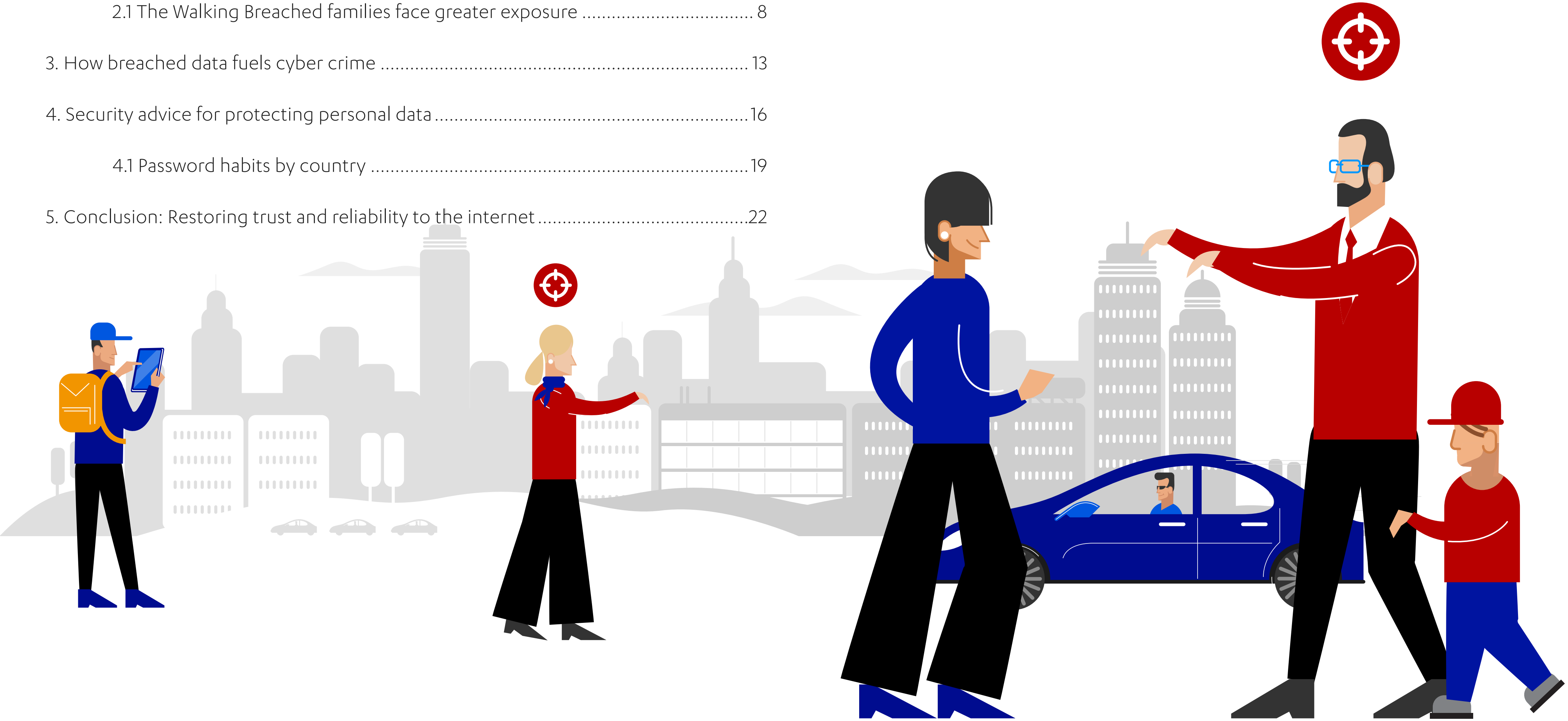
THE WALKING BREACHED

HOW DATA BREACHES PUT PEOPLE AT RISK OF CYBER CRIME

F-Secure

CONTENTS



INTRO: DATA BREACHES AFFECT US ALL

The digitization of society has created massive conveniences for consumers, along with an ever-growing variety of risks.

Millions, if not billions of people have created numerous online accounts. Online services exist for everything from email to photo services to online bill payments. The popularity of these online services has created a massive explosion of data. A 2018 report found that 2.5 quintillion bytes of data are created every day.[1] A quintillion has 18 zeros.

Enjoying these online services puts an individual at constant risk of crimes that did not even exist a few decades ago. A security failing in one online account—and the credentials and personal information connected to the account—can affect numerous other accounts, creating the potential for fraud and identity theft. Even if an adult alive in 2021 has somehow managed to avoid creating any online accounts, his or her data could still find their way into the wrong hands. More than 147 million people learned this sad reality when credit reporting agency Equifax announced a breach in late 2017.[2]

New data breaches make headlines on a constant basis. A total of 540 data breaches were identified in the first half of 2020 — nearly three a day.[3] According to one report, more information was stolen in 2020 than any other year, with 36 billion records stolen in the first three quarters of the year.[4] And while data breaches cost companies money — an average of 3.86 million USD, according to one study[5] — the damage doesn't end at a business' bottom line. According to the Identity Theft Resource Center, over 163 million people had their identities compromised in 540 breaches in the first half of 2020.[6] And while breaches of public-facing corporations often generate media attention, hacks of individual users from users rarely make the news, even though they affect millions, perhaps even billions, of people each year.

> A security failing in one online account—and the credentials and personal information connected to the account—can affect numerous other accounts, creating the potential for fraud and identity theft.

This report exposes the often-neglected connection between cyber crime and hacked accounts to reveal the role that breached or exposed data plays in the overwhelming pervasiveness of crimes committed online. It lays out several reasons why this correlation is significant, explains how exposed data leads to cyber crime, and offers security advice that individuals can follow to mitigate the risks posed by today's online threats.

[1] Data Never Sleeps 5.0 https://www.domo.com/learn/data-never-sleeps-5

[2] Equifax Data Breach Settlement: What You Should Know https://www.consumer.ftc.gov/blog/2019/07/equifax-data-breach-settlement-what-you-should-know

[3] The number of data breaches is actually down 33% so far this year—here's why https://www.cnbc.com/2020/07/14/number-of-data-breaches-down-33-percent-in-first-half-of-2020.html

[4] Number of "Breached" Records Hits 36 Billion in 2020 https://www.infosecurity-magazine.com/news/number-of-breached-records-hits-36/

[5] Cost of a Data Breach Report 2020 https://www.ibm.com/security/data-breach

[6] Identity Theft Resource Center's 2020 Six-Month Data Breach Analysis and Key Takeaways https://www.idtheftcenter.org/wp-content/uploads/2020/09/2020-ITRC-Q1and-Q2-Data-Breach-Trends-One-Pager-V3.pdf

THE WALKING BREACHED

Online services offered by companies often store significant amounts of information about the people that use them. When organizations running online services suffer a data breach, users' information can fall into the wrong hands. Consequentially, people whose data is compromised when the online services they trust are breached — the so-called "Walking Breached" — can often become collateral damage of attacks on corporations.

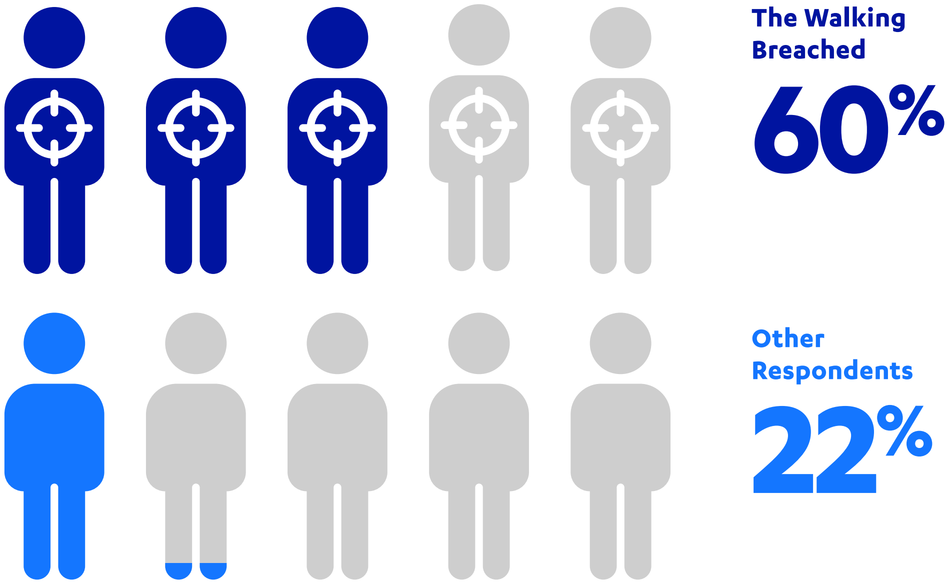
A recent F-Secure consumer survey collected responses from 4,800 participants across 12 different countries (400 per country): Brazil, Finland, France, Germany, Italy, Japan, Mexico, the Netherlands, Poland, Sweden, the United Kingdom, and the United States. The survey, conducted in May 2020, asked participants a variety of questions about their internet habits, their experiences, thoughts, and feelings toward cyber crime, and any measures they take to protect themselves and data from online threats.

Respondents identified as "The Walking Breached" include those who said 1 or more of the online services they use have experienced a breach.

"Other Respondents" consists of the remaining survey respondents, who answered they did not use any breached services, or didn't know.

18% of survey respondents know they're using one or more online services that have been breached, making nearly one in five participants members of The Walking Breached. This does not necessarily mean these respondents' information was stolen (although it's a very real risk in these cases). However, cyber crime was clearly more common among respondents that knew they were using breached services. 60% of these respondents, or 3 out of every 5, reported experiencing one or more types of cyber crime in the 12 months prior to filling out the survey, compared with just 22% of other respondents.

Figure 1. % of respondents that experienced cyber crime in the previous year



Based on the survey results, cyber crime appears to affect about 3 out of every 10 people, with 29% of respondents saying they've experienced one or more different types of cyber crime in the past 12 months. Types of cyber crime included in the survey covered a wide range of offenses, such as credit card fraud, malware/virus infections, cyber bullying, and more.

While the numbers become small when examining particular types of cyber crime, victims that are part of The Walking Breached seemed to experience slightly different types of offenses. Malware infections, credit card fraud, and SMS scams were roughly equally prevalent among victims using breached services and other survey respondents. But account takeovers – unauthorized access to email, social media, and other online services – were more prevalent among The Walking Breached. Identity theft and ransomware attacks were over twice as common among The Walking Breached than other respondents.

Victims are respondents who experienced 1 or more types of cyber crime in the 12 months prior to filling out the survey.

Figure 2. Types of cyber crime experienced by victims

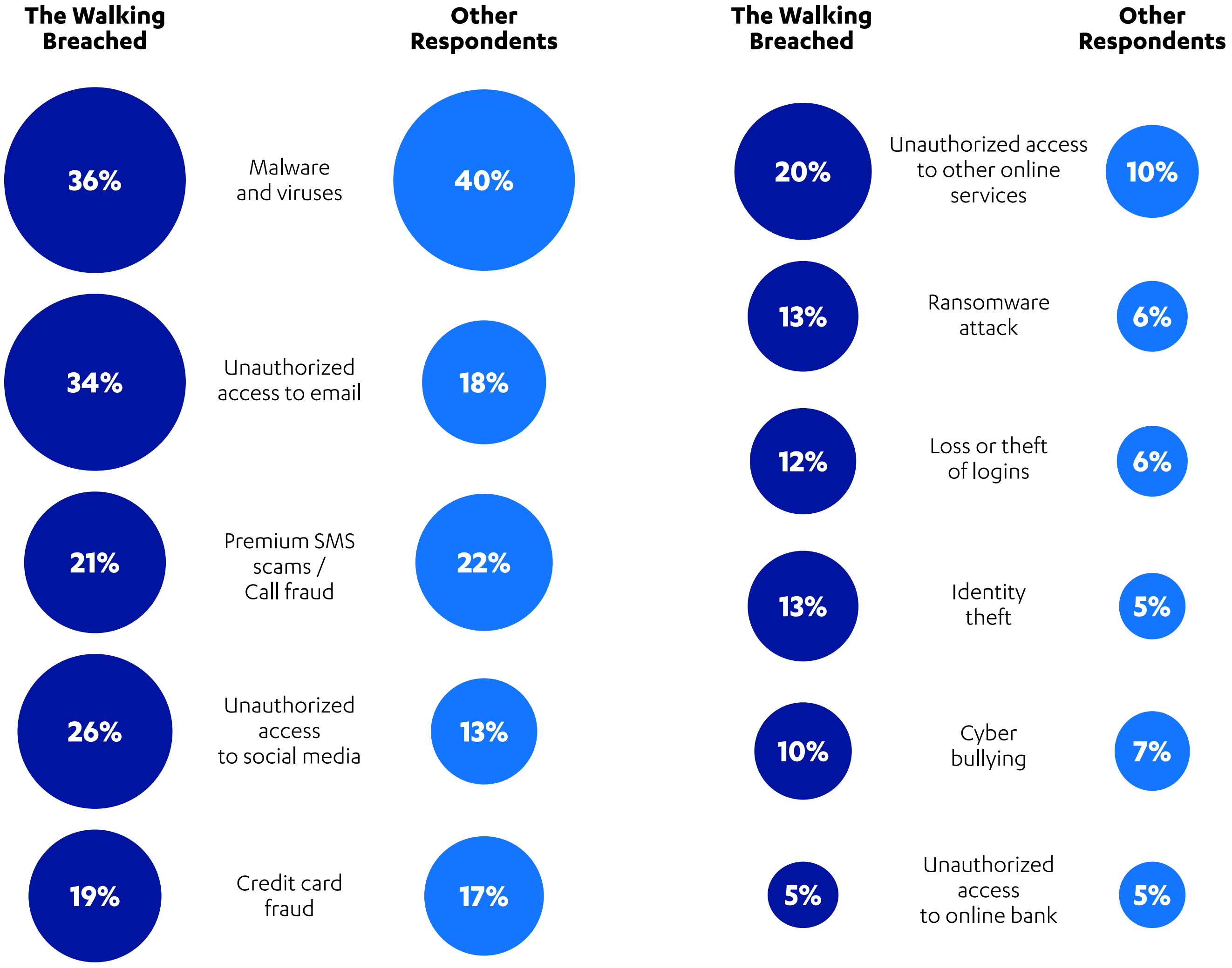
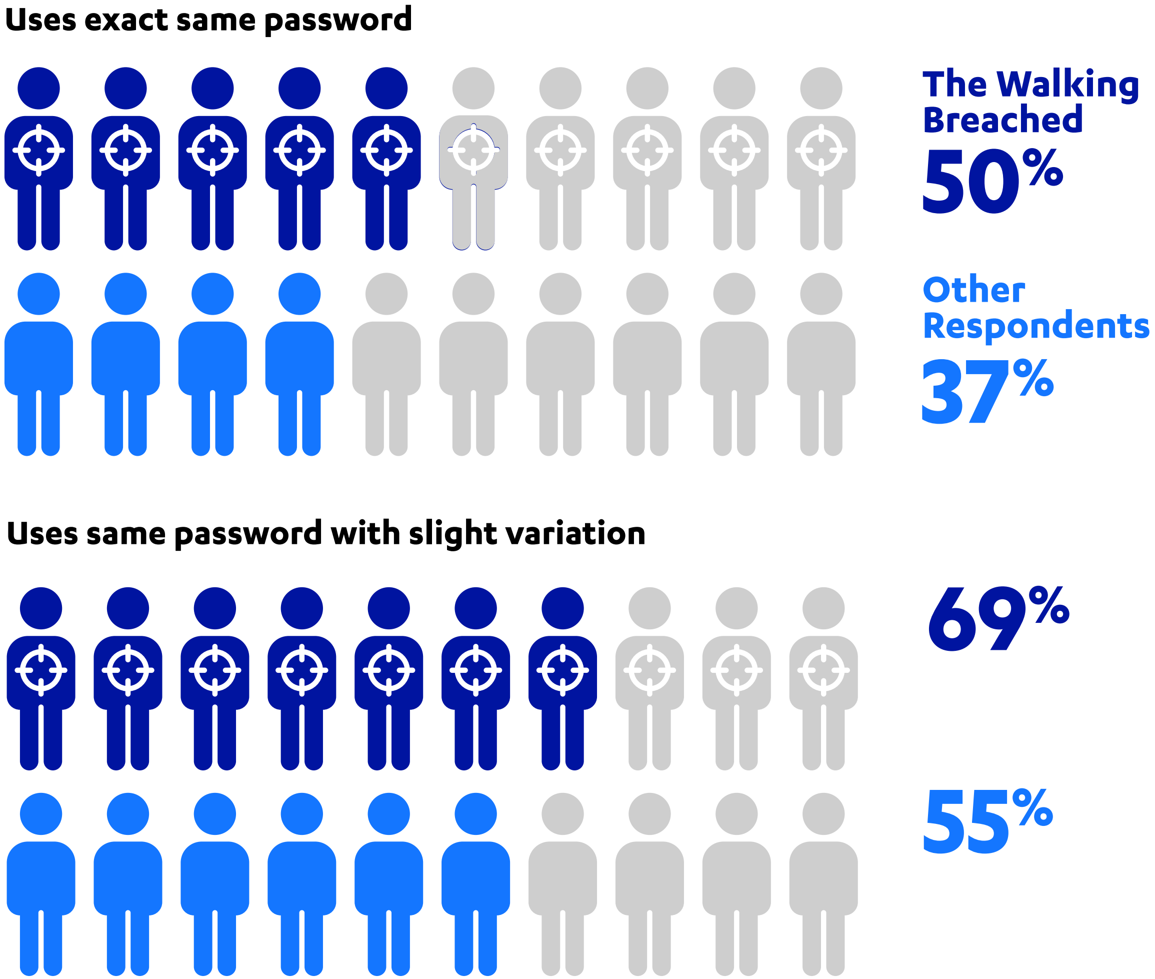
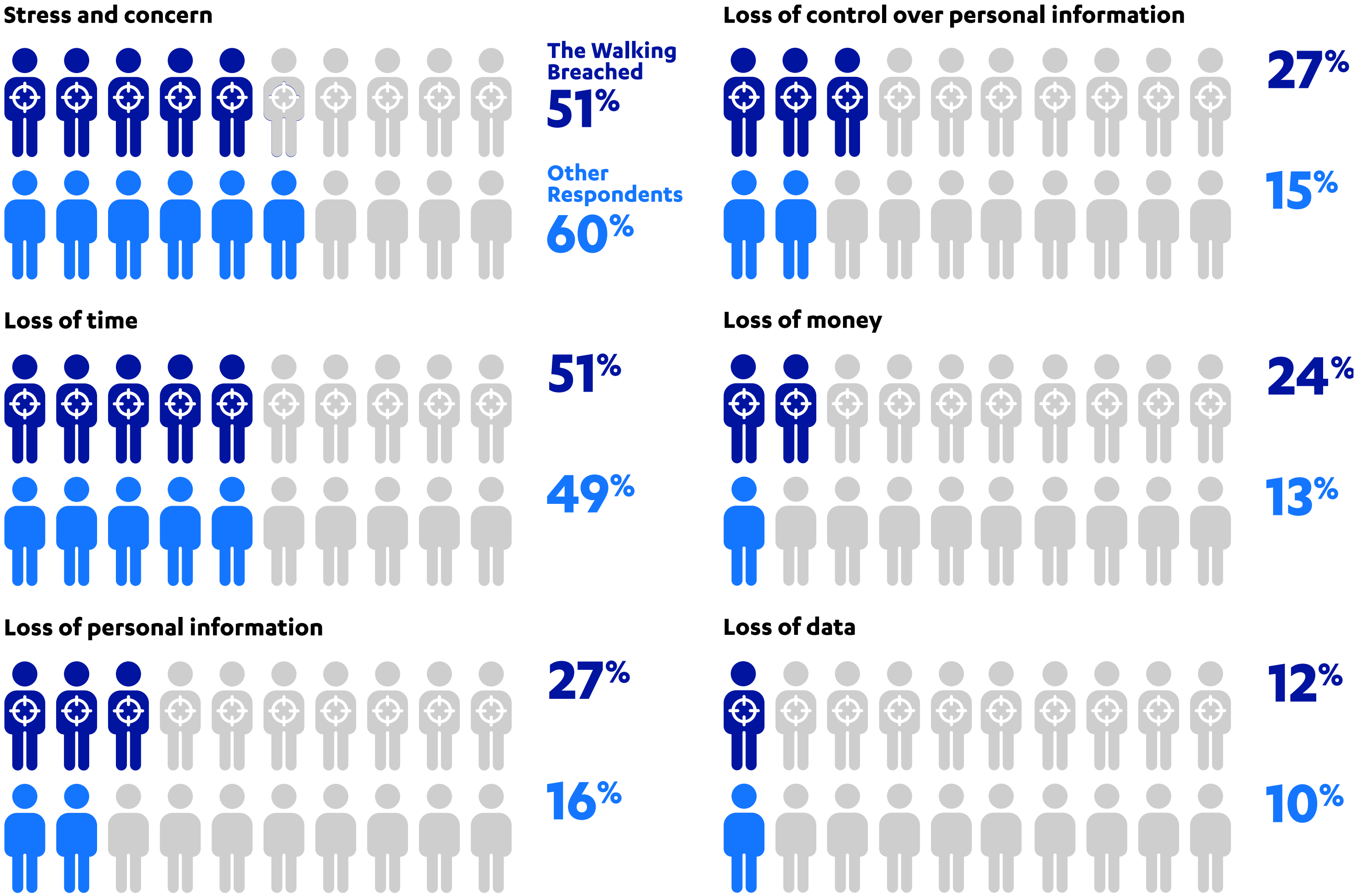


Figure 3. Password habits of cyber crime victims



Of The Walking Breached who have experienced cyber crime in the past year, half reuse exact passwords for different online services, apps, etc. And 69% - nearly 7 out of 10 – reuse passwords with slight variations. These behaviors were less common among other cyber crime victims, with 37% reusing passwords and 55% reusing passwords with slight variations.

Figure 4. Effects of cyber crime experienced by victims



Stress and concern

Loss of control over personal information

Loss of time

Loss of money

Loss of personal information

Loss of data

Cyber crime also had a slightly different impact on The Walking Breached. Stress and concern was actually less common for The Walking Breached's cyber crime victims than victims among other respondents that weren't using a breached service. However, loss of personal information, loss of control over personal information or accounts, and loss of money, were all more common among The Walking Breached, affecting about one-quarter of victims from this group. Loss of time and loss of data were nearly equally prevalent among victims from both groups.

THE WALKING BREACHED FAMILIES FACE GREATER EXPOSURE

Cyber crime was more common among survey respondents with kids than without, indicating additional challenges facing families. According to the survey, 36% of survey respondents with kids experienced some sort of cyber crime in the 12 months prior to filling out the survey, compared to 23% of respondents without kids.

People with kids experienced nearly every type of cyber crime addressed in the survey more frequently than their childless counterparts.

Figure 5. % of respondents that experienced cyber crime in the previous year

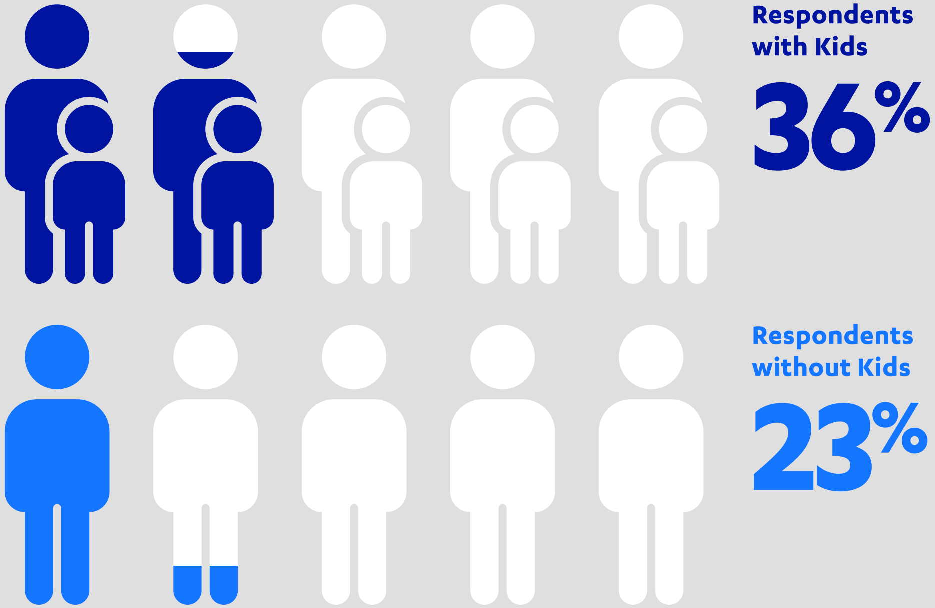
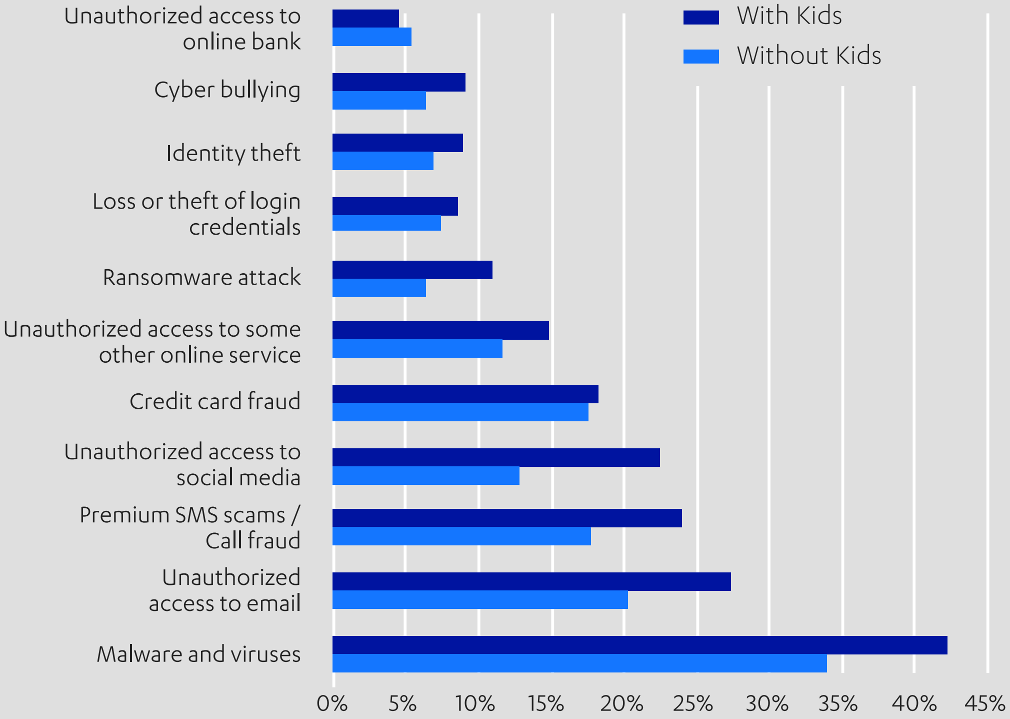


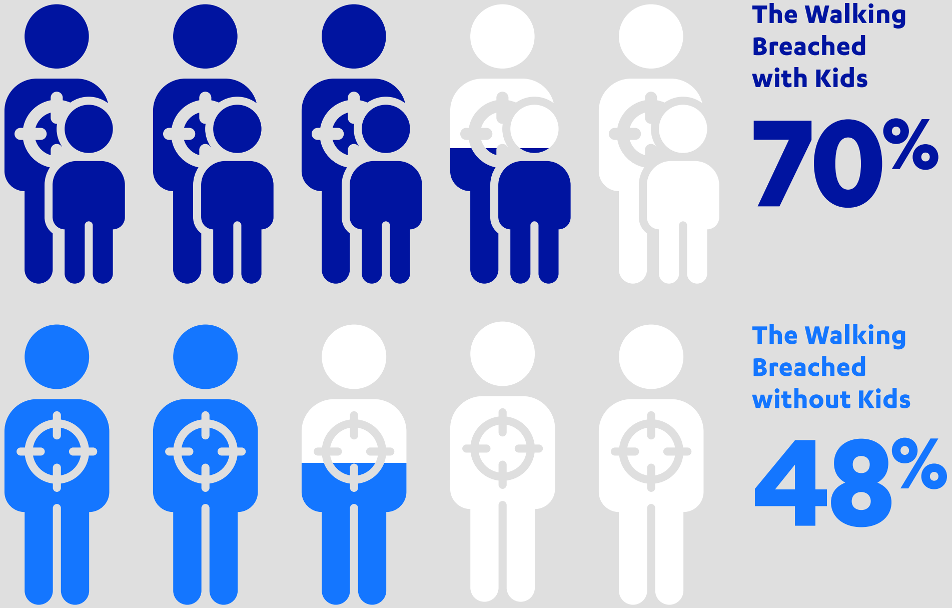
Figure 6. Types of cyber crime experienced by victims



More parents also identified themselves as one of The Walking Breached, with 22% reporting that one or more of the online services they use have been breached or hacked, compared to 15% of respondents without kids.

Notably, it seems that the security challenges faced by people with kids and The Walking Breached add up. 70% of respondents belonging to both groups (people with kids that know they're using one or more services that have been breached) reported experiencing cyber crime in the 12 months leading up to the survey, compared to 48% of The Walking Breached without kids.

Figure 7. % of respondents that experienced cyber crime in the previous year



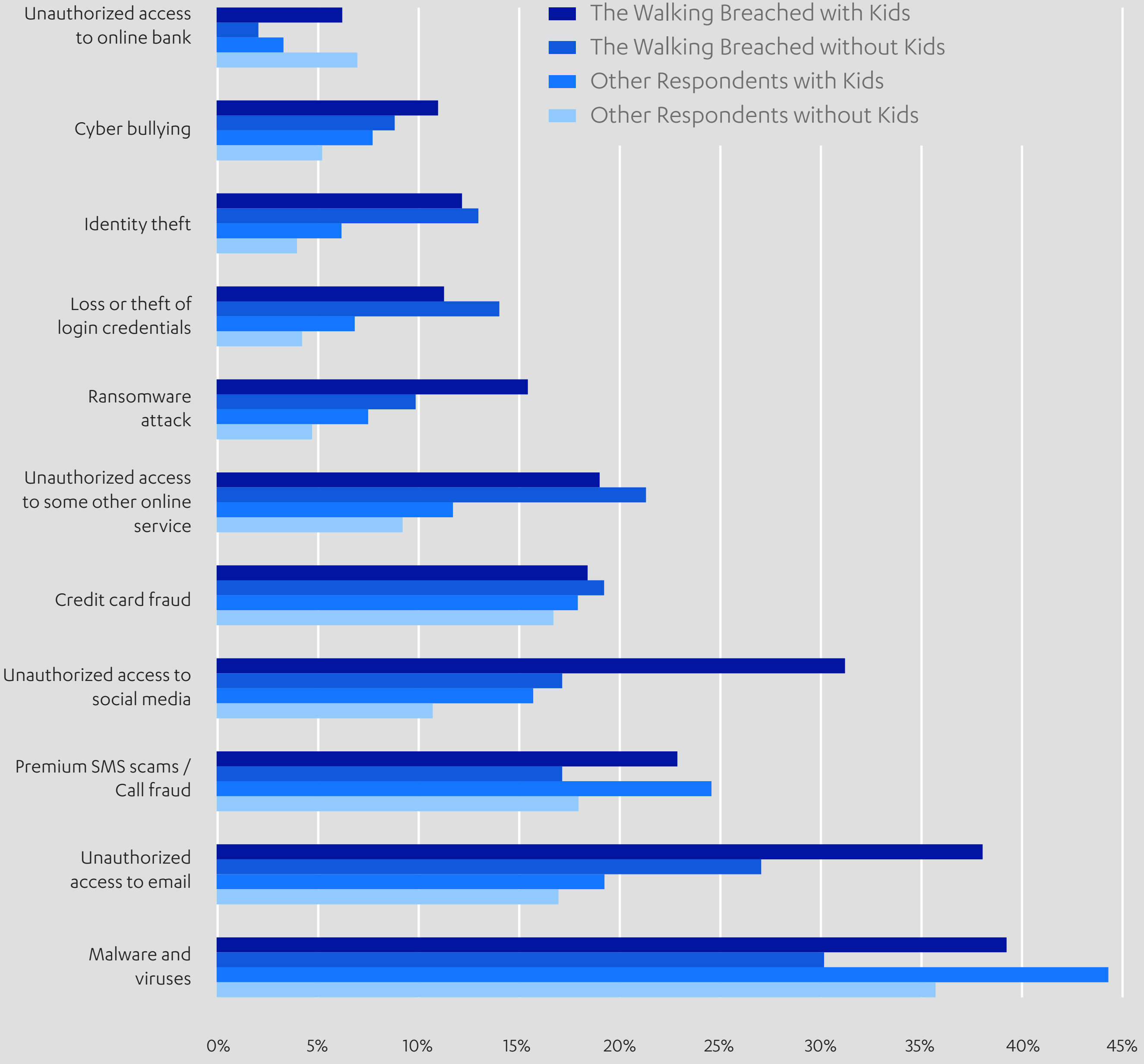
The Walking Breached families reported more occurrences of several cyber crimes than The Walking Breached singles. While the difference in overall numbers can be small in these cases, malware, SMS scams/call fraud, unauthorized access to email, bank, and social media accounts, and cyber bullying were all more common among The Walking Breached families than The Walking Breached singles.

However, malware and SMS scams/call fraud were still less common among The Walking Breached than other respondents.

It is difficult to say for certain why parents seem to experience more cyber crime. It's likely a combination of factors. However, a few possibilities include:

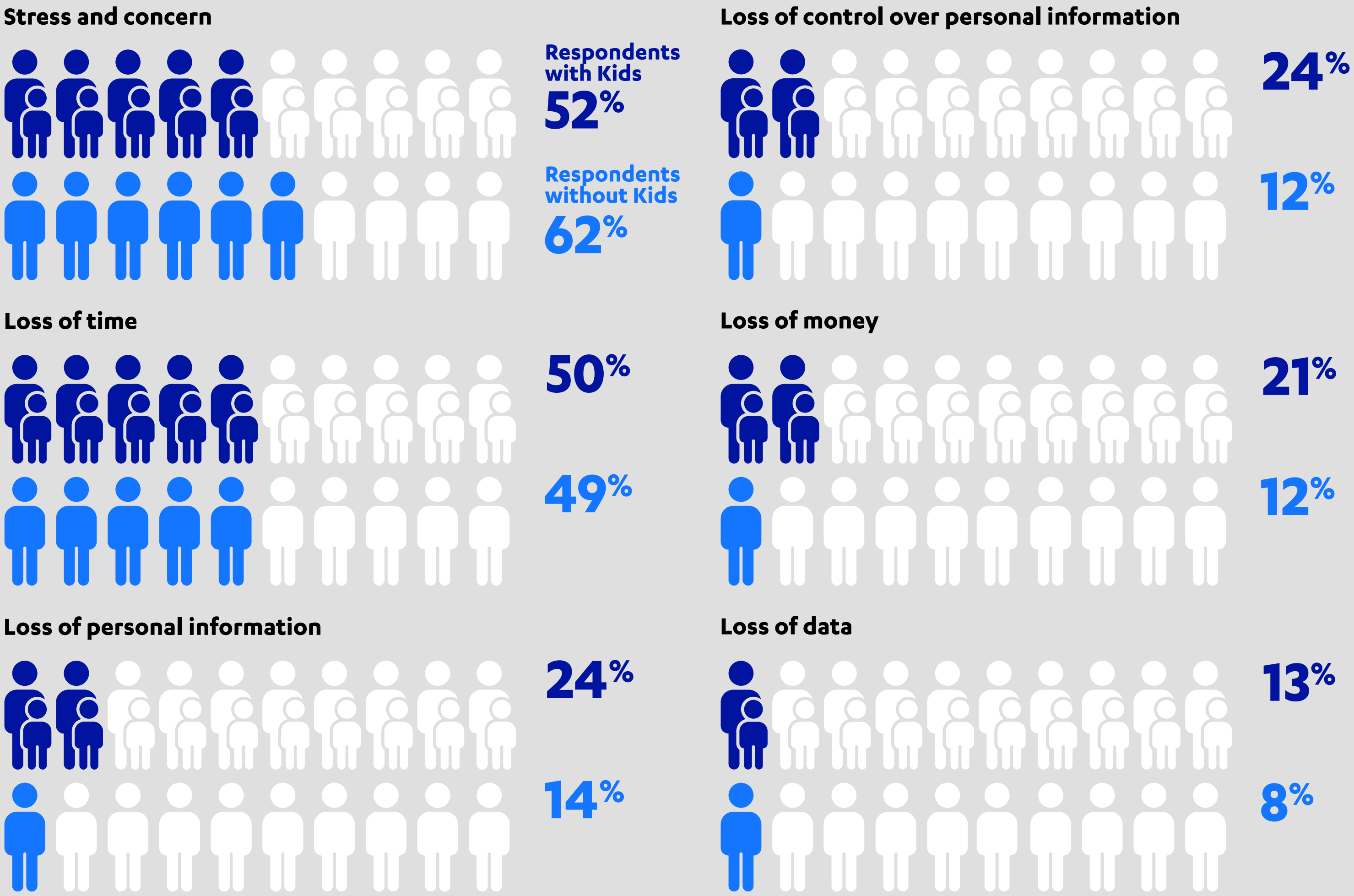
- Less time, energy, and other resources to spend on learning and implementing basic security practices.
- Responsibility for minding accounts, services, and devices on behalf children, who may not provide visibility of potential problems or follow guidance provided by parents.
- Responsibility for more accounts with more services means making more information available online, increasing the chances of exposure to various threats.

Figure 8. Types of cyber crime experienced by victims



Comparing the effects cyber crime have on respondents with kids versus without kids yields similar results to the earlier comparison between The Walking Breached and other respondents. Cyber crime victims with kids were more likely to experience loss of personal information, control over personal information or accounts, money, and data, whereas victims without kids seemed to find the experience more stressful than anything else. Loss of time was nearly equally common among the two groups.

Figure 9. Effects of cyber crime experienced by victims

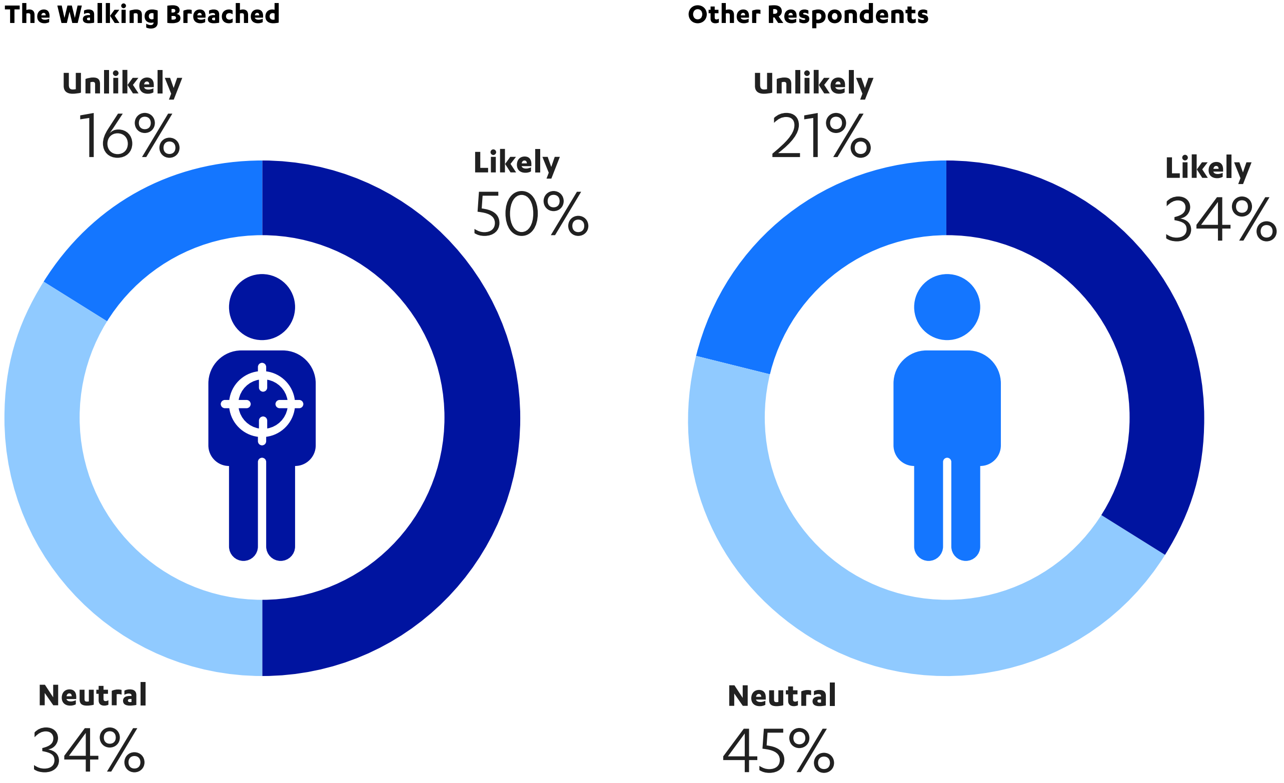


The Walking Breached also seem less confident in their security going forward, with half of them saying they were likely to experience cyber crime or identity theft in the near future, and just 16% saying it was unlikely. Only 34% of other respondents felt they were likely to become cyber crime victims in the near future. 45% expressed no feelings one way or the other.

The 2020 Verizon Data Breach Investigations Report sheds some light on why attacks on companies end up causing problems for people and families. The report found that 86% of security incidents were financially motivated, and a clear majority of victims, 58%, reported that personal data was compromised. Furthermore, organized crime was the most frequent threat actor responsible for breaches, accounting for over half of the cases, 55%, included in the report.[7]

It is beyond the scope of the survey to determine what threat actors were responsible for the cyber crime experienced by participants. However, given the substantial role organized crime and monetary gains plays in acquiring people's personal data from organizations, it's important to understand how cyber criminals profit from this information.

Figure 10. % of respondents who feel they're likely to become a cyber crime victim in the future

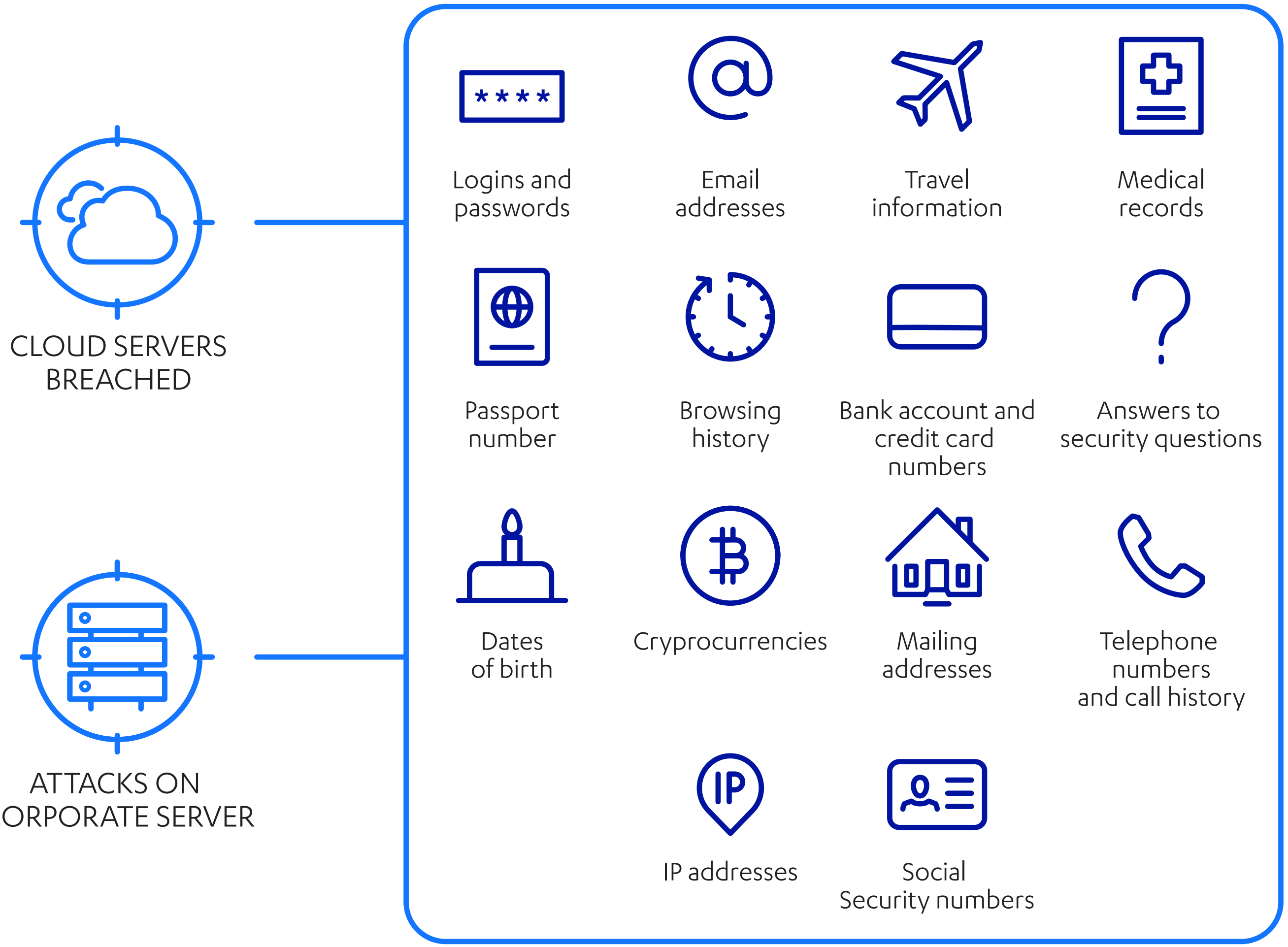


[7] 2020 Data Breach Investigations Report https://enterprise.verizon.com/resources/executivebriefs/2020-dbir-executive-brief.pdf

HOW BREACHED DATA FUELS CYBER CRIME

While survey data does not establish a causal relationship between breached services and people's experience of cyber crime and/or similar phenomena, existing research and real-world cases can help shed some light on the connection between the two.

Figure 11. Personal information at risk



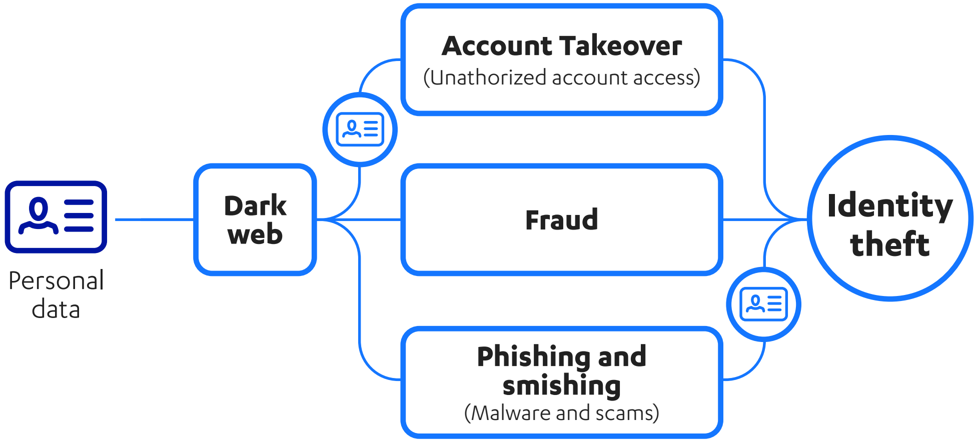
Stolen data, like any stolen object, presents opportunities and risks for the criminal. But monetizing the theft is made much easier by the illegal industries that have developed to monetize breached data. This shadow industry fuels the risks of fraud and other sorts of identity crimes for people who have had their private information taken from a third party.

> Once personally identifiable information is stolen, one of the easiest ways for attackers to profit is by selling it to other criminals either directly or using underground or dark web sites.

Once personally identifiable information is stolen, one of the easiest ways for attackers to profit is by selling it to other criminals either directly or using underground or dark web sites. A 2020 report found that 15 billion stolen credentials, including 5 billion unique credentials from 100,000 data breaches, were for sale on the dark web.[8] While most credentials are available for free, superscription logins, such as those for Netflix, Uber and Fortnite, can go for about $10, while payment accounts, such as Paypal, range from $50 to $3,400 and hotel loyalty programs fetch about $1500.[9]

For about a decade, criminals who have obtained stolen credentials have used credential stuffing to try them out on tens of thousands of accounts with very little effort. The Open Web Application Security Project defines credential stuffing as when “large numbers of spilled credentials are automatically entered into websites until they are potentially matched to an existing account, which the attacker can then hijack for their own purposes.”[10] Several credential stuffing tools are available online. Some are so advanced that they incorporate tools that make the login requests appear to become different IP addresses and browsers to defeat site security. Some of these tools even work with platforms built to overcome Captchas that require the requesters prove that they are human.[11] Because some people reuse pairs of logins and passwords on multiple services, multiple accounts can be targeted from just one pair of breached credentials.

Figure 12. How criminals use stolen data



A recent smishing attack discovered in January of 2021 employed a familiar tactic to con users into handing over credentials by pretending to be the payment company PayPal asking the user to correct an error with an account. “We’ve permanently limited your account, please click link below to verify,” the message read. Given that PayPal has nearly 300 million users worldwide, a scammer can assume many of any random users it targets would be likely to have a PayPal account and thus prone to fall for this scam.[12] However, these sorts of attacks become more potent the more information that attacker has on the target.

[8] New Dark Web Audit Reveals 15 Billion Stolen Logins From 100,000 Breaches https://www.forbes.com/sites/daveywinder/2020/07/08/new-dark-web-audit-reveals-15-billion-stolen-logins-from-100000-breaches-passwords-hackers-cybercrime/?sh=35d892a2180f
[9] How Much is Your Data Worth on the Dark Web? https://securityboulevard.com/2019/11/how-much-is-your-data-worth-on-the-dark-web/
[10] Credential stuffing https://owasp.org/www-community/attacks/Credential_stuffing
[11] Hacker Lexicon: What is Credential Stuffing? https://www.wired.com/story/what-is-credential-stuffing/
[12] Beware: PayPal phishing texts state your account is ‘limited’ https://www.bleepingcomputer.com/news/security/beware-paypal-phishing-texts-state-your-account-is-limited/

Once an account is cracked, the criminal can takeover that account or use it as a stepping stone to identity theft. In 2019 alone, identity theft cost US consumers more than $3.5 billion, according to reports to the Federal Trade Commission (FTC). And even though 13 million Americans experienced identity theft that year, the crime rarely looks exactly same for any two victims.[13] The definition of what exactly qualifies as identity theft continues to expand as the ways private information is captured and stored evolves.

The credit reporting company Experian has identified 20 forms of identity theft, including debit card fraud or credit card fraud, online shopping fraud, senior identity theft and scams, child identity theft, tax identity theft, biometric ID theft, medical identity theft, mortgage fraud, and internet of things identity fraud.[14] The FTC noted that credit card fraud was by far the most common form of identity theft reported in 2019, followed by the vague "other" forms of identity theft, loan or lease fraud, phone or utilities fraud, bank fraud, employment or tax fraud, and government documents or benefits fraud.

Another reason why identity theft is such an expansive category is that any time a new way to exploit individuals' identities appears, criminals quickly try to take advantage of it. In the spring of 2020, the United States expanded unemployment benefits by $600 to respond to economic impact of the Covid-19 pandemic. USA TODAY reports scammers discovered that some states had few safeguards to prevent fraudulent unemployment claims. Using the identities of Americans they found online, criminals as far away as West Africa applied for the benefits and used so-called "money mules" to capture the gains taken by denying victims legitimate claims or by issuing a fraudulent claim in an unsuspecting individual's name.[15] A report from the US Department of Labor's Office of the Inspector General issued in November of 2020 found that schemes targeting pandemic unemployment benefits resulted in $36 billion in losses.[16]

"Simply selling access to some types of accounts can be profitable. Cyber criminals reportedly make millions of dollars selling access to hacked accounts for online games that feature valuable in-game add-ons, such as skins in Fortnite.[17] According to a survey from Akamai and DreamHack, 8 out of 10 regular esport contestants have seen hacked accounts and assets being sold online."[18]

Looking beyond identity theft, one can see even more types of crime enabled by stolen data. The recent hack of a Finnish psychotherapy center demonstrates how leaked data stolen from companies can have severe repercussions for affected individuals. In late 2020, an attacker leaked private information stolen from a 2018 attack on Finland's Vastaamo clinic, and then emailed more than 40,000 customers, including underaged patients, to extort payment in exchange for not posting their information online.[19]

> In late 2020, an attacker leaked private information stolen from a 2018 attack on Finland's Vastaamo clinic, and then emailed more than 40,000 customers, including underaged patients, to extort payment in exchange for not posting their information online.

The theft of medical histories is an extreme example of the dangers people face from data breaches.

[13] Identity Fraud Losses Increase 15 Percent as Consumer Out-of-Pocket Costs More Than Double, According to 2020 Identity Fraud Report https://www.javelinstrategy.com/press-release/identity-fraud-losses-increase-15-percent-consumer-out-pocket-costs-more-double
[14] The Many Different Forms of Identity Theft https://www.experian.com/blogs/ask-experian/20-types-of-identity-theft-and-fraud/
[15] How scammers siphoned $36B in fraudulent unemployment payments from US https://www.usatoday.com/in-depth/news/investigations/2020/12/30/unemployment-fraud-how-international-scammers-took-36-b-us/3960263001/
[16] Scammers have taken $36 billion in fraudulent unemployment payments from American workers https://www.cnbc.com/2021/01/05/scammers-have-taken-36-billion-in-fraudulent-unemployment-payments-.html
[17] https://threatpost.com/stolen-fortnite-accounts-earn-hackers-millions/158796/
[18] https://www.esportshacked.com/post/every-other-gamer-has-been-hacked-are-you-one-of-them
[19] Hacker seeks to extort Finnish mental health patients after data breach https://www.politico.eu/article/cybercriminal-extorts-finnish-therapy-patients-in-shocking-attack-ransomware-blackmail-vastaamo/

SECURITY ADVICE FOR PROTECTING PERSONAL DATA

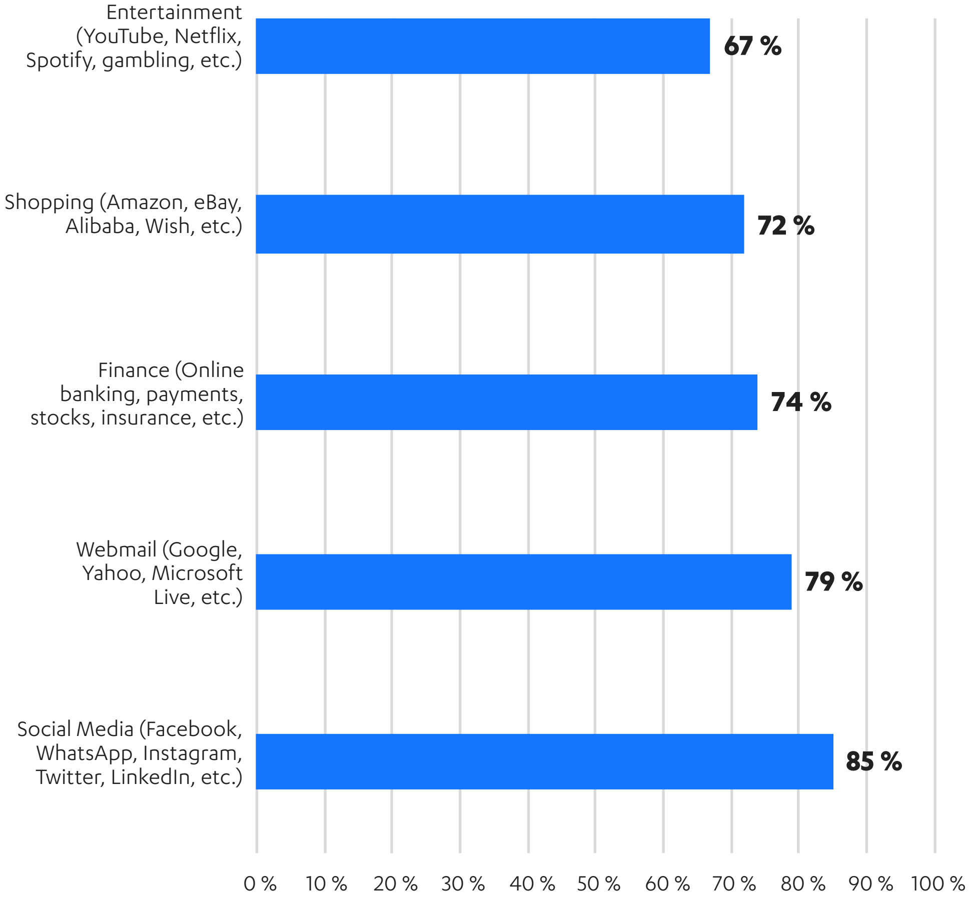
Internet users are stuck between a proverbial "rock" and a "hard place."

The rock is that online services have become embedded in our lives and almost a perquisite for participating in modern society. The five most popular types of online services are used by more the two-thirds of people who use the internet. And three out of four people use the internet to manage at least some of their finances online. Many businesses only exist as online services, and increasingly essential services from banks to governments to grocery stores are driving customers to websites in order to complete crucial transactions.

The hard place is that consumers have to rely on the online services they deal with to protect that data. A breach of any one service can put the consumers who do not employ strong account security practices could spark an escalating series of crimes that could end up threatening their identity. Meanwhile, the financial incentives for criminals to breach and monetize stolen data show no sign of dissipating.

Avoiding becoming a member of The Walking Breached starts with basic password security—using unique, too-strong-to-remember passwords for all important accounts and storing those passwords in a trusted password manager or locker. More than half of online services still rely on passwords as their top form of authentication.[20] For the foreseeable future, people need to recognize their first, and perhaps best, defense against the cyber crime fueled by data breaches is securing passwords.

Figure 13. Online services used by respondents

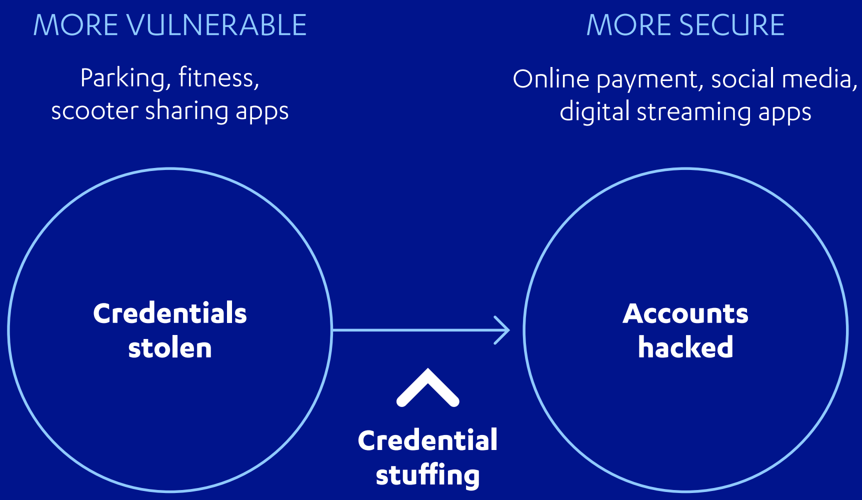


[20] global-fraud-report-2018-infographic.pdf https://www.experian.com/content/dam/marketing/na/assets/im/decision-analytics/infographics/global-fraud-report-2018-infographic.pdf

Here are basic steps people can take to minimize cyber risks to secure their accounts and their identities.

1. Make the effort to use strong, unique passwords

According to F-Secure's survey, 39% of people reuse the exact same passwords on various online online services, apps, etc. 57% reuse passwords with slight variations. Criminals are well aware of this behavior, which is why they often will target sites with less security to steal credentials that can be used to crack accounts for servicesthat are well-protected against breaches.


MORE VULNERABLE
Parking, fitness, scooter sharing apps
MORE SECURE
Online payment, social media, digital streaming apps
Credentials stolen
Accounts hacked
Credential stuffing

People's lack of diligence makes sense considering how many accounts they use: survey respondents have an average of 18.1 unique accounts. But the number may be much higher, given that accounts a user created decades ago may still be active. Remembering dozens of too-strong-to-remember passwords is a challenge that didn't have a simple solution in 2002, so re-using passwords made likely made sense to many. However, this is a security sacrifice people shouldn't continue to make in 2021. Password lockers that encrypt and store as many unique, too-strong-to-remember passwords are widely available. Cyber security experts consistently recommend this essential tool, though only 3 in 10 survey respondents, 30%, reported using them.

2. Do not volunteer private information

More than 8 in 10, 81%, of F-Secure's survey respondents said they avoid filling certain pieces of data in online services. That sort of suspicion needs to be the default position when asked for private information whether it's through email, text or a voice call. The default position is to not share any private information unless using a service directly through the service's app or website, and even then only share what is necessary.

3. Whenever possible, go beyond passwords

Whenever possible—especially on email and financial accounts—use two-factor authentication that employs an additional way to secure an account through some sort of hardware. USB-A and USB-C are good second factors for advanced or business users. A passcode-protected mobile device using an authenticator app is a good choice. Using SMS or email as a second factor is not ideal but is much better than nothing.

5. Monitor the integrity of personal data

The time to act when information ends up on the dark web is immediately. While most law-abiding people are unlikely to spend much time combing through the web's dimmest crevasses, various identity protection and monitoring services are available that promise to do so. There are also free web-based tools people can use on their own to check if private information has been leaked online. Only 2 of 10 of F-Secure's survey respondents, 18%, have tried such a tool, so the people who utilize these tools have an advantage over the rest.

4. Stay on top of accounts

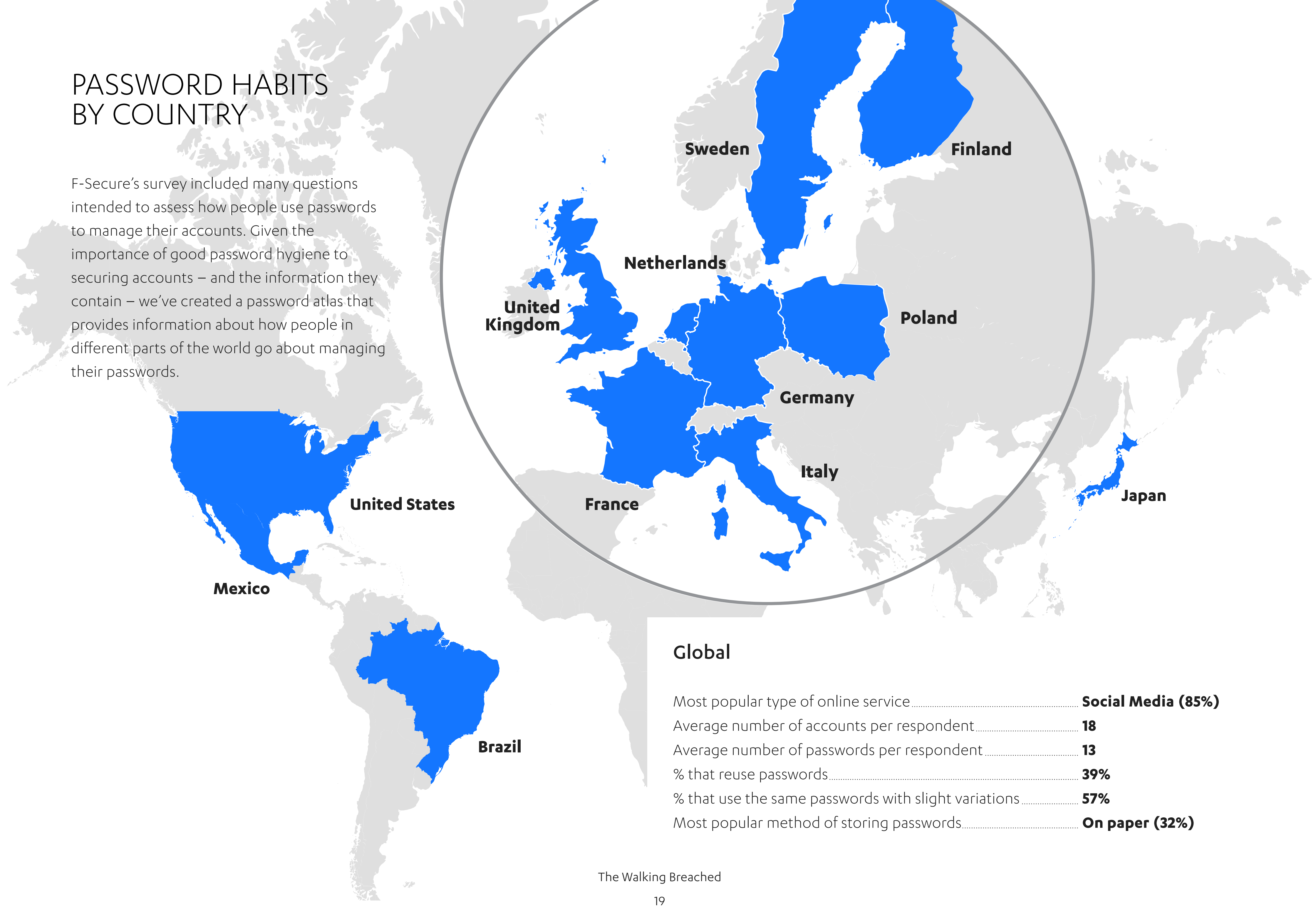
Continually check credit card statements and activate any alerts financial institutions offer in regards to suspicious activity. As soon as any news of relevant breach appears, sign up for a "credit freeze" that prevents new accounts or credit lines from being opened.

6. Don't underestimate exposure to threats

Survey respondents reported an average of 18 accounts. However, given the age of the internet and the ubiquity of free online services, it's likely that many of us have accounts that we opened, but stopped using and forgot about. Accounts can be created quickly and casually, with user data saved on a browser available to populate a form with a click. Exposure can be created without even registering for a new service. Critical personal data—including addresses, emails, and phone and credit card numbers—may be stored on the systems of any service a person uses. Given the growth of these services and their import to consumers' lives, this exposure will only grow, making protecting one's data even more crucial to preventing cyber crime.

PASSWORD HABITS BY COUNTRY

F-Secure's survey included many questions intended to assess how people use passwords to manage their accounts. Given the importance of good password hygiene to securing accounts – and the information they contain – we've created a password atlas that provides information about how people in different parts of the world go about managing their passwords.



Global

Most popular type of online service	**Social Media (85%)**
Average number of accounts per respondent	**18**
Average number of passwords per respondent	**13**
% that reuse passwords	**39%**
% that use the same passwords with slight variations	**57%**
Most popular method of storing passwords	**On paper (32%)**

Brazil

Most popular type of online service	**Social Media (97%)**
Average number of accounts per respondent	**17**
Average number of passwords per respondent	**11**
% that reuse passwords	**43%**
% that use the same passwords with slight variations	**68%**
Most popular method of storing passwords	**On paper (37%)**

Finland

Most popular type of online service	**Webmail (91%)**
Average number of accounts per respondent	**26**
Average number of passwords per respondent	**18**
% that reuse passwords	**35%**
% that use the same passwords with slight variations	**60%**
Most popular method of storing passwords	**I do not store them (35%)**

France

Most popular type of online service	**Social Media and Shopping (80%)**
Average number of accounts per respondent	**11**
Average number of passwords per respondent	**10**
% that reuse passwords	**55%**
% that use the same passwords with slight variations	**72%**
Most popular method of storing passwords	**Use "Forgot password" to access accounts (35%)**

Germany

Most popular type of online service	**Shopping (83%)**
Average number of accounts per respondent	**14**
Average number of passwords per respondent	**12**
% that reuse passwords	**37%**
% that use the same passwords with slight variations	**50%**
Most popular method of storing passwords	**On paper (36%)**

Italy

Most popular type of online service	**Social Media (92%)**
Average number of accounts per respondent	**19**
Average number of passwords per respondent	**12**
% that reuse passwords	**38%**
% that use the same passwords with slight variations	**54%**
Most popular method of storing passwords	**On paper (36%)**

Japan

Most popular type of online service	**Shopping (85%)**
Average number of accounts per respondent	**13**
Average number of passwords per respondent	**10**
% that reuse passwords	**33%**
% that use the same passwords with slight variations	**52%**
Most popular method of storing passwords	**On paper (46%)**

Mexico

Most popular type of online service	**Social Media (97%)**
Average number of accounts per respondent	**13**
Average number of passwords per respondent	**9**
% that reuse passwords	**32%**
% that use the same passwords with slight variations	**58%**
Most popular method of storing passwords	**Use password manager (37%)**

Netherlands

Most popular type of online service	**Social Media (88%)**
Average number of accounts per respondent	**20**
Average number of passwords per respondent	**13**
% that reuse passwords	**47%**
% that use the same passwords with slight variations	**60%**
Most popular method of storing passwords	**Use password manager (36%)**

Poland

Most popular type of online service	**Social Media (94%)**
Average number of accounts per respondent	**12**
Average number of passwords per respondent	**9**
% that reuse passwords	**40%**
% that use the same passwords with slight variations	**56%**
Most popular method of storing passwords	**On paper (36%)**

Sweden

Most popular type of online service	**Webmail (86%)**
Average number of accounts per respondent	**26**
Average number of passwords per respondent	**16**
% that reuse passwords	**45%**
% that use the same passwords with slight variations	**55%**
Most popular method of storing passwords	**I do not store them (31%)**

United Kingdom

Most popular type of online service	**Shopping (81%)**
Average number of accounts per respondent	**22**
Average number of passwords per respondent	**15**
% that reuse passwords	**29%**
% that use the same passwords with slight variations	**47%**
Most popular method of storing passwords	**Use password manager (36%)**

United States

Most popular type of online service	**Webmail (85%)**
Average number of accounts per respondent	**22**
Average number of passwords per respondent	**15**
% that reuse passwords	**36%**
% that use the same passwords with slight variations	**49%**
Most popular method of storing passwords	**Store on paper (32%)**

CONCLUSION: RESTORING TRUST AND RELIABILITY TO THE INTERNET

This report shines a light on the often-obscure relationship between data breaches and consumer-oriented cyber crime. Survey data shows the impact data breaches can have on individuals using services compromised by cyber attacks. The Walking Breached, as described in this report, clearly experience higher rates of cyber crime than other people, and suffer slightly different effects. Having kids acts as a multiplier for these effects, highlighting the security challenges facing today's parents.

While the survey data does not establish a causal relationship between data breaches and the plight of The Walking Breached, an examination of existing research and real-world cases provide insights into how this works. Stolen data can lead directly to fraud or accounts opened up in a victim's name—or it can make all sorts of other attacks, especially phishing and smishing, more effective. These activities are supported by a variety of businesses brokering in stolen information, making it easier for cyber criminals to obtain and exploit people's personal information.

Businesses are in a constant struggle to secure their networks and the data they store. Consumers, however, have to recognize that no one will ever care more about their data than they will. While trusted internet security can protect people from many cyber threats, it cannot prevent attacks that trick people into offering private information or credentials. Nor can it prevent fraud that's being committed using breached data that a person may not even know has been stolen. This does not mean people should abandon internet security software. Rather, they should educate themselves and make use of new technologies that can empower them to manage their online lives safely and responsibly.

> While trusted internet security can protect people from many cyber threats, it cannot prevent attacks that trick people into offering private information or credentials.

> People with more online accounts using more services leave more information on the internet. Anyone that finds themselves increasing their use of online services should ensure they're taking security measures to prevent cyber criminals from turning their digital information against them.

This rings especially true for consumers that are actively using new online services and technologies. People with more online accounts using more services leave more information on the internet. Anyone that finds themselves increasing their use of online services should ensure they're taking security measures to prevent cyber criminals from turning their digital information against them. As mentioned at the beginning of this report, digitization has proven to be a transformative force for both what people do online, and how they need to protect themselves. This is unlikely to change in the foreseeable future, and one can already foresee new, transformative technologies on the horizon.

That last decade has seen a radical transformation in how companies store and access their data, with information migrating from on-premise company networks to the cloud. A 2019 O'Reilly study found that 88% of organizations use some form of cloud infrastructure, and 45% expected to move three quarters or more of their applications to the cloud over the next year.[21] The cloud offers organizations cost savings and the promise of better security—but it isn't a cure-all. While 75% of organizations reported they believe that public clouds were at least somewhat more secure than their on-premise environments, according to the Oracle and KPMG Cloud Threat Report 2020,51% of the same organizations reported that they have discovered some sort of data loss and 92% reported that they have at least a moderate "cloud security readiness gap."[22]

Many businesses who utilize the cloud are moving to a Zero Trust architecture. In these environments, users who remotely connect to network are identified based on their identity and location.[23] This strategy prevents or minimizes breaches, and it also offers a way forward when it comes to securing consumers' accounts. Elements of a Zero Trust architecture can give users of online services better identity control, without putting an increased burden on the users with messy kludges, such as forcing users to continually re-log after an arbitrary amount of time.

Biometrics, such as facial recognition and thumbprints, also offer alternatives to the failings of passwords. These credentials would be much more difficult to steal or spoof, but they also present a conundrum for if and when they are successfully hacked. One can change a stolen password. It is much more difficult to change a face.

Technology can change quickly. People's habit and security needs, however, do not change as quickly. For this reason, challenges to securing one's personal information will likely persist in the foreseeable future.

[21] Cloud Adoption in 2020 https://www.oreilly.com/radar/cloud-adoption-in-2020/
[22] Oracle and KPMG Cloud Threat Report 2020 https://www.oracle.com/a/ocom/docs/cloud/oracle-cloud-threat-report-2020.pdf
[23] ICS security evolves as network perimeter dissolves https://blog.f-secure.com/ics-security-evolves-network-perimeter-dissolves/

ABOUT F-SECURE

Nobody has better visibility into real-life cyber attacks than F-Secure. We're closing the gap between detection and response, utilizing the unmatched threat intelligence of hundreds of our industry's best technical consultants, millions of devices running our award-winning software, and ceaseless innovations in artificial intelligence. Top banks, airlines, and enterprises trust our commitment to beating the world's most potent threats.

Together with our network of the top channel partners and over 200 service providers, we're on a mission to make sure everyone has the enterprise-grade cyber security we all need. Founded in 1988, F-Secure is listed on the NASDAQ OMX Helsinki Ltd.

f-secure.com | twitter.com/fsecure | www.linkedin.com/company/f-secure-corporation