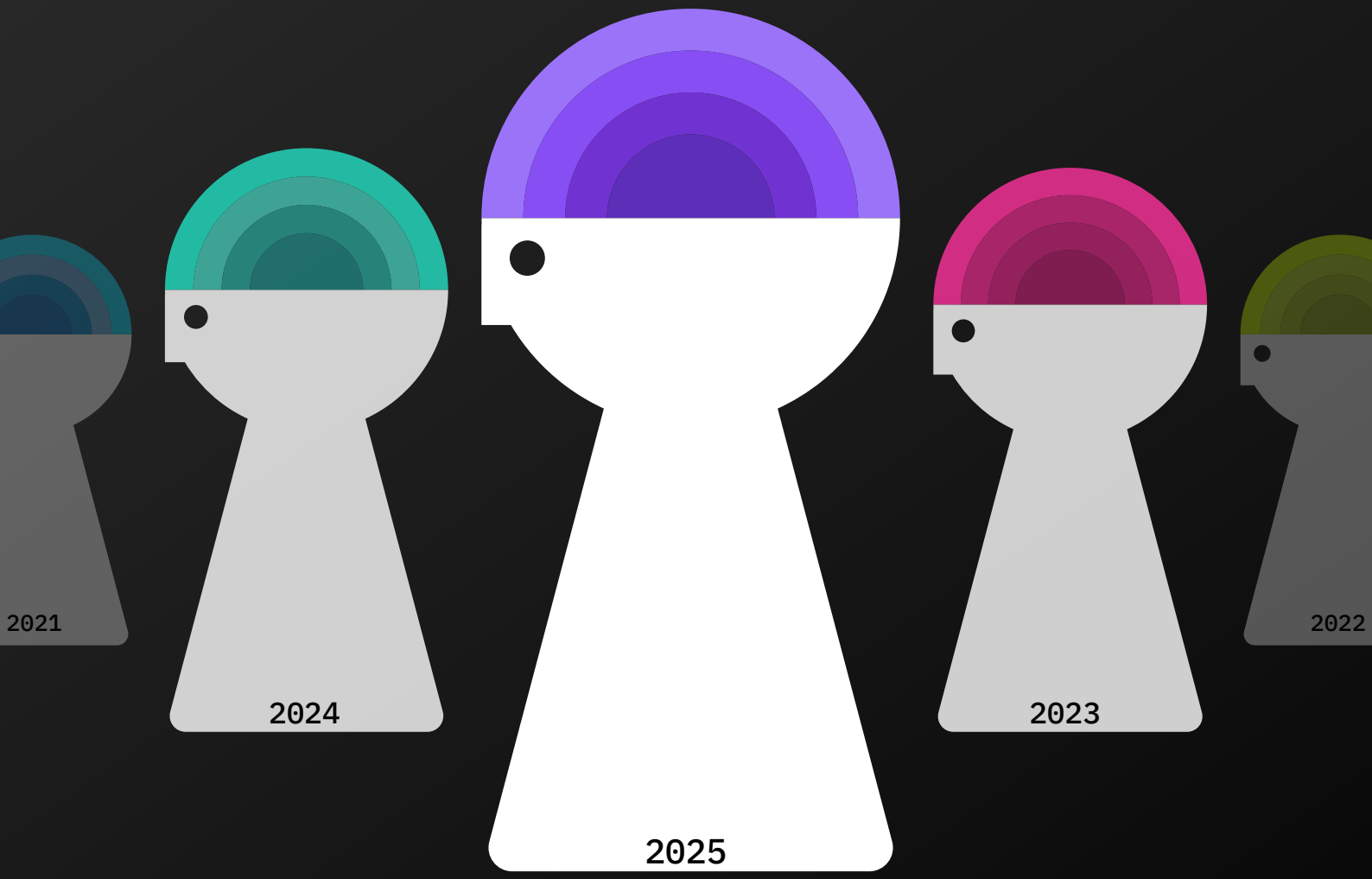
NATIONAL CYBERSECURITY ALLIANCE

CYBSAFE



A COMPARATIVE ANALYSIS OF KEY TRENDS
(THAT EVERY SECURITY LEADER SHOULD KNOW ABOUT)

Oh, Behave!

The Cybersecurity Attitudes and Behaviors Report 2021-2025

Contents

More BS* than an influencer's 4am morning routine 🏋️‍♂️🧘‍♂️

Welcome to the Oh, Behave! Cybersecurity Attitudes and Behaviors Report: 2021-2025.

Five years. Five reports.

If there's one thing we've learned from half a decade of tracking how people actually behave online, it's this: snapshots are useful, but they only tell part of the story. Single-year surveys tell you what people think right now. But trends? Trends tell you where we're actually heading, and how much nervous sweat it's reasonable to be producing about the destination.

Now, we're switching it up. We've gone back through five years of data, from 2021 to 2025, to see what's really changed. Not just the headlines. Not just the percentage jumps. But the patterns that have been vibing in the background the whole time.

The long view reveals what snapshots miss

Here's what we found when we stopped asking 'What's happening?' and started asking 'What's been happening?'

Some things look good. MFA awareness increased. People are creating longer passwords. Cyberbullying reporting rates have increased. You look at those numbers and think, 'Nice. Gold star for humanity'.

Then you turn the page.

MFA usage has collapsed. The share of people who 'always' install updates has dropped. The number of people who consistently check for phishing has decreased. And nearly half now feel so overwhelmed by security information that they're doing less to protect themselves.

In other words, we're getting better at knowing and worse at doing. And that gap is stretching like the elastic in a very old pair of sweatpants.

Trends don't lie (but they do surprise)

The beauty of comparing data is that it shows you what's sticking and what's just a one-year wonder. A single year might show a spike in training attendance. Five years show you that access to training has barely budged, and the people who do attend report declining impact.

One year might suggest people trust MFA. Five years reveal they're actively abandoning it, not because they don't understand it, but because they've decided their passwords are 'strong enough'.

Trends drag the awkward stuff into the light. Like the fact that time pressure as a barrier to reporting phishing is up, not because people are busier, but because security has slipped into the 'nice if we have time' column when the deadlines are looming. Or that security fatalism (believing efforts are pointless) has nearly doubled in three years.

These aren't blips. They're patterns. And patterns demand different answers to one-off problems.

Why this one isn't for the 'I'll get to it later' pile

We're at a crossroads. The data shows people aren't apathetic, they're exhausted. They're not ignorant, they're overwhelmed. And they're not careless, they're making rational trade-offs in an environment that makes secure behavior feel like the hardest option.

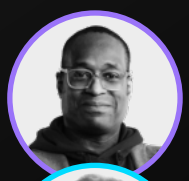
Understanding how we got here is the only way to figure out where to go next. That's why this five-year view matters. It's not about celebrating wins or catastrophizing losses. Essentially, we're turning the big light on, looking at everything properly, and identifying what actually needs to be fixed, rather than just shutting the door on it and hoping for the best.

So buckle up. This report is big, sprawling, and occasionally uncomfortable. You'll see where we've made progress, where we've stalled, and where we're quietly sliding backward on a wobbly office chair. You'll see why awareness campaigns aren't enough, why training keeps bouncing off busy brains, and why motivation, not knowledge, is now the biggest barrier to security action.

Most importantly, you'll see the trends. And once they're on your radar, they're not just going to politely disappear.

Here's to five years of data, five years of insights, and the (slightly sweaty, extremely necessary) hard work ahead to close the gap between what people know and what they actually do.

Oz & Lisa



Oz Alashe, MBE
CEO & Founder, CybSafe

Lisa Plaggemier
Executive Director, The National Cybersecurity Alliance

* Behavioral science, of course.

Report aim & structure

What's this report all about, then?

Our Oh, Behave! Cybersecurity Attitudes and Behaviors Report: 2021-2025 aims to provide the first comprehensive, five-year analysis of people's cybersecurity attitudes and behaviors across a broad mix of people in different regions.

This year-on-year comparison report is based on the data published in our previous Oh, Behave! Report, from its inception in 2021 till 2025. Using over half a decade of data, we analyze critical trends and persistent challenges that shape people's security habits today.

Who's it for?

You. Because chances are if you're reading this, you're someone who owns or influences human risk programs: CISOs, security leaders, risk owners, policy makers, and partners in HR and compliance.

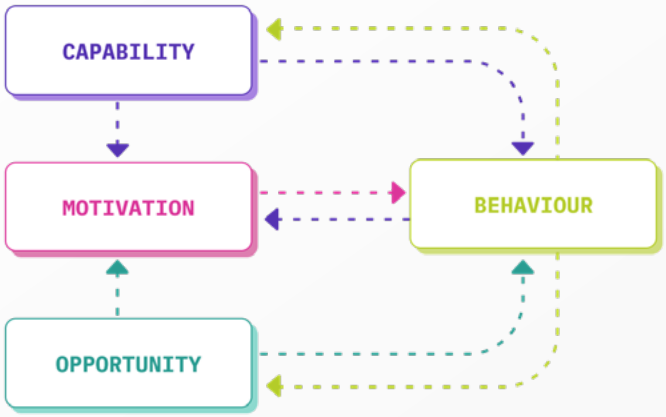
So, this one goes out to you. You can use it to decide which behaviors to prioritize, where to invest, and how to evidence change.

What guided our thinking?

This report uses the COM-B[1] (Capability-Opportunity-Motivation-Behavior) model as its analytical framework. COM-B recognizes that for any behavior to occur, three essential components must be present:

- **Capability** – the psychological and physical ability to perform the behavior (knowledge, skills, cognitive capacity)
- **Opportunity** – external factors that make the behavior possible (time, resources, environmental support)
- **Motivation** – the cognitive and emotional processes that drive action (attitudes, beliefs, intentions)

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



This framework helps us understand why people do or don't perform security behaviors. A person may have high motivation (positive attitudes toward security) but still not act if they lack capability (don't know how to enable MFA) or opportunity (no time for training). Looking at all three together gives us deeper insight into the things that stop people turning good intentions into safer behavior, because (spoiler) this is a persistent pattern that appears throughout the findings.

In this report we use COM-B to pinpoint where people are already motivated but stuck, where they have the skills but lack the time or support, and where the environment may be subtly working against them. This helps you, dear reader, see which lever's missing for each behavior and where to put your efforts and resources.

What human cyber risks did we measure?

Our analysis centers on changes in core security attitudes and behaviors, including:

- **Attitudes and perceptions**: Assessing motivation, self-efficacy, and the growing barriers (cost, confusion, and overwhelm) to security.
- **Responsibility and ownership**: Analyzing who individuals believe is responsible for security in personal and professional contexts.
- **Cybercrime victimization**: Tracking the rising prevalence of incidents and the related attitudes.
- **Cybersecurity training**: Investigating the access, prevalence, and perceived efficacy of training programs.
- **Five specific groups of security behaviors**:
  - Ensuring password hygiene[2] (length, creation habits, management techniques).
  - Using multi-factor authentication (MFA)[3].

2 SebDB behaviors: [SB003] Authenticates with a strong password (or passphrase), [SB016] Authenticates with a unique password (or passphrase)

3 SebDB behavior: [SB001] Authenticates with MFA

- Installing the latest software updates[4].
- Backing up data[5].
- Checking messages for signs of phishing[6] and reporting them[7].

We analyzed five years' worth of data, except for a few questions where we only had three or four years' worth of data.

HAVE YOU HEARD OF SEBDB?

SebDB is the world's cybersecurity behavior database. This open-source resource defines everyday security behaviors and maps these behaviors to impacts, threat actor tactics, intervention strategies, and security frameworks like MITRE ATT&CK and NIST CSF. It brings structure, meaning, and actionability to human cyber risk.

Each year, we leverage SebDB to inform the entire survey process, from initial design to framing the final findings. The links to each studied behavior can be found in the footnotes.

Why this five year review matters to you?

Understanding long-term trends in cybersecurity behavior is critical for developing effective interventions. While much research focuses on snapshots in time, this five-year analysis reveals how attitudes and behaviors evolve, which barriers persist, and where the gaps between knowledge, intention, and action continue to widen.

This report compares results across the years from 2021 to 2025 to uncover the motivations and concerns that drive long-term trends in individual cybersecurity. We want this report to give cybersecurity professionals, policymakers, and educators (so people like you!) actionable insights that shape more effective strategies to improve online security for everyone. This moves us all beyond just 'we think people behave like this', into 'we know they do, and we can show how it's changing'. These insights are essential for moving forward.

Finally, in the Appendix, we detail our research methodology, participant demographics, and the full sample base used across the five-year period.

---

4 SebDB behavior: [SB024] Keeps software up-to-date

5 SebDB behavior: [SB061] Backs up data

6 SebDB behaviors: [SB058] Checks a website for signs of deception, [SB081] Checks a message for signs of deception

7 SebDB behavior: [SB087] Reports a suspicious message

Executive summary

💡 AT A GLANCE:

▶️ People care about security and think it's possible, yet they struggle to turn that intent into consistent behavior.

▶️ Structural barriers, time pressure, and cognitive overload keep getting in the way of good decisions.

▶️ The biggest blockers have shifted from glitchy tech to human bandwidth, belief, and everyday environments.

Online presence: Forever online, rarely on the ball

The findings reveal two key, contrasting trends in people's digital lives today: everything's getting more connected, and all of that online activity is increasingly squeezed into a smaller set of accounts and services.

People are spending more time online, with the proportion of participants who are 'always connected' rising sharply by 12% over four years (2022-2025). This massive shift confirms that being online almost all the time is now the default for most people, driven largely by people moving from spending 'a few times per day' online into constant connection.

However, at the same time, people are trying to cut back on how much sensitive data they share. The percentage of users reporting 10 or more sensitive accounts saw a sharp decline in 2025, suggesting a move toward consolidation or greater security awareness among consumers. This positive trend is complicated by the fact that a large portion of the population reports they don't know or have lost count of their total accounts, reminding us that many people still don't see the full extent of their online accounts even as they attempt to reduce it.

👉 INTERESTED IN ONLINE CONNECTIVITY PATTERNS AND ACCOUNT MANAGEMENT TRENDS? JUMP TO CHAPTER 1 NOW.

Attitudes, beliefs & perceptions: Strong motivation, thin patience?

The findings here reveal a core tension: participants possess high motivation and self-belief but are paralyzed by high levels of confusion, overwhelm, and structural barriers.

The foundational attitude toward security has strengthened: the belief that 'staying secure online is worth the effort' increased from 69% in 2023 to 77% in 2025. This high motivation is coupled with high self-efficacy, as participants increasingly feel security is 'possible' (74% in 2025, up from 51% in 2022) and 'under their control' (58% in 2025, up from 52% in 2022).

However, this positive belief is undercut by external and cognitive pressures. The complexity of security information is leading to high rates of confusion (45% in 2025, up from 39% in 2021) and overwhelm (43% in 2025, up from 34% in 2022), causing nearly half the participants to minimize their protective actions.

This psychological fatigue is made worse by structural barriers, the largest being perceived cost (rising from 43% in 2021 to 53% in 2025) and a worrying rise in security fatalism, the belief that efforts are pointless because data is already online (which saw a sharp increase from 22% in 2023 to 34% in 2025).

In summary, it seems that the primary challenge isn't people's intent but the complexity, cost, and psychological fatigue imposed by the security environment, which is pushing many people toward tuning out of security despite their initial motivation.

👉 IS GETTING DATA ON MOTIVATION, CONFIDENCE, AND PERCEIVED RISK AT THE TOP OF YOUR WISH LIST? JUMP TO CHAPTER 2 NOW.

Responsibility: Whose job is it, anyway?

Participants overwhelmingly see themselves as the main person responsible for protecting their personal information each year (ranging from 56% in 2024 to 66% in 2023). This is reinforced by a strong and growing expectation that apps and platforms should also play their part (rising from 37% in 2022 to 42% in 2025). Conversely, people see government and internet providers as less responsible than before (from 31% in 2021 to 24% in 2025, and from 43% in 2021 to 29% in 2025, respectively).

This view contrasts sharply with attitudes toward organizational data. Responsibility for protecting workplace information has shifted away from external bodies (the government, from 38% in 2021 to 28% in 2025) and onto internal teams, particularly the IT (from 38% in 2021 to 45% in 2025) and security (from 29% in 2021 to 40% in 2025) departments. While the perception of personal responsibility in the workplace peaked in 2023, it has since declined.

👉 DIVE INTO THE DETAILS OF RESPONSIBILITY RATES IN CHAPTER 3.

Cybercrime victimization & reporting: More hits, more noise?

The overall trend shows a significant increase in fatalistic attitudes toward both financial and data loss, particularly between 2024 and 2025.

Overall victimization rates rose from 34% in 2021-2022 to 44% in 2025 (a 10% increase in five years) with the steepest rise occurring between 2024 and 2025. This increase mirrors the growing worry about cybercrime, which climbed from 57% in 2022 to 68% in 2025.

On a positive note, cyberbullying reporting has seen an improvement. While victimization increased from 13% in 2022 to 23% in 2025, reporting rates surged from 52% in 2022 to 88% in both 2024 and 2025, meaning nearly nine out of ten cyberbullying victims now report incidents, representing a 36% increase in just four years.

👉 ARE YOU MOST INTERESTED IN VICTIMIZATION RATES OF SPECIFIC TYPES OF CYBERCRIME? JUMP TO CHAPTER 4.

Cybersecurity training: Safety net or comfort blanket?

Overall, the findings reveal a pronounced, persistent gap in people's cybersecurity education. Despite modest improvements over the five-year period, the majority of participants consistently report having no access to formal training resources (from 63% in 2021 to 55% in 2025).

There has also been a shift away from the annual training model: the percentage of those receiving training more than once a year is increasing (from 31% in 2022 to 35% in 2025), and there's a noteworthy rise in reactive, incident-based training (from 10% in 2022 to 17% in 2025).

Over the past four years, time constraints (from 29% in 2022 to 21% in 2025), perceived knowledge (from 25% in 2022 to 16% in 2025), and doubt about training's efficacy (from 17% in 2022 to 20% in 2025) are the three largest barriers preventing participants from engaging with the available training.

The data on how much people feel training actually helps reveals that while participants report positive impacts across various behaviors, the impact is narrow, and getting smaller. While attendees reported noticeable positive changes in key security behaviors (e.g., recognizing and reporting phishing, MFA use, and strong password adoption), the impact has generally decreased over the four years on most measured behaviors. Furthermore, these positive impacts were consistently reported by less than half the participants from 2023 onwards.

👉 ARE YOU PRIORITIZING MOVING BEYOND COMPLETION RATES AND DELIVERING ACTUAL IMPACT? JUMP TO CHAPTER 5.

Cybersecurity behaviors: Pwned with good intentions

The data reveals a persistent and widespread intention–behavior gap across all measured security behaviors. While participants demonstrate high confidence and motivation, there's a clear inconsistency in maintaining protective behaviors, with the biggest problems in day-to-day habits that need regular effort.

Password hygiene shows mixed progress: there has been a shift toward longer passwords (from 16% in 2022 to 25% in 2025), but this is undermined by a concerning rebound in shorter passwords (rising to 31% in 2025) and an increased use of risky creation techniques, particularly incorporating personal information, which rose from 25% (in 2022) to 37% (in 2025).

The five-year trend for MFA reveals a clear gap between knowledge and consistent action. While awareness grew from 52% in 2021 to 77% in 2025, regular usage decreased from a peak of 94% in 2022 to just 53% in 2025. Moreover, those reporting they don't know how to use MFA more than doubled to 21% in 2025, showing that awareness doesn't translate into sustained action or functional capability.

Updating devices and software has decreased notably, with those who 'always' install updates dropping from 44% in 2021 to 31% in 2025, a 13% decline. Similarly, automatic backup adoption declined from 29% in 2021 to 22% in 2025, with the majority (30-32%) backing up only 'sometimes'.

Finally, phishing defense reveals a troubling contradiction: confidence in identifying phishing messages remained stable and high (66-70%), yet the percentage who 'always' check messages for phishing dropped dramatically from 51% in 2021 to 36% in 2025, a 15% decrease. This demonstrates that confidence doesn't guarantee consistent security action.

👉 IS LEARNING MORE ABOUT SECURITY BEHAVIORS AT THE TOP OF YOUR TO-DO LIST? JUMP TO CHAPTER 6.

Main findings

1. Online presence: Forever online, rarely on the ball
2. Attitudes, beliefs, & perceptions about online security: Strong motivation, thin patience?
3. Responsibility: Whose job is it, anyway?
4. Cybercrime victimization & reporting: More hits, more noise?
5. Cybersecurity training: Safety net or comfort blanket?
6. Cybersecurity behaviors: Pwned with good intentions

Main findings

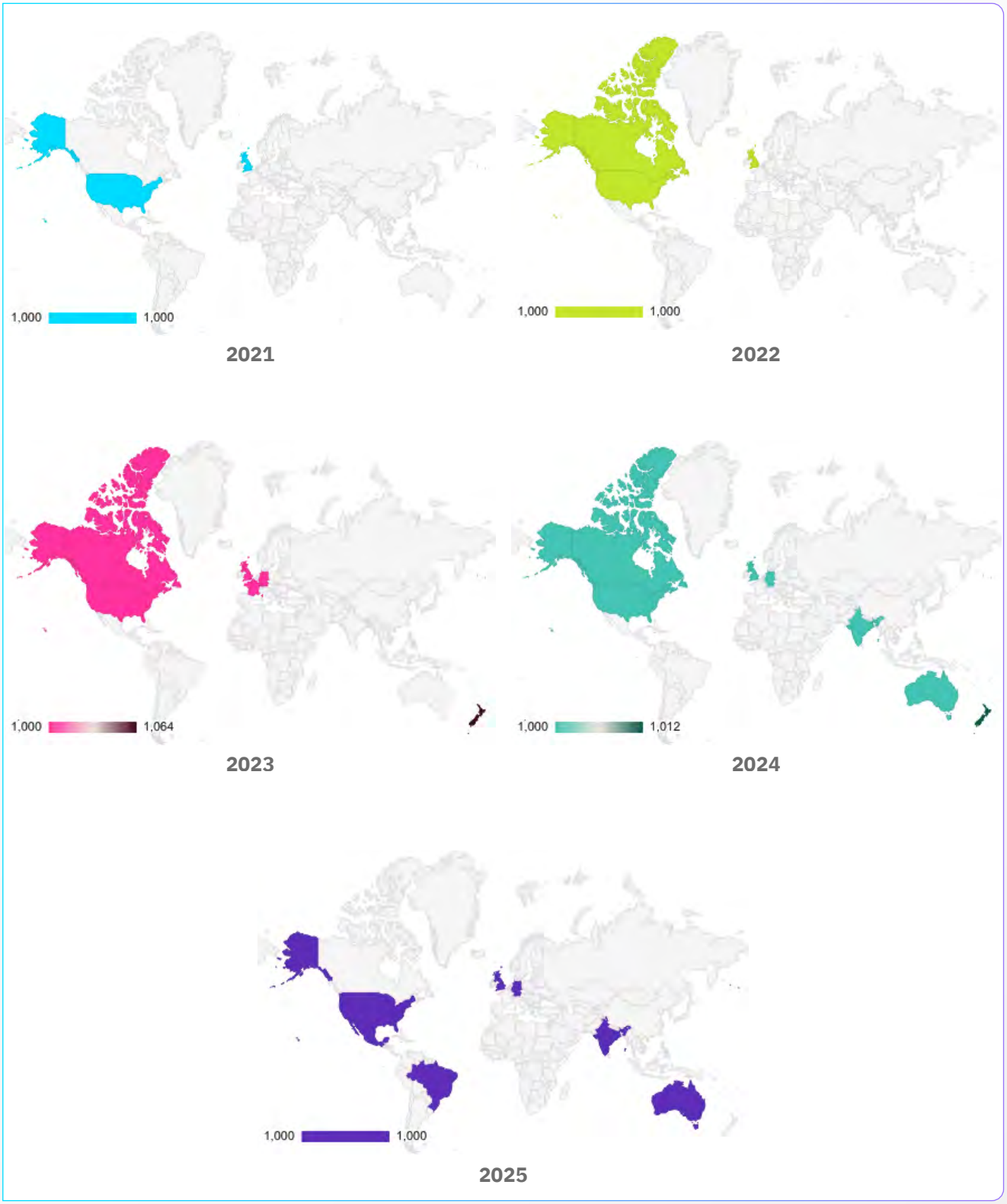
Before we get into each theme, it helps to know who we heard from and how broad the picture is.

We gathered all data for survey questions in the published Oh, Behave! Reports between 2021 and 2025, where at least three years' worth of data were collected. This approach allows us to identify trends and persistent challenges in cybersecurity attitudes and behaviors across the participant base.

Across the five years, more than 25,000 adults aged 18+ took part in the surveys, drawn from multiple countries and with samples balanced by age and gender each year. Table 1 shows how many people took part in each country and year, and the maps below give a quick visual of the coverage. (If you want the full demographic breakdown, you'll find it in the Appendix.)

Table 1. Number of participants from various countries each year

	2021 (N=2000)	2022 (N=3000)	2023 (N=6064)	2024 (N=7012)	2025 (N=7000)
United States	1000	1000	1000	1000	1000
United Kingdom	1000	1000	1000	1000	1000
Canada		1000	1000	1000	
France			1000		
Germany			1000	1000	1000
New Zealand			1064	1012	
Australia				1000	1000
India				1000	1000
Brazil					1000
Mexico					1000


1,000
1,000
2021
1,000
1,000
2022
1,000
1,064
2023
1,000
1,012
2024
1,000
1,000
2025

1. Online presence:
Forever online, rarely on the ball

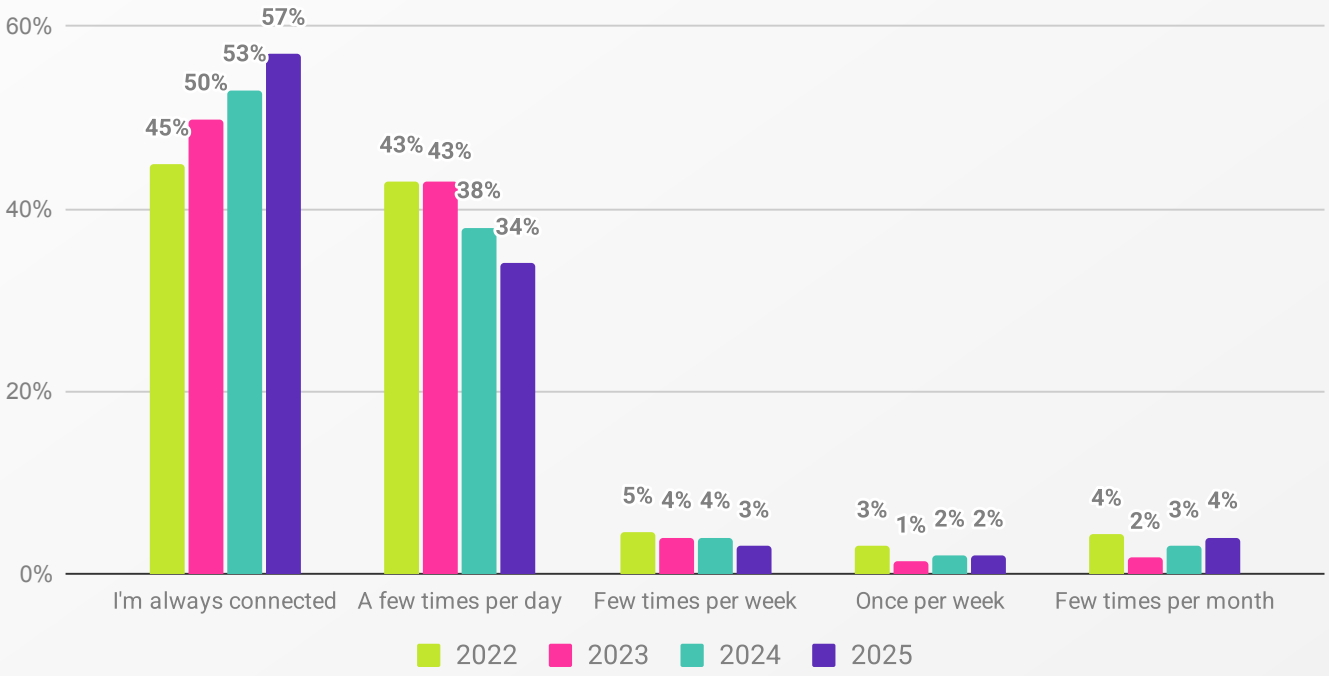
In an increasingly hyper-connected world, this chapter examines participants' online connectivity and the number of online accounts they have.

Across the four years from 2022 to 2025, the findings show a notable and accelerating trend toward constant online engagement (Figure 1).

The percentage of participants reporting they're 'always connected' has risen sharply and consistently, increasing by a total of 12% over four years.

The proportion of individuals using the internet 'a few times per day' decreased, dropping from 43% in 2022 to 34% in 2025.

Figure 1. ***'How frequently do you use the Internet?'***



Base: US [2022-2025]; UK [2022-2025]; Canada [2022-2024]; France [2023]; Germany [2023-2025]; Australia [2024-2025]; New Zealand [2023-2024]: India [2024-2025]; Brazil [2025]; and Mexico [2025]. Total number of participants (age 18+): 23,076 [Cumulative]; 3000 [2022], 6064 [2023], 7012 [2024], 7000 [2025].

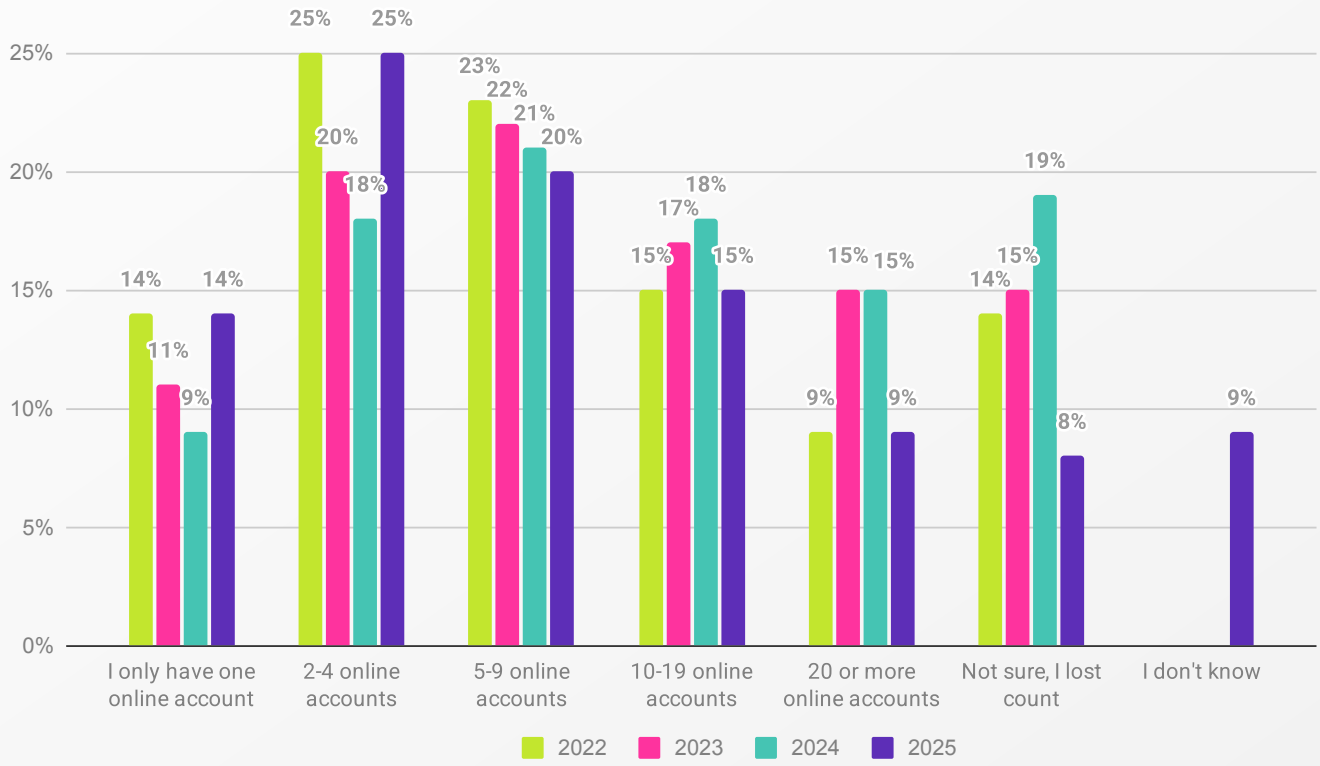
While the number of online accounts people hold was on the rise between 2021 to 2024, it has declined since (Figure 2).

The percentage of those who have 20 or more online accounts has declined by 6% from 15% in both 2023 and 2024 to just 9% in 2025. The combined proportion of participants with 10 or more accounts dropped from 33% in 2024 to 24% in 2025.

Interestingly, in 2021 and 2025, the highest proportion of participants reported having 2-4 online accounts (25% both), while in 2023 and 2024, the highest percentage had 5-9 accounts (22% and 21%, respectively).

The combined percentage of those who don't know how many accounts they have and those who have lost count highlights a sizable group who don't have a clear view of their own accounts.

Figure 2. ***'Overall, how many online accounts do you own that hold personal information?'***



Base: US [2022-2025]; UK [2022-2025]; Canada [2022-2024]; France [2023]; Germany [2023-2025]; Australia [2024-2025]; New Zealand [2023-2024]: India [2024-2025]; Brazil [2025]; and Mexico [2025]. Total number of participants (age 18+): 23,076 [Cumulative]; 3000 [2022], 6064 [2023], 7012 [2024], 7000 [2025]. Note: The 'I don't know' option was only provided to participants in 2025, hence the lack of data in previous years.

KEY TAKEAWAYS

Connectivity up, accounts down
Two contrasting trends emerged. ‘Always’ connected users rose by 12% (2022-2025), yet users with 10+ sensitive accounts dropped from 33% (2024) to 24% (2025).

More deliberate exposure or SSO
People appear to be intentionally consolidating or cutting back on sensitive accounts. SSO adoption may be driving account consolidation as platforms allow single-credential authentication.

👉 IN **CHAPTER 2**, WE’LL MOVE FROM THE SURFACE TO THE HEADSPACE. WE’LL TAKE A LOOK AT HOW PEOPLE FEEL ABOUT STAYING SECURE IN THIS ENVIRONMENT: HOW MUCH THEY CARE, HOW CONFIDENT THEY ARE, AND WHERE FRUSTRATION AND FATIGUE HIT THE FAN. IF CHAPTER 1 SETS THE SCENE, CHAPTER 2’S SET TO TELL US ABOUT THE MINDSET OF THE PEOPLE STANDING IN IT.

2. Attitudes, beliefs, & perceptions about online security: Strong motivation, thin patience?

According to the COM-B[8] model of behavior, three factors are essential for behavior to occur: Capability, Opportunity, and Motivation. Motivation, encompassing attitudes, beliefs, and perceptions about security, plays a crucial role in security behavior. However, positive attitudes alone are insufficient to drive action when individuals lack the capability to perform security behaviors or when their environment fails to provide opportunity.

This chapter looks at these motivational factors through participants' attitudes, beliefs, and perceptions about online security, including the value and priority they place on security, their confidence in their ability to stay secure (self-efficacy), and their perceptions of barriers like cost.

The findings show that while the majority of participants recognize the importance of security, they also feel the burden of achieving it (Figure 3).

Over the past five years, there has been an increase in the percentage of participants who view staying secure online as a priority. While this peaked in 2023, with 84%, and slightly decreased to 82% in 2025, it still represents a 6% increase in five years. This suggests that security consciousness is firmly embedded in the mindset of the majority of participants.

While security is a high priority, it's also tied to negative feelings, including frustration and intimidation, showing that people find the process of staying secure challenging.

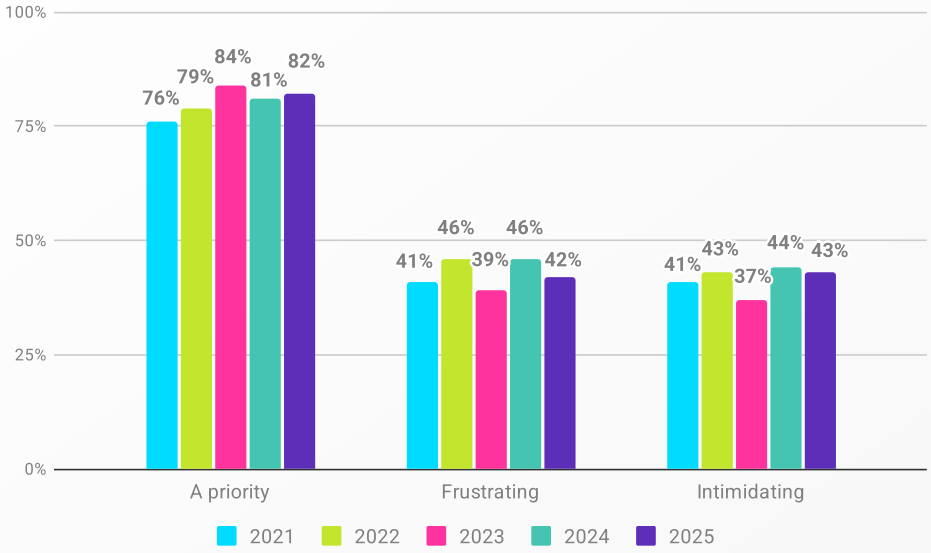
People finding staying secure online frustrating has remained relatively high, fluctuating between a low of 39% in 2023 and a high of 46% in 2022 and 2024. However, we saw a decrease (-4%) in people finding staying secure online frustrating in 2025 (42%).

Similarly, people finding staying secure online intimidating remained steady over the five-year period, despite the slight fluctuation over the years, reaching 43% in 2025.

This indicates that despite the high priority placed on security, the actual execution of security measures remains a significant hurdle for nearly half of the participants each year.

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

Figure 3. *'I feel that staying secure online is a priority, frustrating, and intimidating.'*



Base: US [2021-2025]; UK [2021-2025]; Canada [2022-2024]; France [2023]; Germany [2023-2025]; Australia [2024-2025]; New Zealand [2023-2024]: India [2024-2025]; Brazil [2025]; and Mexico [2025]. Total number of participants (age 18+): 25,076 [Cumulative]; 2000 [2021], 3000 [2022], 6064 [2023], 7012 [2024], 7000 [2025].

The data measuring participants' beliefs about their personal ability to stay secure online reveals a clear upward trajectory in confidence and a growing sense of personal agency over online safety, particularly in 2025 (Figure 4).

The belief that staying secure online is achievable has been consistently high and stable, from 66% in 2022 to 69% in 2025[9], affirming that most participants don't view security as an impossible goal.

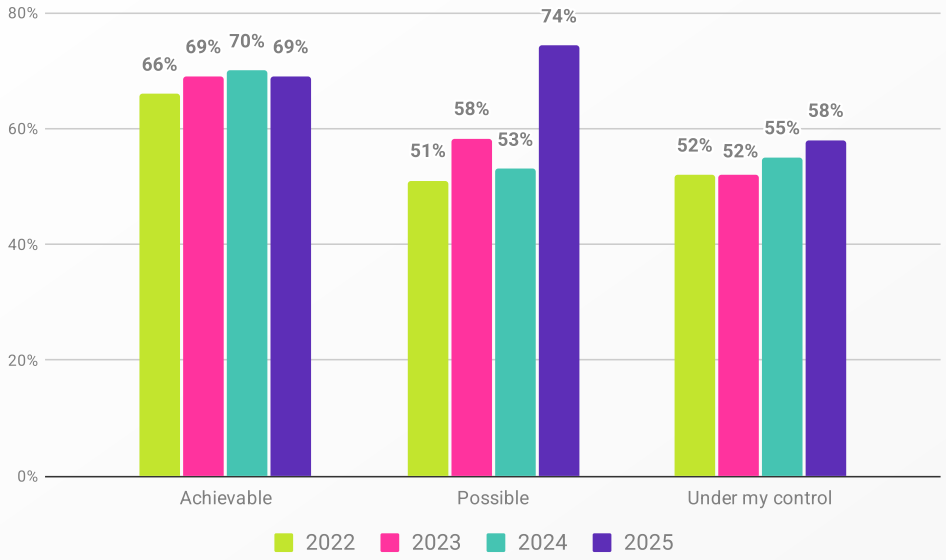
The percentage of those feeling that staying secure online is possible has increased dramatically from 51% in 2022 to 74% in 2025. This 21% surge suggests a fundamental shift in optimism, with nearly three-quarters of participants believing effective online security is within their reach.

And those feeling that security is under their control have also increased over the years, from 52% in 2022 to 58% in 2025.

In summary, the yearly comparisons show a positive transformation in people's mindset: security is viewed as something that is attainable and can be managed by the individual.

9 In 2025, participants were provided with the option 'Possible', a change from previous years when it was worded negatively ('Not possible'). While we believe the resulting percentage change is too notable to be explained by this wording difference alone, it's possible that the revised phrasing contributed to participants' responses.

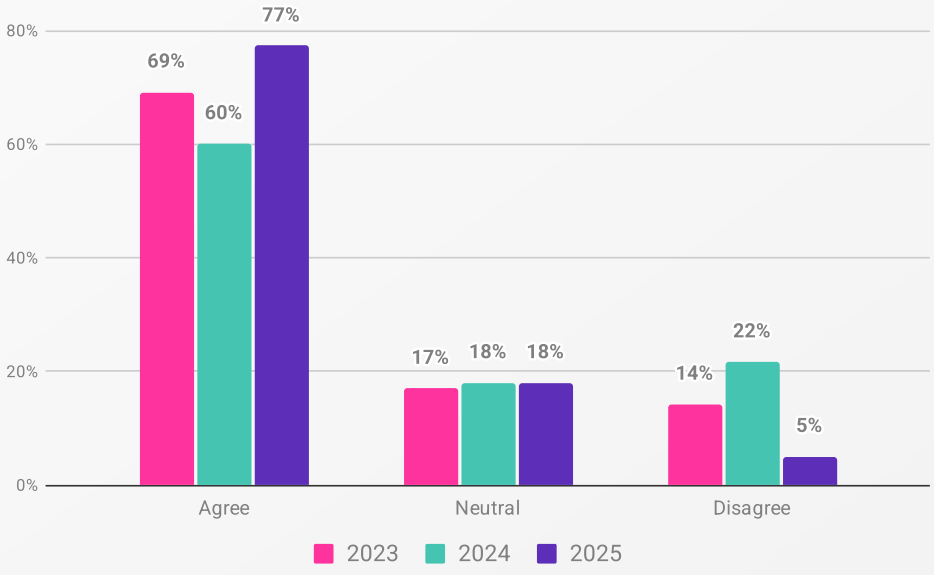
Figure 4. *'I feel that staying secure online is achievable, possible, and under my control.'*



Base: US [2022-2025]; UK [2022-2025]; Canada [2022-2024]; France [2023]; Germany [2023-2025]; Australia [2024-2025]; New Zealand [2023-2024]: India [2024-2025]; Brazil [2025]; and Mexico [2025]. Total number of participants (age 18+): 23,076 [Cumulative]; 3000 [2022], 6064 [2023], 7012 [2024], 7000 [2025].

The data reveal an increase in people seeing their security efforts as worthwhile over the three-year period (Figure 5). In 2023, 69% felt that staying secure online was worth the effort, which then dropped to 60% in 2024. However, this has increased notably in 2025, with 77% finding their security efforts valuable[10].

Figure 5. *'I feel that staying secure online is worth the effort.'*



Base: US [2023-2025]; UK [2023-2025]; Canada [2023-2024]; France [2023]; Germany [2023-2025]; Australia [2024-2025]; New Zealand [2023-2024]: India [2024-2025]; Brazil [2025]; and Mexico [2025]. Total number of participants (age 18+): 20,076 [Cumulative]; 6064 [2023], 7012 [2024], 7000 [2025].

10 In 2025, participants were provided with the option 'Worth the effort', a change from previous years when it was worded negatively ('Not worth the effort'). While we believe the resulting percentage change is too notable to be explained by this wording difference alone, it's possible that the revised phrasing contributed to participants' responses.

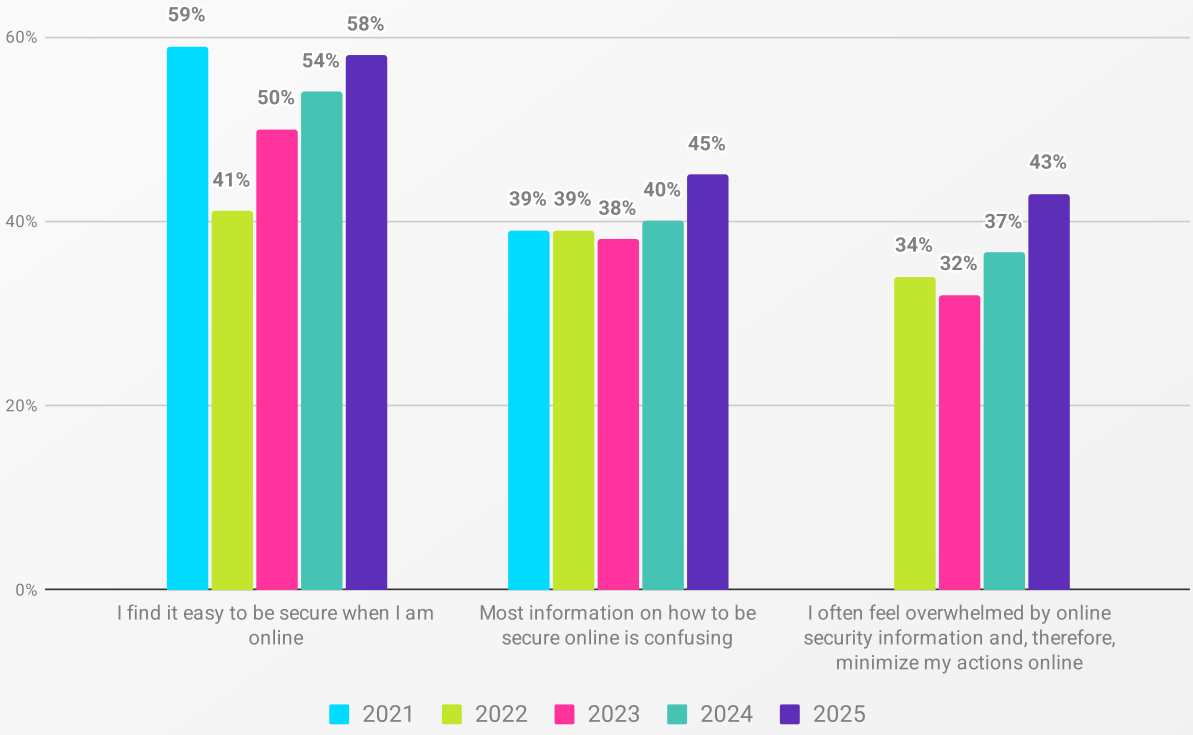
The findings show rising confusion and overwhelm, even though views on ease are more mixed (Figure 6). The percentage of those who find it easy to stay secure online has dropped notably, by 18% from 2021 (59%) to 2022 (41%). Since then, the percentage has consistently increased every year, reaching 58% in 2025.

People now find security information and guidance less clear than they did five years ago. In 2021, 39% reported they found security information on how to be secure online confusing, which has increased by 6% since then. Nearly half of the participants (45%) in 2025 find guidance unclear, indicating a growing frustration.

The percentage of those minimizing their online actions because of online security information overwhelm has consistently increased over the past three years, from 34% in 2022 to 43% in 2025. This 9% increase means that nearly half of the participants (43%) are now experiencing security information overload, leading to a paralyzing effect where they choose to do less to protect themselves.

In summary, the findings show a negative shift in the psychological experience of security. The marked increase in both confusion and overwhelm over the years indicates that the complexity of the security environment is leading directly to security apathy and inaction among nearly half of the participants.

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



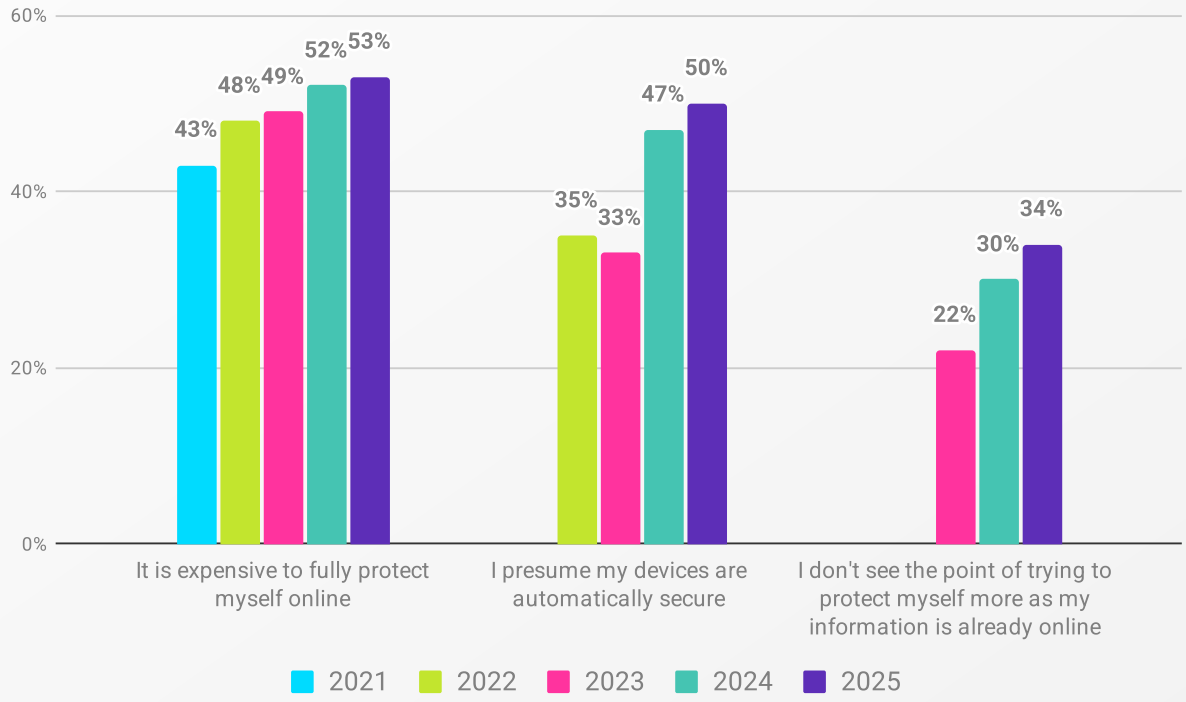
Base: US [2021-2025]; UK [2021-2025]; Canada [2022-2024]; France [2023]; Germany [2023-2025]; Australia [2024-2025]; New Zealand [2023-2024]: India [2024-2025]; Brazil [2025]; and Mexico [2025]. Total number of participants (age 18+): 25,076 [Cumulative]; 2000 [2021], 3000 [2022], 6064 [2023], 7012 [2024], 7000 [2025].

Over the past five years, participants have consistently believed that it's expensive to fully protect themselves online, increasing from 43% in 2021 to 53% in 2025 (Figure 7). This shows that over half of the participants see the cost of tools, software, or services as a major barrier to personal online security.

The percentage of those who presume their devices are automatically secure has increased sharply over the four-year period, rising from 35% in 2022 to 50% in 2025. The 15% increase in this belief suggests that half of the participants assume their devices are automatically secure and don't need their input.

Finally, in the past three years, the percentage of those who feel there's no point in trying to protect themselves, as their information is already online, has seen a sharp and accelerating increase, from 22% in 2023 to 34% in 2025.

Figure 7. Perceived barriers to personal online security.



Base: US [2021-2025]; UK [2021-2025]; Canada [2022-2024]; France [2023]; Germany [2023-2025]; Australia [2024-2025]; New Zealand [2023-2024]: India [2024-2025]; Brazil [2025]; and Mexico [2025]. Total number of participants (age 18+): 25,076 [Cumulative]; 2000 [2021], 3000 [2022], 6064 [2023], 7012 [2024], 7000 [2025].

KEY TAKEAWAYS

Positive attitudes strengthening
Belief that 'staying secure online is worth the effort' increased from 69% (2023) to 77% (2025). People increasingly feel security is 'possible' (51% in 2022 to 74% in 2025) and 'under their control' (52% in 2022 to 58% in 2025).

Confusion and overwhelm undermining action
Confusion over how to interpret or follow security information rose from 39% (2021) to 45% (2025), while those feeling so overwhelmed they minimize protective actions increased from 34% (2022) to 43% (2025).

Structural barriers persist
Perceived cost remains the largest barrier, rising from 43% (2021) to 53% (2025). Security fatalism is also accelerating: those who feel efforts are pointless because data is already online jumped from 22% (2023) to 34% (2025).

The core tension
The primary challenge isn't people's intent but the complexity, cost, and psychological fatigue driving apathy despite positive attitudes.

👉 IN **CHAPTER 3** WE SWITCH FROM ATTITUDES TO ACCOUNTABILITY. WHO DO PEOPLE THINK SHOULD BE CARRYING THE LOAD FOR STAYING SECURE: THEMSELVES, THEIR EMPLOYERS, OR THEIR PROVIDERS? AND WE'LL BE EXAMINING HOW THAT DIFFERS FOR WORK VERSUS PERSONAL INFORMATION. BECAUSE AS WELL AS KNOWING HOW PEOPLE FEEL, WE NEED TO KNOW WHO PEOPLE EXPECT TO STEP UP.

3. Responsibility:
Whose job is it, anyway?

In this chapter, we'll look at how people divide responsibility for protecting information between themselves, their employer, technology providers, and external bodies like the government.

We track how that split changes between personal and work contexts, and how it's shifted over time. The patterns that emerge help explain why some security tasks get done, some get dropped, and some never feel like 'my job' in the first place.

🔷 3.1 Protecting workplace information:
Shirking 9 to 5?

This chapter looks at who people think is responsible for the protection of online information and compares personal and professional security. It details who is deemed most and least responsible for protecting workplace information versus private data. Feelings of responsibility shape how people put time, effort, and resources into security, and confusion over ownership (or the lack of it) often results in key protective behaviors getting skipped.[11]

Each year, we asked participants to identify the party they felt most, somewhat, and least responsible for protecting their workplace's information. Figure 8 shows the degree to which participants felt each party was most responsible.

In 2021, people saw the government (38%) and their workplace's IT department as the most responsible parties for protecting their workplace's information, followed by the security department (29%).

A striking shift occurred in 2022, when the government was no longer seen as the most responsible party (dropping sharply to 26%, -12% from 2021). Instead, the largest responsibility was attributed to the workplace's IT department (36%), followed by the security department (28%).

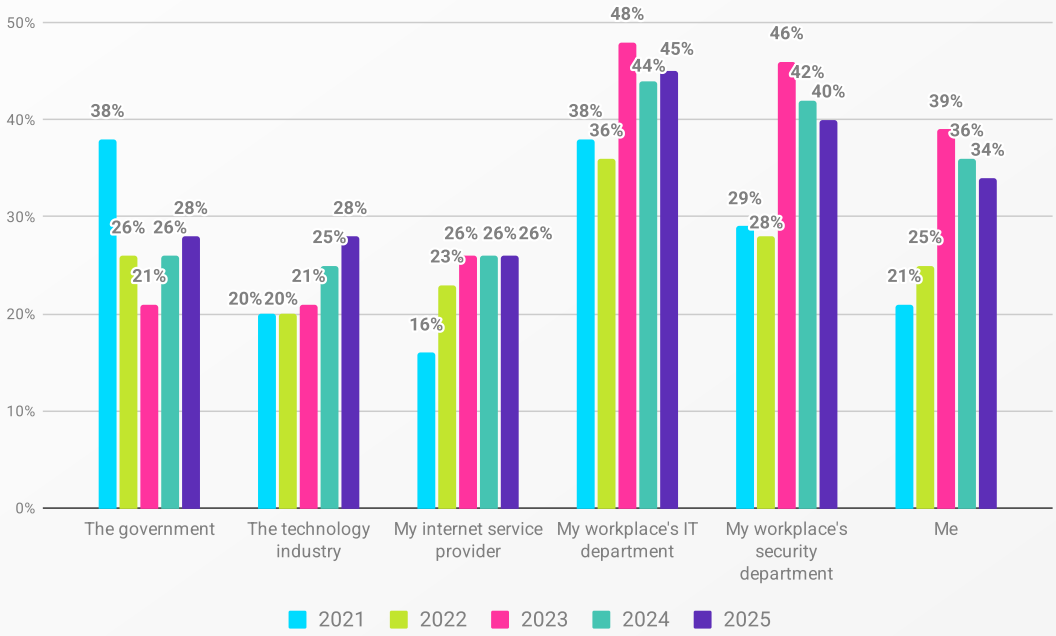
11 Ali, R. F., Dominic, P. D. D., Ali, S. E. A., Rehman, M., & Sohail, A. (2021). Information security behavior and information security policy compliance: A systematic literature review for identifying the transformation process from noncompliance to compliance. *Applied Sciences, 11*(8), 3383.

From 2023 to 2025, the trend of consistently attributing most responsibility to the organization continued:

- IT department (48% in 2023, 44% in 2024, 45% in 2025),
- security department (46% in 2023, 42% in 2024, 40% in 2025).

The group who saw themselves as the most responsible show an interesting pattern. 21% reported themselves to be most responsible in 2021, which has increased to 25% in 2022 and peaked in 2023 (39%). However, perceptions of personal responsibility have decreased in the following years, to 36% in 2024 and 34% in 2025.

Figure 8. *'In your view, who is most responsible for protecting your workplace's information?'*



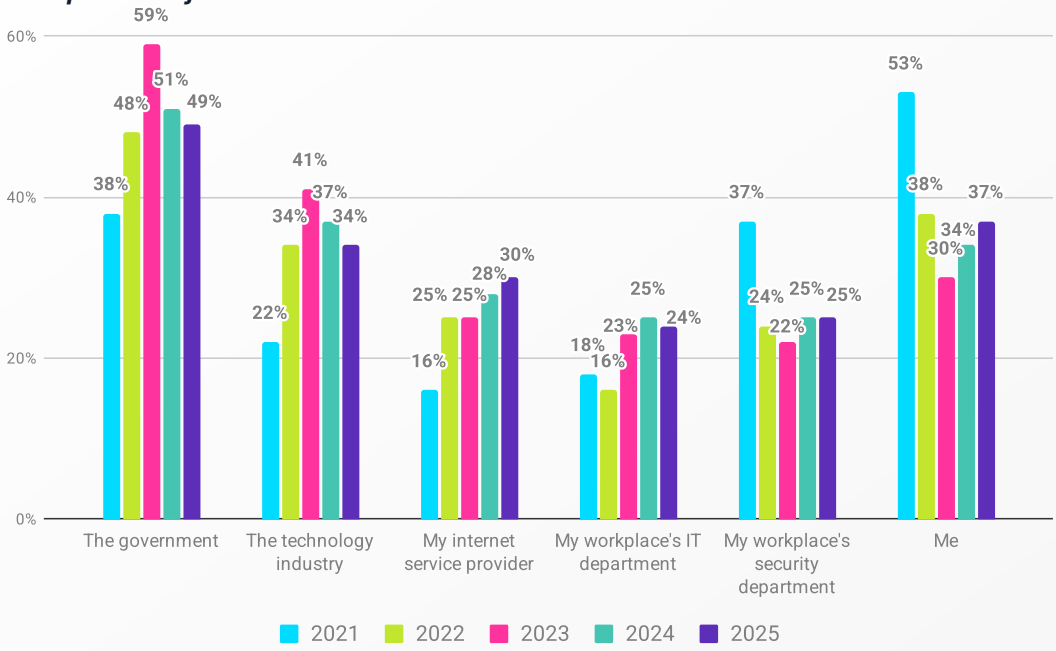
Base: US [2021-2025]; UK [2021-2025]; Canada [2022-2024]; France [2023]; Germany [2023-2025]; Australia [2024-2025]; New Zealand [2023-2024]: India [2024-2025]; Brazil [2025]; and Mexico [2025]. Total number of participants (age 18+) who are employed: 16,164 [Cumulative]; 1105 [2021], 1762 [2022], 4021 [2023], 4721 [2024], 4555 [2025].

The trend around personal responsibility is even more apparent when looking at who people see as least responsible for protecting workplace information (Figure 9).

In 2021, over half of the participants saw themselves as the least responsible party (53%). In subsequent years, this perception shifted, and the government was consistently attributed the least responsibility:

- 48% in 2022
- 59% in 2023
- 51% in 2024
- 49% in 2025.

Figure 9. *'In your view, who is least responsible for protecting your workplace's information?'*



Base: US [2021-2025]; UK [2021-2025]; Canada [2022-2024]; France [2023]; Germany [2023-2025]; Australia [2024-2025]; New Zealand [2023-2024]: India [2024-2025]; Brazil [2025]; and Mexico [2025]. Total number of participants (age 18+) who are employed: 16,164 [Cumulative]; 1105 [2021], 1762 [2022], 4021 [2023], 4721 [2024], 4555 [2025].

The data on security responsibility reveals a big shift in perception: responsibility for protecting workplace information has moved inward from external actors like the government and toward the organization's IT and security departments (consistently attributed the most responsibility). While the perception of personal responsibility peaked in 2023, it has since declined. This indicates that cybersecurity is now treated more as an organizational and technical duty than a strictly personal one.

🔷 3.2 Protecting personal information: Streaming, scrolling … safeguarding?

What about the responsibility for protecting personal information?

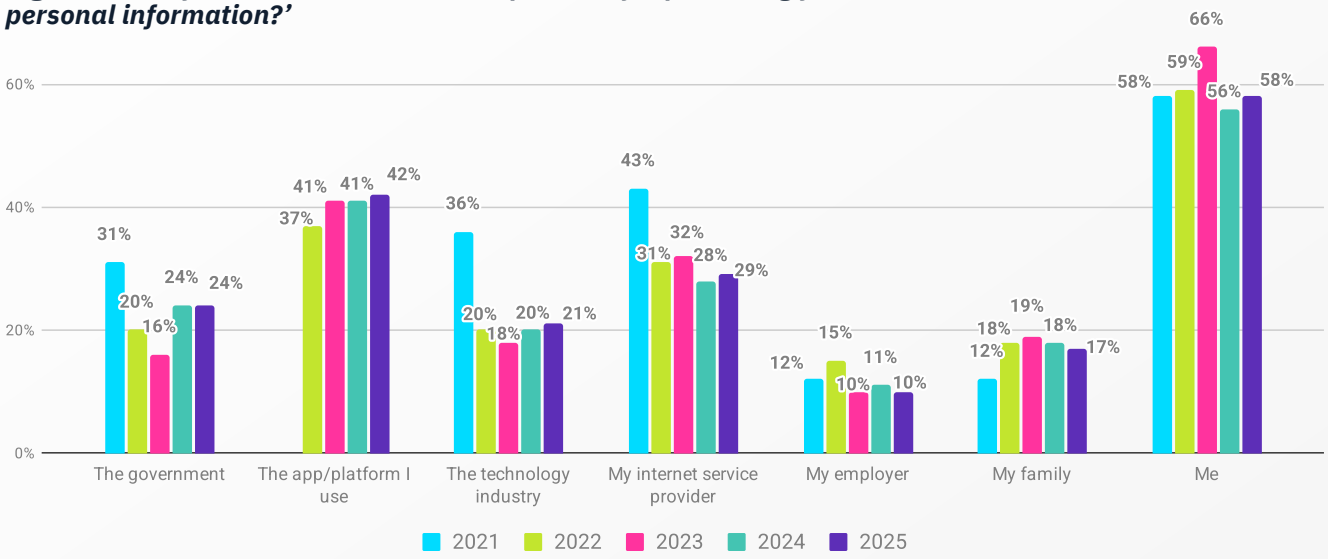
Participants consistently viewed themselves as the most responsible party for protecting their own information over the past five years (Figure 10). In 2021, 58% attributed responsibility to themselves, which increased to 66% in 2023 and dropped back to 58% in 2025.

This contrasts sharply with the findings on responsibility for workplace information, where participants overwhelmingly shifted responsibility to the IT and security departments. This difference shows a clear split in how people see things: responsibility for security shifts from personal for private data to organizational for company data.

The second highest responsibility was attributed to the application or platform, showing a clear upward trend from 37% in 2022 to 42% in 2025. This indicates that a growing portion of people expect security as a standard from the services they use.

Furthermore, responsibility attributed to the government and the internet service provider has dropped over the past five years, from 31% (2021) to 24% (2025), and from 43% (2021) to 29% (2025), respectively.

Figure 10. ***'In your view, who is most responsible for protecting your personal information?'***

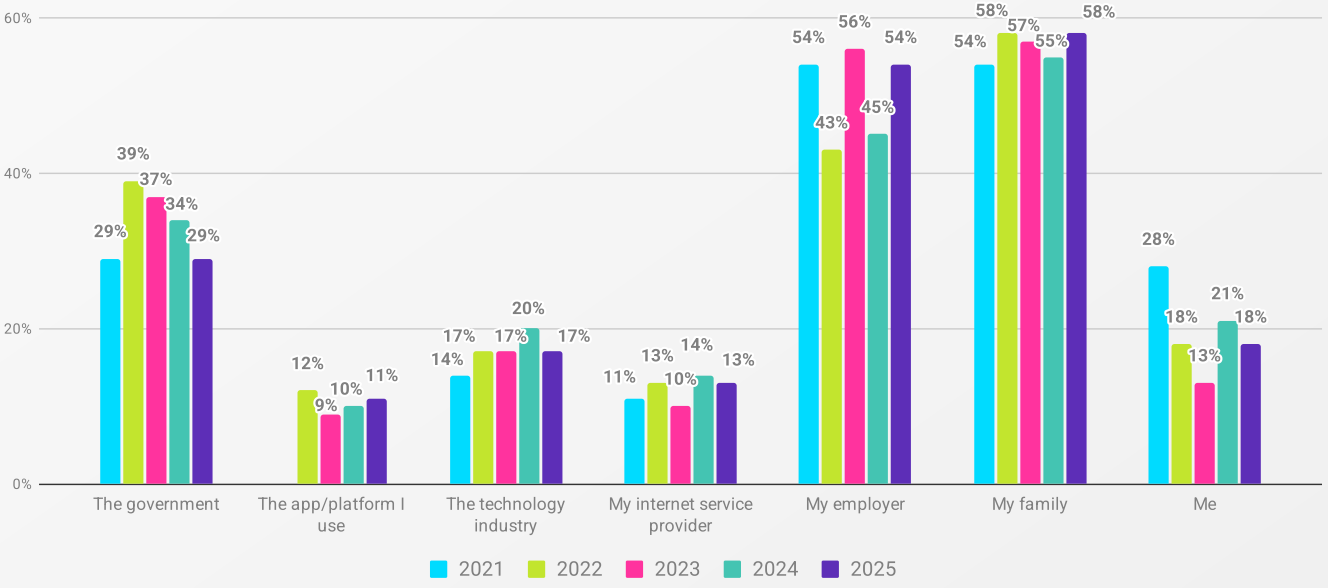


Base: US [2021-2025]; UK [2021-2025]; Canada [2022-2024]; France [2023]; Germany [2023-2025]; Australia [2024-2025]; New Zealand [2023-2024]: India [2024-2025]; Brazil [2025]; and Mexico [2025]. Total number of participants (age 18+): 25,076 [Cumulative]; 2000 [2021], 3000 [2022], 6064 [2023], 7012 [2024], 7000 [2025]. Note: In 2021, participants were not provided with the option 'The app/platform I use', hence the missing data.

The data show that participants consistently attributed the least amount of responsibility to their own family and their employer across all five years (Figure 11).

To break it down, family was viewed as the least responsible party in every year, ranging between 54% (2021) and 58% (2022 and 2025), except in 2021 when the responsibility of the employer and family were viewed equally low (54% in both years).

Figure 11. ***'In your view, who is least responsible for protecting your personal information?'***



Base: US [2021-2025]; UK [2021-2025]; Canada [2022-2024]; France [2023]; Germany [2023-2025]; Australia [2024-2025]; New Zealand [2023-2024]: India [2024-2025]; Brazil [2025]; and Mexico [2025]. Total number of participants (age 18+): 25,076 [Cumulative]; 2000 [2021], 3000 [2022], 6064 [2023], 7012 [2024], 7000 [2025].

KEY TAKEAWAYS

Personal vs workplace: a clear split
Responsibility for personal security is seen mainly as the individual's job (56%-66% across all years), with a growing expectation that apps and platforms should also help (up from 37% in 2022 to 42% in 2025).

This contrasts sharply with workplace data, where responsibility has shifted to the organization (IT: from 38% to 45%; security department: from 29% to 40%, both 2021-2025), not the individual.

👉 IN **CHAPTER 4**, WE MOVE FROM WHO SHOULD BE RESPONSIBLE TO WHAT HAPPENS WHEN THINGS GO WRONG. WE'LL LOOK AT CYBERCRIME VICTIMIZATION AND REPORTING: HOW OFTEN ARE PEOPLE HIT, HOW DO THEY FEEL ABOUT IT, AND WHEN DO THEY ACTUALLY TELL PEOPLE?

4. Cybercrime victimization & reporting: More hits, more noise?

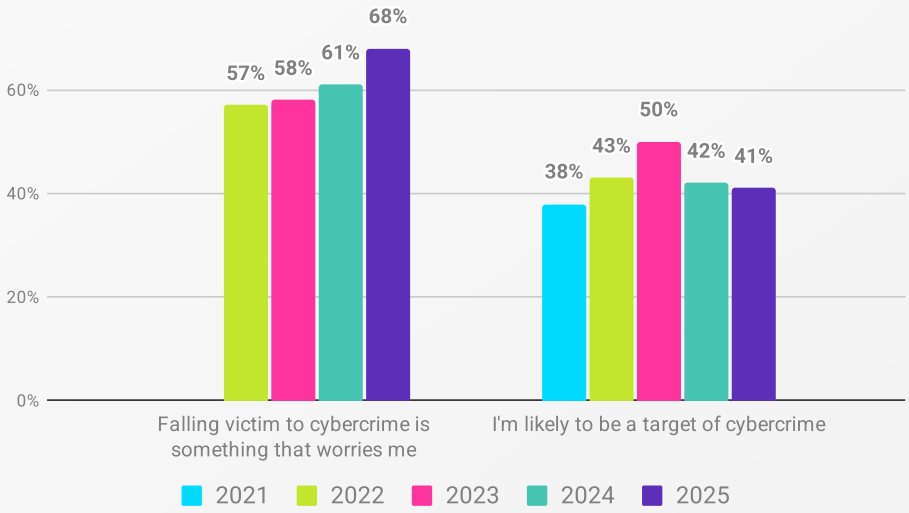
This chapter investigates the stark reality of the threat landscape, exploring trends in attitudes toward victimization (including worry and fatalism), the accelerating rate of actual victimization (loss of money or data), and the specific types of incidents encountered. We also analyze cyberbullying, detailing its rising prevalence and who's reporting it (and who isn't).

🔷 4.1 Attitudes toward victimization: From 'couldn't be me' to 'oh no'

Worry about falling victim is high and growing (Figure 12). In 2022, 57% reported being worried about cybercrime victimization, and the percentage climbed every year, reaching 58% in 2023, 61% in 2024, and peaking at 68% in 2025. This represents a notable 11% increase in four years.

Thirty-eight percent of participants thought of themselves as likely targets of cybercrime in 2021, and this has increased to 50% in 2023. Although the percentage since then dropped to 42% in 2024 and 41% in 2025, that's still a substantial portion of participants who view themselves as likely targets.

Figure 12. Attitudes toward victimization



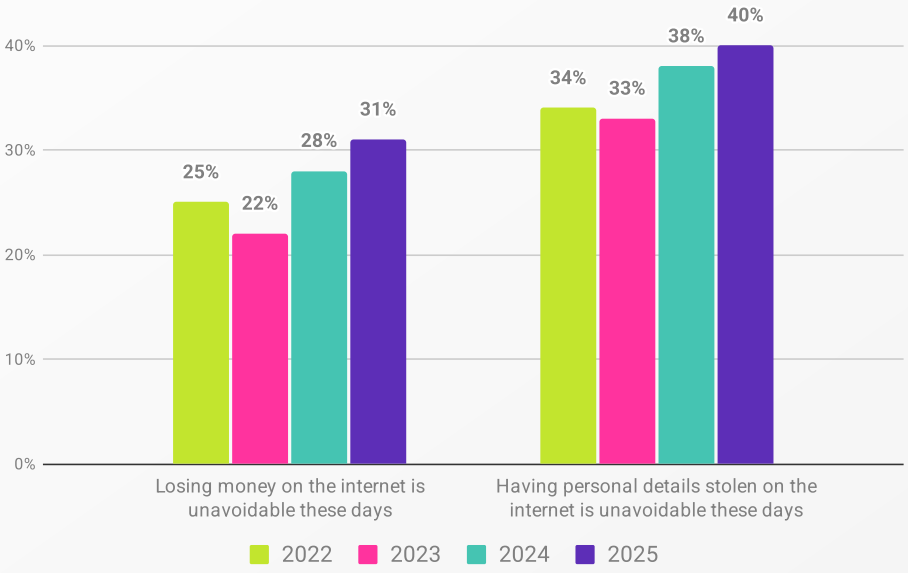
Base: US [2021-2025]; UK [2021-2025]; Canada [2022-2024]; France [2023]; Germany [2023-2025]; Australia [2024-2025]; New Zealand [2023-2024]: India [2024-2025]; Brazil [2025]; and Mexico [2025]. Total number of participants (age 18+): 25,076 [Cumulative]; 2000 [2021], 3000 [2022], 6064 [2023], 7012 [2024], 7000 [2025].

Perceptions on the avoidability of losing money and personal details on the internet have both increased notably over the past four years (Figure 13).

In 2022, 25% felt that losing money on the internet is unavoidable, and after a 3% drop in 2023 (22%), the percentage increased to 28% in 2024 and 31% in 2025, representing a 6% overall increase. This increase shows that nearly one-third of participants now view financial loss as an unavoidable risk of being online.

The percentage of those believing that having personal details stolen is unavoidable has also increased over the past four years, from 34% in 2022 to 40% in 2025.

Figure 13. Perceptions on the avoidability of losing money or personal details on the internet.



Base: US [2022-2025]; UK [2022-2025]; Canada [2022-2024]; France [2023]; Germany [2023-2025]; Australia [2024-2025]; New Zealand [2023-2024]: India [2024-2025]; Brazil [2025]; and Mexico [2025]. Total number of participants (age 18+): 23,076 [Cumulative]; 3000 [2022], 6064 [2023], 7012 [2024], 7000 [2025].

The overall trend shows a significant increase in fatalistic attitudes toward both financial and data loss, particularly between 2024 and 2025. Such fatalism is a key behavioral barrier, as the belief often leads to security apathy and a reduced motivation to engage in protective security behaviors.

It's important to note, however, that this perception of 'unavoidability' may not be purely fatalistic, but rather a realistic risk assessment. Given the pervasive nature of global cyber threats, participants may be acknowledging the reality that perfect security is impossible.

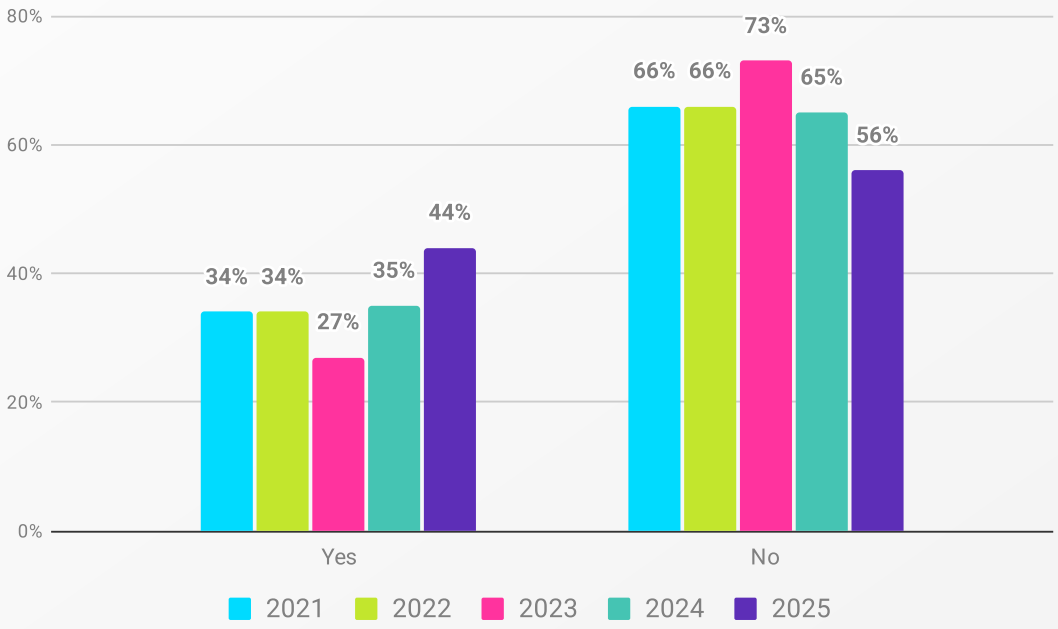
🔷 4.2 Cybercrime prevalence:
More hits, more losses

The data reveal a significant and accelerating trend toward increased cybercrime victimization across the five-year period (Figure 14).

Victimization rates began at 34% in 2021 and 2022. The rate then saw a slight dip to 27% in 2023 before surging upward in the final two years. In 2025, 44% reported being victimized, representing a 10% increase in five years.

This accelerating rate of personal money or data loss directly aligns with the findings showing that worry about falling victim to cybercrime is high and growing (Figure 12).

Figure 14. *'Have you ever personally been a victim of online scams where you have lost money or data?'*



Base: US [2021-2025]; UK [2021-2025]; Canada [2022-2024]; France [2023]; Germany [2023-2025]; Australia [2024-2025]; New Zealand [2023-2024]: India [2024-2025]; Brazil [2025]; and Mexico [2025]. Total number of participants (age 18+): 25,076 [Cumulative]; 2000 [2021], 3000 [2022], 6064 [2023], 7012 [2024], 7000 [2025].

The number of cybercrime incidents for various types of cybercrimes in each year is presented in Table 2, to supplement the data presented in Figure 14. The numbers in the table underline the notable increases in victimization over the years.

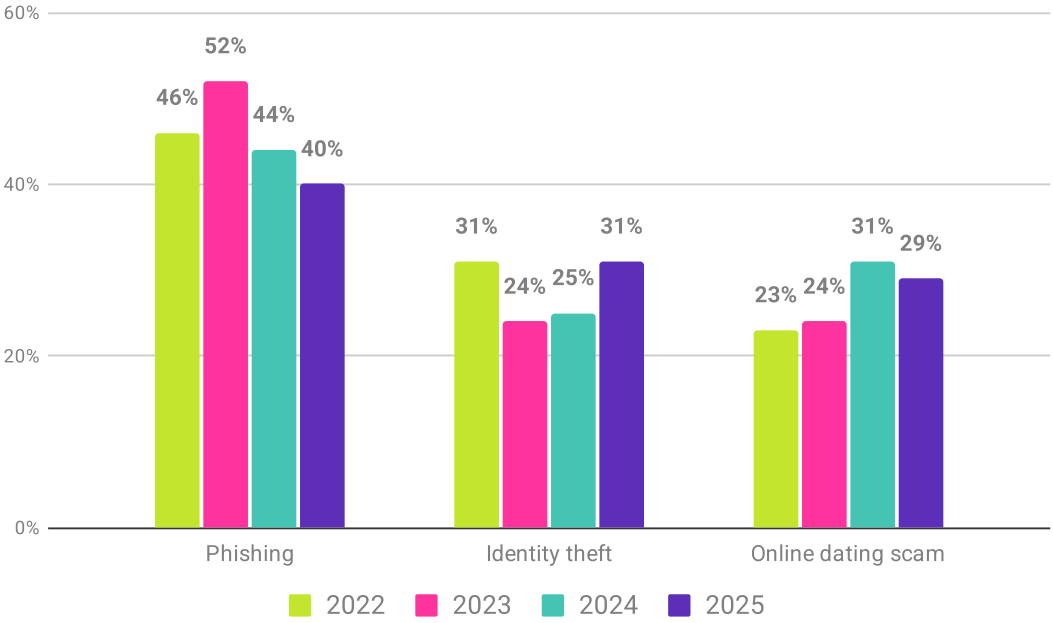
Table 2. Number of victimization incidents reported each year[12]

	2021 (N=2000)	2022 (N=3000)	2023 (N=6064)	2024 (N=7012)	2025 (N=7000)
Phishing	N/A	610	665	1463	1364
Identity theft	380	410	304	855	1066
Online dating scam	N/A	295	311	1028	974
Crypto investment fraud	N/A	N/A	N/A	N/A	683
Tech support scam	N/A	N/A	N/A	N/A	476
Other	N/A	N/A	N/A	N/A	182
Total number of incidents	680	1315	1280	3346	4745

And the data presented in Table 2 is further visualized in Figure 15 below. Out of all types of incidents, phishing was the highest in every year over the four-year period, peaking at 52% in 2023.

The percentage of online dating scams has increased over the past four years, from 22% in 2022 to 29% in 2025. And while the percentage of identity theft incidents were the same in 2025 as in 2022 (31%), that still represents a 5% increase from 2024.

Figure 15. Types of cybercrime incidents.



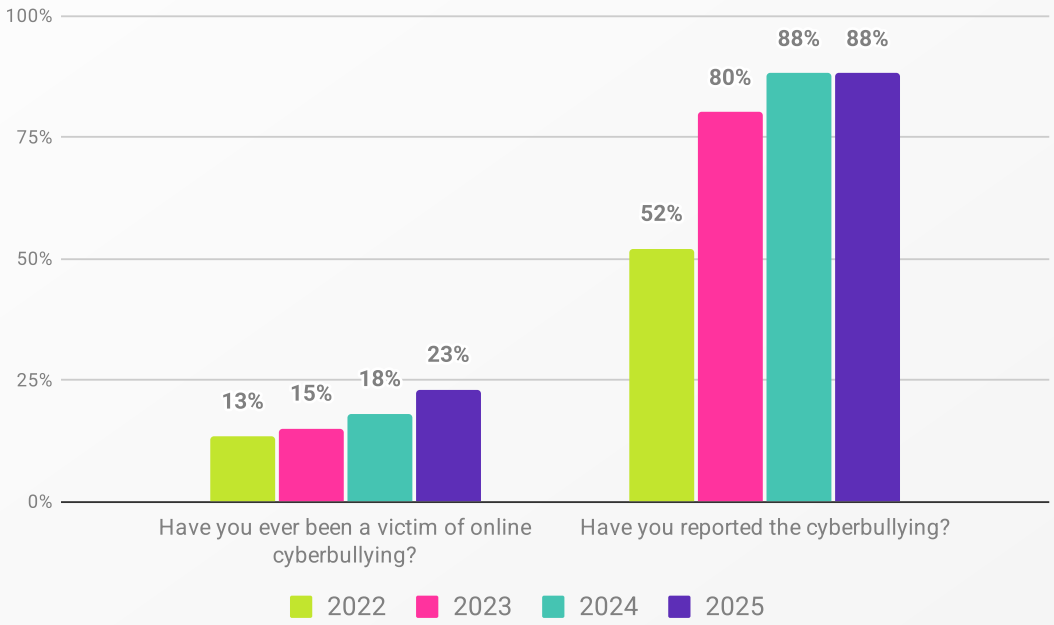
Base: US [2022-2025]; UK [2022-2025]; Canada [2022-2024]; France [2023]; Germany [2023-2025]; Australia [2024-2025]; New Zealand [2023-2024]: India [2024-2025]; Brazil [2025]; and Mexico [2025]. Total number of phishing, identity theft, and online dating scam incidents: 9345 [Cumulative]; 1315 [2022], 1280 [2023], 3346 [2024], 3404 [2025].

12 In 2021, the survey question and answers were worded differently. Participants were asked 'Have you ever been a victim of harmful cyber activities online (e.g. phishing attempts or data leaks) that have resulted in the loss of money or data?' with the options 'No'; 'Yes, once'; 'Yes, 2-3 times'; 'Yes, 4-5 times'; 'Yes, more than 6 times'. The only specific type of cybercrime victimization question participants received was about identity theft. Furthermore, N/A means the specific cybercrime options were not provided to the participants.

There has been a consistent and substantial increase in the percentage of people who say they've been victims of cyberbullying (Figure 16).

The percentage of victims started at 13% in 2022 and has increased every year, by 10% overall to 23% in 2025.

Figure 16. Cyberbullying victimization and reporting.



Base: US [2021-2025]; UK [2021-2025]; Canada [2022-2024]; France [2023]; Germany [2023-2025]; Australia [2024-2025]; New Zealand [2023-2024]: India [2024-2025]; Brazil [2025]; and Mexico [2025]. Total number of participants (age 18+): 25,076 [Cumulative]; 2000 [2021], 3000 [2022], 6064 [2023], 7012 [2024], 7000 [2025]. Total number of participants who have experienced cyberbullying (age 18+): 4213 [Cumulative]; 402 [2022], 921 [2023], 1268 [2024], 1622 [2025].

On a positive note, the percentage of cyberbullying victims who reported the incident has risen sharply across the four years. The reporting rate began at just 52% in 2022, and it rose to 80% in 2023.

The rate then stabilized at a high level, peaking at 88% in both 2024 and 2025. This consistent rise and stabilization mean that nearly nine out of ten cyberbullying victims now report the incident, representing a 36% increase in reporting since 2022.

KEY TAKEAWAYS

Victimization accelerating
Overall victimization rates rose from 34% (2021) to 44% (2025), with the steepest rise between 2024 and 2025.

Worry at an all-time high
Concern about falling victim to cybercrime climbed from 57% (2022) to 68% (2025).

Fatalism rising
Fatalistic attitudes toward both financial and data loss increased significantly. Those viewing financial loss as unavoidable rose from 25% (2022) to 31% (2025), while those seeing data theft as unavoidable increased from 34% (2022) to 40% (2025).

Cyberbullying reporting improved
While cyberbullying victimization rose from 13% (2022) to 23% (2025), reporting rates surged from 52% (2022) to 88% (2024-2025). Nearly nine out of ten victims now report incidents.

👉 WITH THAT IN MIND, IT'S TIME TO JUMP FROM INCIDENT TO SUPPORT. IN **CHAPTER 5** WE'LL LOOK AT CYBERSECURITY TRAINING: WHO GETS IT, BARRIERS TO ACCESS, AND ITS IMPACT ON BEHAVIORS. WE KNOW WHAT HAPPENS WHEN THINGS GO WRONG, BUT WHAT DOES TRAINING TO DO HELP PEOPLE GET IT RIGHT NEXT TIME?

5. Cybersecurity training: Safety net or comfort blanket?

Cybersecurity training aims to build the Capability needed for secure behavior through knowledge and skills. However, the COM-B model shows that training effectiveness also depends on Opportunity (access and time to attend) and Motivation (willingness to engage and belief in training's value).

This chapter explores the state of security education, covering access to cyber training, prevalence of mandatory training, the main psychological and practical barriers to attendance, and the self-reported impact of training.

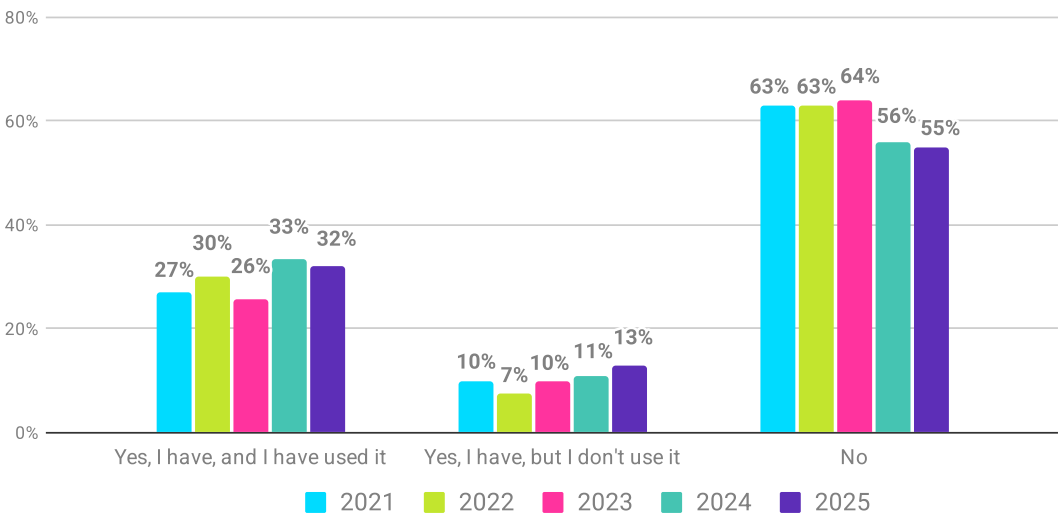
🔷 5.1 Access to training and prevalence of mandatory training: Who actually gets a seat

The data shows that while access to cybersecurity training has increased, the majority of participants still report having no access at all (Figure 17).

Over half of the participants have consistently reported not having access to training, peaking at 64% in 2023. While access to training has increased since to 45% in 2025, over half still report being without an accessible, formal option for security training.

The percentage of those who have used cyber training has seen a modest increase, from 27% in 2021 to 32% in 2025. And so did those who chose not to use the training available to them, from 10% in 2021 to 13% in 2025.

Figure 17. ***'Do you have access to cybersecurity training (e.g., at work, school, library or other public location)?'***



Base: US [2021-2025]; UK [2021-2025]; Canada [2022-2024]; France [2023]; Germany [2023-2025]; Australia [2024-2025]; New Zealand [2023-2024]: India [2024-2025]; Brazil [2025]; and Mexico [2025]. Total number of participants (age 18+): 25,076 [Cumulative]; 2000 [2021], 3000 [2022], 6064 [2023], 7012 [2024], 7000 [2025].

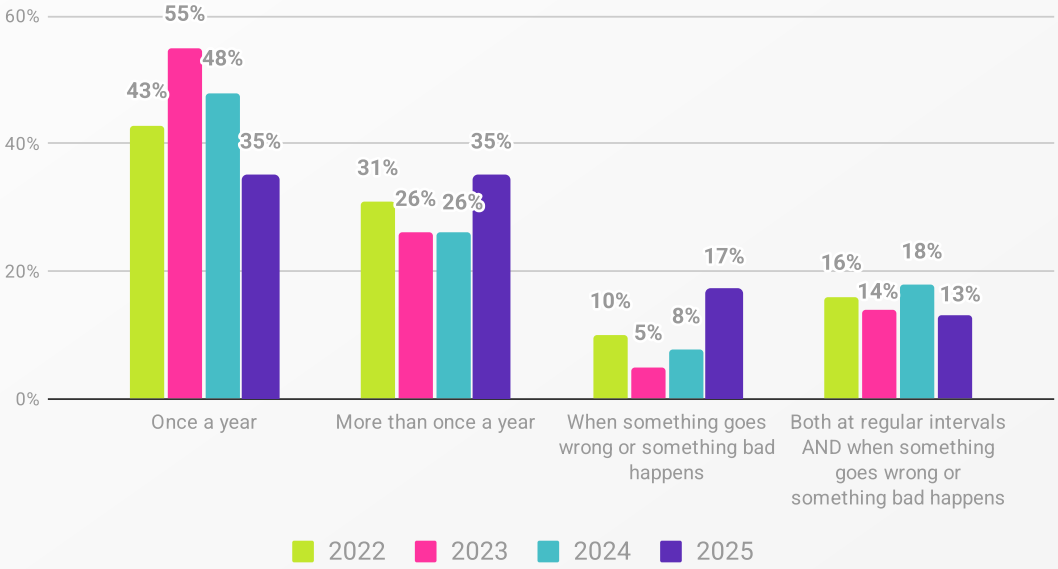
Having to complete mandatory training once a year was the most common practice in the past four years (Figure 18), ranging from 35% (in 2025) to 55% (in 2023).

The percentage of those completing training more than once a year has increased from 31% in 2022 to 35% in 2025, despite the two-year drop to 26% in 2023 and 2024.

Completing training when something goes wrong or something bad happens has increased notably from 10% in 2022 to 17% in 2025; this is after dips in 2023 and 2024.

Training completion, both at regular intervals and when something goes wrong, has decreased from 16% in 2022 to 13% in 2025.

Figure 18. *'How often are you required to complete training?'*



Base: US [2022-2025]; UK [2022-2025]; Canada [2022-2024]; France [2023]; Germany [2023-2025]; Australia [2024-2025]; New Zealand [2023-2024]: India [2024-2025]; Brazil [2025]; and Mexico [2025]. Total number of participants (age 18+) who are required to complete mandatory training: 5150 [Cumulative]; 522 [2022], 947 [2023], 1432 [2024], 2249 [2025].

Overall, the findings reveal a pronounced, persistent gap in people's security education. Despite modest improvements over the five-year period, the majority of participants consistently report having no access to formal training resources. Over half the connected audience is left to navigate the evolving threat landscape without security guidance, while simultaneously, a growing minority with access chooses not to utilize it.

The findings also show a shift away from the annual training model: the percentage of those receiving training more than once a year is increasing, and there's a clear rise in reactive, incident-based training.

This evolution may reflect a growing recognition that the traditional once-a-year, generic training approach has no or limited long-term impact on behavior change and risk reduction, as demonstrated by numerous research in the field.

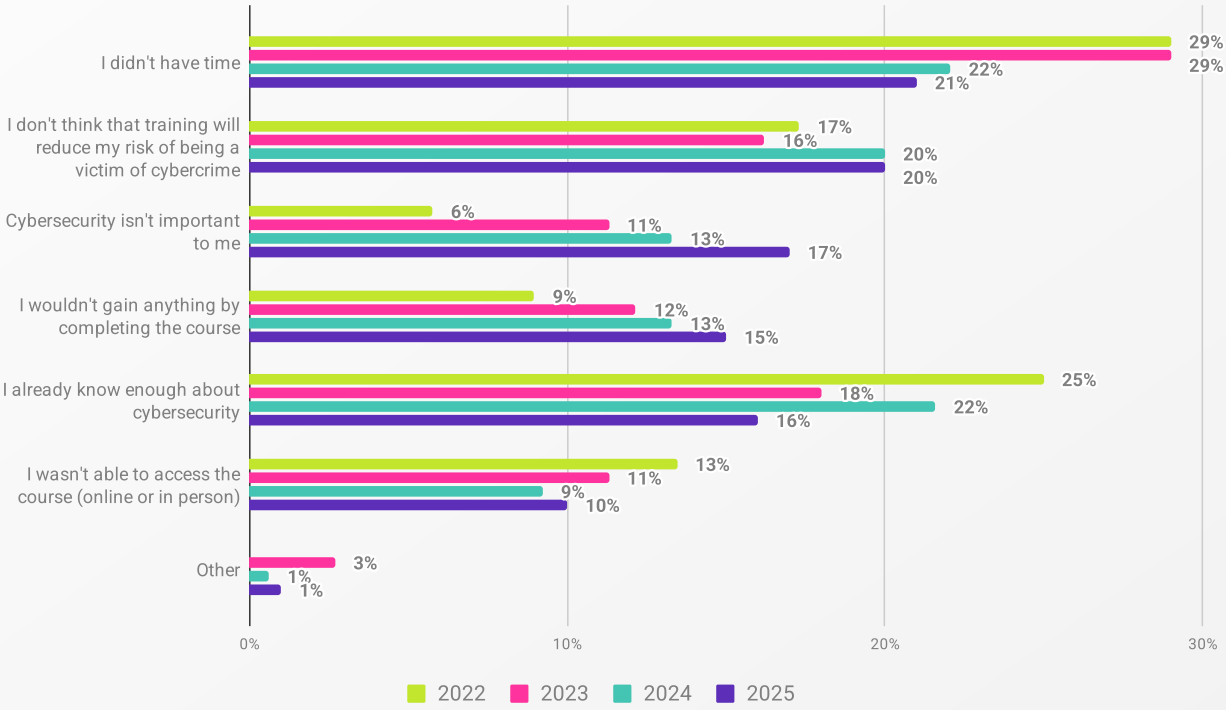
For instance, it's been shown that the benefits of initial training significantly degrade after just six months[13], or that annual training programs offer no significant practical value in meaningful risk reduction[14].

This move toward more frequent, timely, or event-triggered training (away from the passive, once-a-year requirement) suggests organizations may be adopting a modern, continuous approach to building user capability, even as the overall availability of training remains a challenge.

🔷 5.2 Barriers to attendance: Inbox 1, training 0

The data shows that over the past four years, time constraints, perceived knowledge, and doubt about training's efficacy are the three main barriers stopping people from engaging with the available training (Figure 19).

Figure 19. *'What is the main reason you didn't use the opportunity to attend a cybersecurity training course?'*



Base: US [2022-2025]; UK [2022-2025]; Canada [2022-2024]; France [2023]; Germany [2023-2025]; Australia [2024-2025]; New Zealand [2023-2024]: India [2024-2025]; Brazil [2025]; and Mexico [2025]. Total number of participants (age 18+) who didn't attend cybersecurity training: 2280 [Cumulative]; 156 [2022], 592 [2023], 639 [2024], 893 [2025]. Note: In 2022, the 'Other' option was not provided to the participants, hence the lack of data.

13 Reinheimer, B., Aldag, L., Mayer, P., Mossano, M., Duezguen, R., Lofthouse, B., ... & Volkamer, M. (2020). An investigation of phishing awareness and education over time: When and how to best remind users. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)* (pp. 259-284).

14 For example: Ho, G., Mirian, A., Luo, E., Tong, K., Lee, E., Liu, L., ... & Voelker, G. M. (2025, May). Understanding the efficacy of phishing training in practice. In 2025 *IEEE Symposium on Security and Privacy (SP)* (pp. 37-54). IEEE.

The number one reason for not attending cybersecurity training was not having enough time in all four years (ranging from 29% in 2022 to 21% in 2025, representing an 8% decrease). However, in 2024, the same percentage of participants (22%) provided 'already knowing enough about cybersecurity' as the main reason. In fact, already having sufficient knowledge was the second most common reason for not engaging in training in 2022 (25%) and in 2023 (18%).

In 2024 and 2025, however, the percentage of those thinking that training won't reduce their risk of cybercrime victimization has increased to 20% (from 16% in 2023), making it the second most common reason in those years.

Interestingly, those who feel that cybersecurity isn't important to them have also increased over the years, quite sharply, rising from 6% in 2022 to 17% in 2025. This 11% increase in the most negative attitudinal response suggests that a growing number are actively disengaged from security.

The data clearly indicates that resistance to cybersecurity training stems from a complex mix of Motivation, Capability, and Opportunity factors. The largest barriers are practical (time constraints), attitudinal (perceived irrelevance), and rooted in high self-efficacy (prior knowledge).

Therefore, time constraints ('I didn't have time') represent a barrier to Opportunity, and high self-efficacy ('I already know enough about cybersecurity') represents a psychological Capability barrier. Regarding Motivation, the attitudinal barriers are the most pronounced. Doubts that 'training will reduce my risk' reflect low reflective Motivation, as users don't believe the training is effective. Feeling that 'Cybersecurity isn't important to me' reflects the growing problem of low automatic Motivation, a foundational disregard for the security itself.

🔷 5.3 Impact on security behaviors: Needle moved or time wasted?

In the past four years, people consistently reported the highest perceived impact of cybersecurity training to be on their ability to recognize and report phishing messages (Figure 20), with 58% in 2022 to 47% in 2025. And despite the highest impact, this still represents an 11% drop in the four-year period.

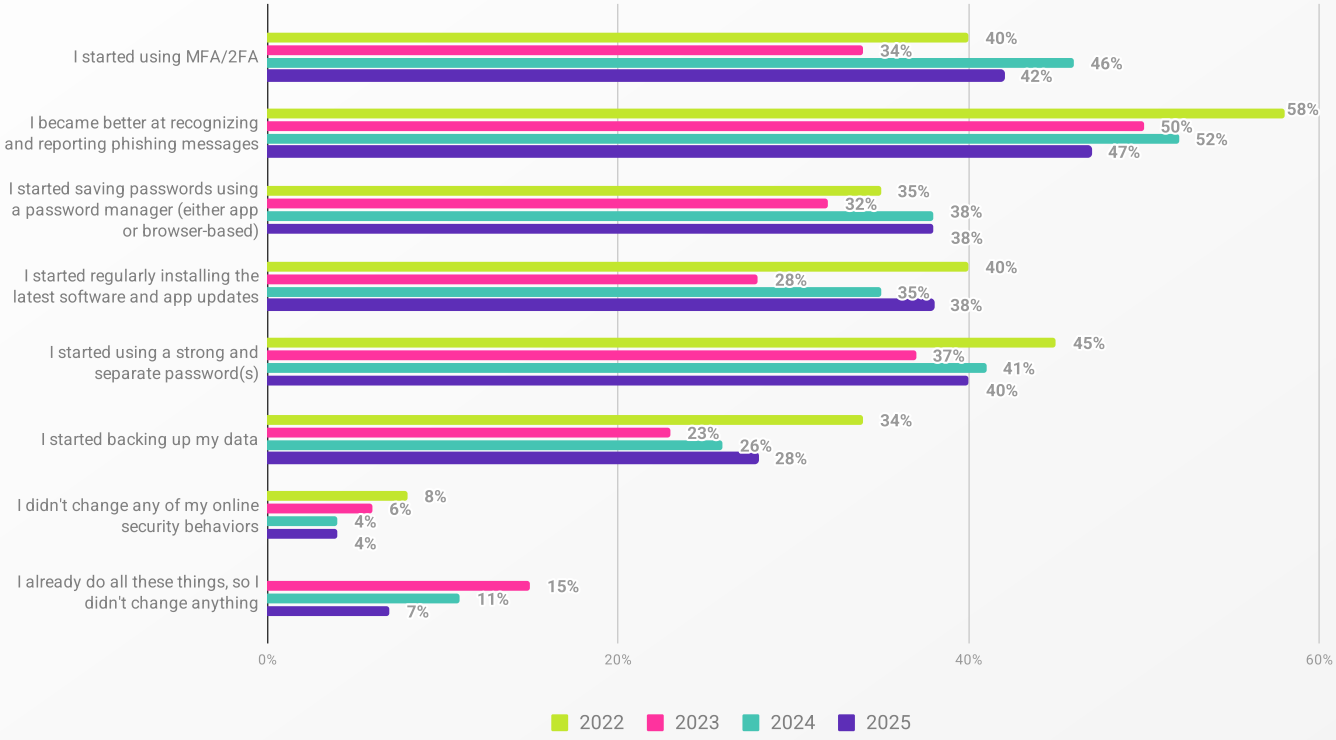
The second highest impact of training was on people's MFA use in 2024 (46%) and in 2025 (42%), and their use of strong and separate passwords in 2022 (45%) and 2023 (37%). However, both of these behaviors showed a recent decline, with MFA use decreasing from 46% in 2024 to 42% in 2025, and the use of strong passwords decreasing from 41% in 2024 to 40% in 2025.

The use of password managers as a result of training has increased over the four years from 35% to 38% in 2025. However, the impact of training on the rest of the measured behaviors has decreased over four years:

- Installing software updates from 40% (2022) to 38% (2025)
- Backing up data from 34% (2022) to 28% (2025).

On a positive note, the percentage of those who felt training didn't impact their security behaviors generally has decreased over the period, from 8% (2022) to 4% (2025).

Figure 20. ***'When you attended cybersecurity training, how did it influence your security behaviors?'***



Base: US [2022-2025]; UK [2022-2025]; Canada [2022-2024]; France [2023]; Germany [2023-2025]; Australia [2024-2025]; New Zealand [2023-2024]: India [2024-2025]; Brazil [2025]; and Mexico [2025]. Total number of participants (age 18+) who attended cybersecurity training: 6792 [Cumulative]; 905 [2022], 1559 [2023], 2060 [2024], 2268 [2025]. Note: In 2022, the 'I already do all these things, so I didn't change anything' option was not provided to the participants, hence the lack of data.

The data on perceived training efficacy reveals that while participants report positive impacts across various behaviors, the reach of this impact is both limited and declining. While attendees reported clear positive changes in key security behaviors (e.g., recognizing and reporting phishing, MFA use, and strong password adoption), the impact has generally decreased over the four years on most of the behaviors measured. Furthermore, these positive impacts were consistently reported by less than half the participants from 2023 onwards.

KEY TAKEAWAYS

Access gap persists
The majority of participants consistently report having no access to formal training resources (63% in 2021 to 55% in 2025). Thereby meaning that over half are left to navigate the threat landscape without security guidance.

Shift away from annual training
Training is becoming more frequent, with 'more than once a year' rising from 31% (2022) to 35% (2025). Reactive, incident-based training also increased from 10% (2022) to 17% (2025), suggesting a move toward continuous rather than once-a-year approaches.

Barriers are practical and attitudinal
Time constraints remain the top barrier (29% in 2022 to 21% in 2025), followed by perceived existing knowledge (25% in 2022 to 16% in 2025) and doubts about training's efficacy (17% in 2022 to 20% in 2025).

Impact is limited and declining
While attendees report positive changes in behaviors like phishing recognition and MFA use, impact has generally decreased over four years. Positive impacts were reported by less than half of participants from 2023 onwards.

👉 NEXT, IT'S TIME TO LEAVE THE DOJO AND GET UP CLOSE WITH LIVE ACTION: WHAT DO PEOPLE ACTUALLY DO? IN THE FINAL CHAPTER, WE'LL COVER DAY-TO-DAY CYBERSECURITY BEHAVIORS (PASSWORD HYGIENE, MFA USE, SOFTWARE UPDATES, BACKUPS, AND PHISHING RECOGNITION AND REPORTING), AND WE'LL MAP THE INTENTION–BEHAVIOR GAP THAT RUNS THROUGH ALL OF THEM.

6. Cybersecurity behaviors: Pwned with good intentions

The report so far has explored the core elements required for security behavior, including Motivation (Chapter 2), Capability, and Opportunity (Chapter 5). This chapter now moves beyond attitudes and beliefs to focus on the protective behaviors people say they carry out: password practices (including creation techniques, the use of unique passwords, and preferred management strategies), MFA adoption, installing software updates, backing up data, and recognizing and reporting phishing messages.

🔷 6.1 Password hygiene: Small keyboard energy

The National Institute of Standards and Technology (NIST) guidelines[15] for password hygiene are:

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

Most of these show up in guidance across all participating countries and/or regions: NCA[16], NCSC (UK)[17], BSI[18], ACSC[19], CNIL[20], Get Cyber Safe[21], CERT-In[22], NCSC (New Zealand)[23], CERT.br[24], and SSPC[25].

In this section, we examine password hygiene, including:

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

15 https://pages.nist.gov/800-63-4/sp800-63b.html#appA

16 https://www.staysafeonline.org/articles/passwords

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

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

19 https://www.cyber.gov.au/protect-yourself/securing-your-accounts/passphrases

20 https://www.cnil.fr/fr/mots-de-passe-recommandations-pour-maitriser-sa-securite

21 https://www.getcybersafe.gc.ca/en/secure-your-accounts/passphrases-passwords-and-pins

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

23 https://www.ownyouronline.govt.nz/personal/get-protected/guides/how-to-create-good-passwords/

24 https://cartilha.cert.br/dicas-rapidas/

25 https://www.gob.mx/sspc/prensa/sspc-emite-recomendaciones-por-el-dia-mundial-de-la-contrasena?idiom=es&utm

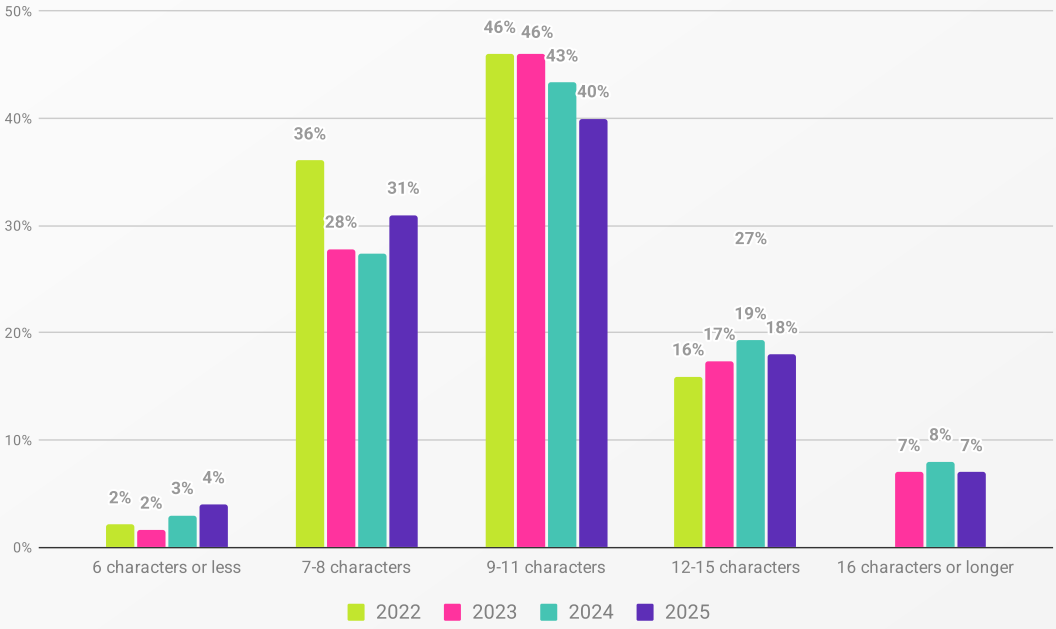
The data on password length reveals a positive shift toward stronger, longer passwords, but this progress is complicated by a worrying rebound in easily crackable, shorter options in 2025 (Figure 21).

The majority of participants in the past four years have consistently reported creating 9-11 character passwords: 46% in 2022 and 2023, 43% in 2024, and 40% in 2025.

The percentage of participants creating passwords 12 characters or longer (the recommended, best practice by the country-relevant guidance detailed above, e.g., NIST) shows a clear overall increase, rising from 16% in 2022 to 24% in 2023 and peaking in 2024 at 27%. The percentage dropped by 2% to 25% in 2025.

The use of shorter passwords (7-8 characters) fell from 36% in 2022 to 27% in 2024, but has increased to 31% in 2025.

Figure 21. *'How long are the password(s) you usually create?'*



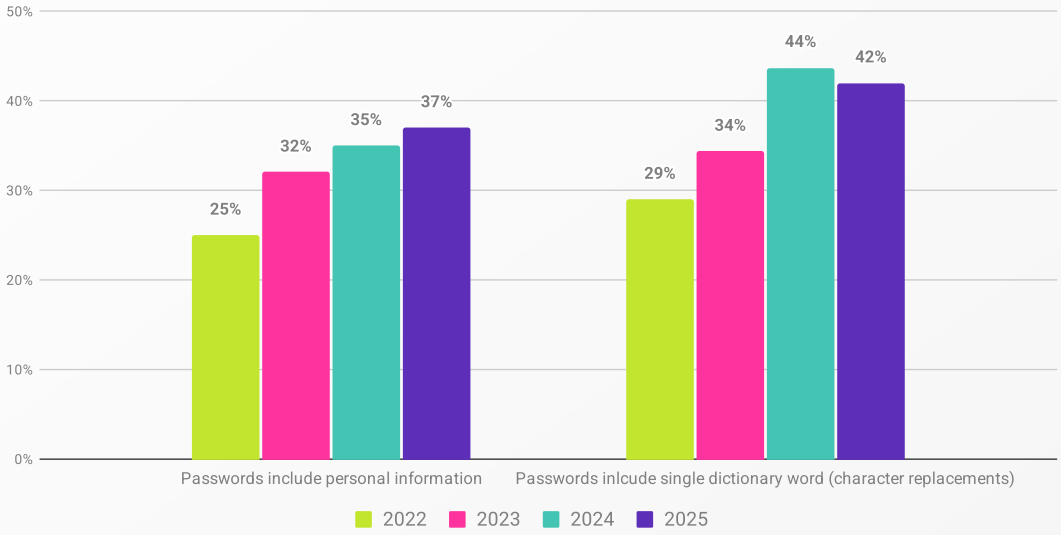
Base: US [2022-2025]; UK [2022-2025]; Canada [2022-2024]; France [2023]; Germany [2023-2025]; Australia [2024-2025]; New Zealand [2023-2024]: India [2024-2025]; Brazil [2025]; and Mexico [2025]. Total number of participants (age 18+): 23,076 [Cumulative]; 3000 [2022], 6064 [2023], 7012 [2024], 7000 [2025]. Note: In 2021, participants were not provided with the option '16 characters or longer'. Instead, the '12-15 characters' option was worded as '12 characters or longer'.

The data tracking risky password creation techniques (including personal information and simple dictionary words) shows that both remain common, with the biggest recent growth in using personal information (Figure 22).

Passwords including personal information (e.g., pet names, birthdates) have seen a clear upward trend over the four years, increasing from 25% to 37% in 2025. The 12% increase shows that a growing percentage of participants is incorporating easily guessable data into their passwords, making their accounts highly susceptible to social engineering and dictionary attacks.

The use of single dictionary words with character replacements (e.g., 'L1ly' for 'Lily') has also remained very common; it increased from 29% in 2022 to 44% in 2024, then dipped to 42% in 2025. This high usage means nearly half of the participants still rely on password creation methods that offer minimal security value. Simple character replacements are easy for modern tools to guess and crack.

Figure 22. Password creation techniques used by participants.



Base: US [2022-2025]; UK [2022-2025]; Canada [2022-2024]; France [2023]; Germany [2023-2025]; Australia [2024-2025]; New Zealand [2023-2024]: India [2024-2025]; Brazil [2025]; and Mexico [2025]. Total number of participants (age 18+): 23,076 [Cumulative]; 3000 [2022], 6064 [2023], 7012 [2024], 7000 [2025].

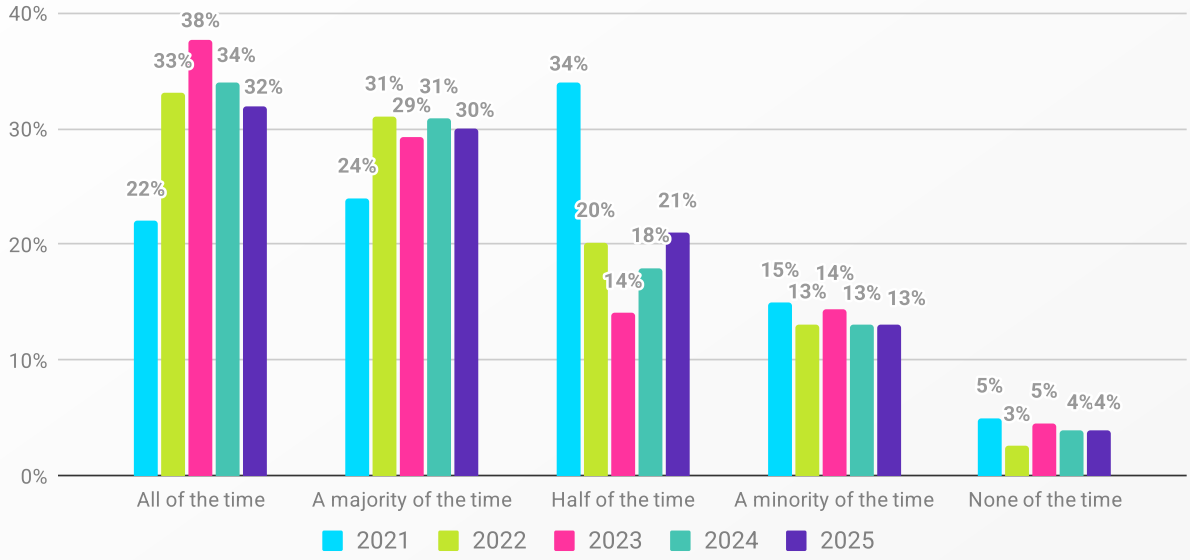
The percentage of those using unique passwords for their important accounts 'all of the time' increased from 22% in 2021 to 38% in 2023, but consistently dropped in the past two years to 32% in 2025 (Figure 23). That still represents a 10% increase within the five-year period.

Using unique passwords 'a majority of the time' has increased from 24% in 2021, and remained high, fluctuating between 29% and 31% in the subsequent years.

The percentage of participants who use unique passwords 'half of the time' has dropped from 34% in 2021 to 14% in 2023, and has increased since to 18% in 2024 and 21% in 2025. Despite the consistent increase since 2023, the behavior has dropped 13% over the five years.

People using separate passwords 'a minority of the time' or 'none of the time' remained a minority over five years, ranging from 16% (in 2022) to 20% (in 2021).

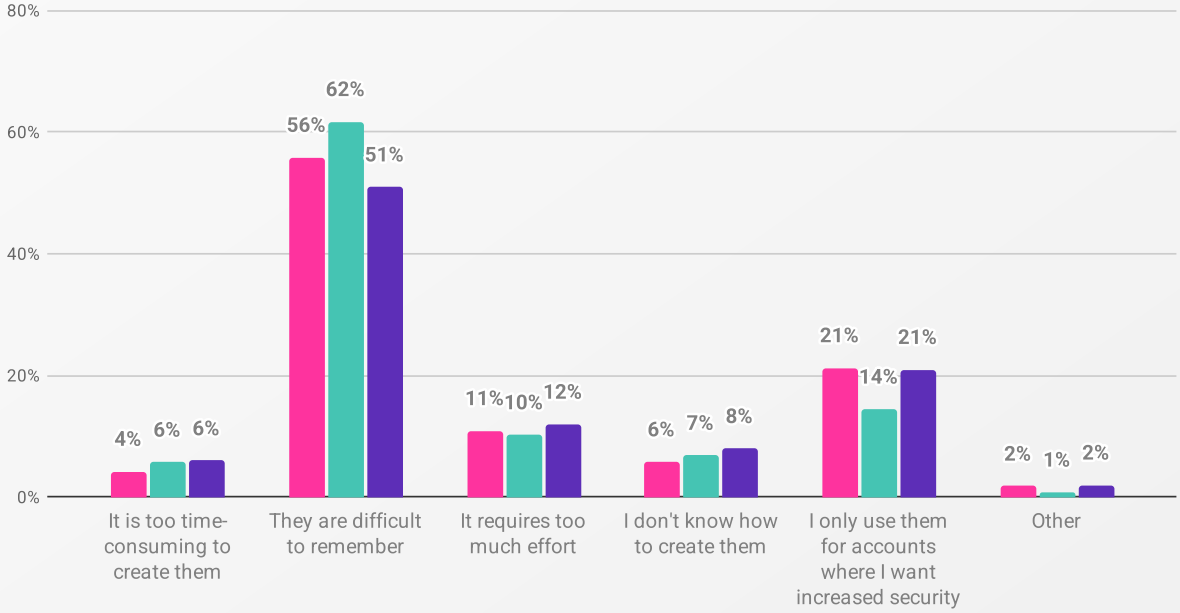
Figure 23. *'How often do you use unique passwords for your important online accounts (e.g., emails, social media, payment-related sites)?'*



Base: US [2021-2025]; UK [2021-2025]; Canada [2022-2024]; France [2023]; Germany [2023-2025]; Australia [2024-2025]; New Zealand [2023-2024]: India [2024-2025]; Brazil [2025]; and Mexico [2025]. Total number of participants (age 18+): 24,665 [Cumulative]; 2000 [2021], 2589 [2022], 6064 [2023], 7012 [2024], 7000 [2025].

Figure 24 shows that the most common reason for not using unique passwords was the difficulty in remembering them (56% in 2023, 62% in 2024, 51% in 2025), followed by only using separate passwords for accounts where people want increased security (21% in 2023, 14% in 2024, 21% in 2025).

Figure 24. *'What is the main reason you rarely, if at all, use unique passwords for your online accounts?'*

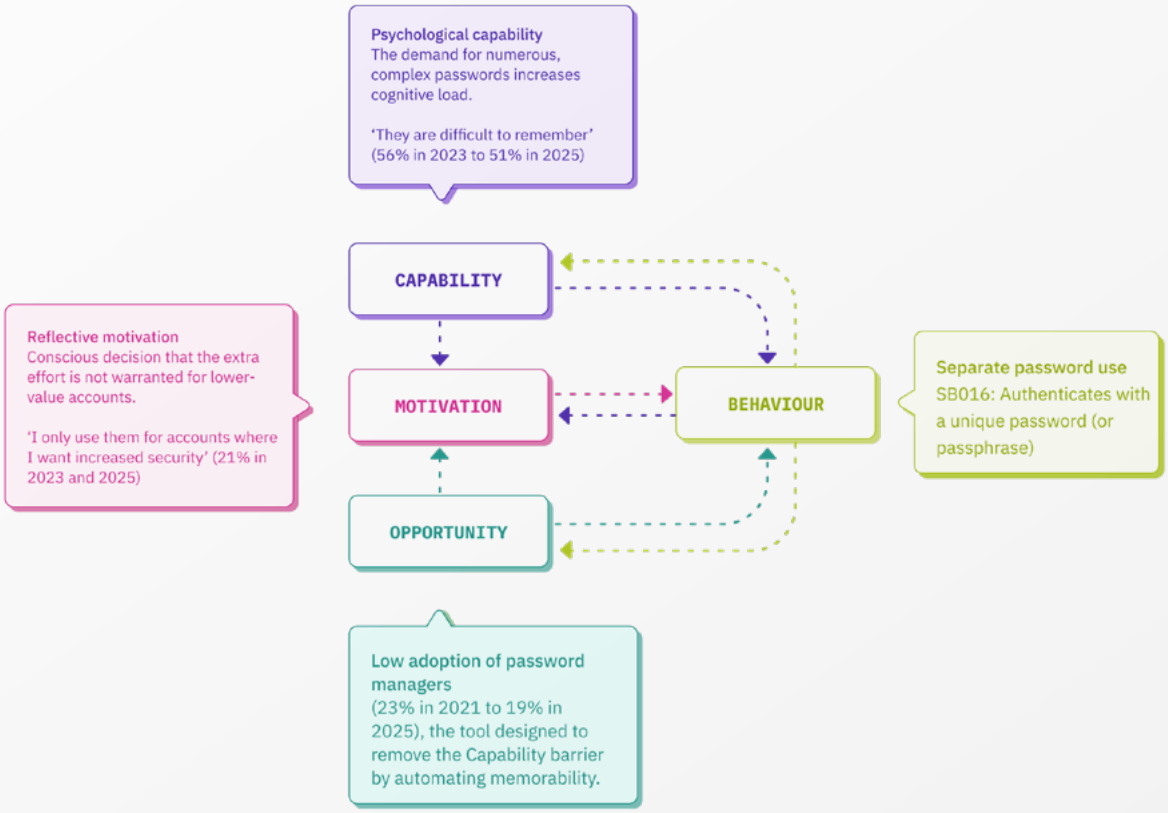


Base: US [2023-2025]; UK [2023-2025]; Canada [2023-2024]; France [2023]; Germany [2023-2025]; Australia [2024-2025]; New Zealand [2023-2024]: India [2024-2025]; Brazil [2025]; and Mexico [2025]. Total number of participants (age 18+) who 'rarely' or 'never' use unique passwords: 3070 [Cumulative]; 1151 [2023], 711 [2024], 1208 [2025].

In summary, the biggest barrier to healthy password habits is the cognitive load of managing numerous strong, unique passwords. Research that measures pupil dilation as a sign of mental effort shows that creating stronger passwords creates a higher cognitive load than creating weak passwords.[26]

As this cognitive burden increases, people find it harder to remember their passwords, which often leads to higher operational costs for organizations (e.g., increased help desk calls for password resets, productivity losses from locked accounts).[27] This pressure and difficulty drive predictable coping behaviors, which we see in the data: instead of adopting secure tools, people choose options that cut mental effort, such as password reuse, choosing simpler passwords, and the incorporation of memorable (but easily guessable) personal information.

Beyond the psychological capability barrier, the cognitive pressure drives changes in reflective motivation, leading them to make a deliberate trade-off to minimize effort by consciously choosing to only use separate passwords for accounts deemed most important.



26 Abdrabou, Y., Abdelrahman, Y., Khamis, M., & Alt, F. (2021, May). Think harder! Investigating the effect of password strength on cognitive load during password creation. In Extended Abstracts of the 2021 *CHI Conference on Human Factors in Computing Systems* (pp. 1-7).

27 Mujeye, S., & Levy, Y. (2013). Complex passwords: How far is too far? The role of cognitive load on employee productivity. *Online Journal of Applied Knowledge Management, 1*(1), 122-132.

This is compounded by limited practical opportunity, evidenced by the consistently low adoption of password manager tools (Figure 25, coming up) designed to eliminate the memorability burden by automating the creation and storage of credentials. Together, these factors may explain the high rate of password reuse and reliance on manual, high-risk workarounds.

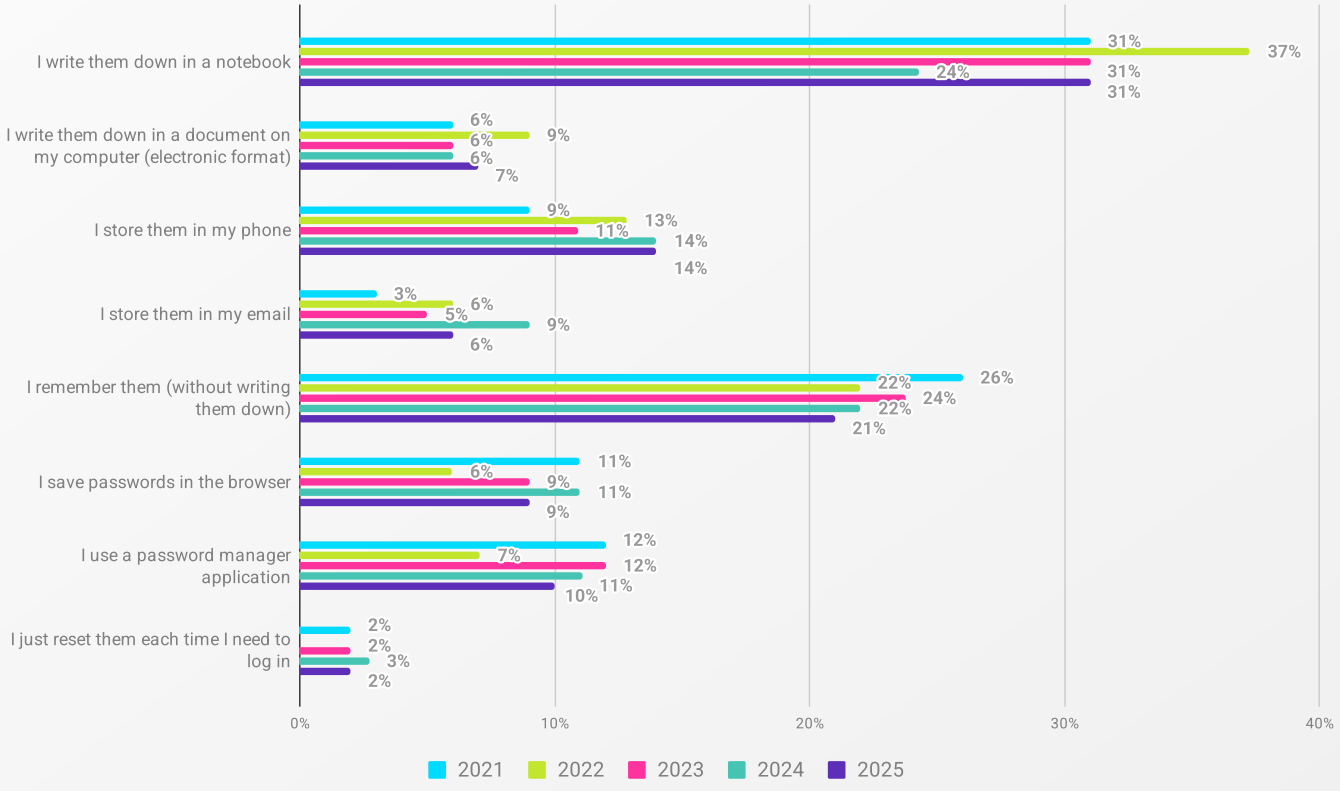
To understand how people handle multiple passwords, we asked about their preferred way of remembering them (Figure 25). Interestingly, writing them down in a notebook remains the leading method over the five-year period. This behavior peaked in 2022 at 37% and, despite fluctuating, it has increased by 7% from 2024 to 31% in 2025.

Remembering passwords (without writing them down) has consistently been the second most common response, although it has declined from 26% in 2021 to 21% in 2025.

The use of password managers (both browser-based and standalone apps) has stayed low and dropped from 23% in 2021 (at its peak) to 19% in 2025.

The consistently low adoption of password managers directly relates to the cognitive burden participants face: difficulty remembering passwords is the primary barrier to using unique ones (Figure 24). Yet fewer than one in five use the very tools built to automate this challenge and eliminate the memorability burden entirely.

Figure 25. '*What is your preferred method of remembering multiple passwords?*'

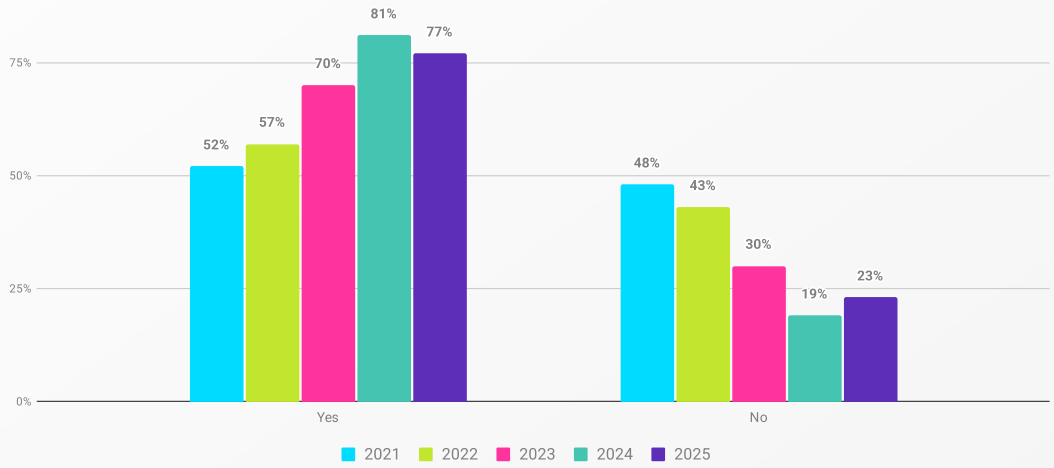


Base: US [2021-2025]; UK [2021-2025]; Canada [2022-2024]; France [2023]; Germany [2023-2025]; Australia [2024-2025]; New Zealand [2023-2024]: India [2024-2025]; Brazil [2025]; and Mexico [2025]. Total number of participants (age 18+) with more than two accounts: 25,076 [Cumulative]; 2000 [2021], 2589 [2022], 5403 [2023], 4408 [2024], 5400 [2025]. Note: In 2022, the 'I just reset them each time I need to log in' option was not provided to the participants, hence the lack of data.

🔷 6.2 Enabling multi-factor authentication (MFA), AKA trust issues (in a good way)

The percentage of participants who have heard of MFA has grown substantially every single year (Figure 26), climbing from 52% in 2021 to a peak of 81% in 2024. In 2025, awareness remained very high at 77%. Although this represents a 4% dip from the 2024 peak, the long-term trend is one of widespread knowledge, with over three-quarters of participants familiar with MFA.

Figure 26. ***'Have you ever heard of Multi-Factor Authentication (MFA)?'***



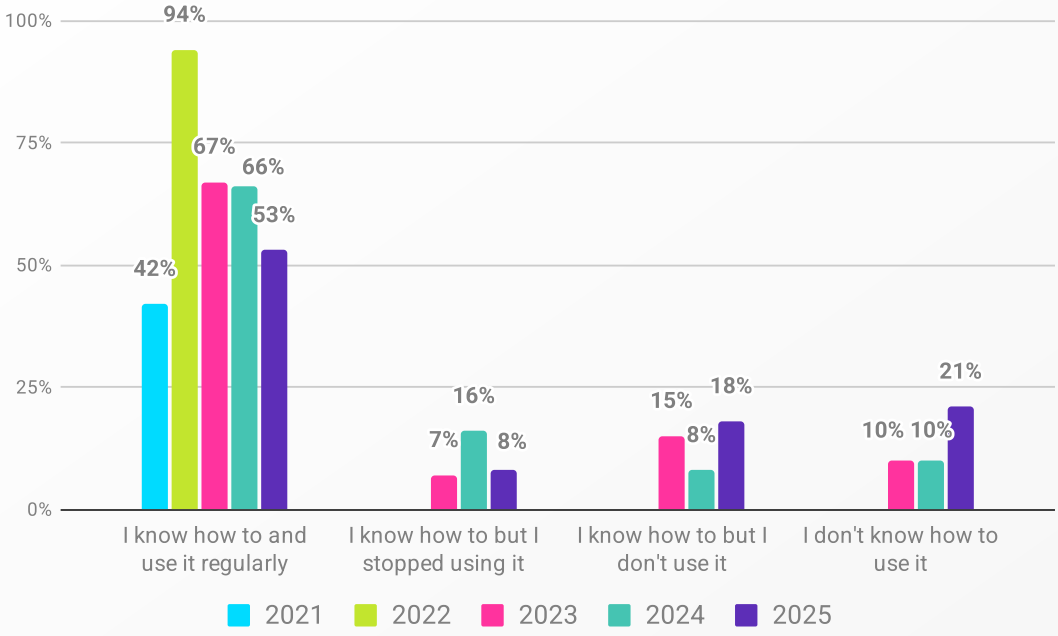
Base: US [2021-2025]; UK [2021-2025]; Canada [2022-2024]; France [2023]; Germany [2023-2025]; Australia [2024-2025]; New Zealand [2023-2024]: India [2024-2025]; Brazil [2025]; and Mexico [2025]. Total number of participants (age 18+): 25,076 [Cumulative]; 2000 [2021], 3000 [2022], 6064 [2023], 7012 [2024], 7000 [2025].

Every year, we asked participants who have heard of MFA whether they knew how to use it. The data clearly shows that the percentage of those who regularly use it has notably declined over the five-year period (Figure 27). Regular usage experienced a spike in 2022, with 94% reporting it. Following this 2022 spike, regular usage dropped sharply to 67% in 2023 and continued its decline, falling to 66% in 2024 and a low of 53% in 2025.

Interestingly, those who decided not to use MFA despite knowing how to, dipped from 2023 (15%) to 2024 (8%) but rose notably to 18% in 2025. The opposite trend occurred among those who have stopped using MFA, with an increase from 7% (in 2023) to 16% (2024), but dropped to 8% in 2025.

The percentage of those who don't know how to use it more than doubled, rising from 10% in 2024 to 21% in 2025.

Figure 27. *'Do you know how to use MFA?'*



Base: US [2021-2025]; UK [2021-2025]; Canada [2022-2024]; France [2023]; Germany [2023-2025]; Australia [2024-2025]; New Zealand [2023-2024]: India [2024-2025]; Brazil [2025]; and Mexico [2025]. Total number of participants who have heard of MFA (age 18+): 18,147 [Cumulative]; 1036 [2021], 1710 [2022], 4274 [2023], 5694 [2024], 5433 [2025]. Note: The survey question was worded differently in 2021 and 2022, hence the lack of data. Participants were asked whether they use MFA and were provided with binary 'Yes' and 'No' responses.

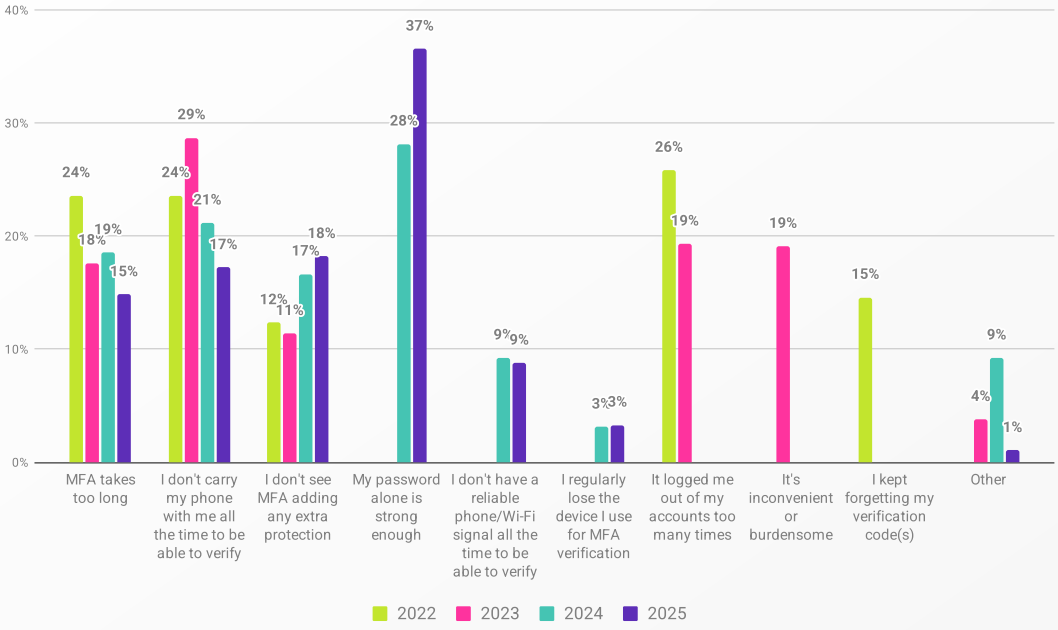
And what about those who don't or stopped using MFA, in spite of knowing how to? From 2022 onwards, we asked participants to share the main reason behind their lack of MFA use (Figure 28).

In 2022, the majority reported not using MFA because it logged them out of their accounts too many times (26%), which dropped to 19% in the following year. In 2023 the main barrier shifted to not carrying their phones with them to verify (29%).

A shift occurred in 2024, when we added additional options relating to perceptions and beliefs about MFA, not only to usability barriers. And interestingly, perceived lack of necessity emerged as the primary barrier to MFA use: in 2024 and 2025, the majority felt that their passwords were strong enough (28% and 37%, respectively), and therefore opted not to use MFA. Additionally, not seeing MFA as adding any extra protection has increased over the years, from 12% to 18% in 2025.

In summary, the primary reason for not using MFA has evolved from initial functional frustration (e.g., being logged out too often) to attitudinal barriers (believing the password alone is adequate).

Figure 28. *'What is the main reason you don't use (or stopped using) MFA?'*



Base: US [2022-2025]; UK [2022-2025]; Canada [2022-2024]; France [2023]; Germany [2023-2025]; Australia [2024-2025]; New Zealand [2023-2024]: India [2024-2025]; Brazil [2025]; and Mexico [2025]. Total number of participants (age 18+) who don't use MFA: 3832 [Cumulative]; 89 [2022], 947 [2023], 1374 [2024], 1422 [2025].

The five-year trend for MFA highlights a clear gap between knowledge and consistent action. Awareness of MFA grew substantially, climbing from 52% in 2021 to a peak of 81% in 2024, confirming the term is now familiar to over three-quarters of participants.

However, this is undercut by a sharp decline in actual usage. Following a peak adoption of 94% in 2022, the proportion of participants who regularly use MFA collapsed to just 53% in 2025.

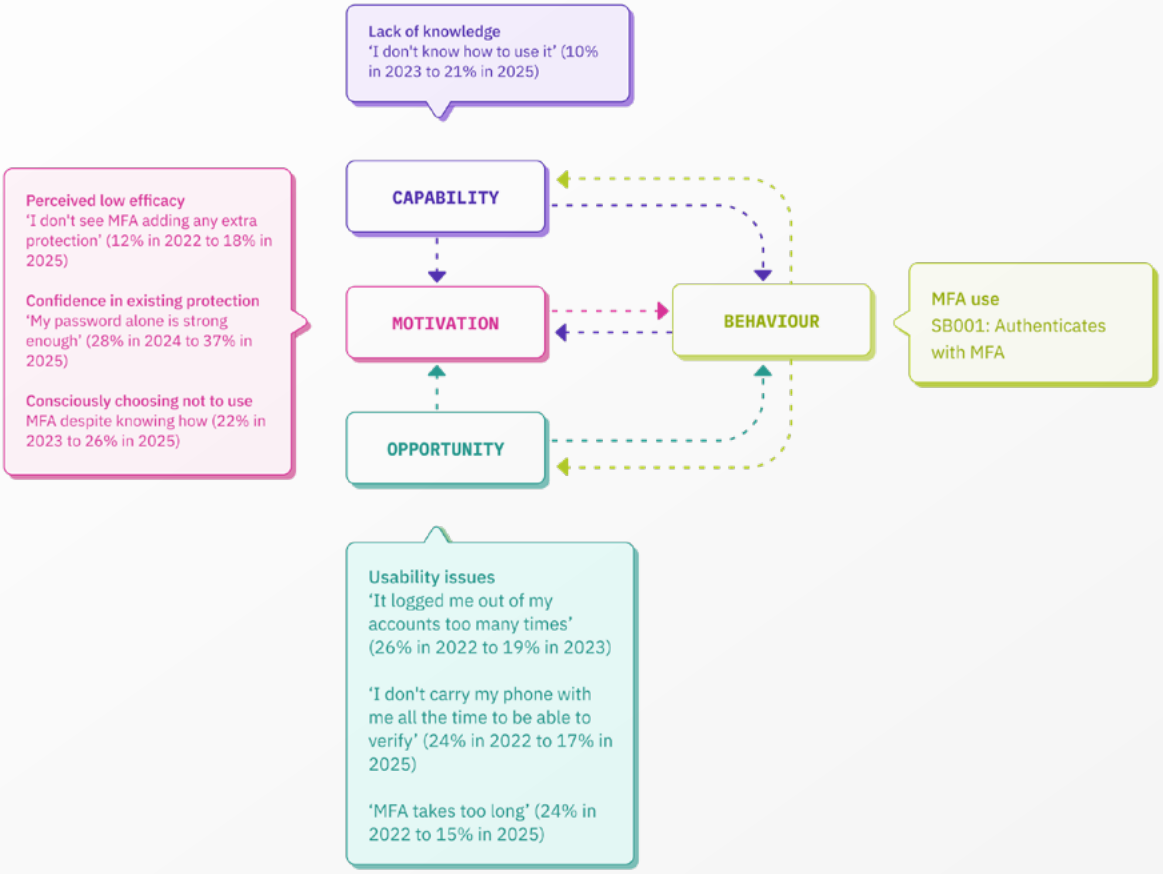
So, while MFA is no longer an unknown concept, high awareness by itself isn't enough to sustain adoption. The data suggests that there are three interconnected barriers when considering MFA adoption and use:

- **Capability**: A growing number of people still don't know how to use MFA; this more than doubled in 2025.
- **Motivation**: A major shift in attitudes and perceptions, where the majority felt their passwords were strong enough, and that MFA adds no extra protection.
- **Opportunity**: While initial functional friction (e.g., MFA taking too long) has decreased, these practical issues still potentially deter use.

Our findings line up with research[28] that consistently shows that despite MFA's security benefits, usability challenges raise concerns that lead to a lack of user motivation and difficulty understanding risk trade-offs.

28 Das, S., Wang, B., & Camp, L. J. (2019). MFA is a Waste of Time! Understanding Negative Connotation Towards MFA Applications via User Generated Content. arXiv preprint arXiv:1908.05902.

In summary, while MFA is no longer an unknown concept, high awareness and even initial adoption don't guarantee sustained, consistent action without addressing both opportunity and motivational barriers.



🔷 6.3 Installing software & app updates: Who's snoozing on patching?

The data for software installation shows a decline in consistent, immediate action (Figure 29).

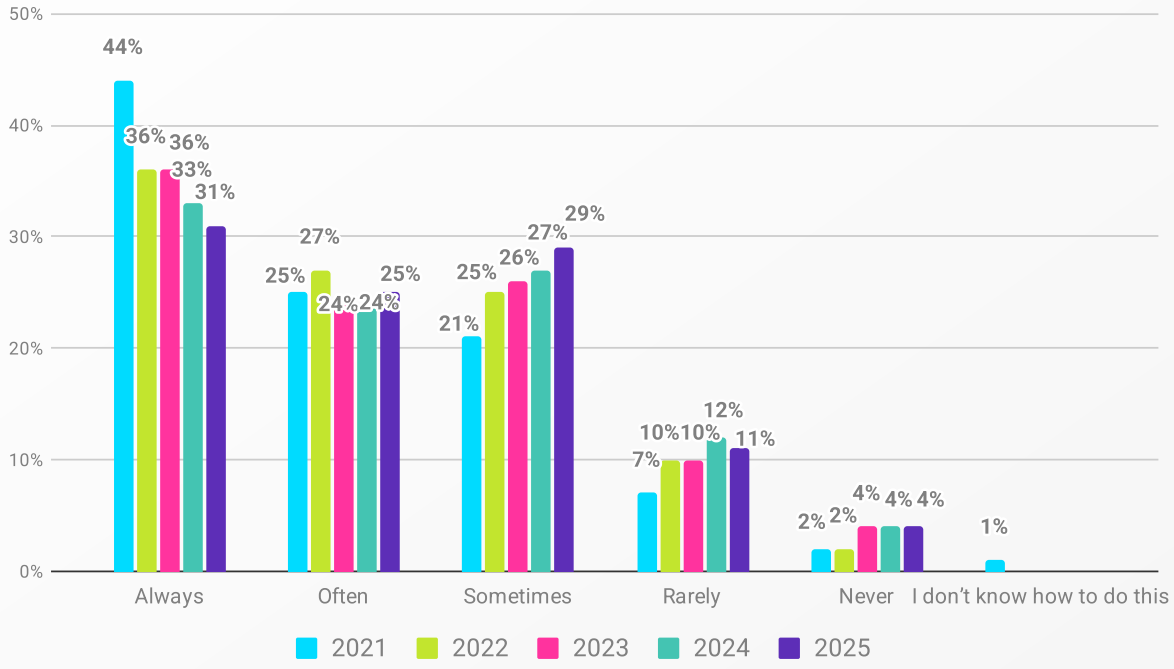
The largest proportion of participants each year have reported 'always' installing software and app updates, but this has dropped from 44% in 2021 to 31% in 2025.

The most notable growth was in those who 'sometimes' install updates, increasing from 21% in 2021 to 29% in 2025. This suggests that nearly one-third now treat updates as something to do now and then, rather than as soon as they appear.

The percentage of participants who update 'often' remained relatively stable across the five years, with 25% in 2021 and 2025, 24% in 2023 and 2024, and 27% in 2022.

The percentage of those who 'rarely' and 'never' update has increased over the years from 7% to 11% and from 2% to 4%, respectively.

Figure 29. ***'How often do you install the latest software or application updates to your devices when notified that they are available?'***



Base: US [2021-2025]; UK [2021-2025]; Canada [2022-2024]; France [2023]; Germany [2023-2025]; Australia [2024-2025]; New Zealand [2023-2024]: India [2024-2025]; Brazil [2025]; and Mexico [2025]. Total number of participants (age 18+): 25,076 [Cumulative]; 2000 [2021], 3000 [2022], 6064 [2023], 7012 [2024], 7000 [2025]. Note: The 'I don't know' option was only provided to participants in 2021, hence the lack of data in the subsequent years.

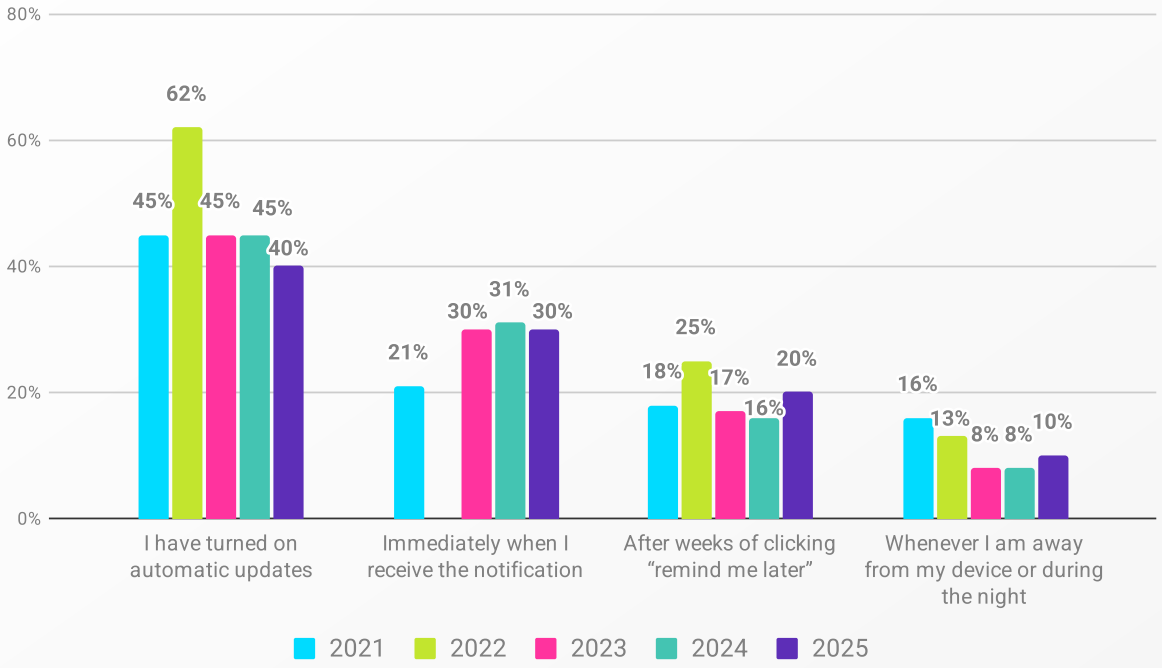
This shift to intermittent and delayed action leaves a much larger share of people exposed to known vulnerabilities, even though most modern systems make updates easy and automated.

The way people actually choose to run updates backs this up. While most have consistently reported turning auto-updates on, this behavior has declined over the five-year period (Figure 30) from 45% to 40%. This highlights that fewer participants rely on this simple set-and-forget security feature.

On the positive side, updating immediately after receiving a notification saw a jump, rising from 21% (in 2021) to 30% (in 2025). This suggests that a strong minority stays committed to updating manually straight away.

The data of those who update after weeks of clicking 'remind me later' shows fluctuation, but increased to 20% in 2025, up from 16% in 2024. This means one-fifth of participants are actively putting off critical security updates, leaving their devices vulnerable for extended periods.

Figure 30. ***'When do you install updates on your devices?'***



Base: US [2021-2025]; UK [2021-2025]; Canada [2022-2024]; France [2023]; Germany [2023-2025]; Australia [2024-2025]; New Zealand [2023-2024]: India [2024-2025]; Brazil [2025]; and Mexico [2025]. Total number of participants (age 18+) who at least sometimes update their devices: 21,556 [Cumulative]; 1926 [2021], 2631 [2022], 5217 [2023], 5871 [2024], 5911 [2025]. Note: In 2022, the 'Immediately when I receive a notification' was not an option provided to participants, hence the lack of data.

The findings suggest people are shifting away from the simplest security solution and relying more on inconsistent manual habits (particularly those that involve significant delays), increasing the overall time devices spend unpatched and vulnerable.

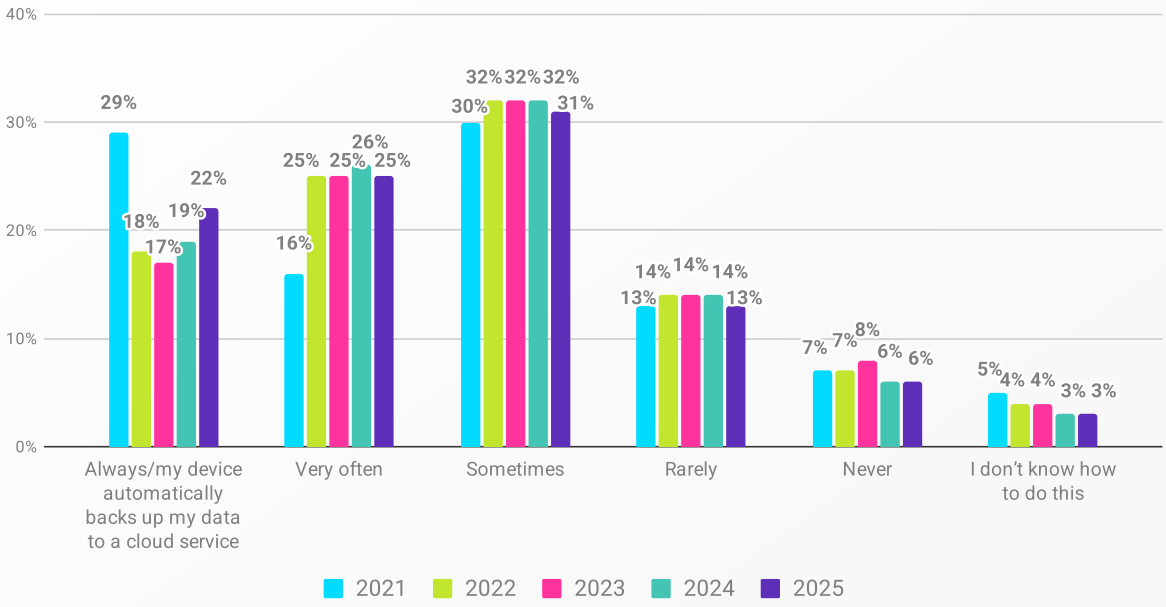
🔷 6.4 Backing up data: CTRL+S your life

People's backup behavior was at its best in 2021, with 29% 'always' backing up their data, or having it set to auto-backup (Figure 31). While this has fallen to 22% in 2025, it's still a small increase from 2023 (17%) and 2024 (19%).

Still, the biggest group each year say they only sometimes back up their data, ranging from 30% (in 2021) to 32% (in 2022, 2023, and 2024).

On a more positive note, the percentage of people who never back up data or don't know how to has also declined slightly, from 7% (in 2021) to 6% (in 2025), and from 5% (in 2021) to 3% (in 2025), respectively.

Figure 31. ***'How often do you back up your most important data?'***



Base: US [2021-2025]; UK [2021-2025]; Canada [2022-2024]; France [2023]; Germany [2023-2025]; Australia [2024-2025]; New Zealand [2023-2024]: India [2024-2025]; Brazil [2025]; and Mexico [2025]. Total number of participants (age 18+): 25,076 [Cumulative]; 2000 [2021], 3000 [2022], 6064 [2023], 7012 [2024], 7000 [2025].

Finally, backing up data is still something most people only do now and then. The largest proportion consistently reports backing up data 'sometimes'. While the percentage of those who 'always' back up has recovered slightly from its low point, the behavior still isn't automatic for most people.

🔷 6.5 Recognizing & reporting phishing messages: See something, say nothing?

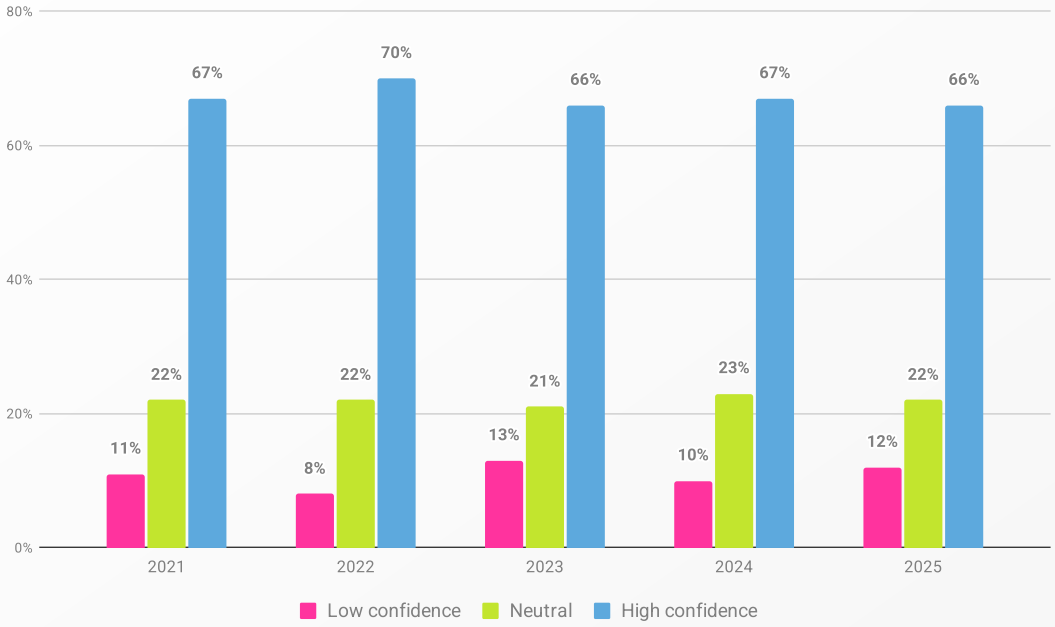
Participants consistently reported high confidence in identifying a phishing email or a malicious link over the five-year period (Figure 32). This self-efficacy has remained exceptionally stable, peaking in 2022 with 70% reporting high confidence (+3% increase from 2021), and ranging between 66% (in 2023 and 2025) and 67% (in 2024) in the years since.

This consistency is remarkable: while most security attitudes and behaviors in this report have shifted over the five-year period, (over)confidence in phishing identification has remained one of the most stable metrics.

Only a small minority report low confidence, fluctuating between 8% and 13% over the past five years.

The data points to a strong belief that people can spot phishing attempts. However, this high confidence should be viewed with care given the rising cybercrime rates and the increasingly sophisticated AI-enabled threats that challenge people's perception of their own skills.

Figure 32. ***'How confident are you in your ability to identify a phishing email or a malicious link?'***



Base: US [2021-2025]; UK [2021-2025]; Canada [2022-2024]; France [2023]; Germany [2023-2025]; Australia [2024-2025]; New Zealand [2023-2024]: India [2024-2025]; Brazil [2025]; and Mexico [2025]. Total number of participants (age 18+): 25,076 [Cumulative]; 2000 [2021], 3000 [2022], 6064 [2023], 7012 [2024], 7000 [2025].

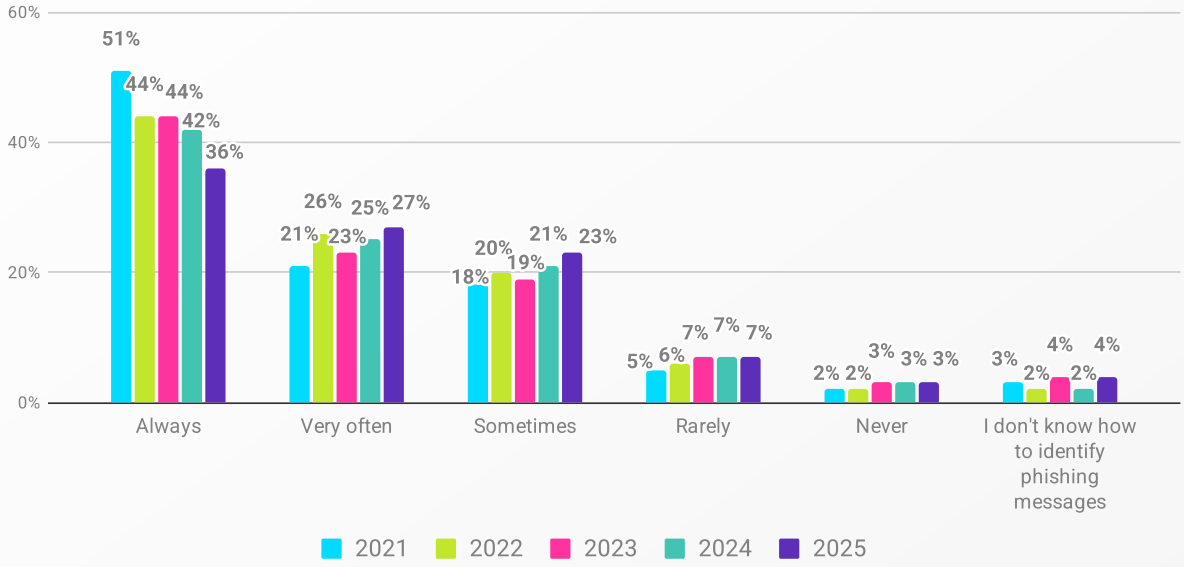
While a large portion of participants act cautiously, the percentage of those who 'always' check messages for signs of phishing has been declining over the past five years (Figure 33).

The percentage of those who 'always' check messages for phishing peaked in 2021 at 51%. It's declined each year since, falling to 44% in 2022 and 2023, 42% in 2024, and 36% in 2025, marking a 15% drop since 2021.

Most of the drop in those who 'always' inspect suspicious messages seems to have moved into 'very often' (increased from 21% in 2022 and 2023 to 27% in 2025) and 'sometimes' (increased from a low of 18% in 2022 to 23% in 2025).

Low-frequency checks and uncertainty have stayed low over the years. Only a minority neglect checking messages entirely, with 'rarely' and 'never' accounting for 7% to 9% of responses.

Figure 33. ***'How often do you check messages (e.g., emails, texts, or social media) for signs of phishing before clicking any links or responding to them?'***



Base: US [2021-2025]; UK [2021-2025]; Canada [2022-2024]; France [2023]; Germany [2023-2025]; Australia [2024-2025]; New Zealand [2023-2024]: India [2024-2025]; Brazil [2025]; and Mexico [2025]. Total number of participants (age 18+): 25,076 [Cumulative]; 2000 [2021], 3000 [2022], 6064 [2023], 7012 [2024], 7000 [2025].

In summary, the trend shows an erosion of continuous protective action. The drop in always checking suspicious messages stands in direct contradiction to the high levels of confidence in identifying threats, highlighting that confidence isn't translating into consistent security behavior.

What about reporting phishing messages (Figure 34)?

Reporting behavior tends to be selective rather than consistent.

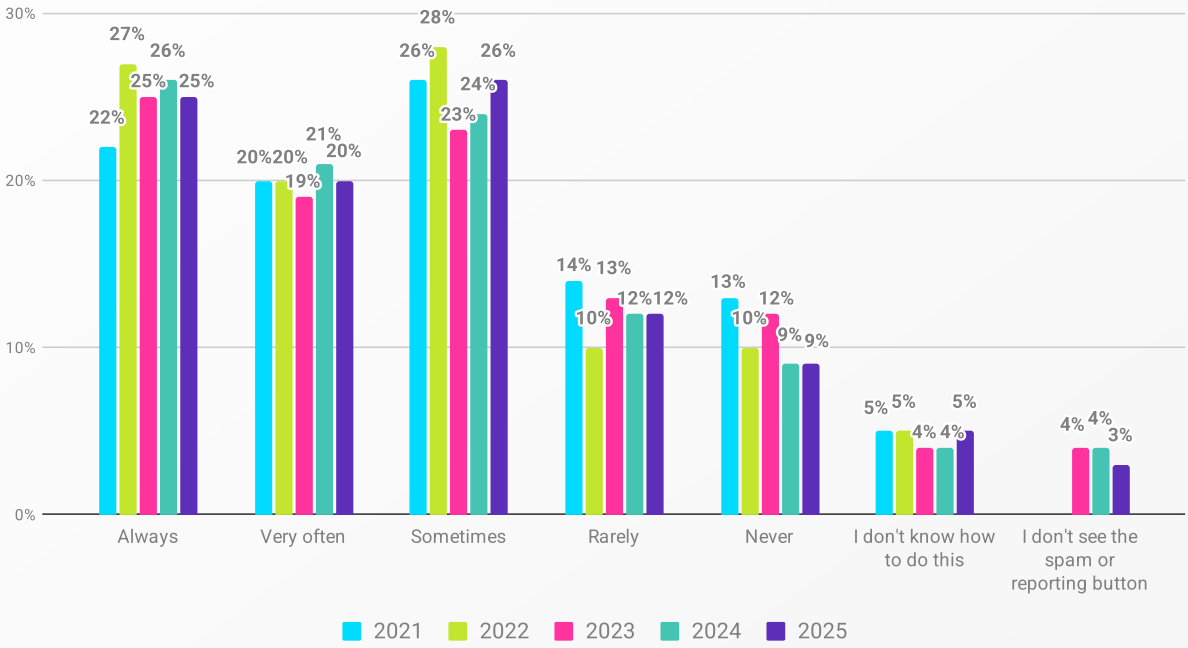
While the largest proportion of participants reported phishing messages 'sometimes' in 2021 (26%), 2022 (28%), and 2025 (26%), the most frequent response shifted to 'always' in 2023 (25%) and 2024 (26%). This pattern points to a lack of consistent reporting habits.

Over the five-year period, the percentage of consistent phishing reporters (those who report 'always' and 'very often') has increased slightly from 42% in 2021 to 45% in 2025, but peaked in 2022 with 47%.

Those who 'rarely' and 'never' report still make up a sizable group, at 21% in 2025, only slightly down from 24% in 2021.

Overall, the findings show that while most people believe they can identify a threat, consistent reporting isn't a habit for most and has declined slightly over the five-year period.

Figure 34. ***'How often do you report phishing messages (e.g., email or social media) by using the 'spam' or 'report phishing' button?'***



Base: US [2021-2025]; UK [2021-2025]; Canada [2022-2024]; France [2023]; Germany [2023-2025]; Australia [2024-2025]; New Zealand [2023-2024]: India [2024-2025]; Brazil [2025]; and Mexico [2025]. Total number of participants (age 18+): 25,076 [Cumulative]; 2000 [2021], 3000 [2022], 6064 [2023], 7012 [2024], 7000 [2025]. Note: In 2021 and 2022, the option 'I don't see the spam or reporting button' was not provided to the participants, hence the lack of data.

To understand why participants may not consistently report phishing messages despite high confidence in identifying them, we asked those who rarely or never report to rate the reasons why (Figure 35).

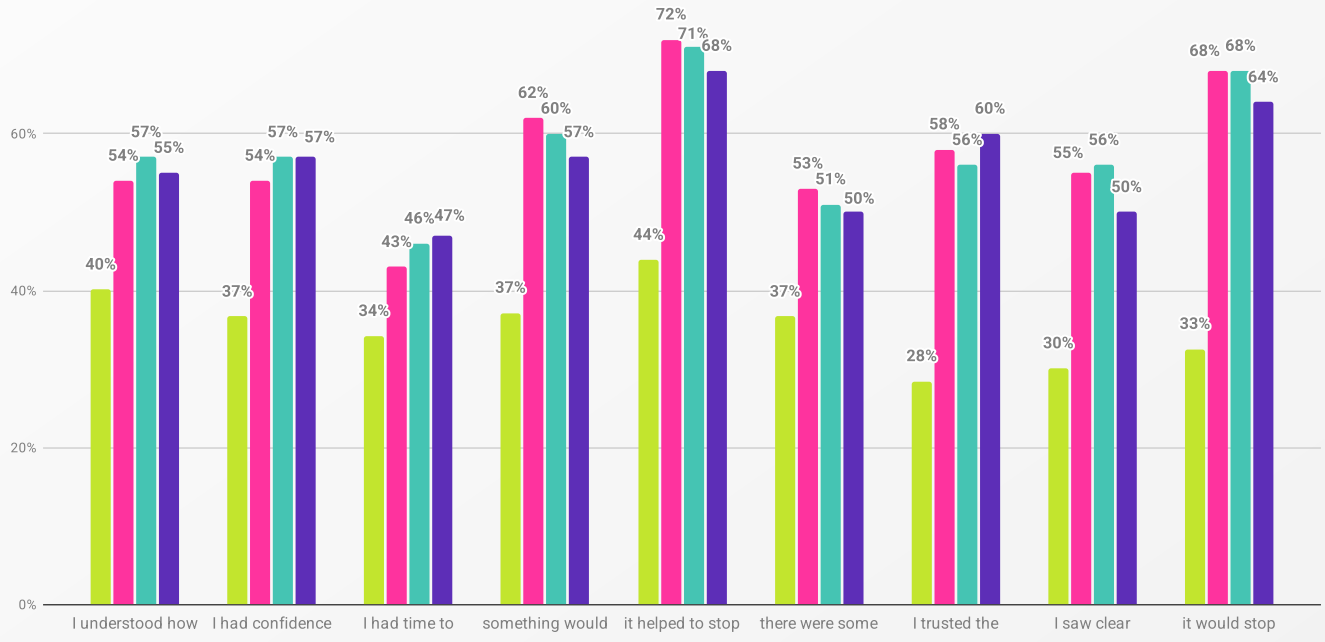
Every year from 2022 (44%) to 2025 (68%), the primary barrier to reporting was the perception that it doesn't help stop cybercriminals.

The second most common barrier between 2023 and 2025 was spam-related: 68% (in 2023 and 2024) and 64% (in 2025) indicated they don't report because they don't believe it would stop spam messages from getting into their inboxes.

Over half of the participants between 2023 and 2025 cited additional barriers: they don't believe something happens as a result of reporting (62% in 2023 to 57% in 2025), they don't trust the reporting process (58% in 2023 rising to 60% in 2025), they haven't seen clear negative consequences (55% in 2023 to 50% in 2025), and they don't see personal benefits from reporting (53% in 2023 to 50% in 2025).

The data shows an interesting pattern: there was a substantial increase across nearly all potential reasons from 2022 to 2023, followed by relatively stable or slightly declining levels through 2025. The only barrier showing a different pattern is time constraints: while only 34% cited lack of time as a reason for not reporting in 2022, this increased steadily to 47% in 2025, indicating a growing opportunity barrier. More modest but consistent increases were observed for lack of understanding (54% in 2023 to 55% in 2025) and lack of confidence (54% in 2023 to 57% in 2025).

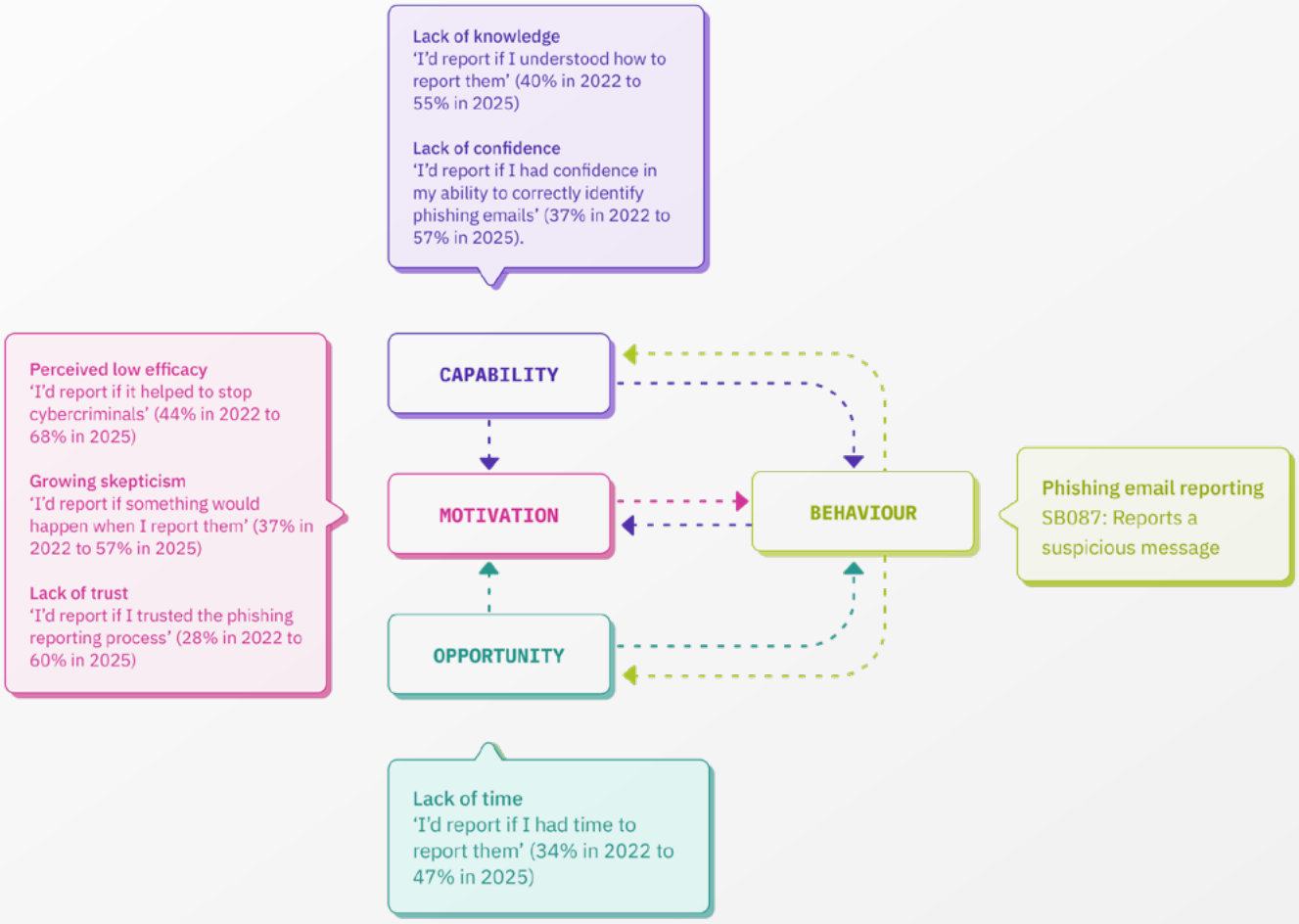
Figure 35. *'I would report phishing emails, if...'*



Base: US [2022-2025]; UK [2022-2025]; Canada [2022-2024]; France [2023]; Germany [2023-2025]; Australia [2024-2025]; New Zealand [2023-2024]: India [2024-2025]; Brazil [2025]; and Mexico [2025]. Total number of participants (age 18+) who 'never' or 'rarely' report phishing emails: 5091 [Cumulative]; 608 [2022], 1513 [2023], 1500 [2024], 1470 [2025].

The findings reveal that barriers to phishing reporting span all three COM-B components.

- **Capability** gaps persist, with over half of non-reporters lacking either the knowledge of how to report or confidence in their ability to identify threats correctly.
- **Opportunity** barrier is growing, with nearly half citing insufficient time.
- However, the most substantial barriers are **Motivational**: participants question whether their reports matter, whether the process can be trusted, and whether there are tangible benefits, either collective (stopping cybercriminals) or personal (reducing their own spam).



KEY TAKEAWAYS

The intention-behavior gap persists
This chapter revealed a persistent and widespread intention–behavior gap[29] in cybersecurity. While participants demonstrate high confidence and motivation, there's a clear inconsistency in maintaining protective behaviors. The greatest challenges occur in areas requiring routine discipline, for example, the percentage of users who 'always' install updates dropped by 13% (to 31% in 2025). MFA adoption remained unstable, with regular usage decreasing to just 53% in 2025.

Password hygiene: mixed progress
People are moving toward longer passwords (12+ characters up from 16% in 2022 to 25% in 2025), but this is undercut by increased use of personal information in passwords (up from 25% in 2022 to 37% in 2025) and declining adoption of password managers (down from 23% in 2021 to 19% in 2025).

MFA: awareness up, usage down
MFA awareness grew from 52% (2021) to 77% (2025), yet regular usage dropped from 94% (2022) to just 53% (2025). The main barrier shifted from usability issues (e.g., 'logs me out too often': 26% in 2022 to 19% in 2023) to believing passwords alone are strong enough (28% in 2024 to 37% in 2025).

Software updates declining
Those who 'always' install updates dropped from 44% (2021) to 31% (2025). Auto-update use also fell from 45% (2021) to 40% (2025).

Phishing: confidence without action
Confidence in identifying phishing remained stable and high (66%-70% across all years), yet those who 'always' check messages dropped from 51% (2021) to 36% (2025). The top barrier to reporting grew: those believing it doesn't help stop cybercriminals rose from 44% (2022) to 68% (2025).

👉 THAT'S A WRAP ON THE CHAPTERS

BUT IN THE CONCLUSION WE'LL STEP BACK AND LOOK FOR PATTERNS RUNNING THROUGH THE WHOLE PICTURE. AND WE'LL DRAW OUT THREE BIG THEMES THAT MATTER FOR ANY HUMAN RISK PROGRAM.

Conclusion

1. The capability crisis: Awareness is on blast, action’s left on read
2. The opportunity gap: Calendar says no
3. The evolving nature of barriers: Error messages to eye rolls

Conclusion

The capability crisis: Awareness is on blast, action's left on read

Across multiple behaviors, people show high awareness but lack the practical know-how to translate that into consistent action. This is most evident in the MFA usage gap: awareness grew substantially from 52% in 2021 to 77% in 2025, yet regular usage declined from 94% to 53%, with those not knowing how to use it doubling to 21%.

Similarly, the majority (ranging between 66% in 2023 and 2025 to 70% in 2022) report confidence in identifying phishing, yet far fewer (from 51% in 2021 to 36% in 2025) now say they always check messages for signs of phishing before clicking.

These findings show that knowledge and confidence (capability) don't automatically translate into security action. Indeed, the COM-B model confirms this: capability is necessary, but it's not enough without motivation and opportunity.

Research[30] on traditional security awareness campaigns backs this up, highlighting that the primary reason they don't work is the mistaken assumption that increased awareness and knowledge automatically result in a change in security behavior. Awareness alone is not enough.

The opportunity gap: Calendar says no

Structural barriers continue to limit security behaviors. One of the biggest problems is still access: More than half of the participants have consistently reported having no access to cybersecurity training (55% in 2025, down from a peak of 64% in 2023).

Furthermore, for those who do have access, lack of time is still the biggest blocker. It is consistently cited as the primary reason for not attending training (though this percentage has decreased from 29% in 2022 to 21% in 2025). Conversely, time constraints are a substantially increasing reason for not reporting phishing emails, rising from 34% in 2022 to 47% in 2025.

30 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.*

This matches wider research[31] highlighting that lack of time is a major barrier preventing employees from engaging with cybersecurity training. Time creates a critical friction point in security decision-making. People are often called upon to make security decisions while focused on a primary task[32], and research shows that under time pressure, people tend to focus more on immediate losses (task interruption) than long-term gains (security). When the time cost for a secure action is high, individuals are driven to choose less safe, low-friction alternatives.[33]

This opportunity barrier is particularly concerning because even when people possess the capability (knowledge and skills) and motivation (positive attitudes) to act securely, lack of access or time turns security from a priority into something that's easy to put off or skip entirely.

The evolving nature of barriers: Error messages to eye rolls

As technical barriers have eased, a more fundamental challenge has emerged: people now question how necessary, useful, and trustworthy security is, and it holds behavior back.

The clearest evidence of this shift appears in MFA adoption barriers. At first, most complaints were about convenience: being logged out too frequently (26% in 2022), not carrying phones for verification (24% in 2022), and MFA taking too long (24% in 2022). By 2025 (and 2023, in the case of the logging-out friction), these technical friction points had substantially declined (to 19%, 17%, and 15%, respectively). Practical complaints have been replaced by attitudinal barriers: 37% now believe their passwords alone are strong enough (up from 28% in 2024), 18% don't see MFA adding extra protection (up from 12% in 2022), and 26% consciously choose not to use MFA despite knowing how (up from 22% in 2023). This represents a fundamental shift from 'I can't use this' to 'I don't need this'.

The motivational crisis is even more pronounced in phishing reporting. Each year, the primary barrier was the belief that reporting doesn't make a difference. This view increased from 44% in 2022 to 68% in 2025. Additional motivational barriers add to this skepticism: 64% (in 2025, up from 33% in 2022) don't believe reporting stops spam, 60% (in 2025, up from 28% in 2022) don't trust the reporting process, and 50% (in 2025, up from 30% in 2022) see no personal benefits or any negative consequences from not reporting. These beliefs suggest people no longer expect their actions to make a difference. Social cognitive theory[34] tells us how that belief is crucial for keeping any behavior going.

---

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

32 West, R. (2008). The psychology of security. *Communications of the ACM, 51*(4), 34-40.

33 Kahneman, D., & Tversky, A. (2013). Prospect theory: An analysis of decision under risk. In *Handbook of the fundamentals of financial decision making: Part I* (pp. 99-127).

34 Bandura, A. (1986). *Social foundations of thought and action: A social cognitive theory.* Prentice-Hall.

This pattern aligns with what we see in research[35] on security fatigue and learned helplessness. When people take protective steps again and again without tangible results or feedback, their motivation fades, even if they started out skilled and committed.

Beyond these beliefs, the data reveal a troubling rise in security overconfidence, a form of optimism bias where people think their current protections are stronger than they are. The primary reason for not using MFA in 2024 (28%) and 2025 was the belief that passwords alone are sufficient – this demonstrates the overconfidence bias[36] at play, where people see the general risk but underestimate their own exposure. This cognitive bias is particularly dangerous because it can push people to talk themselves into unsafe choices[37]. For example, people who find MFA inconvenient could justify non-adoption by exaggerating password strength instead of taking an honest look at their real risk.

And finally, when the perceived costs (in time, effort, and cognitive burden) consistently feel higher than the visible benefits, people make what feel like rational decisions to disengage, particularly when they operate under fatalistic beliefs that data loss is inevitable.[38] This is demonstrated by our finding that 34% (in 2025, up from 22% in 2023) believe efforts are pointless because data is already online.

The findings paint a sobering picture: the problem isn't that people don't understand cybersecurity's importance, but that the complexity, cost, and cognitive burden of today's security environment are driving them toward apathy despite positive intentions. Effective interventions need to address all three COM-B components together: building capability through accessible education and intuitive tools, creating opportunity by reducing time and resource barriers, and strengthening motivation by showing visible impact and rebuilding trust in security processes. Without this holistic approach, the gap between awareness and action will continue to widen, leaving users increasingly vulnerable in an escalating threat landscape.

Against this backdrop, five years of data won't solve risk for you, but it does away with some guesswork. It shows you the outlines of how people live, think, and make choices online. And, vitally, where intentions get derailed by reality.

Your security controls don't exist in a vacuum. Our data gives you a clearer view of the context that inevitably affects your controls and interventions.

35 Stanton, B., Theofanos, M. F., Prettyman, S. S., & Furman, S. (2016). Security Fatigue. *IT Professional, 18*(5), 26-32.

36 Alnifie, K. M., & Kim, C. (2023). Appraising the manifestation of optimism bias and its impact on human perception of cyber security: A meta analysis. *Journal of Information Security, 14*(2), 93-110.

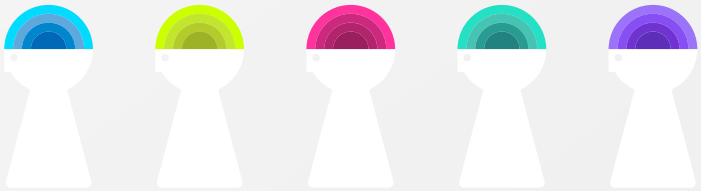
37 Gomez, M. A. (2019). Past behavior and future judgements: seizing and freezing in response to cyber operations. *Journal of Cybersecurity, 5*(1), tyz012.

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

Of course, people's lives will keep on changing, as will threats, as will the tensions between Capability, Opportunity, and Motivation. The real test is in how quickly you're willing to update your assumptions about people. And how committed you are to treating behavior data as a core input to strategy.

So, keep listening, keep measuring, keep adjusting. **Treat your people as partners in risk** rather than problems to be fixed. And everything else in your human risk program can flow from there.

Stick around for the methodology section if that's your speed. But before we go, we want to thank you for spending time with this report, and for the work you already do to make people safer online.



Appendix

Appendix: Methodology

Survey design

The surveys each year 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').

Procedure

A call for participation was placed by the Toluna[39] platform for the United States, the United Kingdom, Germany, Australia, India, Brazil, and Mexico, between 2021 and 2025. In 2022, for Canada, the call for participation was carried out by Elemental Data Collection[40]. In 2023 and 2024, for New Zealand, the call for participation was carried out by the CERT NZ[41].

Participants responded to the survey in their preferred language according to country (e.g., German for Germany).

Participants who completed the survey were compensated for their time. They were briefed about the survey, and their informed consent was required before they could begin.

Participants were told not to reveal any personal information in their responses and that their responses would be anonymized. It was stressed that participation was entirely voluntary, and respondents had the right to withdraw whenever they pleased. The Science and Research (S&R) team at CybSafe did not collect any personally identifiable information.

Data collection was conducted on the following dates:

- 2021: August 10 - August 18.
- 2022: June 29 - July 19.
- 2023: April 13 - April 27.
- 2024: March 6 - April 22.
- 2025: May 2 - May 27.

The survey was designed to be completed in under 30 minutes.

---

39 https://uk.toluna.com

40 https://elementaldci.com

41 https://www.cert.govt.nz

Sample

Representative samples designed to reflect age and gender in each country were recruited each year. All of the participants were 18 years of age or older, with the average age being:

- 47 years in 2021
- 50 years (SD=10.26) in 2022
- 48 years (SD=17.00)[42] in 2023
- 46 years (SD=16.79) in 2024
- 45 years (SD=17.02) in 2025

Detailed demographic information by country, including gender, age, and employment status, is presented in Table 3.

Table 3. Participant demographics by each year.

Demographic		2021 (N=2000)	2022 (N=3000)	2023 (N=6064)	2024 (N=7012)	2025 (N=7000)
Age	Gen Z (1997-2012)	241 12%	285 9.5%	749 13%	1064 15.8%	1480 21.1%
	Millennials (1981-1996)	572 29%	810 27%	1589 27.7%	2011 29.8%	2112 30.2%
	Gen X (1965-1980)	513 26%	798 26.6%	1605 27.9%	1911 28.3%	1869 26.7%
	Baby Boomers (1946-1964)	585 29%	964 32.1%	1689 29.4%	1663 24.6%	1436 20.5%
	Silent Generation (1928-1945)	89 4%	122 4.1%	116 2%	100 1.5%	103 1.5%
	Prefer not to say	N/A	21 0.7%	N/A	N/A	N/A
Gender	Female	1087 54%	1525 50.8%	3155 52.0%	3501 49.9%	3454 49.3%
	Male	885 44%	1466 48.9%	2888 47.6%	3509 50%	3546 50.7%
	Non-binary / Third gender	17 1%	0 0%	17 0.3%	2 0.1%	0 0%
	Prefer not to say	11 1%	9 0.3%	4 0.1%	0 0%	0 0%
Employment status	Employed	1079 54%	1729 57.6%	3908 64.4%	4586 65.4%	4379 62.6%
	Full-time	826 41%	1381 46%	3062 50.5%	3522 50.2%	3388 48.4%
	Part-time	253 13%	348 11.6%	846 13.9%	1064 15.2%	991 14.2%
	Students	77 4%	92 3.1%	270 4.5%	346 5%	471 6.7%
	Not working	51 3%	59 2%	157 2.6%	211 3%	295 4.2%
	Working student	26 1%	33 1.1%	113 1.9%	135 2%	176 2.5%
	Retired	434 22%	743 24.8%	1328 21.9%	1327 18.9%	1319 18.8%
	Don't work or study outside home[43]	410 20%	436 14.5%	558 9.2%	753 10.7%	831 11.9%

Data quality

The survey providers included measures to ensure data quality. If a participant's response was determined to be of a 'low' quality (e.g., incomplete responses), they were excluded and replaced by another participant to meet the required sample size.

Data analysis

Each year, descriptive statistical analyses were conducted on all Likert-based questions, providing frequencies (N) and proportions (%). Proportions were visualized in various data visualization techniques, including tables and charts.

For this five-year comparison report, frequencies (N) and proportions (%) were gathered from each year where three or more years of data were available. We ensured that the survey question or option wording had not been significantly altered to maintain validity.

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

Previous Oh, Behave! reports

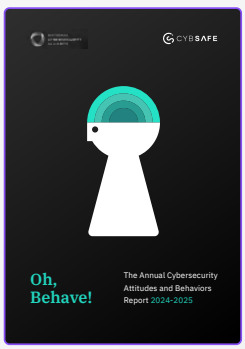
The full historical series of Oh, Behave! reports (2021 - 2025), which form the basis for the year-on-year analysis, can be accessed below:

➡️ 2021

➡️ 2022

➡️ 2023

➡️ 2024



➡️ 2025

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 a cybersecurity software platform transforming how organizations manage human risk in the AI era. It integrates with your existing tools and uses behavioral data and intelligent automation to surface real risk signals, deliver science-backed interventions, and track behavior change, which all help to reduce the likelihood and impact of cyber incidents before they disrupt the business.

At the heart of CybSafe's behavioral security platform is SebDB – the world's cybersecurity behavior database – offering insight into every security behavior capable of minimizing human cyber risk.

Authors

Dr. Suzie Dobrontei, CPsychol, Behavioral Scientist, CybSafe

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

Contact us: research@cybsafe.com

Expert contributors

Oz Alashe MBE, CEO & Founder, CybSafe

Lisa Plaggemier, Executive Director, The National Cybersecurity Alliance

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

Acknowledgments

Famia Humayun

Thalia Saghbini

Cliff Steinhauer, The National Cybersecurity Alliance

Max McKenna, The National Cybersecurity Alliance

Adam Brett, Senior Account Executive, ModOp

Patrice Gamble, Account Director, ModOp

Alice Cooke, Copywriter, CybSafe

Veronika Bondareva, Head of Creative & Design, CybSafe