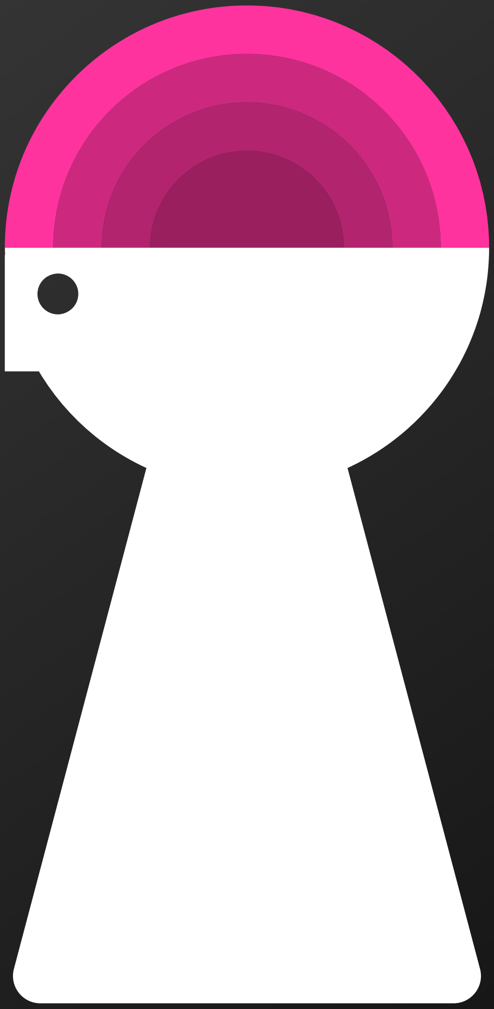
NATIONAL CYBERSECURITY ALLIANCE

CYBSAFE



Oh, Behave!

The Annual Cybersecurity Attitudes and Behaviors Report 2023

TABLE OF CONTENTS

Hope *(is not a strategy)*

Welcome to the 2023 Annual Cybersecurity Attitudes and Behaviors Report. Or, as it's known 'round these parts, Oh, Behave! ✷

It's early September. As we pen the final parts to this year's behemoth, summer is a sizzlin', and good feelings are in the air.

So break out the bunting, because this year marks the 20th anniversary of Cybersecurity Awareness Month. It happens every October, and it has the laudable goal of educating and inspiring behavior change.

Since the inception of Cybersecurity Awareness Month, the threats we face have evolved, significantly. The importance of cybersecurity has never been greater.

There's no doubt the security professionals of 2003 knew people's behavior was important. But there was a disconnect when it came to the human factors that contribute to security breaches and incidents. The belief went like this: If we just made people aware of the risks, they'll start behaving more securely.

That was wrong. Now we know better. And when you know better, you do better.

Today, as security professionals with a keen eye on the evidence, we know awareness is not enough. It's not enough to tell people about risks, and hope they remember what they need to do at the point of action. Or, indeed, hope they care enough to act in the first place!

From the risk-takers to the rule-followers, we need to understand why people behave the way they do, and what motivates them to change their behavior.

Behavioral science plays a vital role in strengthening cybersecurity.

That's why we created this report. Again.

Double the fun

This year, we got ambitious. We surveyed over 6,000 people across the United States, Canada, the United Kingdom, Germany, France, and New Zealand to get a better understanding of our security behaviors and attitudes. Double the participants. Double the countries. Double the fun!

We asked people about their knowledge of cybersecurity risks, their security best practices, and the challenges they face in staying safe online.

The findings are eye-opening, to say the least. They show, even though people are becoming more aware of risks, they're not always taking the necessary steps to protect themselves.

For example, only 60 percent of people use strong passwords, and only 40 percent use multi-factor authentication. And even though most people know about phishing scams, they're still falling for them.

Full of BS*

The good news is there are things we can do to improve people's security behavior. This report provides a number of recommendations for organizations and individuals.

We know changing people's behavior isn't easy. But if we want to make the digital world a safer place, it is essential.

We're particularly excited about this year's report because it shines a spotlight on the workforce. Cybercriminals know if they want to target an organization, they need to target its people. We believe this report will help organizations to better protect themselves and their people.

We hope you enjoy reading this report as much as we enjoyed producing it.

Grab your lab coat. You've got a date with behavioral science.

Oz & Lisa

Oz Alashe, MBE
CEO & Founder, CybSafe

Lisa Plaggemier
Executive Director, The National Cybersecurity Alliance

* Behavioral science.

Report aim & structure

It’s all about you, the people! Specifically, how you feel and how you act when it comes to cybersecurity.

Tech ninjas. Click-curious newbies. Everybody in between. Our third Cybersecurity Attitudes and Behaviors report uncovers the nitty gritty of how people engage with the digital realm.

That’s the general public, and the workforce too. That’s right, we’re no slouches.

Our goal? To paint a vibrant picture of the cybersecurity behaviors and attitudes that shape our digital existence.

You’re looking at a comprehensive, international snapshot across representative global samples. This year, it’s never been truer: there’s something for everyone.

But we’re not just here to chat. We’ve been busy building on the last two years’ findings. We’ve really gotten into it with five game-changing security behaviors that keep the virtual world spinning:

1. Ensuring password hygiene:
    - Password creation habits (i.e., using strong and separate passwords)
    - Frequency of changing passwords
    - Password management techniques
2. Using Multi-Factor Authentication (MFA)
3. Installing the latest device updates
4. Checking emails for signs of phishing and reporting them onward
5. Backing up data

Up close and personal

We’ve got an exciting journey ahead of us. Zooming in on people’s access to cybersecurity training. Dissecting how the media/news coverage influences cybersecurity perceptions. Getting up close and personal with people’s experiences of cybercrime victimization. And how people report incidents—if indeed they do.

Psst! Heads-up, we've organized the results into themes:

- How deep is people's online presence?
- What do people *really* think about cybersecurity? The good, the bad, the need-to-know truths.
- Who's got your back at work and at home?
- Who's got access to training, and how do people use it?
- What types of cybercrimes do people encounter?
- How people like you—yes, you—engage with those five key security behaviors.

What's that? You're curious about our behind-the-scenes magic? Of course you are. In the appendices we:

- unveil our research methodology,
- introduce you to the diverse participant pool, and
- even toss in the country-specific numbers.

Pretty sweet, no?

Feverishly fresh!

It's our third report in the series, so we're really hitting our stride. Our research design and data collection was already on point (head to Appendix A to learn more). But we've switched some things up to deliver even more illumination and insight.

Here's what's new:

- **Double the fun:** We doubled the sample size from 3000 to over 6000 people (6,064, to be precise).
- **Going global:** New countries = new perspectives. Germany, France, and New Zealand have entered the party. They join the United States (US), Canada, and the United Kingdom (UK).
- **Strategic targeting:** We wanted to shine a spotlight on the general public *and* the global workforce. This year's sample boasts a whopping 66 percent of employed participants. Making the findings super-useful for organizations.
- **Fresh questions:** We asked new questions about training engagement and preferences (e.g., delivery style), the media/news impact, and a bunch of password-related behaviors.
- **Question makeover:** We reworded questions and made multi-choice options sleeker. Why? Because making sure participants have a smooth, clear survey experience leads to better data. And because—go figure—not everyone are cyber geeks like us, we've added some examples and key terms to keep everyone on the same page.
- **Qualitative questions:** The survey remains mostly multiple-choice. But this year participants could also share their thoughts in their own words through our new qualitative questions. Figuring out people's cybersecurity feelings means letting them speak from the heart.

Key terms

We get it—these report thingamajigs often come with a side of brain cramps.

Fret not. Here's the lowdown on the lingo.

The key terms we've used throughout the report are:

(Security) attitude: A psychological disposition we have towards making an evaluative judgment about security (i.e., the way we think or feel about it). For reporting attitudes, we have used 5- and 10-point Likert scales (e.g., "strongly disagree" to "strongly agree") to examine positive and negative views people hold about particular security topics.

(Security) behaviors: For this report, we have narrowed down our investigation to five security behaviors. These include: password hygiene (password creation, management, and frequency of change), applying MFA, installing the latest updates, checking messages for signs of phishing and reporting them, and backing up data.

Cyberbullying: Bullying is unwanted, aggressive behavior that involves a real or perceived power imbalance. This power imbalance can be physical. It can also revolve around popularity or the bully having access to embarrassing information about the victim. Generally, bullying is a repeated behavior, or it has the potential to be repeated. Cyberbullying, then, is when these bullying behaviors occur online, either through messaging, social media, or other digital channels.

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

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

Identity theft: When a cybercriminal steals someone's personal information and uses it to assume their identity. This can involve the criminal applying for credit and loans, or even filing taxes using the victim's identity, potentially damaging their credit status.

Multi-Factor Authentication (MFA): The process of using two or more pieces of information to log in to an account. This can be a password and code sent to a phone. Also known as Two-Factor Authentication (2FA) and Two-Step Verification (2SV).

Password hygiene: Creating unique and separate passwords for sensitive online accounts, managing passwords using browser or stand-alone applications, and the tactics of changing passwords.

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

Phishing (scams): Cybercriminals trick people into providing information or installing dangerous software to steal money or data from them. This is often done via fake emails that appear to be from trusted senders, encouraging people to click malicious links or open malicious attachments.

Online dating scam: Cybercriminals adopt a fake online identity to create the illusion of a romantic or close relationship to manipulate and/or steal from the victim. They often use highly emotive requests for money, claiming they need emergency medical care or must pay for transport costs to visit the victim if they are overseas.

Sensitive (important) online accounts: Online accounts holding details of identity, address, and bank cards (e.g., payment-related sites, social media accounts, and work accounts).

Vocab session over. Who’s ready for the highlights?

Step this way.

Executive summary

Our online presence is getting swole

We’re frustrated and doubtful about online security

Move over cybersecurity training, nudges are coming

Cybercrime victims are reporting more

Are we behaving?

Executive summary

Our online presence is getting swole

A whopping 93 percent of participants are online at least daily. Just seven percent of people in our sample reported being connected to the Internet less than once a day.

All of us hold at least a few online accounts, across different websites and applications, and some include our sensitive personal information.

But here's the big reveal: It turns out that almost half (47%) of the participants have ten or more sensitive online accounts, like payment-related and primary email accounts. And—get this—15 percent admitted they'd lost count (Figure 1).

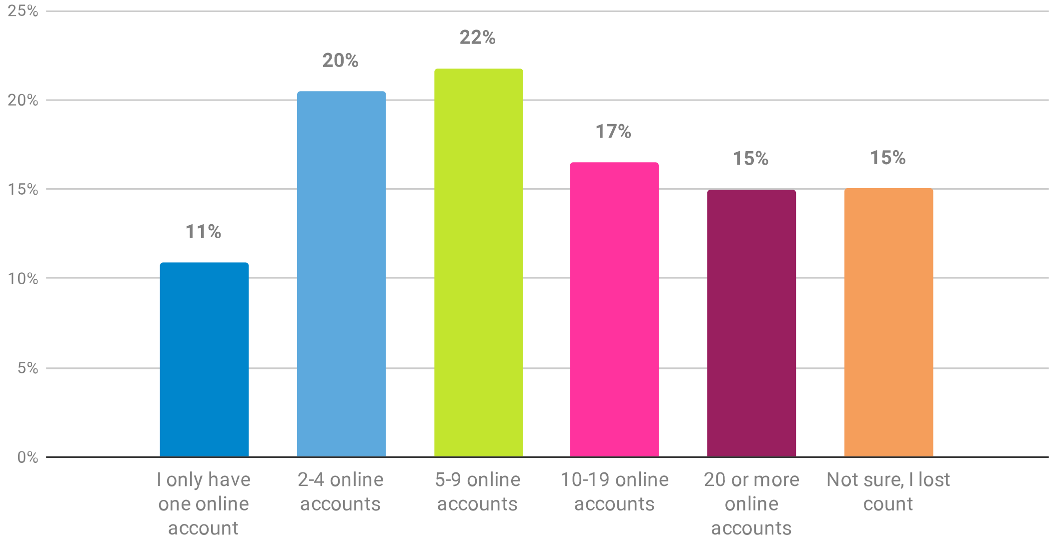


Figure 1. ***"Overall, how many sensitive online accounts that hold personal information do you have?"***

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants: 6064, dates conducted: April 13, 2023 - April 27, 2023.

We’re frustrated and doubtful about online security

Attitudes towards online security remain positive. A solid 84 percent consider staying secure a priority, and 69 percent perceive it as achievable. But not everyone’s having a chill time. A sizable 39 percent of participants felt frustrated, and 37 percent were intimidated by staying secure online (Figure 2).

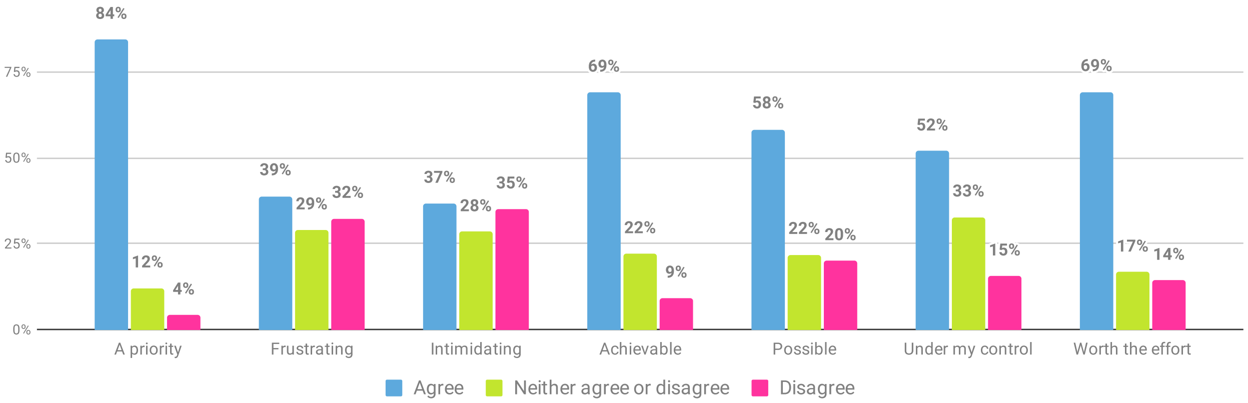


Figure 2. ***“I feel that staying secure online is…”***

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants: 6064, dates conducted: April 13, 2023 - April 27, 2023.

One in three (32%) often feel overwhelmed by cybersecurity information, scaling down their online actions as a result. Plus, the cost of taking protective action online doesn’t come cheap, according to almost half of us (49%).

A cool 69 percent of participants thought staying secure online is worth the effort. But the younger generations (21% of Gen Z and 23% of Millennials) are skeptical about the return on investment. They were more than twice as likely as Baby Boomers (6%) and the Silent Generation (9%) to doubt online security is worth the effort (Figure 3).

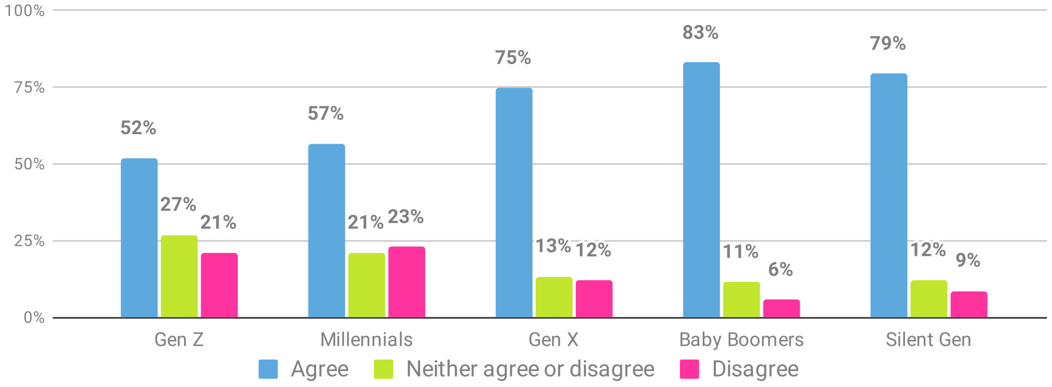


Figure 3. Participants’ levels of agreement when answering *“I feel that staying secure online is worth the effort”* by generation.

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants with generation information: 5748, dates conducted: April 13, 2023 - April 27, 2023.

Over half of the participants (56%) said the news motivates them to take protective security actions. And 51 percent find the media/news coverage helps them stay informed about online security (Figure 4). But it's not all sunshine—44 percent of the participants said the media evokes fear, and 42 percent felt it overcomplicates online security.

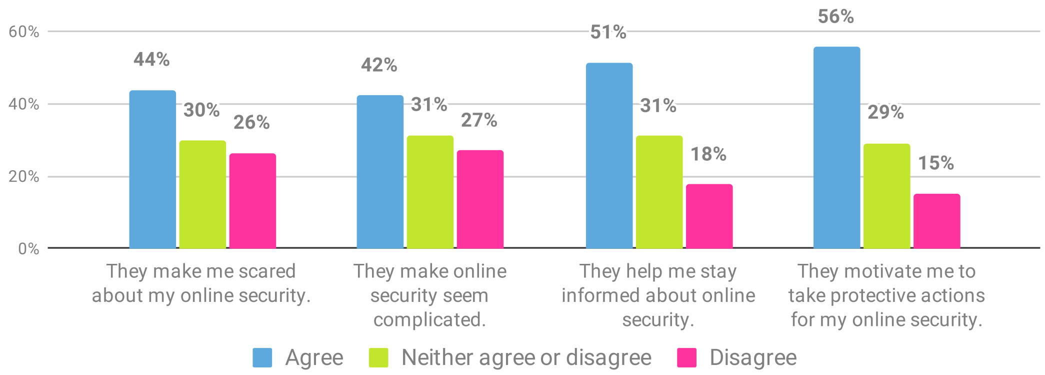


Figure 4. ***"What impact does the media/news have on your views towards online security?"***

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants: 6064, dates conducted: April 13, 2023 - April 27, 2023.

Move over cybersecurity training, nudges are coming

Access to training

Let's turn our attention to the training scene. First up, just over a quarter of participants (26%) reported having access to, and taking advantage of, cybersecurity training. Meanwhile, an eyebrow-raising two-thirds (64%) noted they had no access to training whatsoever (Figure 5).

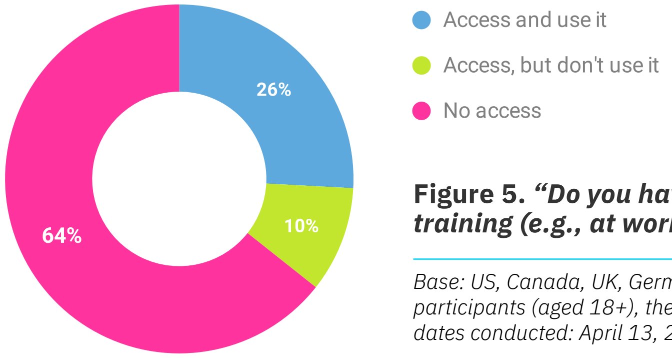


Figure 5. ***"Do you have access to cybersecurity training (e.g., at work, school, or library)?"***

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants: 6064, dates conducted: April 13, 2023 - April 27, 2023.

Hold up, who's getting the training? Mainly, it's people in employment (47%) or those studying (49%). They had better training access than retirees (8%) or people not in active employment or studying (15%, Figure 6).

But get this: Even among the employed, more than half (53%) are out in the cold when it comes to training access.

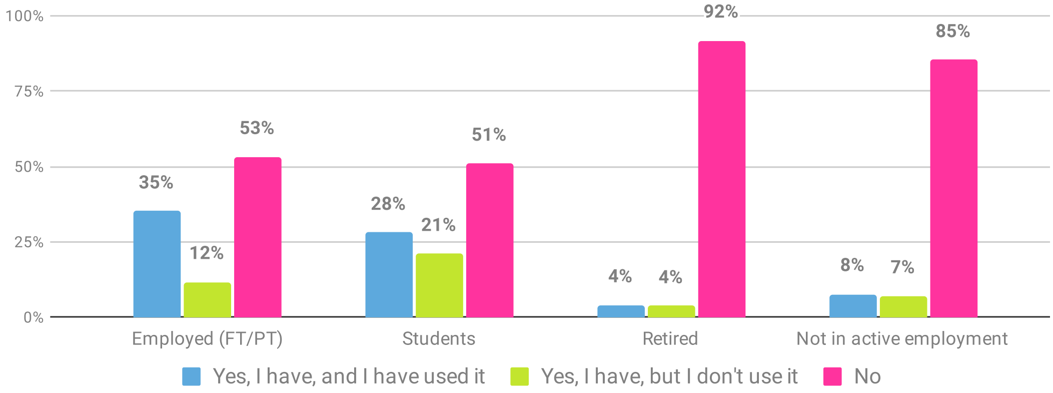


Figure 6. *"Do you have access to cybersecurity training (e.g., at work, school, or library)?"* by employment status.

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants: 6064, dates conducted: April 13, 2023 - April 27, 2023.

Wondering how people like to be shown the security ropes? When asked about their preference for learning about cybersecurity topics, almost half (47%) of employed participants favored online training courses over in-person training (24%). On the flip side, preference towards nudges and alerts is growing, with nearly a fifth (19%) preferring to receive just-in-time alerts and notifications.

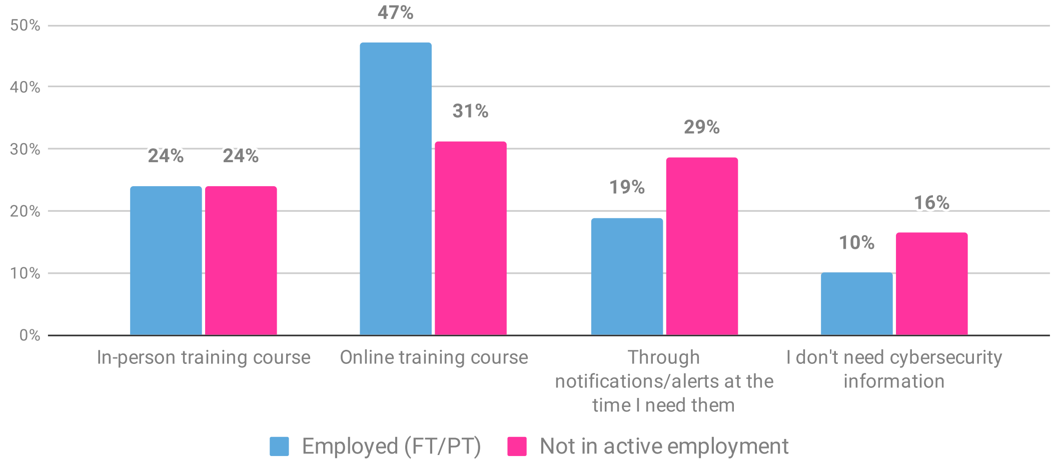


Figure 7. *"How would you most prefer cybersecurity training to be delivered?"* by employment.

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants: 6064, dates conducted: April 13, 2023 - April 27, 2023.

Cybersecurity training

Does training make a splash? Most people rated cybersecurity training as useful (84%) and engaging (78%), no matter whether they'd done it at home or work.

Seventy-nine percent of participants reported having put the cybersecurity advice into action. Only six percent reported that they didn't change any of their cybersecurity behaviors, and 15 percent believed they were already doing the right things, and therefore didn't need to change their behaviors (Figure 8).

But what did training do for people? Half of the participants (50%) felt they became better at recognizing and reporting phishing messages, 37 percent had started using strong and unique passwords, and a third (34%) had begun using MFA.

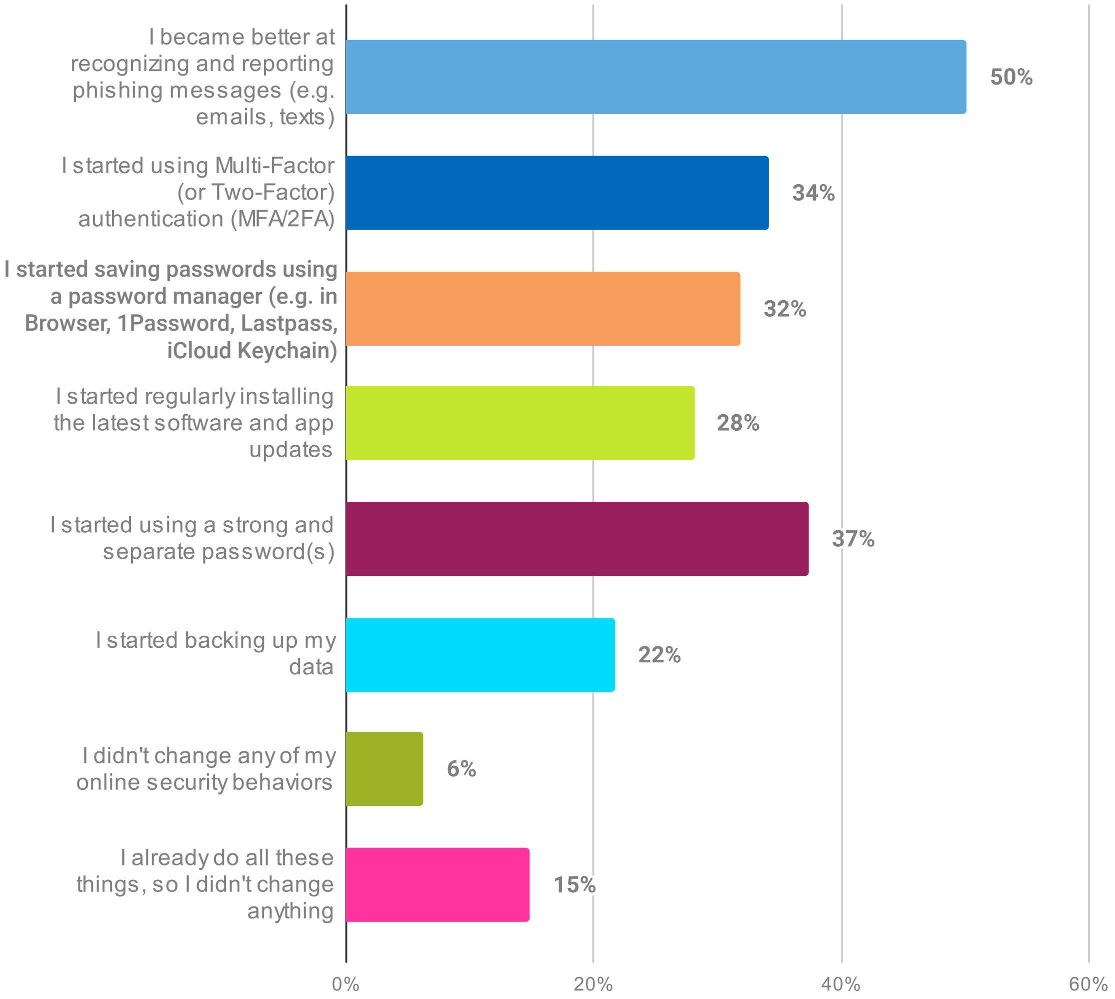


Figure 8. ***"When you attended training course(s), how did it influence your security behaviors?"***

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants who had attended training courses: 1559, dates conducted: April 13, 2023 - April 27, 2023. Note: Multiple-choice question.

Cybercrime reporting is increasing

Who's getting hit, and by which cyber nasties?

Our participants disclosed 2,047 incidents led to losing money or data. Think phishing, identity theft, and online dating scams.

Over a quarter (27%) reported having been a victim of at least one type of cybercrime. The good news is that's a seven percent drop on last year's figures.

Here's the less good news: There was a seven percent increase in the number of people who feel they may become victims of cybercrime. In fact, half of the participants (50%) thought they were potential targets for cybercriminals (Figure 9).

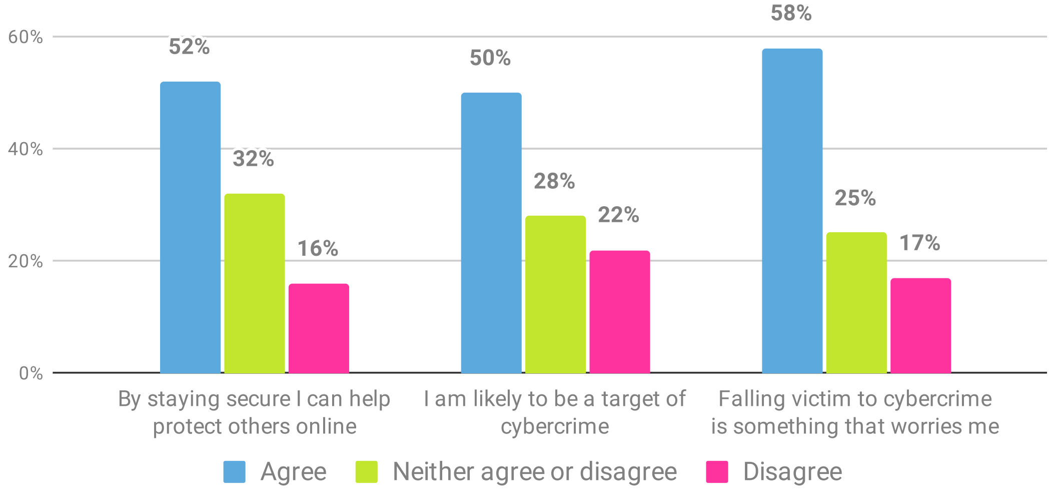


Figure 9. Participants' responses to statements about how staying secure online can help protect others, perceived likelihood of becoming a target of cybercrime, and concerns about falling victim to cybercrime.

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants: 6064, dates conducted: April 13, 2023 - April 27, 2023.

Phishing is the out-and-out star of the shady cybercrime show. Overall, phishing incidents accounted for the highest proportion of total incidents (47%, Figure 10). And, check this out: Online dating scams (27%) took the lead over identity thefts (26%) compared to last year.

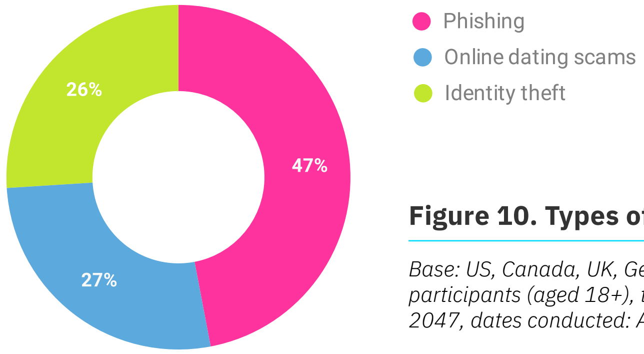


Figure 10. Types of cybercrime incidents.

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of cybercrime incidents 2047, dates conducted: April 13, 2023 - April 27, 2023.

Millennials, looks like the cybercrime spotlight's on you. You're leading the pack with incidents (Figure 11). Specifically, online dating scams (44%) were the apple of your eye, followed by phishing (36%) and identity thefts (37%). Putting aside the Silent Generation due to their small sample size, Gen Zs and Baby Boomers reported the fewest identity thefts (15% and 17% respectively).

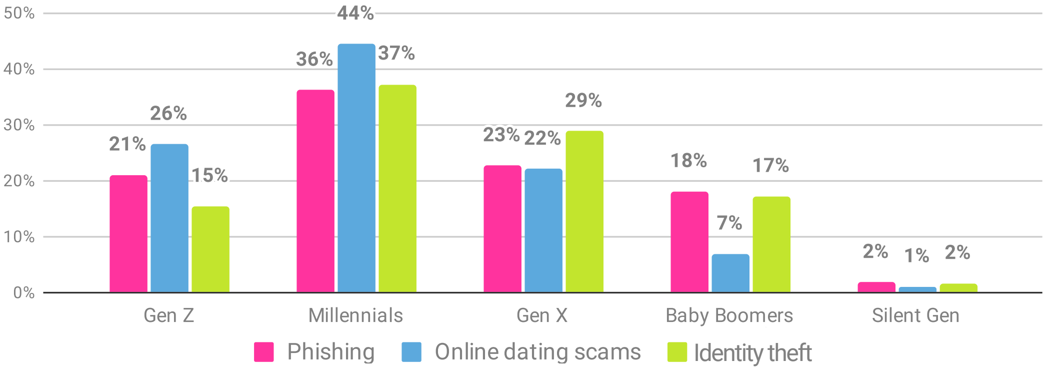


Figure 11. Cybercrime incidents by generations.

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of cybercrime victims: Phishing, 911; Online dating scam, 541; Identity theft, 508 (excluding any cybercrime incidents noted by 316 participants from New Zealand, who didn't provide their age), dates conducted: April 13, 2023 - April 27, 2023.

But now for some cheering news—yes, even if you're a romantically inclined Millennial.

Most folks (88%) reported their cybercrime experiences to someone. Incident reporting rates were favorable for all crime types. Only a smidge of incidents which led to data or money loss went unreported: 14 percent of phishing, 16 percent of online dating scams, and eight percent of identity thefts (Figure 12).

When it came to reporting, the type of crime made a difference. Fifty-nine percent of phishing victims reported the incident to their bank or credit card company, and 54 percent of identity theft, and 42 percent of online dating scams did likewise. This is encouraging.

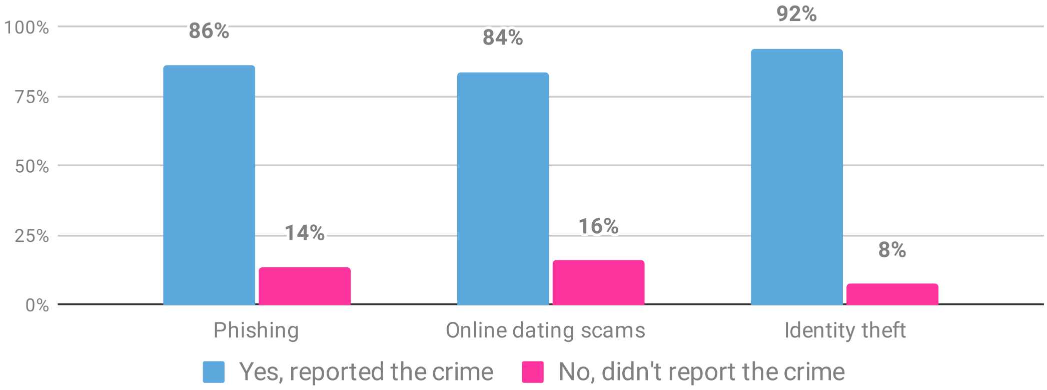


Figure 12. Crime reporting frequency by crime type.

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of cybercrime victims: Phishing, 961; Online dating scam, 555; Identity theft, 531, dates conducted: April 13, 2023 - April 27, 2023.

Are we behaving?

We wouldn't have enjoyed our summer as much if we hadn't done a deep dive on the nitty-gritty of behavior. Specifically those five key behaviors that spell good cybersecurity.

> Need a reminder? We've got you:
> - Ensuring good password hygiene
> - Using MFA
> - Installing the latest device updates
> - Checking messages for signs of phishing and reporting them
> - Backing up data

Password hygiene

We peeled back the layers of password hygiene through its three sub-behaviors: frequency of changing passwords, creation of strong and separate passwords, and password management strategies.

While NIST guidelines[1] have ditched the requirement to change passwords periodically, some people and organizations still think this is the gold standard for good password hygiene. However, over a third (34%) said they only change their sensitive online account passwords if they have to. Meanwhile, 31 percent change theirs every few months.

Almost half (48%) of those who changed their passwords mentioned they used their own techniques for creating new passwords. This technique was prevalent with older generations (e.g., 62% of Baby Boomers).

How about the more fresh-of-face, then? Well, over a quarter of Gen Zs (26%) opted for passwords suggested by websites or apps. However, younger generations dabbled more with risky password practices. Plenty (37% of Gen Z and 44% of Millennials) admitted to only updating a few characters or a couple of words in their passwords compared to older generations (27% of Baby Boomers and 26% of Silent Generation, Figure 13).

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

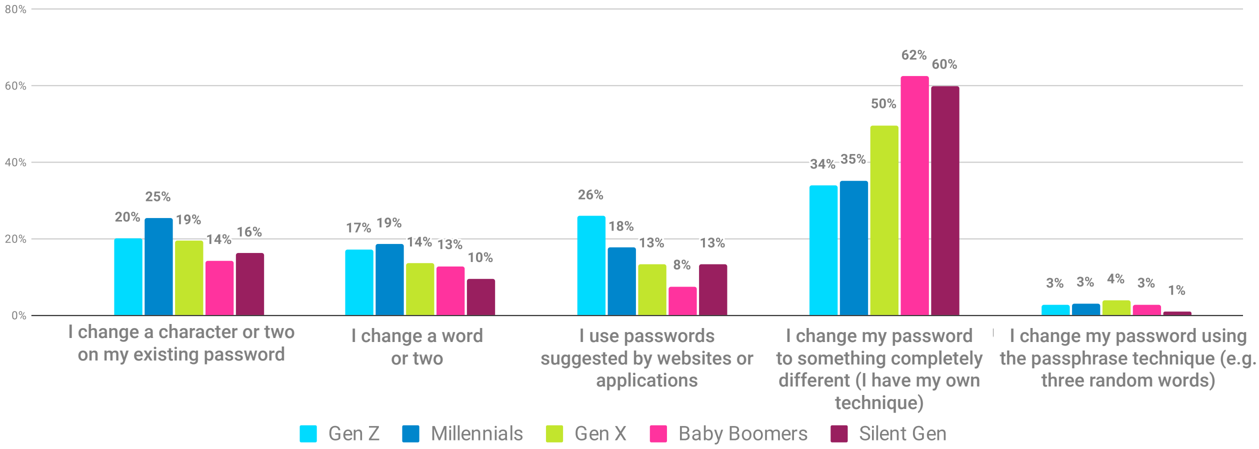


Figure 13. *"What action do you most often take when changing your password(s)?"* by generation

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants with generation information and excluding those who 'never' or 'less than yearly' change their passwords: 4983, dates conducted: April 13, 2023 - April 27, 2023.

Next up! Eyes on the size. According to the national guidelines the recommended standards for password length is more than 12 characters or using a string of three or more words (e.g., NCA[2], NCSC's CyberAware[3], Get Cyber Safe[4] and CERT NZ[5])

Forty-six percent of participants create passwords nine to 11 characters long. Almost a third (30%) go shorter than that though. Oh, and here's something really interesting: Older folks tend to go briefer (32% of Baby Boomers and 36% of Silent Generation), while younger generations lean a tad longer (Figure 14).

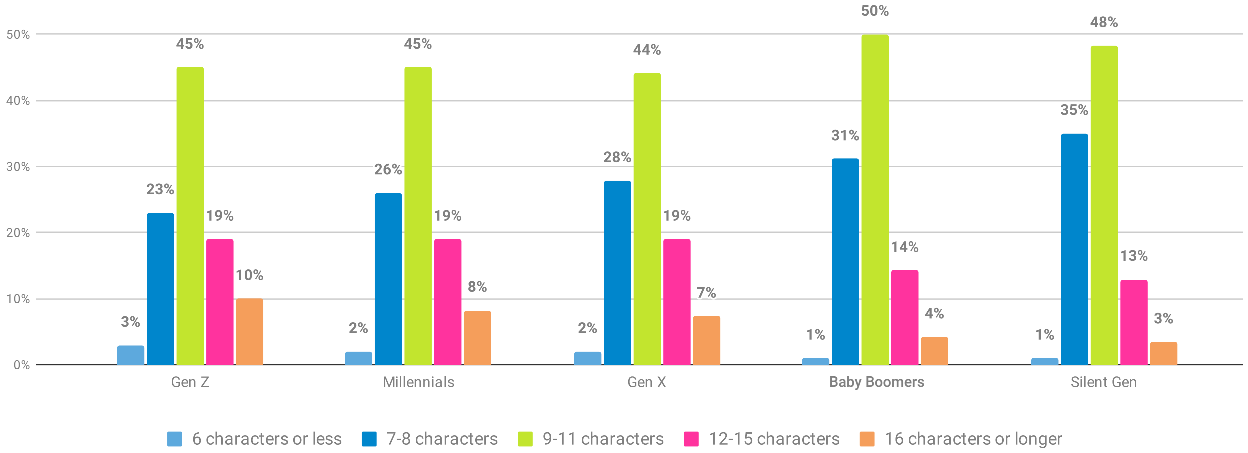


Figure 14. *"How long are the password(s) you usually create?"* by generation

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants with generation information: 5748, dates conducted: April 13, 2023 - April 27, 2023.

[2] https://staysafeonline.org/online-safety-privacy-basics/passwords-securing-accounts/
[3] https://www.ncsc.gov.uk/blog-post/the-logic-behind-three-random-words
[4] https://www.getcybersafe.gc.ca/en/secure-your-accounts/passphrases-passwords-and-pins
[5] https://www.cert.govt.nz/individuals/guides/how-to-create-a-good-password/

Despite creating long passwords, over a third (34%) resort to using a single dictionary word or someone's name, simply throwing in a few numbers and/or symbols for good measure.

The majority (67%) rock separate passwords for their important online accounts either 'all of the time' or 'the majority of the time'. A third (33%) were more laid back, juggling fewer passwords for their important online accounts (Figure 15).

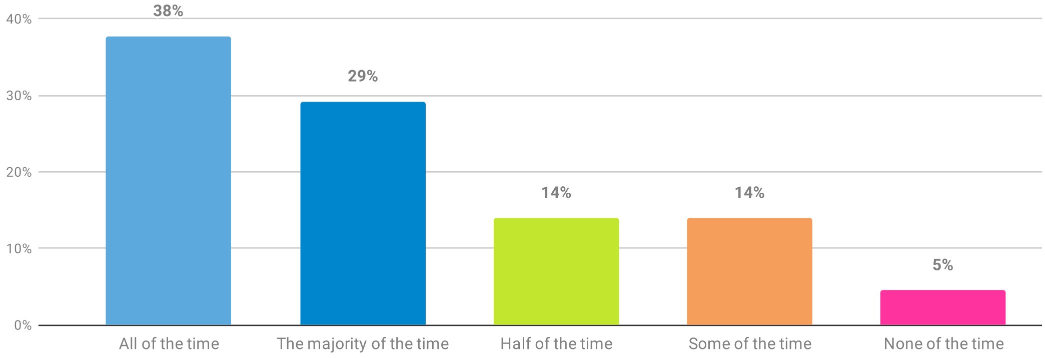


Figure 15. ***"How often do you use unique passwords for your important online accounts*** **(e.g., emails, social media, payment-related sites)?"**

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants: 6064, dates conducted: April 13, 2023 - April 27, 2023.

Managing passwords

Hold onto your hats for this one—over half (56%) have never used a password manager. But 31 percent are giving it a go. The hottest password wrangling technique? Writing passwords into a notebook takes the cake (31%). One in four of us are memory machines: A quarter (24%) say they remember their passwords without storing or writing them anywhere (Figure 16). Some folks even rely on resetting their password each time they login as opposed to remembering it (3%)!

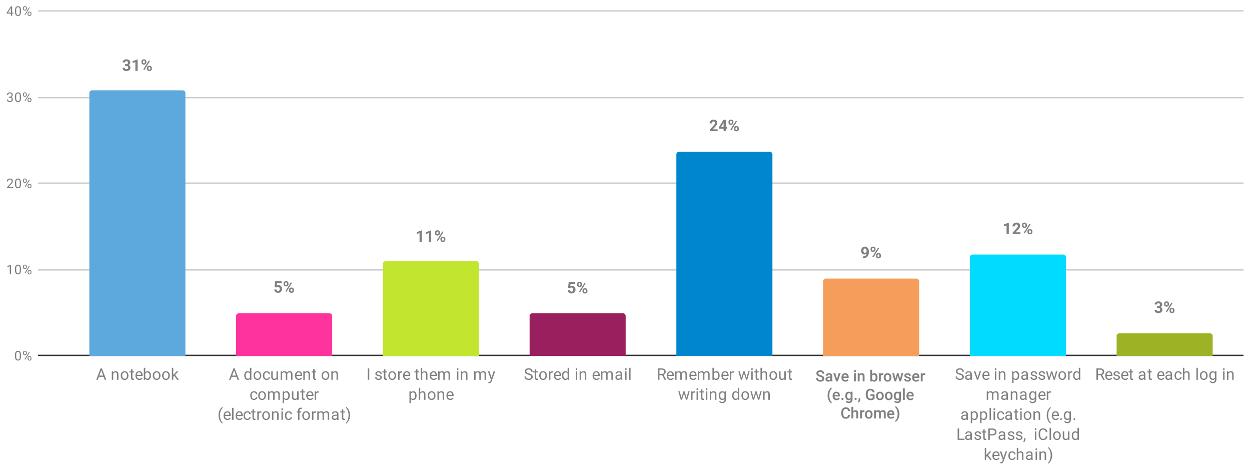


Figure 16. Preferred password management strategies.

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants with multiple passwords: 5403, dates conducted: April 13, 2023 - April 27, 2023.

For those who use password managers, there's an even split between using a free stand-alone password manager (38%) or an internet browser (39%). Less than a quarter (23%) mentioned paying for a stand-alone password manager.

Applying Multi-Factor Authentication (MFA)

Almost a third (30%) of us have (still) never heard of MFA.

The generation gap seen in previous reports is alive and well. A majority of Gen Z (77%) and Millennials (77%) had come across MFA before (Figure 17). However, a sizable chunk of older generations remain in the dark about MFA (37% of Baby Boomers and 41% of Silent Generation never having heard of it).

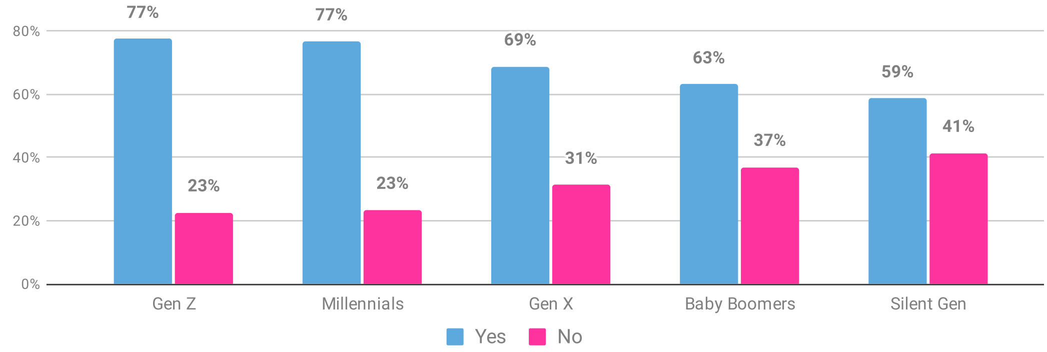


Figure 17. *"Have you ever heard of Multi-Factor Authentication (MFA)? Also known as Two-Factor or Two-Step Verification"* by generations.

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants with generation information: 5748, dates conducted: April 13, 2023 - April 27, 2023.

Installing software updates and backing up data

Sixty-five percent of us know the drill when it comes to keeping devices updated. And 60 percent noted they either 'always' or 'very often' update their devices when notified about available updates (Figure 18).

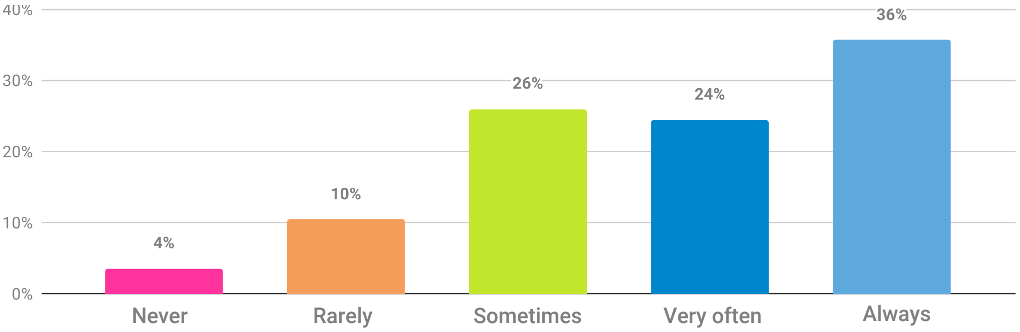


Figure 18. *"How often do you install the latest software or application updates to your devices when notified that they are available?"*

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants: 6064, dates conducted: April 13, 2023 - April 27, 2023.

A close-up on back-ups: Fifty-six percent are in the know and on the case when it comes to backing up their data. A solid 42 percent said they perform frequent backups (i.e., 'very often' or 'always'), but over a quarter (26%) stated they 'never', 'rarely' do so, or they don't have the know-how (Figure 19).

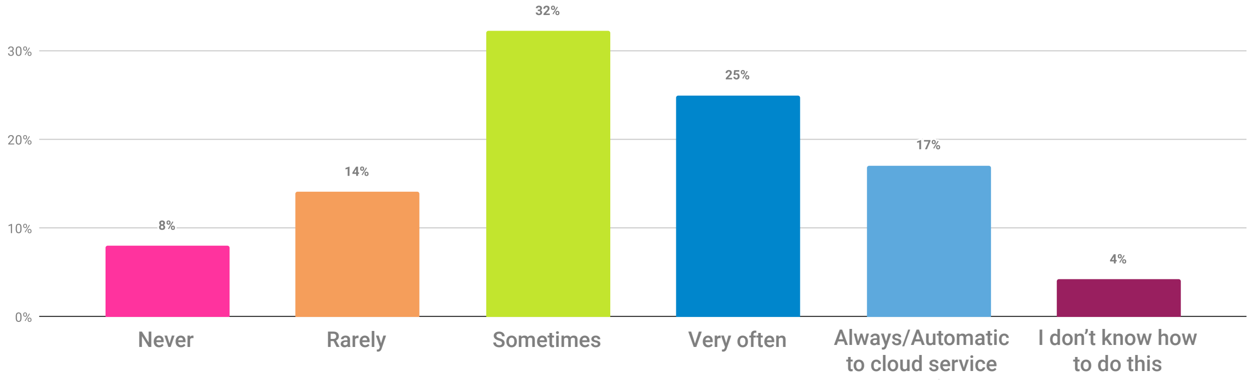


Figure 19. *"How often do you backup your most important data?"*

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants: 6064, dates conducted: April 13, 2023 - April 27, 2023.

Recognizing and reporting phishing messages

A hefty 63 percent rated their phish-spotting skills. However, over a quarter either didn't know how to identify (18%) or didn't know what phishing scams were (8%). What's more, 67 percent reported they 'very often' or 'always' check whether messages are genuine before clicking any links or responding to them (Figure 20).

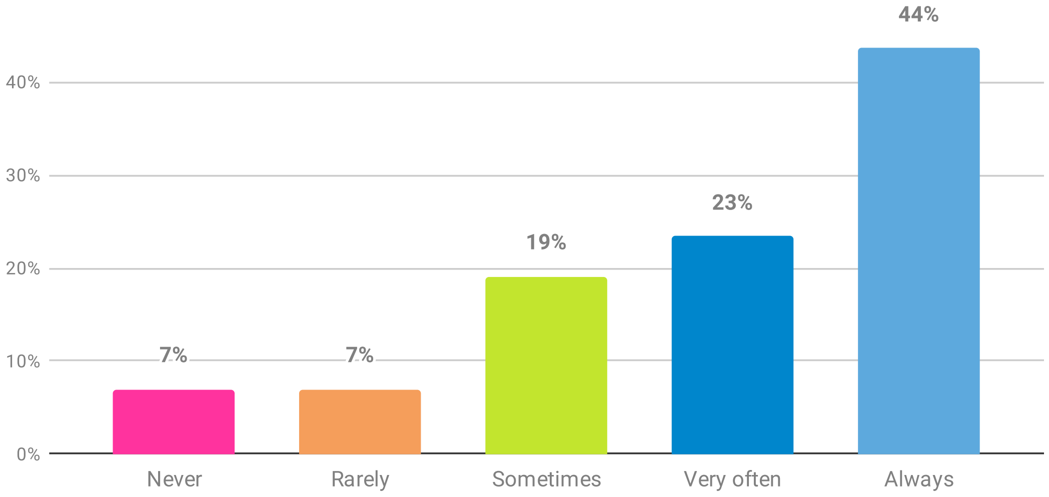


Figure 20. Frequency of checking messages for signs of phishing before taking action.

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants: 6064, dates conducted: April 13, 2023 - April 27, 2023.

Spotting's all well and good. But how about reporting phishing messages? Forty-four percent of participants said they're all in, hitting that 'spam' or 'report phishing' button 'very often' or 'always' (Figure 21). Conversely, a third of us (33%) either lacked the know-how, 'never', or 'rarely' reported phishing.

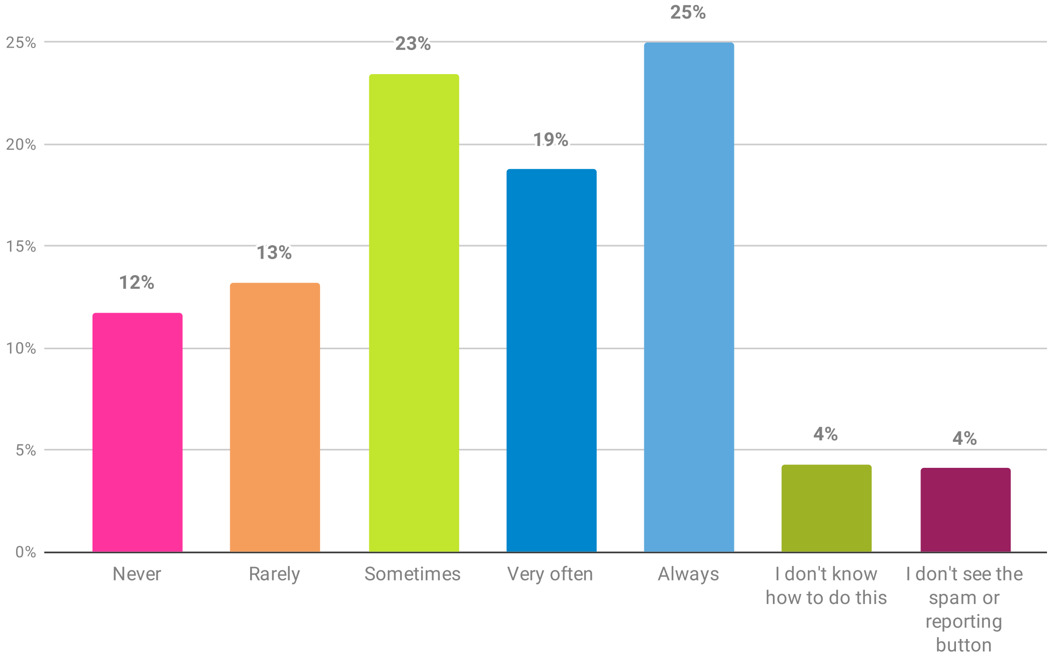


Figure 21. ***"How often do you report phishing messages using the 'spam' or 'report phishing' button?"***

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants: 6064, dates conducted: April 13, 2023 - April 27, 2023.

There you have it, a tour of the major landmarks of what people think and do when it comes to cybersecurity.

The adventure's just beginning, though. Join us as we get our teeth into the truth, bit by bit.

The main findings

Our online presence

Online security and reliance on others

General attitudes to online security

Cybersecurity responsibility

Cybersecurity training

Cybercrime victimization

Cybersecurity behaviors and practices

The main findings

Our trip into the ever-so-serious realm of research began in April 2023. We ran our third survey online between April 13th and April 27th.

Representative samples—meticulously matched in terms of age and gender—were obtained from the United States, Canada, the United Kingdom, France, Germany, and New Zealand. Toluna[6] ran the survey in every corner except for New Zealand, where CERT NZ[7] handled the data collection. A whopping six thousand and sixty-four participants generously shared their thoughts.

Sorry, kids! This was all about the grown-ups. We surveyed the adult population (18+), with the average age being 48 years (SD=17.00)[8]. Sixty-six percent of the participants stated they were in either full- or part-time employment. As per the previous year, we explored the sample population and delved into differences between age groups.

Age group % within country of residence	United States (N=1000)	Canada (N=1000)	United Kingdom (N=1000)	Germany (N=1000)	France (N=1000)	New Zealand (N=1064)	Total (N=6064)
Gen Z (18-26)	159 15.9%	122 12.2%	135 13.5%	107 10.7%	130 13.0%	96 9.0%	749 13.0%
Millennials (27-42)	283 28.3%	278 27.8%	278 27.8%	245 24.5%	246 24.6%	259 24.3%	1589 27.7%
Gen X (43-58)	268 26.8%	268 26.8%	285 28.5%	287 28.7%	307 30.7%	190 17.9%	1605 27.9%
Baby Boomers (59-77)	249 24.9%	301 30.1%	282 28.2%	344 34.4%	310 31.0%	203 15.9%	1689 29.4%
Silent Generation (78+)	41 4.1%	31 3.1%	20 2.0%	17 1.7%	7 0.7%	0 0.0%	116 2.0%
Inconclusive (age not provided)	0 0.0%	0 0.0%	0 0.0%	0 0.0%	0 0.0%	316[9] 29.7%	316 5.2%

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

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

[7] https://www.cert.govt.nz/

[8] This excludes participants from New Zealand (N=1064), who were asked to use age brackets instead stating their exact age.

[9] New Zealand, who had overlapping age grouping categories were excluded from the generational analysis. Where generational differences are reported in the main findings section, these participants are excluded.

We've shone light on differences related to employment status, where applicable, and for our fellow number nerds we've further analyzed the country differences separately in Appendix B. Table 1 shows the number of participants in each age group and their employment statuses are shown in Figure 22. In fact, we've even given you further participants' demographics in Appendix A. Don't say we never spoil you.

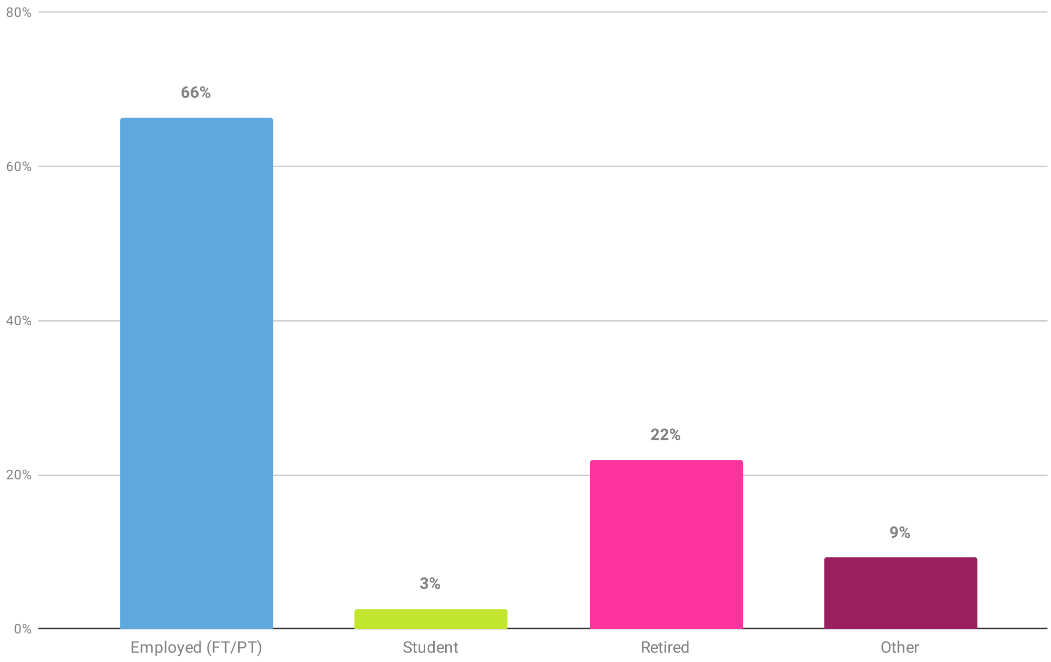


Figure 22. Participants' employment status.

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants: 6064, dates conducted: April 13, 2023 - April 27, 2023.

> **Sixty-six percent of the participants stated they were in either full- or part-time employment**

Our online presence

Let's be clear. We're not talking hit rates and followers. We'll leave that to the influencers.

It turns out most of us are glued to the internet like a barnacle to a rock. All. Day. Long. A full 50 percent of us are always connected. Only seven percent connect less than once a day (e.g., once per week).

Most of us are glued to the internet like a barnacle to a rock

Entirely less shockingly, younger age groups are the most digitally connected. Sixty-nine percent of Gen Z and 64 percent of Millennials are always connected (Figure 23). That's up by five and 16 percent from last year (2022).

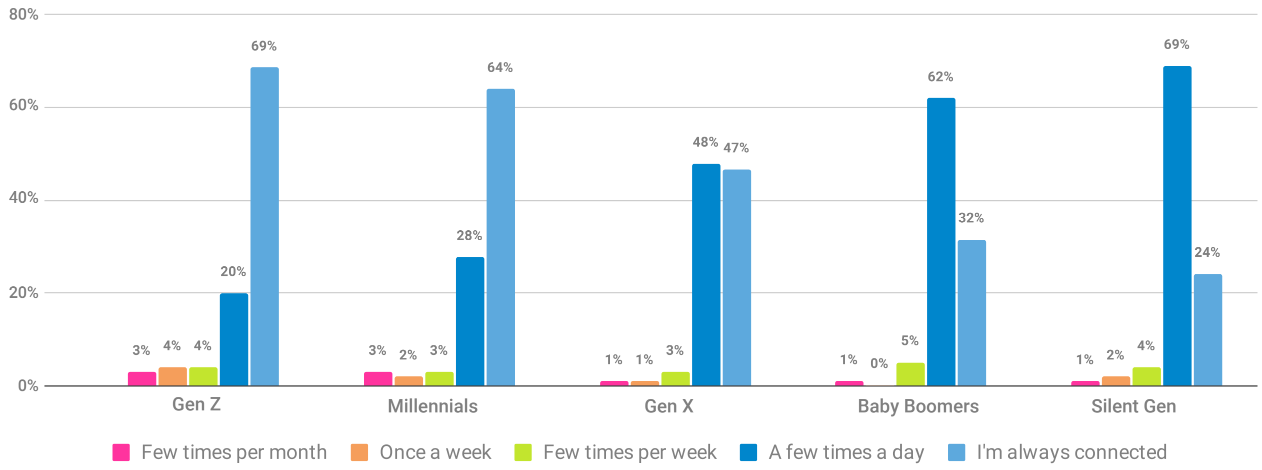


Figure 23. *"How frequently do you use the Internet?"* by generations.

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants: 5748, dates conducted: April 13, 2023 - April 27, 2023.

Right, online accounts. We wanted to know how many online accounts people have containing sensitive information. Almost half (47%) of people have ten or more accounts, including 15 percent confessing that they'd lost count (Figure 24).

Younger generations led the charge here, with Gen Zs (37%) and Millennials (35%) reported having over 20 sensitive online accounts[10]. Meanwhile Baby Boomers (25%) and the Silent Generation (22%) reported having fewer accounts.

[10] This includes those participants who answered 'Not sure, I lost the count'.

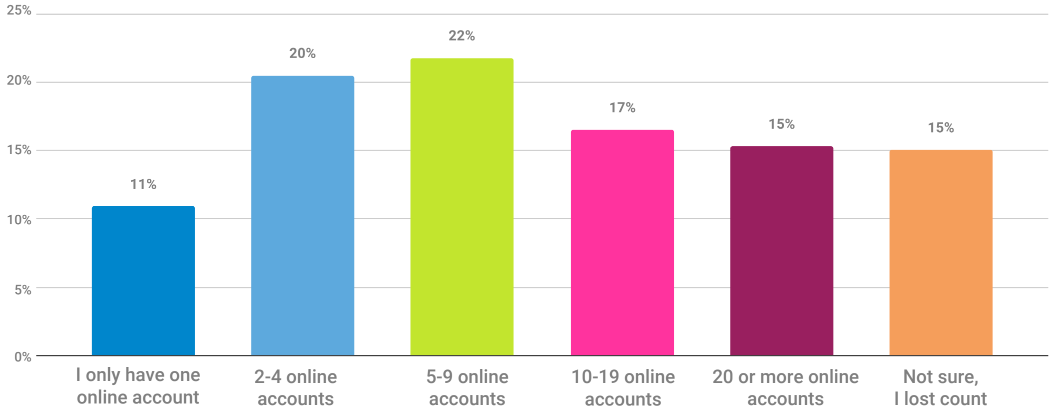


Figure 24. *"Overall, how many sensitive online accounts that hold personal information do you have?"*

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants: 6064, dates conducted: April 13, 2023 - April 27, 2023.

Online security and reliance on others

We were curious about whether people's families depended on them to stay safe online. Over a third (34%) said yes. Another 23 percent said they relied on friends or family to keep them safe online. That's a decrease of 12 percent from last year's report.

Heavy is the head that wears the family tech support crown. Millennials (46%) and Gen Z (39%) report the highest percentage of family members relying on them for online security, compared to just 21 percent of Baby Boomers (21%, Figure 25).

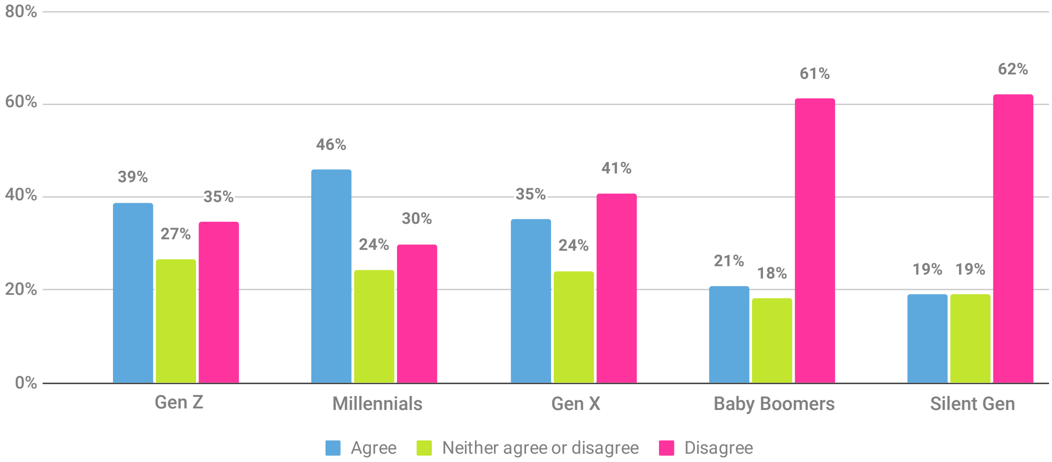


Figure 25. *"Family members rely on me to keep them secure online"* by generations.

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants with generation information: 5748, dates conducted: April 13, 2023 - April 27, 2023.

But then there are the digital lone wolves (56%), who don't need anyone else to stay safe online (Figure 26). For the 23 percent who did seek help, their needs included general security advice (61%), software updates (60%), and backing up data (59%).

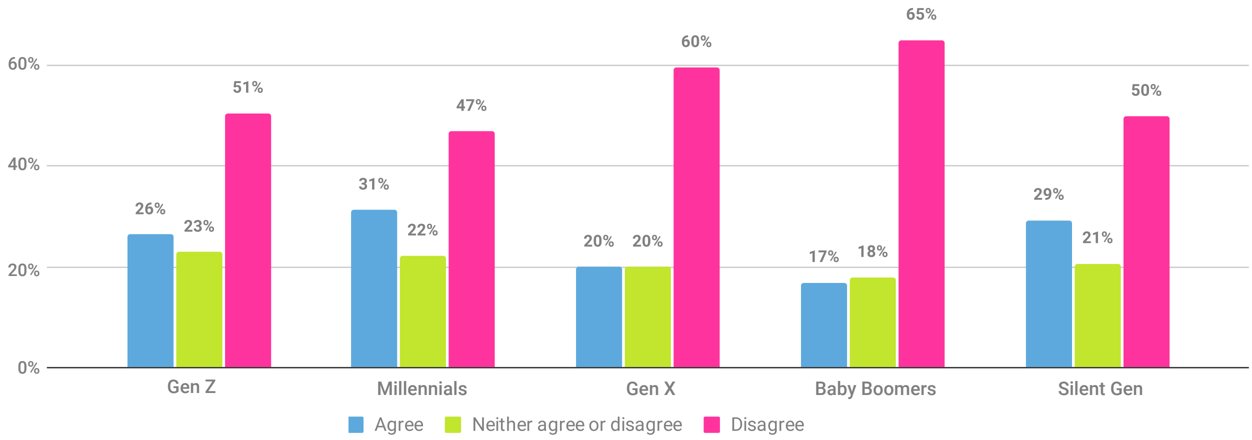


Figure 26. ***"I rely on others (e.g., my family, my colleagues) to keep me secure online"*** **by generations.**

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants with generation information: 5748, dates conducted: April 13, 2023 - April 27, 2023.

General attitudes to online security

Most of us have a sunny cybersecurity attitude, with a blinding eighty-four percent of participants saying that staying secure online was a priority. Plus a cheery 69 percent consider it 'achievable'. These two attitudes had the highest agreement, with mean scores close to 'strongly agree' (Priority: M=8.3, SD=1.9, N=6064; Achievable: M=7.3, SD=2.1, N=6064). Moreover, 69 percent of participants thought staying secure online was worth their effort (Figure 27).

It wasn't clear skies and plain sailing for everyone, though. While feelings of frustration and intimidation were reduced from last year (by 7% and 5%, respectively), 39 percent of participants still felt frustrated, and 37 percent were intimidated by staying secure online. It seems help is reaching the people who need it, but very slowly.

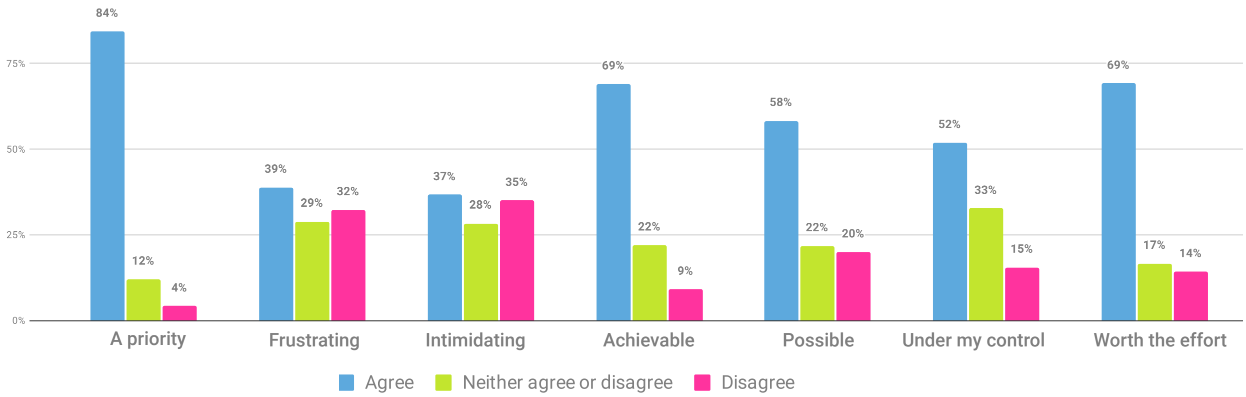


Figure 27. ***"I feel that staying secure online is..."***

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants: 6064, dates conducted: April 13, 2023 - April 27, 2023.

Half of the participants (50%) found staying secure online easy (Figure 28). However, 38 percent agreed that most information about staying safe online was confusing, and sadly this hasn’t fallen since last year. Almost one-third of participants (32%) reported feeling overwhelmed by cybersecurity information, which led them to minimize their online actions.

> **It is important to be able to safely and securely use the internet without having to worry about my information getting leaked.**
> (P3387, United States)

> **Online security means personal data, firewalls and safety online. Data security is one of the most important (e.g., passwords, online tracking) things I worry about.** (P368, United Kingdom)

> **It is impossible to be safe online. Of course I use a virus scanner, update my browser regularly and use different passwords. But I don’t feel sure either.** (P809, Germany)

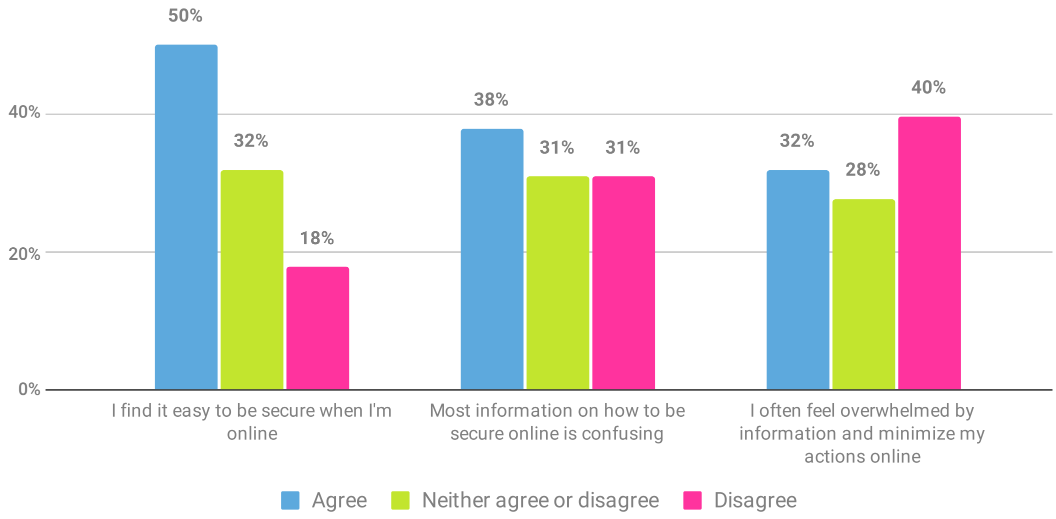


Figure 28. Participants’ levels of agreement with online security ease, clarity, and being overwhelmed.

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants: 6064, dates conducted: April 13, 2023 - April 27, 2023.

Damn. A third of us (33%) presume our devices are automatically secure. That figure is similar to last year. Seemingly our confidence in our devices is hard to shake. Meanwhile, almost half (49%) believed that online protection was costly (Figure 29).

A third of us (33%) presume our devices are automatically secure

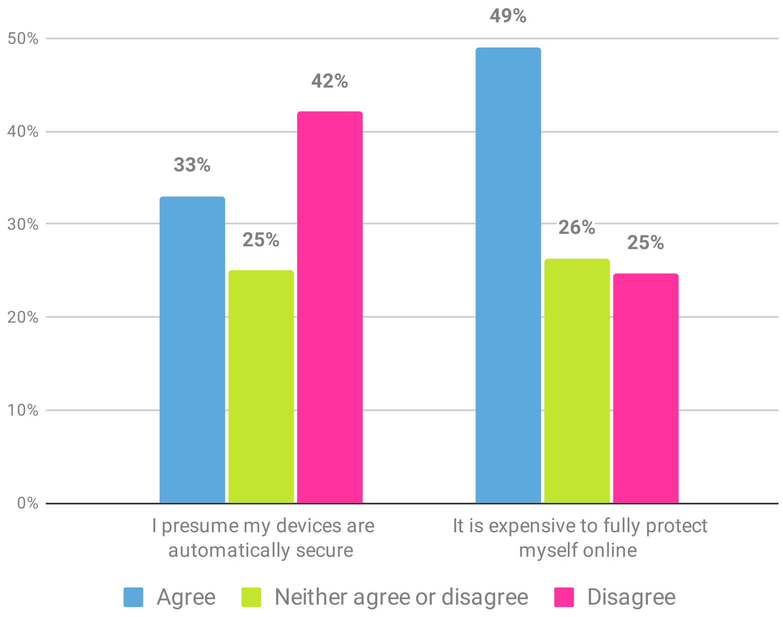


Figure 29. Participants' levels of agreement to presuming their devices are secure and the cost of taking protective action.

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants: 6064, dates conducted: April 13, 2023 - April 27, 2023.

This paragraph should have been sponsored by a casual shrug, or maybe a, 'meh'. Because 22 percent of us don't see the point of trying to protect ourselves further (Figure 30). Similarly, some had a sense of helplessness when it came to losing money online, with 22 percent believing it was unavoidable.

This paragraph should have been sponsored by a casual shrug or maybe a, 'meh'

There was even more 'meh' when it came to theft of personal details, with a third of participants (33%) believing having their personal details stolen online was unavoidable. These results echo last year's data (with only 1-3% differences).

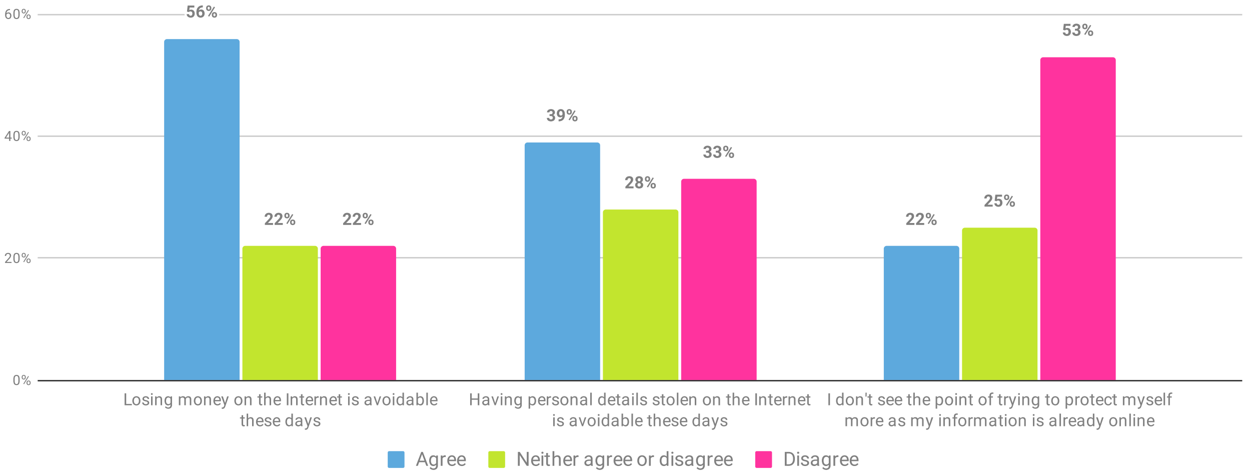


Figure 30. Participants' perceptions about the value of protection and avoidability of losing money or personal details on the Internet.

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants: 6064, dates conducted: April 13, 2023 - April 27, 2023.

Generational differences in attitudes

Age is more than just a number when it comes to cybersecurity attitudes. Our data reveals some intriguing generational disparities. Older generations (91% of Baby Boomers) prioritized online security more than younger generations (69% of Gen Z, Figure 31).

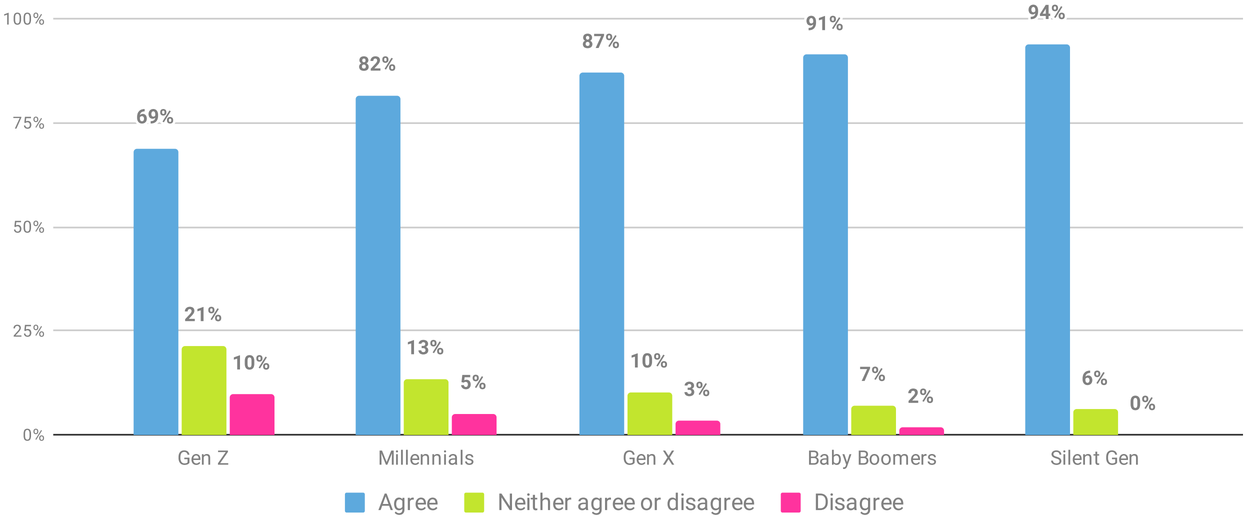


Figure 31. Participants' levels of agreement when answering *"I feel that staying secure online is a priority"* by generation.

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants with generation information: 5748, dates conducted: April 13, 2023 - April 27, 2023.

The Silent Generation (43%) and Millennials (40%) experienced the highest levels of intimidation, while Gen X felt least intimidated by staying secure online (39% disagreed with the statement, Figure 32). Perhaps it's because they grew up in the age of mixtapes and Walkmans, making firewalls and MFA feel like child's play.

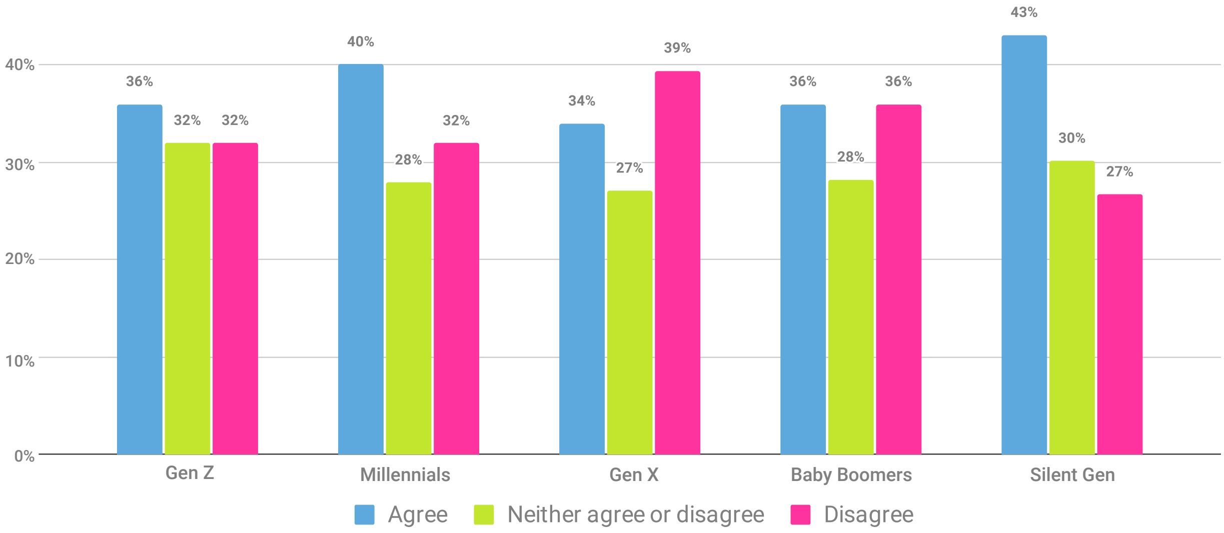


Figure 32. Participants' levels of agreement when answering *"I feel that staying secure online is intimidating"* by generation.

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants with generation information: 5748, dates conducted: April 13, 2023 - April 27, 2023.

Younger generations (21% of Gen Z and 23% of Millennials) were more than twice as likely as Baby Boomers (6%) and the Silent Generation (9%) to disagree with the idea that online security is worth their efforts (Figure 33).

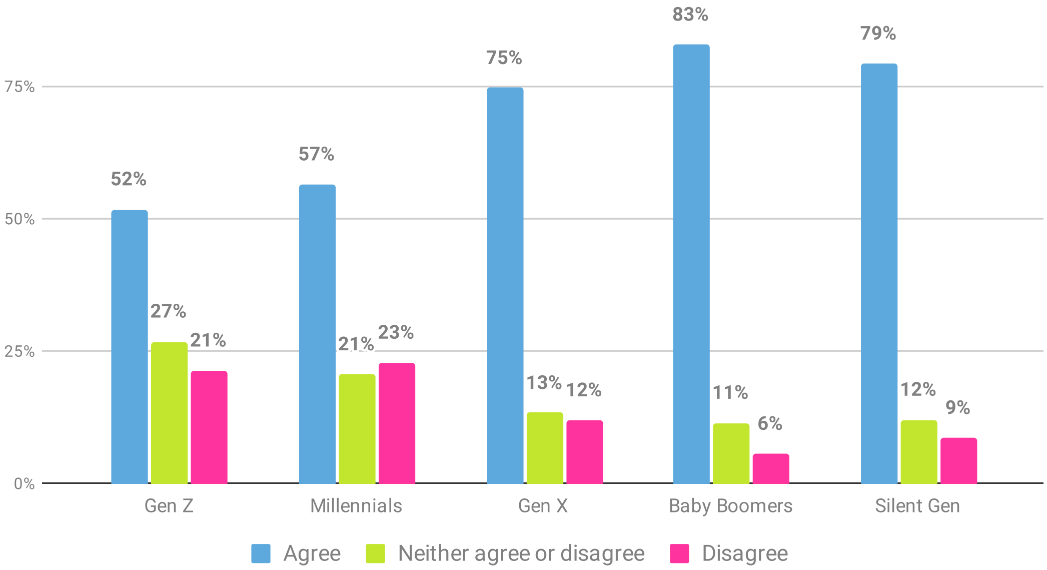


Figure 33. Participants' levels of agreement when answering *"I feel that staying secure online is worth the effort"* by generation.

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants with generation information: 5748, dates conducted: April 13, 2023 - April 27, 2023.

Similar trends and feelings reared their heads when we asked whether online security was seen as achievable. Among Gen Zs, 59 percent believed it was 'achievable', while the other generations agreed anywhere from 68 percent to 79 percent of the time (Figure 34).

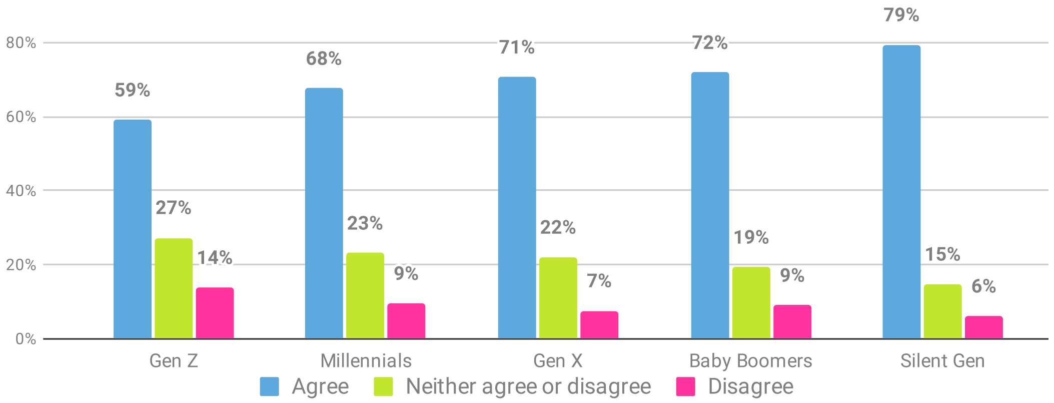


Figure 34. Participants' levels of agreement when answering *"I feel that staying secure online is achievable"* by generation.

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants with generation information: 5748, dates conducted: April 13, 2023 - April 27, 2023.

Which generation are most likely to be masters of their own digital destiny? Certainly not Gen Z, as less than half of them (44%) expressed feeling in control of their online security. Other generations were more confident, with over half of each (ranging from 52% to 53%) agreeing with the sentiment (Figure 35). Twenty-one percent of Gen Zs felt out of control regarding staying secure online, suggesting being a digital native doesn't automatically grant you security self-esteem.

Younger generations (35% of Gen Z and 38% of Millennials) and the Silent Generation (45%) felt overwhelmed. The outcome? They minimized actions online more than Gen X (29%) and Baby Boomers (28%, Figure 36).

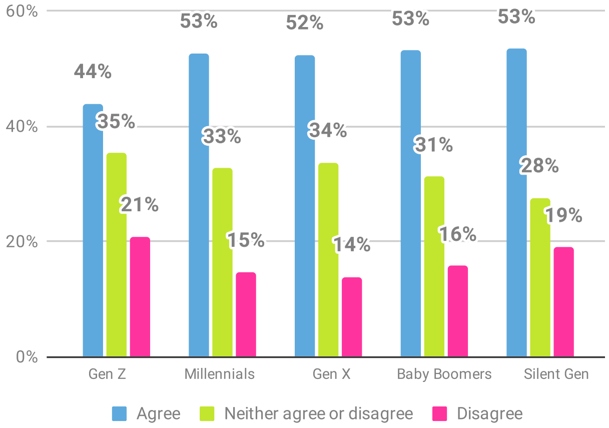


Figure 35. Participants' levels of agreement when answering *"I feel that staying secure online is under my control"* by generation.

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants with generation information: 5748, dates conducted: April 13, 2023 - April 27, 2023.

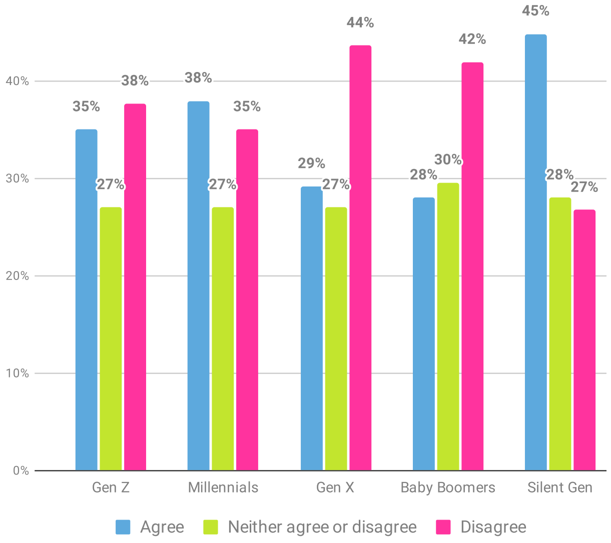


Figure 36. Participants' levels of agreement with answering *"I often feel overwhelmed by information and minimize my actions online"* by generation.

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants with generation information: 5748, dates conducted: April 13, 2023 - April 27, 2023.

Actually, the data suggests growing up with tech makes it more likely you'll be visited by digital demons. The generational data shows digital natives (i.e., Gen Zs and Millennials) and those with little online exposure during active employment (i.e., Silent Generation) are most at risk, tending to struggle with online security.

Media impact on attitudes and behaviors

New question alert! As a new angle this year, we asked participants about the impact of media and news coverage on their views of online security. Let's face it, if the news said jumping up and down while brushing your teeth made your Wi-Fi faster, a large portion of us would be bathroom acrobats by the end of the week.

Surprisingly, 56 percent of the participants reported the media & news motivated them to take protective security actions. Fifty-one percent said it helps them to stay informed about online security (Figure 37). However, 44 percent of participants pointed out the media & news makes them feel scared, and 42 percent believed such coverage complicates online security. A mixed bag for sure.

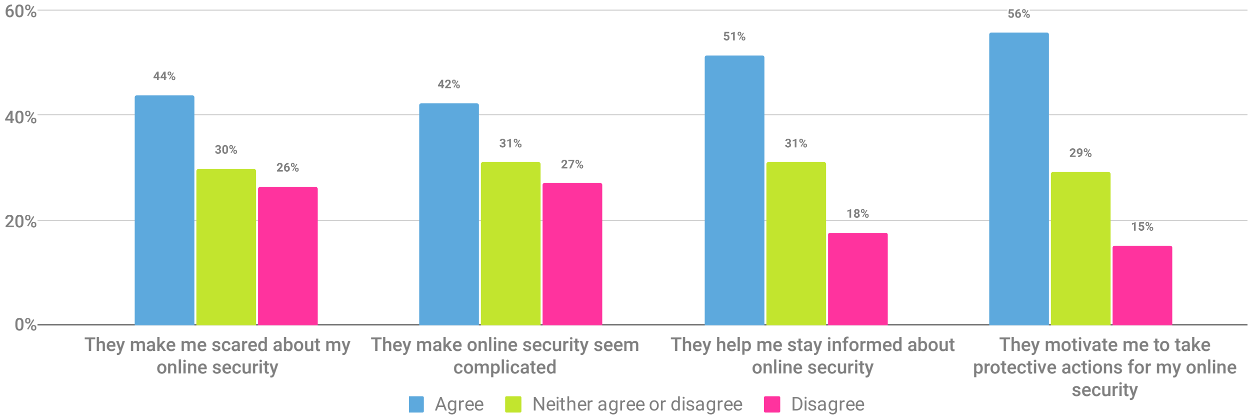


Figure 37. *"What impact does the media/news have on your views towards online security?"*

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants: 6064, dates conducted: April 13, 2023 - April 27, 2023.

We uncovered a few generational differences in media & news-related statements. This is surprising, given how different generations consume news. One important distinction: Gen Zs (22%) tended to disagree more than other generations with the idea that news & media helped them stay informed about online security (Figure 38).

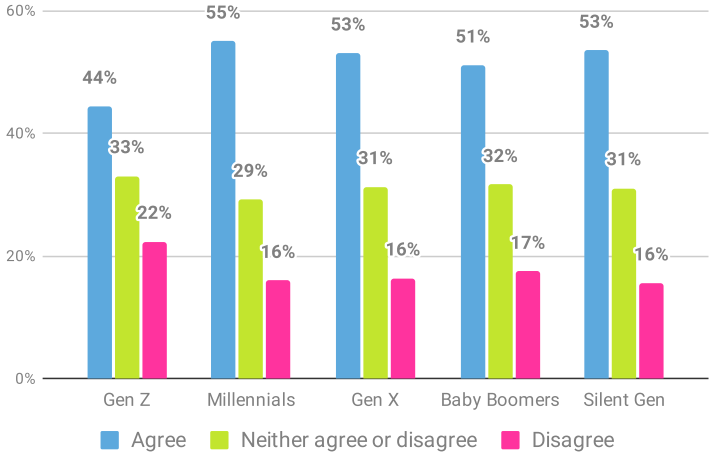


Figure 38. Participants' levels of agreement, by generation, with statement media/news help them to stay informed about online security.

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants with generation information: 5748, dates conducted: April 13, 2023 - April 27, 2023.

Gen Z (47%) also felt least motivated to take protective measures based on the media & news coverage compared to Millennials (58%) and older generations (57% of Baby Boomers and 65% of Silent Generation, Figure 39). Maybe Gen Z are too busy creating the future to worry about the present? Or maybe they're yet to develop the healthy skepticism experienced later in life.

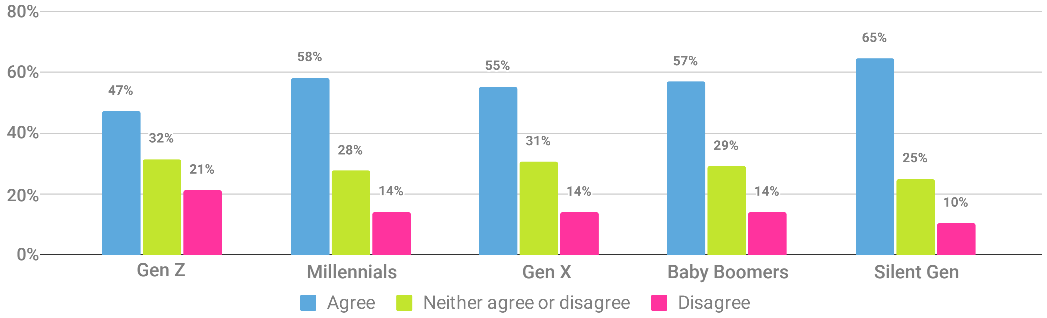


Figure 39. Participants' levels of agreement, by generation, with the statement that the media/news motivates them to take protective online security actions.

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants with generation information: 5748, dates conducted: April 13, 2023 - April 27, 2023.

Cybersecurity responsibility

A vital question we invited people to ponder next: Who shoulders most of the responsibility for protecting online information? Well, ponder they did...

An impressive 66 percent of people pointed to none other than themselves as the primary guardians of their online info (Figure 40). This marks a seven percent increase from last year's survey. Is personal responsibility taking center stage?

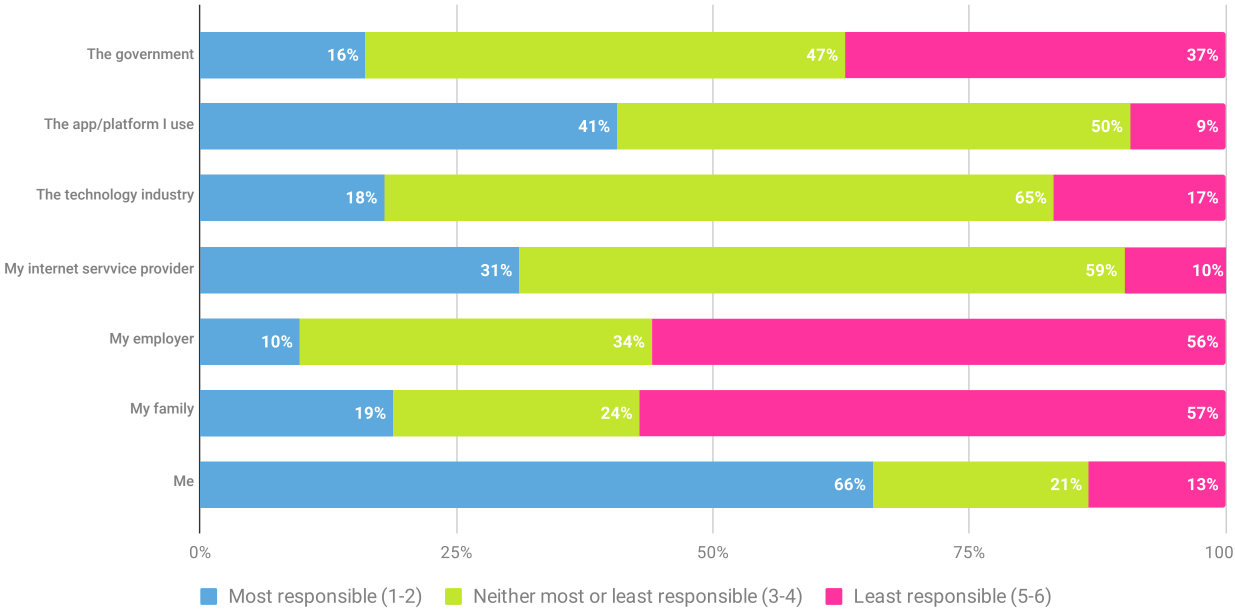


Figure 40. Participants' ranking of responsibility in answering *"Who is most responsible for protecting your information?"*

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants: 6064, dates conducted: April 13, 2023 - April 27, 2023.

Meanwhile, on the flip, we're not keen on entrusting our families (57%), employers (56%), or governments (37%) with our digital wellbeing. Just like last year, these three were seen as the least responsible agencies. But get this—application and platform responsibility edged up by five percent from 2022, to 41 percent. When it comes to trust perceptions, Silicon Valley > the state.

What about workplace information? Here, the country's government takes the unfortunate title of being the least reliable protector, with 59 percent of participants rating it as the least trustworthy agency (Figure 41).

The country's government takes the unfortunate title of being the least reliable protector

So, who is guarding the flock? You are. Apparently.

Individual responsibility is on the rise at work as well as in our home lives. The percentage of people taking it upon themselves to safeguard workplace information has surged from 25 percent in 2022 to a commendable 39 percent this year.

But that wasn't the biggest leap. A positive trend was also noted with more responsibility placed on workplace security departments (from 28% in 2022 to 46% in 2023) and IT departments (from 36% in 2022 to 48% in 2023). This could have been due to the option 'employer' being removed from this year's survey. That was the option with the highest percentage (43% in 2022) in previous years.

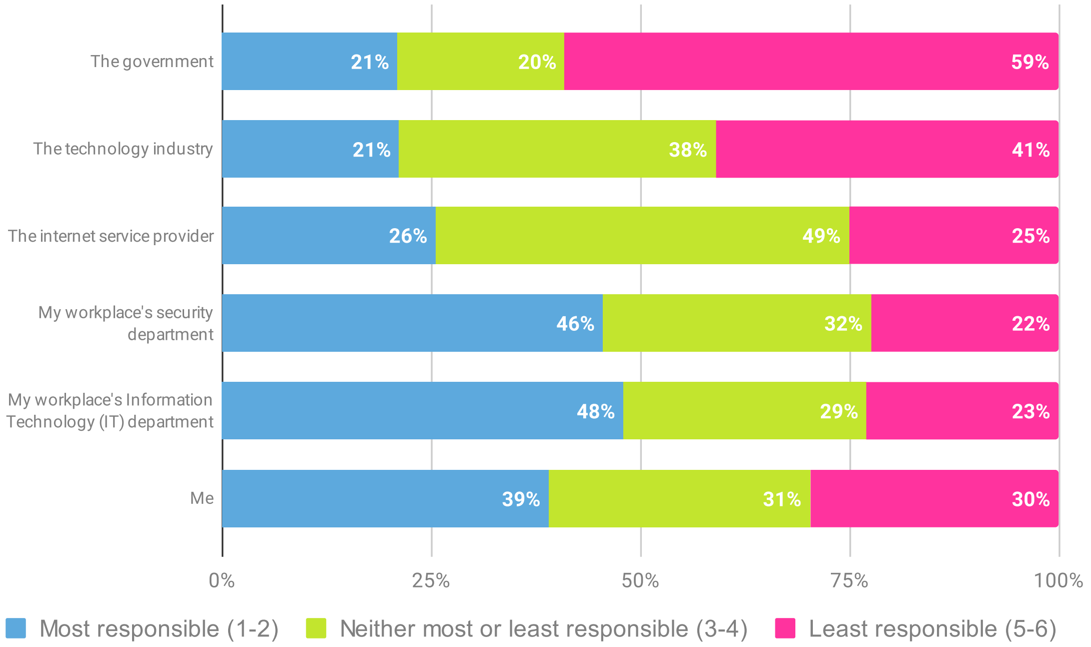


Figure 41. Participants' responsibility rankings in answering *"Who is most responsible for protecting your workplace's information?"*

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants in employment: 4021, dates conducted: April 13, 2023 - April 27, 2023.

Cybersecurity training

Access to training

Deep breath. It's time to tackle the all-important topic of training. For the third year in a row, we found access to cybersecurity advice and training remains alarmingly low. Just 26 percent (Figure 42) of participants said they had access to cybersecurity training and had used it (30% in 2022).

> **For the third year in a row, we found access to cybersecurity advice and training remains alarmingly low**

A staggering 64 percent (a 2% increase from 2022) are without access, despite...oh, you know, all those looming global cybercrime threats. Anyone have a paper bag we can breathe into?

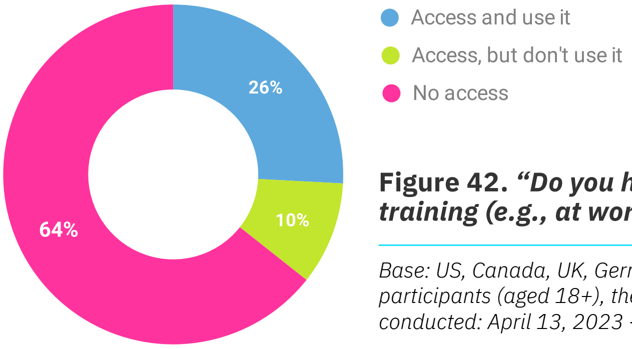


Figure 42. *"Do you have access to cybersecurity training (e.g., at work, school, or library)?"*

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants: 6064, dates conducted: April 13, 2023 - April 27, 2023.

What else about access? There's a dramatic divide between people in employment and education versus those who are not (Figure 43). People who work or study reported having access to training (47% and 49%, respectively), compared to those who were retired (8%) or not in active employment or studying (15%). However, a job isn't your ticket to training, as 53 percent of employed participants reported having no access to cybersecurity training.

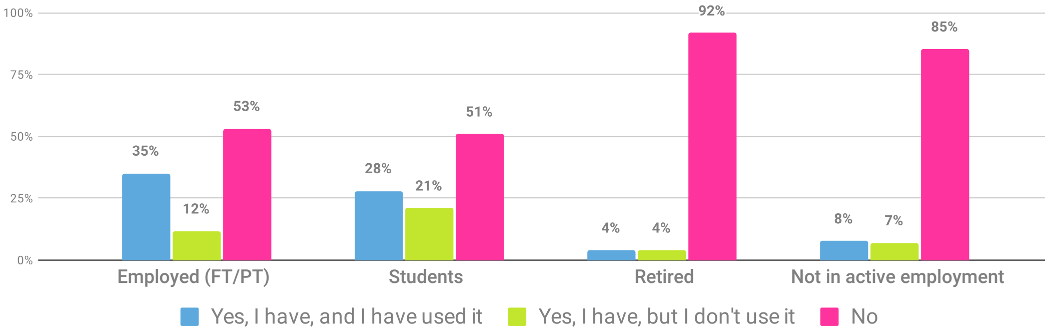


Figure 43. *"Do you have access to cybersecurity training (e.g., at work, school, or library)?"* by employment status.

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants: 6064, dates conducted: April 13, 2023 - April 27, 2023.

This trend pops up in older generations, where 93 percent of the Silent Generation and 85 percent of Baby Boomers (an increase of 10% and 5% from 2022, respectively) reported a cybersecurity training level of 'zilch' (our word, not theirs, Figure 44).

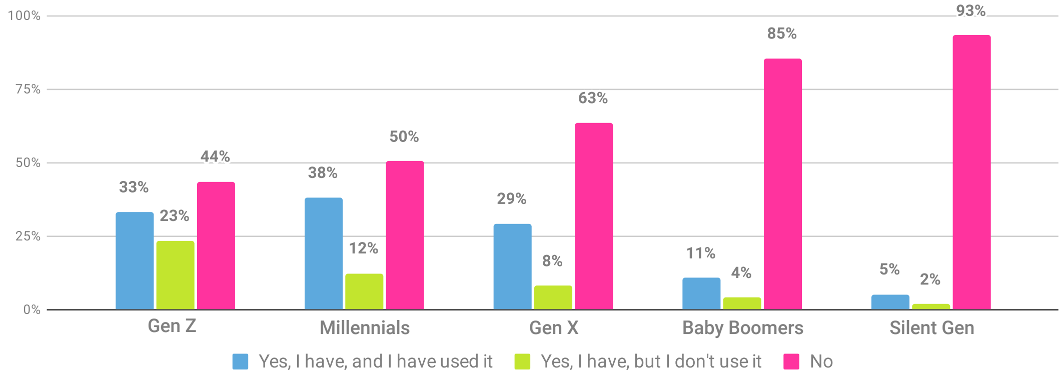


Figure 44. ***"Do you have access to cybersecurity training (e.g., at work, school, or library)?"*** **by generations.**

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants with generation information: 5748, dates conducted: April 13, 2023 - April 27, 2023.

Millennials' access to training is dwindling (down by 9% from 2022), while 23 percent of Gen Zs have access but don't use it (a 12% increase from 2022). Two important things here: training access seems lower than in the past, and while no demographic has stellar access to it, people not in active employment and older generations may be more susceptible to cybercrime, as they lack access to the necessary tools and information to reduce their vulnerability.

Meanwhile, many Gen Zs have the knowledge at their fingertips, but aren't taking advantage of it. In the age of TikTok and short form content, are employers kidding themselves by thinking the future workforce are prepared to sit through hours of static e-learning?

Training locations

Let's dive into the digital dojo. We asked our participants where they sought their cybersecurity training. We made it easier this year by allowing for multiple-choice answers.

Location, location, location. Just like last year, the majority (52%) accessed cybersecurity training at work or place of study. Only 16 percent accessed it from home. We also found 19 percent mixed it up, accessing resources at both work and home. Five percent reported having access to cybersecurity training in multiple locations. As more of us work on the move, and in hybrid setups, that figure's likely to grow.

It seems the allure of traditional training methods remains strong, with 43 percent (N=1559) reporting getting their cybersmarts through one-off individual training courses. Overall, only 30 percent reported continuous training over time, whether individually or in groups.

We've long been proponents that one-time security awareness training doesn't cut it. It needs to be an ongoing activity, helping people understand how to respond to threats as and when threats occur.

We asked how common it is for cybersecurity training to be a mandatory mission. Most training completed at work or place of education was a must (82%, N=1149). And of those reporting having to complete compulsory training, 55 percent completed it once a year (Figure 45). That's up by 13 percent from last year (2022).

Unfortunately, 19 percent of participants have to complete training when something goes wrong or something 'bad' happens (e.g., a security incident at work). Sigh.

Maybe there's a glimmer of hope, as these figures were slightly reduced from last year (by 5%).

A small yet vital side note—it's not a great plan to make folks link 'failing' with training. It turns training into a punishment, and that really doesn't help it do its job effectively.

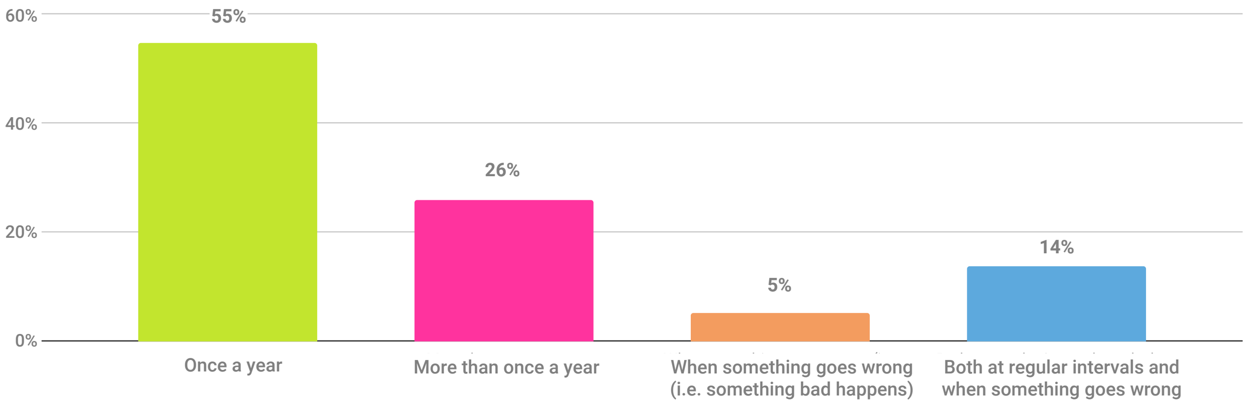


Figure 45. ***"How often are you required to complete training?"***

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants completing mandatory training at work or place of education: 947, dates conducted: April 13, 2023 - April 27, 2023.

The majority of participants still favored traditional methods of training delivery with 42 percent (N=6064) preferring online training courses and 24 percent in-person courses.

Encouragingly, 22 percent indicated they would like training delivered through notifications when needed, such as when deciding whether or not to take a specific action.

When comparing those who had access to training and those who didn't, participants without access to courses were less likely to prefer online courses (35%) and more likely to prefer timely notifications (24%) than those with access to training (Figure 46). Additionally, 17 percent of those without access to training stated they didn't need cybersecurity information. Erm...

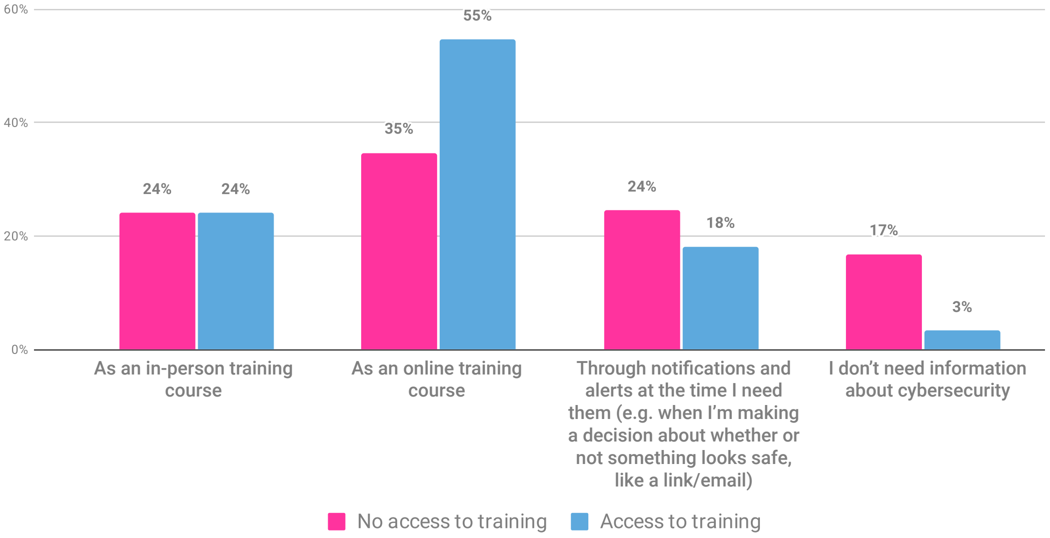


Figure 46. ***"How would you most prefer cybersecurity training to be delivered?"***

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants with access to training: 2151, and without access to training: 3913, dates conducted: April 13, 2023 - April 27, 2023.

It seems traditional training methods hold their appeal for many. Almost half (47%) of participants who were employed, whether full- or part-time, preferred online training courses in comparison to in-person training (24%) or having alerts or notifications at the time they needed them (19%, Figure 47).

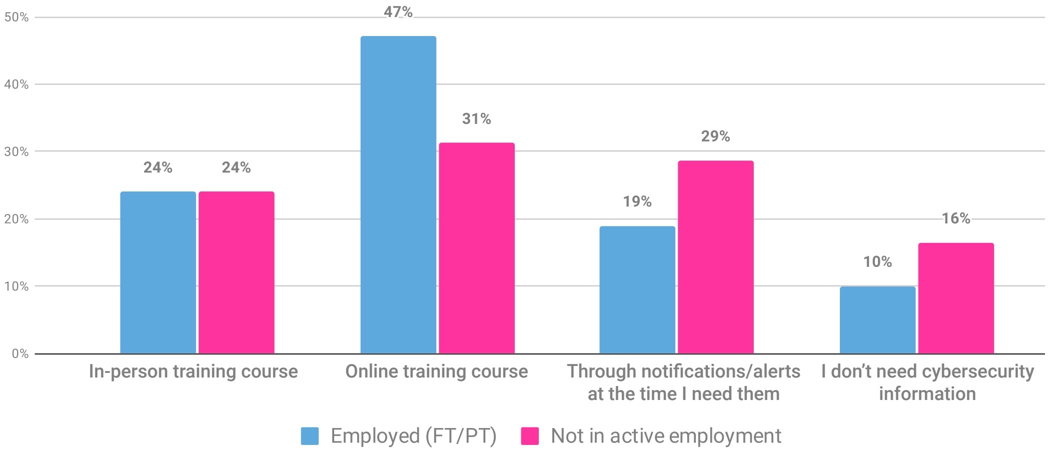


Figure 47. ***"How would you most prefer cybersecurity training to be delivered?"*** **by employment.**

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants: 6064, dates conducted: April 13, 2023 - April 27, 2023.

Some participants (N=592) mentioned they have access to training but wish not to use it. Why? The top reason was lack of time (29%). Meanwhile 18 percent felt they had this cybersecurity thing down already, no need for further improvement (Figure 48).

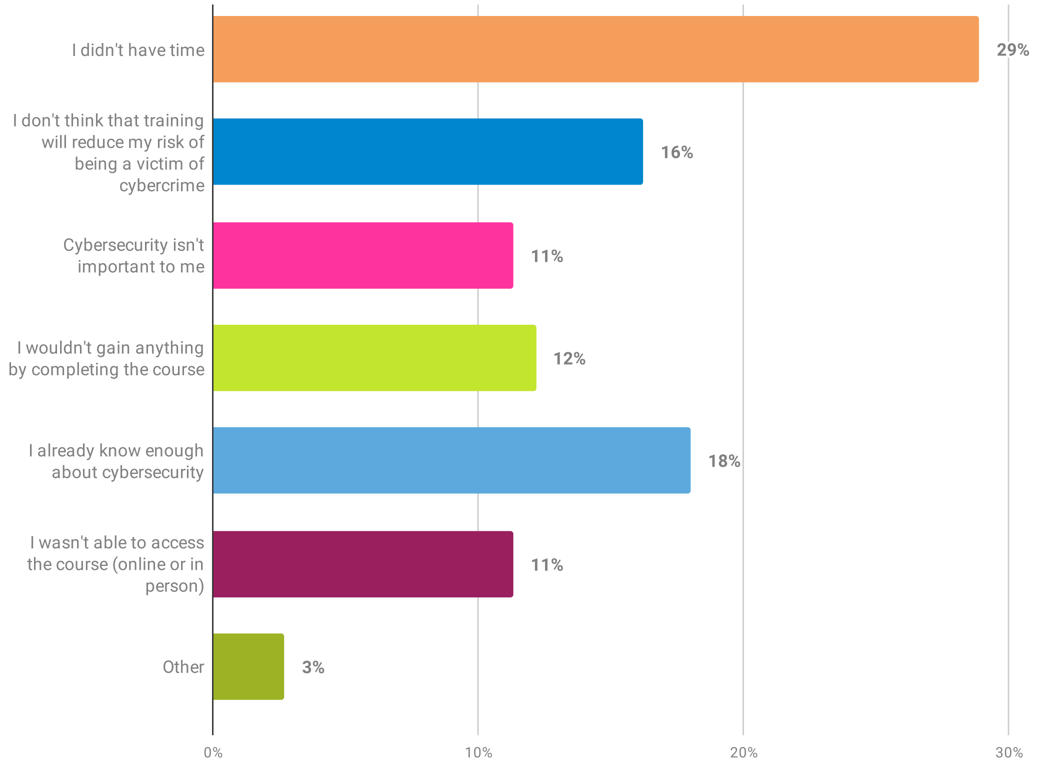


Figure 48. ***"What is the main reason you didn't use the opportunity to attend a cybersecurity training course?"***

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants with access to training but not using it: 592, dates conducted: April 13, 2023 - April 27, 2023.

Another 16 percent believed cybersecurity training would not effectively reduce their risk of falling victim to cybercrime; some (11%) noted cybersecurity was unimportant.

We're not done just yet, because a further 11 percent of participants said they couldn't access training, with a huge 48 percent giving childcare duties as the primary obstacle.

> **I hope my software protects me with regular updates and have also installed a safety program. My fragmentary knowledge of security updates, program possibilities, and cyberattacks is insufficient to feel completely protected!** (P9051, Germany)

> **I think it is difficult to obtain total online security as threats are numerous. You have to be very suspicious.** (P5598, France).

The impact of cybersecurity training

Cybersecurity training courses are beneficial, as long as people can learn from them and apply their learning in practice. So, we asked participants what they learned as part of these courses and whether they had any influence on their online security behaviors.

Like last year, we found that recognizing phishing emails steals the spotlight, being covered in 68 percent of training (Figure 49). This was followed by instructions on using strong and separate passwords (57%) and MFA (54%). Every party has its wallflower, and in this case it's backing up data, which got a mention in just 36 percent of courses.

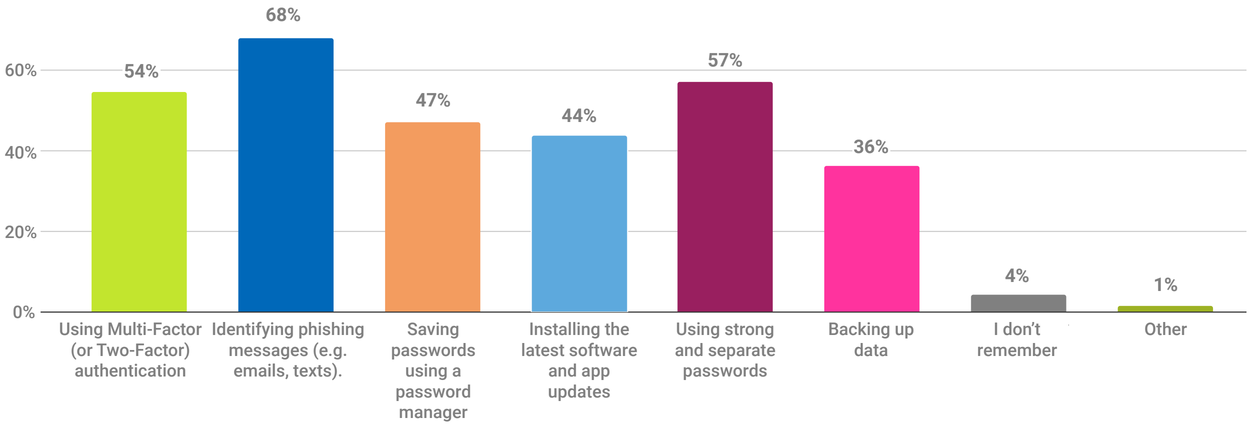


Figure 49. ***"Thinking about your last training course, what did you learn about cybersecurity?"***

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants who had attended training courses: 1559, dates conducted: April 13, 2023 - April 27, 2023. Multiple-choice question.

Most participants (84%) found cybersecurity training 'useful' or 'very useful', regardless of whether it was conducted at home or work (N=1888). The usefulness of training at home (M=8.17, SD=1.66, N=739) and at work (M=7.93, SD=1.85, N=1149) environments were very similar on a 10-point scale. Only two percent of those completing training at home and five percent completing it at work/a place of education found the training 'not at all useful'.

Additionally, 78 percent of participants reported the cybersecurity training as engaging, with high engagement ratings for home (M=8.00, SD=1.84, N=739) and work (M=7.56, SD=2.14, N=1149) environments.

So, most people were listening, but what happened after the training? We wanted to know if people thought their cybersecurity behaviors had been impacted by training. Compared to last year, the percentages were slightly lower (6% to 10% for some key behaviors). This was most likely due to the newly added option (i.e., 'I already do all these things, so I didn't change anything') coming into play.

However, half (50%) reported being better at recognizing and reporting phishing messages, 37 percent had started using strong and unique passwords, and a third (34%) had begun using MFA (Figure 50).

So, yes, training can make a difference. But it's important to remember it may also have a limited impact. This is supported by another recent study from NIST.

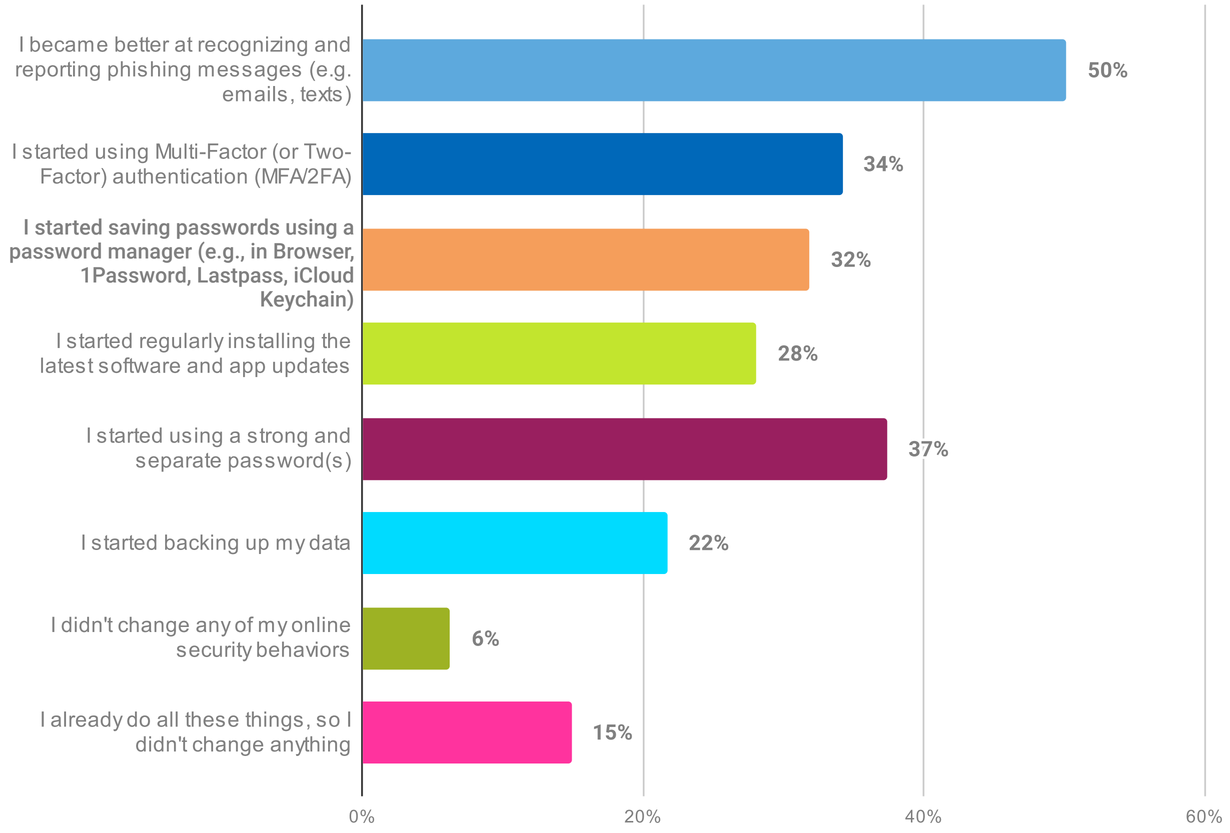


Figure 50. *"When you attended training course(s), how did it influence your security behaviors?"*

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants who had attended training courses: 1559, dates conducted: April 13, 2023 - April 27, 2023. Multiple-choice question.

Improving training effectiveness

Teach behaviors, not awareness
Security awareness training initiatives need to go further than simply educating people about different cyber security risks. The Security behavior database, or SebDB, can be used to determine the risk outcomes important for your organization, and target the right behaviors to reduce risk.

Design security awareness training for everyone
There is no one-size-fits-all approach, training content needs to be personalized.

Security training isn't a one-time event
Encourage people to continually improve their cyber hygiene by regularly setting goals and sending nudges and alerts.

Also, consider providing an on-demand library of security training resources. Here, people can get relevant knowledge whenever they need it.

Leverage data and reporting
Using data metrics and insights, you can identify the most significant human cyber risks impacting your organization and cover these in your security awareness training.

Grab people's attention
An effective security awareness programme will make it clear to people that good cybersecurity is vital and that they have an essential role in enabling this.

Don't view people as the weakest link
This attitude is outdated. And it can undermine the fundamental aims of security awareness initiatives.

Get everyone involved
Whether you're the CEO or an intern, everyone is responsible for practicing healthy cybersecurity behaviors and contributing to a safer workplace.

🔗 www.cybsafe.com/blog/how-to-make-your-security-awareness-training-more-effective/

Cybercrime victimization

In this section, we explore participants' perceptions and attitudes toward being victims of cybercrime. How did they feel about the possibility of falling prey to cybercriminals? And had they experienced any of the three primary types of cybercrime—phishing, identity theft, or online dating scams—resulting in the loss of money or data?

Cyberbullying gets its own section, because unlike cybercrime, the incidents don't always lead to loss of money or data.

Vitally, we take a look at the reporting rates of these crimes and discuss why they tend to be underreported.

> **I received an email from Costco once...a special offer, and I took them up on it, and within minutes, my debit card was being used.** (P469, United States)

Attitudes towards victimization

Perceptions of becoming a victim of cybercrime have increased by seven percent since last year, as half the participants (50%) felt they were potential targets of cybercriminals (Figure 51).

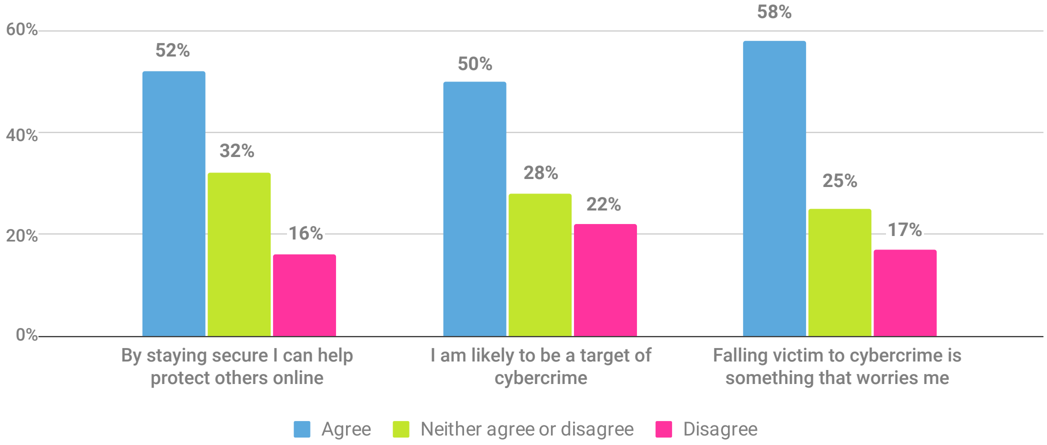


Figure 51. Participants' responses to statements about how staying secure online can help protect others, perceived likelihood of becoming a cybercrime target, and worries about falling victim to cybercrime.

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants: 6064, dates conducted: April 13, 2023 - April 27, 2023.

Like last year (57% in 2022), most participants (58%) were worried about falling victim to cybercrime. Additionally, over half (52%) agreed they can help protect others online by staying secure.

Cybercrime prevalence

Participants disclosed 2,047 cybercrime incidents (i.e., phishing, identity theft, and online dating scams) that had resulted in the loss of money or data. Overall, 27 percent of participants disclosed being victims of at least one type of cybercrime—which had fallen by seven percent from last year.

Out of 1,614 victims of cybercrime, the majority had experienced phishing crimes (60%).

Overall, phishing incidents were the tricksiest trickster of them all, accounting for the highest proportion of total incidents (47%, Figure 52). In contrast to the previous year, where identity theft held the position of the second-highest reported crime type (24% in 2022), closely followed by online dating scams (17% in 2022), this year saw a shift. Online dating scams took the lead, becoming more prevalent (27% of incidents) compared to identity thefts (26%). Like the 80s hit says, love is a battlefield.

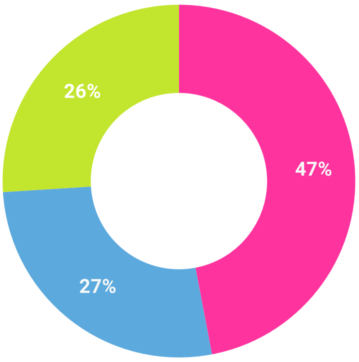


Figure 52. Types of cybercrime incidents.

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of cybercrime incidents 2047, dates conducted: April 13, 2023 - April 27, 2023.

It's high time we busted a misconception: Far from making you "cyber-streetwise", growing up around the internet actually puts you at more risk of getting hit by cybercriminals. Digital natives had the highest numbers of cybercrime victimization. Specifically, 43 percent of Gen Zs mentioned losing money or data due to cybercrime, followed by 36 percent of Millennials (Figure 53). As in the previous year, Baby Boomers (15%) reported the lowest numbers of victimization rates, followed closely by the Silent Generation (20%) and Gen Xs (23%).

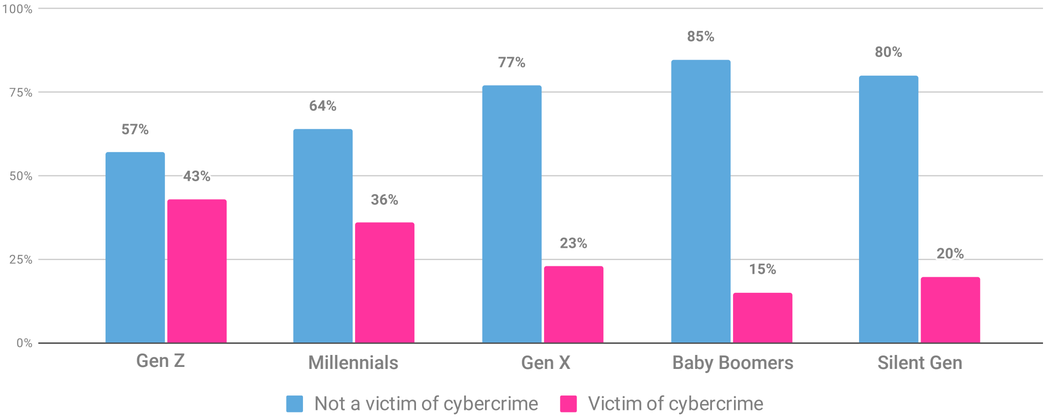


Figure 53. Victimization by generation.

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants: 5748, dates conducted: April 13, 2023 - April 27, 2023.

Millennials take the unenviable crown, reporting the highest proportions of all types of crimes (Figure 54). For instance, 44 percent of victims of online dating scams were Millennials, compared to 22 percent of Gen X and seven percent of Baby Boomers.

Millennials also accounted for over a third of phishing (36%) and identity theft (37%) crimes. If not taking into account the Silent Generation (due to the small participant pool), identity thefts were lowest in Gen Zs (15%) and Baby Boomers (17%) generations.

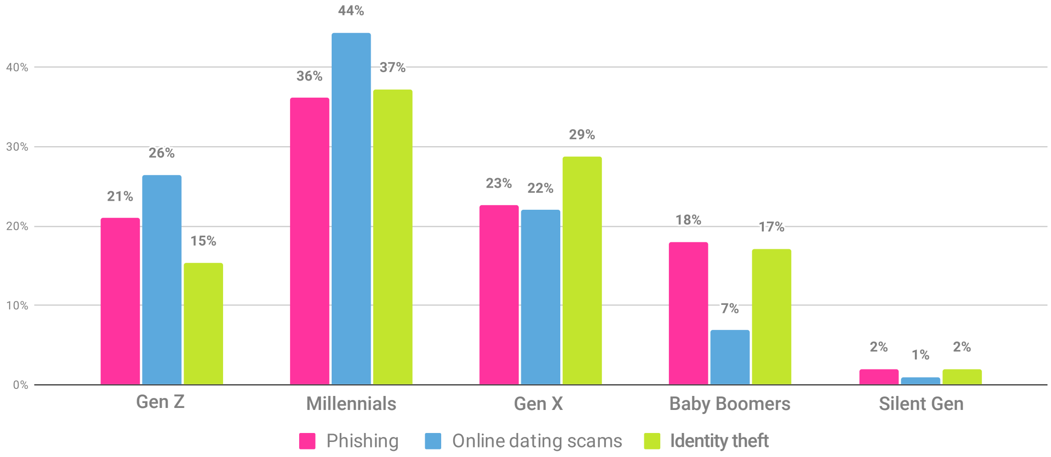


Figure 54. Cybercrime incidents by generations.

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of cybercrime victims: Phishing, 911; Online dating scam, 541; Identity theft, 508 (excluding any cybercrime incidents noted by 316 participants from New Zealand, who didn't provide their age), dates conducted: April 13, 2023 - April 27, 2023.

> **Being an honest person, I like to put faith in others and tend to trust everyone until proven wrong.** (P533, United States)

Cybercrime reporting

'Not on my watch!' The reporting rates for all crime types were favorable, with 88 percent of cybercrime victims reporting the incident to someone. This year, only 14 percent of phishing, 16 percent of online dating scams, and eight percent of identity thefts, which had led to losing money or data, went unreported (Figure 55).

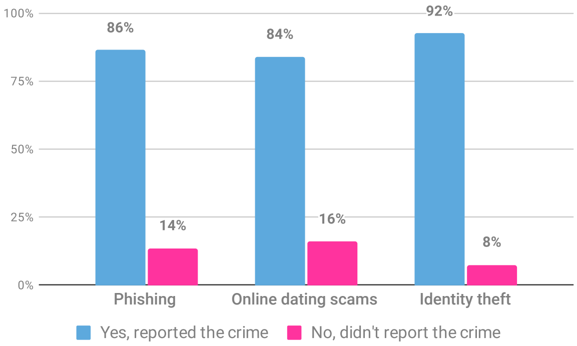


Figure 55. Crime reporting frequency by crime type.

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of cybercrime victims: Phishing, 961; Online dating scam, 555; Identity theft, 531, dates conducted: April 13, 2023 - April 27, 2023.

This is a mammoth shift from 2022. Back then, 31 percent of phishing, 42 percent of online dating scams, and 26 percent of identity thefts went unreported. We love to see it.

> **This is a mammoth shift from 2022**

On average, crime reporting rates were consistently high across the generations (ranging from 82% to 92%). The highest rate of unreported cyber crimes occurred in Gen Xs (18%), with the lowest reporting rates for online dating scams (74%). It seems cybercriminals are getting away with putting a damper on a little middle-aged romance. A crime in itself.

Those who had been victims of cybercrime favored reporting the incident to their bank or credit card company (59% phishing, 54% identity theft, and 42% online dating scams, Figure 56). The second most common course of action was to report the incident to the authorities, such as the police. Interestingly, victims of online dating scams also opted to report the incident to the designated person or department at their place of work or education (28%) and to their network/broadband or phone provider (26%).

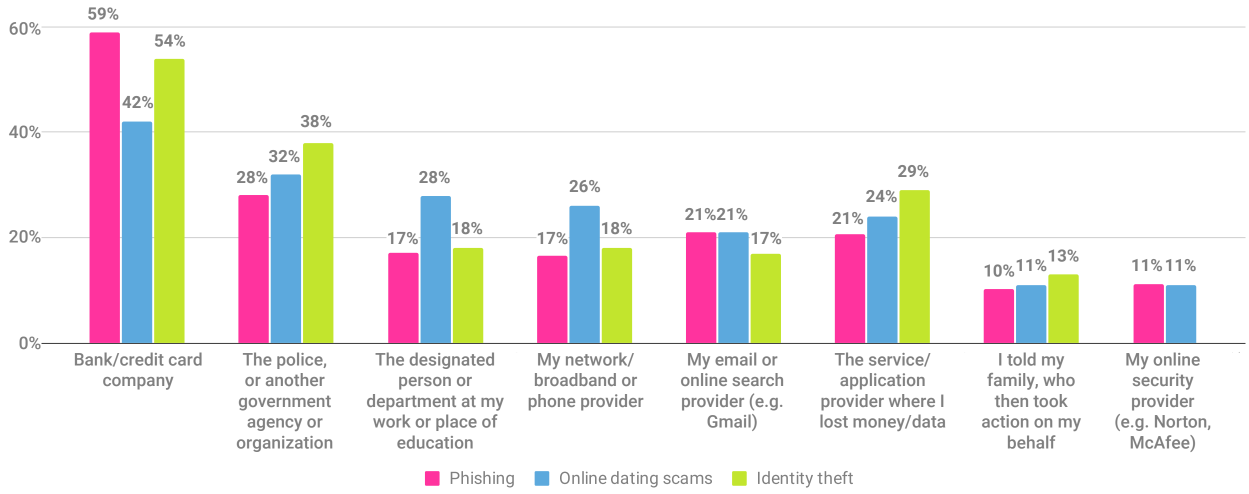


Figure 56. Who were the cybercrimes reported to?

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants who had reported cybercrime: Phishing, 830; Online dating scam, 466; Identity theft, 491, dates conducted: April 13, 2023 - April 27, 2023. Multiple-choice question. 'My online security provider' wasn't given as a choice for identity theft.

We wanted to dig into the reasons behind the reporting. Most victims of phishing (50%), online dating scams (39%), and identity theft (39%) reported the incident to relevant authorities because they wanted to prevent it from happening again to themselves or others. And for both phishing (29%) and identity theft (42%) victims, wanting their money back was a key driver for sounding the alarm.

Many people stated they knew how and to whom to report phishing scams (49%, Figure 57). Also, identity theft (39%) reporting seemed reasonably straightforward for some, but a quarter (25%) of the victims had to dig deep, finding the reporting process challenging but eventually succeeding.

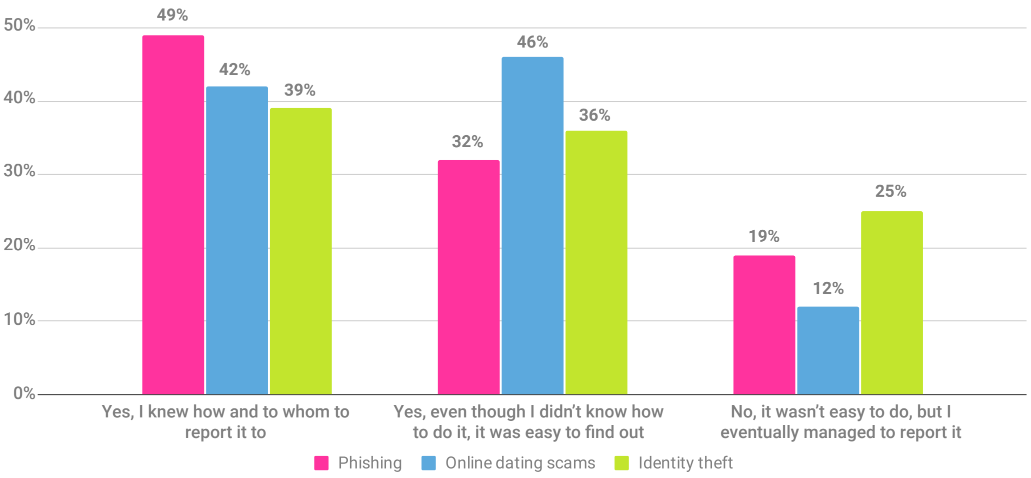


Figure 57. Easiness of the reporting process by crime type.

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants who had reported cybercrime[11]: Phishing, 813; Online dating scam, 466; Identity theft, 480, dates conducted: April 13, 2023 - April 27, 2023.

But the picture's incomplete if we don't also look at those who didn't report. What were their reasons for not doing so? The top cited reasons for phishing incidents were that the amount of money/data lost was negligible or unimportant to them (19%), and they felt there was no point in reporting as no action would have been taken (18%, Figure 58).

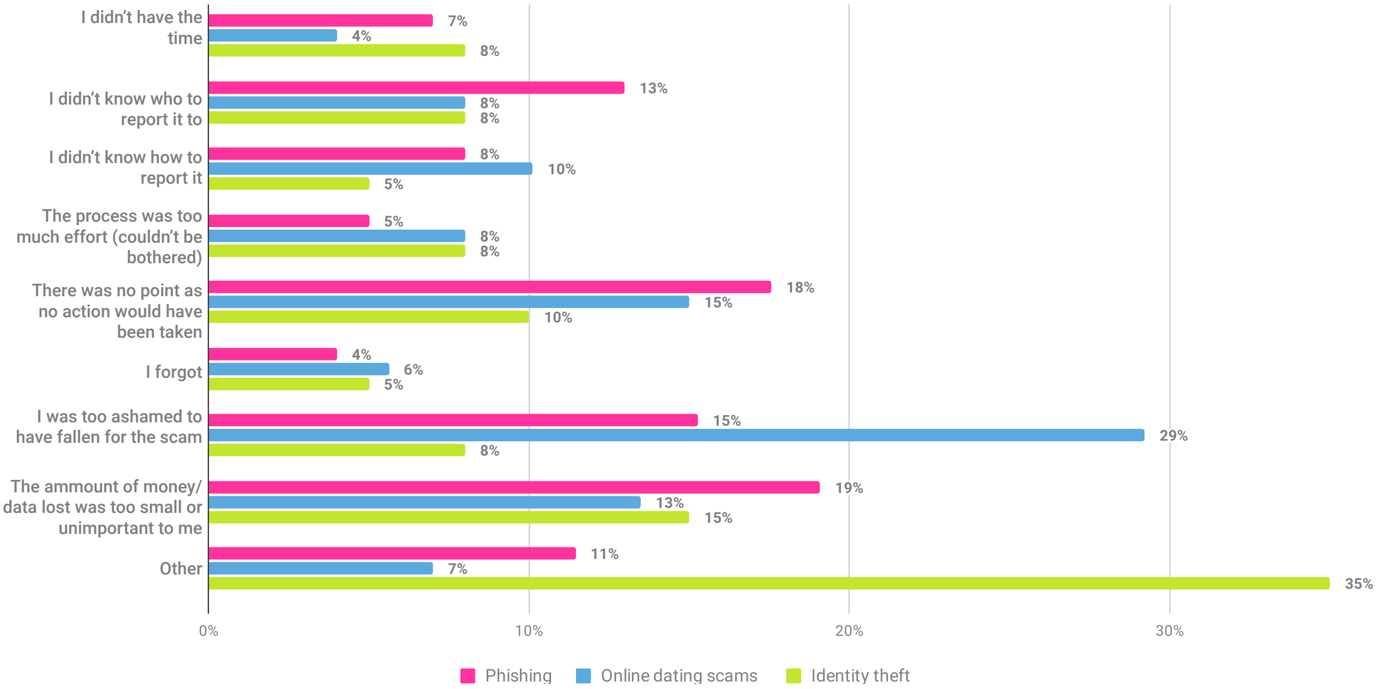


Figure 58. Reasons given for not reporting the incident by crime type.

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants who had not reported cybercrime: Phishing, 131; Online dating scam, 89; Identity theft, 40, dates conducted: April 13, 2023 - April 27, 2023.

[11] Those phishing (N=17) and identity theft scam (N=11) victims who asked a family member to take action were not asked about the easiness of the reporting process.

When reporting online dating scams, those who didn't report the incident mentioned they were too ashamed for having fallen for the fraud (29%), and some noted there was no point in doing so (15%).

A sizable 35 percent of identity theft victims who didn't report revealed various 'other' reasons. Most of them said it was because the companies (e.g., banks) or service providers flagged it and dealt with it directly.

> **I had reported it to the service provider several times and received no reaction.** (P8181, Germany)

Cyberbullying

When we think about cyberbullying, sharp exchanges on social media most likely come to mind. But make no mistake: Cyberbullying is a growing threat for individuals and organizations alike.

In general terms cyberbullying involves the use of electronic communication to bully, harass, or intimidate someone. The motive? Simply causing the victim to feel emotional distress.

> **Cyberbullying is a growing threat for individuals and organizations alike**

Contrary to popular belief, cyberbullying isn't confined to children and teenagers. It affects people of all ages.

And that means cyberbullying has significant implications for cybersecurity. Not only does it compromise mental well-being, but it can also disrupt good cyber hygiene habits.

Incident frequency

Participants reported 921 incidents of cyberbullying. And, similar to last year's data, while no one's immune, there's a strong age pattern. Gen Zs (38%) reported the highest rates of being victims of cyberbullying (Figure 59). The number of cyberbullying incidents declined through the generations, with the Silent Generation noting only four cases (3%) of cyberbullying.

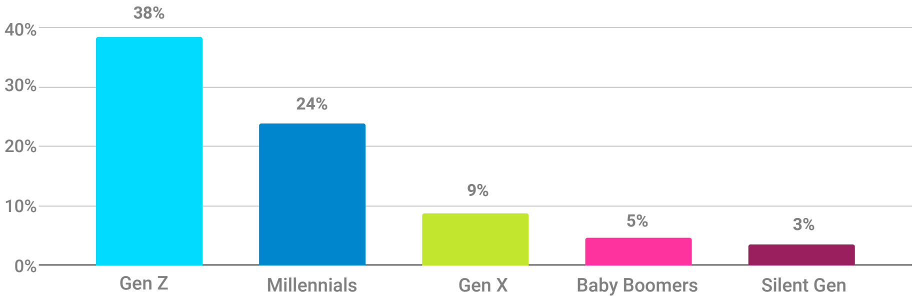


Figure 59. Victim of cyberbullying by generation.

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of cyberbullying victims with generation information 889, dates conducted: April 13, 2023 - April 27, 2023.

Reporting cyberbullying incidents

Many victims reported cyberbullying to various places (Figure 60). The top two options were the police or other authorities (33%) and schools or workplaces (29%). Additionally, 31 percent mentioned they talked about it with their peers or family members. Twenty percent of victims didn't report or mention the incident to anyone.

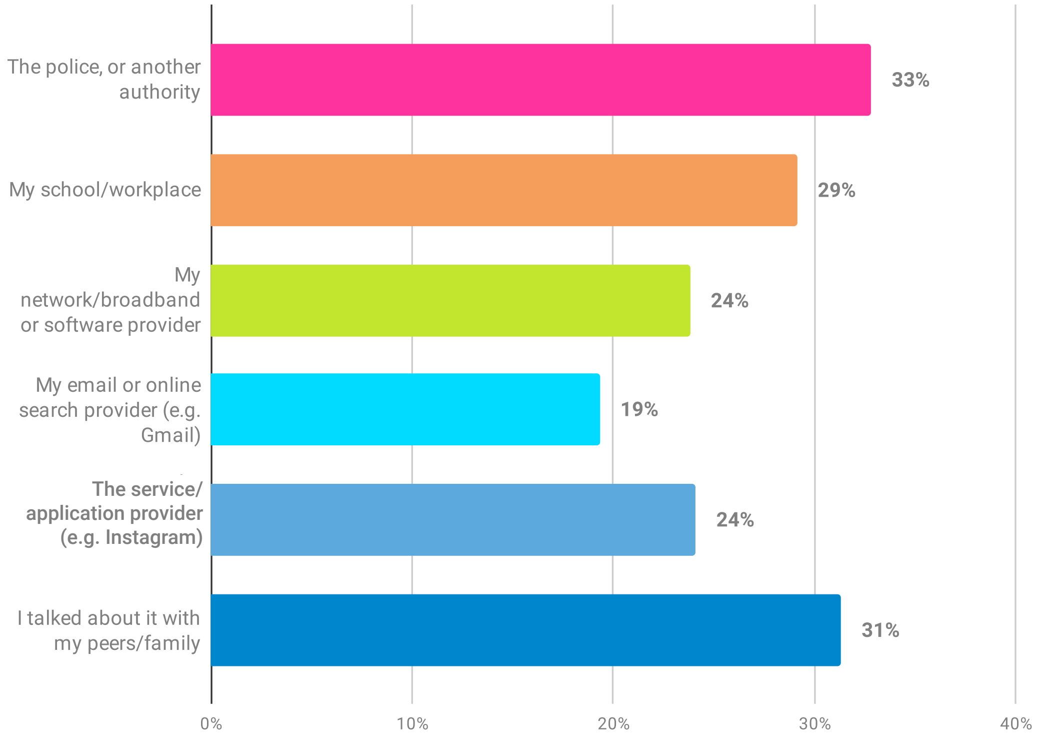


Figure 60. Agencies where cyberbullying is reported to.

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of cyberbullying victims who reported the incident 734, dates conducted: April 13, 2023 - April 27, 2023. Multiple-choice question.

Most cyberbullying victims (85%, N=612[12]) found the reporting process easy, with only 15 percent finding it complicated but managing to find support eventually.

The most common reasons for reporting cyberbullying were to stop the bully (36%, N=734) and they considered it important to notify authorities to prevent it from happening again to them or others (28%). Also, some took action because they wanted to reduce feelings of fear, needed comfort, or felt responsibility to do so.

Among the 187 victims who didn't report the crime, 36 percent felt there was no point as no action would be taken. They also mentioned not knowing who to report the incident to (15%) and feeling ashamed (15%).

[12] This question was asked from those participants who didn't select options 'I talked about it with my peers/family' or 'No, I didn't mention it to anyone'.

Resilience, reporting, and bullying

One thing's clear: helping foster resilience against cybercrimes and cyberbullying is good for business.

Educate
Train everyone on how to recognize and avoid phishing scams, social engineering, cyberbullying and other types of cyber threats. Encourage them to use strong passwords, MFA, and to be wary of suspicious emails or phone calls.

Use protection
Offer protection services (e.g., for identity theft) as a job benefit. These can include credit monitoring, identity guard, and insurance coverage if the worst happens.

Show people how to report cybercrimes
Help people understand the benefits of reporting incidents and suspected incidents.

Support
Provide access to mental health resources and assistance programs.

Establish policies
Lay out what appropriate online behavior looks like and the consequences for breaking the rules.

Create a culture of respect
Celebrate diversity and promote respectful communication and interactions among your team.

Have a plan
Have a plan in place for how to respond. Whatever your plan, make sure that everyone is aware of it and understands their role.

www.cybsafe.com/blog/damage-cyberbullying-does-organizations/

Cybersecurity behaviors and practices

It'll come as a surprise to precisely no one that we're all rocking at least "a couple" of online accounts. As mentioned previously, almost half (47%) of participants are juggling ten or more. So how do they fend off cybercriminals and keep their information, accounts, and devices secure?

Remember those five key cybersecurity behaviors we mentioned in the introduction? Well, hang tight, because in this section we examine the topic through the lens of those all-important elements: ensuring good password hygiene (i.e., creation and strength and password management strategies), using MFA, installing the latest device updates, checking messages for signs of phishing and reporting them, and backing up data.

Password hygiene

Let's look at password hygiene through its three sub-behaviors: frequency of changing passwords, creation of strong and separate passwords, and password management strategies. Here, the National Institute of Standards and Technology (NIST)[13] guidelines for password hygiene are:

- Check passwords against breached password lists (e.g., using the 'haveibeenpwned'[14] 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 have been reflected in all participating countries and/or regions: NCA[15], NCSC's CyberAware[16], Get Cyber Safe[17], CERT NZ[18], and European Union Agency for Cybersecurity (ENISA)[19] guidelines for password hygiene.

Changing passwords

Advice to make regular password changes was once gospel—but no longer. Recent updates to the NIST guidelines[20] have removed this requirement. The new tune? You no longer need to change passwords frequently, which is excellent news for people who find periodical password change requests annoying and struggle to invent unique, new passwords, like anyone who is not a computer. However, old habits die hard, so we were curious to see how deeply rooted this advice is in our collective password hygiene.

[13] https://pages.nist.gov/800-63-3/sp800-63b.html
[14] https://haveibeenpwned.com/
[15] https://staysafeonline.org/online-safety-privacy-basics/passwords-securing-accounts/
[16] https://www.ncsc.gov.uk/blog-post/the-logic-behind-three-random-words
[17] https://www.getcybersafe.gc.ca/en/secure-your-accounts/passphrases-passwords-and-pins
[18] https://www.cert.govt.nz/individuals/guides/how-to-create-a-good-password/
[19] https://www.enisa.europa.eu/topics/incident-response/glossary/authentication-methods
[20] https://pages.nist.gov/800-63-3/sp800-63b.html

Our query was simple: How often do people change their passwords for sensitive online accounts? Over a third (34%) responded they didn't change it unless they had to, which was slightly higher (5%) than the previous year (Figure 61). This was closely followed by 31 percent who changed it every few months, five percent lower than in 2022. Compared to the previous year, the other percentages either remained the same or had minor changes (1%).

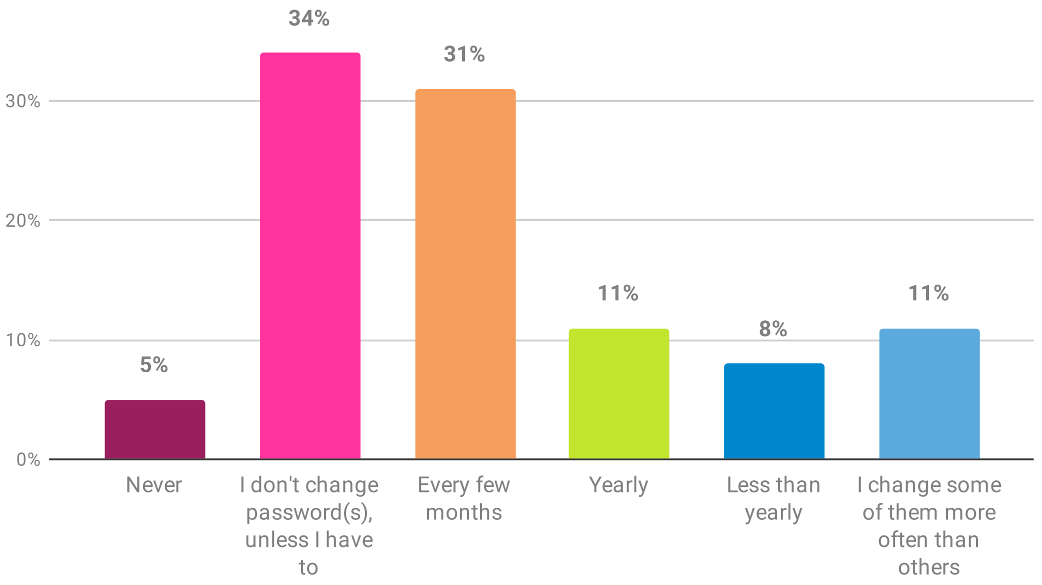


Figure 61. Password change frequency *"How often do you change your passwords?"*

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants: 6064, dates conducted: April 13, 2023 - April 27, 2023.

But what strategies do individuals use to invent their next digital deadbolt? Turns out there's a rich tapestry of approaches. The good news is, almost half (48%) of participants are creative visionaries, using their own techniques and changing their password(s) to something completely different. However, over a third (35%) were feeling less inspired, only changing a few characters or a word in their passwords. These figures closely reflect last year's results.

When examining generational differences, older age groups tend to rely on their own techniques (e.g., 62% of Baby Boomers) in comparison to Gen Zs (34%) and Millennials (35%, Figure 62).

We seem to opt for what is convenient, even if it's a neon-lit invitation to criminals

Over a quarter (26%) of Gen Zs reported using passwords suggested by websites or applications. Also, younger generations appear to engage with more risky password practices, such as only updating characters or a word (37% of Gen Z and 44% of Millennials), in comparison to older generations (27% of Baby Boomers and 26% of Silent Generation). It seems the older generations might have a thing or two to teach whippersnappers about passwords.

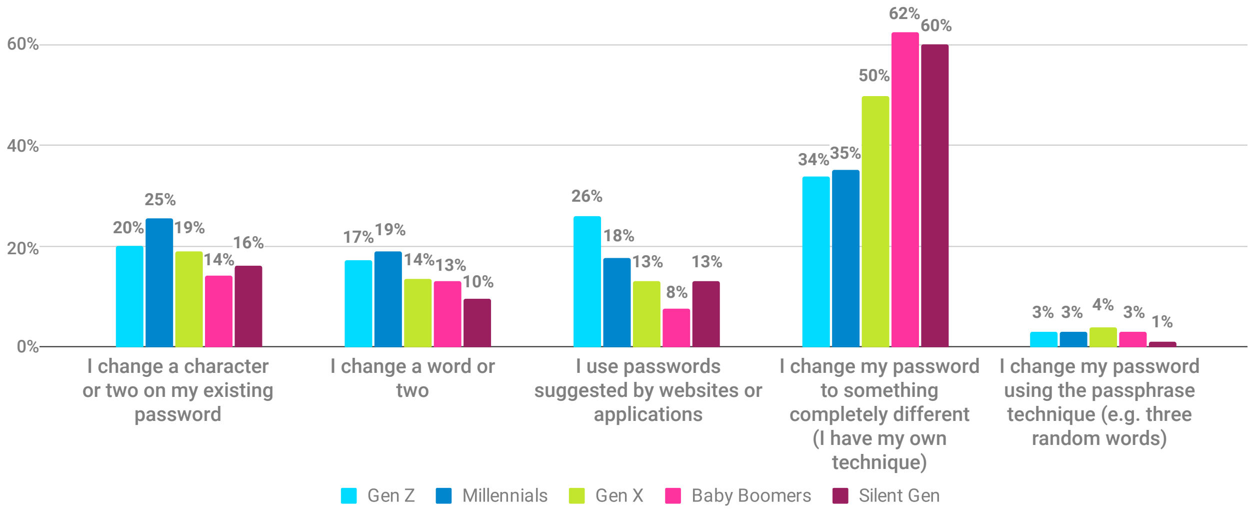


Figure 62. ***"What action do you most often take when changing your password(s)?"*** **by generations.**

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants with generation information and excluding those who 'never' or 'less than yearly' change their passwords: 4983, dates conducted: April 13, 2023 - April 27, 2023.

Using unique and separate passwords

Many of us are creatures of habit. We cling to a handful of memorable phrases and merrily recycle them for every login prompt that comes our way. This can be okay if your phrase is robust enough to withstand a bruteforce bashing. But it doesn't mitigate against credential stuffing. We seem to opt for what is convenient, even if it's a neon-lit invitation to criminals.

Password creation tactics

Reducing risk doesn't have to be rocket science. Building new habits for password creation and management does the job well. Many of the country/region guidelines mentioned earlier recommend using passphrases or "three random words"[21] to conjure up formidable fortifications.

What's more, recent NIST guidelines[22] advise complex passwords don't have to mean swimming in a soup of upper and lower-case letters, numbers, special characters, hieroglyphs, and gang signs. Word.

So, back in the real world, how good are we at using unique passwords for sensitive accounts?

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

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

The majority (76%) of participants claimed they knew how to create unique and strong passwords, and they actively did so. Eighteen percent noted they knew how to create strong passwords, but didn't bother to do so. Maybe for the intoxicating thrill of danger? Who can say. Only six percent mentioned they had no idea how to create unique and strong passwords.

> **Although the length of passwords had somewhat increased, people's tactics for creating passwords appeared slightly less inventive than last year**

So, exactly how do people create their passwords? We asked them to spill the beans about the average length of their passwords and whether they used any personal information or single dictionary words when doing so. We spotted something here: Although the length of passwords had somewhat increased, people's tactics for creating passwords appeared slightly less inventive than last year.

PASSWORD LENGTH

Forty-six percent of participants reported creating passwords between nine and 11 characters long, the same as in 2022. Almost a third (30%) of participants created passwords shorter than this. However, there was a positive change in creating passwords longer than 12 characters. Almost a quarter (24%, N=6064) of participants created long passwords, a promising eight percent increase from last year (2022).

There were some small generational differences. Older participants are more likely to keep their passwords short and sweet (32% of Baby Boomers and 36% of Silent Generation) compared to younger generations (26% of Gen Zs and 28% of Millennials, Figure 63).

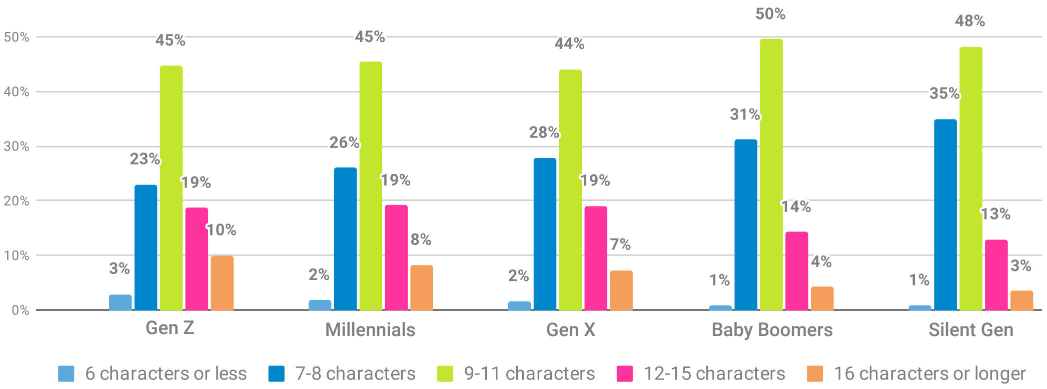


Figure 63. *"How long are the password(s) you usually create?"* by generations.

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants with generation information: 5748, dates conducted: April 13, 2023 - April 27, 2023.

USE OF PERSONAL INFORMATION

Almost a third (32%, N=6064, an increase of 3% from 2022) reported including personal information—names, for instance—when creating their passwords. This tactic appeared to be more popular with younger generations. Half of Gen Z (50%) and 41 percent of Millennials admitted using names of family members or pets, dates, and places when creating passwords (Figure 64). Perhaps it's time to change your pets, folks?

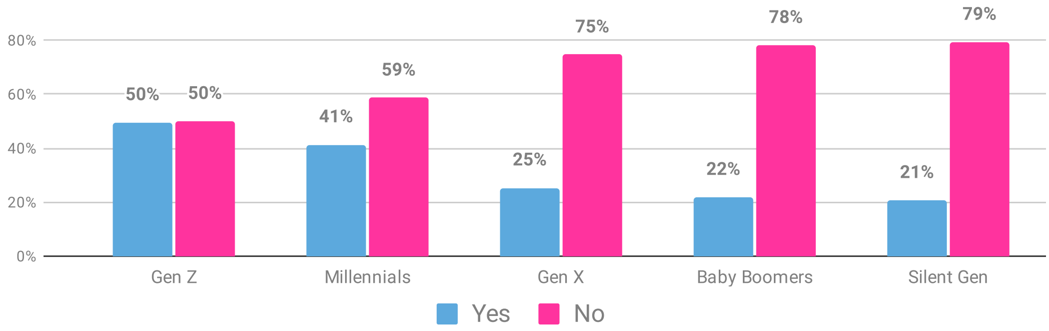


Figure 64. *"Do you tend to create password(s) that include references to personal information? For example, names of family members/pets, dates, and places."* by generations.

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants with generation information: 5748, dates conducted: April 13, 2023 - April 27, 2023.

USING A SINGLE DICTIONARY WORD

Similarly, over a third of participants (34%, N=6064, a 5% increase from 2022) were likely to create passwords using a single dictionary word or someone's name, replacing some of the characters with numbers and/or symbols (e.g., p@ssw0rd or Jon@th4n). Despite the character-swapping shenanigans, these types of passwords are vulnerable to brute-force dictionary attacks.

Younger generations were more likely to use this technique (43% of Gen Zs and 43% of Millennials) than older generations (30% of Gen Xs and 27% of both Baby Boomers and Silent Generation, Figure 65).

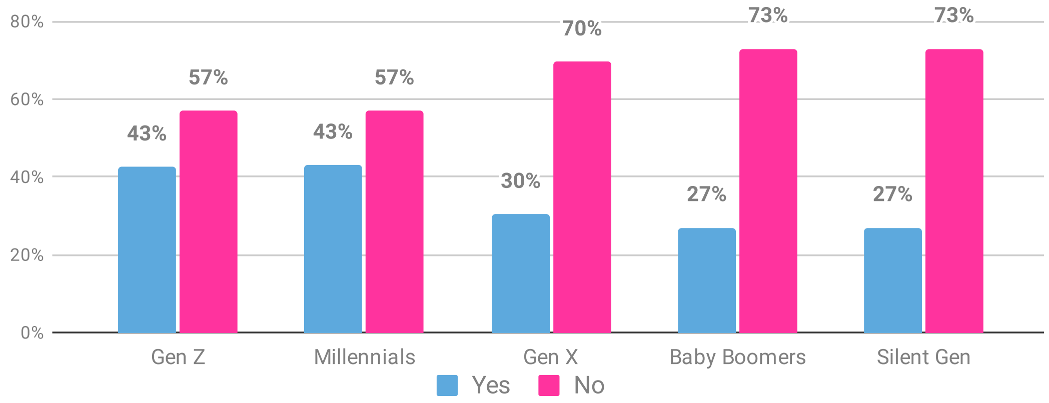


Figure 65. *"Do you tend to create password(s) that are made up of a single dictionary word or name, and you replace some characters with numbers or symbols? For example, p@ssw0rd, Jon@th4n or H0usepl4nt."* by generations.

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants with generation information: 5748, dates conducted: April 13, 2023 - April 27, 2023.

Using separate passwords

A solid 67 percent of participants play it safe by using separate passwords for important online accounts either ‘all of the time’ or ‘the majority of the time’ (an increase of 3% from 2022). However, that remaining third (33%) were less frequent with their use of separate passwords (Figure 66).

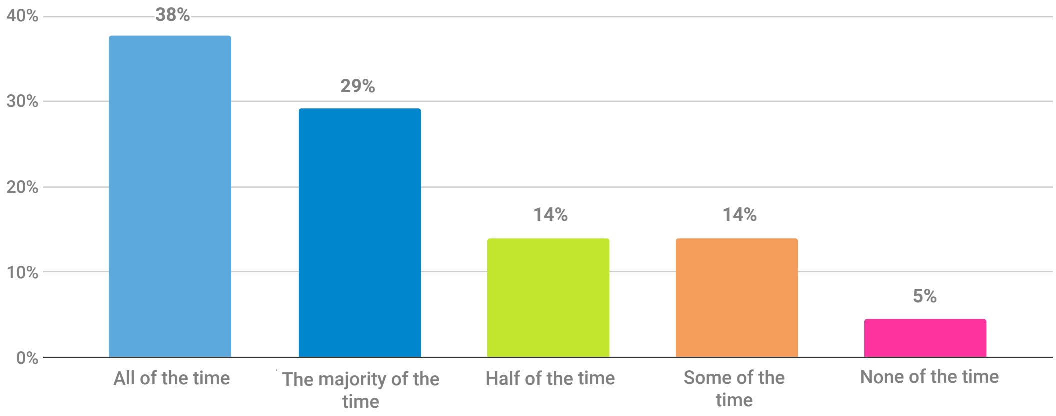


Figure 66. *“How often do you use unique passwords for your important online accounts (e.g., emails, social media, payment-related sites)?”*

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants: 6064, dates conducted: April 13, 2023 - April 27, 2023.

We were curious about those mavericks who were less likely to use separate passwords for their important online accounts (N=1151). The majority (56%) reported difficulty remembering multiple passwords. Another 21 percent mentioned they only used separate passwords for accounts requiring increased security. Additionally, 15 percent mentioned having separate passwords was time-consuming or required extra effort.

Password management strategies

People often have multiple accounts and use various tactics to create passwords, but how do they manage them?

Preferred password management strategies

We asked participants about their preferred techniques for managing passwords and found the favorite technique was writing passwords into a notebook (31%, a decrease of 6% from 2022). Almost a quarter (24%) of participants reported remembering passwords without storing or writing them down anywhere (Figure 67).

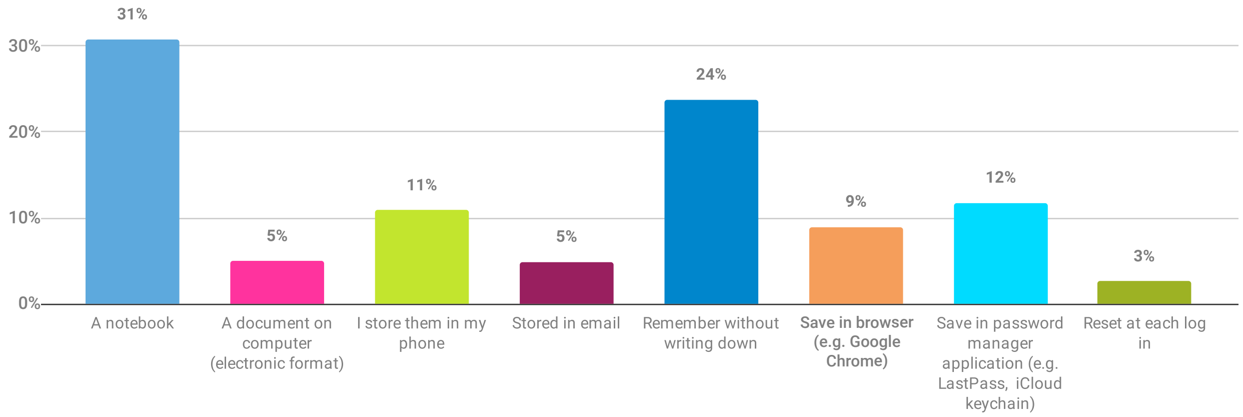


Figure 67. Preferred password management strategies.

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants with multiple passwords: 5403, dates conducted: April 13, 2023 - April 27, 2023.

Generally, most people gave browser or stand-alone password managers the cold shoulder, with only 21 percent of participants actively using them. However, that represents an eight percent increase from 2022. Additionally, three percent of participants admitted resetting their passwords at the login stage, which is a cumbersome management strategy, but not the worst way to do things.

> **I write mine down because if cybercriminals hack your computer, they can get into your password manager.**
> (P3358, United States)

Let's get to those generational observations: 47 percent of Baby Boomers and 59 percent of the Silent Generation used notebooks to record passwords. In comparison, only 18 percent of Gen Z and 19 percent of Millennials did so.

> **I prefer to keep my passwords separate from my computer and phone. There's no way anyone can read my notebook online. I live alone, and no one else can access my computer or notebook. I've been online for 28 years and had a critical account hacked only once because I had a weak password.** (P1122, New Zealand)

For Gen Zs (23%) and Millennials (16%), the preferred ways to manage passwords were to store them on the phone as well as just remember them without writing them down (23% and 27%, respectively).

Use of password manager applications

Based on the low numbers of password management users, we also asked participants whether they had ever used a password manager (e.g., LastPass, iCloud keychain, or a browser-based manager). More than half (56%) reported never using a password manager, with 31 percent noting they currently use one (Figure 68).

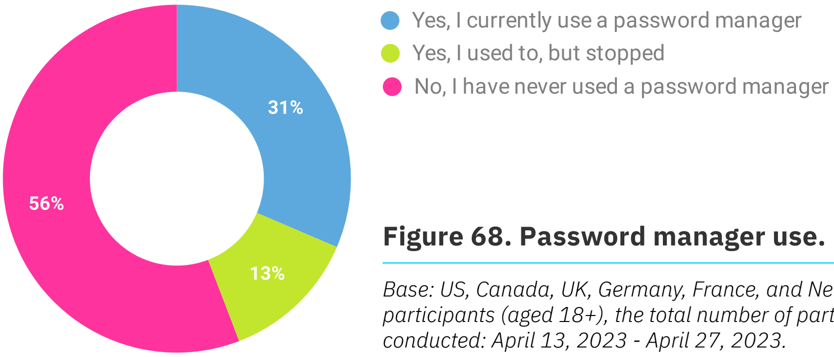


Figure 68. Password manager use.

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants: 6064, dates conducted: April 13, 2023 - April 27, 2023.

Among the 1906 participants who reported using password managers, 38 percent used a free stand-alone password manager, and 39 percent used their Internet browser. Only 23 percent had purchased a stand-alone password manager.

Why are password managers still unpopular?

We asked those not using a password manager (N=4158) why they hadn't jumped in. The top four reasons align with existing research:

1. Too many choices, not enough time. Not knowing which password manager to choose (statement agreed by 46%), known as 'decision paralysis'[23]. With limited attention and time and the lack of motivation to choose from several providers, people tend to stick with their status quo - i,e., nothing. Performing a cost-benefit analysis would take effort.
2. A lack of trust in password managers (statement agreed with by 39%). Recent news coverage around the security of password managers has fueled this view. People think password managers are not secure. But despite these compromises, password managers are still considered to be the safest option.
3. The cost of purchasing a password manager (statement agreed with by 35%).
4. Not understanding how to use a password manager (statement agreed with by 35%).

Simply put, people just don't want to go through the trouble of looking into it, paying for one, or setting it up.

> **A password manager means that cybercriminals only need to gain access to one application and voila! They have all your passwords. That is NOT security.** (P1376, United Kingdom)

[23] Schwartz, B (2004). The paradox of choice. Harper Perennial, New York.

Store all its eggs in the same basket ... and if access to the managers is cracked, all my access is open to the hacker. (P6917, France)

How can you trust who you are giving your information to, it's like giving someone else the keys to your house. (P1176, New Zealand)

The manufacturers are unknown to me. I trust them a little but they are just too expensive for me! The free versions are not fully usable and therefore unusable for me. (P9085, Germany)

Encouraging password manager use

Have researchers uncovered the golden ticket for password manager adoption: catering to the human desire for autonomy and relatedness? People respond positively to a sense of choice and control. So that's likely what any password manager worth its "salt" (see what we did there) should do.

Research[24] also uncovered the power of sharing. Sharing experiences and being able to invite others elicits those warm and fuzzy feelings of relatedness. What's more, it seems receiving referrals from others doesn't undermine that sense of autonomy. Instead, it engages people in a decision-making process where they can follow their own preferences.

The takeaway here is this: Password managers are great. The main idea we should emphasize is the positive message regarding password managers. Not only do they help you craft strong slogans, they also free you from the perpetual dread of forgetting them.

That said, we see the frequent news reports of password managers getting hit for six (that's a cricket reference for "walloped"). We know the struggle is real, and we understand why people would be skeptical. More assurance from password manager companies wouldn't go amiss, they are still the safest option available for most people.

[24] Alkaldi, N. & Renaud, K. (2019). Encouraging Password Manager Adoption by Meeting Adopter. Self-Determination Needs. Proceedings of the 52nd Hawaii International Conference on System Sciences.

Encouraging strong password hygiene

Nudge people
Research has found simply nudging people to create longer passwords (i.e., by adding the word 'long' into instructions) helps people.

Use SSO
Reduce cognitive burden by using Single Sign-On (SSO) wherever possible.

Don't enforce regular password expiry
Regular password changing harms rather than improves security.

Ditch complexity requirements
Forcing people to create "complex" passwords is a poor defense against guessing attacks. It places an extra burden on users, many of whom will use predictable patterns (e.g., replacing the letter 'o' with a zero) to meet the required "complexity" criteria.

Instead, lean into passphrases
Passphrases are significantly easier to remember than complex passwords. They also hold up significantly longer to brute force attacks. The easier and more convenient security is, the more likely people are to follow it.

www.ncsc.gov.uk/collection/passwords/updating-your-approach/
www.staysafeonline.org/online-safety-privacy-basics/passwords-securing-accounts/

Applying Multi-Factor Authentication (MFA)

Nowadays, MFA has become as ubiquitous as that morning cup of coffee, especially when it comes to guarding sensitive data and online accounts.

This year, we added two common terms for MFA to improve its clarity: Two-Factor (2FA) or Two-Step Verification (2SV). This little tweak improved the results from previous years. But here's the kicker: Almost a third (30%) of participants had never heard of MFA (Figure 69). This result was 13% lower than in 2022, showing some promising progress.

Similar to last year's report, we found generational differences. A majority of Gen Z (77%) and Millennials (77%) have crossed paths with the concept of MFA (Figure 70). Compared to the previous year, the number of people who've heard about MFA has increased in each generation (between 9% and 19%, with the highest increase for Millennials). However, it is still common for older generations to have no knowledge of MFA (37% of Baby Boomers and 41% of Silent Generation).

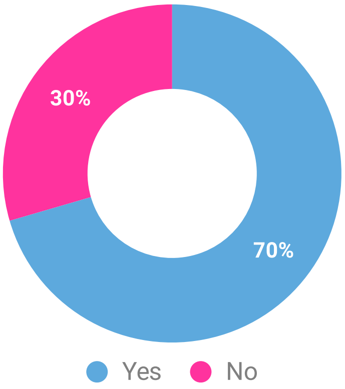


Figure 69. ***"Have you ever heard of Multi-Factor Authentication (MFA)? Also known as Two-Factor or Two-Step Verification."***

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants: 6064, dates conducted: April 13, 2023 - April 27, 2023.

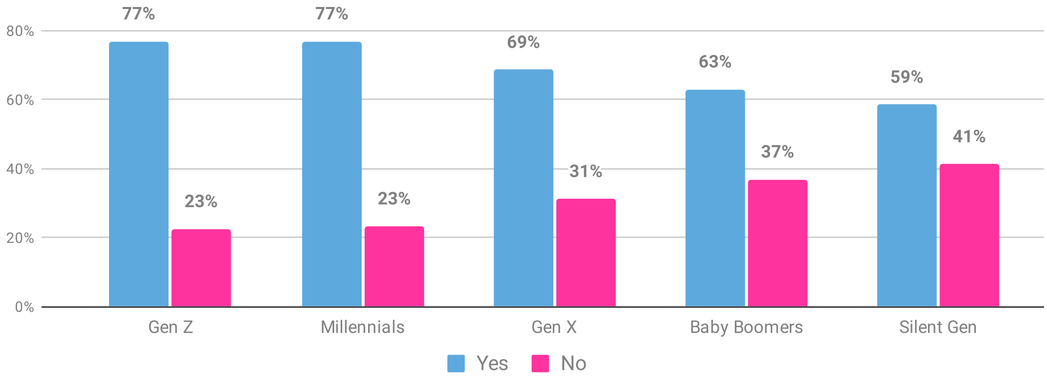


Figure 70. ***"Have you ever heard of Multi-Factor Authentication (MFA)? Also known as Two-Factor or Two-Step Verification"*** **by generations.**

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants with generation information: 5748, dates conducted: April 13, 2023 - April 27, 2023.

Among those who knew what MFA was, 67 percent knew how it worked and were using it regularly. Twenty three percent reported they either don't use MFA or stopped using it despite knowing how to (Figure 71). Yikes.

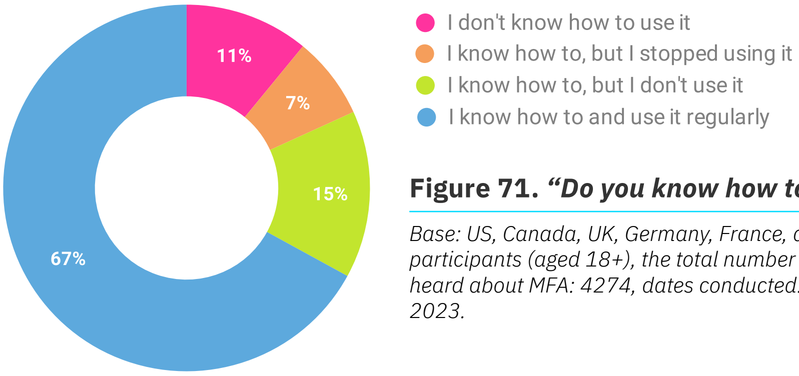


Figure 71. ***"Do you know how to use MFA?"***

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants who had heard about MFA: 4274, dates conducted: April 13, 2023 - April 27, 2023.

Of the 947 participants (7%) who had stopped using MFA, 29 percent said the deal-breaker was that it required carrying their phone with them all the time to be able to verify themselves. They weren't a fan of that idea.

MFA's got to be a breeze if we want people to jump on board

Also, 19 percent considered MFA as inconvenient or burdensome, and another 19 percent reported being locked out regularly thanks to MFA. For 18 percent of participants, MFA was annoying and took too much time. The takeaway here: MFA's got to be a breeze if we want people to jump on board.

Increasing MFA adoption

Prompt first
A simple prompt to set up MFA will sometimes be enough, so don't overlook that as a first step.

Minimize friction
People hate to be inconvenienced, so minimizing hassle is key to making MFA adoption stick. For example, authentication via a text message is more convenient than opening an app.

Purists, pipe down! We know apps are more secure than text messages. If 70 percent of a workforce adopts text-based MFA, vs 40 percent of another workforce adopting app-based MFA, which workforce is more secure overall?

Start with why
Even with a simple task, people need to understand the point of it. You still need to sell the idea. Sell the benefits, sell the "why" (how does it help me), and sell what might happen if they don't engage.

Incentivize
We hope you're sitting down for this next point because it's a real shocker: people like being given things, especially rewards, so there's mileage considering appropriate incentives for adopting MFA.

Foster trust
Gaining trust is crucial; MFA often requires a phone number to authenticate. The concept of "give us more personal data so we can protect your personal data" can, rightly, come across a little contradictory. Fostering a culture of trust and support can be game-changing.

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

Installing software updates

In the tech world, the saying "change is the only constant" rings loud. Software inevitably comes with its share of flaws and vulnerabilities. And a vulnerability is an invitation for cybercriminals to do some of their favorite things.

This is precisely why enabling auto-updates is one of the most effective defenses against cybercrime.

Yet, as the infamous WannaCry[25] ransomware attacks taught us, people and organizations alike often procrastinate or ignore updates. The result? Digital carnage.

> **Ensure you take all reasonable steps to protect your online 'stuff'. Protecting passwords, installing software to protect you from attempts to compromise your online data, and ensuring you always have up-to-date cyber security products installed on all your connected devices.**
> (P1775, United Kingdom).

Knowing how to install updates

Who's keeping their tech up to date? A commanding 65 percent of participants said they know how to install the latest software and application updates across their devices (N=6064). However, 18 percent admitted the opposite, and another 17 percent knew how to, but tended not to install the updates. Proof, if we needed any more of it, that "awareness & education" doesn't always lead to the right behaviors.

The frequency of software and application updates was similar to last year, with 60 percent of participants saying they either 'always' or 'very often' update their devices when notified (Figure 72). However, 215 people (4%) claimed they never updated their devices. Ever.

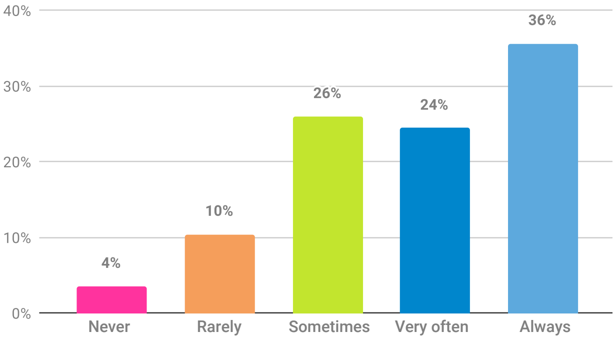


Figure 72. ***"How often do you install the latest software or application updates to your devices when notified that they are available?"***

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants: 6064, dates conducted: April 13, 2023 - April 27, 2023.

[25] https://www.cybsafe.com/blog/wannacry-wont-be-the-last-high-profile-cyber-attack-we-suffer/

Frequency of installing updates

Out of 5217 participants, 45 percent of those who updated their devices more frequently than 'sometimes' did so using automatic updates. Hurrah! Thirty percent took matters into their own hands, opting to manually update their devices upon receiving a notification.

Some participants (17%) admitted to delaying updates with the trusty 'remind me later' button, or ignoring the message a few times. This is a widespread behavior, with the rationale being to cling to productivity in the here and now. However, procrastination means there's a higher chance of facing the very high productivity cost of a potential attack.

Why aren't people enabling auto-updates?

It's all too easy to 'save it for later' ... and then forget about it. Updates aren't exactly thrilling. That means we're quick to undervalue their importance.

So, what were the top three reasons for not performing updates? Among those (N=847) who admitted 'never' or 'rarely' installing them, they were:

> 1. Lack of understanding of how to take action (44% agreed with this statement).
> 2. Lack of confidence in their ability to update devices (43% agreed with this statement).
> 3. They believe they have to pay for the updates they cannot afford (41% agreed with this statement).

Furthermore, a significant group (to the tune of 39%) claimed they didn't have time to check the latest updates. The age-old productivity vs. security debate is alive and well.

Updating devices

Take away choice
Humans are predisposed to "go with the flow", so auto-updates are presented as the default option, people are more likely to enable them. It's a small but effective behavioral 'nudge' that can be easily adopted in any organization.

Test, test, and test again
Make sure to test updates before roll-out. When updates cause issues for people, they are less likely to update in future for fear of more problems.

Carve out time for updates
Give people the option to install updates during specific times, like the last 10 minutes of the day, or during lunch breaks.

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

Backing up data

Backing up data. It can stand between us and a world of pain. File corruption, hardware fails, cyberattacks, and physical disasters like fires and flooding.

Knowing how to back up data

After recovering from the initial shock of losing data, we tend to ask a simple question: 'Was the data backed up?'.

The good news is 56 percent of participants said they had the back-up know-how and weren't afraid to use it. On the contrary, 24 percent stated they didn't know how to back up their data, with some even asking, "What do you mean by 'backups'?". Worryingly, 19 percent said they knew how to perform backups but admitted to not doing so.

Backing up data frequency

Shifting our gaze to how often people backed up data, we found the 2023 situation closely reflected last year's. Under half (42%) of participants reported performing frequent backups (i.e., 'very often' or 'always'). Over a quarter (26%) stated they 'never' or 'rarely' perform backups, or lack the know-how (Figure 73).

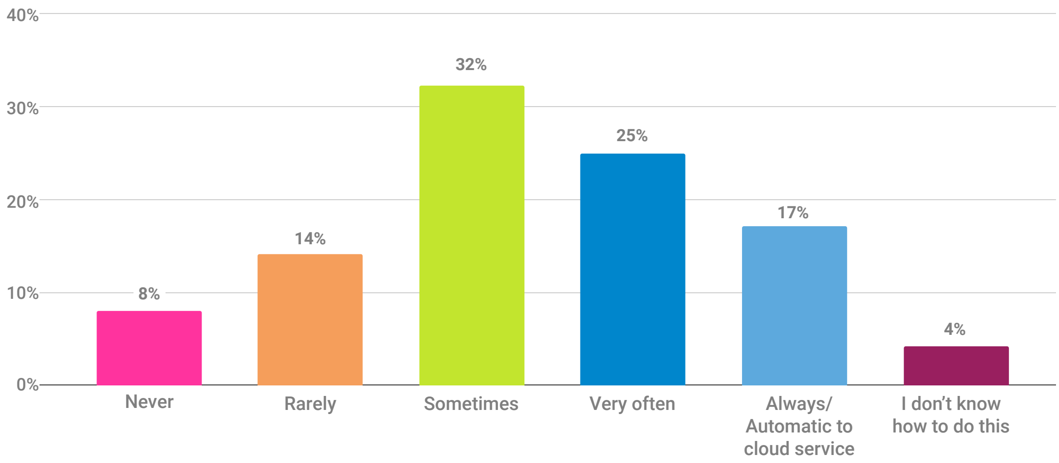


Figure 73. ***"How often do you back up your most important data?"***

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants: 6064, dates conducted: April 13, 2023 - April 27, 2023.

Why aren't people backing up data?

Good question. Despite some people's love of BASE jumping, bull riding, and bobsleighing, on the whole we're hardwired to avoid danger. So, we asked the thrill seekers who indicated they 'never' or 'rarely' perform backups (N=1305), "why?"

The top three reasons were:

1. Not knowing which cloud service to use (50% agreed with this statement).
2. Lack of understanding of how to perform backups (44% agreed with this statement).
3. Inability to afford an external hard drive or subscribe to a cloud service (43% agreed with this statement).

Boosting backups

Remove the burden
Look to solutions that automatically backup. Cloud services are the most convenient—and that means they're the most likely to be adopted. Cloud storage is not 100% secure, but it saves you from bigger risks than it presents.

Highlight the ease
People are more likely to adopt automatic backups if they understand how easy and convenient it is. In comparison, threat appraisal is shown to be less effective at influencing adoption of backups—although people who feel vulnerable to data loss are likely to make use of it.

3-2-1, backup!
We like the 3-2-1 rule for sensitive data. Make three backups, over two devices, and keep one offsite. Provide encrypted flash drives to employees to reduce barriers to adopting this behavior.

Backup culture
Make auto-backup part of your culture. A no-brainer set-and-forget. Something you can't afford not to do. Praise those who do. And remind those who don't—regular monthly emails asking people, "Have you backed up your data recently using cloud or removable storage?" work well.

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

Recognizing and reporting phishing messages

Phishing attacks are a certified menace. What's more, they're still on the rise.

Cybercriminals have been putting in the hours over the past few years. But it's worth their while, because they're catching valuable data.

Criminals are getting more sophisticated and creative. Every. Darn. Day. Yes, the good old traditional phishing email still snags its fair share of people, but there are always new bells and whistles being whipped up. Thanks, ChatGPT.

> **It is important to keep your personal info from getting away from you. You need to disregard/delete links that you don't recognize.** (P2168, United States)

Recognizing phishing

Some phishing attacks are rudimentary. With their typos, grammatical gaffes, pixelated logos and conspicuous twists on sender names, they should stick out like sore thumbs, no?

A considerable number of participants (63%, N=6064) reported a high ability to recognize phishing in email and messaging platforms. However, over a quarter (26%) either didn't know how to recognize (18%) or didn't know what phishing was (8%), leaving many people vulnerable to phishing tactics.

> **The scams are so broad, you never know which emails are real.** (P2141, United States)

CONFIDENCE IN ONE'S ABILITY TO RECOGNIZE PHISHING MESSAGES

Overall, participants reported high confidence in their ability to recognize phishing emails or malicious links (M=6.96, SD=2.29, N=6064, as reported on a 10-point scale). Specifically, 66 percent of participants expressed their confidence in their abilities, but 13 percent (a 5% increase from 2022) reported feeling uncertain in their ability to identify phishing emails or malicious links (Figure 74).

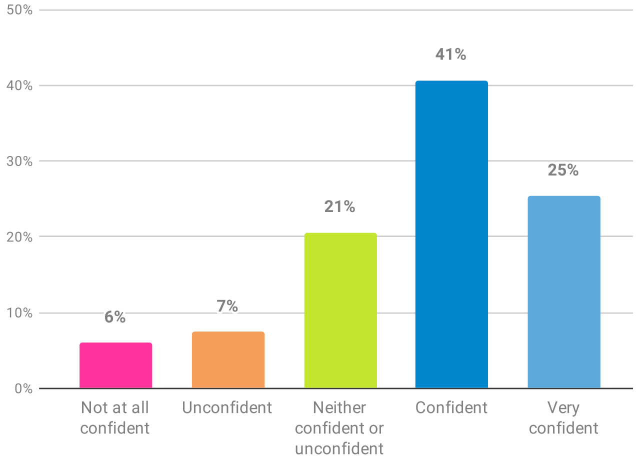


Figure 74. ***"How confident are you in your ability to identify a phishing email or a malicious link?"***

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants: 6064, dates conducted: April 13, 2023 - April 27, 2023.

Dare we say it? Is people's self-reported confidence in their ability to recognize phishing emails similar to the 93% of motorists who judge themselves 'above average' at driving?

Millennials felt most confident identifying malicious messages, with 70 percent declaring themselves cyber sleuths extraordinaire. Gen X is no slouch either at a respectable 68 percent. Meanwhile, older generations were overall less confident (i.e., 20% of the Silent Generation and 17% of Baby Boomers).

I'm doubtful in my ability to recognize phishing messages because:

> **...I am quite young and not tech savvy.** (P2495, United States)

> **Phishing techniques can be very sophisticated and criminals disguise these, I am also often rushing!**
> (P4080, United Kingdom)

> **...The people sending the emails or malicious links are getting more sophisticated and are continually coming up with better scams that are more difficult to detect.**
> (P1379, United Kingdom)

CHECKING MESSAGES FOR SIGNS OF PHISHING

Sixty-seven percent reported they 'very often' or 'always' check whether messages (e.g., emails, texts, or social media) are genuine before clicking any links or responding to them (Figure 75). However, 14 percent reported they 'never' or 'rarely' do so, a four percent increase from 2022.

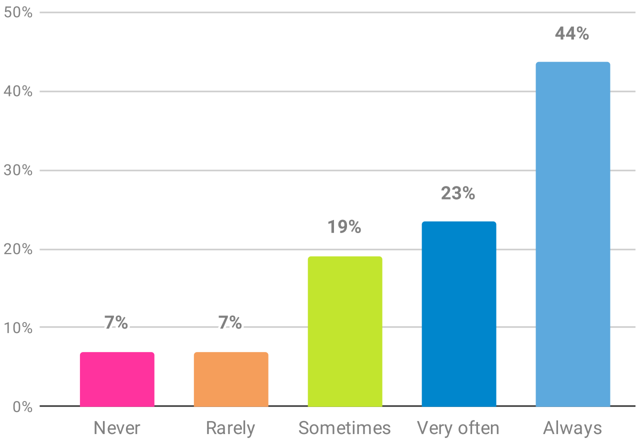


Figure 75. Frequency of checking messages for signs of phishing before taking action.

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants: 6064, dates conducted: April 13, 2023 - April 27, 2023.

How do people recognize phishing messages compared to genuine ones?

Over half (54%) tend to check the sender's email address using the 'From:' line, and 29 percent rely on spotting scams because of content and spelling errors (Figure 76). Only 14 percent report hovering over the links in the email to check the real link destinations.

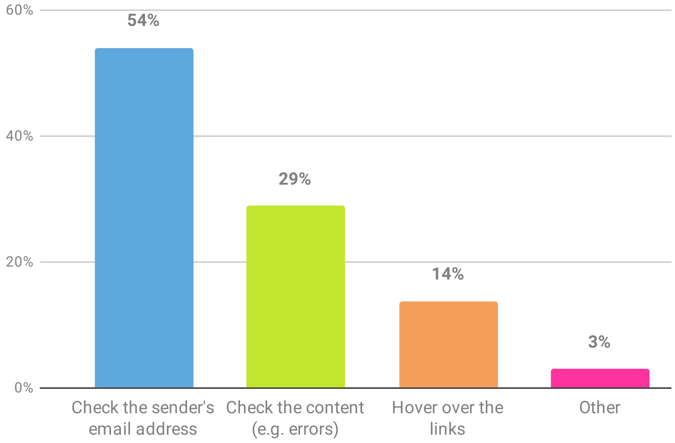


Figure 76. *"What is your first action to ensure a message is not phishing?"*

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants who reported checking messages for signs of phishing more often than 'sometimes': 5223, dates conducted: April 13, 2023 - April 27, 2023.

While it's important to be able to spot phishing messages and malicious links, it's also crucial to check with the sender if they did indeed send the message—and alert them if they didn't. A third (32%, up by 4% from 2022) admitted to 'never' or 'rarely' reaching out to the person who they thought the message was from. Ominously, and by contrast, 44 percent reported contacting the sender either 'very often' or 'always' (Figure 77).

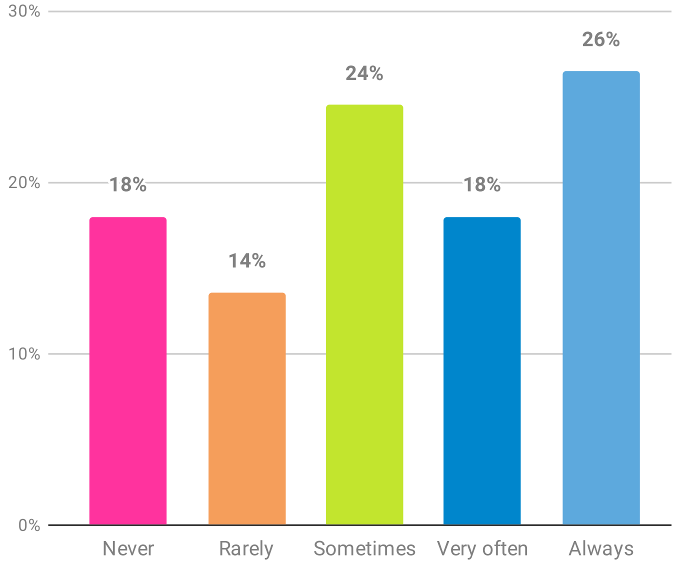


Figure 77. *"If someone you know sends you a message you're unsure of (a potential phishing message), how often do you reach out to the person to ask about it before you click the link or open the attachment?"*

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants: 6064, dates conducted: April 13, 2023 - April 27, 2023.

Reporting phishing messages

Confronting phishing attempts head-on may not always be the best course of action. Luckily, 'spam' and 'report phishing' buttons are built into email and social media tools, meaning it's quick and easy to flag up criminal concerns.

Despite their convenience, only 44 percent of us report making use of them 'very often' or 'always' (a 3% decrease from 2022, Figure 78). If we combine those who couldn't locate reporting buttons and those who didn't have the know-how (8%), together with people who 'never' or 'rarely' report phishing attacks (25%), this results in a cool one-third (33%) of participants who are not taking action against cybercriminals.

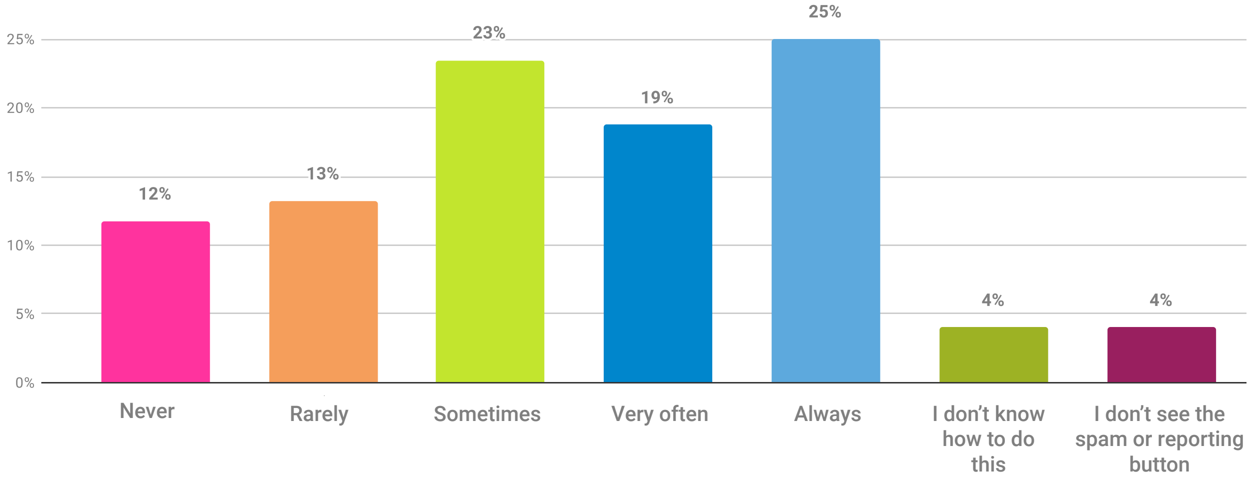


Figure 78. ***"How often do you report phishing messages by using the 'spam' or 'report phishing' button?"***

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants: 6064, dates conducted: April 13, 2023 - April 27, 2023.

Why aren't people reporting phishing attempts?

So, what's the snag? A staggering 72 percent of participants[26] believe reporting phishing does not stop cybercriminals. Those who 'never' or 'rarely' reported phishing messages mentioned they would do so if:

1. It would stop spam messages from getting into their inbox (68% agreed with this statement).
2. Something would happen when reporting them (62% agreed with this statement), like an acknowledgment.
3. They had more trust in the reporting process (58% agreed with this statement).

[26] N=1513 who 'never' or 'rarely' report phishing messages.

Staying safe from phishing

Train people to spot the signs of phishing
If you receive an email you weren't expecting, ask yourself:

1. Do the 'From:' details match the sending details?
2. Does it ask you to carry out an action you wouldn't usually do?
3. Does it include a link or attachment you don't recognise?

Measure more than click rates, report rates, and dwell times when simulating
Measure why people click on simulated phishing emails. This can be done with point-of-click surveys, post-click surveys, or by baking influencing techniques into simulated phishing templates. Follow up with tailored support based on the data.

Create an environment that encourages reporting
Have a quick, frictionless process for users to report. Quickly provide acknowledgement of the report and feedback on what action is taken. Avoid creating a punishment or blame-oriented culture around phishing—such as assigning training to people who click on simulates.

🔗 www.cybsafe.com/value/simulated-phishing/
🔗 www.staysafeonline.org/theft-fraud-cybercrime/phishing/
🔗 www.ncsc.gov.uk/guidance/phishing

Conclusion

Security fatigue is real

Security vs. productivity

Generational challenges

The role of the media

Cybersecurity training

Conclusion

There you have it. A global snapshot of people's cybersecurity attitudes and behaviors. What have we uncovered?

Amongst examining people's perceptions and attitudes towards online security, cybercrime victimization, and cybersecurity training, we looked at five critical security behaviors: password hygiene; using MFA; installing the latest updates; backing up data and staying safe from phishing scams.

This year's survey was conducted globally. Our findings show consistent trends in people's attitudes and behaviors towards cybersecurity. We're confident they are reflected across most—if not all—of the Western working world.

Security fatigue is real

We're online. A lot. People of all ages have multiple online accounts. This means we are very exposed to cybersecurity risks - with or without our knowledge - and have to make constant decisions about how to stay secure online.

As noted by researchers[27], this can lead to 'security fatigue', with people becoming desensitized to the dangers of the Internet. Indeed, our data shows people feel somewhat helpless when it comes to losing money or personal details online. The loss of control, together with belief in one's ability to take protective action (i.e., self-efficacy) are important psychological factors.

For people unfamiliar with security, protecting themselves can seem overwhelming. Indeed, this sentiment was echoed by over half of our sample, who felt it was pointless to protect themselves.

Feelings of resignation and loss of control associated with cybersecurity behaviors present a challenge to security awareness activities. More personalized and hands-on approaches can help people take steps to make security usable, and relevant:

> 1. Limit the number of security decisions people have to make (e.g., using SSO so people don't have to remember multiple passwords).
> 2. Simplify and make it easy for people to take protective cybersecurity action.
> 3. Make sure advice is consistent, that it doesn't confuse people, and that it doesn't introduce unnecessary friction to people's work.

[27] Furnell, S. & Thomson, K.L. (2009). Recognising and Addressing 'Security Fatigue,' Computer Fraud and Security, 7–11.

The above points are correlated to our human tendency of being a 'cognitive miser'[28]. We tend to rely on simple rules to make decisions as we are limited in our cognitive resources, such as time, knowledge, attention, and memory—regardless of our intelligence.

Security vs. productivity

Research supports the role of situational factors, such as the compliance budget[29] in cybersecurity. Engaging with security is a delicate balance between its perceived benefits and costs to individuals and businesses.

At the individual level, cybersecurity is often related to a loss of time and mental effort, which can impact productivity (especially in the workplace) and monetary costs (e.g., buying a stand-alone password manager). If security measures hinder people's primary goals (like logging into email, using social media, completing work tasks, making payments, etc.), they are less likely to take protective cybersecurity measures.

We observed the security-productivity seesaw with key security behaviors, including backing up data, MFA, and password management strategies.

When it comes to backing up data, cost is a recurring issue. People mentioned they cannot afford to buy external hard drives or subscribe to cloud services. Many people expect these services to be unlimited, and free.

While most people know what MFA is, many still don't use it to secure accounts. They perceive it as an inconvenience to require another device, such as a phone, to be available at all times to work effectively. Having SMS-based MFA also relies on owning a mobile phone and having a good mobile network signal, which in some remote - and even some cities - locations around the world is not necessarily a given.

In addition, some MFA methods rely on authenticator applications and, similar to password managers, can elicit issues of trust and 'decision paralysis'. Put simply, when security doesn't work for people, it doesn't work. Our primary task, such as sending the email or making a payment, will happen even in unsafe environments.

When it comes to passwords, people prefer their own methods, like writing them down in notebooks. They do not trust having all their passwords sit within one tool, especially given the recent media attention on password managers failing to protect users. Additionally, people do not want to spend time researching the best options, setting up, or paying for a password manager. Security just isn't viewed that importantly in their lives.

[28] Fiske, S.T. & Taylor, S.E. (1991). Social Cognition (2nd ed.). New York: McGraw-Hill.

[29] Beautement, A., Sasse, M. A., & Wonham, M. (2008, September). The compliance budget: managing security behaviour in organisations. Proceedings of the 2008 New Security Paradigms Workshop (pp. 47-58).

Generational challenges

We observed positive attitudes towards online security, with people considering it an achievable priority, and worthwhile. However, online security also intimidates and frustrates many individuals, despite their good intentions. Intention to change behavior doesn't always result in action.

Many were concerned about falling victim to cybercrime, with around half admitting they were likely targets for criminals. Even so, some, like Gen Zs, tended to have a "laissez-faire" attitude towards online security. They don't prioritize online security as much as older generations, and half didn't think staying safe online was worth their effort.

Digital natives felt overwhelmed by the amount of information, leading to a tendency to minimize their actions online. However, whether they minimize their actions sufficiently is up for debate as cybercrime among Gen Z and Millennials was noticeably higher than other generations.

Some held application providers and device manufacturers responsible for online security, assuming their devices should be out-of-the-box secure. Some feel online security is expensive, while others have come to accept losing data or money over the Internet is unavoidable.

The role of the media

We were always online, exposed to various media streams. Many people felt scared. For others, media coverage increased their motivation to take action to protect themselves.

Catastrophizing platforms or organizations failing to protect data or money without explaining why it happened and what it means to an average citizen is not helpful. It can lead to people miscalculating risks, simply because it has been in the news recently (i.e., availability bias). To the contrary, if the incident had never been reported by the media, then people might think it is not very likely.

Media organizations frequently scare people (just search "prospect theory" to see why). News headlines containing negative language are significantly more likely to be clicked on than those with positive wording. It sells ad space. But these breaking stories also represent opportunities to give people the advice, information, and tools needed to stay safe themselves online. There is opportunity to do better.

Cybersecurity training

It’s widely assumed those in active employment have high exposure to cybersecurity training. This appears closer to “fifty-fifty”.

Retired individuals or those not in active employment remain vulnerable as they report little to no access to training resources. The internet has no shortage of high-quality, free content. Perhaps the thing to note here is it’s not being publicized enough to the right audiences?

Online cybersecurity training was preferred overall, and those who had completed courses found training content useful and engaging, whether learning at home or in work environments. Of note,we’re starting to see more people opt for different strategies to engage with security, such as being provided with timely notifications or alerts when making decisions that can put them at risk.

That’s a wrap!

2023 marks 20 years of Cybersecurity Awareness Month. While we’ve come a long way since the early 2000s, we still have work to do to help people stay safe online. We—the team responsible for this third Annual Cybersecurity Attitudes and Behaviors Report—will continue our efforts to make our interconnected safer. We hope this year’s edition has given you food for thought.

Until next year...that’s a wrap!

Appendices

Appendix A: Methodology

Survey design

The survey was designed to explore five cybersecurity behaviors: ensuring good password hygiene, using MFA, installing the latest device updates, performing data backups and checking messages for signs of phishing and reporting them.

Most of the survey included multiple- or single-choice questions with 5- or 10-point Likert scales with written options (e.g., 'all of the time' to 'none of the time') or two anchor points (e.g., 'strongly disagree' to 'strongly agree'). Also, qualitative questions with an essay text box were added to the survey. This was to gather people's views on what comes to their minds when they hear "online security". However, limited questions requiring text-based responses were included in the rest of the survey with exceptions to some questions including an option 'other, please specify'.

Participants from New Zealand (N=1064) were not asked to fill in their exact age, but were given age brackets as options. Therefore, some participants were excluded from generation-based calculations (N=316) to ensure age brackets for New Zealand best matched the other countries.

Procedure

A call for participation was placed by the Toluna[30] platform for the United States, Canada, the United Kingdom, Germany and France. For New Zealand, the call for participation was carried out by the CERT NZ. Participants could respond to the survey in their preferred language according to country (i.e., French for Canada/France, 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 didn't collect any personally identifiable information.

All data collection was conducted between April 13th, 2023, and April 27th, 2023.

The survey was designed to be completed in under 30 minutes. The average time participants spent completing the survey was approximately 22 minutes[31].

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

[31] This excludes New Zealand whose survey provider didn't provide duration of survey completion.

Sample

A representative sample (based on gender and age) was recruited by the survey provider Toluna. CERT NZ also ensured a representative sample for New Zealand. All of the participants were above 18 years of age.

Table 2 describes the demographics for the survey sample. Those countries sampled by Toluna had 1000 participants per country, and New Zealand had a sample size of 1064, which brings the total survey sample size to 6064 participants.

For generational counts, we had to exclude those people from New Zealand who didn't fit into any of the generation brackets. Thus, 316 people from New Zealand were excluded from the generational data analysis.

This year, our data had similar proportions of Millennials (28%), Gen X (28%) and Baby Boomers (29%). Gen Z (13%) and Silent Generation (2%) were represented less, although there were still 749 people, who were between 18 and 26 years old.

The majority (66%) of participants reported being in some type of employment (whether full- or part-time, including students who were working). This year, just over a third (34%) reported not being employed (including 22% of retired participants).

Over half of the participants (52%) didn't hold a university degree, and of those who did, 30 percent had completed an undergraduate degree (Table 3).

Demographic		United States (N=1000) % within country of residence	Canada (N=1000) % within country of residence	United Kingdom (N=1000) % within country of residence	Germany (N=1000) % within country of residence	France (N=1000) % within country of residence	New Zealand (N=1064, except for age N=748) % within country of residence	Total (N=6064) % within country of residence
Gender (N=6064)	Female	514 (51.4%)	503 (50.3%)	529 (52.9%)	506 (50.6%)	516 (51.6%)	587 (55.2%)	3155 (52.0%
	Male	486 (48.6%)	487 (48.7%)	465 (46.5%)	493 (49.3%)	484 (48.4%)	473 (44.4%)	2888 (47.6%)
	Non-binary / third gender	0 (0.0%)	8 (0.8%)	4 (0.4%)	1 (0.1%)	0 (0.0%)	4 (0.4%)	17 (0.3%)
	Prefer not to say / Prefer to self-describe	0 (0.0%)	2 (0.2%)	2 (0.2%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	4 (0.1%)
Age (N=5748)	Gen Z (18-26)	159 (15.9%)	122 (12.2%)	135 (13.5%)	107 (10.7%)	130 (13.0%)	96 (12.8%)	749 (13.0%)
	Millennials (27-42)	283 (28.3%)	278 (27.8%)	278 (27.8%)	245 (24.5%)	246 (24.6%)	259 (34.6%)	1589 (27.7%)
	Gen X (43-58)	268 (26.8%)	268 (26.8%)	285 (28.5%)	287 (28.7%)	307 (30.7%)	190 (25.4%)	1605 (27.9%)
	Baby Boomers (59-77)	249 (24.9%)	301 (30.1%)	282 (8.2%)	344 (34.4%)	310 (31.0%)	203 (27.2%)	1689 (29.4%)
	Silent Generation (78+)	41 (4.1%)	31 (3.1%)	20 (2.0%)	17 (1.7%)	7 (0.7%)	0 (0.0%)	116 (2.0%)
Employment Status (N=6064)	Employed (%)	650 (65.0%)	625 (62.5%)	631 (63.1%)	665 (66.5%)	650 (65.0%)	687 (64.6%)	3908 (64.4%)
	Full-time	512 (51.2%)	500 (50.0%)	468 (46.8%)	508 (50.8%)	557 (55.7%)	517 (48.6%)	3062 (50.5%)
	Part-time	138 (13.8%)	125 (12.5%)	163 (16.3%)	157 (15.7%)	93 (9.3%)	170 (16.0%)	846 (13.9%)
	Students (%)	52 (5.2%)	43 (4.3%)	40 (4.0%)	42 (4.2%)	54 (5.4%)	39 (3.6%)	270 (4.5%)
	Not working	26 (2.6%)	24 (2.4%)	24 (2.4%)	25 (2.5%)	35 (3.5%)	23 (2.1%)	157 (2.6%)
	Working student	26 (2.6%)	19 (1.9%)	16 (1.6%)	17 (1.7%)	19 (1.9%)	16 (1.5%)	113 (1.9%)
	Retired (%)	237 (23.7%)	222 (22.2%)	225 (22.5%)	232 (23.2%)	225 (22.5%)	187 (17.6%)	1328 (21.9%)
	Don't work or study outside home	61 (6.1%)	110 (11.0%)	104 (10.4%)	61 (6.1%)	71 (7.1%)	151 (14.2%)	558 (9.2%)

Table 2. Participant demographics by country.

Education level	United States (N=1000) % within country of residence	Canada (N=1000) % within country of residence	United Kingdom (N=1000) % within country of residence	Germany (N=1000) % within country of residence	France (N=1000) % within country of residence	New Zealand (N=1064) % within country of residence	Total (N=6064) % within country of residence
Some school/ High school credit, no diploma or qualification	57 (5.7%)	69 (6.9%)	52 (5.2%)	2 (0.2%)	44 (4.4%)	2 (0.2%)	226 (3.7%)
Primary/ secondary education (e.g., GCSEs/ A-levels/ High School Diploma/ GED)	278 (27.8%)	215 (21.5%)	316 (31.6%)	200 (20.0%)	300 (30.0%)	316 (29.7%)	1625 (26.8%)
Trade, technical or vocational training (e.g., BTEC/ HND/NVQ Diploma/CTE qualification)	104 (10.4%)	245 (24.5%)	186 (18.6%)	463 (46.3%)	105 (10.5%)	145 (13.6%)	1248 (20.6%)
Undergraduate degree (e.g., Associates/ Bachelors)	392 (39.2%)	347 (34.7%)	307 (30.7%)	161 (16.1%)	216 (21.6%)	397 (37.3%)	1820 (30.0%)
Postgraduate degree (e.g., Masters/PhD)	144 (14.4%)	98 (9.8%)	121 (12.1%)	109 (10.9%)	296 (29.6%)	174 (16.4%)	942 (15.5%)
Professional degree (e.g., MD/DDS/JD)	25 (2.5%)	26 (2.6%)	18 (1.8%)	65 (6.5%)	39 (3.9%)	0 (0.0%)	173 (2.9%)
Prefer not to say	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	30 (2.8%)	30 (0.5%)

Table 3. Participants' education levels by country.

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. The survey included two attention checks to exclude potential 'bots' and participants who were just clicking through the survey without reading the questions.

Seventy-five participants completed the survey in four minutes or less, so an additional check was done to confirm whether these participants properly engaged with the survey[32]. Several of these responses were checked for validity (e.g., if they claimed not to know how to create strong passwords but subsequently indicated they create strong passwords for all their online accounts). The responses were deemed to have an acceptable error rate and were retained for analysis.

Data analysis

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.

[32] Checks were done randomly for New Zealand participants.

Appendix B: Country comparisons

This section examines country-wise differences between the United States, Canada, the United Kingdom, Germany, France, and New Zealand regarding attitudes and behaviors towards cybersecurity, access to training and cybercrime victimization[33]. In particular, we focused on the areas of difference between the six countries. We were keen to examine whether cultural differences influenced values and decision-making capabilities.

Country differences in online presence

Participants in North America (55% of Americans and 56% of Canadians) as well as New Zealanders (59%) report being 'always connected' in comparison to Europeans (i.e., 38% of Germans, 40% of French and 50% of British participants, Figure 79).

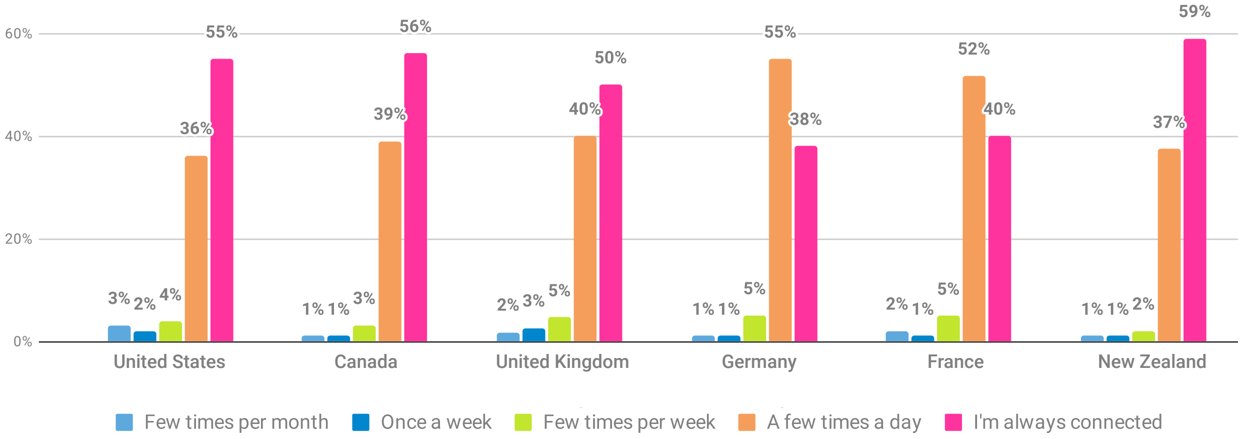


Figure 79. Use of the Internet by countries: *"How frequently do you use the Internet?"*

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants: 6064, dates conducted: April 13, 2023 - April 27, 2023.

[33] From this point onwards participants from United States will be referred to as 'Americans', participants from Canada as 'Canadians' and participants from New Zealand 'New Zealanders'.

Country differences in cybersecurity attitudes

There were very few differences between the countries on attitudes towards online security.

Whereas New Zealanders (81%) agreed with online security being a priority, this was lower than for North Americans (88% of Canadians and 87% of Americans, Figure 80). Online security being viewed as something 'achievable' was lowest for French participants (63% agreed with the statement) and New Zealanders (67%) in comparison to other countries (agreements ranging between 70% and 72%).

The most considerable attitudinal differences between the countries were concerning feelings of frustration. Here, almost half of British participants (48%) viewed online security as frustrating, whereas New Zealanders (30%) and French participants (31%) were the least frustrated by it.

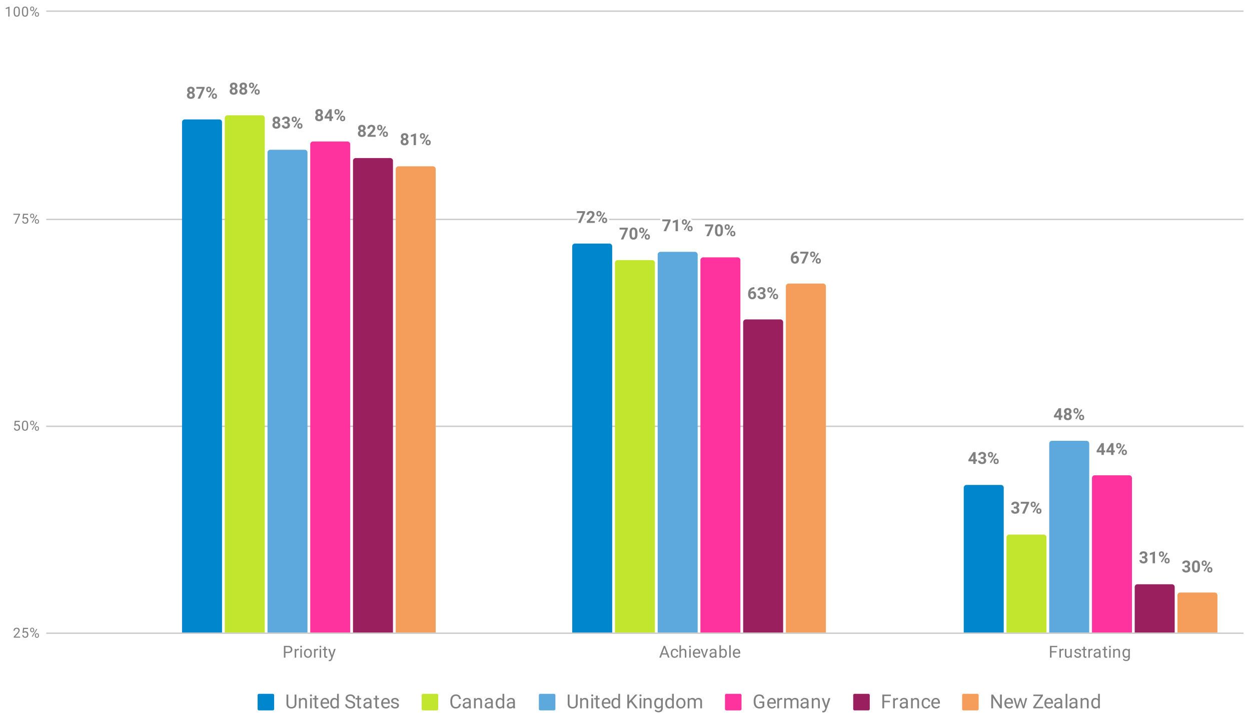


Figure 80. *"I feel that staying secure online is..."* percentage agreed by country.

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants: 6064, dates conducted: April 13, 2023 - April 27, 2023. Graph shows only 'agreed' statement data.

Germans reported being most at ease with online security (54%), and Canadians (46%) the least in comparison to other countries (ranging between 49% and 52%, Figure 81).

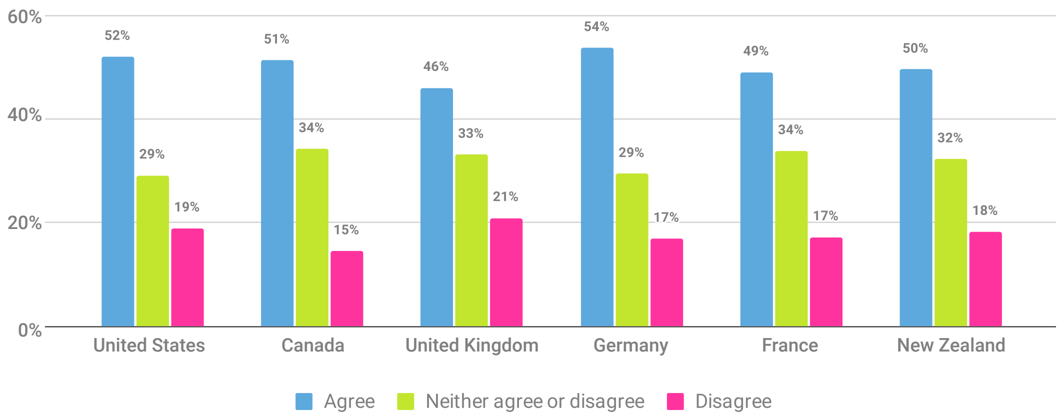


Figure 81. *"I find it easy to be secure when I'm online"* by country.

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants: 6064, dates conducted: April 13, 2023 - April 27, 2023.

Also, Germans (48%) felt the least overwhelmed by online security information compared to Canadians (34%, Figure 82). Here, Canadians (36%) and British participants (36%) tended to be more overwhelmed in comparison to other countries (ranging between 28% and 32%).

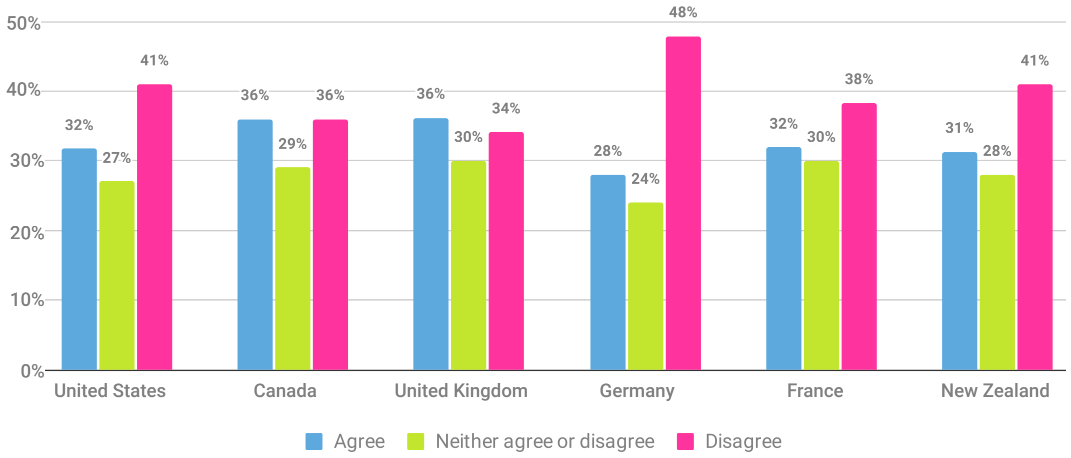


Figure 82. *"I often feel overwhelmed by information and minimize my actions online"* by country.

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants: 6064, dates conducted: April 13, 2023 - April 27, 2023.

While participants felt overall confused with the security information online, Canadians (42%) and French participants (41%) thought they were most confused about it (Figure 83). Only 20 percent of French participants were not confused by the information compared to other countries (30% to 38% disagreeing with the statement).

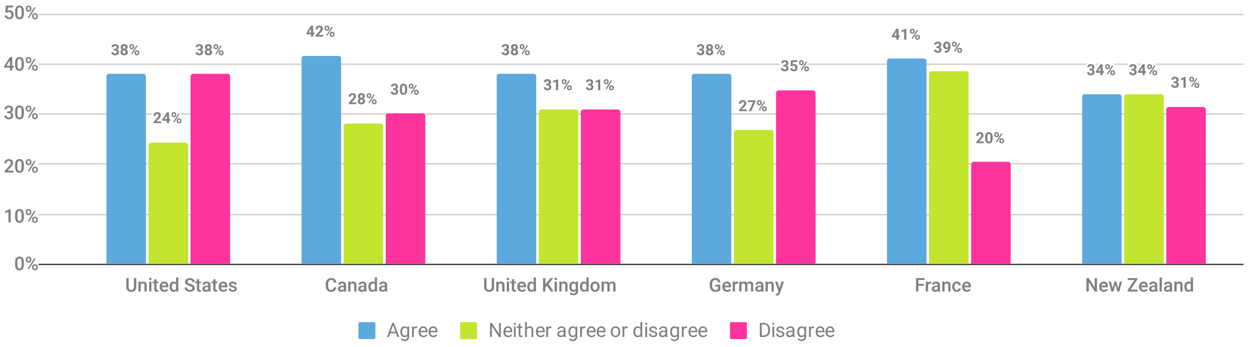


Figure 83. *"Most information on how to be secure online is confusing"* by country.

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants: 6064, dates conducted: April 13, 2023 - April 27, 2023.

More than half of Germans (52%) didn't assume their devices were automatically secure, whereas 40 percent of New Zealanders presumed so (Figure 84).

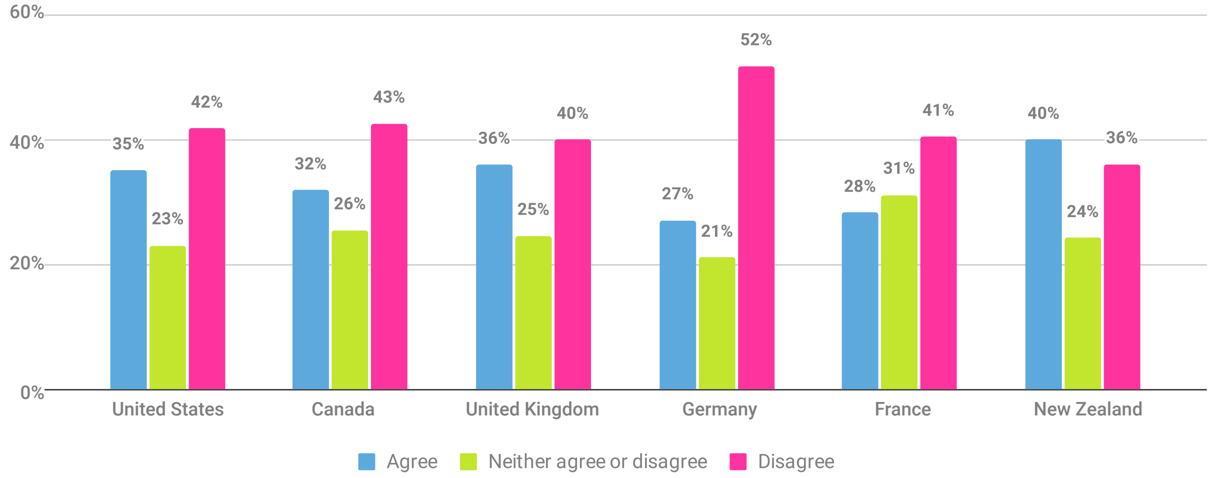


Figure 84. *"I presume my devices are automatically secure"* by country.

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants: 6064, dates conducted: April 13, 2023 - April 27, 2023.

More than half of Germans (52%) didn't assume their devices were automatically secure, whereas 40 percent of New Zealanders presumed so (Figure 84).

The cost of online protection was perceived to be high, with over half of the participants from France (56%) and from Canada (53%) agreeing with the statement in comparison to other countries (statement agreed between 45% to 49%, Figure 85).

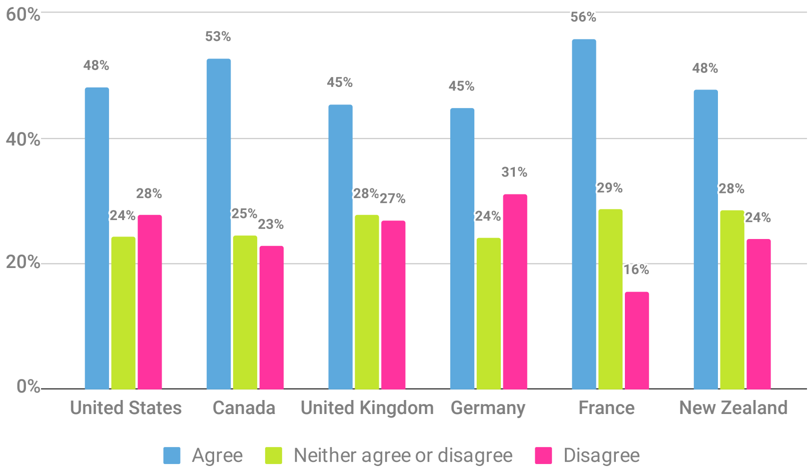


Figure 85. *"It is expensive to fully protect myself online"* by country.

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants: 6064, dates conducted: April 13, 2023 - April 27, 2023.

Country differences in media/news impact

We observed some country differences in terms of the media/news impact on peoples' feelings towards online security.

Almost half of French participants (48%) felt news/media coverage made them feel scared about online security compared to New Zealanders (39% agreed and 24% disagreed with the statement, Figure 86).

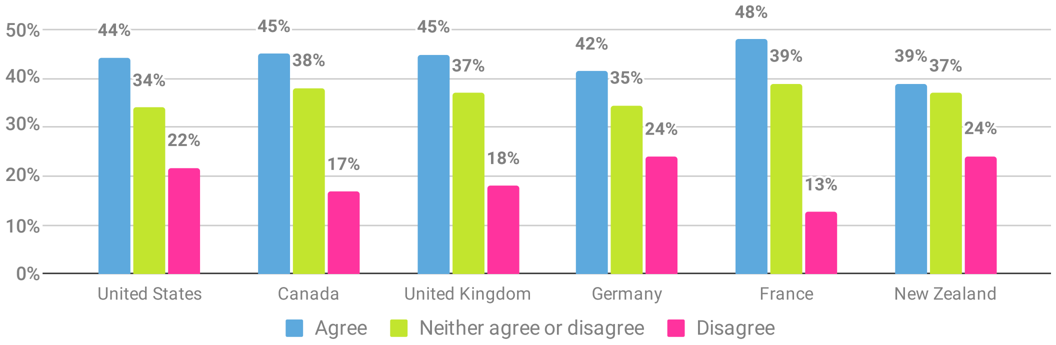


Figure 86. *"What impact does the media/news have on your views towards online security? They make me scared about my online security"* by country.

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants: 6064, dates conducted: April 13, 2023 - April 27, 2023.

Fifty-nine percent of Germans agreed that media/news help them to stay informed about online security compared to New Zealanders (44%) and French participants (47%, Figure 87).

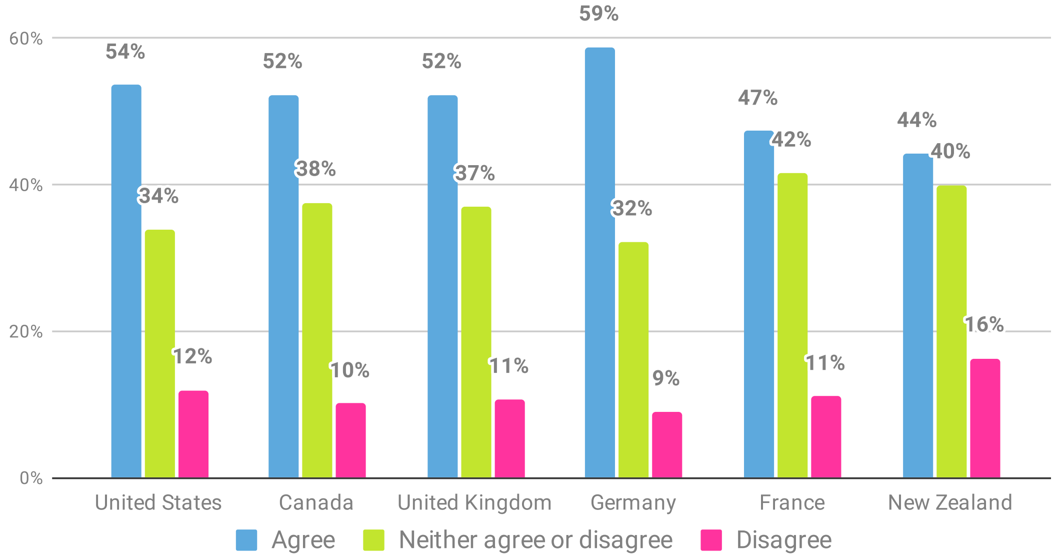


Figure 87. *"What impact does the media/news have on your views towards online security? They help me stay informed about online security"* by country.

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants: 6064, dates conducted: April 13, 2023 - April 27, 2023.

Additionally, New Zealanders (48% agreed and 14% disagreed with the statement) felt least motivated by news/media coverage, while most Germans (61%) and Americans (61%) felt inspired to take protective action as a result (Figure 88).

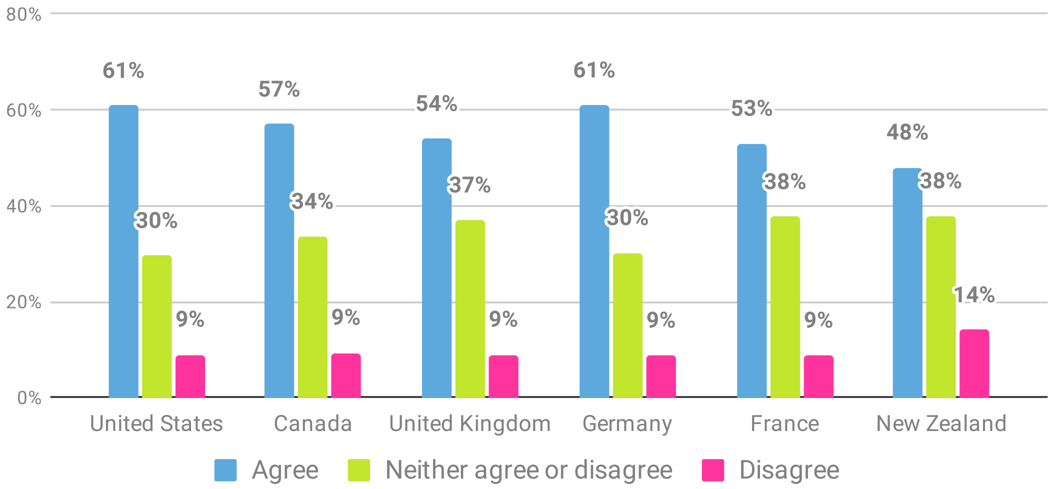


Figure 88. *"What impact does the media/news have on your views towards online security? They motivate me to take protective actions for my online security"* by country.

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants: 6064, dates conducted: April 13, 2023 - April 27, 2023.

Country differences in access to training

Overall, access to cybersecurity training was poor across the countries. French participants (70%) reported having no access to training, followed by Canadians (67%, Figure 89). Americans (44%) reported having the most opportunities to access cybersecurity training.

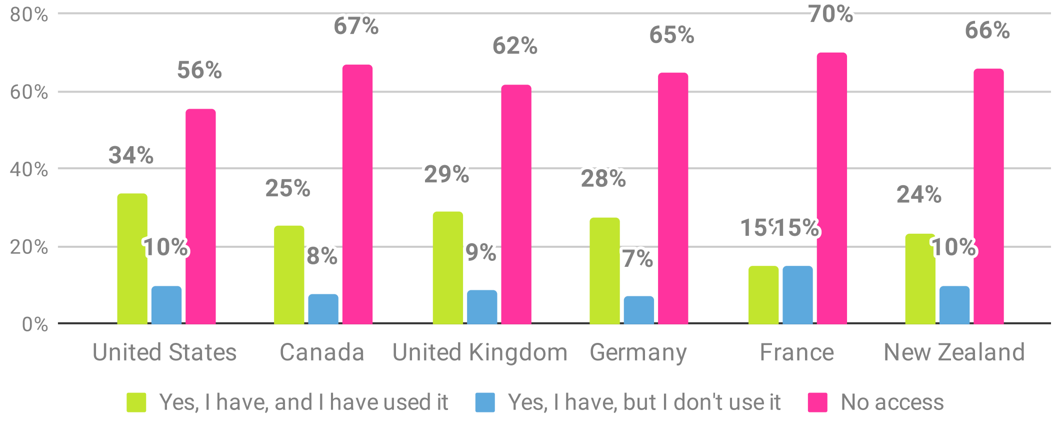


Figure 89. Access to cybersecurity training by country.

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants: 6064, dates conducted: April 13, 2023 - April 27, 2023.

Those with access to training (N=2065) were asked where they tend to learn about cybersecurity. Here, over half of Canadians (59%), New Zealanders (57%), British participants (56%), and Germans (51%) accessed training at work (Figure 90). A third of Americans (33%) and Germans (33%) reported accessing training at home, whereas French (23%) participants were more likely to access training in a public location (e.g., a library).

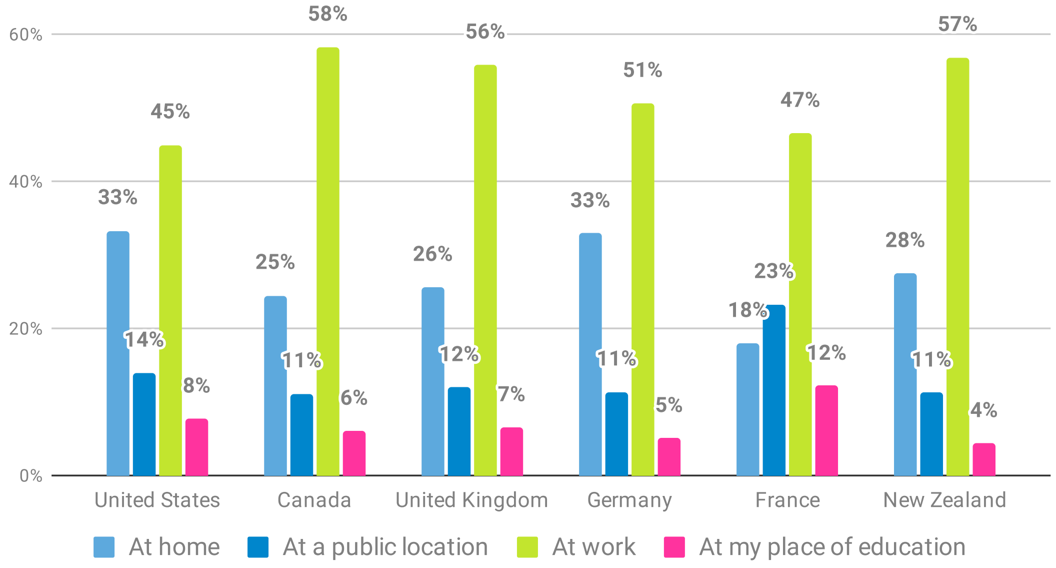


Figure 90. *"Where do you access the training?"* by country.

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants with access to training: 2065, dates conducted: April 13, 2023 - April 27, 2023.

Completing mandatory training at work or a place of education was highest for the British participants (88%) and lowest for the French participants, with almost a quarter (24%) reporting cybersecurity training as a non-mandatory exercise (Figure 91).

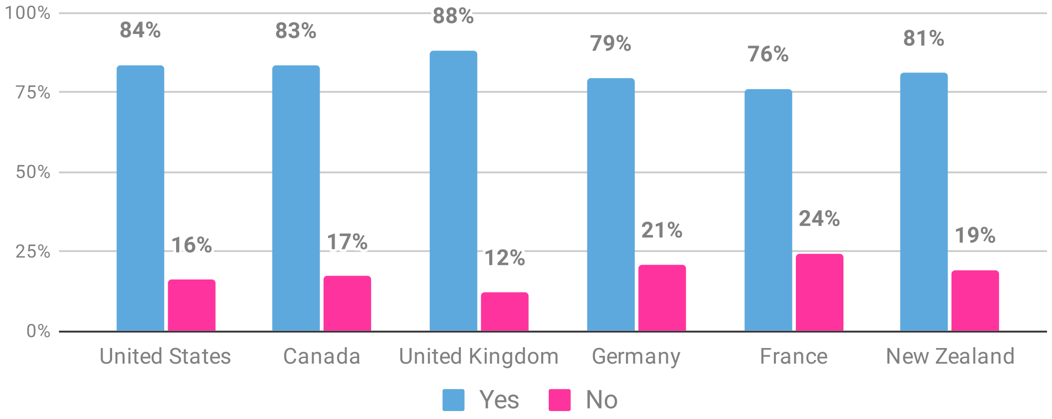


Figure 91. ***"Are you required to complete mandatory cybersecurity training at work or your place of education?"*** **by country.**

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants working/studying with access to training: 1149, dates conducted: April 13, 2023 - April 27, 2023.

Over half of the participants, having to complete mandatory training in each country, reported doing so once a year, with the highest training requirement mentioned by Germans (64%, Figure 92). Furthermore, 29 percent of French participants noted they are required to complete training at regular intervals and/or when something goes wrong.

Compared to last year (2022), once-per-year training had increased for Americans (by 18%), Canadians (by 3%), and British participants (by 8%), and regular training decreased for Americans (by 10%) and for Canadians (by 1%).

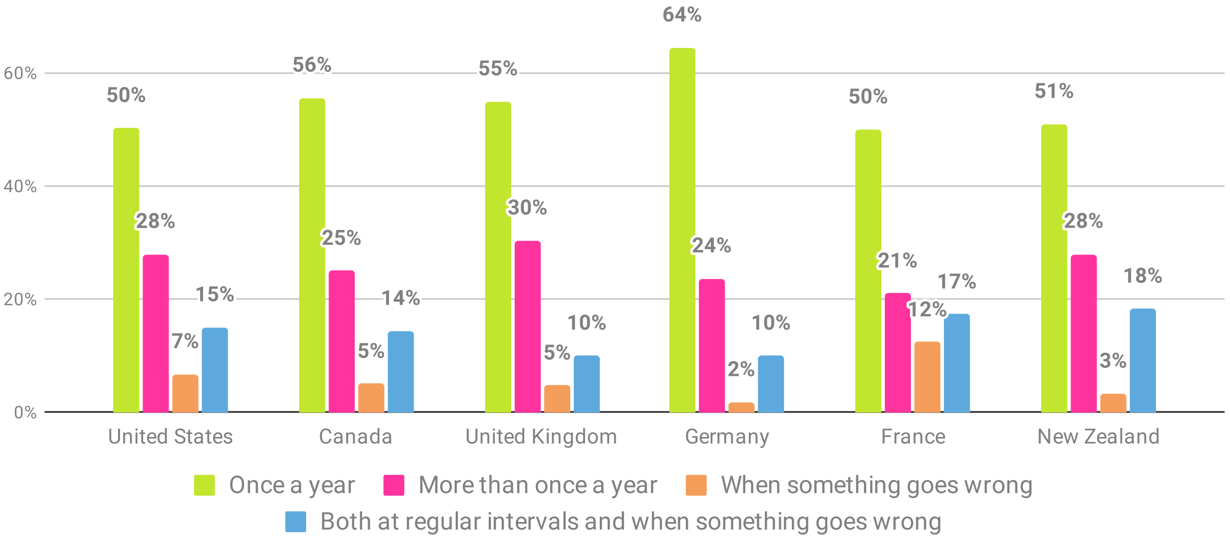


Figure 92. ***"How often are you required to complete training?"*** **by country.**

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants completing mandatory training at work or place of education: 947, dates conducted: April 13, 2023 - April 27, 2023.

Compared to last year (2022), once-per-year training had increased for Americans (by 18%), Canadians (by 3%), and British participants (by 8%), and regular training decreased for Americans (by 10%) and for Canadians (by 1%).

Preference for cybersecurity training delivery as an online training course was highest for Americans (49%), whereas French participants (35%) preferred classroom-style training courses (Figure 93). Over a quarter of New Zealanders (27%) also indicated they preferred to receive bite-sized information through notifications and alerts when needed.

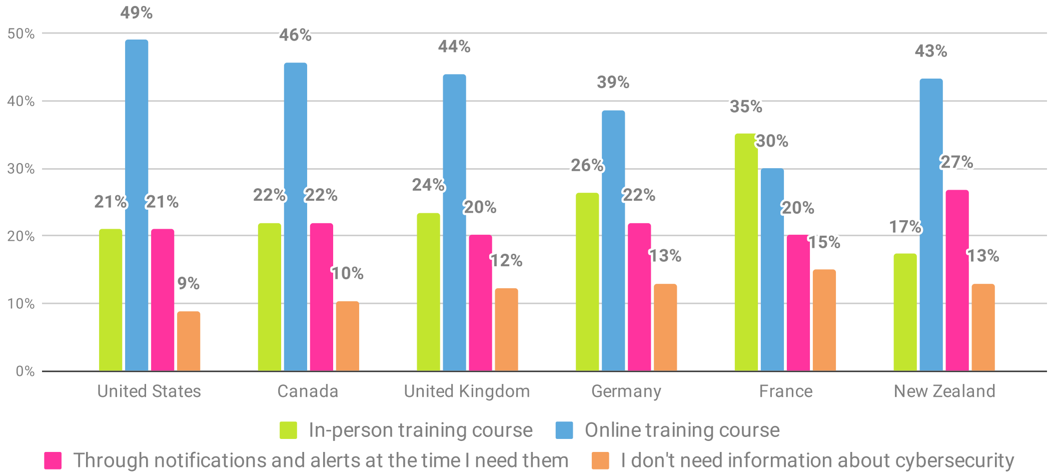


Figure 93. *"How would you most prefer cybersecurity training to be delivered?"* by country.

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants: 6064, dates conducted: April 13, 2023 - April 27, 2023.

Country differences in victimization

Attitudes toward the likelihood of becoming a victim of cybercrime were indifferent to the global outlook. However, Germans (45%) felt the least worried about falling victim to cybercrime compared to other countries (ranging from 57% to 63%, Figure 94).

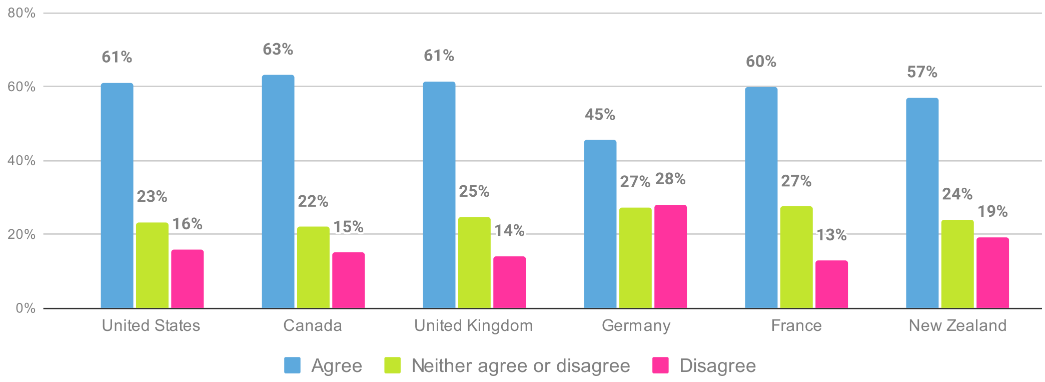


Figure 94. *"Falling victim to cybercrime is something that worries me"* by country.

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants: 6064, dates conducted: April 13, 2023 - April 27, 2023.

Americans (61%) had a reason to be worried about becoming a victim of cybercrime, as over a third (36%) of them reported having been a victim of one or more cybercrime types (Figure 95). Canadians (23%) and Germans (23%) had the lowest cybercrime victim numbers.

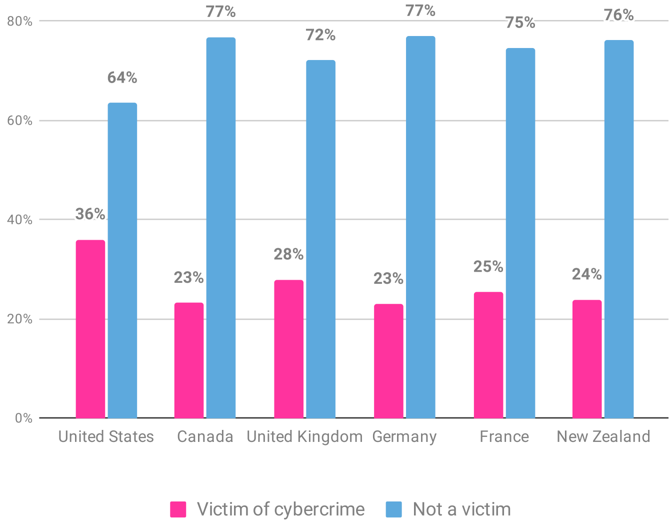


Figure 95. Percentage of cybercrime victims by country.

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants: 6064, dates conducted: April 13, 2023 - April 27, 2023.

Similar to last year, Americans were consistently more likely to have been a victim of any type of cybercrime. When examining each crime type, Americans (27%) reported most of the identity thefts compared to other countries - especially participants from France (9%, Figure 96).

Compared to other cybercrimes, British participants (19%) were more likely to fall victim to online dating scams than other crime types (16% phishing and 18% identity theft).

Seventy-seven percent of Canadians and Germans reported not having lost money/ data due to cybercrime. This was closely followed by New Zealanders (76%).

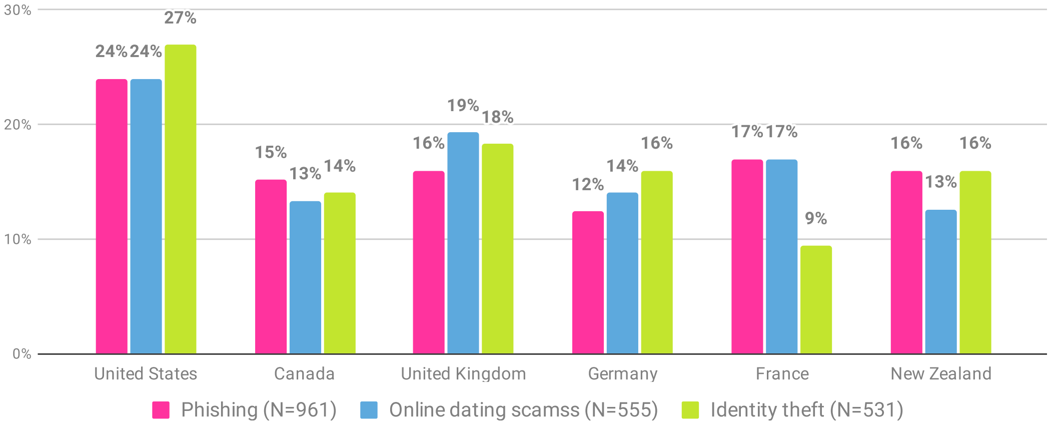


Figure 96. Crime prevalence by incident type by country.

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of incidents: 2047 (total number of participants losing money to one or more incidents: 1614), dates conducted: April 13, 2023 - April 27, 2023.

Country differences in cybercrime reporting

Crime reporting rates were highest for the British participants in terms of phishing (89%) and online dating scam (93%) reporting (Figure 97). Overall, New Zealanders were less likely to report crimes, with 82 percent of phishing scams, 69 percent of online dating scams, and 83 percent of identity thefts being reported.

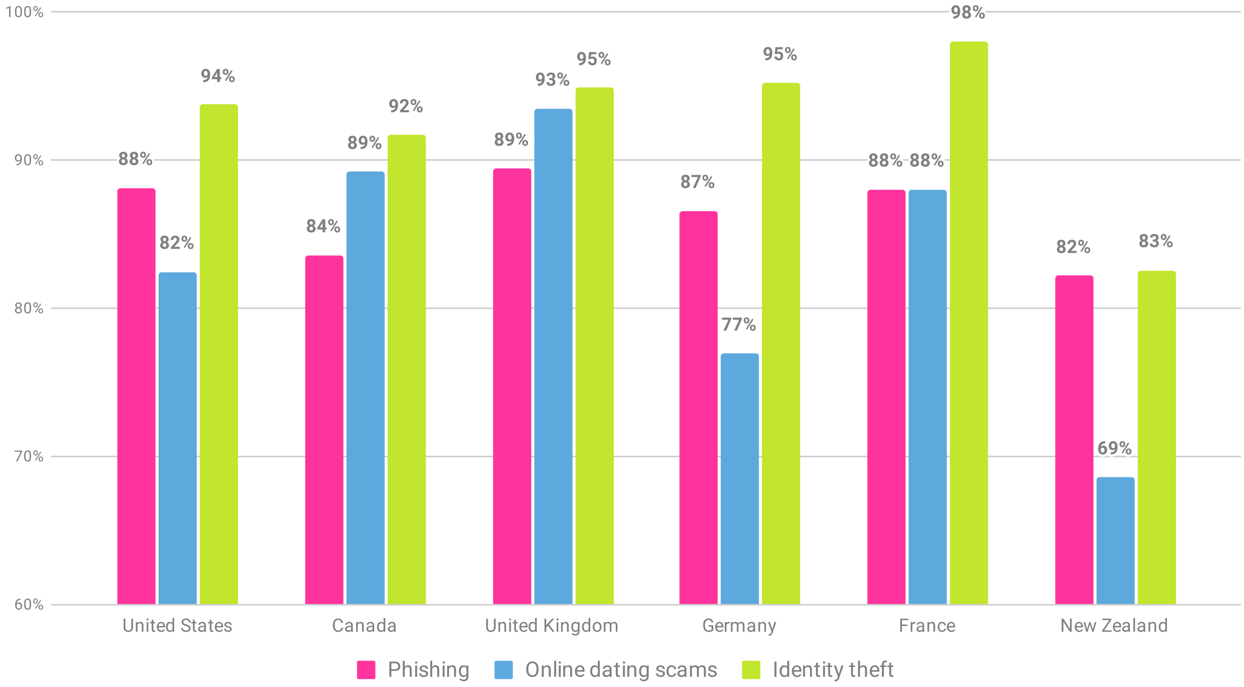


Figure 97. Percentage of cybercrimes reported to authorities, agencies, or organizations by country.

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of reported incidents: 1787 (total number of incidents: 2047), dates conducted: April 13, 2023 - April 27, 2023.

The overall increase in phishing reporting rates for North American and British participants were up by 19 percent on average from last year (2022). Canadian and British participants reporting rates for online dating scams were up by 45 percent, and for Americans, 19 percent. Also, reporting of identity thefts increased by 29 percent for British participants, 19 percent for Americans, and 11 percent for Canadians.

Country differences in cybersecurity behaviors

Password hygiene

Maintaining password hygiene can be challenging due to the number of passwords for various accounts. Over a third of British participants (36%) mentioned they have more than 20 online accounts (including those who had simply lost count of them). Americans (57%), Canadians (55%), and New Zealanders (55%) claimed to hold less than nine online accounts (Figure 98). Sixteen percent of French participants reported holding only one online account compared to other countries (ranging from 8% to 12%).

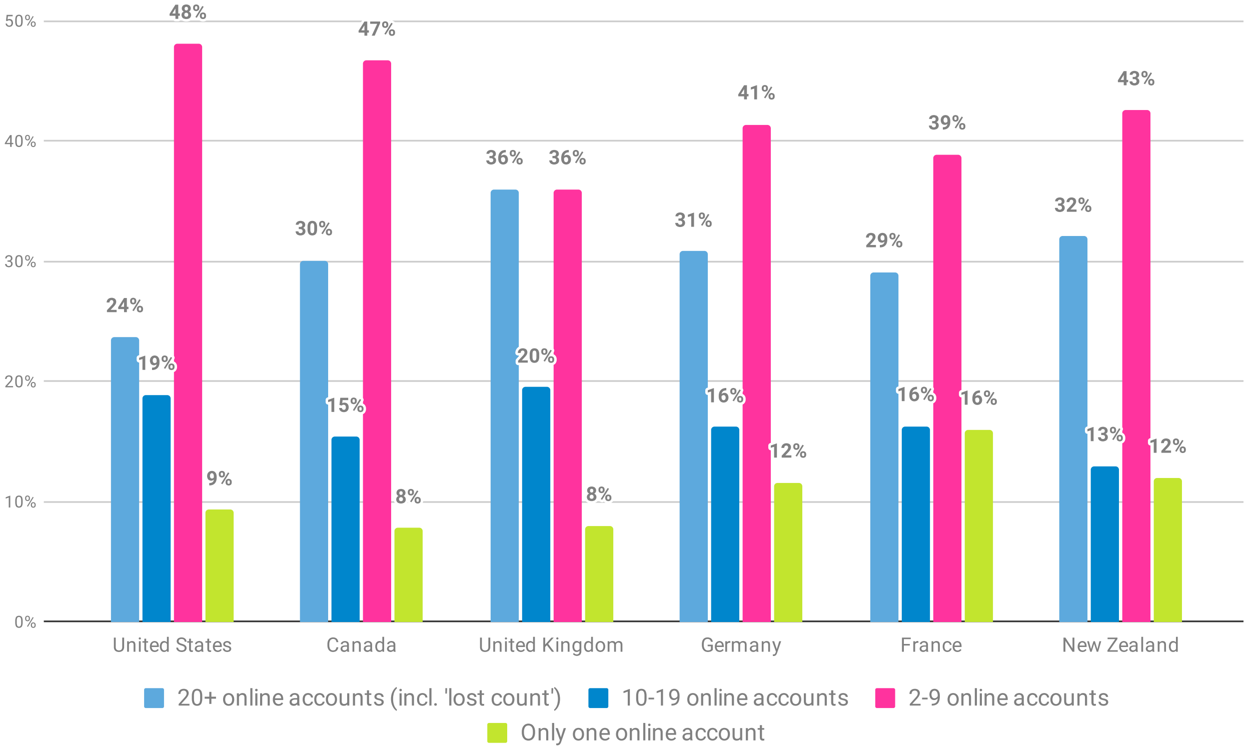


Figure 98. Number of sensitive online accounts[34] by country.

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants: 6064, dates conducted: April 13, 2023 - April 27, 2023.

[34] Online accounts holding details of your identity, address and bank cards (e.g. payment-related sites, social media accounts and work accounts).

Using separate passwords for sensitive online accounts was reported mainly by North Americans (44% by both Americans and Canadians). French participants (28% indicating 'all of the time' and 27% 'the majority of the time') tended not to use unique passwords as often as other countries (Figure 99).

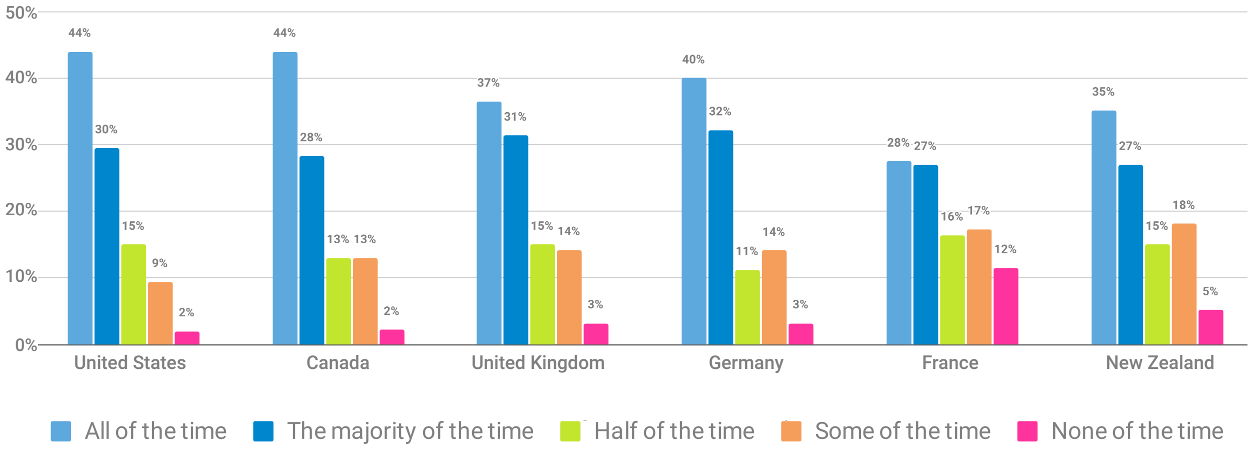


Figure 99. *"How often do you use unique passwords for your important online accounts?"* by country.

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants: 6064, dates conducted: April 13, 2023 - April 27, 2023.

We also asked if they used references to personal information (e.g., names and dates of birth) or if their passwords included a single dictionary word or name they had replaced some characters with numbers or symbols.

Americans admitted to doing so the most (38% include personal information, and 40% include words with character replacements, Figure 100). Over a third of British participants (39%) were also keen to use passwords that consisted of only a single dictionary word or a name with character replacements (e.g., p@ssw0rd, Jon@th4n), whereas for French participants (34%), using personal information was a more common technique. Germans (25%) reported using personal information in their passwords the least.

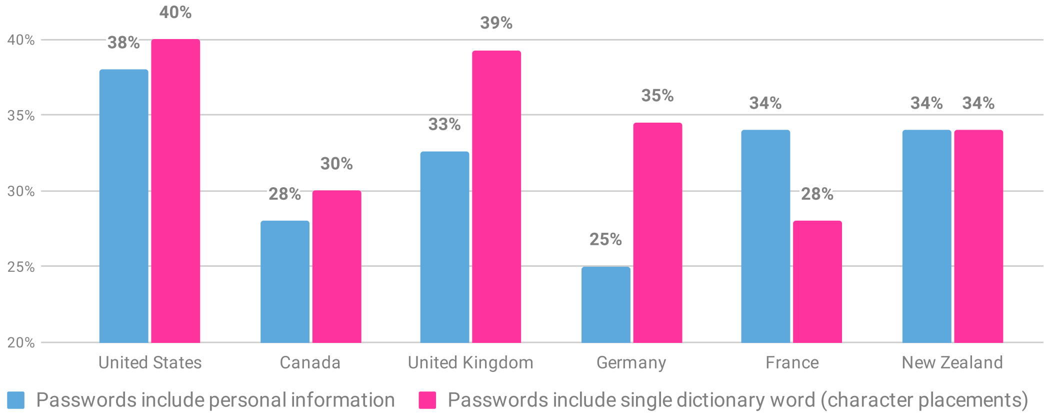


Figure 100. Password creation techniques used by the participants by country.

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants: 6064, dates conducted: April 13, 2023 - April 27, 2023.

Password management techniques

Americans (38%) reported currently using a password manager the most (Figure 101). Also, British participants (34%), Germans (34%), and Canadians (33%) were currently using a password manager. The lowest uptake of password managers was in France (65%) and New Zealand (60%), where they reported never using one.

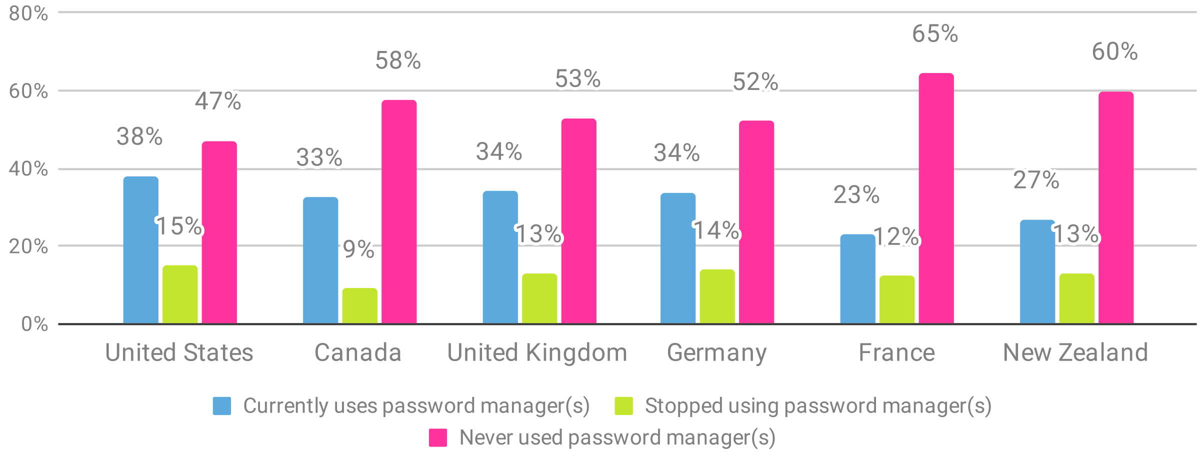


Figure 101. Use of password management application(s) by country.

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants: 6064, dates conducted: April 13, 2023 - April 27, 2023.

The highest number for paid password manager use was in Germany, where 33 percent reported buying one (Figure 102). Paying for a password manager was uncommon among French participants (16%) and New Zealanders (15%). French participants (45%) preferred free stand-alone password managers, whereas New Zealanders (50%) tended to save passwords in their Internet browser.

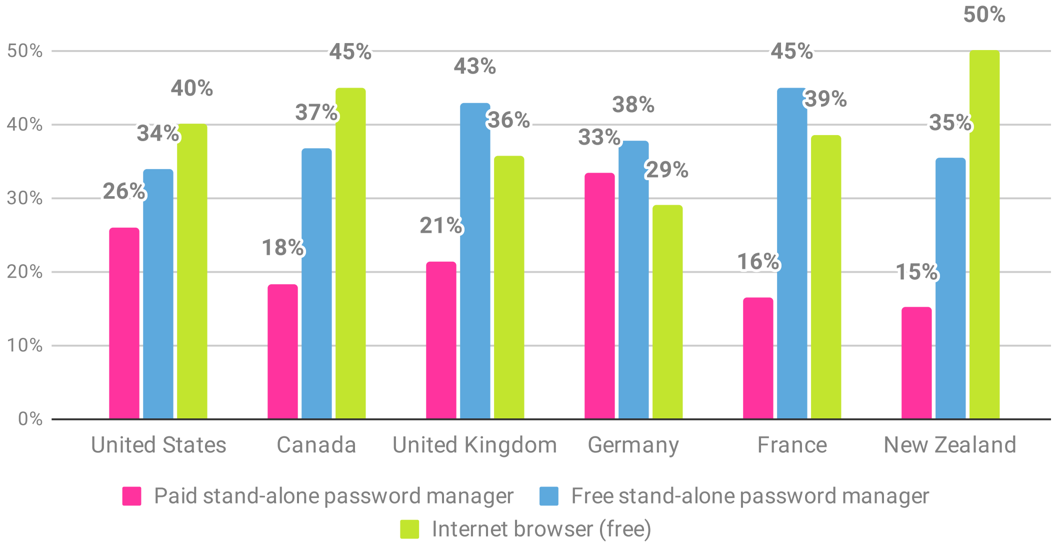


Figure 102. Preferred password management application by country.

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants using a password manager: 1906, dates conducted: April 13, 2023 - April 27, 2023.

Use of MFA

Canadians (83%) and Americans (79%) were most likely to know about MFA (Figure 103). For Canadians, this was a 26 percent increase from last year most likely due to a mean reduction in the number of retired people within the sample. On average, only 22 percent of North American and British participants reported having yet to hear of MFA. This is a 21 percent decrease (better) than last year's (2022) figures. However, 60 percent of French participants mentioned they had never heard of it.

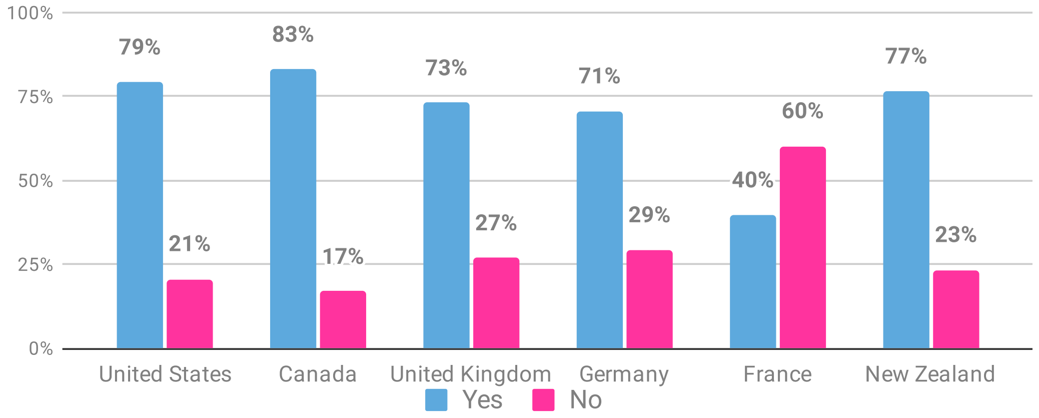


Figure 103. ***"Have you ever heard of Multi-Factor Authentication (MFA)? Also known as Two-Factor or Two-Step Verification."*** **by country.**

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants: 6064, dates conducted: April 13, 2023 - April 27, 2023.

Those who reported having heard of MFA were asked if they knew how to use it. Here, most Canadians (76%) and Americans (70%) said they know how to and use MFA regularly (Figure 104). Nearly a quarter of French participants (24%) admitted they have the know-how but don't use it.

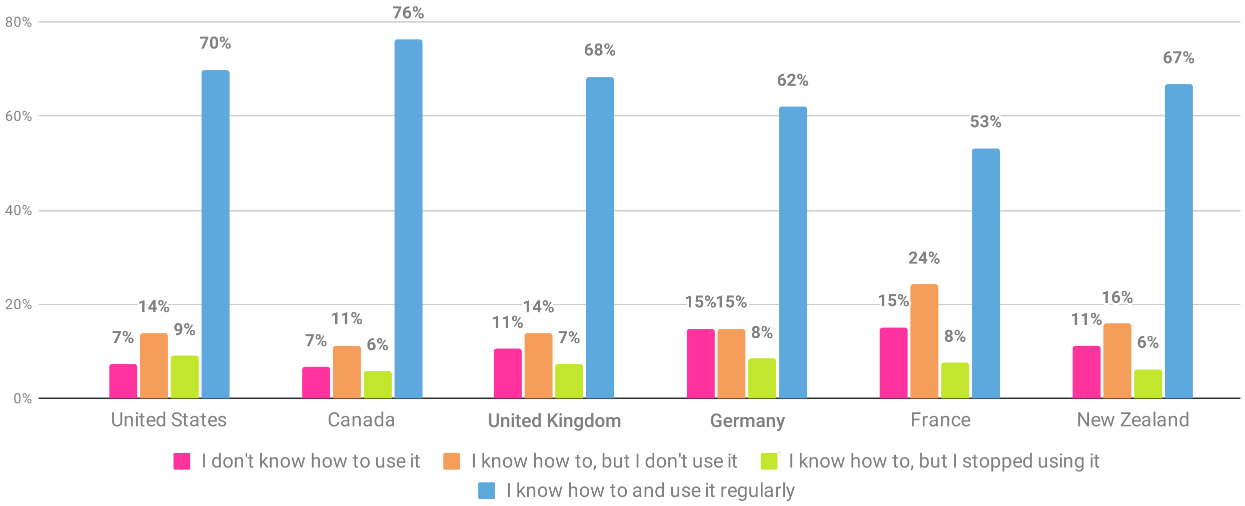


Figure 104. ***"Do you know how to use MFA?"*** **by country.**

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants who have heard about MFA: 4274, dates conducted: April 13, 2023 - April 27, 2023.

Installing the latest device updates

Ensuring people's devices run with the latest version of software and/or applications was reported highest in Germany (41% reported 'always' doing so, Figure 105). Seventeen percent of New Zealanders and 16 percent of British participants admitted they 'rarely' or 'never' installed the latest versions of updates.

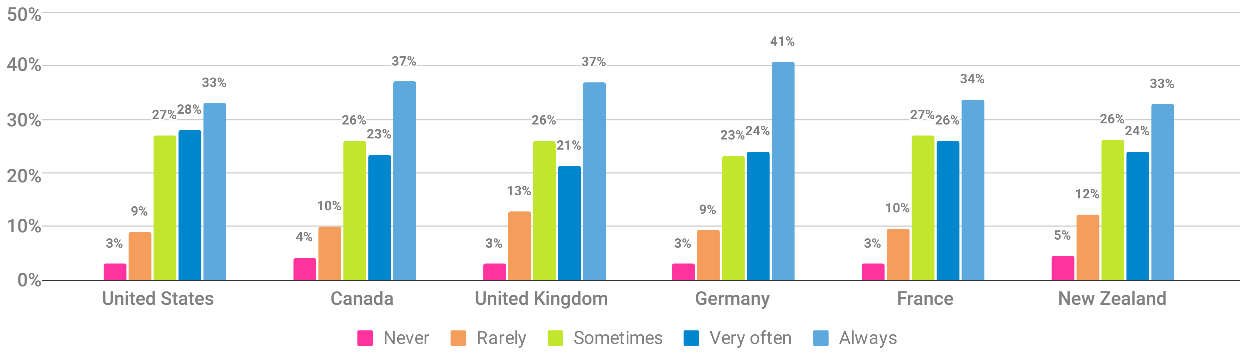


Figure 105. *"How often do you install the latest software or application updates to your devices when notified that they are available?"* by country.

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants: 6064, dates conducted: April 13, 2023 - April 27, 2023.

Backing up data

Overall, backing up data was performed 'sometimes' (highest percentages in each country ranging from 29% to 34%) by all participants in their respective countries (Figure 106). Almost half of Americans (48%) reported backing up data 'always' or 'very often', with 22 percent doing so 'never' or 'rarely'. Over a quarter of New Zealanders (34% 'never' or 'rarely') didn't back up their data very often.

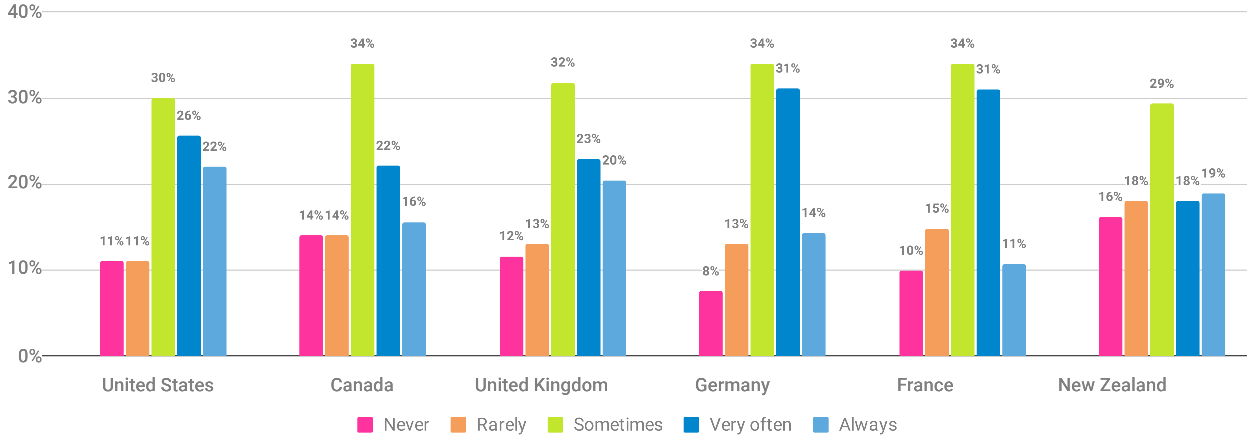


Figure 106. *"How often do you backup your most important data?"* by country.

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants: 6064, dates conducted: April 13, 2023 - April 27, 2023.

Recognizing and reporting phishing messages

New Zealanders (70%) and Americans (69%) felt most confident in recognizing phishing messages and malicious links (Figure 107). Germans (16%) felt least confident in doing so. However, 60 percent of French participants were confident in recognizing phishing messages, with 27 percent feeling neither confident nor unconfident.

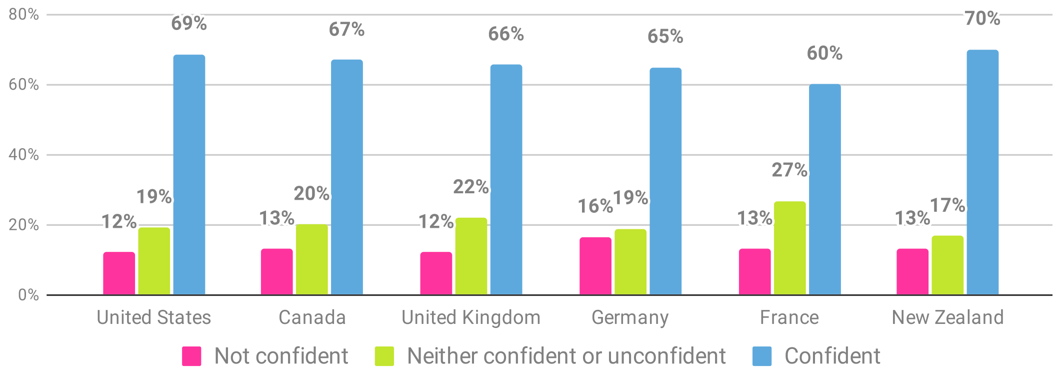


Figure 107. Confidence in the person's ability to recognize phishing emails or malicious links by country.

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants: 6064, dates conducted: April 13, 2023 - April 27, 2023.

Checking messages for signs of phishing was similar across the six countries. Here, 48 percent of Canadians and 46 percent of Germans 'always' checked the legitimacy of messages before taking action compared to 41 percent of British and French participants (respectively).

Over half of Americans (51%) reported phishing messages onward 'always' or 'very often' compared to Germans (39%, Figure 108). Americans (14%) also had the lowest number of those who 'didn't know how to report to' or 'never' report crime incidents compared to other countries (i.e., Germany, France and New Zealand, ranging between 21% and 22%).

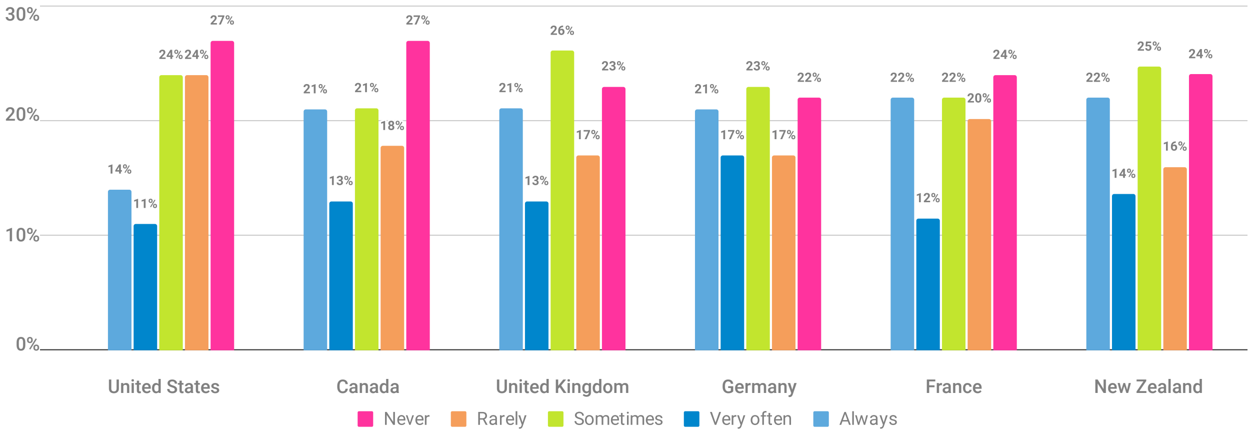


Figure 108. ***"How often do you report phishing messages (e.g., email or social media) by using the 'spam' or 'report phishing' button?"*** **by country.**

Base: US, Canada, UK, Germany, France, and New Zealand based participants (aged 18+), the total number of participants: 6064, dates conducted: April 13, 2023 - April 27, 2023. Option 'never' includes those 509 participants who don't know how to report or can't see the spam/reporting button.

NATIONAL CYBERSECURITY ALLIANCE

A leading non-profit organization, the National Cybersecurity Alliance (NCA) is dedicated to creating a more secure, interconnected world.

Advocating for the safe use of all technology, the NCA aims to educate everyone on how best to protect themselves, their families, and their organizations from cybercrime.

The organization also creates strong partnerships between governments and corporations to foster a greater “digital” good, and amplify the message that only together can we realize a more secure, interconnected world.

CYBSAFE

CybSafe is the human risk management platform designed to reduce human cyber risk in the modern, remote, and hybrid work environment, by measuring and influencing specific security behaviors.

CybSafe is powered by SebDB—the world’s security behaviors database—and built by the industry’s largest in-house team of psychologists, behavioral scientists, analysts, and security experts. An award-winning, fully scalable, and customizable solution, it’s the smart choice for any organization.

- 91% Reduction in high-risk phishing behavior
- 55% Improvement in security behaviors
- 4x More likely to engage in cybersecurity initiatives

Authors

Dr. Inka Karppinen, CPsychol, Lead Behavioral Scientist, CybSafe
Dr. Jason R.C. Nurse, Director of Science & Research, CybSafe
Joanne Varughese, Research Analyst, CybSafe

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
Toby Tracey, Research Analyst, CybSafe

Acknowledgements

Brittani Johnson, Senior Marketing Manager, Iris Powered by Generali
Jodie Kerr, CERT-NZ
Bex Ambler, CERT-NZ
Barry Eitel, Content Writer, the National Cybersecurity Alliance
Adam Brett, Senior Account Executive, Crenshaw Communications
Joe Giddens, Director of Content & Communication, CybSafe
Alice Cooke, Copywriter, CybSafe
Marina Soto, Visual Designer, CybSafe