

**Oh,
Behave!**

The Annual Cybersecurity
Attitudes and Behaviors
Report 2021

TABLE OF CONTENTS

01

Oh, Behave! 3

02

Report aim and structure 4
Key terms 4

03

Key findings 6

04

Our findings 10
How we connect 12
The victims of cybercrime and identity theft 13
Reporting cybercrime and identity theft 14

05

Perceptions of cybersecurity practices 15
Attitudes to cybersecurity 16
Whose responsibility is cybersecurity? 18
Reliance on others for cybersecurity behaviours 20
Awareness, engagement, and attitudes towards core security behaviors 21
Password behaviors 21
Using password management strategies 22
Using Multi-Factor Authentication (MFA) 23
Installing software and applications 24
Confirming the legitimacy of an email 25
Recognizing and reporting phishing emails 25
Backing up data 26

06

Barriers to cybersecurity behaviors 27
Password management applications 29
Use of Multi-factor authentication (MFA) 30
Installing the software and applications 31
Reporting phishing messages 32
Backing up data 33

07

Advice sources for cybersecurity behaviors 34

08

The future and the Internet of Things 36
Cybersecurity knowledge 37
IoT devices 38

09

Conclusion 41

10

Appendix 44
Methodology 45
Survey design 45
Procedure 45
Data quality 49
Data analysis 49

11

Differences in victimization, security attitudes, and behaviors by country 50
The US and the UK comparisons 50
About 53
Authors 53

Oh, Behave!

Welcome, dear readers, to the Annual Cybersecurity Behaviors and Attitudes Report 2021! You're probably wondering what the significance of the title of this report is... If you guessed that it's one of Austin Powers' many catchphrases, you're right! But it also nicely ties in to the theme of this report - understanding cybersecurity behaviors.

This inaugural issue published during Cybersecurity Awareness Month 2021 marks the launch of an annual research report series. We aim to better understand and share insights into people's security attitudes and behaviors. This report is the first of its kind and sheds light on one of the most important aspects of cyber risk - the human factor.

People –yes, we pesky human beings– are widely recognized as one of the most critical components of cyber resilience and risk reduction. But, one of the least understood areas is that of security behaviors and attitudes. Specifically, the gap or disconnect between knowledge and action.

We often make assumptions when trying to understand how to reduce the cyber risk associated with people. Sometimes, these assumptions are wrong. Even when they're right, we can miss the real reason behind the truth and therefore draw the wrong conclusions. It's time for this to stop.¹

Current behavior patterns provide us some of the best predictors of future human behavior-related risk. And so, we've decided to build a body of research data that enables anyone to optimize their approach to how they influence security awareness attitudes and behaviors in the future.

Two thousand people from the US and the UK completed a specially designed survey to assess security attitudes and behavior across the general public.

In this first report, we've concentrated on a handful of core cybersecurity behaviors:

1. Creating and managing passwords
2. Applying Multi-Factor Authentication (MFA)
3. Installing the latest updates
4. Checking message legitimacy
5. Recognizing and reporting phishing
6. Backing up data

The work doesn't stop here! Along with the above core behaviors, this research report looks to answer questions on the general public's levels of security awareness and engagement. What motivates the application of security advice leading to good security behaviors? *What are the main barriers to not applying security advice in practice? Why do people willingly hand over personal data to see which "Harry Potter" character they most relate to?*²

Examining the trends in cybersecurity core behaviors helps us personalize and tailor our security awareness efforts. Instead of providing 'one-size-fits-all' advice, we can harness individual differences and trends in security awareness, attitudes, and behaviors. The world would be quite boring if we were all the same, no?

This is another big step in making society a more secure digital place. So settle down, grab yourself a cup of your favourite hot beverage, and take it all in. We're delighted to be on this journey with you!



Oz Alashe MBE,
CEO, CybSafe



Lisa Plaggemier,
Executive Director, The National
Cybersecurity Alliance

1 Reading this report is a great place to start (if we do say so ourselves)

2 We've all been there, Harry Potter is no joke!

Report aim and structure

We aim to provide a snapshot of people’s security awareness, engagement, and attitudes towards good cybersecurity behaviors. This annual research report series will grow to form a body of work that becomes more comprehensive each year. This year, we’ve concentrated on the top few topics to get the ball rolling.

We start with a summary of the key findings, then dive straight into the research results. No extra fuss! We’ve organized the results under the following themes:

1. How are people connected online?
2. Who are the victims of cybercrime?
3. People’s perceptions and attitudes to cybersecurity
4. Awareness, engagement, and attitudes towards seven core security behaviors
5. What are the barriers to good cybersecurity behavior?
6. Where do people get advice that affects their cybersecurity behaviors?
7. The future, and other connected devices (Internet of Things)

Finally, we conclude with information on the way things were done (i.e. methodology), provide more detail on participant demographics, and our approach to data collection and analysis.

We can’t wait to share our findings with you! Before we get stuck in, here’s an explanation of the key terms we’ve used throughout the research report:

Key terms

(Security) Attitude³: A psychological disposition we take 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) Core behaviors: During our research development phase and stakeholder meetings, we selected seven security behaviors that were seen as some of the top priorities according to the official guidance (US: Stay Safe Online⁴ and UK: Cyber Aware⁵). These include: creating strong passwords, using password management strategies, using multi-factor authentication, installing the latest software/applications, checking messages for their legitimacy, reporting phishing emails, and backing up data.

3 This is not the same type of attitude displayed by melodramatic teenagers as they seek more independence - they get sassy!

4 <https://staysafeonline.org/stay-safe-online/online-safety-basics/>

5 <https://www.ncsc.gov.uk/cyberaware/home>

REPORT AIM AND STRUCTURE

Cybersecurity risk: Cybersecurity risk is the probability of exposure, loss of critical assets and sensitive information, or reputational harm as a result of a cyberattack or breach within an organization's network.

Cybercrime: Harmful and illegal cyber activities online (e.g. phishing attempts or data leaks).

Identity theft: When a cybercriminal steals the personal information of an individual usually to commit fraud. This information may be used to apply for credit and loans or even file taxes, potentially damaging credit status.

Internet of things (IoT): A network of internet-connected devices with the ability to collect and transfer data over a wireless network without human intervention (e.g. Smart TV, Alexa and gaming consoles).

Multi-Factor Authentication (MFA): Multi-Factor Authentication is the process of using two or more pieces of information to log in to an account. This can be done through a code sent to one's phone, a fingerprint scan, or similar.

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

– *Why don't you update your devices?*

“I would install the latest updates and software to my devices but...

I have no money to protect. Zero secrets to cover. Basically, I have nothing to lose. Nothing to protect”

Key findings

KEY FINDINGS

One-third of the research survey participants (34%) reported having experienced harmful cyber activity at least once in their lives. Another 19% reported they had been victims of identity theft. However, the number of people who said they reported cybercrime to the authorities was low.

Let’s look at these numbers: 61% of cybercrime victims and 37% of identity theft victims said they didn’t report the incident.

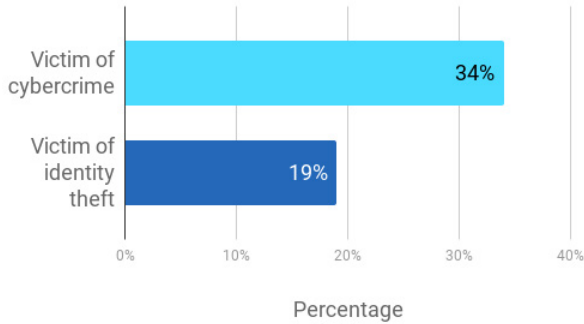


Figure 1. Percentage of cybercrime and identity theft victims.

Base: UK & US based participants, total number: 2000, aged 18+, dates conducted: August 10, 2021 - August 18, 2021.

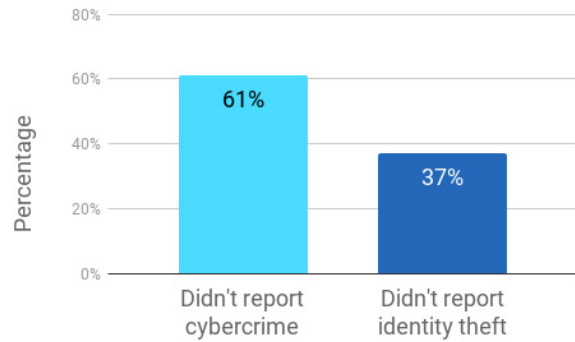


Figure 2. Percentage of victims not reporting cybercrime and identity theft.

Base: UK & US based participants, total number: 676 for cyber crime and 389 for identity theft, aged 18+, dates conducted: August 10, 2021 - August 18, 2021.

We found generational differences in the reporting behaviors of the victims of cybercrime and identity theft. “Baby Boomers” were most likely to report cybercrime (64%) and identity theft (85%) while “Gen Z” were least likely to do so (21% and 35%, respectively).

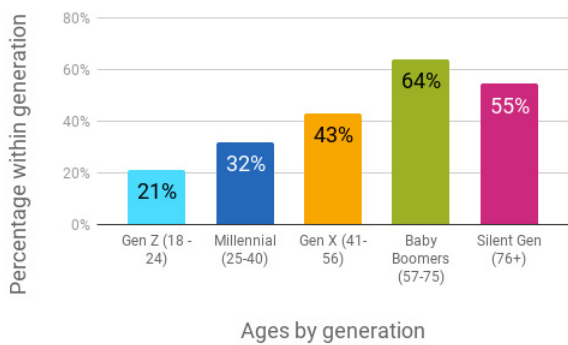


Figure 3. Percentage of participants reporting cybercrime by age group.

Base: UK & US based participants, total number: 676, aged 18+, dates conducted: August 10, 2021 - August 18, 2021.

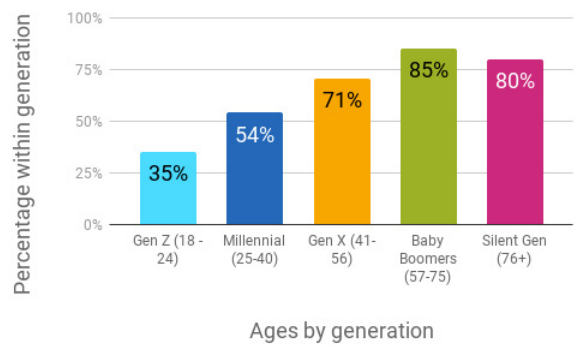


Figure 4. Percentage of participants reporting identity theft by age group.

KEY FINDINGS

Fostering knowledge of cybersecurity is critical. However, in our sample, 48% of the participants didn't know what Multi-Factor Authentication (MFA) was. This was exacerbated further with 64% of the participants reporting that they didn't have access to any kind of cybersecurity advice or training. Of those participants with access to cybersecurity training, most made use of it (73%), demonstrating people's willingness to learn more about ways to protect themselves online when information is available to them.

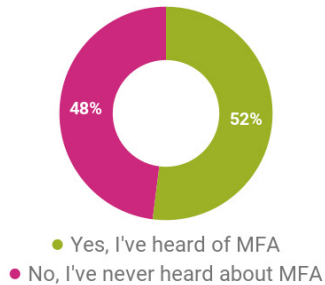


Figure 5: Participants' awareness of MFA.

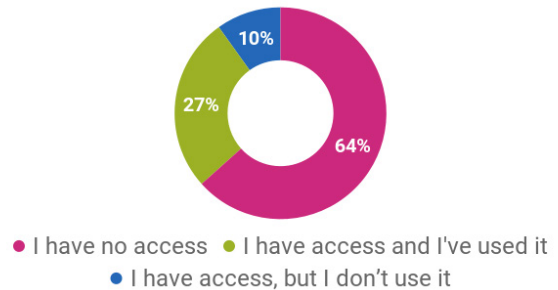


Figure 6. Participants' access to cybersecurity training.

Base: UK & US based participants, total number: 2000, aged 18+, dates conducted: August 10, 2021 - August 18, 2021

Large numbers of participants reported having a hard time adopting cybersecurity best practices, such as using password managers or applying MFA to keep them safe online. There was a diverse range of reasons given for this. These included lack of knowledge and not perceiving cybersecurity practices as a high priority.

Additionally, the data indicates a significant proportion of people simply don't see themselves as responsible for looking after their workplace's sensitive information.

Here, over a third (40%) of the full-time and part-time employees participating considered themselves to be the least responsible agency for their organization's cybersecurity.

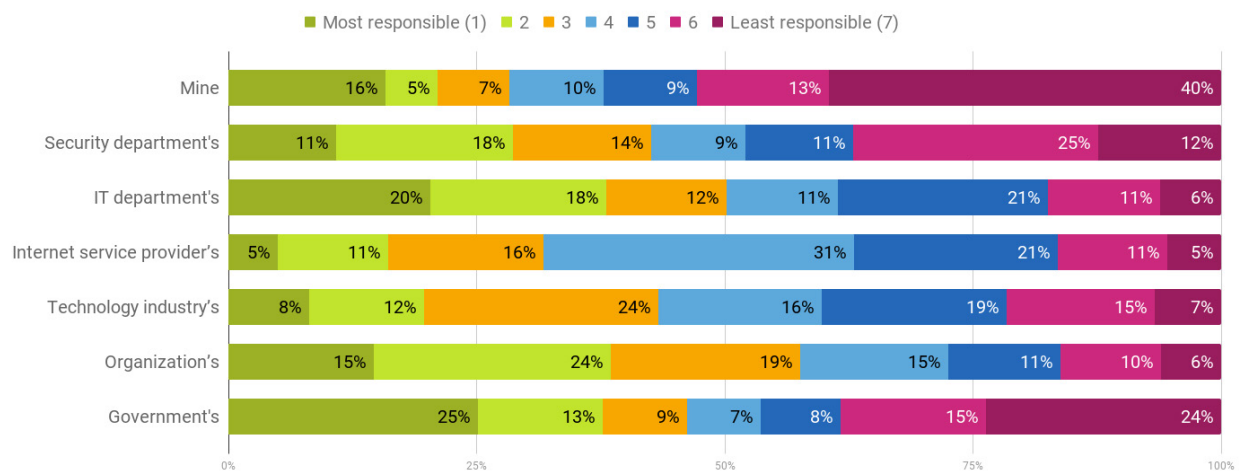


Figure 7. "Whose main responsibility is it to protect your workplace's online information?"

Base: UK & US based participants, total number: 1105, aged 18+, dates conducted: August 10, 2021 - August 18, 2021.

KEY FINDINGS

For the minority of participants who adopted good security behaviors, the top sources of security advice were websites or applications. Overall, these participants actively searched for information online.

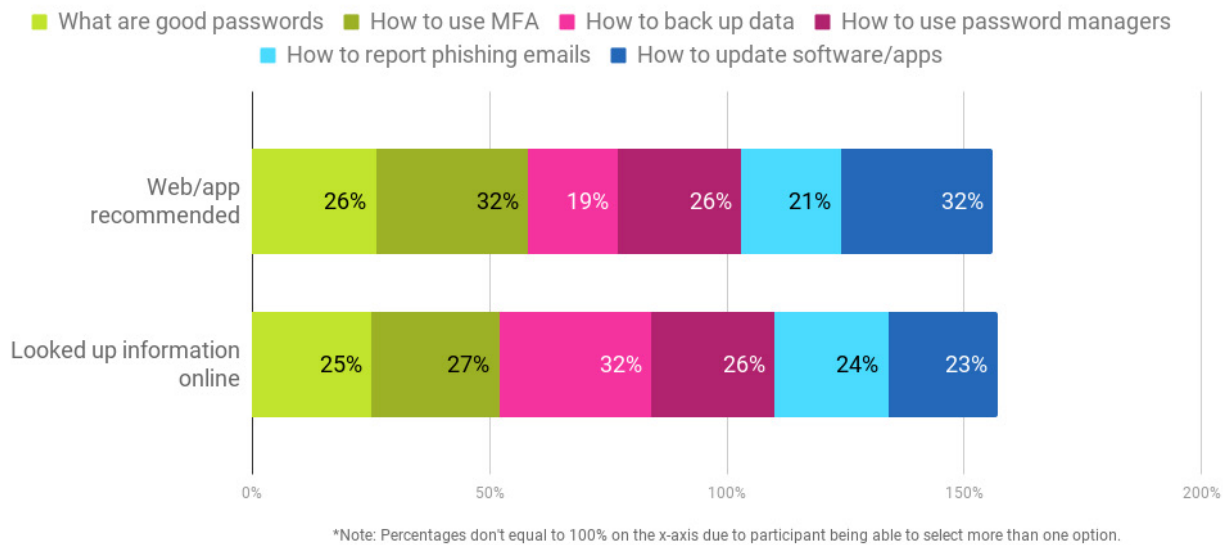


Figure 8. Top sources of advice for seven core security behaviors.

Base: UK & US based participants, total number: 2000, aged 18+, dates conducted: August 10, 2021 - August 18, 2021.

– Why didn't you report phishing?

“Data leaks happen all the time. I’ve had my details stolen from many different companies over the years. Who would I report it to?!”

– Why didn't you report ID fraud?

“It happened at a time when my credit was already bad, so I wrote it off”

Our findings

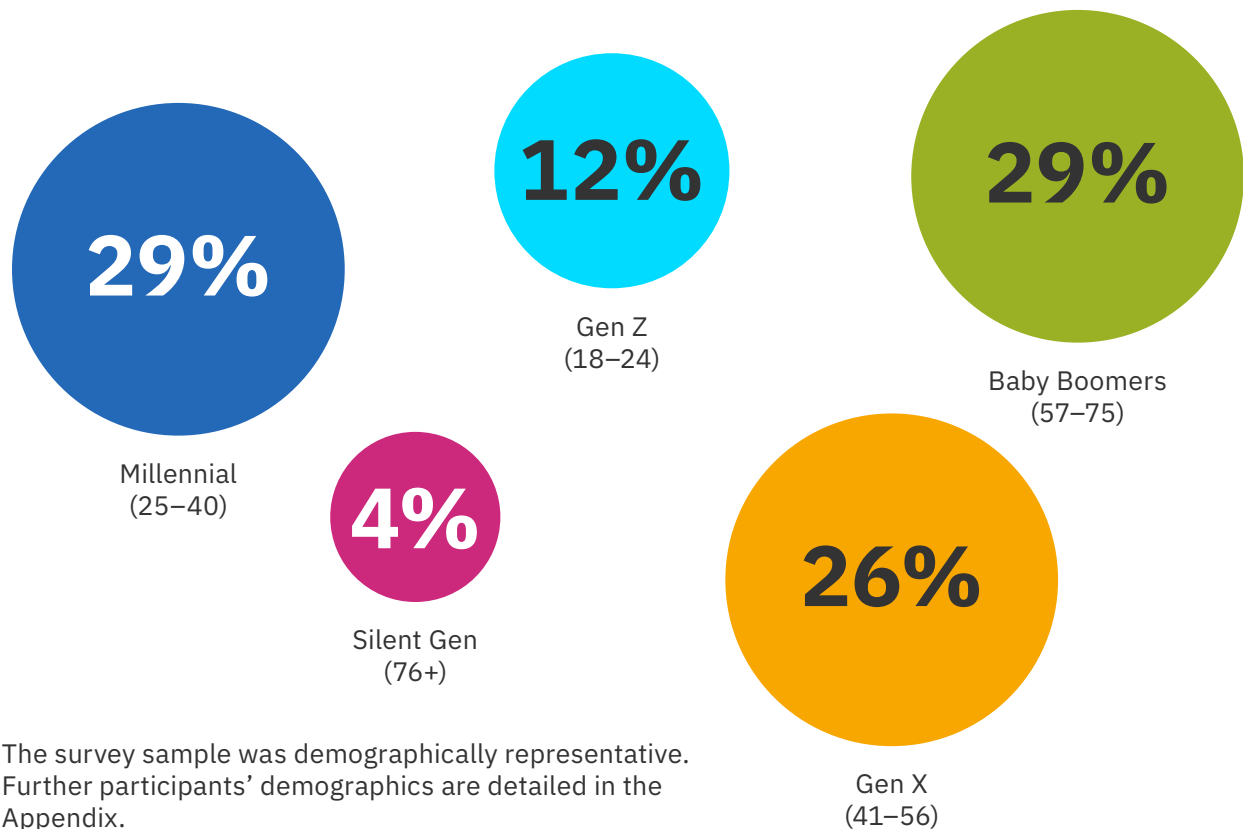
OUR FINDINGS

We conducted the cybersecurity attitudes and behaviors survey online between August 10th and 18th, 2021. The survey was distributed by Toluna⁶. Two thousand participants provided information online in response to questions about their security behaviors.

The survey sample consisted of adults (18 years or older), with the average age being 47 years. We divided the participants into five age groups from “Gen Z” to “Silent Gen”. The number of participants in each group is shown in Table 1.

Age	Number of participants (%)
Gen Z (18–24)	241 (12%)
Millennial (25–40)	572 (29%)
Gen X (41–56)	513 (26%)
Baby Boomers (57–75)	585 (29%)
Silent Gen (76+)	89 (4%)

Table 1. Number of participants per age group.



The survey sample was demographically representative. Further participants’ demographics are detailed in the Appendix.

⁶ <https://uk.toluna.com/>

How we connect

80%
of people aged between 18 and 56 connect to the internet via smartphones

57%
of the “Silent Gen” prefer to use the desktop to access information online

1%
don’t have access to the internet

vs

53%
with their laptops

58%
are always connected to the internet

93%
are online every day

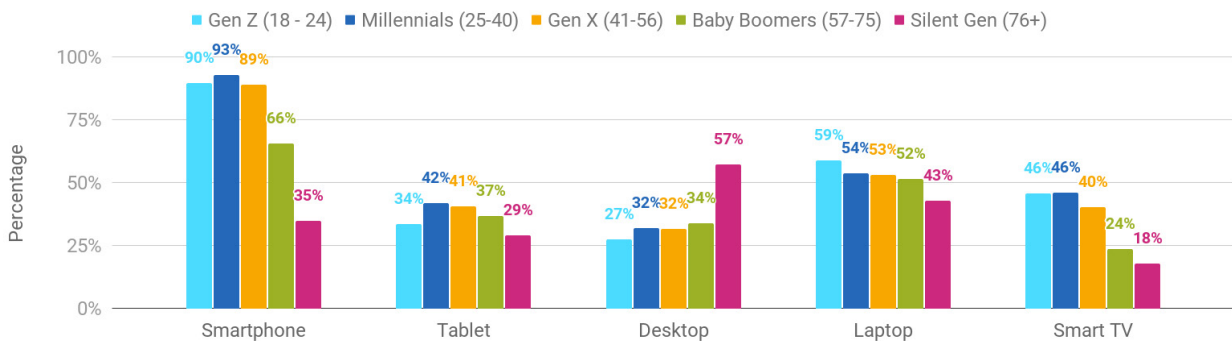


Figure 9. Devices used to access the internet by age groups.

Base: UK & US based participants, total number: 2000, aged 18+, dates conducted: August 10, 2021 - August 18, 2021.

The most popular Internet of Things (IoT) devices were:

59%
smart televisions

41%
gaming consoles

35%
smart speakers

21%
didn’t own any IoT devices

Victims of cybercrime and identity theft

Overall, 34% of the participants had experienced harmful cyber activity at least once in their life. 19% reported having been victims of identity theft.

Younger generations (51% of “Gen Z” and 44% of “Millennials”) were more likely to be victims of harmful cyber activity (e.g. phishing attempts or data leaks) that resulted in the loss of money or data compared to older generations (21% of “Baby Boomers”, and 13% of “Silent Gen”).

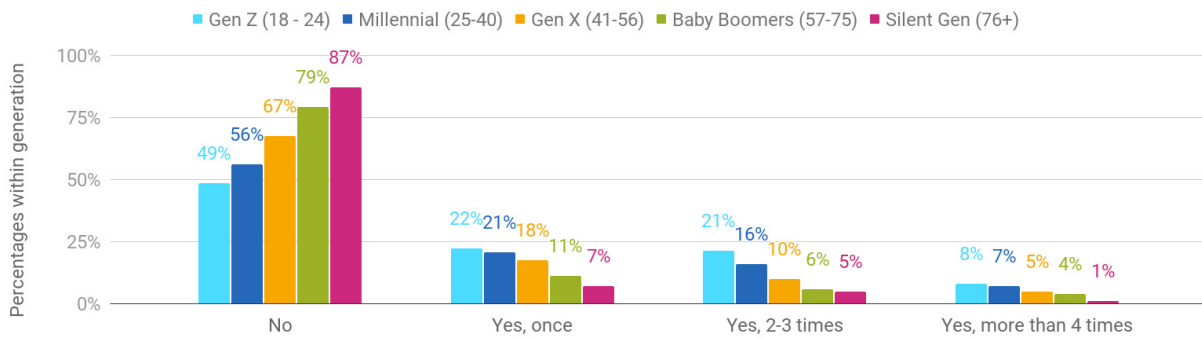


Figure 10. “Have you ever been a victim of harmful cyber activities online that have resulted in the loss of money or data?”

Base: UK & US based participants, total number: 2000, aged 18+, dates conducted: August 10, 2021 - August 18, 2021.

A similar trend of vulnerability was visible in victims of identity theft. Here, 24% of ‘Gen Z’ and 25% of ‘Millennials’ reported having their identity stolen at least once. 86% of ‘Baby Boomers’ reported that they’d never had their identity stolen.

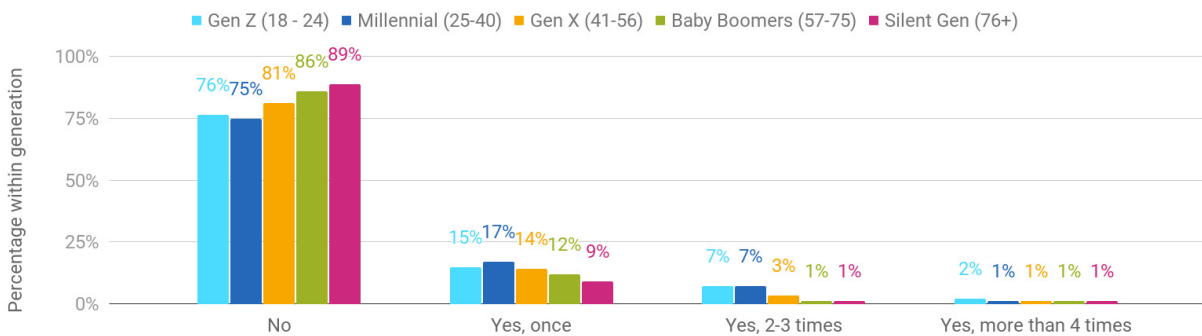


Figure 11. “Have you ever been a victim of identity theft?”

Base: UK & US based participants, total number: 2000, aged 18+, dates conducted: August 10, 2021 - August 18, 2021.

Reporting cybercrime and identity theft

More than half of the cybercrime victims (61%) chose not to report the incident with only 39% reporting it. ‘Baby Boomers’ (64%) were most likely to report cybercrime while ‘Gen Z’ (21%) were least likely to do so. The main reasons given for non-reporting were not knowing how or who to report the crime to. The majority of participants who said they did report the crime did so to the police and the bank.

Overall, 63% of identity theft victims reported the incident, and 37% of participants chose not to report it. “Baby Boomers” were again relatively active in reporting identity theft (85%) when compared to other generations. The group that seemed to report the least was ‘Gen Z’ (35%).

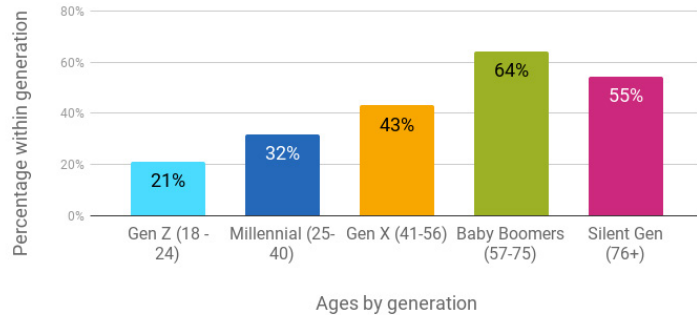


Figure 12. Percentage of participants reporting cybercrime by age group.

Base: UK & US based participants, total number: 676, aged 18+, dates conducted: August 10, 2021 - August 18, 2021.

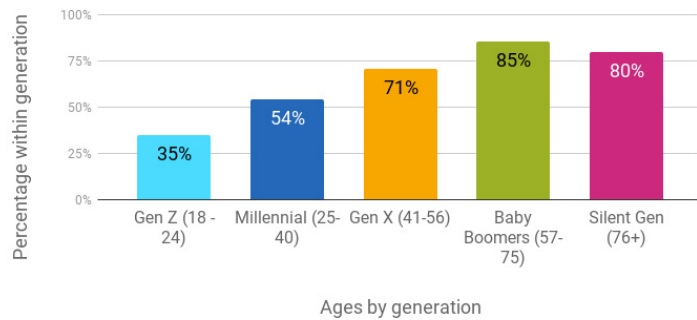


Figure 13. Percentage of participants reporting identity theft by age group.

Base: UK & US based participants, total number: 389, aged 18+, dates conducted: August 10, 2021 - August 18, 2021.

61%
of the cybercrime victims chose not to report the incident”

– Why don't you update your devices?

“I feel my devices are secure and don't think it's necessary to update them often”

**Perceptions
of cybersecurity
practices**

PERCEPTIONS OF CYBERSECURITY PRACTICES

This section provides a snapshot of people’s attitudes and confidence when it comes to cybersecurity practices. We’ve examined their views on perceived responsibility and reliance on other people (e.g. family members) when undertaking actions online (e.g. resetting the Netflix password... again).

Attitudes to cybersecurity

Overall, participants reported staying secure online is important to them (85%), and they prioritize online security (76%).

Less than half of the participants (41%) stated they find staying secure online frustrating and another 41% reported feelings of intimidation concerning cybersecurity matters.

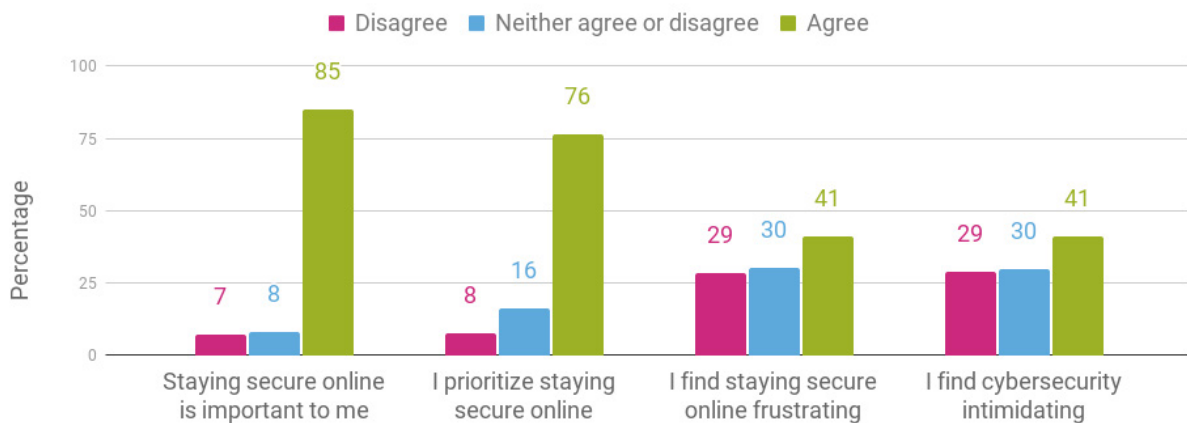


Figure 14. Participants’ levels of agreement to four cybersecurity statements.

Base: UK & US based participants, total number: 2000, aged 18+, dates conducted: August 10, 2021 - August 18, 2021.

41%
of participants
felt intimidated by
cybersecurity matters

PERCEPTIONS OF CYBERSECURITY PRACTICES

Most participants (67%) felt confident about their ability to identify a malicious email from a cybercriminal.

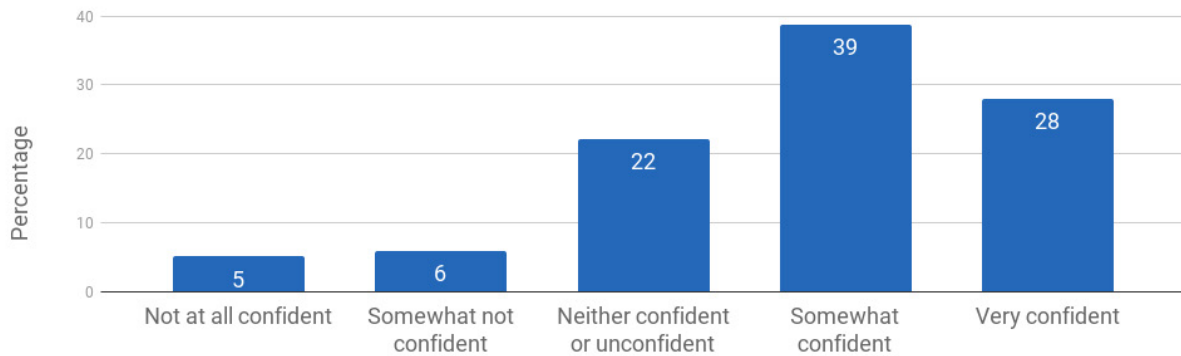


Figure 15. Participant’s confidence in their ability to identify malicious and/or illegitimate emails/links from a cybercriminal.

Base: UK & US based participants, total number: 2000, aged 18+, dates conducted: August 10, 2021 - August 18, 2021.

Over half of the participants (59%) found it easy to be secure online. However, 43% noted the cost of applying online protection was too expensive. A further 39% felt confused about the online security information presented to them. The perceived cost and confusion may also be reflected in the perceived likelihood of becoming a victim of cybercrime. Here, 38% considered themselves to be a likely target of a cybercriminal.

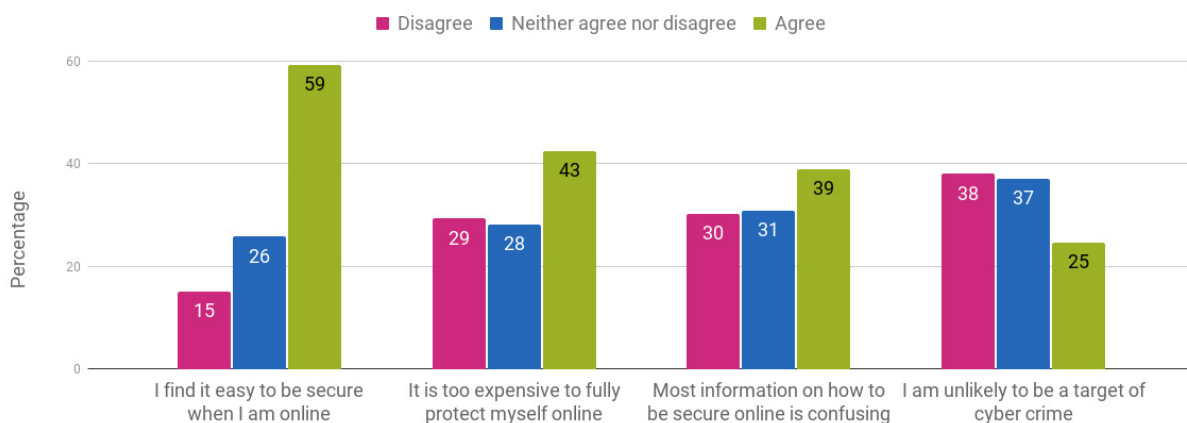


Figure 16. Participants’ levels of agreement to four cybersecurity attitude statements.

Base: UK & US based participants, total number: 2000, aged 18+, dates conducted: August 10, 2021 - August 18, 2021.

Whose responsibility is cybersecurity?

We all hold information that is valuable for cybercriminals. From our personal information (e.g. banking details) to credentials that enable access to various organizations’ networks or critical systems. So what happens when cybercriminals attempt to exploit these vulnerabilities? Whose responsibility is it to protect the people or the organizations they work in? Let’s look at some data about people’s perceptions of responsibility.

First, we asked participants⁷ who they perceived had the main responsibility to protect their organization’s information online. Participants organized stakeholders from “most” to “least” responsible.

40% of the participants perceived themselves to be the least responsible for protecting workplace information (shotgun, not it!) with the government, organization, and the IT department holding the top responsibility.

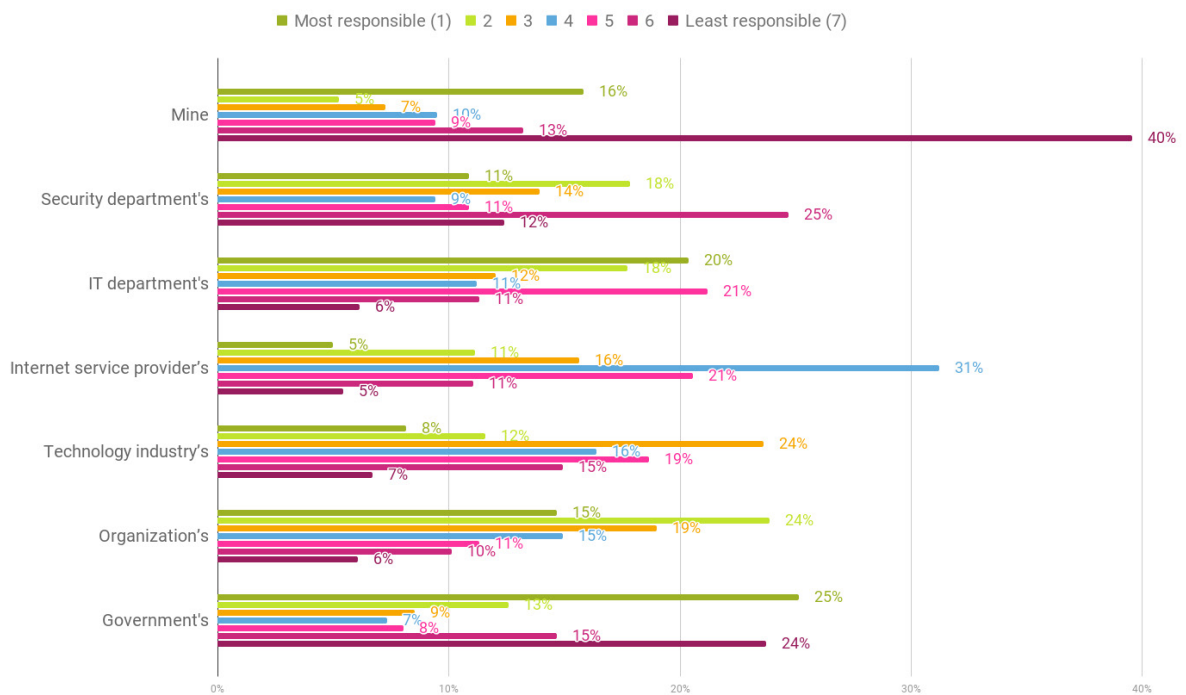


Figure 17. “Whose main responsibility is it to protect your workplace’s online information?”

Base: UK & US based participants, total number: 1105, aged 18+, dates conducted: August 10, 2021 - August 18, 2021.

7 This question was only asked to those participants who engaged in full- or part-time employment (55% of the participants).

PERCEPTIONS OF CYBERSECURITY PRACTICES

Similarly, we asked whose responsibility it was to protect an individual’s personal information online. All participants were asked to organize different stakeholders from “most” to “least” responsible. Over half of the participants (51%) stated that it was their own responsibility to protect their personal information with their family and employer being held as the least responsible to do so.

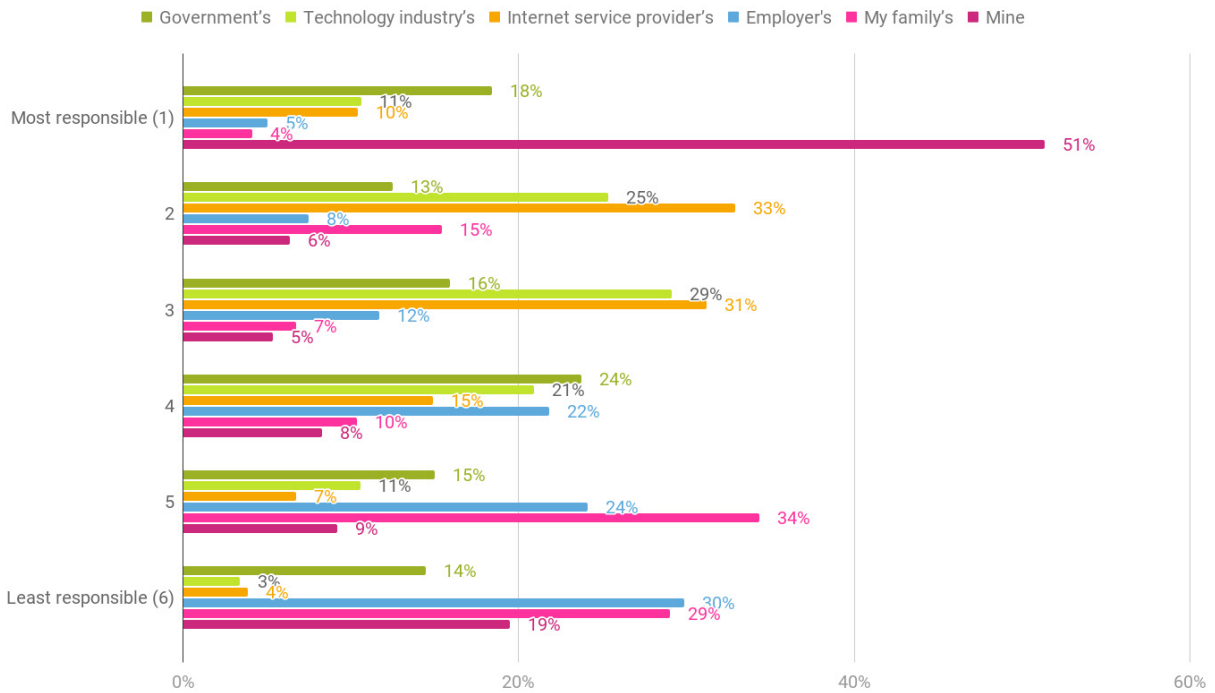


Figure 18. “Whose main responsibility is it to protect your online information?”

Base: UK & US based participants, total number: 2000, aged 18+, dates conducted: August 10, 2021 - August 18, 2021

Reliance on others for cybersecurity behaviors

When participants were asked about their reliance on others when performing various online activities, over half of participants reported being independent and not reliant on external help for various online behaviors. Overall, there was very little change in reliance on others between the different statements. Here, the most often independently performed activity was the creation of online accounts.

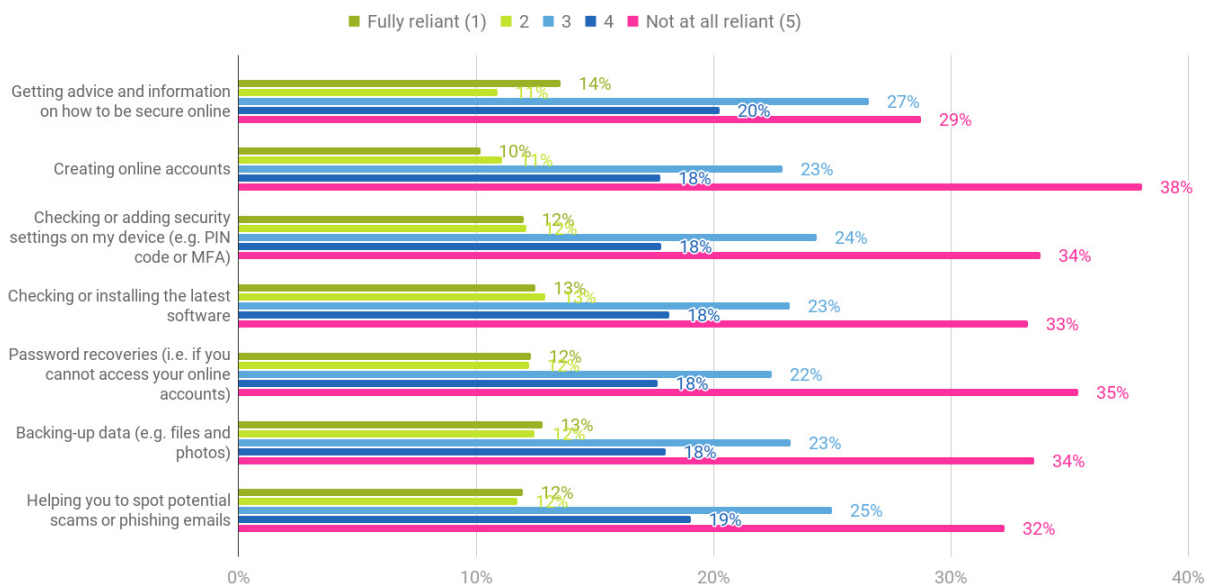


Figure 19. “How much do you rely on others (e.g. your family members, colleagues, or friends) to perform the following things...”

Base: UK & US based participants, total number: 2000, aged 18+, dates conducted: August 10, 2021 - August 18, 2021.

Awareness, engagement, and attitudes towards core security behaviors

Why do people do what they do? It’s a question that keeps a lot of us up at night! In this section, we’ve sought to provide a ‘temperature check’ on security attitudes in relation to seven⁸ core security behaviors.

These behaviors have been chosen and designated as ‘core’ during our research development phase. They were based on security behaviors mentioned in official guidance websites of the UK and US (US: Stay Safe Online⁹ and UK: Cyber Aware¹⁰) and included: creating strong passwords, using password management strategies, using Multi-Factor Authentication, installing the latest software/applications, checking messages for their legitimacy, reporting phishing emails and backing up data.

Password behaviors

43% of participants reported creating long and unique passwords for their online accounts “very often” or “always”. However, almost a third (28%) stated that they didn’t do so¹¹.

Similarly, using a different password for most important online accounts (“very often” or “always”) was reported by 46% of participants. Only 20% didn’t use separate passwords for these accounts.

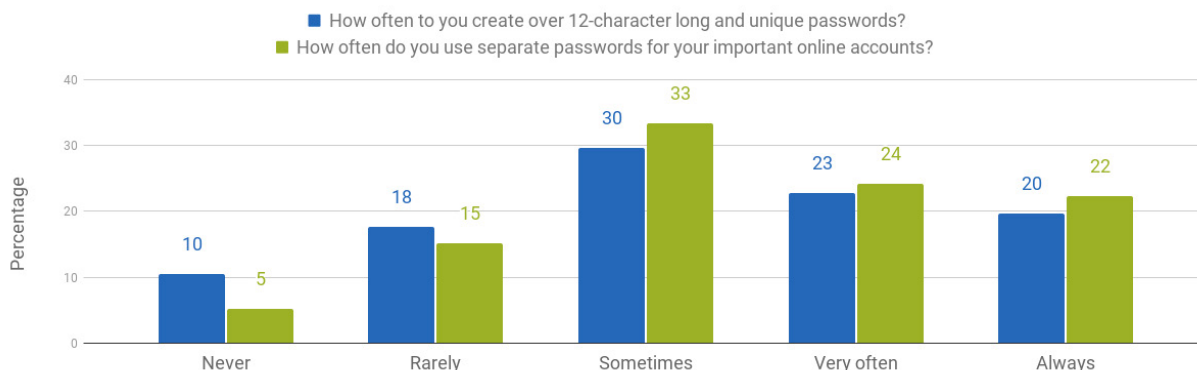


Figure 20. Participants’ password habits in relation to creating long and unique passwords and using separate passwords in their accounts.

Base: UK & US based participants, total number: 2000, aged 18+, dates conducted: August 10, 2021 - August 18, 2021.

8 Password behavior includes two of the core behaviors: creating long and unique passwords and using different password for each important online account.

9 <https://staysafeonline.org/stay-safe-online/online-safety-basics/>

10 <https://www.ncsc.gov.uk/cyberaware/home>

11 Includes responses “rarely”, “never” and “I don’t know what this is”.

Using password management strategies

The most commonly used password management strategy was writing them down in a notebook (31%). Remembering passwords was also seen as a popular technique reported by 26% of the participants. (Remember pets make great friends but terrible passwords.) Only 12% of the participants reported using a stand-alone password manager application with another 11% saving their passwords in their browser. 20% reported using other methods of password management strategies, including storing them on their email or phones.

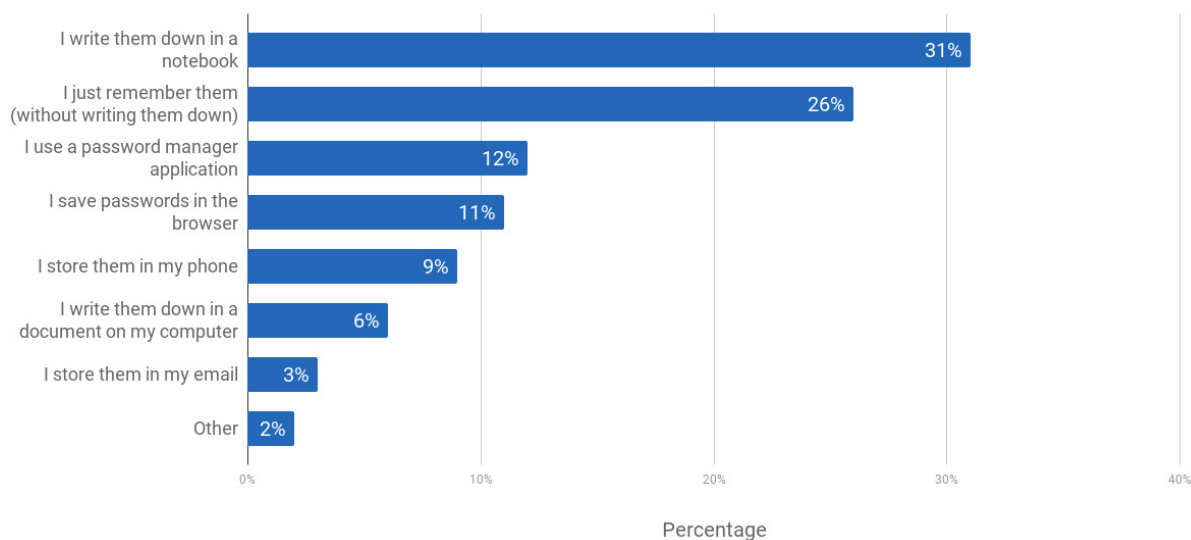


Figure 21. Participants’ preferred methods of remembering multiple passwords.

Base: UK & US based participants, total number: 2000, aged 18+, dates conducted: August 10, 2021 - August 18, 2021.

Use of a stand-alone password manager application was uncommon, with almost half (49%) of the participants noting they ‘never’ or ‘rarely’ used one. Additionally, 10% reported they didn’t know how to use one. Only 23% of participants reported using a password manager application regularly. Of those participants who reported having used a password manager, they had done so for four years on average.

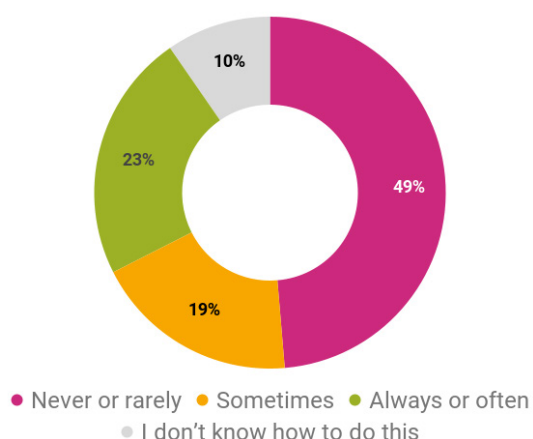


Figure 22. Use of password manager applications.

Base: UK & US based participants, total number: 2000, aged 18+, dates conducted: August 10, 2021 - August 18, 2021.

Using Multi-Factor Authentication (MFA)

Nearly half of all participants (48%) had either never heard of MFA. Of those who knew about it (52%), most had applied MFA to their online accounts (81%) and were still using it (90%).

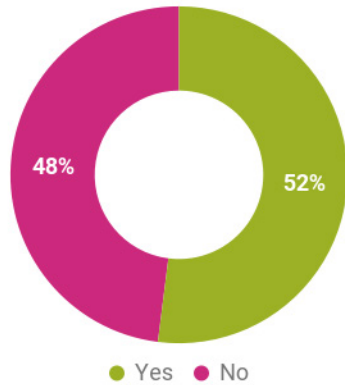


Figure 23. Have you ever heard of MFA?

Base: UK & US based participants, total number: 2000, aged 18+, dates conducted: August 10, 2021 - August 18, 2021

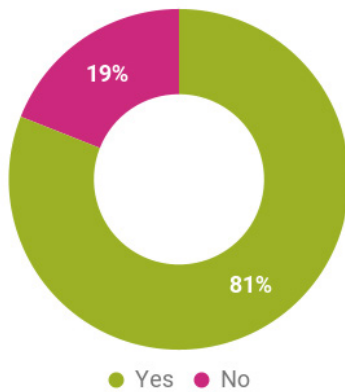


Figure 24. Have you ever applied MFA to your online accounts?

Base: UK & US based participants, total number: 1036, aged 18+, dates conducted: August 10, 2021 - August 18, 2021

– What’s the reason you have stopped using MFA?

“ I don’t feel safe using the services ”

“ It’s a total pain ”

“ My systems didn’t support it ”

“ Because it locks me out of my stuff too much ”

“ My company hasn’t recommended this ”

“ Too difficult and time-consuming ”

48%
of participants said they have never heard of MFA

Installing software and applications

68% of the participants reported installing the latest updates and software as soon as these are available. A little under 10% admitted that they don't update their software and applications when updates become available. (Even though we all know that installing software updates isn't a cunning rouse to get more people to buy more software!)

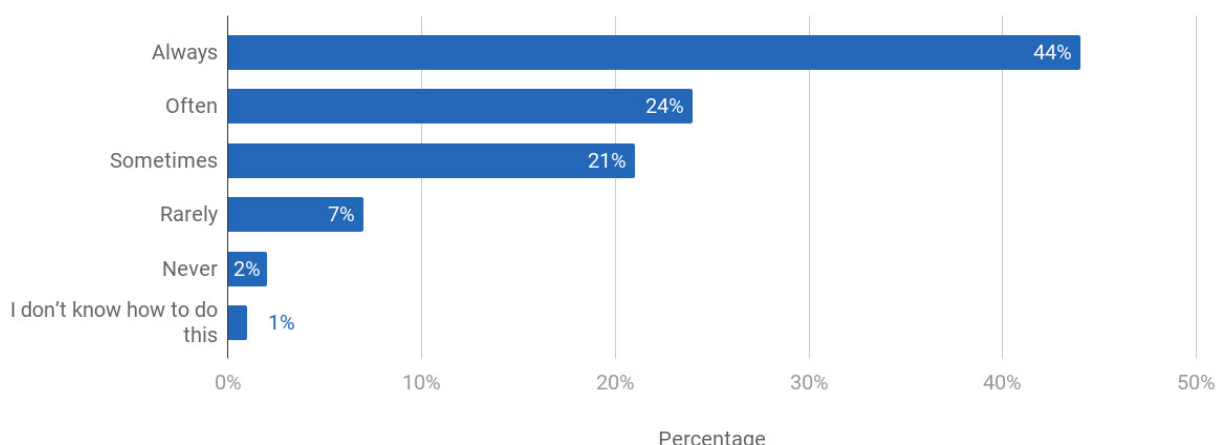


Figure 25. “How often do you install the latest updates and software when notified that they are available?”

Base: UK & US based participants, total number: 2000, aged 18+, dates conducted: August 10, 2021 - August 18, 2021.

Of those who reported installing the latest updates to their devices¹², 45% had turned on automatic updates. A further 21% noting that they take immediate action when they receive a notification.

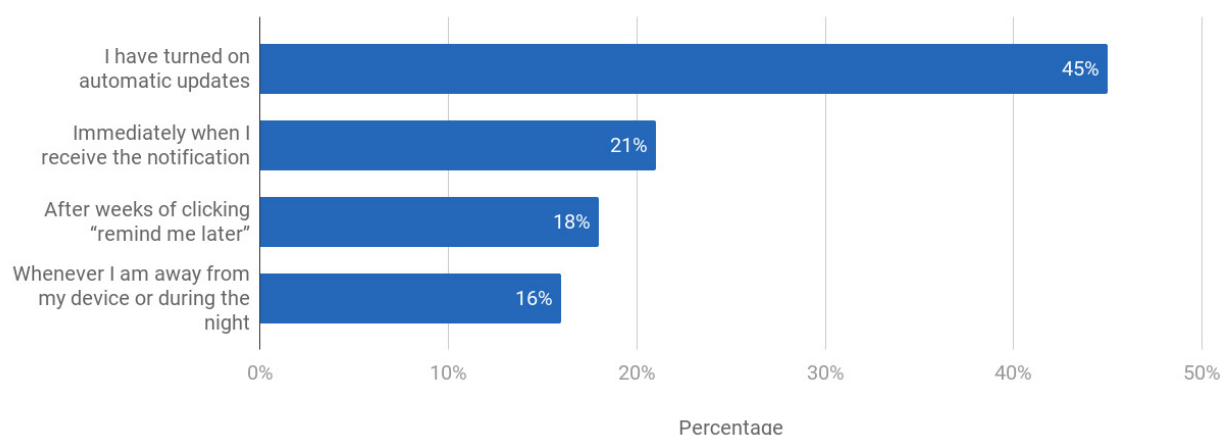


Figure 26. “When do you install updates on your devices?”

Base: UK & US based participants, total number: 1926, aged 18+, dates conducted: August 10, 2021 - August 18, 2021.

12 Includes responses “rarely”, “sometimes”, “very often” and “always”.

Confirming the legitimacy of an email

Most participants (72%) reported that they checked to see whether messages were legitimate (i.e. phishing or a scam) compared to 10% who reported not doing so.

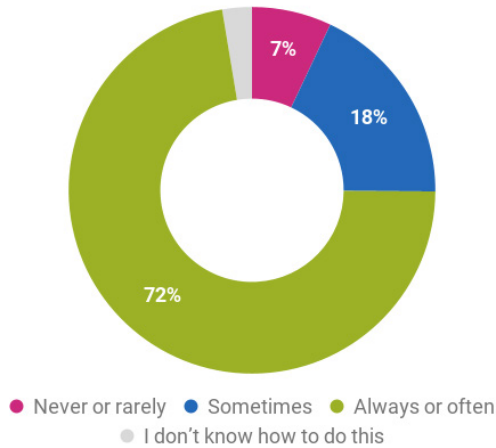


Figure 27. “When I receive a message(e.g. email)I ensure that it is genuine before clicking any links or responding to it”

Base: UK & US based participants, total number: 2000, aged 18+, dates conducted: August 10, 2021 - August 18, 2021.

Recognizing and reporting phishing emails

Nearly half of the participants (48%) reported phishing emails to the sender (e.g. the real person the cyber criminal tried to impersonate by sending the phishing email). 42% of the participants said they used the reporting capability on a platform (e.g. Gmail) “very often” or “always”.

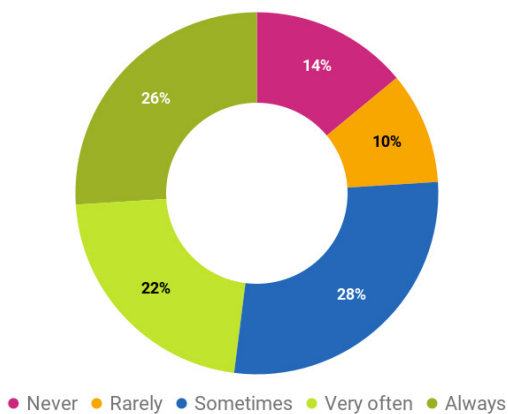


Figure 28. “If I receive a message from a known contact that sounds odd and/or includes links,I reach out to the person to inquire about it.”

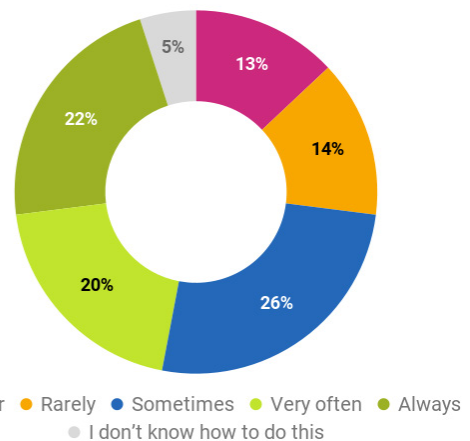


Figure 29. “How regularly do you report any phishing emails by hitting the ‘spam’ or ‘report phishing’ button?”

Base: UK & US based participants, total number: 2000, aged 18+, dates conducted: August 10, 2021 - August 18, 2021.

Backing up data

Nearly a third of the participants (30%) reported they back up their data frequently. An additional 15% noted they don't have to perform backups as they have turned on automatic updates. 19% reported they "never" or "rarely" backed up their data with some not knowing how to take action (5%).

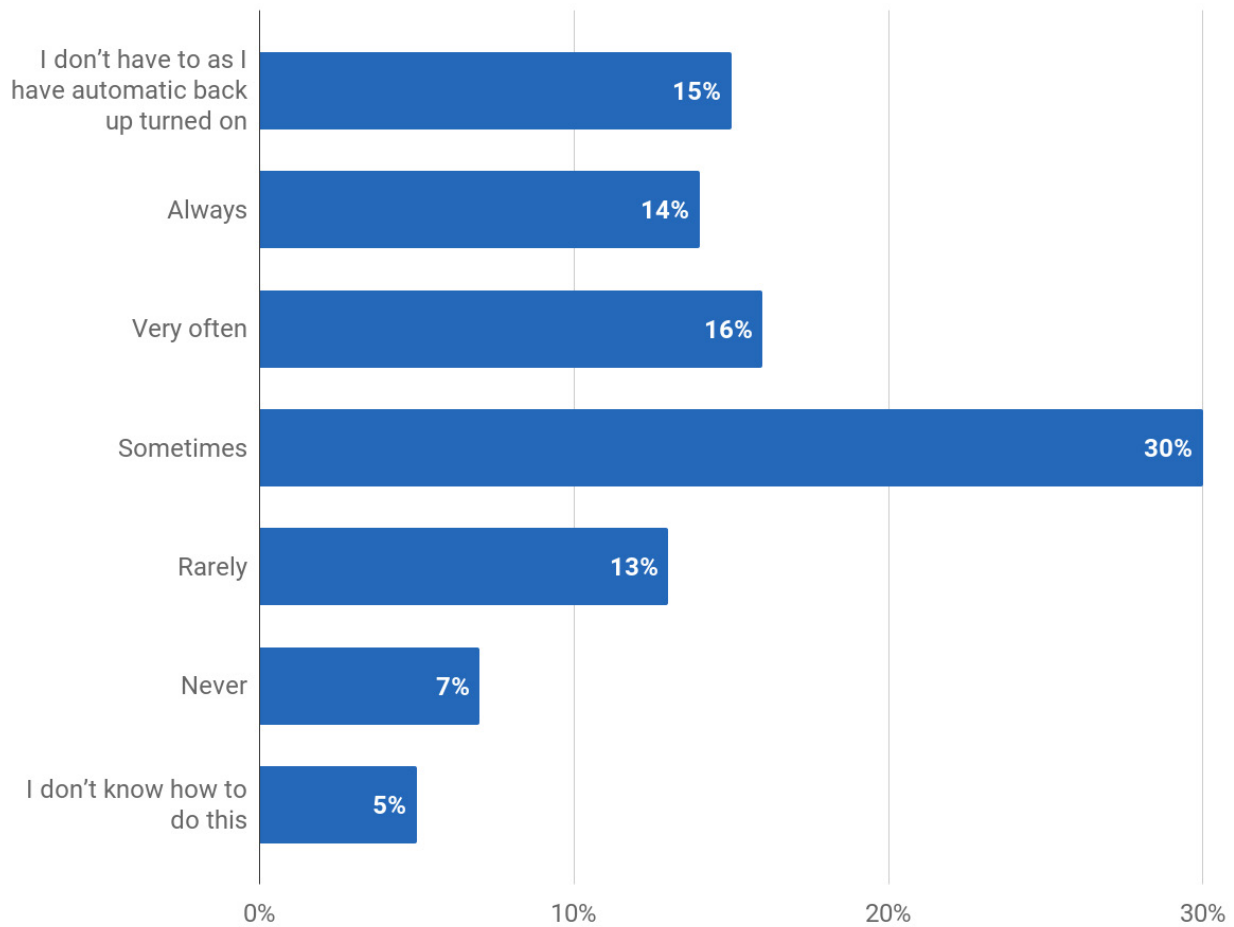



Figure 30. "How often do you manually back up your most important data?"

Base: UK & US based participants, total number: 2000, aged 18+, dates conducted: August 10, 2021 - August 18, 2021.

– I would report phishing attempts but...

“Nothing happens when you do”



**Barriers to
cybersecurity
behaviors**

Q: What do security awareness initiatives and New Years' resolutions have in common?

A: Telling people (or yourself) what you should do is a hell of a lot easier than *actually* doing it!

Like many of us on 1st January, security awareness initiatives have great intentions. They tend to focus on educating people on good cybersecurity practices, whether through public campaigns or inside organizations.

We're surrounded by various sources of cybersecurity information, each telling us how to best protect ourselves online. However, simply increasing knowledge and increasing awareness doesn't directly translate to changes in people's security behaviors^{13 14}. So why don't people translate their cybersecurity learnings (*knowing*) into practice (*doing*)? (People *know* smoking is bad for their health, but knowing alone doesn't enable most smokers to stop. What translates awareness to action?)

To better understand the "knowing-doing" gap, we looked into the potential drivers and barriers to cybersecurity behaviors. Here, we used a well-established behavior change framework, COM-B¹⁵.

COM-B states that for behavior change to occur one must have Capability, Opportunity, and Motivation to take action (equals Behavior).

This framework covers a wide range of topics from usable cybersecurity to people's attitudes and beliefs.

Those participants who reported not performing the core security behaviors were asked reasons why they didn't do so. The statements closely followed potential barriers to capability, opportunity, and motivation (as per the COM-B model) and varied according to the core security behavior in question.

The main two reasons for not performing the core security behaviors were: lack of knowledge (i.e. not knowing how best to take action) and the need to take action being rated as a low priority.

13 Gundu, T. (2019). Acknowledging and Reducing the Knowing and Doing Gap in Employee Cybersecurity. International Conference on Cyber Warfare and Security Conference. May 2019.

14 Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2020). Cyber security awareness, knowledge and behavior: A comparative study. Journal of Computer Information Systems, 1-16.

15 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.

Password management applications

When asked why they didn't use password manager application, 37% of the participants noted they don't trust any single provider with managing all their passwords. 18% didn't see password managers as a priority, and 14% didn't know how to use them, even if they wanted to. 'Other'¹⁶ reasons reported included having previous bad experiences using password managers, and not being aware of their existence.

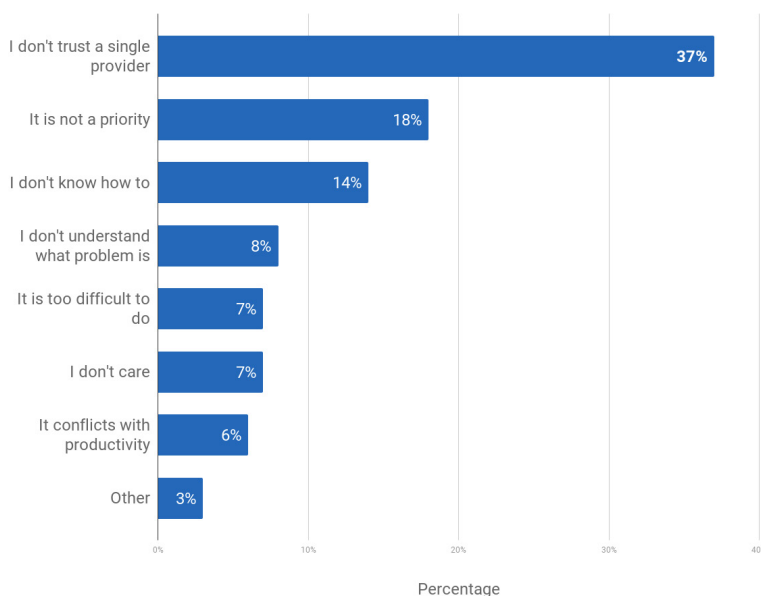


Figure 31. “I would use a password manager application, but...”

Base: UK & US based participants, total number: 1428, aged 18+, dates conducted: August 10, 2021 - August 18, 2021.

16 All 'other' reasons were collected using an open text field.

Only 43%

create a long and unique password either “always” or “very often”

– “I would use a password manager application but....”

“ I am not happy passing on sensitive info to an unknown third party ”

“ I used it and it failed locking me out of many websites. Never trust another again! ”

“ I feel that to use it properly I would need to get all my passwords from everything I use and it will take forever to do ”

Use of Multi-factor authentication (MFA)

When asked why they didn't use MFA a number of participants reported MFA isn't easy to use, (24%), while other participants didn't know how to best apply it to their online accounts (22%). Some had noted they understood the risks but never understood what the problem behind the risk was (18%) and others didn't believe or care about the risks of not having MFA (15%). 'Other' reasons for not using MFA included laziness in doing so, the perception that it might increase the chance of cybercriminals attacking you, and simply not having any interest in applying it.

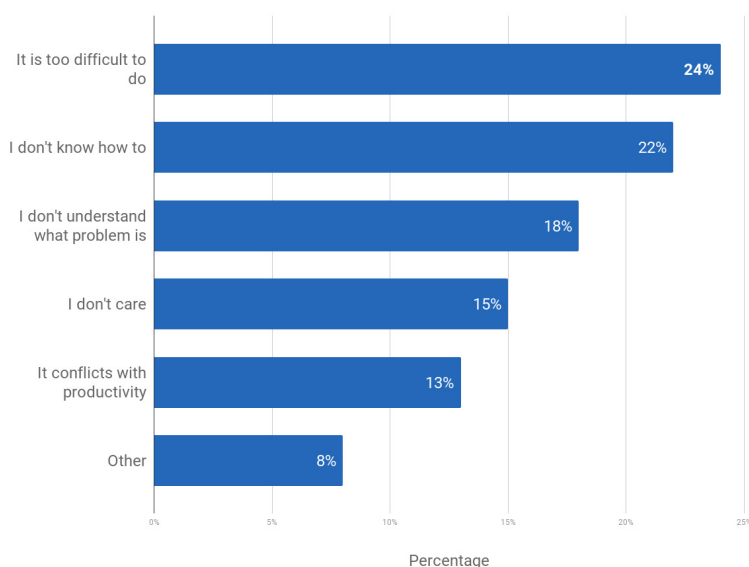


Figure 32. “I would use a multi-factor authentication (MFA) application but..”

Base: UK & US based participants, total number: 1161, aged 18+, dates conducted: August 10, 2021 - August 18, 2021.

– “I would use MFA but...”

“ Providing more information gives potential hackers more data to use ”

“ Waste of time ”

“ It is too much hassle for how very little I use the internet ”

“ I would have to research to see if this is really a good idea or not and figure it out on my own ”

“ It is such a bloody hassle! Plus I don't have a smartphone! ”

“ I am not interested in doing so and am not interested in having additional data like my phone number etc... known by every company whose sites I use ”

“ There have been multiple problems with using face recognition and fingerprints that's why I don't want it ”

“ I just want to log in easily ”

Installing the software and applications

32% of participants reported they generally didn't install the latest software or applications on their devices¹⁷. Out of these participants, 21% noted that despite wanting to ensure they run the latest versions, they didn't know how best to do it. 38% of the participants understood the risks of not running updates but either didn't care about or understand what the problem was. 'Other' reported reasons included the cost of installing updates, previous bad experiences of a device malfunction (as a result of an update), and perceptions they had 'nothing to protect'.

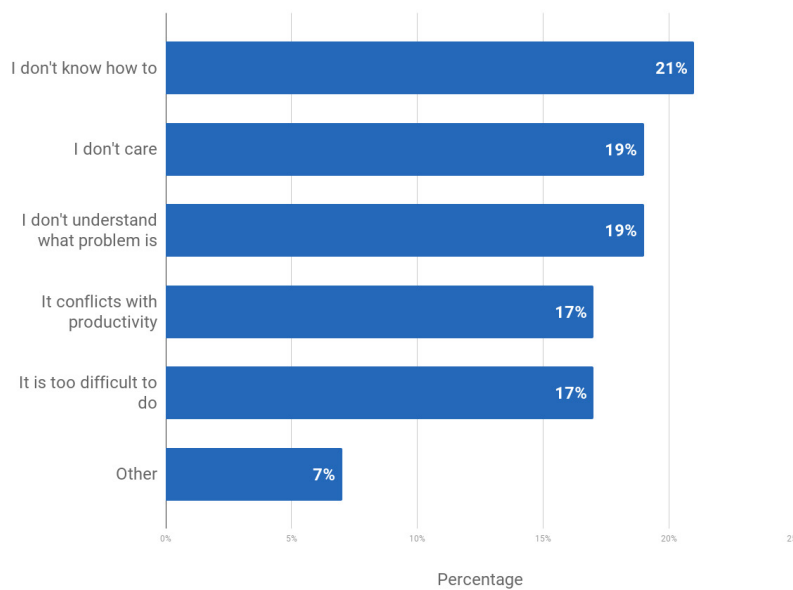


Figure 33. “I would install the latest updates and software to my devices, but...”

Base: UK & US based participants, total number: 640, aged 18+, dates conducted: August 10, 2021 - August 18, 2021.

17 This statement was presented only to those participants who reported not updating their devices often.

– “I would install the latest updates and software to my devices but...”

“ When I get an update I worry it is spam or a virus so don't do it ”

“ I have no money to protect. No secrets to cover. Basically, I have nothing to lose. Nothing to protect ”

“ They take up too much device storage ”

“ I delay the MS updates because of a past experience of one of them bugging up my computer! ”

“ It slows up my devices use ”

“ Avoiding unwanted changes to the program's functionality ”

“ I just hate doing it. Lazy ”

“ I worry that the new updates will confuse me because I will have to do things differently ”

“ It is too expensive ”

Reporting phishing messages

Over half of the participants stated they didn't report phishing attempts (58%) "very often" or "always". Out of these participants, 28% believed it is worth reporting phishing attempts, but they didn't see it as their priority. Another 28% wanted to report phishing but didn't know how best to do it. 'Other' reasons included reporting buttons not being available and perceptions it doesn't make any difference (e.g. rarely followed up) and are a waste of time.

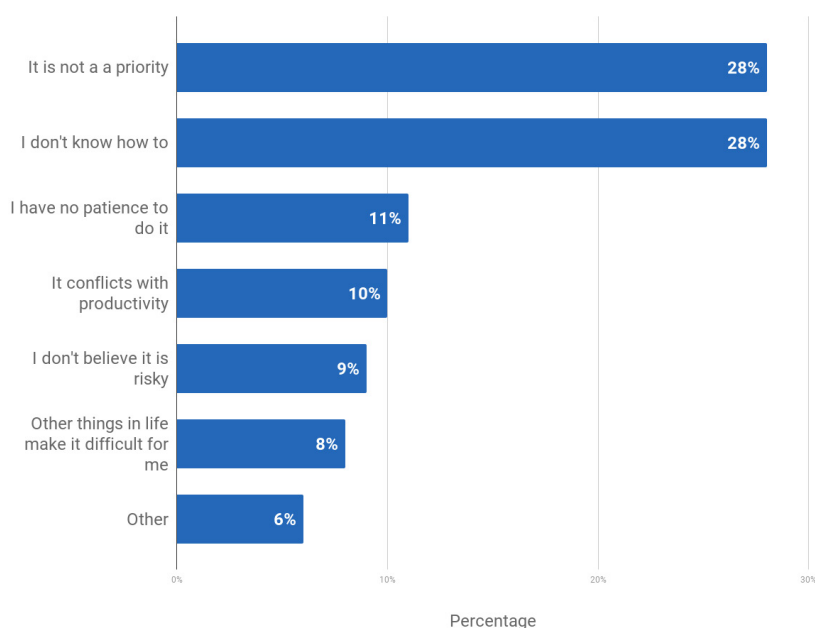


Figure 34. "I would report phishing messages, but..."

Base: UK & US based participants, total number: 1160, aged 18+, dates conducted: August 10, 2021 - August 18, 2021.

– "I would report phishing messaging but...."

“ There isn't always a reporting option available ”

“ At one point I made frequent reports, but it fizzled out ”

“ I don't believe the authorities care enough to act on the information ”

“ I'm not sure where I should be doing this, or how ”

“ Nothing happens when you do ”

“ I get so many I don't have the time! ”

Backing up data

Over half of the participants (54%) mentioned they didn't back up their data regularly. When asked why, 25% of these participants didn't see backing up data as their priority, although they acknowledged it would be worth it. Another 19% didn't know how best to do it even if they wanted to. Also, some participants didn't trust any single provider (e.g. cloud services) with their data. 'Other' reasons reported included the cost of backing up and not being bothered.

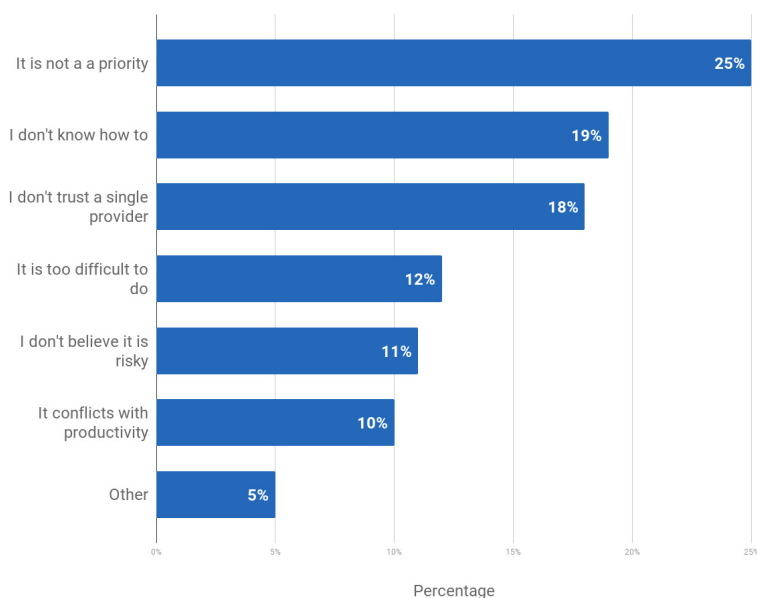


Figure 35. “I would back up my data (e.g. to an external hard drive or to a cloud) but...”

Base: UK & US based participants, total number: 1080, aged 18+, dates conducted: August 10, 2021 - August 18, 2021.

– **“I would back up my data (e.g. to an external hard drive or to a cloud) but...”**

“ I have little I need to back up ”

“ It can be expensive ”

“ I don't even know what a cloud service is! ”

“ I have no need to as I have nothing worth backing up ”

– Why didn't you report phishing?

“Data leaks happen all the time. I've had my details stolen from many different companies over the years. Who would I report it to?!”

**Advice sources
for cybersecurity
behaviors**

ADVICE SOURCES FOR CYBERSECURITY BEHAVIORS

A large portion of participants (64%) reported they didn't have access to cybersecurity advice or training. Out of the 37% who did have access, most had made use of it (73%), but the remaining 27% felt no need to benefit from the learning opportunity.

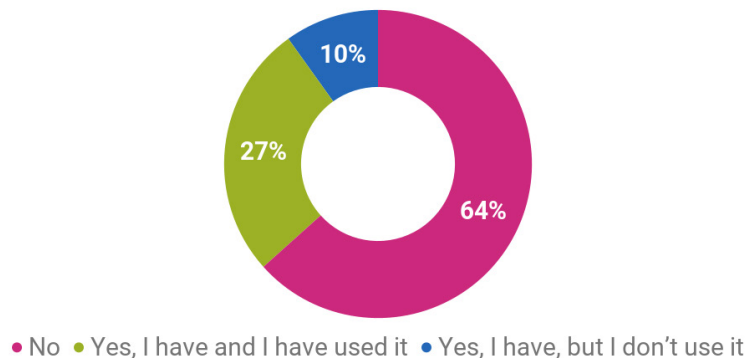


Figure 36: “Do you have access to cyber security advice or training (e.g. at work, place of education or library)?”

Base: UK & US based participants, total number: 2000, aged 18+, dates conducted: August 10, 2021 - August 18, 2021.

Participants who had stated they had applied a core security behavior (e.g. used a password manager application) were asked where they had learned about the specific behavior. Overall, the top sources for seeking information online were websites or applications. Additionally, participants reported they looked up information online on their own. The least common advice sources reported were learning through experience, hearing from others, and learning through a course.

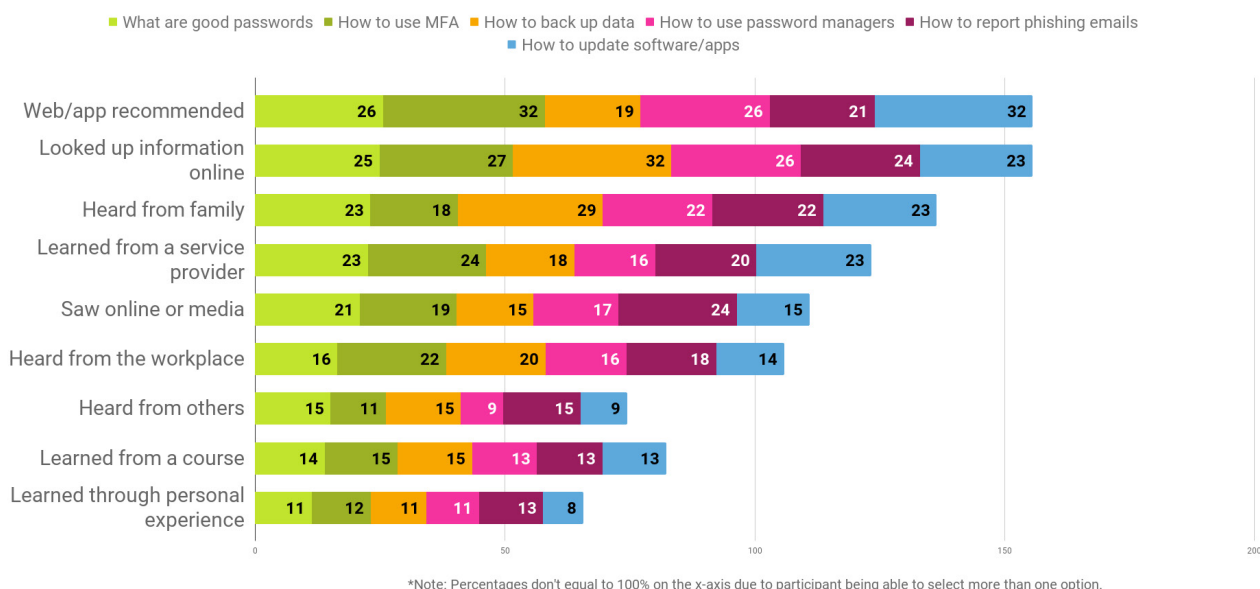


Figure 37. Advice sources: “Where did you learn about...”

Base: UK & US based participants, total number: 2000, aged 18+, dates conducted: August 10, 2021 - August 18, 2021.

– I would report phishing messages but...

“I don’t believe the authorities care enough to act on the information”

An abstract graphic consisting of several overlapping circles. Each circle is filled with a pattern of thin, parallel lines that radiate from the center, creating a sense of depth and movement. The circles are arranged in a way that they appear to be layered, with some in front of others. The overall effect is a dynamic, geometric composition.

The future and the Internet of Things

With the number of connected devices in our daily lives growing, cybersecurity behaviors are becoming increasingly complex. To better understand the security issues that may arise in the future, we asked people additional questions about their cyber security knowledge (e.g. ransomware) as well as attitudes and behaviors relating to Internet of Things (IoT) devices (e.g. smart home devices).

Cybersecurity knowledge

We asked how confident people felt in their knowledge of protecting themselves from harmful cyber activity. Over half of the participants (60%) reported reasonably high or very high confidence in their abilities. However, reflecting on the core security behaviors described earlier, 48% of the participants stated they had never heard of MFA. (This seems to be the same phenomenon afflicting terrible car drivers, ability and ambition are often misconstrued!)

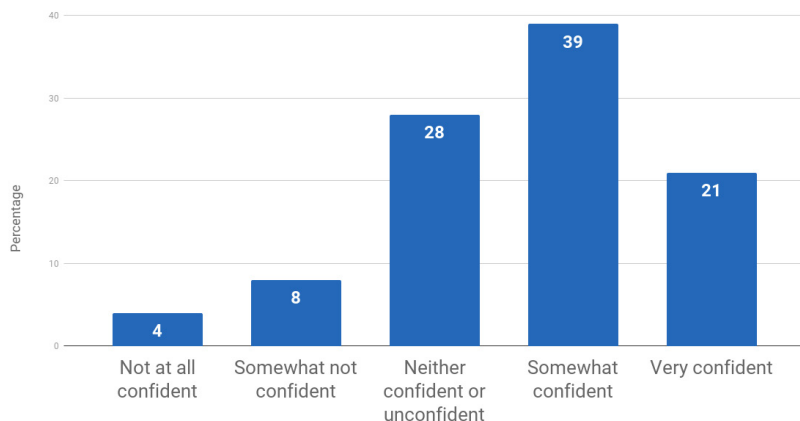


Figure 38. Confidence in knowing how best to protect oneself from harmful cyber activity.

Base: UK & US based participants, total number: 2000, aged 18+, dates conducted: August 10, 2021 - August 18, 2021.

When we asked about ransomware, 21% said they didn't know what ransomware was, with a further 14% providing an incorrect answer - ("It's how the cyber criminal evaded the police..." Ker-pish. Get it??;-))

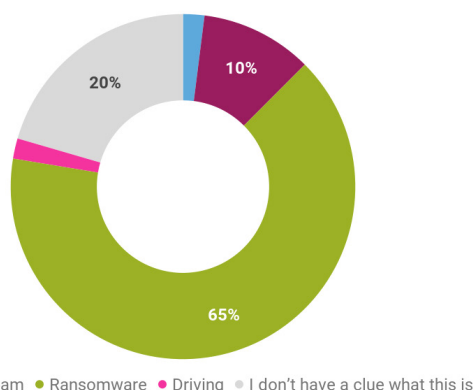


Figure 39. Participants' knowledge of ransomware.

Base: UK & US based participants, total number: 2000, aged 18+, dates conducted: August 10, 2021 - August 18, 2021.

IoT devices

The most common internet-connected device was the Smart TV, owned by 60% of participants. The second most common connected device in households were video gaming consoles (e.g. Xbox 360 or PlayStation). A portion of the participants (21%) did not own any smart devices.

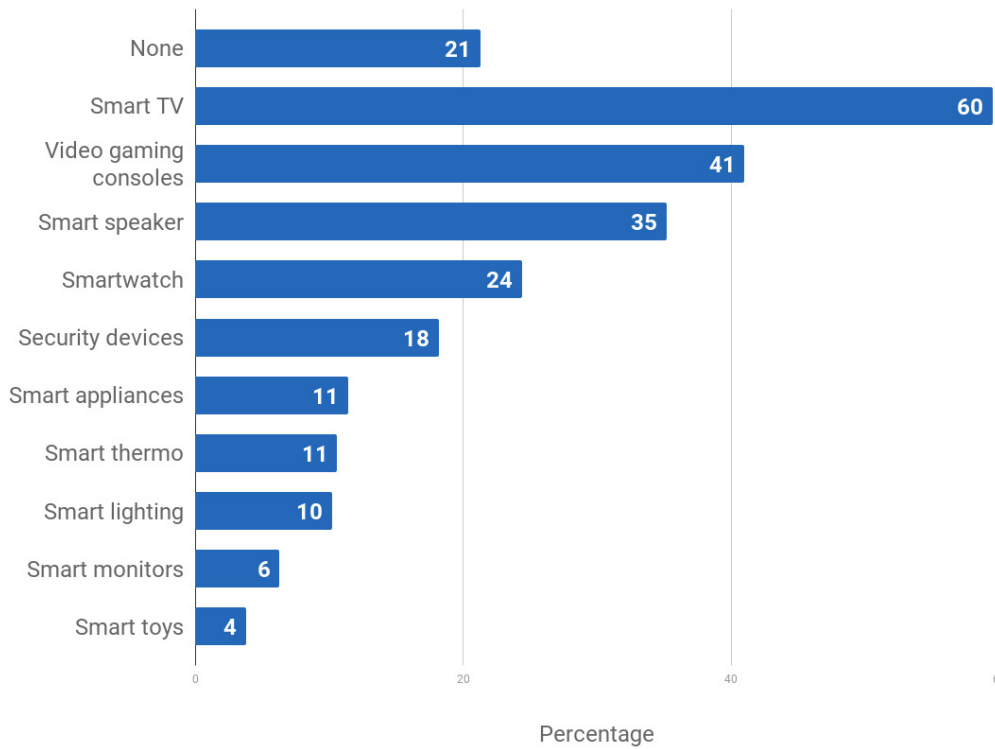


Figure 40. IoT device ownership.

Base: UK & US based participants, total number: 2000, aged 18+, dates conducted: August 10, 2021 - August 18, 2021.

48%
of respondents said
they have never
heard of MFA

THE FUTURE AND THE INTERNET OF THINGS

We asked participants how long they would spend researching the security of a device before buying it. 29% reported they tend to buy the item without examining its security features. Interestingly, 47% of the participants reported spending a few hours or a day of their time researching the device’s security-related information.

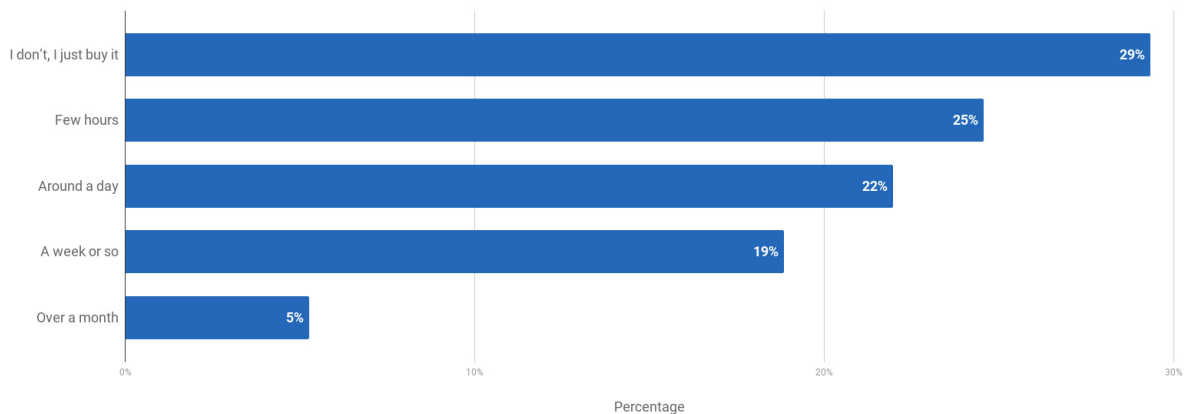


Figure 41. Time spent researching the device’s security features before buying.

Base: UK & US based participants, total number: 2000, aged 18+, dates conducted: August 10, 2021 - August 18, 2021.

Overall, participants noted they are ‘somewhat’ confident in the security of their connected home devices (40%). When asked how regularly they update their devices, over half of participants (54%) performed updates regularly (or had them turned on to update automatically). Almost a quarter (24%) of participants responded “rarely” or “never” or that they “do not know how to” take action. (This means your smart fridge probably will tell your partner about your chocolate cake addiction!)

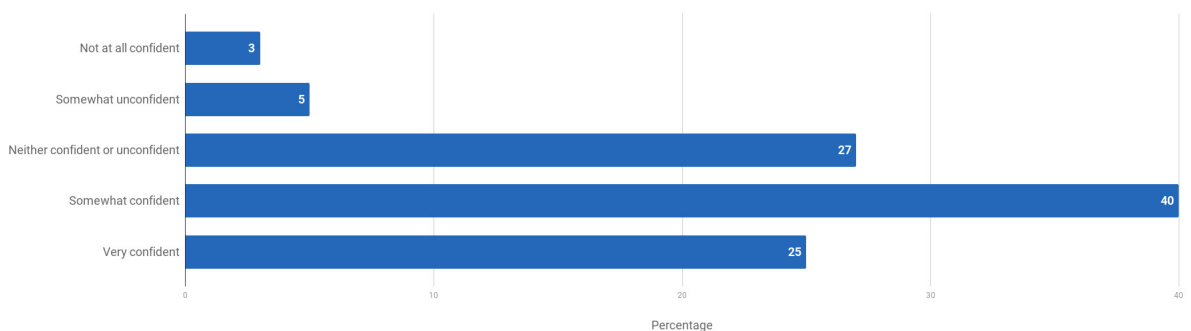


Figure 42. “How confident are you in the security of the connected devices you have in your home?”

Base: UK & US based participants, total number: 2000, aged 18+, dates conducted: August 10, 2021 - August 18, 2021.

THE FUTURE AND THE INTERNET OF THINGS

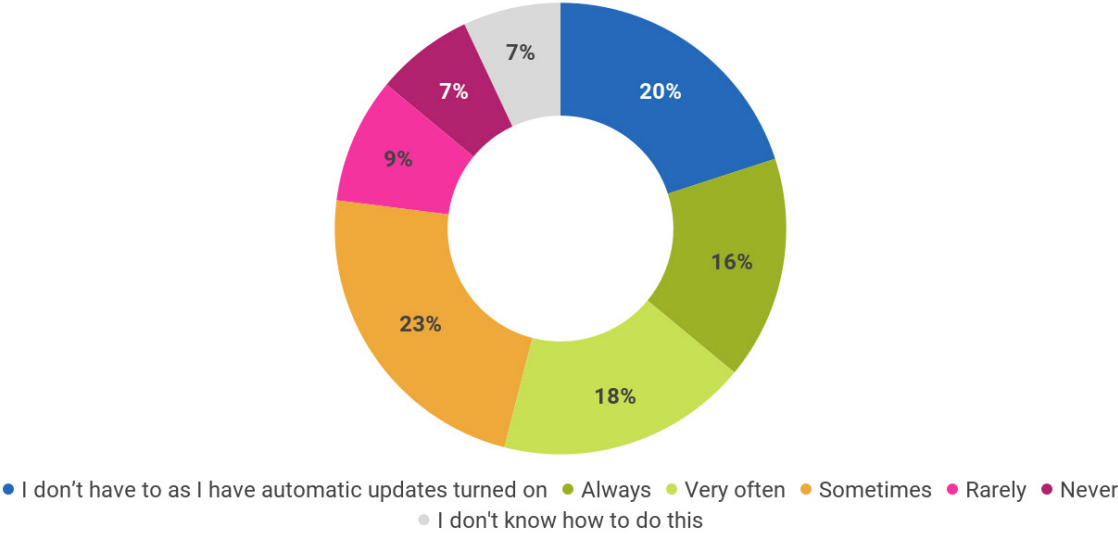


Figure 43. Frequency of updating IoT devices.

Base: UK & US based participants, total number: 2000, aged 18+, dates conducted: August 10, 2021 - August 18, 2021.

– *I would use a MFA but...*

“Providing more information gives potential hackers more data to use”

Conclusion

CONCLUSION

We've been educating people on good cybersecurity practices for decades. Public campaigns and organizations show us the best ways to protect ourselves online and stay safe from cybercriminals. Yet, cybercrime is still a major global challenge.

This report has provided a snapshot of public levels of security awareness, engagement, and attitudes towards good cybersecurity behaviors. We've explored the gaps between 'knowing' and 'doing' and applied a well-known behavioral change framework (COM-B) to examine potential drivers and barriers to good cybersecurity behaviors.

The truth? Several factors contribute to the adoption of good cybersecurity behaviors, such as individual capability and motivation (and coffee, coffee is a big contributor ;-)).

The survey response data reveals a mixed picture of people's engagement and attitudes to good security behaviors. A large proportion of participants reported staying secure online was important to them (85%), and they perceived it as a high priority (76%), feeling confident in their knowledge of protecting themselves from harmful cyber activity (60%). But many of their core security behaviors suggest otherwise.

Our key findings indicate

people don't exhibit core security behaviors for a variety of reasons.

It is in part due to a lack of knowledge (i.e. not knowing how best to take action). An example of this is that nearly half of all participants (48%) had never heard of MFA (that's Multi-Factor Authentication btw, in case you are in the 48%!). The biggest barrier for those who had heard about it, but not applied it in practice, was the lack of knowledge on how best to apply it to their online accounts. However, it's also clear many perceive some of the core behaviors as a pretty low priority (e.g. why would you waste time backing up data!).

The data also exposed cases where the result might have been expected but the reasons were arguably less obvious prior to the research. An example would be the use of a password management application, which was fairly low, with almost half of the participants (49%) stating they "never" or "rarely" used it. One of the key reasons people gave for not using a password manager was actually the lack of trust in a single provider (37%)!

Interestingly 64% of participants stated they didn't have access to cybersecurity advice or training - despite the wealth of information available. 43% reported the cost of applying online protection was too expensive. 41% of people found staying secure frustrating. 39% felt confused about the online security information available to them. And 38% consider themselves to be a likely target of a cybercrime.

Over one-third of the survey participants reported they had experienced harmful cyber activity at least once in their lives. However, most participants (61%) stated they didn't report cybercrime to anyone. This was another area in which we observed clear generational differences.

CONCLUSION

The research data reinforced the importance of awareness and engagement efforts to drive good security behaviors through public campaigns. It's also clear from the data that websites and other online sources are important sources of information, as stated by those who had reported the adoption of good security behaviors. Whether it's reporting cybercrime, phishing attempts, or installing the latest updates and software'- the report helps shed light on a variety of important security behaviors, all necessary to reduce individual and organizational risk.

For this first edition of our annual report, we've looked at the prominent trends in core cybersecurity behaviors and analyzed them with the aim that these can help organizations and individuals to personalize or tailor security initiatives. The report provides data that can be used to support both public and private campaigns to increase security awareness, challenge security attitudes, and create behavior change.

We hope you enjoyed the Annual Cybersecurity Behaviors and Attitudes Report 2021. We look forward to discussions and welcome your feedback.



An abstract graphic consisting of two overlapping circles. The circles are filled with a pattern of thin, parallel lines that radiate from the center of each circle, creating a sense of depth and movement. The lines are light blue and set against a darker blue background.

Appendix

Methodology

Survey design

The self-report survey was designed to examine the desired cybersecurity behaviors listed earlier. Most multiple-choice survey items were measured with a 5-point Likert scale. Some security perception items (e.g. confidence) were measured using a 10-point sliding scale with two anchor points. Limited text fields were recorded if the participant selected options like 'other,' 'please specify' or 'why did you not do X'.

Procedure

Call for participation was placed on the Toluna platform, which has an online participation panel in 70+ global markets. Participants signed up through the website to take part in the study and were compensated for their participation. Survey participants 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 didn't collect any identifiable personal information.

Sample

A representative sample (i.e. age and education) was sought from the UK or US population. Those over 18 years of age and fluent English speakers were able to take part.

Table 2 describes the survey sample demographics with an equal split of US and UK participants from various backgrounds. 54% of participants identified as female, and over half of the participants (55%) stated they were in employment. Tables 3 and 4 describe the race/ethnic background of the participants, with the majority identifying as white (81%)¹⁸. Tables 5 and 6 describe the education level of the participants.

18 Based on a total sample of 2000 participants in the US and the UK.

Demographic		Number of participants (%)
Country of residence	US	1000 (50%)
	UK	1000 (50%)
Gender	Female	1087 (54%)
	Male	885 (44%)
	Non-binary	17 (1%)
	Other	11 (1%)
Employment status	Employed	1079 (54%)
	Full-time	826 (41%)
	Part-time	253 (13%)
	Student	77 (4%)
	Not working	51 (3%)
	Working	26 (1%)
	Retired	434 (22%)
	Not in active employment or study	358 (17%)
Other	52 (3%)	

Table 2: Participant demographics.

Race (US)	Number of participants (%)
White	743 (74.3%)
Black or African American	150 (15.0%)
Asian	28 (2.8%)
Native Hawaiian or other Pacific Islander	7 (0.7%)
Hispanic, Latino or Spanish origin	42 (4.2%)
Mixed or multiple race	14 (1.4%)
Prefer not to say	7 (0.7%)
Other	9 (0.9%)

Ethnicity (UK)	Number of participants (%)
White	883 (88.3%)
Mixed or multiple ethnic groups	19 (1.9%)
Asian or Asian British	59 (5.9%)
Black, African, Caribbean or Black British	25 (2.5%)
Another ethnic group	6 (0.6%)
Prefer not to say	8 (0.8%)

Tables 3 and 4: Participant race/ethnicity.

Education Level (US)	Number of participants (%)
Some high school credit, no diploma or equivalent	40 (4%)
High school graduate, diploma, or the equivalent (e.g. GED)	290 (29%)
Some college credit, no degree	198 (20%)
Trade, technical or vocational training	38 (4%)
Associate degree	124 (12%)
Bachelor's degree	202 (20%)
Master's degree	88 (9%)
Professional degree	8 (1%)
Doctorate degree	11 (1%)
Other	1 (0%)

Education Level (UK)	Number of participants (%)
Apprenticeship	27 (3%)
GCSE or equivalent	270 (27%)
NVQ or equivalent	123 (12%)
A and AS level or equivalent	214 (22%)
Degree-level or higher	342 (34%)
Other	24 (2%)

Tables 5 and 6: Participant's educational level.

Data quality

Data was checked for quality by the research team. In the first instance, 85 ‘bots’ and responses deemed as ‘low quality’¹⁹ were omitted. They were replaced by Toluna reopening the survey to ensure a full dataset of 2000 people.

Data analysis

The survey items included a large number of descriptive questions amongst 5-point or 10-point (e.g. items measuring confidence) Likert scale questions. We have descriptively analyzed most of the close-ended questions.

19 By low quality we mean responses that included open text fields with meaningless text combined with completion time being only a few minutes.

Differences in victimization, security attitudes, and behaviors by country

For this additional section, we explored whether any differences existed between the two country samples. Cultural differences relate to our values and underpin our decision-making processes. They've been examined as a factor to explain people's security behaviors and we were keen to explore if they had an influence on cybersecurity attitudes and behaviors²⁰.

The US and the UK comparisons

There were no distinct differences in attitudes relating to the importance of staying secure online between the two countries (63% US and 60% UK agreed with the statement). However, US citizens (78% agreed) prioritized security online slightly more than UK citizens (74% agreed).

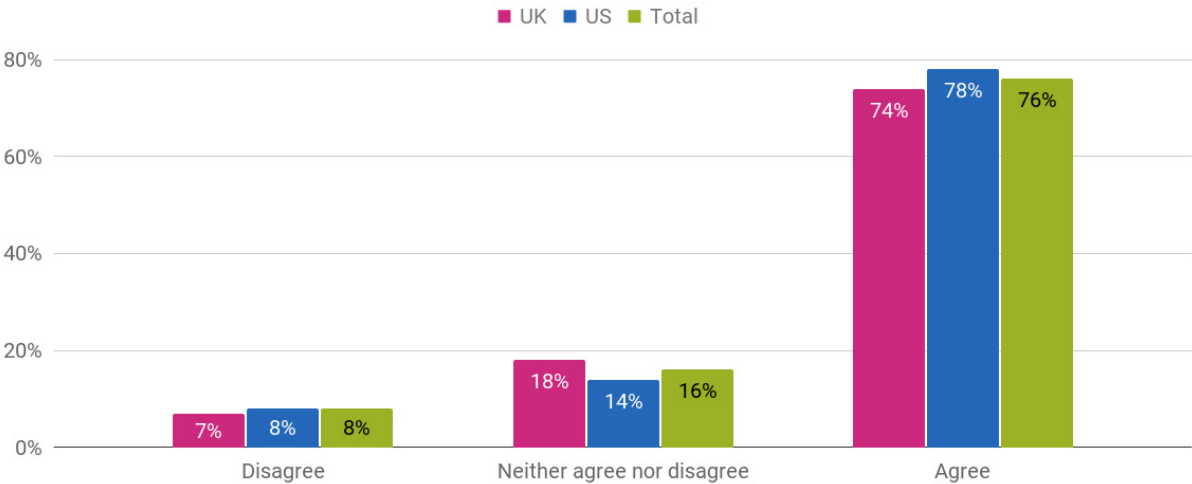


Figure 44. Prioritization of cybersecurity by country: “I prioritize staying secure online”.

Base: UK & US based participants, total number: 2000, aged 18+, dates conducted: August 10, 2021 - August 18, 2021.

20 Henshel, D., Sample, C., Cains, M. G., & Hoffman, B. (2016). Integrating cultural factors into human factors framework and ontology for cyber attackers. In *Advances in Human Factors in Cybersecurity: Proceedings of the AHFE 2016 International Conference on Human Factors in Cybersecurity* (pp. 123–137).

Participants from the US leaned towards finding cybersecurity more frustrating (44%) and intimidating (44%) than UK citizens (38% and 38% respectively).

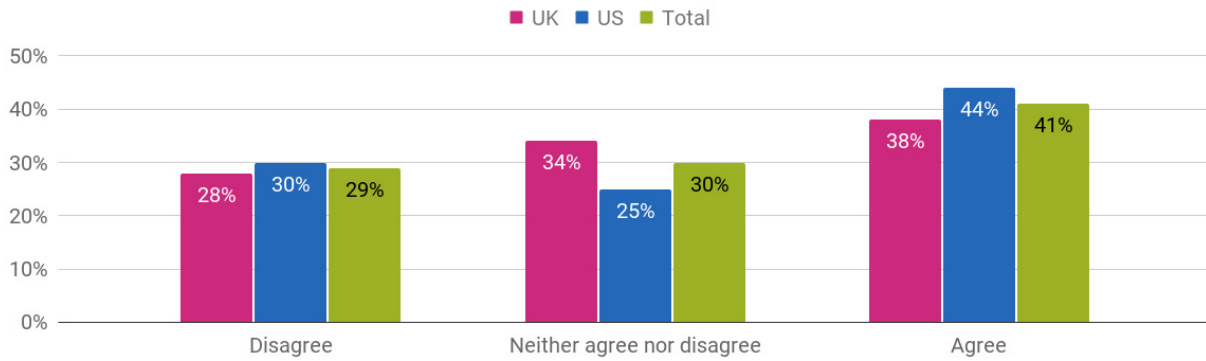


Figure 45. Feelings of intimidation of cybersecurity by country: “I find cybersecurity intimidating”

Base: UK & US based participants, total number: 2000, aged 18+, dates conducted: August 10, 2021 - August 18, 2021.

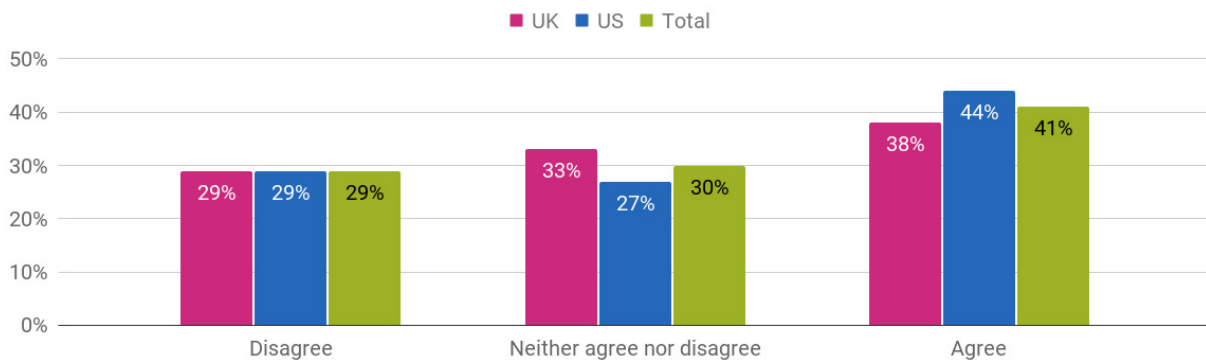


Figure 46. Feelings of frustration of cybersecurity by country: “I find staying secure online frustrating”

Base: UK & US based participants, total number: 2000, aged 18+, dates conducted: August 10, 2021 - August 18, 2021.

Overall, US citizens felt more confident in their ability to identify malicious emails (e.g. phishing).

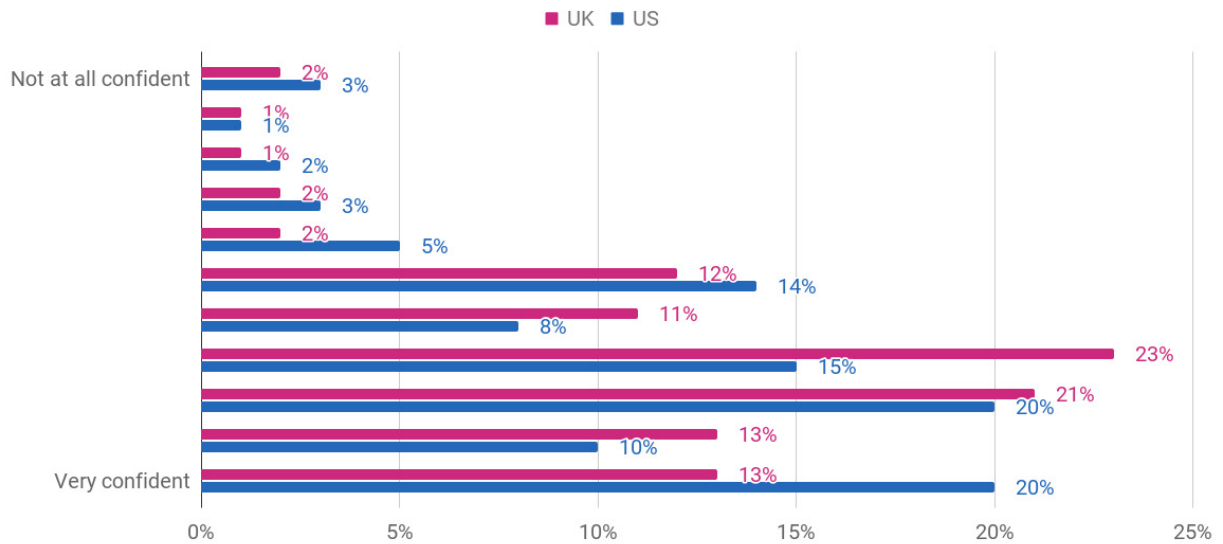


Figure 47. Confidence in recognizing malicious and/or illegitimate email from a cybercriminal by country.

Base: UK & US based participants, total number: 2000, aged 18+, dates conducted: August 10, 2021 - August 18, 2021.

US citizens (38% for cybercrime and 24% for identity theft) were more likely to have been victims than their UK counterparts (29% for cybercrime and 15% for identity theft). In terms of reporting those crimes, there was only a 4% difference between the countries.

ABOUT



A leading non-profit organisation, The National Cybersecurity Alliance is dedicated to creating a more secure, interconnected world. Advocating for the safe use of all technology, The National Cybersecurity Alliance aims to educate everyone on how best to protect themselves, their families, and their organisations from cybercrime.

The National Cybersecurity Alliance 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 is a UK-based cyber security and data analytics software company focused on behavioural security, working to make it easy to manage human cyber risk.

With a team made up of psychologists, behavioural scientists and security experts, CybSafe delivers a range of leading security research initiatives aimed at better understanding human decision making and security behaviour.

CybSafe is designed for the modern, hybrid workforce and is on a mission to revolutionise the way society addresses the human aspect of cyber security. At the heart of CybSafe’s behavioural security platform is SebDB, the world’s most comprehensive security behaviour database, offering insight into every security behaviour capable of minimising human cyber risk.

Expert contributors

Oz Alashe MBE, CEO & Founder, CybSafe

Lisa Plaggemier, Executive Director,
The National Cybersecurity Alliance

Leah DeLancey,
The National Cybersecurity Alliance

Jennifer Cook,
The National Cybersecurity Alliance

Veronika Bondareva, CybSafe

Samuel Faiers, CybSafe

Dorothy Crenshaw,
Crenshaw Communications

Cliff Maroney,
Crenshaw Communications

Holly Mercer, Resonance

Savan Patel, Resonance

Authors

Dr. Inka Karppinen, Behavioral Scientist,
CybSafe

Ruya Ince, Survey Specialist,
CybSafe

Contact us: research@cybsafe.com