NATIONAL CYBERSECURITY ALLIANCE

CYBSAFE

Oh, Behave!

The Annual Cybersecurity Attitudes and Behaviors Report 2022

TABLE OF CONTENTS

Oh, Behave!
A whole lot of BS[1] about cybersecurity!

Boom!

We're back for another round, and we couldn't be more excited!

Listen up. Almost half of us say we're online all the time. Yes. You read right. Almost half of us say we're online... All! The! time!

That, no doubt, rings true for the security professionals reading this. So, how does it feel knowing so many people are always connected to the internet, with many of those people having sloppy security habits?

Do you have chills? Are they multiplying?

Don't spit your latte out just yet. We've spent the summer immersed in data. We've uncovered insights that hopefully lead us to a better understanding of how we can improve everyone's security behaviors.

Behavior. It's the most tumultuous variable in cybersecurity. So, for the second time in two years we went out and asked some real, living, breathing humans about how they behave on the internet or when using tech. We're pleased to present these findings in our Annual Cybersecurity Attitudes and Behaviors Report 2022 or, as it's known 'round here, (best Austin Powers' impressions at the ready) the **"Oh, Behave!" report.**

1 behavioral science!

It's been an open secret in our industry for too long: people do not start behaving in a secure manner once they become "aware" of security risks.

This thinking is flawed. It has been for many years. Awareness, and even intent, does not itself lead to behavior change. This annoying truism likely makes intuitive sense based on your own experience.

As security professionals then, we have a problem. Eighty-two percent of breaches and security incidents relate to human factors.[1] And it's likely these numbers barely scratch the surface. We need to dive deeper into human behavior to understand 'why'.

Why?

It's an important question.

If we don't understand why Johnny doesn't want to use a password manager, it can lead us to misdiagnose the root cause ("He's lazy!", or "He's unaware!"). This can lead to prescribing the wrong remedy (like telling him off, or making him do more training).

But this doesn't work.

Scaring and bullying people to influence security behavior does not sustainably change behavior. Worst case scenario? It increases resistance. This is hardly surprising.

Research into human cybersecurity behavior is still uncharted territory in many respects. This report, as with last year's, is closing the gap.

We focus on the problem. What are the human factors associated with cybersecurity behaviors that can be harnessed to improve the effectiveness of security awareness and behavior change campaigns, both for organizations and the general public?

For many, this can help to explain why interventions often don't work.

This year, we have improved the precision of our survey and sampled more people than last year. We've surveyed three thousand people across the general public from the US, the UK, and Canada.

To influence security behaviors we need to be able to measure them. But we also need to get specific. So, this year we have concentrated on a distinct set of core cybersecurity behaviors:

1. Ensuring password hygiene
2. Applying Multi-Factor Authentication (MFA)
3. Installing the latest updates
4. Checking emails for signs of phishing
5. Backing up data

Along with the above key behaviors, this research report seeks to answer questions on the general public's security awareness and attitudes:

- What motivates people to follow advice on good security behaviors?
- What hinders and helps people when applying security advice in practice?
- What can we learn that might help us better realize desired behavior change?

Thanks for taking the time to read the report. We're happy to be on this journey with you, again!

Oz & Lisa.

Oz Alashe, MBE
CEO & Founder, CybSafe

Lisa Plaggemier
Executive Director, The National Cybersecurity Alliance

1 https://www.verizon.com/business/resources/reports/dbir/

Report aim and structure

We know you can't wait to get to all the fun, colorful graphs and tables, but don't skip over this part! It'll be worth your while. Promise!

If you didn't read the 2021 report (shame on you!) then you might be wondering what this is all about. Like its predecessor, the 2022 report provides a comprehensive international snapshot of people's cybersecurity attitudes and behaviors across representative samples. But with new insights, of course.

So, this second report builds on last year's findings and concentrates on five critical security behaviors, these are:

1. Password hygiene:
   - Password creation
   - Password management
   - Password frequency of change
2. Using Multi-Factor Authentication (MFA)
3. Installing the latest updates
4. Checking emails for signs of phishing
5. Backing up data

We examine people's access to cybersecurity resources, dive into their experience of cybercrime victimization, and consider the actions they subsequently take when it comes to reporting.

We've explored topical crimes like romance and phishing scams, reflected on security behaviors and the barriers people face when trying to be secure online, and broken down password hygiene into three sub-behaviors: creating passwords, managing passwords, and the frequency of changing them. In other words, it was just a regular summer for us.

Oh, and, we also discuss two other sub-behaviors—recognizing and reporting phishing messages—as ways to stay safe from phishing scams. Seriously, we've got to do something to reign in those long-lost princes. Ahem, see what we did there with the word 'reign'?

Alright, back to behaviors! We've organized the results under the following research themes:

1. What is the level of people's online presence?
2. Who has access to training, and do people use it?
3. What types of online-related crimes do people experience?
4. What are people's general attitudes toward cybersecurity?
5. How do people engage with cybersecurity, and what are their attitudes towards the five specific security behaviors?
6. What are the main barriers, if any, to good cybersecurity behaviors?

Finally, unlike your appendix (gosh, we are funny), ours has a function. In it, we detail our research methodology and share insight into the data and the participant demographics.

What's new?

Remember, the 2022 report follows on from last year's. So, overall research questions, participant sampling, and data collection methods have stayed the same. But like any great sequel, we've mixed things up a little—gotta stay relevant, right? So, we've made a number of updates to the survey, including:

- Additional survey questions to get a more detailed snapshot of security behaviors and associated topics:
  - We expanded the section on cybersecurity training to cover access to training, completion rates, and types of training.
  - We also looked at whether and how frequently people were required to complete training (at work/in place of education) and examined the types of security behaviors covered by the courses.
  - And, we looked at the extent to which training was perceived to have an impact.
- Two new types of cybercrime—romance scams and cyberbullying.
- A more thorough analysis of people's password hygiene behaviors, including separate questions from password creation (e.g. how personal information is used to create passwords) to using the same passwords across sensitive online accounts.
- An extended question set categorizing security behaviors around the Capability, Opportunity, and Motivation ('COM-B') model of behavior change[1]. This model has been used widely in health-related research[2] (like reducing drinking and smoking behaviors). We've used it to investigate barriers to cybersecurity behaviors. We examined three barriers for behavior change across all five security behaviors.

1 Michie, S., Atkins, L., & West, R. (2014). The behaviour change wheel. A guide to designing interventions. 1st ed. Great Britain: Silverback Publishing, 1003-1010.

2 Michie, S., Van Stralen, M. M., & West, R. (2011). The behaviour change wheel: a new method for characterising and designing behaviour change interventions. Implementation science, 6(1), 1-12.

Key terms

We know the language used in these kinds of reports can make reading them... challenging. So, we've done what we can to make this report, well, readable. That starts with defining the key terms we've used throughout the report:

(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: We narrowed down five security behaviors that were seen as some of the top priorities according to official guidance (US: Stay Safe Online[1], UK: Cyber Aware[2] and Canada: Get Cyber Safe[3]). These include: password hygiene (password creation, management, and frequency of change), applying MFA, installing the latest updates, staying safe from phishing (recognizing and reporting phishing), and backing up data.

COM-B: Capability + Opportunity + Motivation = Behavior. This model encourages behavior change by influencing one or more of its components. **Capability** refers to psychological and physical capacity to perform a behavior. **Opportunity** relates to anything that makes being secure possible/impossible that lies outside the person. **Motivation** concerns the mental processes energizing and directing behavior.

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

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 the person's 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.

1 https://staysafeonline.org/stay-safe-online/online-safety-basics/
2 https://www.ncsc.gov.uk/cyberaware/home
3 https://www.getcybersafe.gc.ca/en/secure-your-accounts/passphrases-passwords-and-pins

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.

Password hygiene: Creating unique and separate passwords for sensitive online accounts, managing passwords using browser or stand-alone applications, and the frequency 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: Cyber criminals 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.

Romance 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 have to 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).

> **“Cyber Criminals and the multiple ways they look to disrupt our business and personal lives are like a gift that keeps on giving, so we need to keep everyone we know professionally (and personally) able to unwrap the dangers and respond. Demonstrating and sharing good behavior should be our gift and not a stick in sight if we want to really see a dynamic culture evolve.”**

Caroline Bansraj, Chief Security Office (CSO) - Global Cyber Culture and Awareness & CSO People and Development, Credit Suisse

Key findings

Online presence

Most of us, including 88 percent of the survey participants, are connected to the Internet on a daily basis (if not, always). The majority (62%) of surveyed participants reported holding a 'manageable' number of sensitive online accounts (1-9 accounts), with over a third (38%) holding more than 10 sensitive online accounts *(Figure 1).*

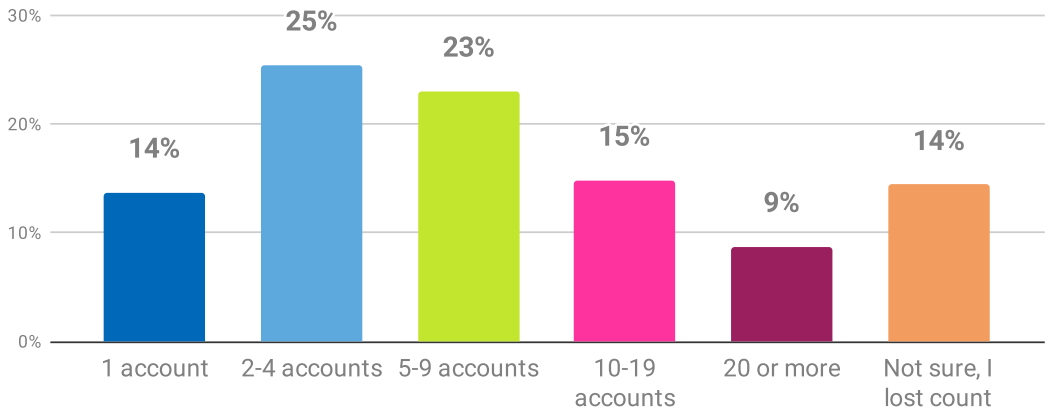


Figure 1. "Overall, how many sensitive online accounts that hold personal information do you have?"

Base: US, UK, & Canada based participants (aged 18+), total number of participants: 3000, dates conducted: June 29 2022 - July 19 2022.

"We have to change the view on security training. We cannot look at it as an annual corporate compliance task. We have to help users recognise how they (and their families) can be more cyber secure wherever they are. Giving them skills to be more secure at home is a great way to help embed the right security behaviors for the workplace."

Mark Parr, Global Head of Information Tech, HFW

Cybersecurity training

Access to training

Access to training remains low. Similar to our previous report findings, we found 62 percent did not have access to cybersecurity training *(Figure 2)*.

Training is more accessible for those in active employment (52%) or education (54%). Retirees (84%) and those not engaging in employment or study (86%) reported having no access to training *(Figure 3)*.

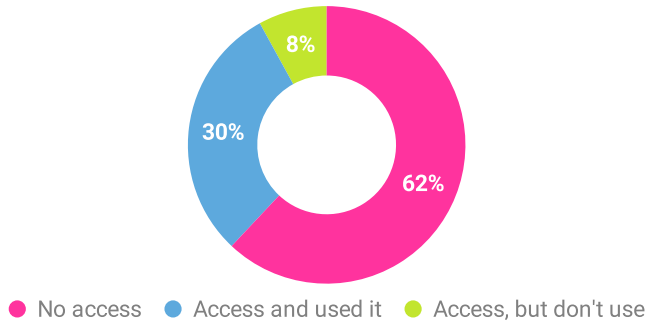


Figure 2. "Do you have access to cybersecurity advice or training?"

Base: US, UK, & Canada based participants (aged 18+), total number of participants: 3000, dates conducted: June 29 2022 - July 19 2022.

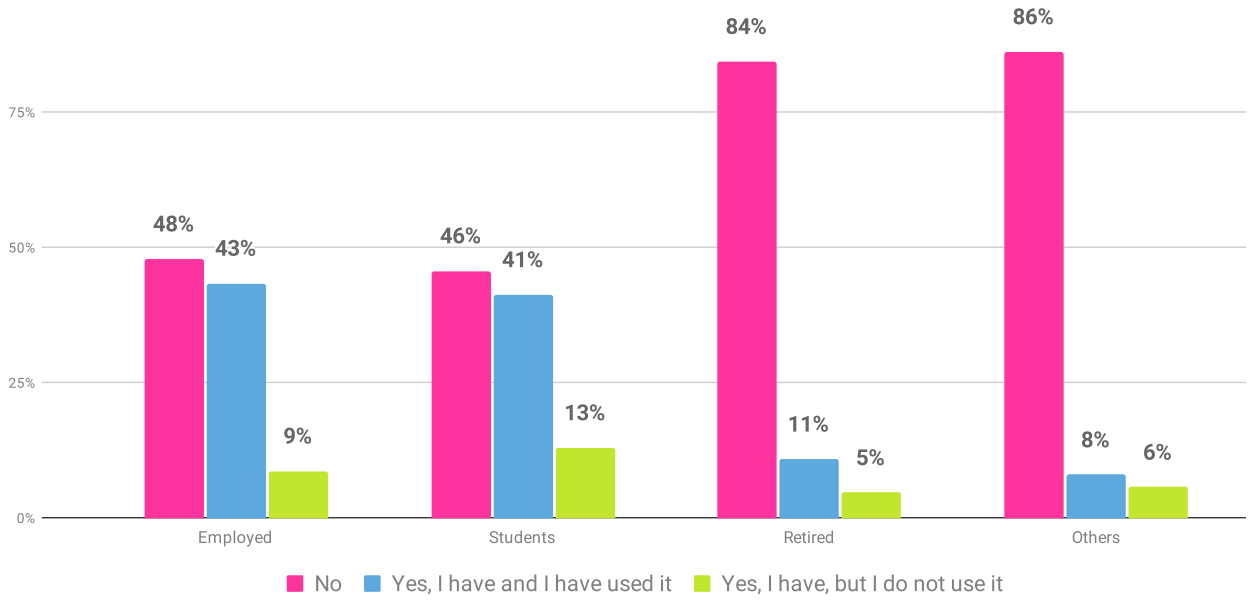


Figure 3. "Do you have access to cybersecurity advice or training?" by employment status.

Base: US, UK & Canada based participants (aged 18+), total number of participants: 3000, dates conducted: June 29 2022 - July 19 2022.

Participants with access to cybersecurity training accessed it at their work or place of education (57%), in comparison to home environments (28%). Here, 59 percent reported completing one-off training courses, and only 24 percent reported continuous training over a period of time.

Impact of cybersecurity training

More than half (58%) of the participants who had received training reported they were better at recognizing phishing messages. 45 percent had started using strong and separate passwords *(Figure 4)*.

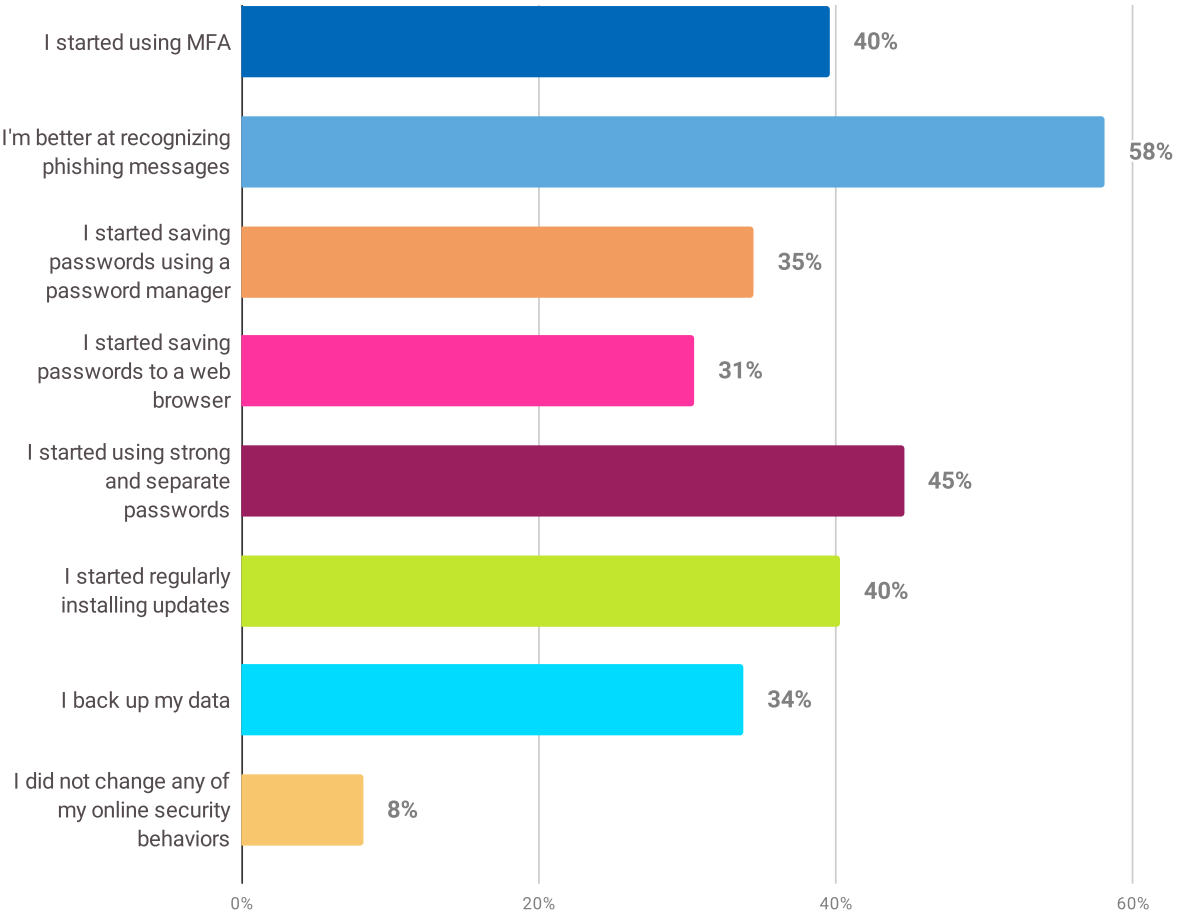


Figure 4. How training influenced participants' security behaviors.

Base: US, UK, & Canada based participants (aged 18+), total number of participants: 905, dates conducted: June 29 2022 - July 19 2022.

59%
reported completing one-off training courses, and only 24 percent reported continuous training over a period of time.

Cybercrime victimization

Attitudes towards victimization

Looking at general attitudes towards cybercrime, 78 percent of participants felt staying secure online was a priority.

Approximately half felt it was possible (51%) and under their control (52%; *Figure 5)*. However, just under half stated staying secure online was frustrating (46%) and intimidating (44%).

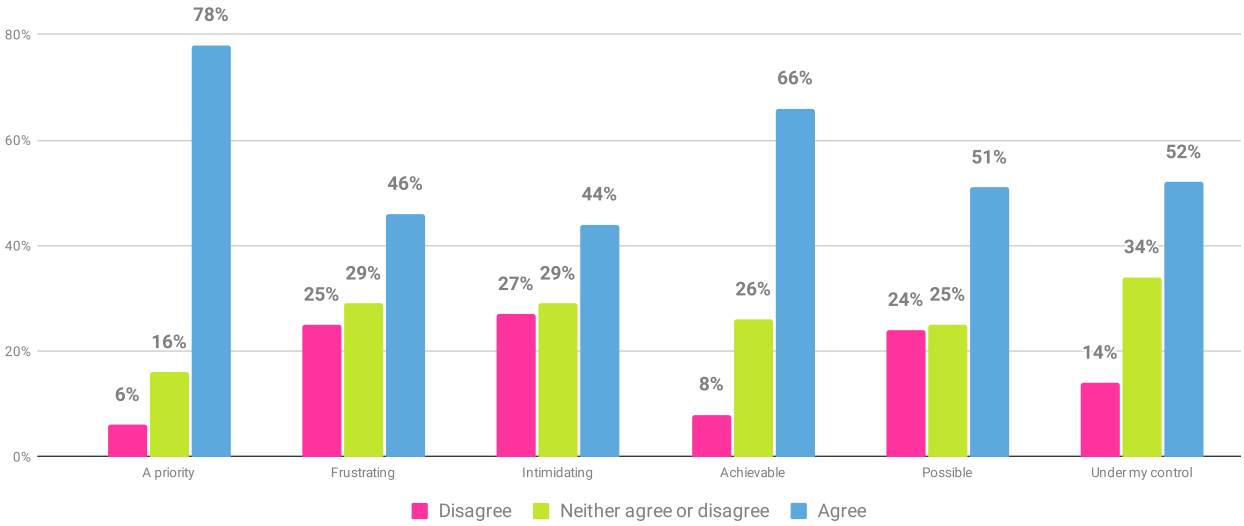


Figure 5. Participants' levels of agreement with answering "I feel that staying secure online is..."

Base: US, UK, & Canada based participants (aged 18+), total number of participants: 3000, dates conducted: June 29 2022 - July 19 2022.

Cybercrime prevalence

Overall, 1,717 incidents of cybercrime were disclosed. 34 percent of participants disclosed being a victim of at least one type of cybercrime. Phishing (36%) incidents that had led to a loss of money or data were the most reported followed by identity thefts (24%; *Figure 6*).

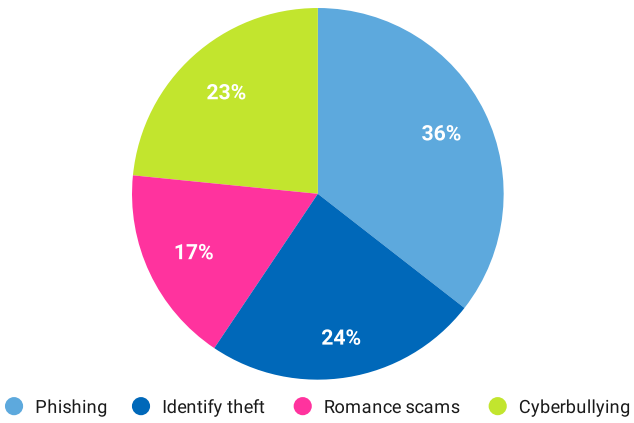


Figure 6. Types of crime incidents.

Base: US, UK, & Canada based participants (aged 18+), total number of incidents: 1,717, dates conducted: June 29 2022 - July 19 2022.

Examining each type of crime individually, younger generations (Gen Z and Millenials) disclosed higher rates of victimization when it comes to phishing, identity theft, romance scams, and cyberbullying *(Figure 7)*. And no, we don't think it's because "kids these days complain about everything".

Of those participants who disclosed being a victim of a phishing incident, most (69%) reported phishing to a person, to the organization in question, or to the authorities *(Figure 8)*.

However, 31% didn't report the crimes that had led to loss of money and/or data. Similarly, most (74%) participants mentioned reporting identity theft. 45% of romance scams and 48% of cyberbullying-related crimes were unreported.

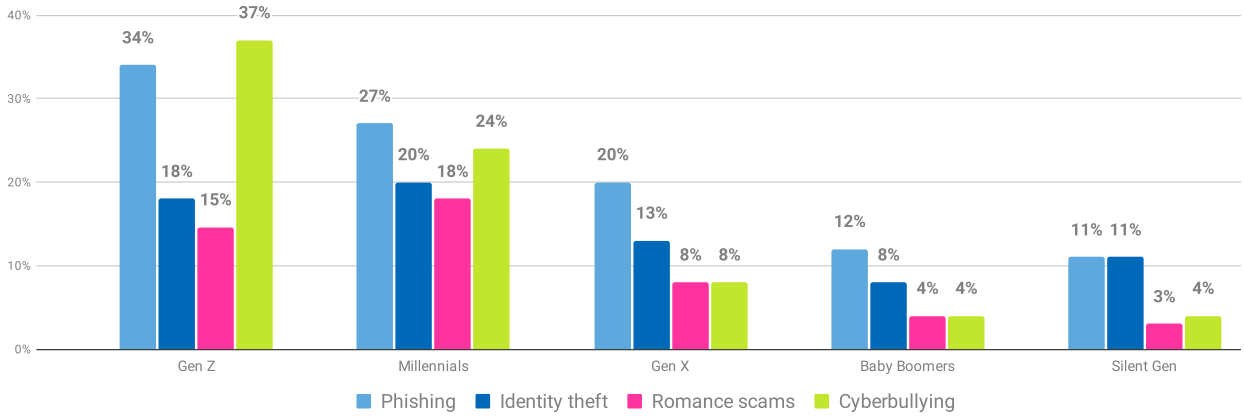


Figure 7. Types of crime incidents by generation.

Base: US, UK, & Canada based participants (aged 18+), total number of participants per reported incident: phishing 607, identity theft 409, romance scams 295, cyberbullying 401. Dates conducted: June 29 2022 - July 19 2022.

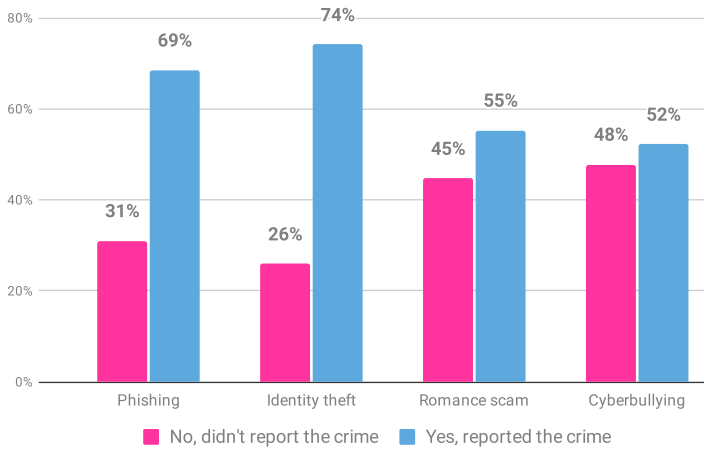


Figure 8. Crime reporting frequency by crime type.

Base: US, UK, & Canada based participants (aged 18+), total number of incidents: 1,717, dates conducted: June 29 2022 - July 19 2022.

Cybersecurity behaviors, practices, and attitudes

Password hygiene

We examined five main behaviors for good cybersecurity practices. When it came to ensuing password password hygiene (e.g. password creation, length, use, and frequency of change), the results were discouraging.

Some (29%) participants created passwords made up of a single dictionary word or a name, with numbers or symbols replacing some of the characters. Only 16 percent of participants reported creating passwords over 12 characters long *(Figure 9)*. This is one of the few cases where size does matter.

Over a third (36%) of participants reported using unique passwords half of the time or less *(Figure 10)*. Another 36 percent changed their passwords every few months, with some (35%) admitting they only changed a character or two.

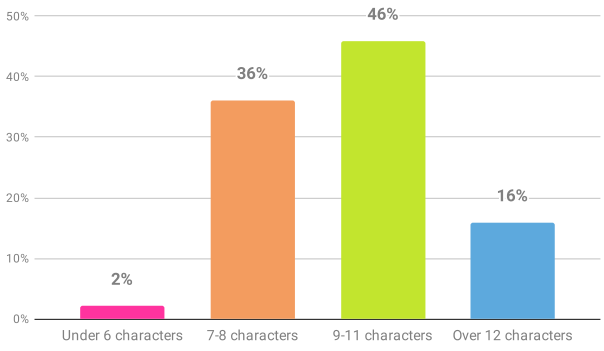


Figure 9. Typical length of passwords created by the participants.

Base: US, UK, & Canada based participants (aged 18+), total number of participants: 3000, dates conducted: June 29 2022 - July 19 2022.

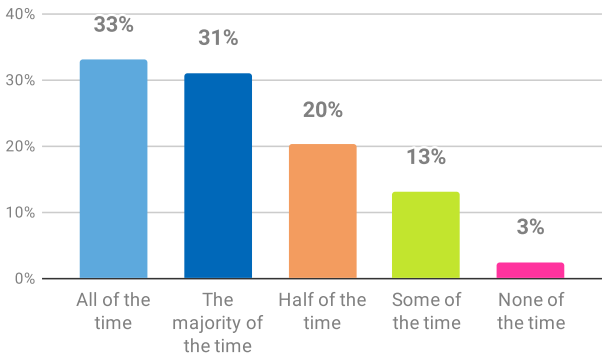


Figure 10. How often do you use unique/separate passwords for your important online accounts?[1]

Base: US, UK, & Canada based participants (aged 18+), total number of participants: 2589, dates conducted: June 29 2022 - July 19 2022.

33%

A third of the participants mentioned they 'very often' or 'always' saved passwords in their browsers, if prompted.

Further, 18 percent mentioned they'd downloaded a stand-alone password manager.

We asked participants to report on their preferred method of remembering passwords. Over a third (37%) preferred to write passwords in a notebook, with 28 percent storing them electronically (e.g. in a document, phone—or, shudder—an email).

1 This question was only asked to participants who noted having more than one account.

Some (22%) even reported they 'just remember passwords without writing them down' *(Figure 11)*. We'd like to know what these people eat for breakfast.

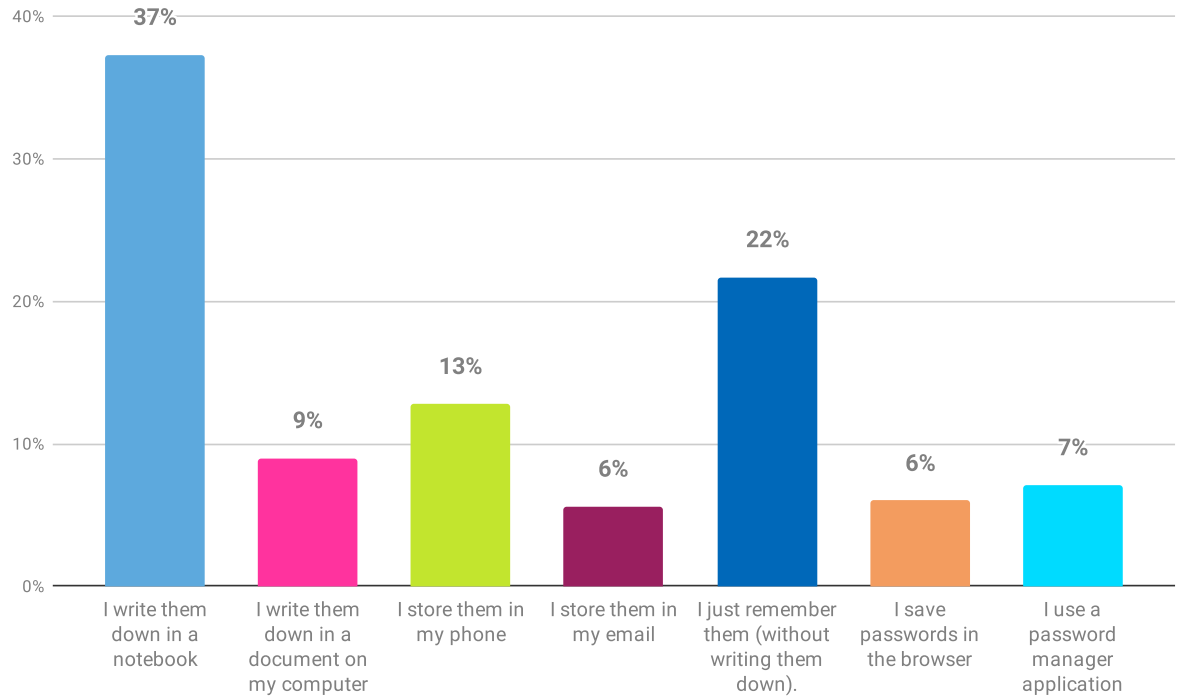


Figure 11. What is your preferred method of remembering passwords?

Base: US, UK, & Canada based participants (aged 18+), total number of participants: 2589, dates conducted: June 29 2022 - July 19 2022.

Applying multi-factor authentication

Similar to our findings last year, 43 percent of participants had never heard of multi-factor authentication (MFA) *(Figure 12)*.

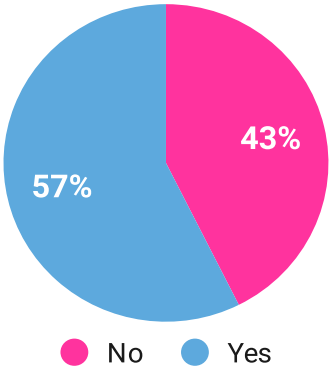


Figure 12. "Have you ever heard of Multi-Factor Authentication?"

Base: US, UK, & Canada based participants (aged 18+), total number of participants: 3000, dates conducted: June 29 2022 - July 19 2022.

Installing software updates and backing up data

On a positive note, most (63%) of participants 'always' or 'very often' installed the latest updates and software *(Figure 13)*.

43 percent of participants mentioned they 'always' or 'very often' backed up their important data. 21 percent noted they 'rarely' or 'never' do so *(Figure 14)*. That 21 percent is probably the same people whose pens ran out of ink in the middle of a test and never had a spare.

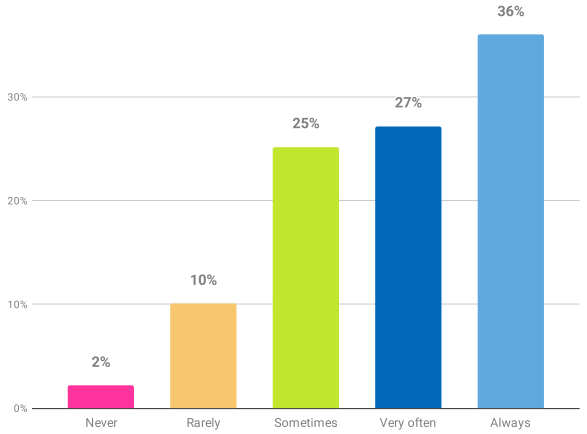


Figure 13. "How often do you install the latest updates and software when notified that they are available?"

Base: US, UK, & Canada based participants (aged 18+), total number of participants: 3000, dates conducted: June 29 2022 - July 19 2022.

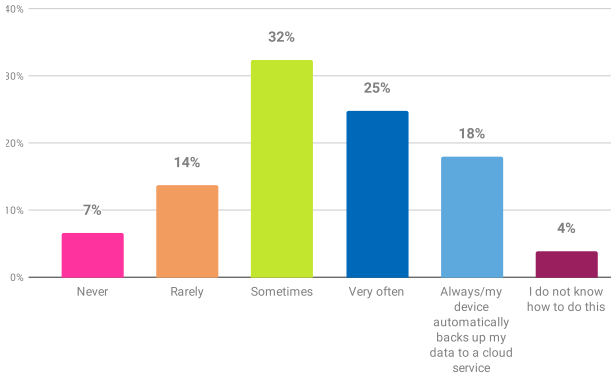


Figure 14. "How often do you back up your most important data?"

Base: US, UK, & Canada based participants (aged 18+), total number of participants: 3000, dates conducted: June 29 2022 - July 19 2022.

Barriers to cybersecurity behaviors

We found participants' lack of motivation (40% reporting low vs 25% reporting high ratings) the greatest barrier overall when completing security behaviors *(Figure 15)*.

Opportunity barriers—with most ratings in the 'neither agreeing nor disagreeing' range—demonstrated participants' lack of opportunities to complete the behaviors (e.g. resources and time). We also noted higher capability (35%), but only a quarter felt motivated to take action.

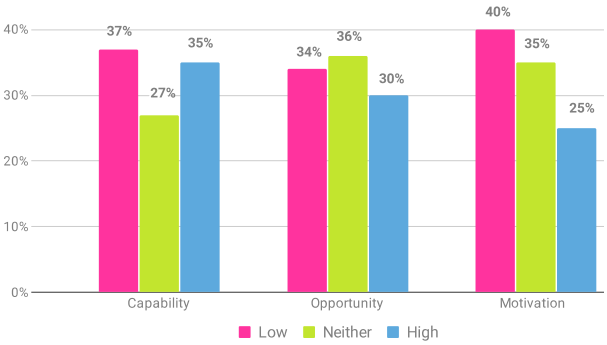


Figure 15. Overall barriers to five security behaviors by capability, opportunity and motivation.

Base: US, UK & Canada based participants (aged 18+), total number of participants per security barrier reported: software update 297, MFA use 446, reporting phishing 608, password manager use 2585 and backing up data 609. Dates conducted: June 29 2022 - July 19 2022.

“The vast majority of organizations have flocked to compliance-driven awareness training in recent years, as a way of ticking boxes to meet government and regulatory requirements.

However, while the message around cybersecurity awareness has improved, evidence suggests that our collective behaviors are still a long way from where we need our security-first culture to be.

I’m delighted to endorse this report that explores what is holding back the implementation of smarter practices to human cyber risk management.”

Martin Smith MBE, Chairman & Founder,
SASIG (Security Awareness Special Interest Group)

Our findings

We conducted our second cybersecurity attitudes and behaviors survey online between June 29th and July 19th, 2022.

Representative samples (according to age and gender) were obtained from the US and the UK, with Canada providing a representative sample based on its yearly Statistic Census.

In the US and the UK, the survey was run by Toluna[1]. In Canada the survey was distributed by Elemental Data Collection[2]. Overall, 3,000 participants shared their views about their online and cybersecurity behaviors.

We surveyed the adult population (18 years or older). As per the last year, we set out to explore the complete sample population, as well as examine differences between age groups.

Fifty-eight percent of the participants stated they were in either full- or part-time employment. We noted differences in employment status and explored country differences separately in the Appendix.

The number of participants in each age group and employment status are shown in *Table 1* and *Figure 16*, with further participants' demographics detailed in the Appendix.

Generation (age) % within country of residence	US (N=1000)	UK (N=1000)	Canada (N=1000)	Total (N=3000)
Gen Z (18-25)	**138** 13.8%	**127** 12.7%	**20** 2.0%	**285** 9.5%
Millennials (26-41)	**300** 30.0%	**311** 31.1%	**199** 19.9%	**810** 27%
Gen X (42-57)	**271** 27.1%	**266** 26.6%	**261** 26.1%	**798** 26.6%
Baby Boomers (58-76)	**253** 25.3%	**265** 26.5%	**446** 44.6%	**964** 32.1%
Silent Gen (77+)	**38** 3.8%	**31** 3.1%	**53** 5.3%	**122** 4.1%
Prefer not to say	**0** 0%	**0** 0%	**21** 2.1%	**21** 0.7%

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

1 https://uk.toluna.com

2 https://elementaldci.com

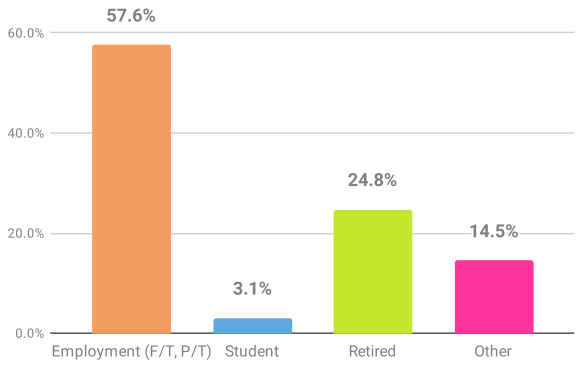


Figure 16. Participants' employment status[1].

Base: US, UK, & Canada based participants (aged 18+), total number of participants: 3000, dates conducted: June 29 2022 - July 19 2022.

Our online presence

No, this isn't the beginning of another marketing speech about the importance of "building an online presence." This is about all the things people do online, like, 'Googling' and mindless social media scrolling. And the less important stuff like banking, shopping, and working remotely.

Of course, it's not a surprise to see people are connected to the Internet most of the time. Overall, 88 percent of participants said they are either connected 'all the time' or go online 'a few times per day'.

Only 12 percent of participants reported accessing the Internet on a 'less than daily' basis (e.g. once per week).

Further investigation of the generational differences *(Figure 17)* revealed Gen Zs (64%) tend to be 'always connected' to the Internet (i.e., they have entered The Matrix), in comparison to the older generations like Baby Boomers (33%) and Silent Gen (27%).

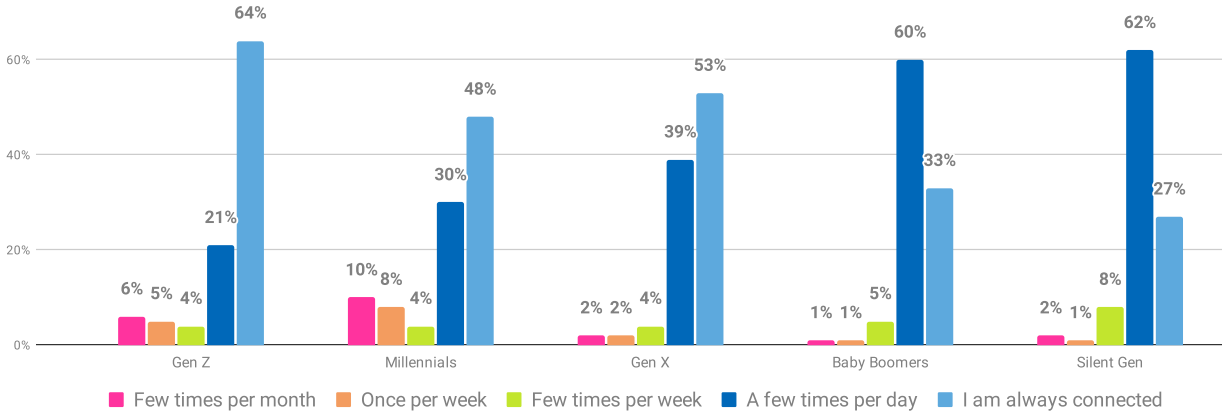


Figure 17. Use of the Internet by generations: "How actively do you use the Internet?"

Base: US, UK, & Canada based participants (aged 18+), total number of participants: 2979, dates conducted: June 29 2022 - July 19 2022.

1 Where generational differences are reported in the main findings section, the 21 participants who stated 'prefer not to say' are excluded

To examine the level of risk people might be exposed to, we asked participants how many accounts they own containing personal information. The majority (62%) hold a 'manageable' number (1-9 accounts; *Figure 18*). However, 38 percent hold more than 10, including those who have lost count of how many they have (14%).

In terms of generations, we didn't see lots of differences. Nearly half of the Silent Gen reported holding less than four sensitive online accounts (45%) in comparison to other age groups (e.g. 29% of Gen Z held less than four sensitive accounts).

We also asked if participants relied on anyone to help them stay secure online. On average, 44 percent did not report such reliance, while approximately a third (35%) relied on the help of friends or family. Furthermore, 35 percent stated family members relied on them in order to keep safe online.

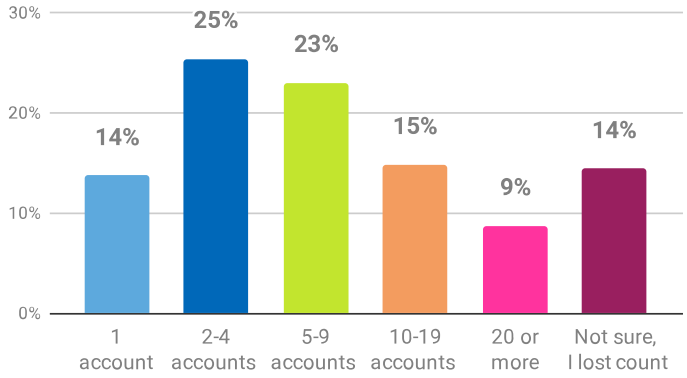


Figure 18. "Overall, how many sensitive online accounts that hold personal information do you have?"

Base: US, UK, & Canada based participants (aged 18+), total number of participants: 3000, dates conducted: June 29 2022 - July 19 2022.

35%
stated family members relied on them in order to keep safe online.

Cybersecurity training

Access to training

Similar to last year's report, 62 percent of participants said they had no access to cybersecurity training. 30 percent stated they had access to training, and had used it *(Figure 19)*.

Mostly, those in employment or studying *(Figure 20)* reported having access to training (52% and 54%, respectively), in contrast to those who weren't in active employment or studying (only 16% of retirees and 14% of others had access to training).

The findings suggest those not in active employment may be more vulnerable to cybercrime as they do not have access to the tools and information to reduce their vulnerability.

Furthermore, it highlights a subgroup of the population is in need of security support and assistance.

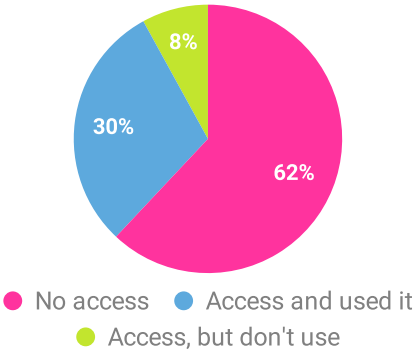


Figure 19. "Do you have access to cybersecurity advice or training?"

Base: US, UK, & Canada based participants (aged 18+), total number of participants: 3000, dates conducted: June 29 2022 - July 19 2022.

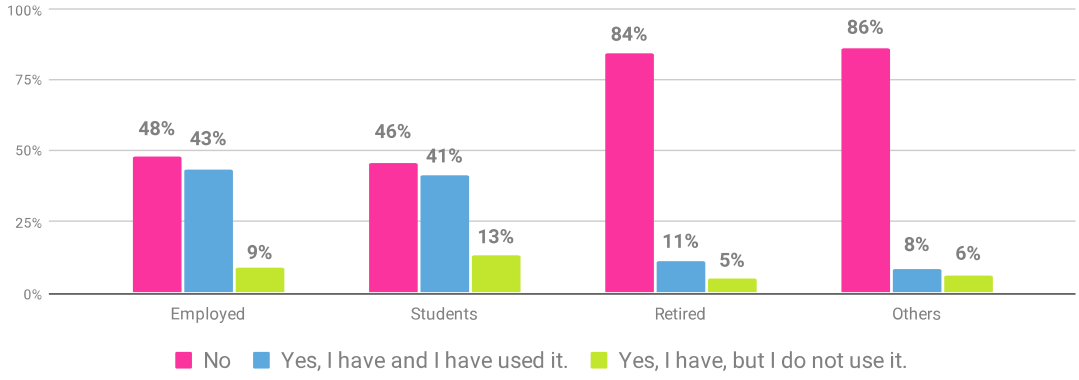


Figure 20. "Do you have access to cybersecurity advice or training?" by employment status.

Base: US, UK, & Canada based participants (aged 18+), total number of participants: 3000, dates conducted: June 29 2022 - July 19 2022.

Additionally, more than half of the younger age groups (51% of Gen Zs and 59% of Millennials) noted they had access to training resources. For those over 58 years old, access to cybersecurity training dropped to 20 percent or less *(Figure 21)*.

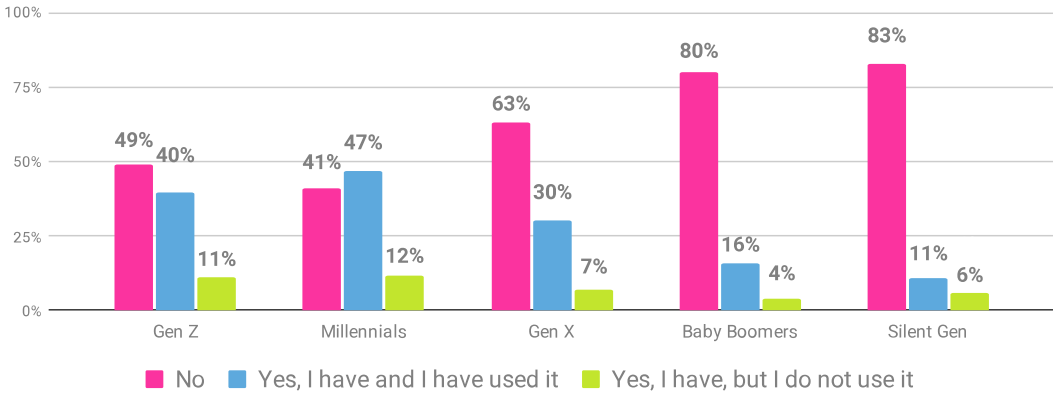


Figure 21. "Do you have access to cybersecurity advice or training?" by generations.

Base: US, UK, & Canada based participants (aged 18+), total number of participants: 2979, dates conducted: June 29 2022 - July 19 2022.

Fifty-seven percent of participants with access to cybersecurity training accessed it at work or place of education. Twenty-eight percent accessed it at home. Furthermore, 15 percent accessed resources at work and at home. Legends.

Most participants (59%) reported completing one-off training courses, with only 24 percent reporting continuous training over a period of time (17% had completed both; *Figure 22*).

Most training completed at work or place of education was mandatory (58%), and completed once a year (43%). Unfortunately, 16 percent of participants mentioned they are required to complete training at regular intervals and when something goes wrong or something 'bad' happens (e.g. a security incident at work), while 10 percent noted only the latter *(Figure 23)*.

Side note: it is a bad idea to cause people to associate 'failing' with training. It positions training as a punishment, which reduces its effectiveness.

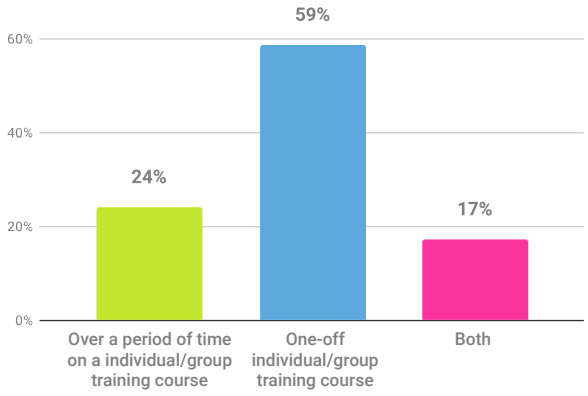


Figure 22. Types of training courses completed by the participants.

Base: US, UK, & Canada based participants (aged 18+), total number of participants: 905, dates conducted: June 29 2022 - July 19 2022.

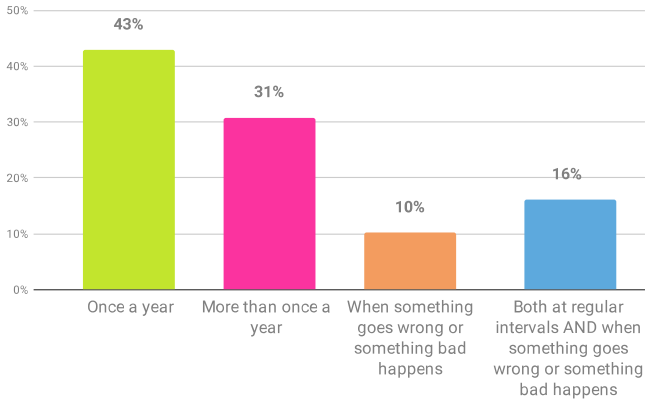


Figure 23. "How often are you required to complete training?" by participants in employment or studying.

Base: US, UK, & Canada based participants (aged 18+), total number of participants: 522, dates conducted: June 29 2022 - July 19 2022.

Lack of time (28%) and already having enough knowledge about cybersecurity (26%) were reported as the main reasons for those participants who mentioned they have access to training, but did not use it (N=222).

Out of the 13 percent who were not able to access training courses (online or in person), affordability and work/childcare commitments (29% and 25%, respectively) were the most common reasons preventing participation.

Impact of cybersecurity training

Completing a training course is simple enough. But, what topics do they cover, and are they useful? Most importantly, does time spent training influence any cybersecurity behaviors? Training courses were reported as covering a wide range of topics.

Most notably, recognizing phishing emails was covered in 68 percent of training *(Figure 24)*. This was followed by instructions on how to use strong and separate passwords (58%). Backing up data was the only training topic reported by less than half of participants.

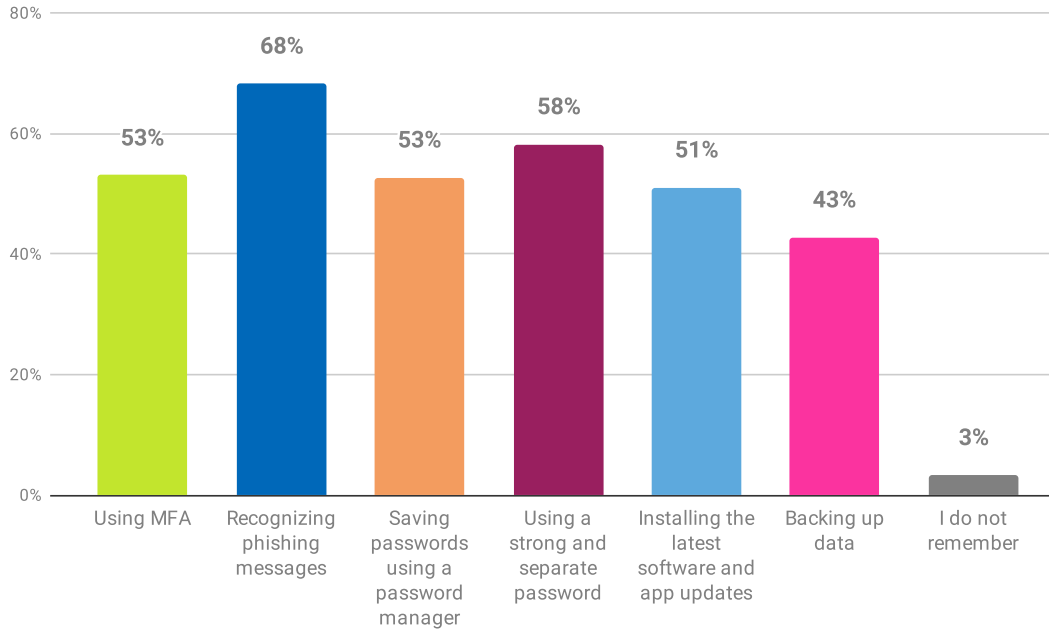


Figure 24. Topics covered in cybersecurity training.

Base: US, UK, & Canada based participants (aged 18+), total number of participants: 905, dates conducted: June 29 2022 - July 19 2022.

Almost half of participants (48%) noted training completed in their home environments were 'extremely useful'. On average, usefulness at home environment was rated highly on a 5-point scale (M=4.2, SD=0.95, N=392[1]).

1 This includes 136 participants who stated they access cybersecurity training at both home and work environments.

Training courses received at work or a place of education were also reported as ‘extremely useful’ by 41 percent of participants. Again, usefulness was rated highly on a 5-point scale (M=4.1, SD=0.97, N=649).

Participants were asked if training had any impact on their cybersecurity behaviors. More than half (58%) noted they were better at recognizing phishing messages and 45 percent had started using strong and unique passwords *(Figure 25)*. 40 percent had started using MFA.

These figures seem positive, but it’s important to remain objective. If you discount people’s ability to recognise phishing emails, the takeaway here is–on average–training doesn’t affect behavior over 60% of the time.

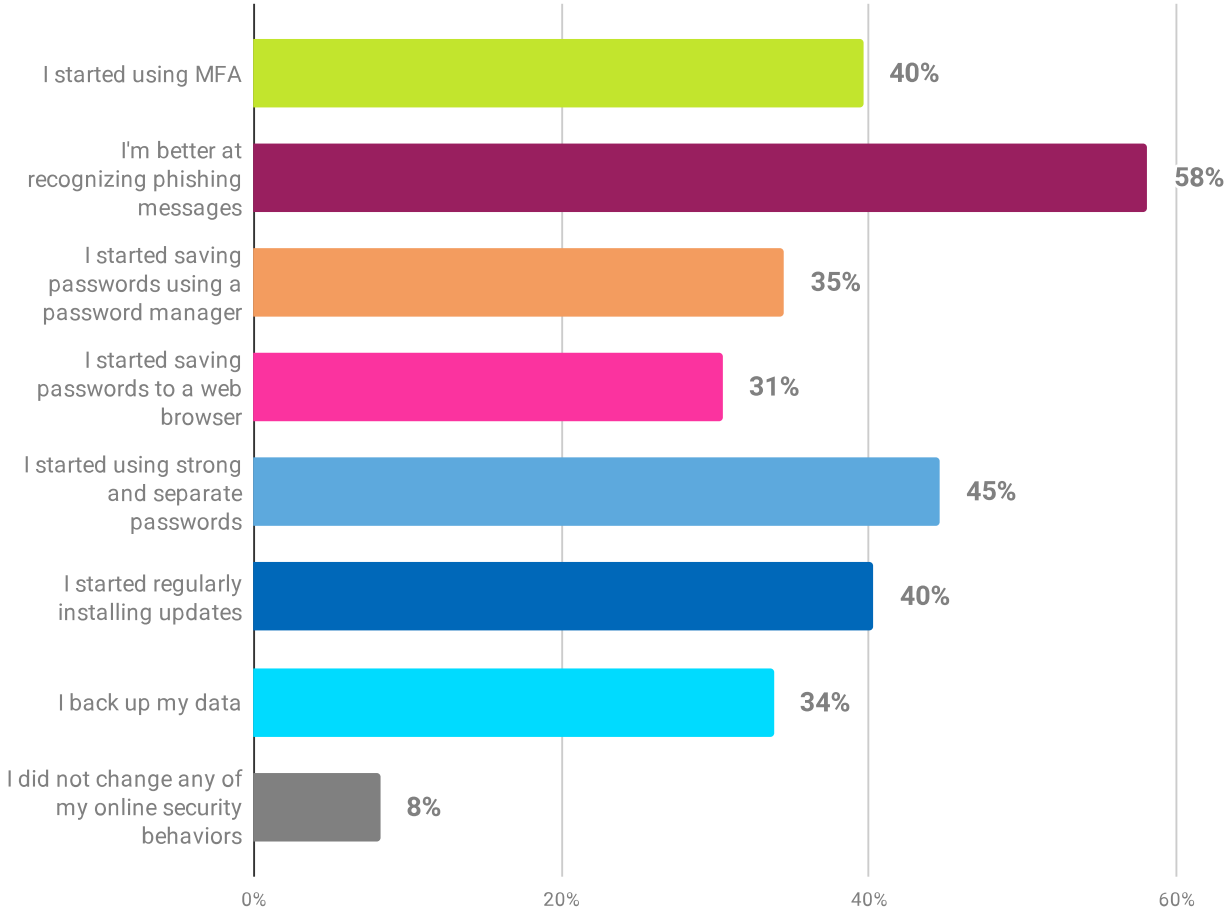


Figure 25. Training impact on participants’ cybersecurity behaviors.

Base: US, UK, & Canada based participants (aged 18+), total number of participants: 905, dates conducted: June 29 2022 - July 19 2022.

Cybercrime victimization

Can we just pause here and take a second to point out we've come all this way and still haven't used an image of a man wearing a black hoodie, hunched over a laptop, with a shadow cast over his face? That's got to be some record for a cybersecurity report, right?

We asked participants about their perceptions and attitudes toward cybercrime victimization, and if they had been victims of any of the four types of cybercrime (phishing, identity theft, romance scams, or cyberbullying). We also covered crime reporting rates and reasons for (not) reporting)

Attitudes towards victimization

The FBI's Internet Crime Complaint Center (IC3) in the US reported $6.9bn losses and Action Fraud in the UK reported £2.35bn losses to cybercrime in their respective 2020/21 annual crime reports reports[1,2]. Thus, we investigated if participants thought themselves to be a likely victim of a cybercrime.

Over a quarter of participants (27%) felt they are unlikely targets of cybercrime, whilst around half (43%) said they could be targeted by criminals *(Figure 26)*.

A larger proportion of participants (57%) were worried about falling victim to cybercrime. This suggests people's perceptions are divided, with some fully unaware of the risk. Yikes.

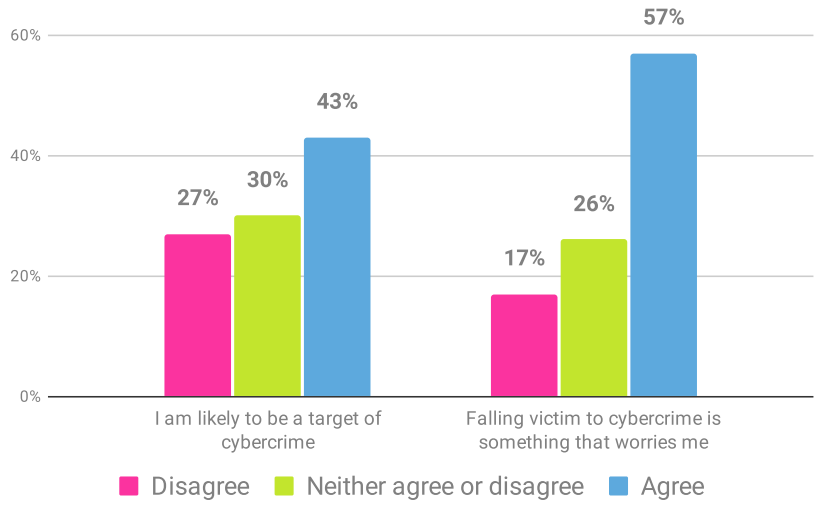


Figure 26. Participants' responses to two statements about perceived likelihood of becoming a victim of cybercrime and concerns about it.

Base: US, UK, & Canada based participants (aged 18+), total number of participants: 3000, dates conducted: June 29 2022 - July 19 2022.

1 https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

2 https://data.actionfraud.police.uk/cms/wp-content/uploads/2021/07/2020-21-Annual-Assessment-Fraud-Crime-Trends.pdf

Over half of participants felt it worthwhile to protect themselves online (53%), and that losing money over the internet is avoidable (53%; *Figure 27*). This is positive, suggesting some people understand the importance of protective security behaviors.

However, 34 percent perceived the loss of personal information as 'unavoidable', viewing themselves as unable to stop their personal details being stolen.

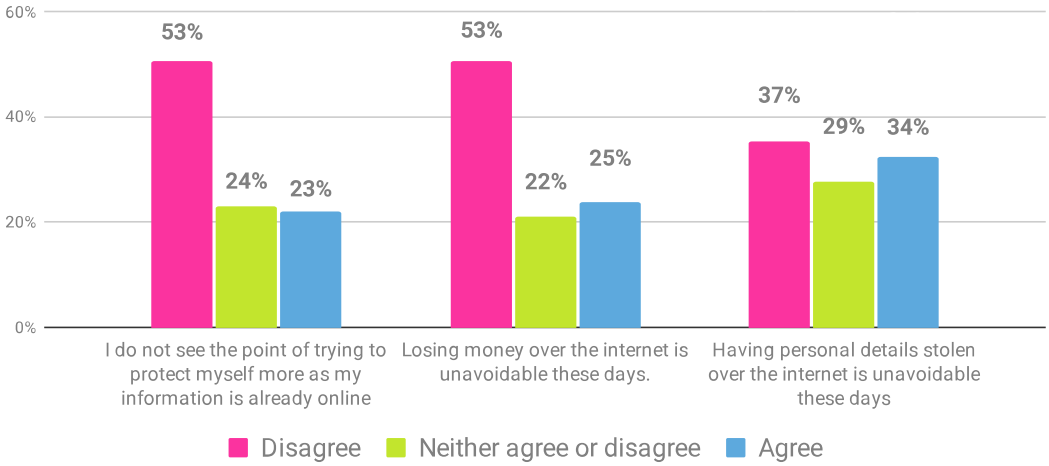


Figure 27. Participants' perceptions about the value of protection and avoidability of losing money or personal details over the Internet.

Base: US, UK, & Canada based participants (aged 18+), total number of participants: 3000, dates conducted: June 29 2022 - July 19 2022.

Cybercrime prevalence

Participants disclosed 1,717 cybercrime-related incidents. 34 percent of participants disclosed being a victim of at least one type of cybercrime—the same proportion as reported in 2021. Fourteen percent of participants had been a victim of two or more types of cybercrime.

The most common type of cybercrime incidents leading to loss of money/data were phishing related (36%; *Figure 28*).

Let's look at each of the crime types in detail.

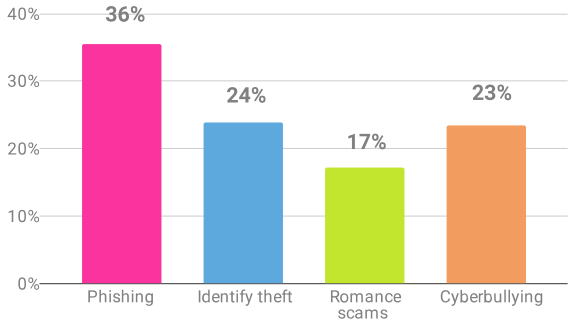


Figure 28. Types of cybercrime incidents.

Base: US, UK, & Canada based participants (aged 18+), total number of incidents: 1,717, dates conducted: June 29 2022 - July 19 2022.

Phishing scams

Cybercriminals trick people with phishing scams using various methods. Their intent is nearly always to gain sensitive information, or to encourage people to click on malicious links to steal money and/or data. In total, 610 phishing incidents resulting in loss of money or data were noted by participants.

As noted earlier, 64 percent of Gen Zs are connected online at all times. Unsurprisingly, over a third of them (34%) reported having lost data or money due to phishing, compared to older generations who were almost three times less likely to have been victims of phishing *(Figure 29)*.

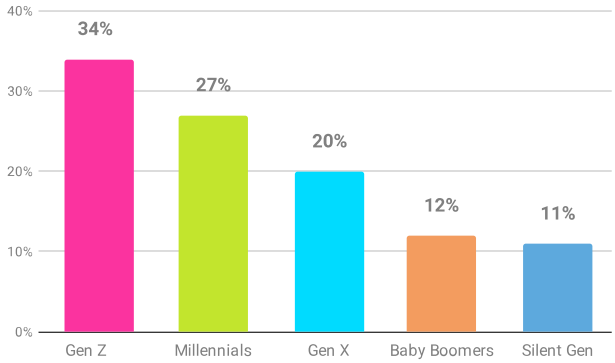


Figure 29. Victim of phishing by generation.

Base: US, UK, & Canada based participants (aged 18+), total number of participants: 607, dates conducted: June 29 2022 - July 19 2022.

Reporting phishing scams

Of those participants who disclosed being a victim of phishing, most (69%) reported to another person, to the company in question, or to the authorities.

Thirty-one percent did not report crime that had led to loss of money and/or data. Those who did report notified their bank (55%) and/or the service/application provider where they had lost their money or data (29%; *Figure 30*).

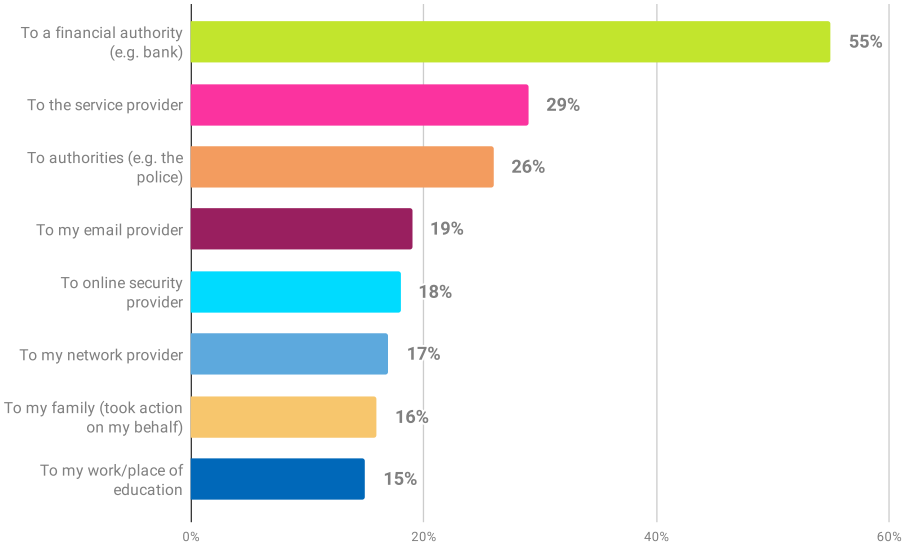


Figure 30. Who was the phishing incident reported to?

Base: US, UK, & Canada based participants (aged 18+), total number of reporting participants: 418, dates conducted: June 29 2022 - July 19 2022.

Of those who'd been victims and reported the incident, the majority (85%) did not perceive reporting as difficult, even if they did not previously know how to do it. The main reason people gave for reporting phishing was to make sure it did not happen to them or others again (51%). Humanity ain't all that bad, folks.

The 31 percent of participants who had been victims of a phishing scam and had not reported were asked why. The top reasons they gave were: not knowing who to report it to (25%), having no need to as they were contacted by the organization (22%), and feeling there was not any point in doing so (20%).

Identity theft

Overall, criminals stealing participants' identities was the second most prevalent incident (24%).

Of those who'd been victims of identity theft, Millennials (20%) and Gen Zs (18%) reported the highest rates of victimization *(Figure 31)*. However, in comparison to other cybercrime types, older age groups also reported higher rates of having been identity theft targets (8% of Baby Boomers and 13% of Silent Gen).

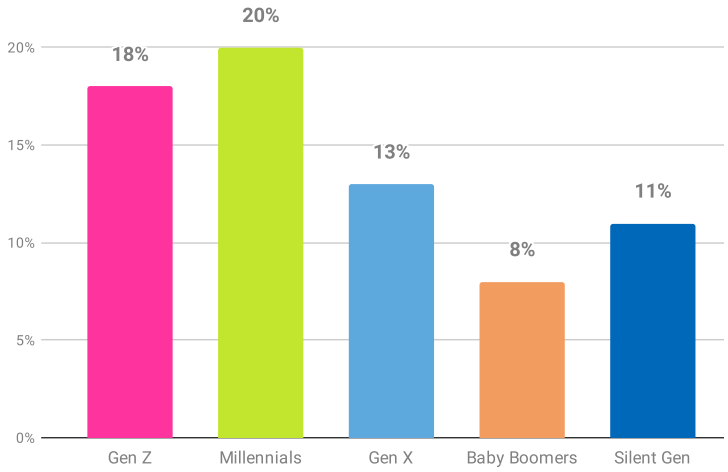


Figure 31. Victim of identity theft by generations.

Base: US, UK, & Canada based participants (aged 18+), total number of participants: 409, dates conducted: June 29 2022 - July 19 2022.

Reporting identity theft

Many participants (74%) mentioned reporting identity theft. An 11 percent increase from last year.

Across the generations, Gen Xs and Baby Boomers (both 81%) reported most of the incidents. Gen Zs and Millennials, in comparison, reported 59% and 69%, respectively *(Figure 32)*. Almost one third of the Millennials (31%) did not report identity theft to anyone, a decrease from last year (46%).

Most of those reporting identity theft (64%) reported to financial organizations (e.g. banks and credit companies; *Figure 33*). However, fewer reports (36%) were made to the authorities (e.g. the police).

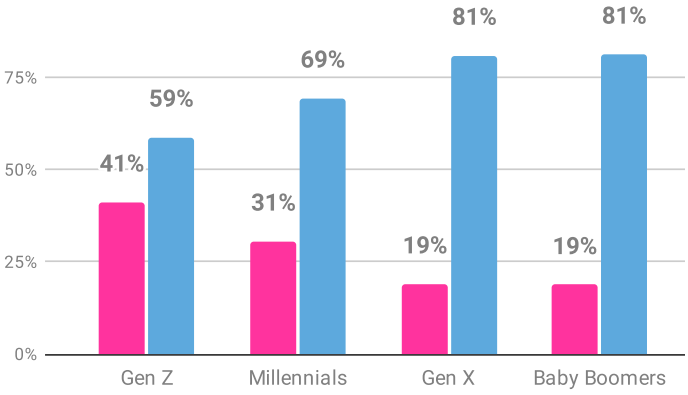


Figure 32. "Did you report the identity theft incident to anyone?" by generation.

Base: US, UK, & Canada based participants (aged 18+), total number of participants: 409, dates conducted: June 29 2022 - July 19 2022.

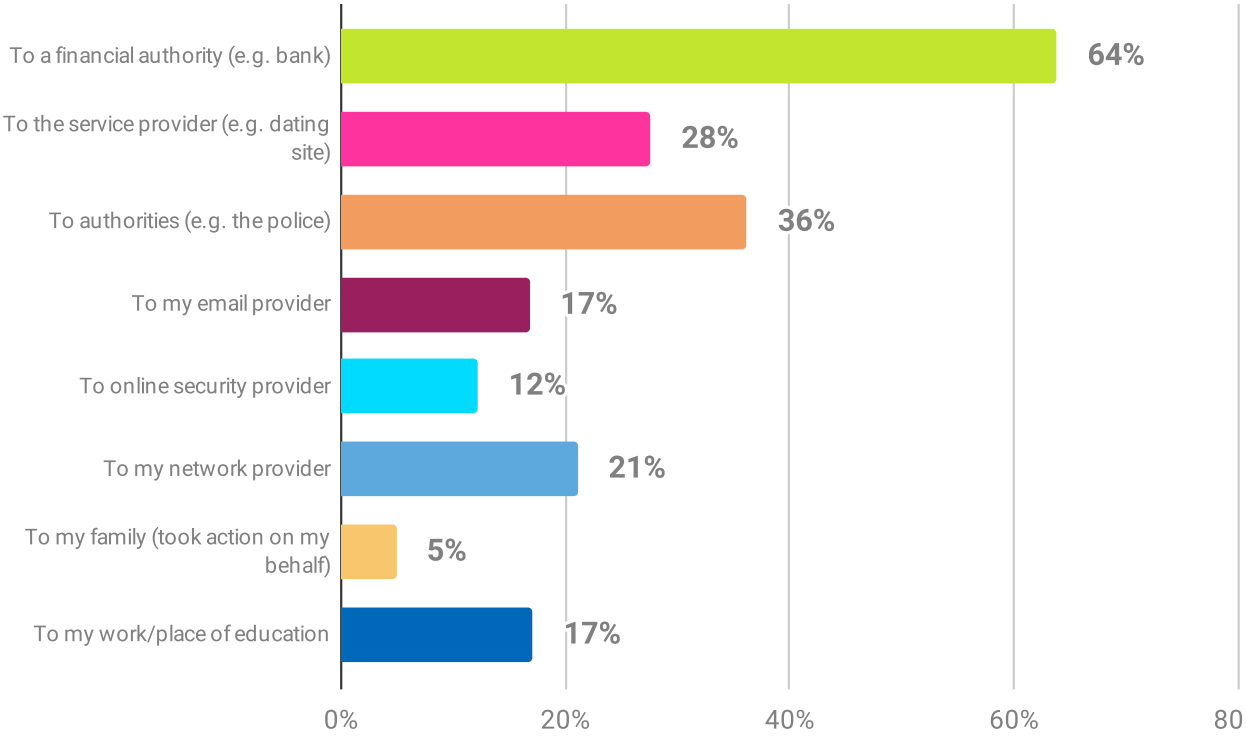


Figure 33. Who was identity theft reported to?

Base: US, UK, & Canada based participants (aged 18+), total number of reporting participants: 304, dates conducted: June 29 2022 - July 19 2022.

Eighty-two percent of participants found reporting identity theft easy, even if they had no previous information about it. Eighteen percent said reporting was difficult, but they eventually managed. The main reason for reporting identity theft was to ensure it does not happen again to them or others (55%). Here's to people looking out for each other!

Of those who did not report identity theft to anyone, 23 percent said they did not know who to report to, and seventeen percent they did not know how. Twenty percent said the process required too much effort.

Romance scams

Despite the recent media attention, romance scams were the least commonly noted crime type. Participants noted 295 incidents of scammers adopting a fake online identity and creating an illusion of a close relationship in order to steal money

Younger generations, Gen Zs (15%) and Millennials (18%), noted higher rates of falling for romance scams than older generations (i.e. over 42 years olds; *Figure 34*).

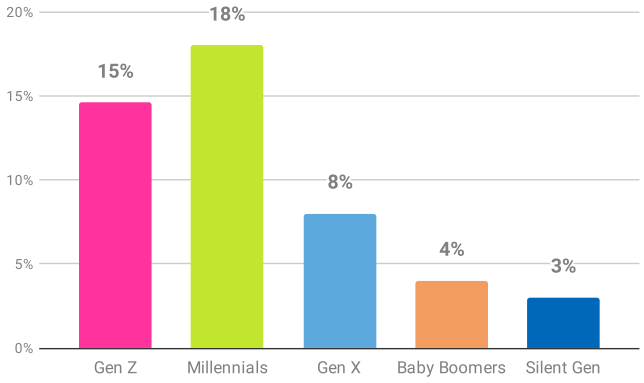


Figure 34. Victim of a romance scam by generation.

Base: US, UK, & Canada based participants (aged 18+), total number of participants: 295, dates conducted: June 29 2022 - July 19 2022.

Reporting romance scams

Fifty-five percent of romance scams were reported. Across the generations, romance scam reporting rates were the highest for Millennials (62%) and lowest for Baby Boomers (33%; *Figure 35*).

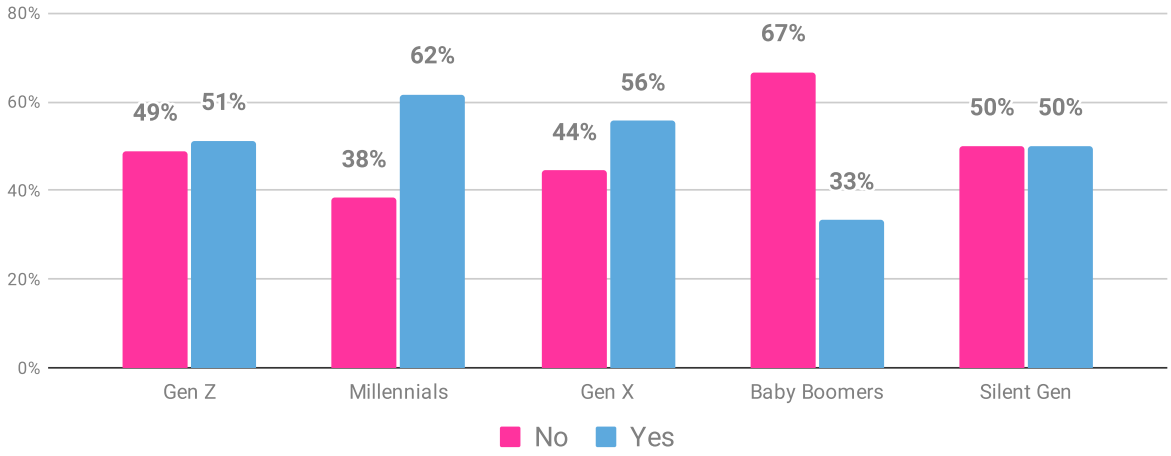


Figure 35. "Did you report the romance scam to anyone?" by generation.

Base: US, UK, & Canada based participants (aged 18+), total number of reporting participants: 295, dates conducted: June 29 2022 - July 19 2022.

Out of 163 participants who had fallen for a romance scam and had reported the incident, 36% reported it to the authorities (e.g. the police). This was followed closely by other parties such as network providers (34%), work or place of education (30%), and online security providers (29%; *Figure 36*).

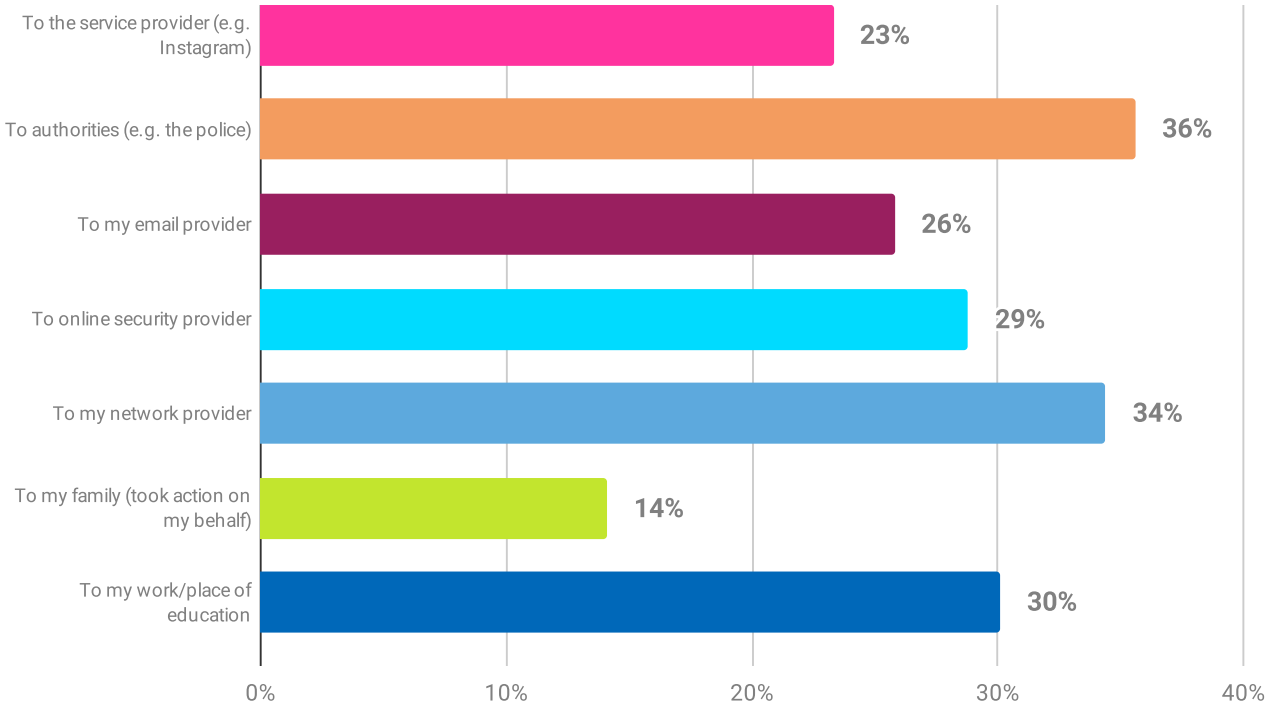


Figure 36. Who was the romance scam reported to?

Base: US, UK, & Canada based participants (aged 18+), total number of reporting participants: 163, dates conducted: June 29 2022 - July 19 2022.

As with phishing incidents, of the participants who reported romance scams, most (85%) found the reporting process easy. Many (63%) highlighted the importance of reporting romance scams so they do not happen to them, or others, again.

Those who did not report romance scams believed there was 'no point' doing so (19%). Seventeen percent did not know who to report to, and another seventeen percent felt too ashamed to.

Cyberbullying

Four hundred and two incidents of cyberbullying were reported by participants. The act of sharing personal or private information to cause embarrassment or humiliation was mainly experienced by younger generations.

Similar to phishing scams, Gen Zs (37%) reported highest rates of having been victims of cyberbullying *(Figure 37)*. Within Silent Gen, only five cases (4%) of cyberbullying were noted.

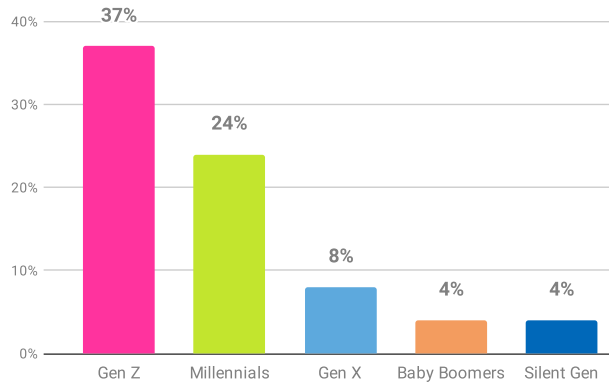


Figure 37. Victim of cyberbullying by generation[1].

Base: US, UK, & Canada based participants (aged 18+), total number of participants: 401, dates conducted: June 29 2022 - July 19 2022.

Reporting cyberbullying

Forty-eight percent of cyberbullying-related crimes were not reported. The reporting rates for cyberbullying across the generations were between 50 and 53 percent [2]. Thirty-eight percent were reported to authorities, to network providers (37%), and to work or place of education (36%; *Figure 38*).

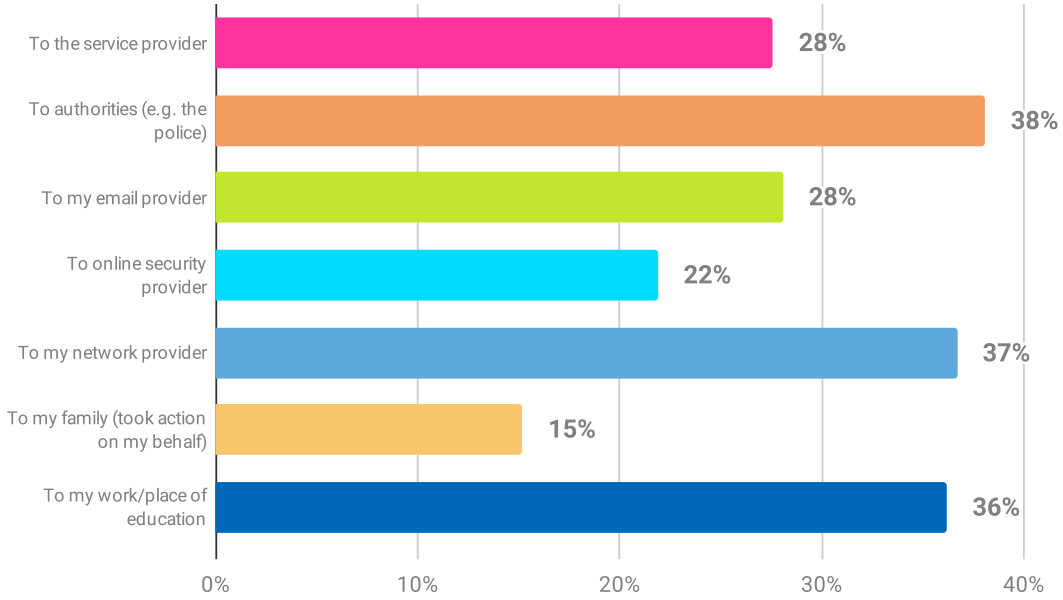


Figure 38. Who was cyberbullying reported to?

Base: US, UK, & Canada based participants (aged 18+), total number of reporting participants: 210, dates conducted: June 29 2022 - July 19 2022.

Of those who had reported cyberbullying, almost all (91%) noted reporting was easy. They either knew who to report or, if they did not know, it was easy to find out.

1 Excludes 1 participant who preferred not to state their age.

2 We have excluded Silent Gen due to only 5 participants. 4 out of 5 had reported cyberbullying to someone.

As with other scams, 64 percent wanted to notify the authorities to prevent others falling victim.

Those who did not report cyberbullying (48%) said they did not believe there was any point doing so (32%), or they did not know who to report it to (25%).

General cybersecurity attitudes

Something we can all relate to coming up...technology is awesome...when it works. When it doesn't, the overwhelming desire to 'defenestrate' things takes over.

In short, we recognise the value in staying safe online, but technology and information about technology can be confusing and frustrating.

Defenestrate: look it up. It's one of the most perfect words in the English language.

We asked participants if they think their devices are 'automatically secure'. Over a third (35%) agreed with the statement *(Figure 39)*. Nearly half (48%) believed it was expensive to fully protect themselves online.

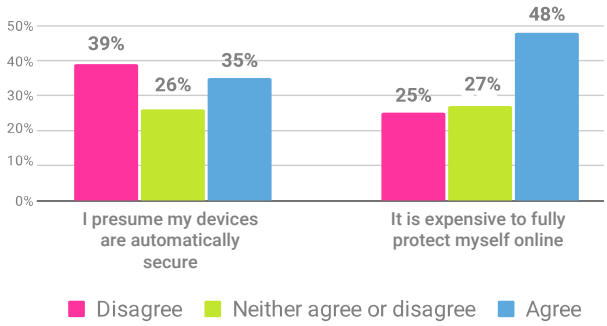


Figure 39. Participants' levels of agreement to device security and cost statements.

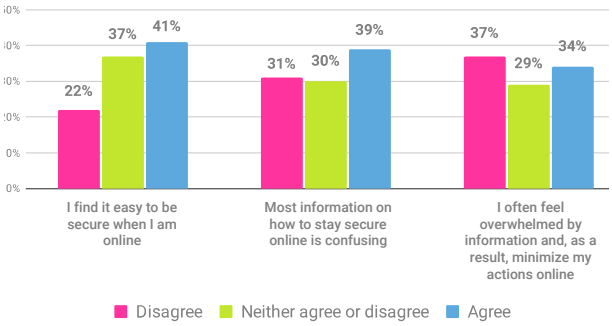
Base: US, UK, & Canada based participants (aged 18+), total number of participants: 3000, dates conducted: June 29 2022 - July 19 2022.

Twenty-two percent found it 'difficult' to stay safe online *(Figure 40)*.

Thirty-nine percent agreed most information on how to stay secure online is confusing. In addition, one third (34%) noted they often feel overwhelmed by information and, as a result, minimize their online actions.

Figure 40. Participants' levels of agreement to cybersecurity ease, clarity, and being overwhelmed.

Base: US, UK, & Canada based participants (aged 18+), total number of participants: 3000, dates conducted: June 29 2022 - July 19 2022.



Older generations (see *Figure 41*) found it more difficult to stay secure online (with 28% of Baby Boomers and 29% of Silent Gens disagreeing with the statement), in comparison to those under 57 years of age (disagreement ≤ 20%).

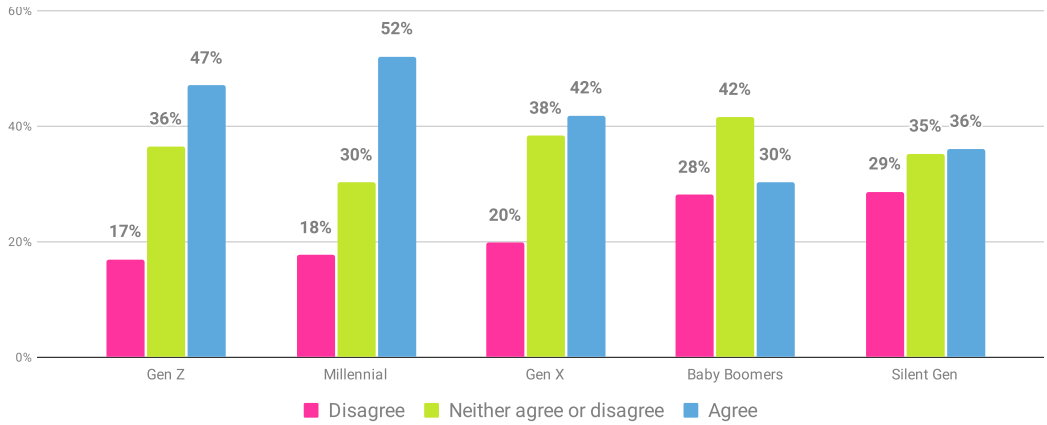


Figure 41. Participants' levels of agreement with the statement "I find it easy to be secure when I am online" by generations.

Base: US, UK, & Canada based participants (aged 18+), total number of participants: 2979, dates conducted: June 29 2022 - July 19 2022.

Gen Zs (39%) and Millennials (45%) often felt overwhelmed by information and, as a result, minimized their actions online. In comparison, the older generations disagreed with the statement *(Figure 42)*.

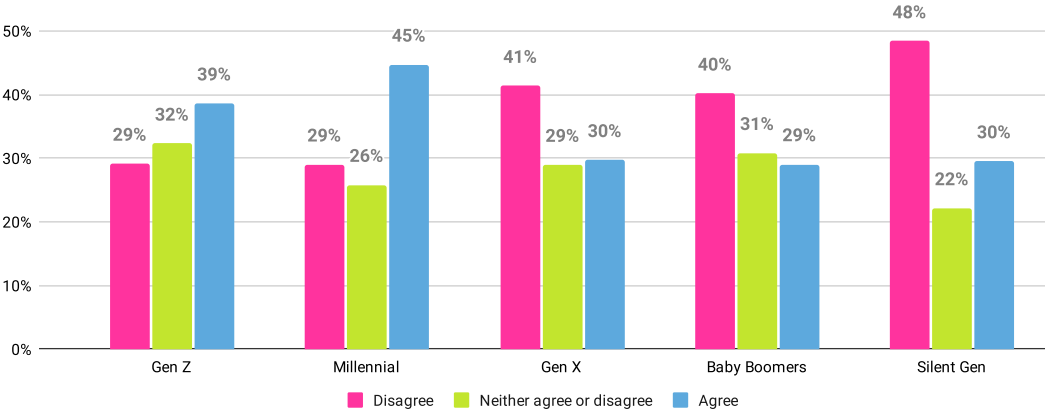


Figure 42. Participants' levels of agreement to the statement "I often feel overwhelmed by information and, as a result, minimize my actions online" by generations.

Base: US, UK, & Canada based participants (aged 18+), total number of participants: 2979, dates conducted: June 29 2022 - July 19 2022.

Some generational differences were found with the general level of confusion with cybersecurity information *(Figure 43)*.

Younger generations (39% of Gen Zs and 48% of Millennials) found security to be confusing, in comparison to older generations where between 32 and 38 percent found information more straightforward.

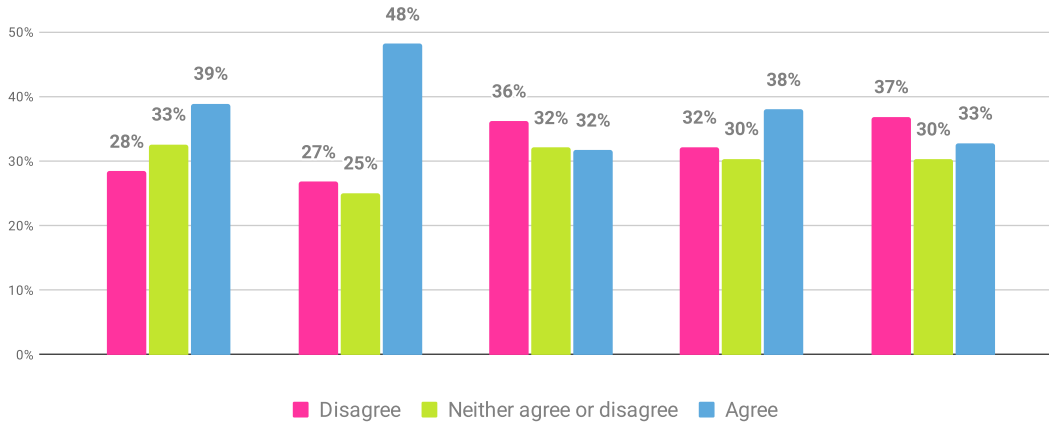


Figure 43. Participants' levels of agreement to the statement "Most information on how to stay secure online is confusing" by generations.

Base: US, UK, & Canada based participants (aged 18+), total number of participants: 2979, dates conducted: June 29 2022 - July 19 2022.

Broadly speaking, and similar to last year's report, feelings towards staying safe online were positive.

Many participants noted staying secure is a priority for them (78%), is achievable (66%), under their control (52%), and possible (51%; *Figure 44*).

That said, participants also felt staying secure was also frustrating (46%), and intimidating (44%).

A note to those providing information: the focus should be on simplifying existing material.

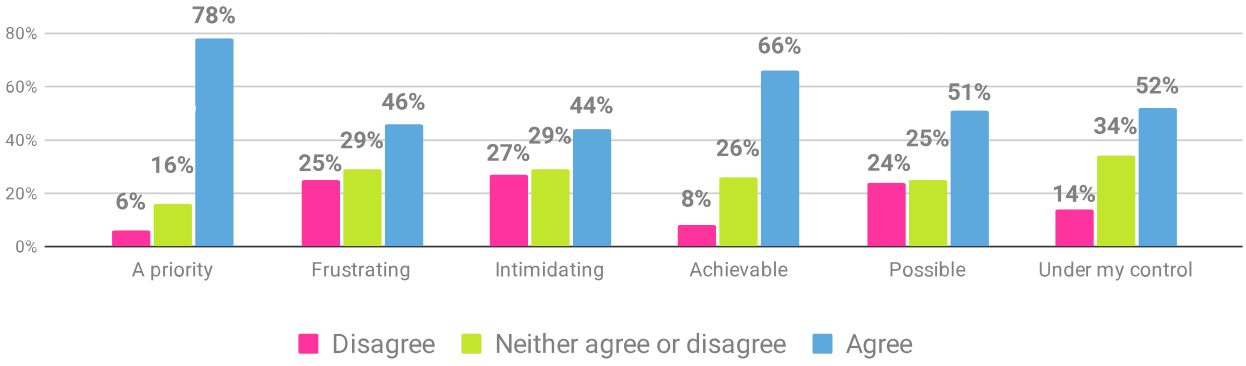


Figure 44. Participants' levels of agreement with answering "I feel that staying secure online is..."

Base: US, UK, & Canada based participants (aged 18+), total number of participants: 3000, dates conducted: June 29 2022 - July 19 2022.

Generational differences were found among three statements concerning priority *(Figure 45)*, cybersecurity being 'possible' *(Figure 46)*, and feeling intimidated *(Figure 47)*.

Gen Zs (64%) did not rate cybersecurity as high a priority as older generations (ranging from Millennials 74% to Silent Gens 87% agreement; *Figure 45*).

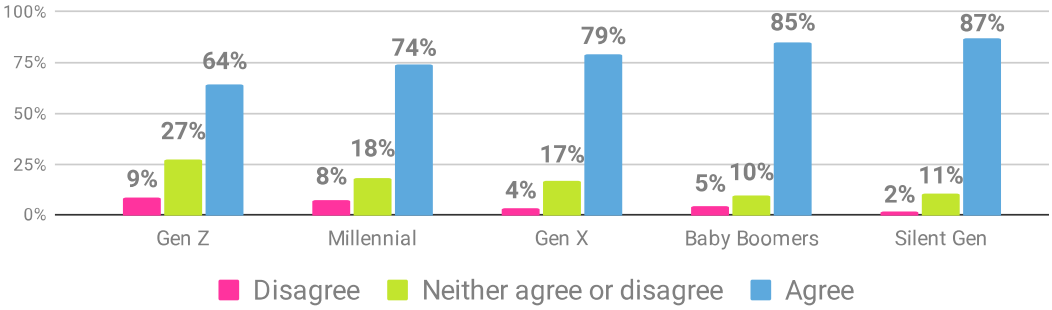


Figure 45. Participants' levels of agreement with answering "I feel that staying secure online is... a priority" by generation.

Base: US, UK, & Canada based participants (aged 18+), total number of participants: 2979, dates conducted: June 29 2022 - July 19 2022.

Younger generations (Gen Zs and Millennials) felt frustrated, saying staying safe online is 'impossible' *(Figure 46)*. Other generations (30% of Gen Zs and 40% of Millennials) felt more positive.

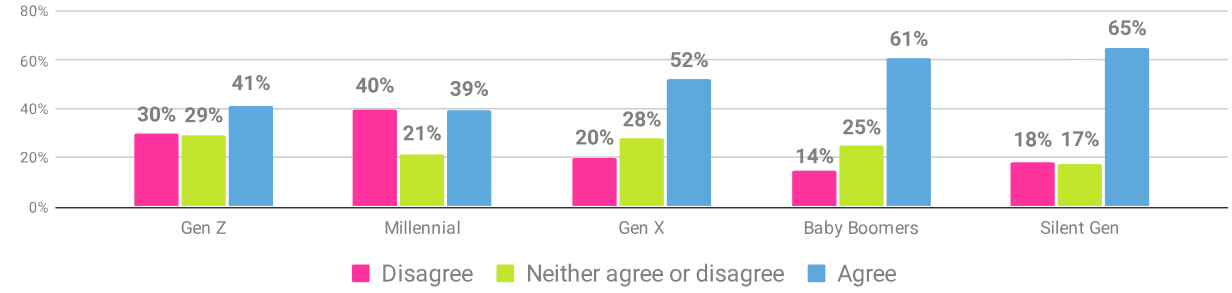


Figure 46. Participants' levels of agreement with the statement "I feel that staying secure online is... possible" by generation.

Base: US, UK, & Canada based participants (aged 18+), total number of participants: 2979, dates conducted: June 29 2022 - July 19 2022.

When asked about feelings of intimidation regarding cybersecurity, Millennials (48%) and Gen Zs (45%) felt most intimidated. Only a quarter of them disagree with the statement *(Figure 47)*.

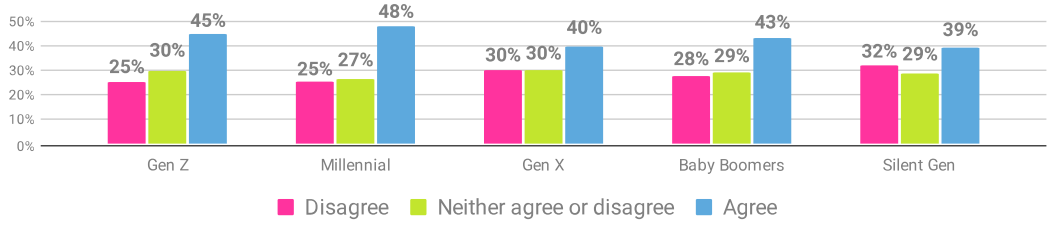


Figure 47. Participants' levels of agreement with the statement "I feel that staying secure online is... intimidating" by generation.

Base: US, UK, & Canada based participants (aged 18+), total number of participants: 2979, dates conducted: June 29 2022 - July 19 2022.

Cybersecurity responsibility

From workplaces to homes, our information is useful to anyone who wants to cause harm. But, who do we think should take responsibility for our online information, or the information of the organizations we work for?

When participants were asked about who had the main responsibility for protecting online information, the responses reflected last year's findings.

The most responsible agent to protect an individual's personal information online was seen as the person themselves (59%). Hoo-ray!

Participants' families (58%), employers (43%), and governments (39%) were seen as the least responsible to do so *(Figure 48)*.

Thirty-seven percent placed responsibility primarily on the application/service providers. This isn't surprising. Lots of information is shared with online platforms, which are often in the news for not keeping our data safe.

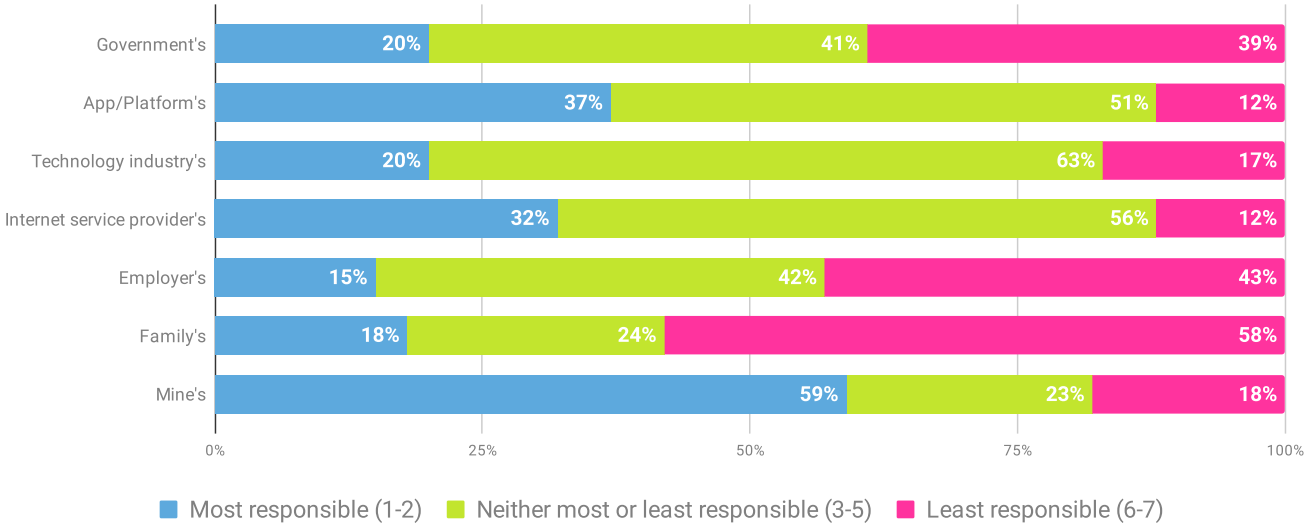


Figure 48. Participants' rankings of responsibility in answering "Whose main responsibility is it to protect your online information?"

Base: US, UK, & Canada based participants (aged 18+), total number of participants: 3000, dates conducted: June 29 2022 - July 19 2022.

Governments (48%) and participants themselves (38%) were perceived to be the least responsible for protecting workplace information.

Here, the organization (43%) and its IT (36%) and security (28%) departments were ranked as the most responsible agencies *(Figure 49)*.

Still, it seems, there is an inherent culture of a lack of personal responsibility for protecting workplace information. As Deanson Senda, Cyber Security Awareness and Culture Consultant, puts it - “They can be aware, but they just don’t care!”

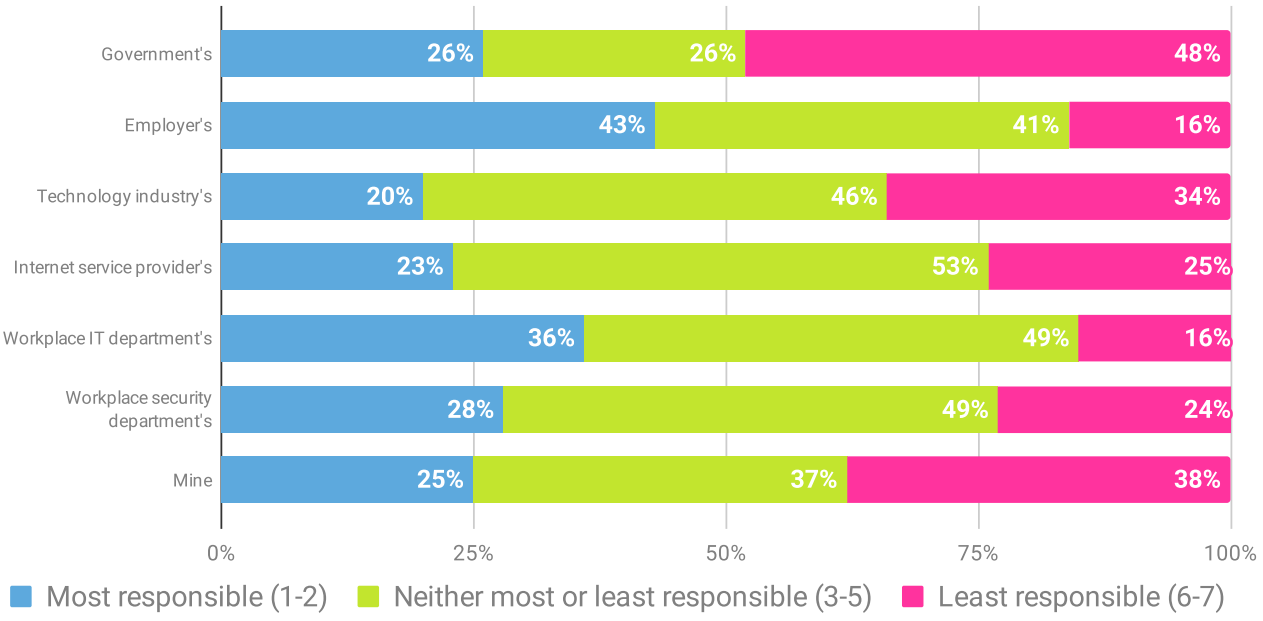


Figure 49. Participants’ rankings of responsibility in answering “Whose main responsibility is it to protect your workplace’s online information?”

Base: US, UK, & Canada based participants (aged 18+), total number of participants: 1762, dates conducted: June 29 2022 - July 19 2022.

Cybersecurity behaviors, practices, and attitudes

Unfortunately, as far as we know, there isn’t a cybersecurity Naughty or Nice List. That means conducting research is the only way to find out if people have been on their best security behavior.

So far, this report has shown a snapshot of general attitudes towards cybersecurity, as well as people’s views on who is responsible for security. It has looked at how people experience cybersecurity training, the rate of victimization, and how different types of cybercrime are reported.

In this section, we look at five security behaviors, and explore the rate of good cybersecurity practices and people’s attitudes towards their undertaking.

Password hygiene

Over a third of participants (38%) noted they held more than 10 important online accounts holding sensitive information (e.g. accounts related to work, social media and payment-related websites).

To this effect we asked participants questions in relation to their passwords behaviors. We were particularly interested in three sub-behaviors: creation of passwords, the frequency of changing them, and password management strategies.

Creation of passwords

When creating their passwords, 29 percent of participants used a single dictionary word or name with some characters replaced with numbers or symbols (e.g. p@ssw0rd and Jon@th4n). In other words, they used weak passwords.

A quarter (25%) of participants also admitted their passwords included references to personal information, such as names and dates. Only 16 percent of participants reported creating passwords over 12 characters long *(Figure 50)*.

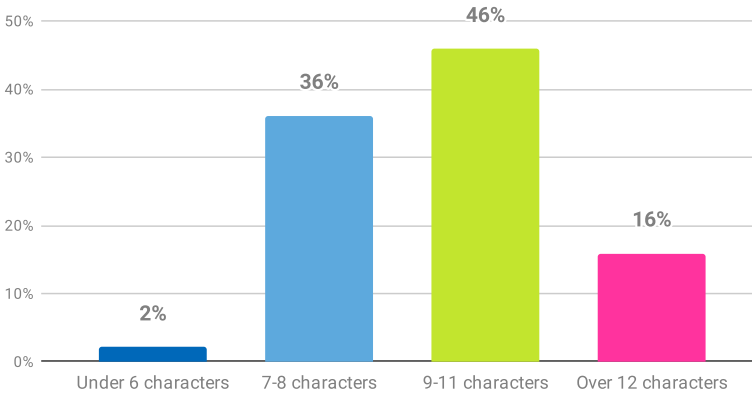


Figure 50. Typical length of passwords created by the participants.

Base: US, UK, & Canada based participants (aged 18+), total number of participants: 3000, dates conducted: June 29 2022 - July 19 2022.

In addition to low password lengths, over a third (36%) reported using separate passwords half of the time, less than half, or not at all *(Figure 51)*.

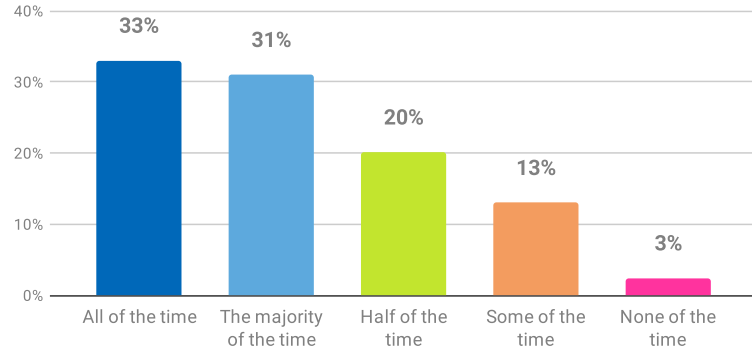


Figure 51. "How often do you use unique/separate passwords for your important online accounts?[1]"

Base: US, UK, & Canada based participants (aged 18+), total number of participants: 2589, dates conducted: June 29 2022 - July 19 2022.

Out of those who said they use separate passwords 'some of the time' (13%) or 'none of the time' (3%), 63 percent said it's because they are too difficult to remember.

Frequency of changing passwords

Thirty-six percent reported that they changed their passwords every few months, with 29 percent saying they do not change them unless they are forced to do so *(Figure 52)*.

1 This question was only asked to participants who noted having more than one account.

The UK's National Cyber Security Center[1] suggests forcing people to change their passwords can backfire, due to the level of inconvenience and perceived burden. This is consistent with the National Institute of Standards and Technology (NIST) guidance in the US[2].

It is a reoccuring theme in this year's report highlighting why people do not always act as securely as they should (see conclusion).

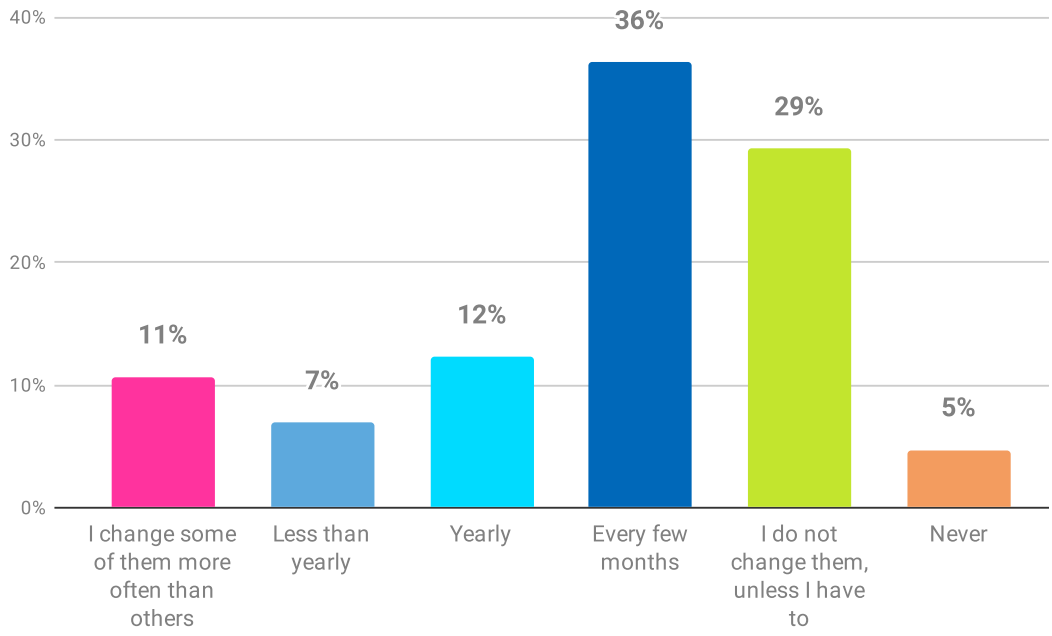


Figure 52. "How often do you tend to change your password(s)?"

Base: US, UK, & Canada based participants (aged 18+), total number of participants: 3000, dates conducted: June 29 2022 - July 19 2022.

Separately, of those who reported changing their passwords, over half (53%) changed to something different, while 35 percent admitted changing either a word, or a few characters (e.g. 'password1!' to 'Password2?').

NCA guidance[3], NCSC's advice[4], and Get Cyber Safe[5] recommend creating separate passwords of at least 12 characters, including letters and numbers, for important online accounts.

1 https://www.ncsc.gov.uk/blog-post/problems-forcing-regular-password-expiry
2 https://pages.nist.gov/800-63-3/sp800-63b.html
3 https://staysafeonline.org/online-safety-privacy-basics/passwords-securing-accounts/
4 https://www.ncsc.gov.uk/blog-post/problems-forcing-regular-password-expiry
5 https://www.getcybersafe.gc.ca/en/secure-your-accounts/passphrases-passwords-and-pins

Over a quarter (29%) included numbers and special characters. A potential reason for low use of long passwords may be the level of user burden and inconvenience.

Despite advice from various sources advocating for 'three random words' (i.e., a passphrase), only six percent reported changing their passwords using this method *(Figure 53)*.

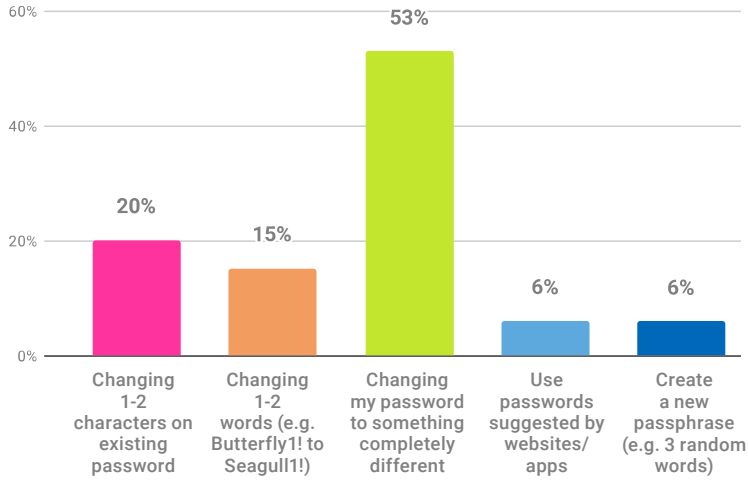


Figure 53. "What action do you most often take when changing your password(s)?"

Base: US, UK, & Canada based participants (aged 18+), total number of participants: 2652, dates conducted: June 29 2022 - July 19 2022.

Use of password management strategies

We asked participants how they manage their multiple passwords online. A third (33%) said they save passwords in their browsers (e.g. Google or Firefox) when prompted 'very often' or 'always' *(Figure 54)*.

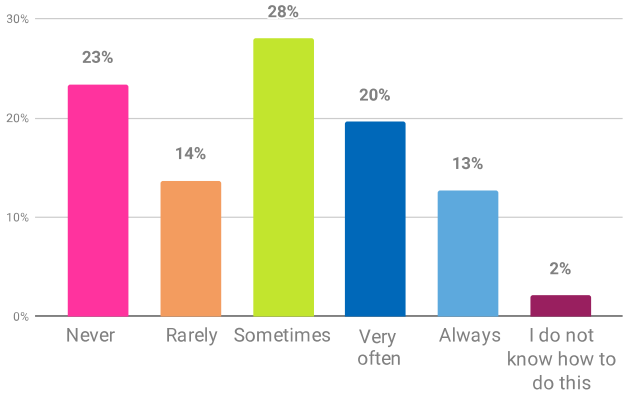


Figure 54. "How often do you save your passwords in the browser when prompted?"

Base: US, UK, & Canada based participants (aged 18+), total number of participants: 3000, dates conducted: June 29 2022 - July 19 2022.

Only 18 percent of participants had downloaded a stand-alone password manager. Of the 541 participants who had downloaded one, 77 percent were still using the application.

Of those who had stopped using a password manager, twenty-nine percent had issues accessing the password manager from other devices, with nineteen percent saying they did not trust the password manager.

Various reasons for not trusting password manager applications were given by the above participants. Interestingly, most comments related to exposing all of the passwords to hackers, as well as the application providers, who could then steal their data.

So, if someone does not use a password manager (browser or stand-alone app) how do they remember their passwords? We asked participants to report on their preferred method of remembering passwords.

Over a third (37%) write them down in a notebook (a five percent increase from last year's report). Twenty-eight percent store them electronically (e.g. on a phone, email, or in a document). Some (22%) reported they 'just remember passwords without writing them down' *(Figure 55)*.

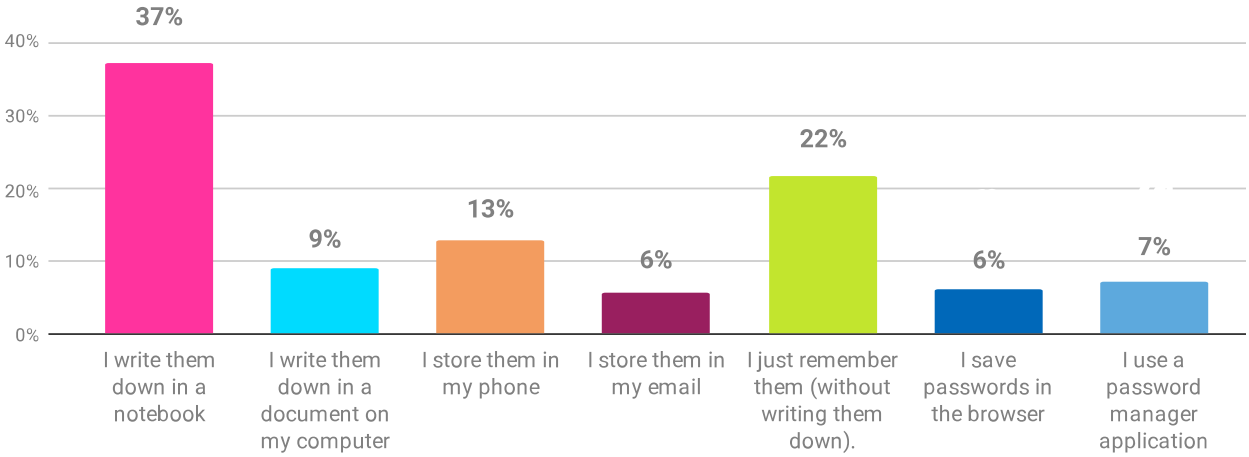


Figure 55. "What is your preferred method of remembering passwords?"

Base: US, UK, & Canada based participants (aged 18+), total number of participants: 2589, dates conducted: June 29 2022 - July 19 2022.

Applying multi-factor authentication (MFA)

Adding MFA (sometimes called two-factor authentication) to online accounts makes them extremely robust. It is disconcerting, then, that 43 percent of participants still hadn't heard about it *(Figure 56)*. Though, this is lower (better) than last year (48%).

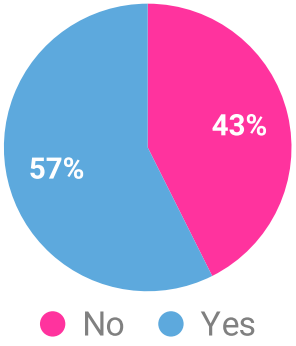


Figure 56. "Have you ever heard of Multi-Factor Authentication?"

Base: US, UK, & Canada based participants (aged 18+), total number of participants: 3000, dates conducted: June 29 2022 - July 19 2022.

Most of the Silent Gen (57%) and over half of the Baby Boomers (46%) had not come across MFA before *(Figure 57).*

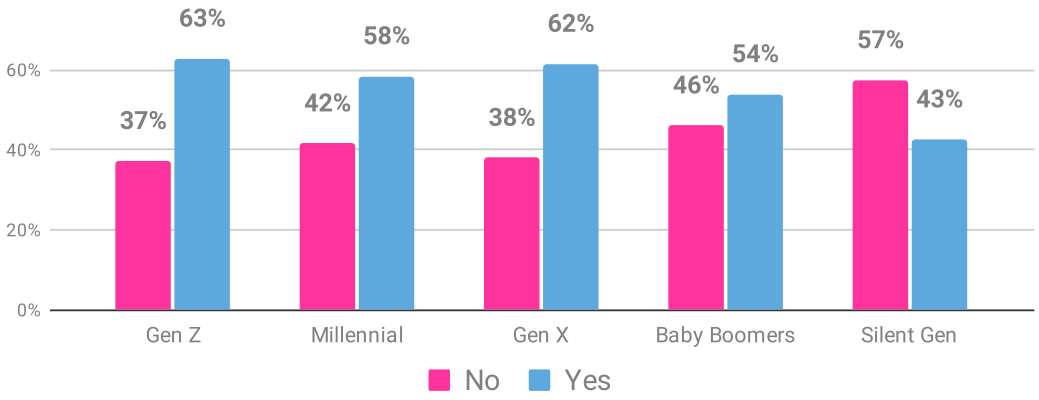


Figure 57. "Have you ever heard of Multi-Factor Authentication?" by generations.

Base: US, UK, & Canada based participants (aged 18+), total number of participants: 2979, dates conducted: June 29 2022 - July 19 2022.

For those who knew what MFA was, 79 percent had applied it at least to one of their accounts and most of them (94%) were still using it.

The six percent who had stopped using MFA mentioned they found it unusable due to devices logging them out too often (26%), not carrying phones with them at all times (24%), and the process taking too long to perform (24%).

Installing software updates and backing up data

Sixty-three percent of participants 'always' or 'very often' installed the latest updates and software *(Figure 58),* a slightly lower number compared to the 2021 report (68%).

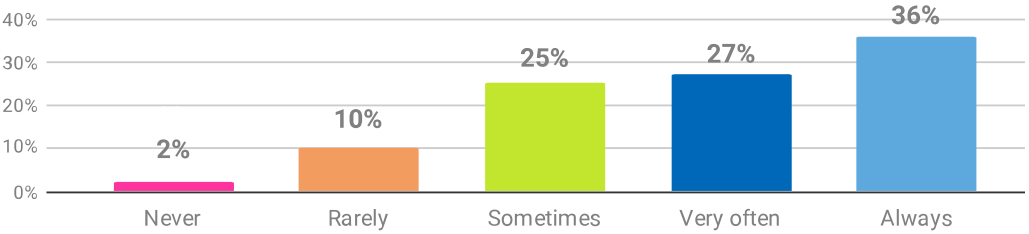


Figure 58. "How often do you install the latest updates and software when notified that they are available?"

Base: US, UK, & Canada based participants (aged 18+), total number of participants: 3000, dates conducted: June 29 2022 - July 19 2022.

Sixty-two percent of participants reported having turned on automatic updates, while a quarter (25%) admitted to clicking 'remind me later' a few times.

Interference with their other applications was the main reason given (30%) by those who 'never' or 'rarely' updated software. Worryingly, 16 percent also reported they do not know how to run updates, with some noting their devices and applications work fine without needing to update them (11%).

Not updating software on devices is a risk. Thus, backing up data is important. Here, 43 percent of participants said they 'always' or 'very often' backup important data, compared to 30 percent in 2021's report. Twenty-one percent said they 'rarely' or 'never' do so *(Figure 59)*.

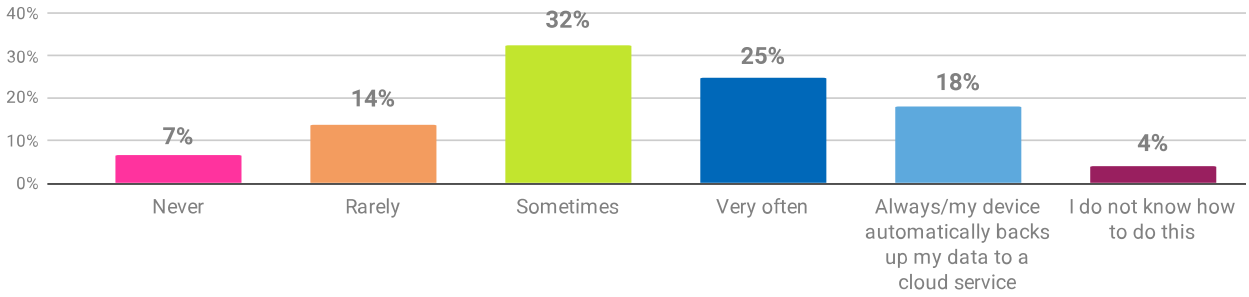


Figure 59. "How often do you back up your most important data?"

Base: US, UK, & Canada based participants (aged 18+), total number of participants: 3000, dates conducted: June 29 2022 - July 19 2022.

Recognizing phishing messages

Participants felt confident in their abilities to recognize phishing emails or malicious links (M=7.3, SD=2.02, N=3000) on a 10-point scale. Overall, 70 percent expressed their confidence in doing so *(Figure 60)*.

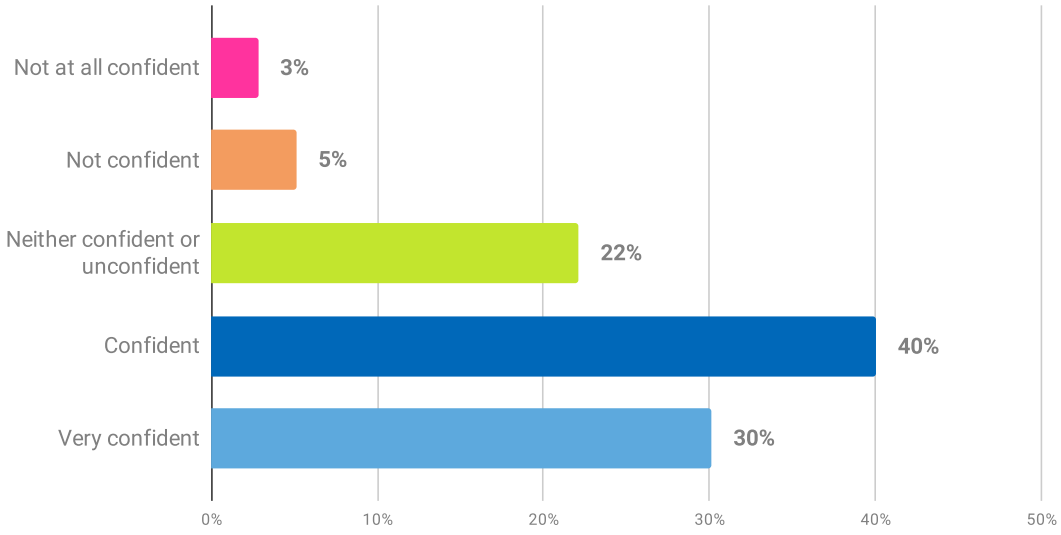


Figure 60. "How confident are you in your ability to identify a phishing email or a malicious link?"

Base: US, UK, & Canada based participants (aged 18+), total number of participants: 3000, dates conducted: June 29 2022 - July 19 2022.

Similarly, 70 percent reported they 'very often' or 'always' check whether messages are genuine before clicking any links or responding *(Figure 61)*. However, 10 percent said they either 'never', 'rarely', or 'do not know how to' check a message for legitimacy.

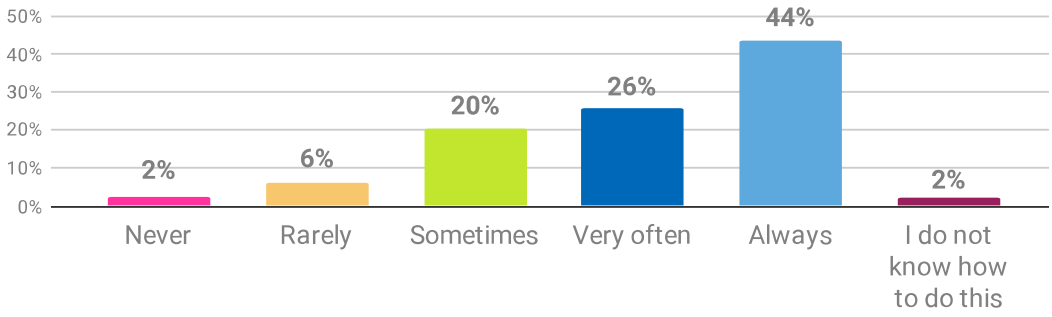


Figure 61. "How often do you check a message is genuine before clicking any links or responding to it?"

Base: US, UK, & Canada based participants (aged 18+), total number of participants: 3000, dates conducted: June 29 2022 - July 19 2022.

Sixty percent of those participants who check message legitimacy check the sender's email address first to make sure the message is genuine, with 27 percent of the participants first paying attention to the message content itself.

Similar to our 2021 report, if they receive an unusual message with links, less than half (45%) report reaching out to the person 'very often' or 'always' to ask about it before clicking *(Figure 62)*.

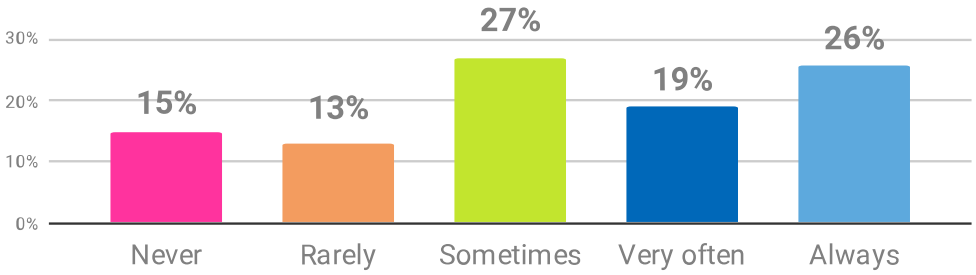


Figure 62. "If someone you know sends you an unusual message with links, how often do you reach out to the person to ask about it before clicking the link?"

Base: US, UK & Canada based participants (aged 18+), total number of participants: 3000, dates conducted: June 29 2022 - July 19 2022.

A quarter (25%) of participants 'never', 'rarely' or 'do not know how to' report phishing emails by marking them as spam or using the 'report' button, while almost half (47%) reported doing so 'very often' or 'always' *(Figure 63).*

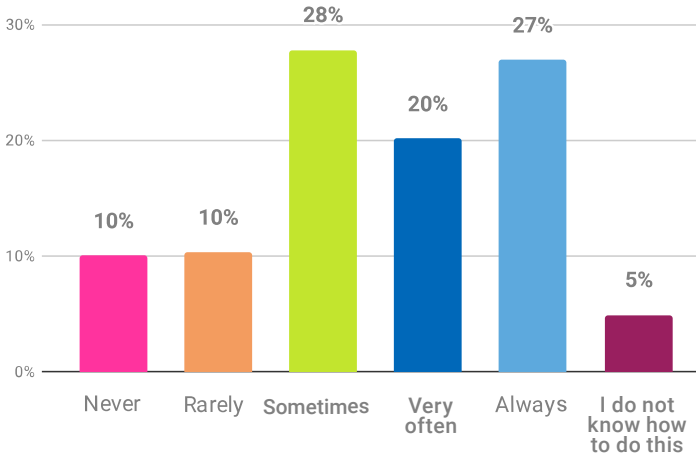


Figure 63. "Do you report any phishing emails by hitting the 'spam' or 'report phishing' button?"

Base: US, UK, & Canada based participants (aged 18+), total number of participants: 3000, dates conducted: June 29 2022 - July 19 2022.

Barriers to cybersecurity behaviors

Yeah, there's always a reason not to do something that's good for you. Like not drinking two liters of water because, you know, it's water, not coffee—urgh. Or not using a stronger password out of fear of forgetting it. But barriers can usually be overcome. The first step is identifying them.

For participants who replied they 'rarely' or 'never' undertake some of the security behaviors (using a password manager, updating devices/applications, using MFA, reporting phishing messages, and backing up data), we asked follow-up questions to explore the barriers preventing them from doing so.

We structured the questions around people's capability, opportunity, and motivation from the COM-B model. COM-B is the most comprehensive psychological model of behavior change, used widely in health-related research[1].

1 Michie, S., Richardson, M., Johnston, M., Abraham, C., Francis, J., Hardeman, W., Eccles, M., Cane, J., & Wood, C. (2013). The behavior change technique taxonomy (v1) of 93 hierarchically clustered techniques: Building an international consensus for the reporting of behavior change interventions. Annals of Behavioral Medicine: A Publication of the Society of Behavioral Medicine, 46.

The COM-B model encourages behavior change by influencing one or more of the COM-B[1] components.

- Capability is a person's psychological and physical capacity to perform a behavior. It includes having the necessary knowledge and skills.
- Opportunity relates to any external factors that make being secure possible/ impossible. This can be both physical and social. For example, having access to training, and time to learn.
- Motivation concerns the mental processes energizing and directing behavior. It includes both automatic (impulses and desires) and reflective (plans and thoughts) motivational processes. For example, people can be motivated to change behaviors through social impact (protecting oneself from cybercriminals also protects others, such as friends, family, and colleagues).

We examined whether participants experienced high or low levels of capability, opportunity, and motivation. We also broke down their main barrier types by each of the five[2] security behaviors.

We found participants' motivation the greatest barrier to performing security behaviors (40% reporting 'low' vs 25% reporting 'high'; *Figure 64*).

Opportunity barriers—with most 'neither agreeing nor disagreeing'— suggested participants had sufficient opportunities to undertake behaviors (e.g. resources and time).

We also noted higher capability (35%), but only a quarter felt motivated enough to take action.

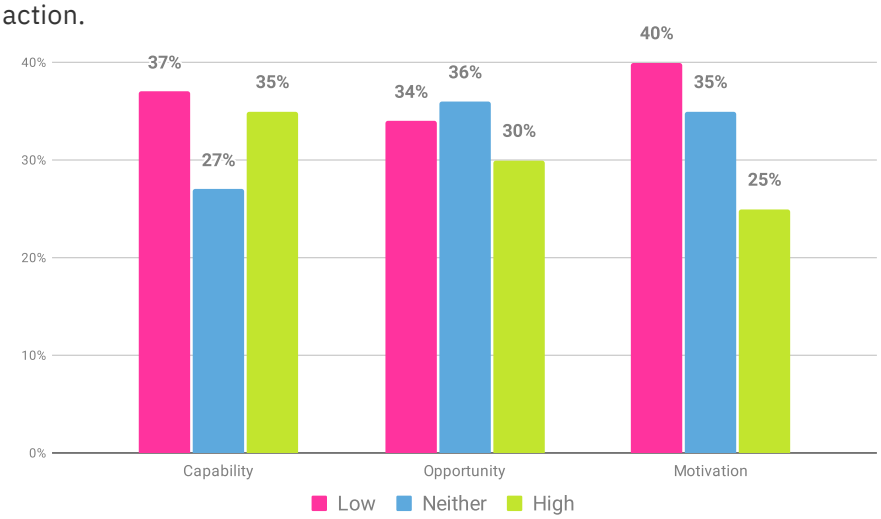


Figure 64. Overall barriers to five security behaviors by capability, opportunity, and motivation.

Base: US, UK, & Canada based participants (aged 18+), total number of participants per security barrier reported: software update 297, MFA use 446, reporting phishing 608, password manager use 2585 and backing up data 609. Dates conducted: June 29 2022 - July 19 2022.

1 Michie, S., Richardson, M., Johnston, M., Abraham, C., Francis, J., Hardeman, W., Eccles, M., Cane, J., & Wood, C. (2013). The behavior change technique taxonomy (v1) of 93 hierarchically clustered techniques: Building an international consensus for the reporting of behavior change interventions. Annals of Behavioral Medicine: A Publication of the Society of Behavioral Medicine, 46.

2 Note that only one of the password hygiene behaviors was included: using password management strategies.

Next, we looked at the differences between each security behavior against each COM-B component.

Capability using MFA was the lowest (36% reported it as low vs 30% high capability; *Figure 65*). Conversely, participants reported higher capability around backing up data (48%) and installing software (45%).

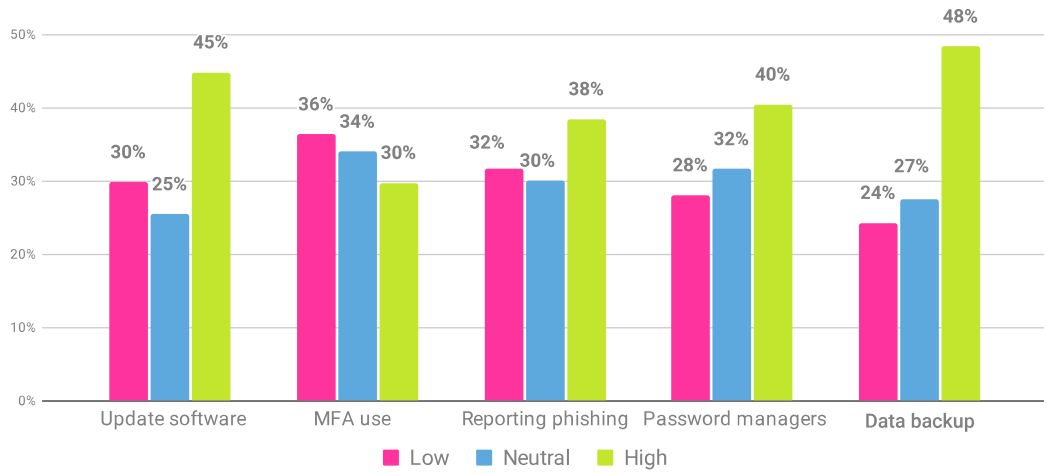


Figure 65. Capability barriers by each security behavior.

Base: US, UK, & Canada based participants (aged 18+), total number of participants per security barrier reported: software update 297, MFA use 446, reporting phishing 608, password manager use 2585 and backing up data 609. Dates conducted: June 29 2022 - July 19 2022.

Across the different behaviors, there was little variation in opportunity to take action. Findings reflected the overall opportunity barriers *(Figure 66)*.

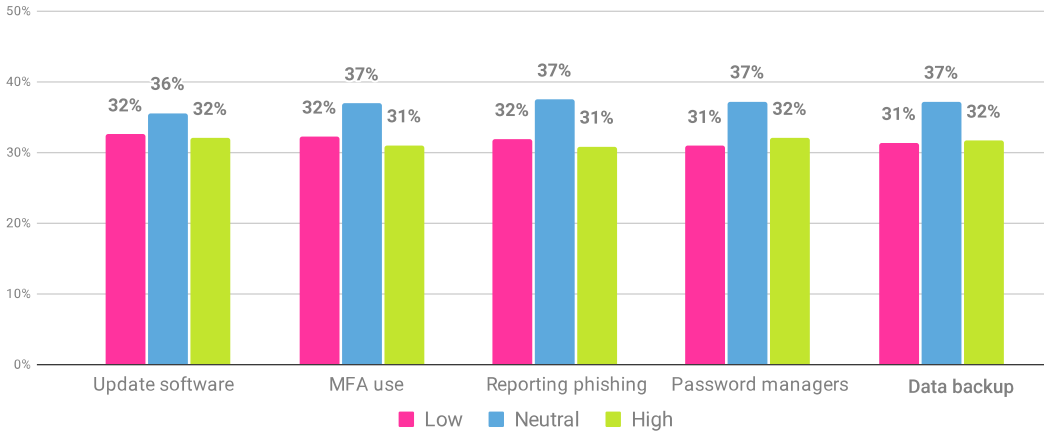


Figure 66. Opportunity barriers by each security behavior.

Base: US, UK, & Canada based participants (aged 18+), total number of participants per security barrier reported: software update 297, MFA use 446, reporting phishing 608, password manager use 2585 and backing up data 609. Dates conducted: June 29 2022 - July 19 2022.

Thirty-two percent reported low motivation for MFA use with just over a quarter motivated to use MFA (28%; *Figure 67*). Participants felt the most motivated to update their devices (43% high vs 25% low) and use a password manager (42% high vs 22% low). This suggests people want to apply good password management strategies.

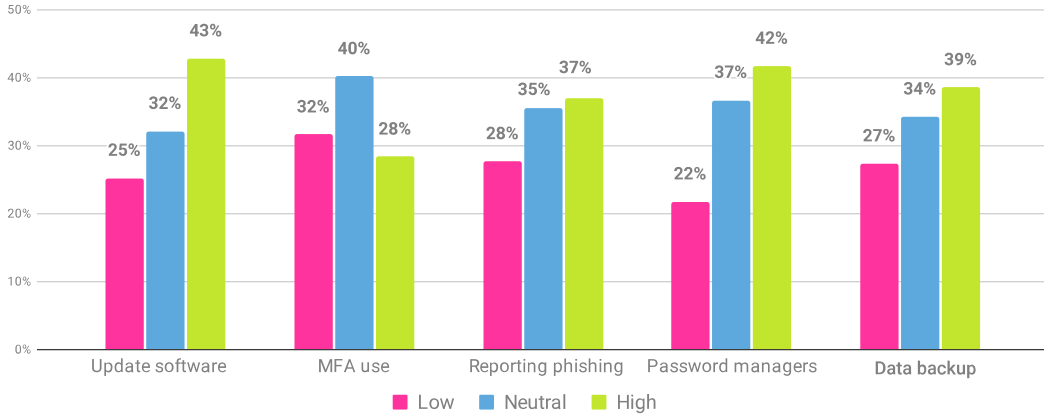


Figure 67. Motivation barriers by security behavior.

Base: US, UK, & Canada based participants (aged 18+), total number of participants per security barrier reported: software update 297, MFA use 446, reporting phishing 608, password manager use 2585 and backing up data 609. Dates conducted: June 29 2022 - July 19 2022.

"We have clear evidence that understanding attitudes and behaviors around cybersecurity is fundamental to building a better support system for people, through tools, programs, and one-to-one relationships."

Andra Zaharia, Content Marketing for cybersecurity companies & specialist

“We are salespeople and selling secure behaviors. Build your brand, understand your audience and most of all, make it fun. Get your investors on board with your mission and be both brave and bold! No one remembers boring!”

Anthony Davis, Information Security Awareness Manager, Ocado Group

Conclusion

The aim of the 2022 Oh, Behave! report was to provide a comprehensive international snapshot of people's cybersecurity attitudes and behaviors. We looked at five security behaviors: password hygiene (password creation, management, and frequency of change); using MFA; installing the latest updates; staying safe from phishing scams (recognizing and reporting messages); and backing up data. We also examined access to cybersecurity training, cybercrime victimization, and barriers to the above security behaviors.

Awareness ≠ secure behavior

The results highlighted people's awareness of the importance of cybersecurity, but also showed their tendency to overestimate their knowledge and ability to keep themselves safe online.

Participants believed they were keeping safe online, and consistently behaving in a secure way (e.g. checking emails for signs of phishing). However, the findings showed that crime rates remained high. Over a third of the participants reported being a victim of at least one of the four cybercrimes this report examined.

We don't need no education!

Gen Zs and Millennials were found to be particularly at risk. Although around half of them have access to training, they reported the highest victimization rates across generations, while simultaneously rating cybersecurity to be less of a priority than other activities. This suggests more support—not more training—is needed to help younger generations stay safe online.

Improving access and impact of training

Older generations – not actively employed – had the least access to training. Their reasons for not having access were financial restraints and other responsibilities making it inaccesible. This highlights the need for targeted support to at-risk groups who cannot access training.

When training is accessed, it is not influencing online security behaviors as much as some might expect. This is reflected in the rates of victimization, which remain high. When accessed, training is typically a once-a-year activity, and, as some note, only when there has been a security incident at work.

There has been a recent shift in opinion on best training practices. More organizations are accepting that training should be continuous, supportive, and transparent—moving away from the punishment-based approach that has traditionally been used (read: inflicted).

Security behaviors

Rates of cybercrime remain high, and the data suggest people not acting securely enough is a high contributing factor. People continue to own a high number of accounts containing personal information, whilst not practicing good password hygiene. Only a few participants used three random words to create their passwords, and/or used a password manager. A small proportion reported using passwords that are at least 12 characters long.

Reassuringly, rates of backing up data and saving passwords in a browser are higher, potentially because these behaviors are easier to perform. Research has shown people are motivated by convenience when creating strong passwords and using password managers[1].

Often, those security behaviors ensuring the highest protection (e.g. using MFA) are viewed as time-consuming with a high level of burden[2]. This was an underlying theme in our research reflected in our participants' reasons for not taking protective action.

MFA significantly boosts account security, even those with weak passwords. That said, only half of participants were familiar with MFA. Similar to perceptions on password management strategies, MFA was viewed as important—but its adoption remains low due to perceptions of ease of use and convenience. Perhaps if MFA was perceived as requiring less time and effort, people would be more motivated to adopt it.

A disparity also exists in people's *beliefs* in their ability to identify phishing emails, and their *actual ability* to identify phishing emails. Phishing remains the most prevalent type of cybercrime.

Learned helplessness

Over half of the participants thought losing money over the internet is avoidable. However, they did not feel the same when it came to personal information, suggesting that people feel somewhat powerless in preventing loss of data.

According to the theory of 'learned helplessness', when people are unable to control or change a situation,they do not try, even when opportunities for change are available. The findings reflect this. Participants did not see any point in protecting themselves online as their information was already readily available. These belief structures must be changed before good behaviors can be adopted.

Reporting remains low

The reported incidents of identity theft, money and data loss amongst participants were low. This is consistent with previous research conducted in the US that found that participants do not trust the government to protect their personal information. This data show, generally, people don't feel responsible for protecting their employers' workplace information, suggesting an embedded employee culture that doesn't embrace individual agency to do so.

Well, there you have it—insight on cybersecurity attitudes and behaviors. We hope our second Annual Cybersecurity Attitudes and Behaviors Report 2022 got you thinking, sharing, and (hopefully) laughing.

Got something to say? Well, we want to hear it! So, don't hesitate to get in touch.

Until next year, friends.

Done.

---

1 Tam, L., Glassman, M., & Vandenwauver, M. (2008). The psychology of password management: A tradeoff between security and convenience: Behaviour & Information Technology: Vol 29, No 3. Behaviour & Information Technology, 233–244.

2 Aurigemma, S., Mattson, T., & Leonard, L. (2017). So much promise, so little use: What is stopping home end-users from using password manager applications? HICSS, 10.

“Remember, if you get an email you weren’t expecting, and you don’t recognise the sender... Stop! Drop! And roll!”

Ian Murphy, Founder of CyberOff

Appendix

Methodology

Survey design

This survey was designed to investigate five cybersecurity behaviors (listed earlier) that have been deemed important by the participating countries' cybersecurity representative bodies.

The survey was entirely based on multiple- or single-choice questions measured with either a 5-point Likert scale (e.g. statements from 'strongly disagree' to 'strongly agree') or a 10-point Likert scales with two anchor points (e.g. 'not at all confident' and 'very confident').

Some survey items were designed with simple descriptive choices (e.g. 'yes, I have and I have used it', 'yes, I have, but I do not use it' and 'no'). In Canada, the survey participants were also provided the option 'prefer not to say' when asked about their gender.

Procedure

Prior to data collection, we pilot tested the survey with the general public. This was to make sure the questions and response options were understandable and the online survey format was easy to navigate and record responses. Altogether, five one-hour long interviews were held with participants representing different age groups. We recruited these study participants via the Prolific[1] platform. Minor amendments to question clarity and logic were made before releasing the survey to wider audiences.

A call for participation was placed on the Toluna[2] platform for the US and the UK participant samples. For Canada, the call for participation was carried out by Elemental Data Collection[3] in Ottawa, Ontario using computer assisted web interviewing (CAWI) technology. Their survey was conducted in the respondent's official language of choice (i.e. English or French).

Participants signed up through the survey platforms to take part in the study and were compensated for their time. They were not requested to provide any personal information when completing the survey. The participant briefing and informed consent form emphasized participation was voluntary, they could withdraw at any time, and their responses would remain anonymous. The research team at CybSafe did not collect any personally identifiable information.

The US and the UK participant sample was collected between June 29th and July 8th 2022, in Canada the sample was collected between July 15th and July 19th 2022.

The survey was designed to be completed in under 30 minutes. The average time participants spent completing the survey was 20 minutes for the US and the UK participants and 13 minutes for participants from Canada.

1 https://www.prolific.co
2 https://uk.toluna.com
3 https://elementaldci.com

Sample

A representative sample (based on age and gender) was sought from the US and the UK populations by Toluna. In Canada, the survey provider weighted their sample by region, gender, and age according to the most recent 'Statistics Canada' census of the population. Quotas were set to make sure the study would target participants proportionate to the stratified regions in Canada: Atlantic Provinces (7.5%), Quebec (23%), Ontario (38%), Prairies (7.5%), Alberta (10.5%), and British Columbia (13.5%).

Here, we acknowledge when stratifying surveys of the general public to this level in detail age can become a source of sample bias in surveys. Particularly, the sample from Canada had older age groups overrepresented.

There was a higher proportion of Baby Boomers in Canada (45%), compared to other countries (25% in the US, and 27% in the UK), which resulted in a higher proportion of retired participants from Canada (37%). However, there were similar proportions of those in full-time employment (47% in the US, 51% in the UK and 40% in Canada). Table 2 and Table 3 describe the survey sample demographics with an equal split of the US, the UK, and participants from Canada from various backgrounds. In total, 182 French-speaking participants from Canada were included in the sample.

Demographic		US (N=1000) % within country	UK (N=1000) % within country	Canada (N=1000) % within country	Total (N=3000) % within demographic
Gender	Female (%)	514 (51.4%)	508 (50.8%)	503 (50.3%)	1525 (50.8%)
	Male (%)	486 (48.6%)	492 (49.2%)	488 (48.8%)	1466 (48.9%)
	Prefer not to say (%)	0 (0%)	0 (0%)	9 (0.9%)	9 (0.3%)
Age	Gen Z (18-25)	138 (13.8%)	127 (12.7)%	20 (2.0%)	285 (9.5%)
	Millennials (26-41)	300 (30.0%)	311 (31.1%)	199 (19.9%)	810 (27.0%)
	Gen X (42-57)	271 (27.1%)	266 (26.6%)	261 (26.1%)	798 (26.6%)
	Baby Boomers (58-76)	253 (25.3%)	265 (26.5%)	446 (44.6%)	964 (32.1%)
	Silent Gen (77+)	38 (3.8%)	31 (3.1%)	53 (5.3%)	122 (4.1%)
	Prefer not to say	0 (0%)	0 (0%)	21 (2.1%)	21 (0.7%)
Employment Status	Employed (%) *Full-time* *Part-time*	586 (58.6%) *468 (46.8%)* *118 (11.8%)*	643 (64.3%) *510 (51.0%)* *133 (13.3%)*	500 (50%) *403 (40.3%)* *97 (9.7%)*	1729 (57.6%) *1381 (46.0%)* *348 (11.6%)*
	Students (%) *Not working* *Working student*	37 (3.7%) *27 (2.7%)* *10 (1.0%)*	44 (4.4%) *25 (2.5%)* *19 (1.9%)*	11 (1.1%) *7 (0.7%)* *4 (0.4%)*	92 (3.1%) *59 (2.0%)* *33 (1.1%)*
	Retired (%)	189 (18.9%)	184 (18.4%)	370 (37.0%)	743 (24.8%)
	Unemployed (%)	87 (8.7%)	41 (4.1%)	47 (4.7%)	175 (5.8%)
	Not working due to disability (%)	45 (4.5%)	42 (4.2%)	32 (3.2%)	119 (4.0%)
	Homemakers (%)	56 (5.6%)	46 (4.6%)	40 (4.0%)	142 (4.7%)

Table 2. Participant demographics by country.

Education Level	US (N=1000) % within country	UK (N=1000) % within country	Canada (N=1000) % within country	Total (N=3000) % within within education level
Some school/high school credit, no diploma or qualification	63 (6.3%)	56 (5.6%)	50 (5.0%)	169 (5.6%)
Primary/secondary education (e.g. GCSEs/A-levels/High School Diploma/GED)	297 (29.7%)	282 (28.2%)	218 (21.8%)	797 (26.6%)
Trade, technical or vocational training (e.g. BTEC/HND/NVQ Diploma/CTE qualification)	113 (11.3%)	175 (17.5%)	237 (23.7%)	525 (17.5%)
Undergraduate degree (e.g. Associates/Bachelors)	365 (36.5%)	255 (25.5%)	337 (33.7%)	957 (31.9%)
Postgraduate degree (e.g. Masters/PhD)	143 (14.3%)	204 (20.4%)	111 (11.1%)	458 (15.3%)
Professional degree (e.g. MD/ DDS/JD)	19 (1.9%)	28 (2.8%)	31 (3.1%)	78 (2.6%)
Prefer not to say	0 (0%)	0 (0%)	16 (1.6%)	16 (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.

Toluna also excluded participants that completed the survey in under four minutes. As 41 participants completed the survey in under four minutes, an additional check was done to ascertain whether these participants had properly engaged with the survey. A quarter of these responses were checked to confirm their responses were valid (e.g. if they claimed to have a great deal of knowledge regarding MFA, they did not subsequently indicate they had never heard of MFA). The responses were deemed to have an acceptable rate of error and were retained for analysis.

There were no lower time limits for participants from Canada, however the provider removed 'low' response quality participants.

Data analysis

All survey items were reported descriptively with frequencies (N) and proportions (%).

“Don’t just make them aware. Give them a certificate of accomplishment to make them proud to be aware.”

Yves Lepage, Cybersecurity leader, Fednav

Differences in victimization, security attitudes, and behaviors by country

This section examines country-wise differences between the US, the UK, and Canada across access to training, cybercrime victimization, and differences in attitudes and behaviors towards cybersecurity. In particular, we focused on the areas of difference between the three countries. We were keen to examine if cultural differences have influenced values and decision-making capabilities.

Summary

Participants from Canada had less access to training than in the US and UK. The highest cybercrime victim rate was in the US, with phishing being particularly high.

US participants were more likely to report romance scams compared to the other countries. Both the UK and Canada felt cybercrime was more avoidable than in the US.

People in the US were more familiar with MFA, and were more likely to back up their data.

Participants in Canada reported lower password hygiene.

Country difference in access to training

Participants from Canada had the lowest rates of access to training *(Figure 68)*, with 70 percent stating they had no access to training, compared to the US (56%) and the UK (61%).

Furthermore, the proportion of participants from Canada who had access to training and had completed it was lower (23%), in comparison to the US and the UK, where around a third had undertaken the training, respectively.

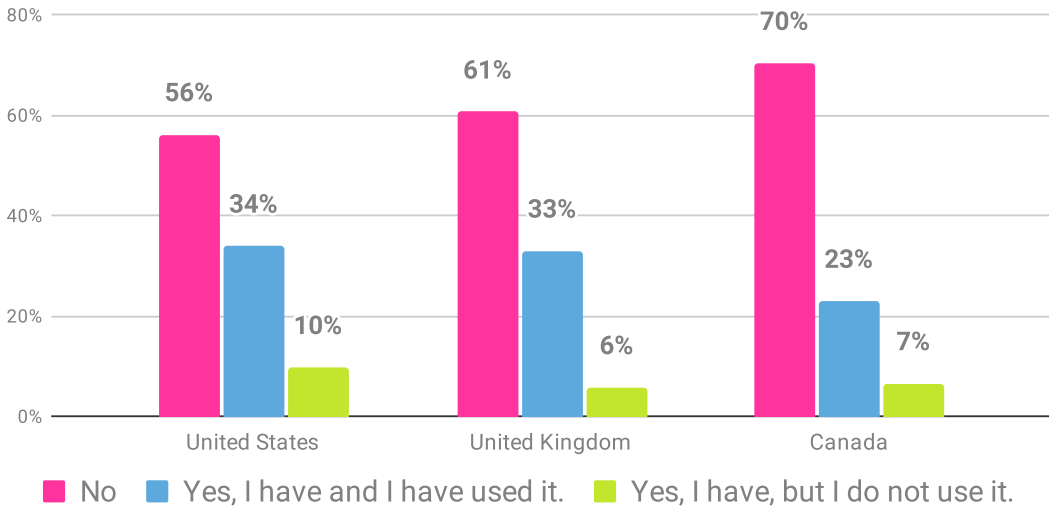


Figure 68. "Do you have access to cybersecurity advice or training?" by country.

Base: US, UK, & Canada based participants (aged 18+), total number of participants: 3000, dates conducted: June 29 2022 - July 19 2022.

Participants in the US reported having to complete mandatory training more frequently (38%) than participants in other countries (see *Figure 69*).

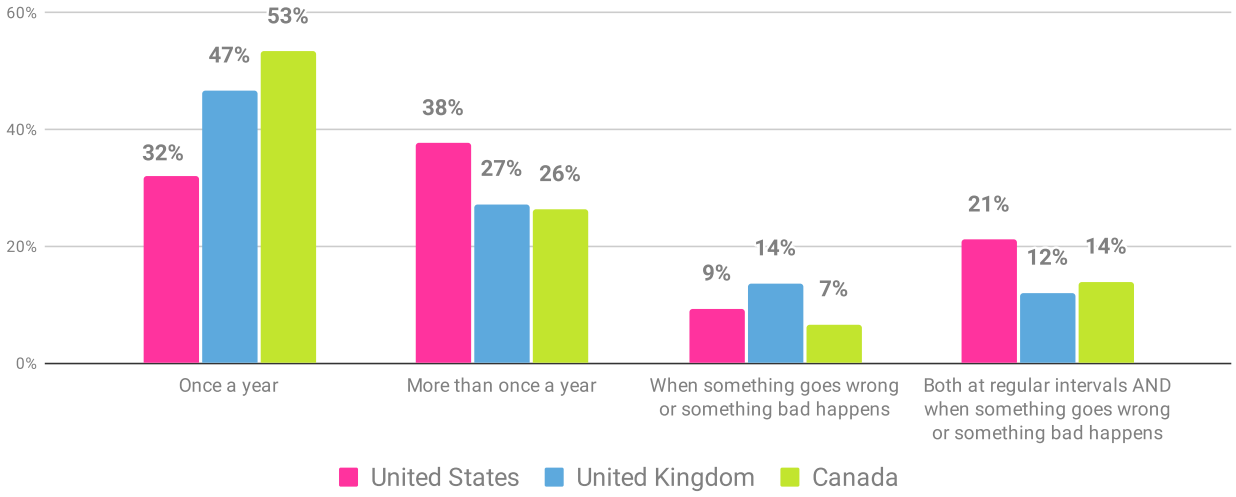


Figure 69. "How often are you required to complete training?" by participants in employment or studying and by country.

Base: US, UK, & Canada based participants (aged 18+), total number of participants: 522, dates conducted: June 29 2022 - July 19 2022.

There were no significant country differences in ratings of cybersecurity training usefulness suggesting, globally, perceptions of the usefulness of training were consistent (ratings between 78% and 83%).

Country differences in victimization

We examined the differences of cybercrime victimization between the countries. We calculated the incident rates by country for cybercrime targeting money or data loss (this excludes cyberbullying).

Participants in the US (49%) were more likely to be a victim of crimes that involved phishing, romance scam, or identity theft, compared to the UK (29%) and Canada (25%; *Figure 70*).

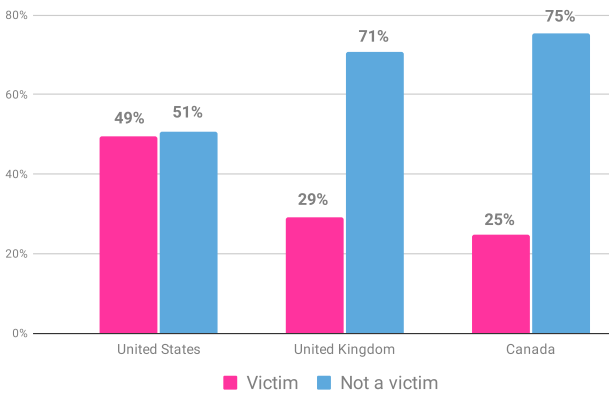


Figure 70. Crime victimization by country.

Base: US, UK, & Canada based participants (aged 18+), total number of participants: 3000, dates conducted: June 29 2022 - July 19 2022.

When breaking down the data further into types of cybercrime *(Figure 71)*, the US experienced over double the number of incidents for all crime types, compared to Canadian participants. Overall, US participants reported the highest rates of phishing victimization (296 incidents), compared to incidents in the UK (175) and in Canada (139).

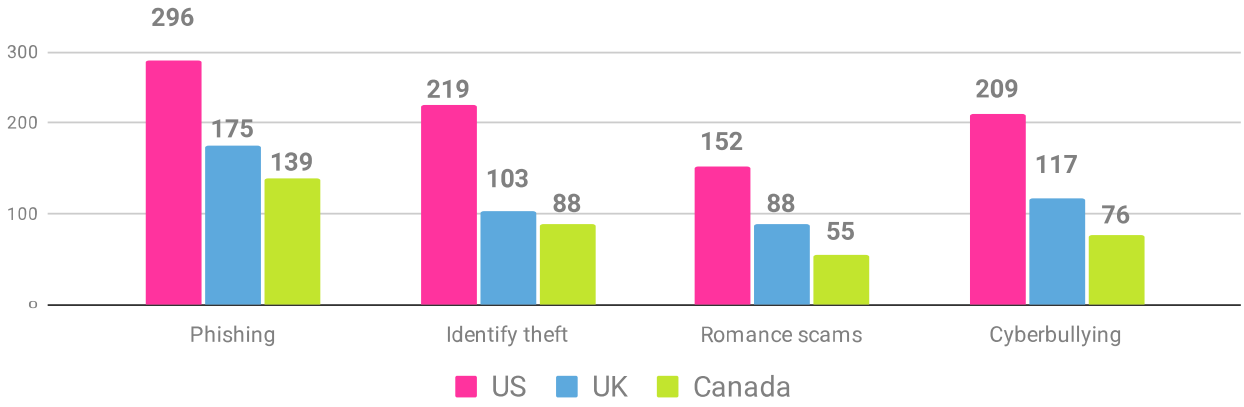


Figure 71. Number of incidents per crime victimization type by country.

Base: US, UK, & Canada based participants (aged 18+), total number of crime incidents: 1717, dates conducted: June 29 2022 - July 19 2022.

Attitudes towards victimization

We found no notable differences in attitudes towards the likelihood of being a target of crime between the countries. However, some differences existed when looking at whether participants found having their personal details stolen over the Internet as something that is perceived as avoidable *(Figure 72)*. Here, 33 percent of participants in the US mentioned the crime being avoidable, in comparison to 39 percent in Canada and the UK. Many US participants reported having personal details stolen as unavoidable (39%).

A higher proportion of participants from Canada felt themselves at a high risk of being a victim of money loss (58%), compared to 51% in the US and UK *(Figure 73)*.

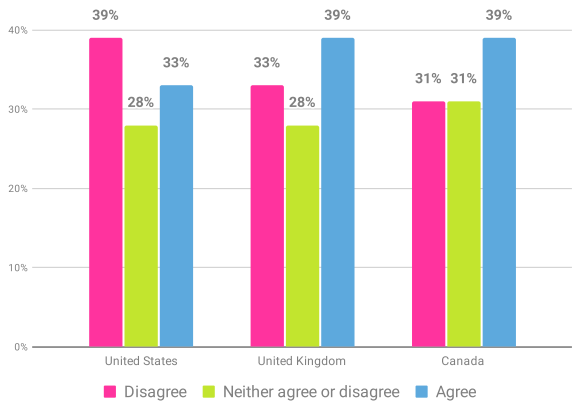


Figure 72. 'Having personal details stolen over the internet is avoidable these days' by country.

Base: US, UK, & Canada based participants (aged 18+), total number of participants: 3000, dates conducted: June 29 2022 - July 19 2022.

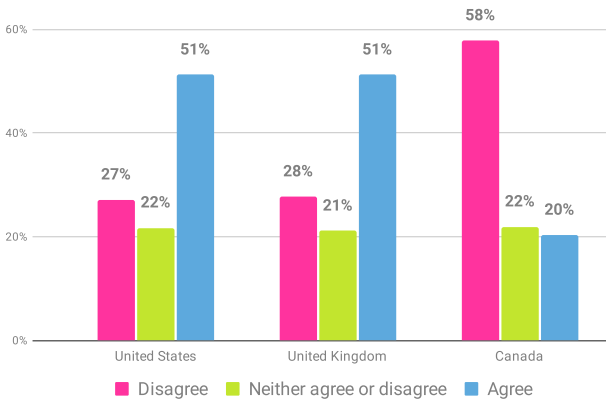


Figure 73. 'Losing money over the Internet is avoidable these days' by country.

Base: US, UK, & Canada based participants (aged 18+), total number of participants: 3000, dates conducted: June 29 2022 - July 19 2022.

Cybersecurity behaviors

Multi-factor authentication

Familiarity with MFA was slightly higher in the US sample (63%), in comparison to the UK (52%), and Canada (57%; *Figure 74*).

Those who were familiar with MFA did not differ in their application of MFA to at least one of their online accounts containing personal information *(Figure 75)*.

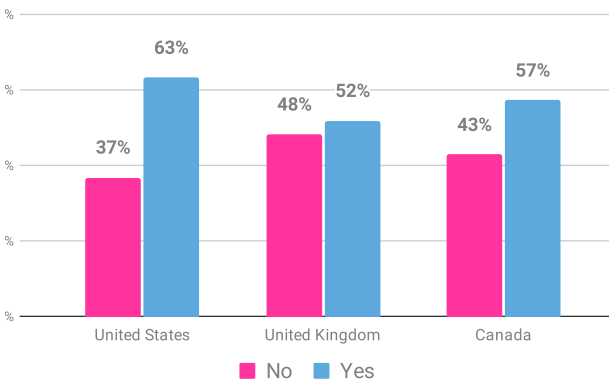


Figure 74.
"Have you ever heard of MFA?" by country.

Base: US, UK, & Canada based participants (aged 18+), total number of participants: 3000, dates conducted: June 29 2022 - July 19 2022.

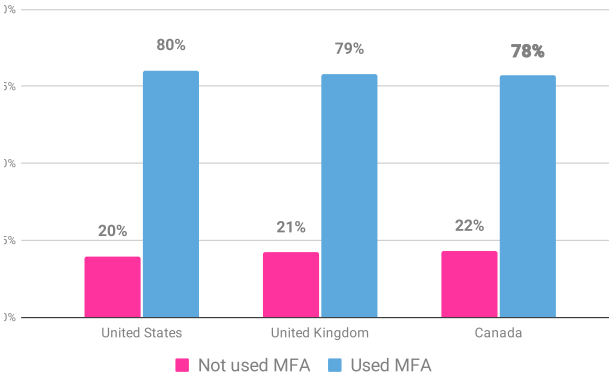


Figure 75.
Usage of MFA by country.

Base: US, UK, & Canada based participants (aged 18+), total number of participants: 1722, dates conducted: June 29 2022 - July 19 2022.

Installing software updates

Installing software updates was relatively consistent across countries *(Figure 76)*. Forty-one percent of the UK participants admitted they 'never', 'rarely' or 'sometimes' installed software updates, in comparison to the US 38%, and Canada 34%.

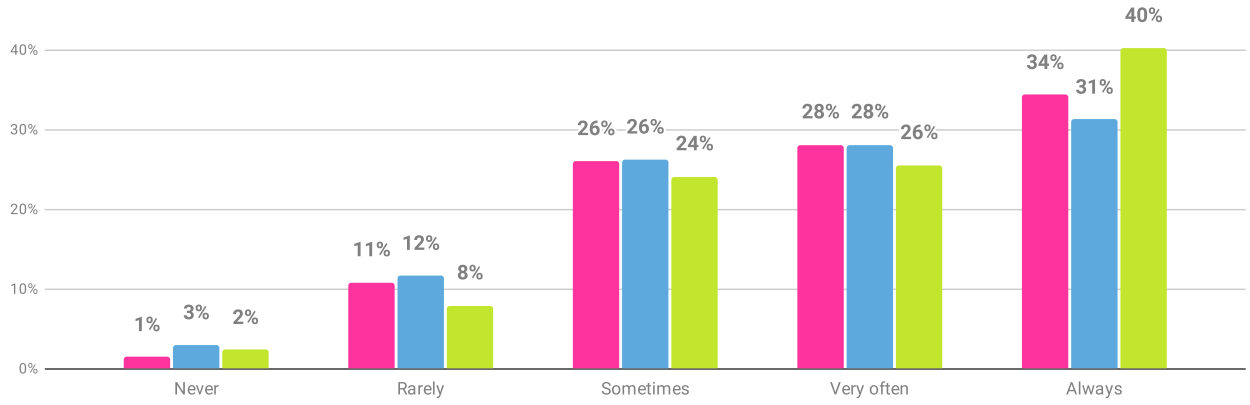


Figure 76. "How often do you install the latest updates and software when notified that they are available?" by country.

Base: US, UK, & Canada based participants (aged 18+), total number of participants: 3000, dates conducted: June 29 2022 - July 19 2022.

Recognizing phishing messages

Checking messages for their legitimacy was relatively consistent across countries *(Figure 77)* with a slightly higher percentage of the UK participants (31%) admitting they 'never', 'rarely' or 'sometimes' check for signs of phishing.

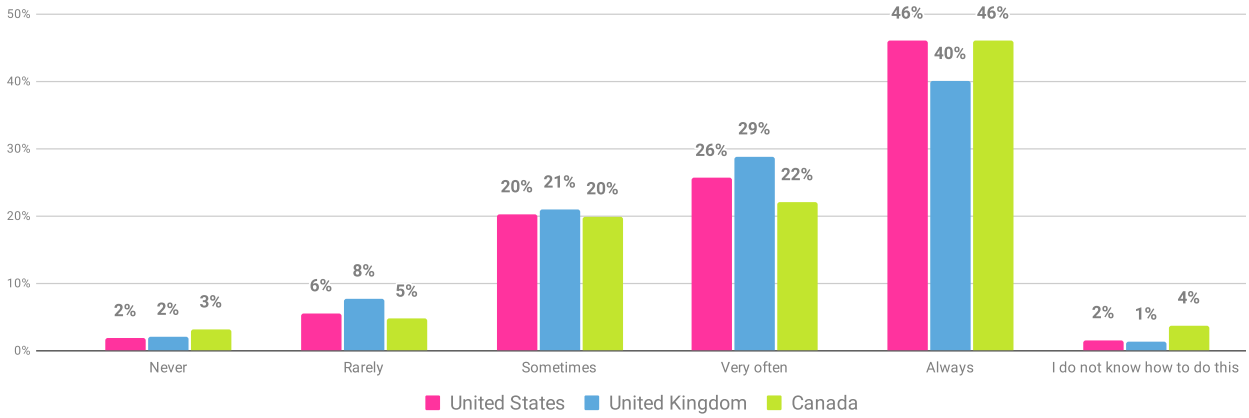


Figure 77. "How often do you check a message is genuine before clicking any links or responding to it?" by country.

Base: US, UK, & Canada based participants (aged 18+), total number of participants: 3000, dates conducted: June 29 2022 - July 19 2022.

Reporting phishing

Phishing reporting was consistent across countries. Half of the US participants (50%) reported phishing either 'very often' or 'always' closely followed by participants from the UK and Canada (both 45%; *Figure 78*).

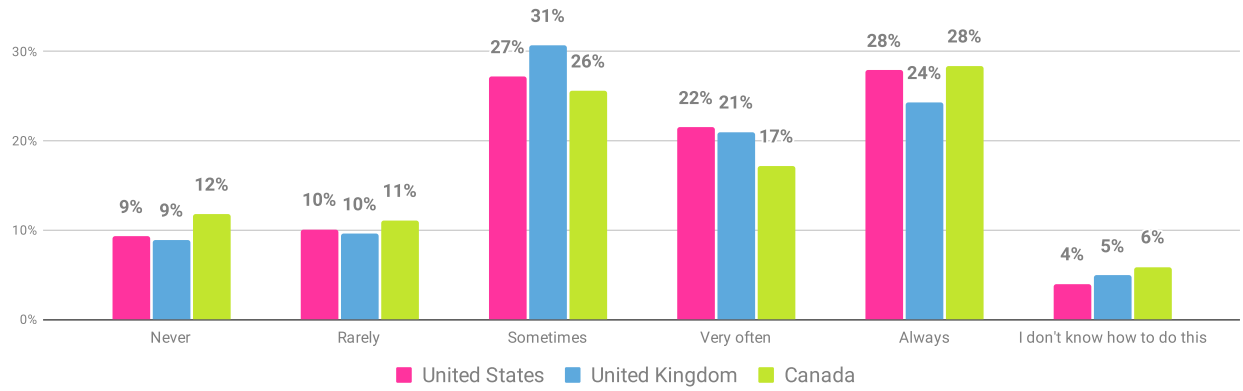


Figure 78. "If someone you know sends you an unusual message with links, how often do you reach out to the person to ask about it before clicking the link?" by country.

Base: US, UK, & Canada based participants (aged 18+), total number of participants: 3000, dates conducted: June 29 2022 - July 19 2022.

Using password management strategies

Password management strategies varied slightly by country. Seventy one percent of participants from Canada stated they 'never', 'rarely' or 'sometimes' saved passwords in a browser, compared to 62 percent in the US and 64 percent in the UK *(Figure 79)*.

At the same time, 89 percent of participants from Canada had never downloaded a standalone password manager, compared to participants from the US (75%) and the UK (83%; *Figure 80*).

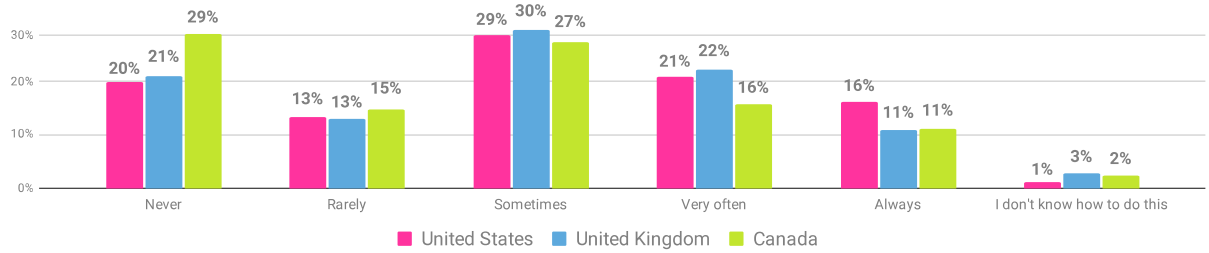


Figure 79. "How often do you save your passwords in the browser when prompted?" by country.

Base: US, UK, & Canada based participants (aged 18+), total number of participants: 3000, dates conducted: June 29 2022 - July 19 2022.

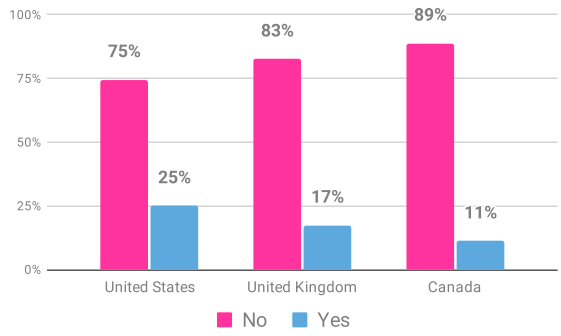


Figure 80. "Have you ever downloaded a stand-alone password manager application?" by country.

Base: US, UK, & Canada based participants (aged 18+), total number of participants: 3000, dates conducted: June 29 2022 - July 19 2022.

Backing up data

Forty-nine percent of participants in the US backed up their data 'very often' or 'always', compared to those in the UK (42%) and in Canada (40%; *Figure 81*).

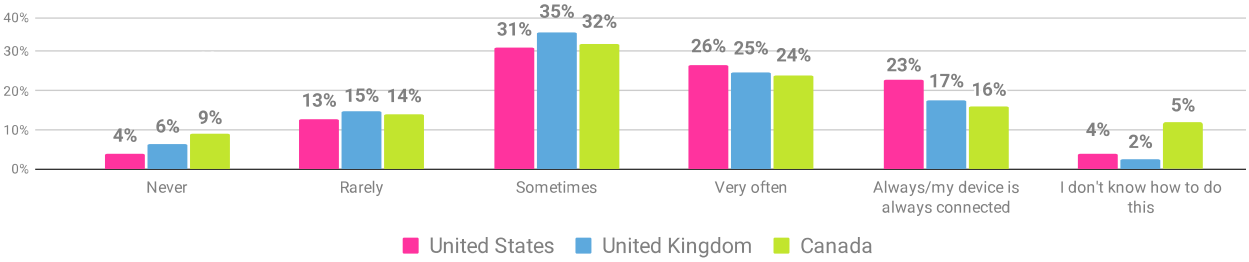


Figure 81. "How often do you back up your most important data?" by country.

Base: US, UK, & Canada based participants (aged 18+), total number of participants: 3000, dates conducted: June 29 2022 - July 19 2022.

NATIONAL CYBERSECURITY ALLIANCE

A leading non-profit organization, the National Cybersecurity Alliance (NCA) is dedicated to creating a more secure, interconnected world. Advocating for the safe use of all technology, The NCA aims to educate everyone on how best to protect themselves, their families, and their organizations from cybercrime. The organization also creates strong partnerships between governments and corporations to foster a greater "digital" good, and amplify the message that only together can we realize a more secure, interconnected world.

CYBSAFE

CybSafe is a cyber security and data analytics software company focused on behavioral security, working to make it easy to manage human cyber risk. With a team made up of psychologists, behavioral scientists and security experts, CybSafe delivers a range of leading security research initiatives aimed at better understanding human decision-making and security behavior.

CybSafe is designed for the modern, hybrid workforce, and is on a mission to revolutionize the way society addresses the human aspect of cyber security. At the heart of CybSafe's behavioral security platform is SebDB—the world's most comprehensive security behavior database—offering insight into every security behavior capable of minimizing human cyber risk.

Authors

Dr. Jason R.C. Nurse, Director of Science & Research, CybSafe
Dr. Inka Karppinen, CPsychol, Lead Behavioral Scientist, CybSafe
Dr. Jo Milward, Senior Behavioral Scientist, 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
Kimberly Duthie, External Communications Officer, Get Cyber Safe

Acknowledgements

Leah DeLancey, Programs & Events Manager, The National Cybersecurity Alliance
Cassie Lowery, Research Assistant, CybSafe
Cliff Maroney, Vice President, Crenshaw Communications
Panashe Marufu, Copywriter, CybSafe
Marina Soto, Visual Designer, CybSafe
Dr. Suzie Dobrontei, CPsychol, Product Content Lead, CybSafe
Joe Giddens, Director of Content & Communication, CybSafe