IS IDENTITY THEFT THE CYBER CRIME WE FEAR MOST?

A look at consumer views on identity theft and cyber crime

F-Secure

CONTENTS

Introduction 3
The Risks 4
Identity Theft Makes Cyber Crime Real 6
Consumer Experiences and Worries.....7
Contrasting Men and Women 11
Conclusion.....15

INTRODUCTION

Does it ever feel as if there's a new data breach every day?

This might be because statistically, there is.

Between January of 2005 and October of 2019, Privacy Rights Clearinghouse recorded 9,705 data breaches.[1] That's an average of 1.8 a day.

Obviously, the press can't cover every instance of private data being stolen or exposed. But the examples that do make headlines seem to affect ever-increasing millions of users and reach into every corner of consumers' financial lives.

The breach that woke many consumers up to the dangers that come from the digitization of our lives involved Equifax, one of the largest credit-reporting agencies in the world. In 2017, about half the population of the United States—approximately 150 million Americans—found out their private data had been compromised, resulting in a settlement with regulators that could cost the company $700 million.[2]

The next year, hotelier Marriot revealed a breach that affected almost 400 million customers, potentially revealing payment information, names, mailing addresses, phone numbers, email addresses and passport numbers.[3]

Before the first month of 2019 ended, news of one of the biggest data breaches ever spread around the world. Cyber security expert Troy Hunt uploaded 773 million combinations of emails and passwords to his Have I Been Pwned website.[4]

In the last twelve months alone, a hacker gained access to 100 million Capital One credit card applications and accounts,[5] Facebook suffered several breaches,[6] and 2.5 million disaster victims had private information leaked by the U.S.'s Federal Emergency Management Agency.[7]

As 2020 began, Microsoft was cleaning up an "enormous security loophole" that left customer service and support records from about 250 million customers accessible to anyone with web access.[8]

What do criminals get access to when they take control of our data?

Anything they can—from stealing our passwords to accessing our critical accounts to taking over our identities.

1 Privacy Rights Clearinghouse: Data Breaches https://privacyrights.org/data-breaches
2 Equifax Breach Affected 147 Million, but Most Sit Out Settlement https://www.nytimes.com/2020/01/22/business/equifax-breach-settlement.html
3 Marriott CEO Reveals New Details About Mega Breach https://www.forbes.com/sites/kateoflahertyuk/2019/03/11/marriott-ceo-reveals-new-details-about-mega-breach/
4 ';--have i been pwned? https://haveibeenpwned.com
5 A hacker gained access to 100 million Capital One credit card applications and accounts https://www.cnn.com/2019/07/29/business/capital-one-data-breach/index.html
6 Unsecured Facebook Databases Leak Data Of 419 Million Users https://www.forbes.com/sites/daveywinder/2019/09/05/facebook-security-snafu-exposes-419-million-user-phone-numbers
7 Hack Brief: FEMA Leaked the Data of 2.3 Million Disaster Survivors https://www.wired.com/story/fema-leaked-the-data-2-million-disaster-survivors/
8 Microsoft accidently exposed 250 million customer service records https://finance.yahoo.com/news/2020-01-22-microsoft-database-exposure.html

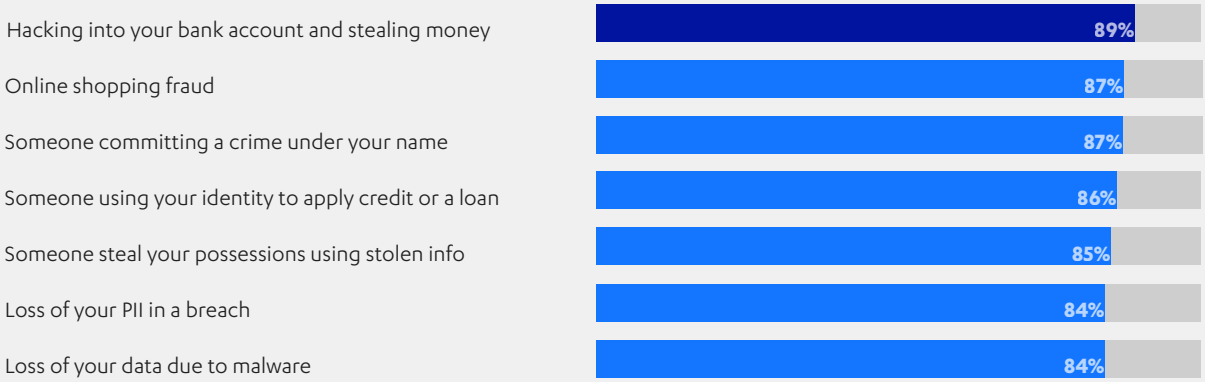
THE RISKS

The average internet user has dozens of passwords for online accounts and even more accounts with personally identifiable information tied to credit cards and other services. A shocking eight in ten consumers reuse passwords on multiple services, a behavior that increases the risks of account compromises significantly.[9]

The sense that our digital data could be used to undermine our identities abounds—possibly because consumers understand that it isn't possible to secure our data everywhere it is stored.

An F-Secure survey conducted in nine countries found that nearly nine in ten consumers are at least somewhat worried about the multiple online risks that occur when our devices, accounts, and data are not properly secured.

HOW WORRIED ARE YOU ABOUT THE FOLLOWING ONLINE THREATS?

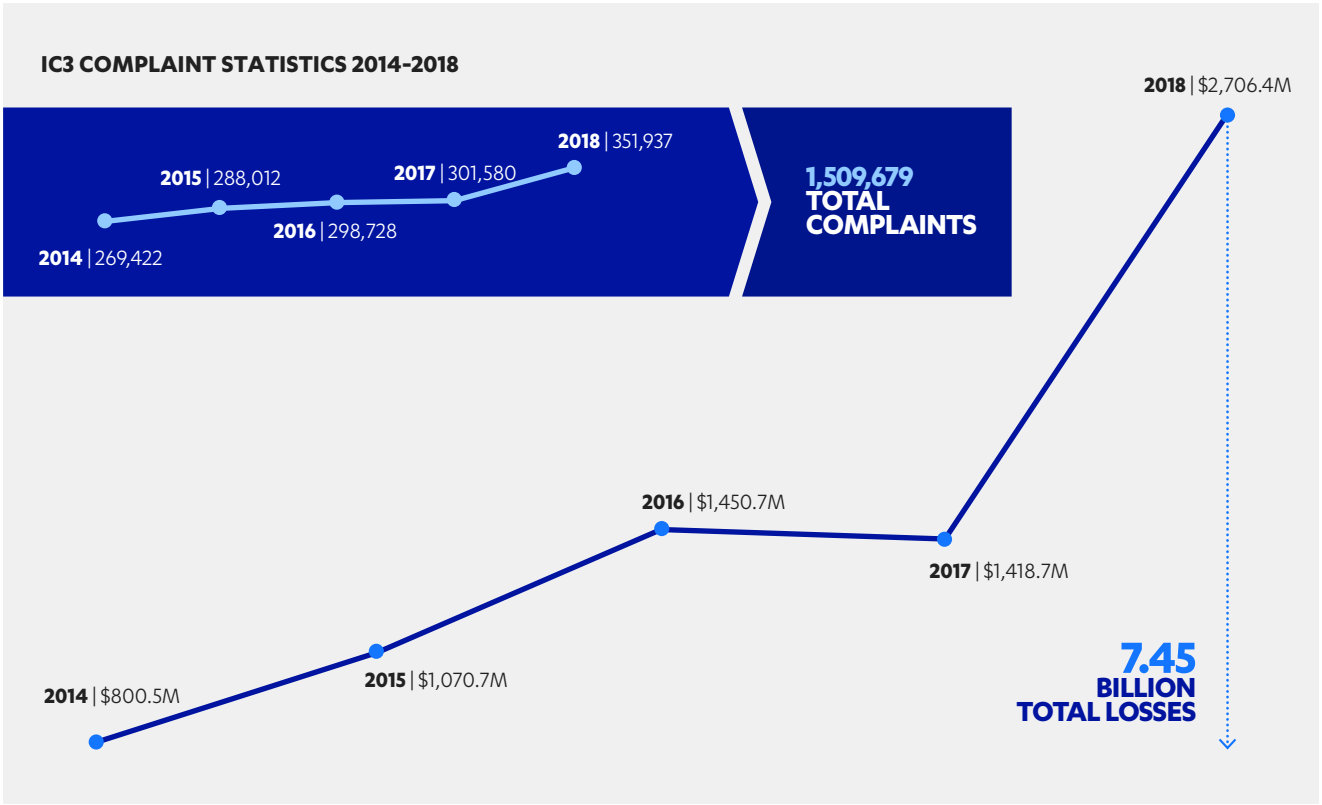


Even if the victims of breaches secured all their data using every possible method, they would still be vulnerable to various techniques crooks use to monetize their data. These include using private data to receive medical care, to avoid law enforcement and to create fraudulent accounts to make purchases, apply for loans or seek credit.

The data suggests consumers understand that the risk they endure by opening the dozens, if not hundreds, of accounts that come with using not only the internet but basic government services and credit cards.

Every year, the number of cyber crimes reported to the Internet Crime Complaint Center (IC3) grows in both in number and in financial impact.[10]

9 Poll: Americans leave their personal info open to thieves https://www.creditcards.com/credit-card-news/data-security-poll.php
10 Internet Crime Complaint Center (IC3) 2018 Internet Crime Report https://pdf.ic3.gov/2018_IC3Report.pdf



The most costly crimes reported almost all involve fraud, scams, or exploitation of personal data.

While "Identity Theft" itself ranks as the fifth most costly crime with loses of over $100 million, many of the crimes that lead to the biggest losses—from Business Email Compromise (BEC) or Email Account Compromise (EAC) to Personal and Corporate Data Breach to Credit Card Fraud—involve aspects of what many people would commonly label identity theft or compromise.

IDENTITY THEFT LOSSES

Crime Type	Loss
BEC/EAC	$1,297,803,489
Confidence Fraud/Romance	$362,500,761
Investment	$252,955,320
Non-Payment/Non-Delivery	$183,826,809
Real Estate/Rental	$149,458,114
Personal Data Breach	$148,892,403
Corporate Data Breach	$117,711,989
Identity Theft	$100,429,691
Advanced Fee	$92,271,682
Credit Card Fraud	$88,991,436
Extortion	$83,357,901
Spoofing	$70,000,248
Government Impersonation	$64,211,765

IDENTITY THEFT MAKES CYBER CRIME REAL

Identity theft is generally defined as acquiring someone's personal information in order to impersonate an individual or gain access to her personal records or services, possibly for financial benefit. Identity theft can result in both online and offline crimes. These crimes involve all sorts of fraud and confidence scams.

The Consumer Sentinel Network database run by the U.S. Federal Trade Commission took in 444,602 reports of identity theft in 2018, including 157,688 reports from "people who said their information was misused on an existing account or to open a new credit card account."[11]

IDENTITY THEFT TYPES

1 Credit Card Fraud
157,688 reports

2 Other Identity Theft
122,499

3 Employment or
Tax-Related Fraud 67,374

4 Phone or Utilities
Fraud 63,563

5 Bank Fraud
52,529

6 Loan or Lease
Fraud 51,856

7 Government Documents
or Benefits Fraud 24,854

Looking at the online threats that consumers worry about most—hacking into your bank account, online shopping fraud, someone committing a crime under your name, someone applying for a loan in your name and someone stealing your possessions using stolen info—they all involve some form of crime that might be labeled identity theft.

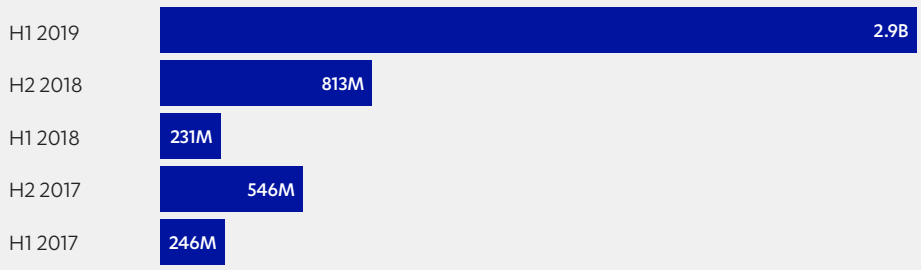
Data increasingly needs to be secured. If criminals get ahold of it, they can take control of our identities or accounts to commit crimes that may damage our abilities to get loans, secure contracts, or even gain employment.

11 Consumer Sentinel Network: Data Book 2018 https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2018/consumer_sentinel_network_data_book_2018_0.pdf

CONSUMER EXPERIENCES AND WORRIES

F-Secure's global network of honeypots measured billions of attack events in the first half of 2019.[12]

TOTAL GLOBAL HONEYPOT ATTACKS PER PERIOD



The threats consumers report facing on their devices and home networks still come from malware and viruses (27%). Credit card fraud (18%), SMS/call fraud (11%), and email or account hacking (10%).[13]

THE MOST COMMON SECURITY INCIDENTS

While internet security solutions prevent infection by most malware and viruses, many of the other most prevalent threats—credit card fraud, call fraud, unauthorized account takeovers and identity theft—require securing data both on consumers devices and in the multiple accounts most users have with a wide variety of services and providers.

In the third decade of the twentieth-century, protecting yourself online doesn't just require securing your devices. It also requires the ability to control your identity and prevent theft and fraud should private data end up in the wrong hands.

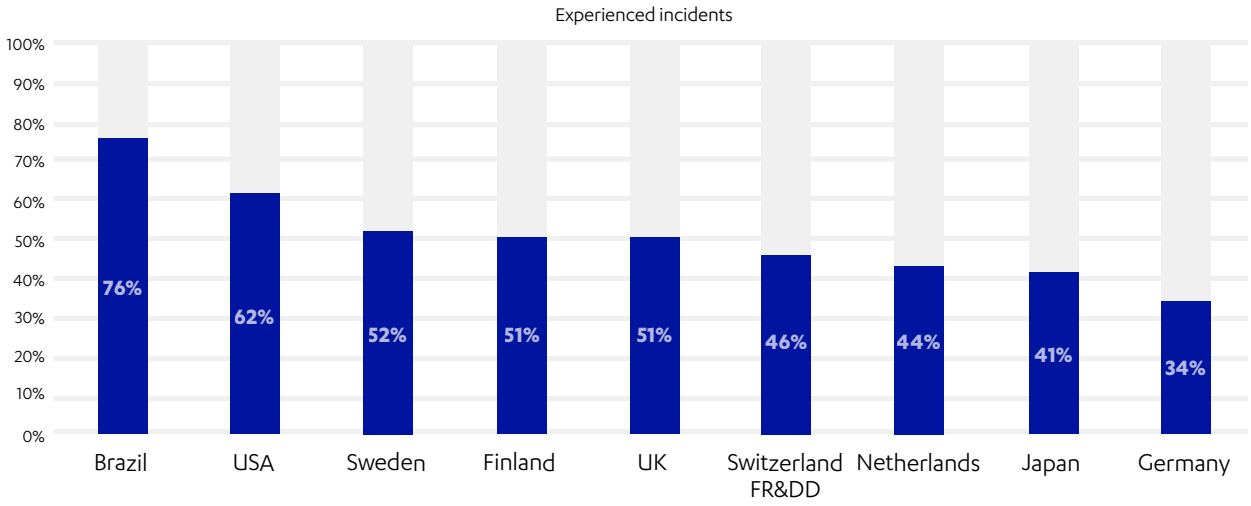
12 Attack Landscape H1 2019: IoT, SMB traffic abound https://blog.f-secure.com/attack-landscape-h1-2019-iot-smb-traffic-abound/

13 Source: F-Secure Identity Protection Consumer (B2C) Survey, May 2019, conducted in cooperation with survey partner Toluna, 9 countries (USA, UK, Germany, Switzerland, The Netherlands, Brazil, Finland, Sweden, and Japan), 400 respondents per country = 3600 respondents (+25years)

Is identity theft the cyber crime we fear most?

Who has been affected?

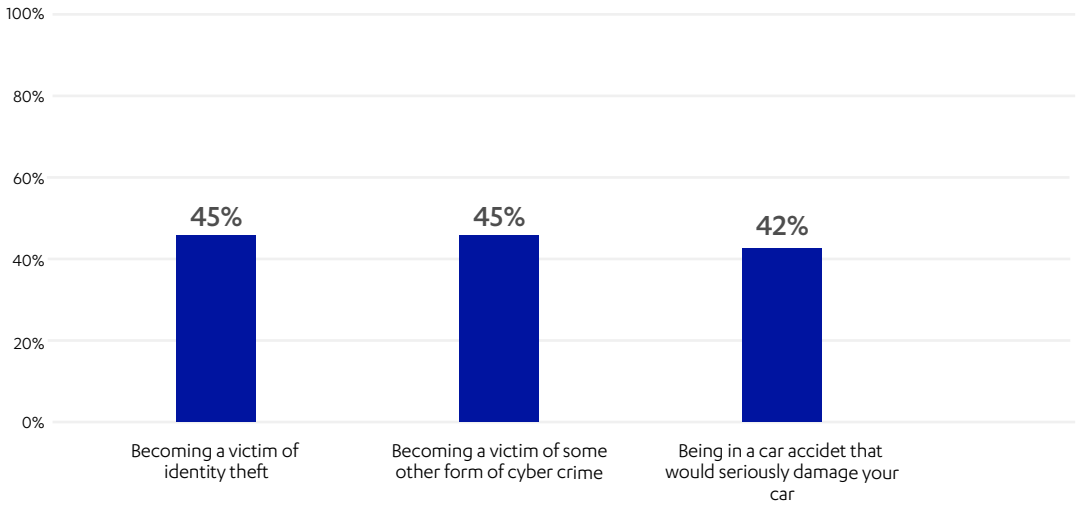
HAVE YOU OR SOMEONE IN YOUR FAMILY BEEN AFFECTED BY CYBER CRIME?



Brazil is the country where you're most likely to have been affected by cyber crime, with a whopping three out of four people (76%) reporting an incident experienced in their family. A majority of families in the US (62%), Sweden (52%), Finland (51%) and the UK (51%) have all suffered from cyber crime.

Globally most people (51%) have been affected by cyber crime, with one in four (26%) reporting dealing with several incidents. Germans, however, are doing something right, with only about one in four (34%) reporting an incident in the family.

HOW WORRIED ARE YOU ABOUT EACH OF THE FOLLOWING STATEMENTS?

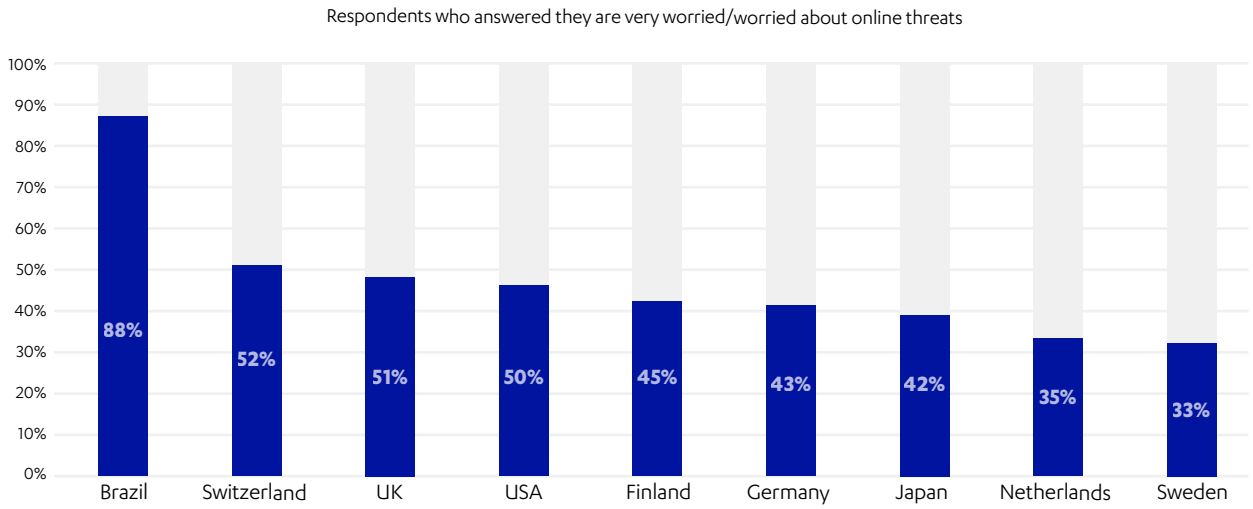


Is identity theft the cyber crime we fear most?

Around the world, fears of identity theft (45%) and cyber crime (45%) rise just above the fear of a being in a car accident that would seriously damage the vehicle (42%). Yes, consumers sense that a damaged identity is likely to cause more problems than a damaged car.

It's easy to find a mechanic to fix a car. Repairing a compromised identity is rarely simple.

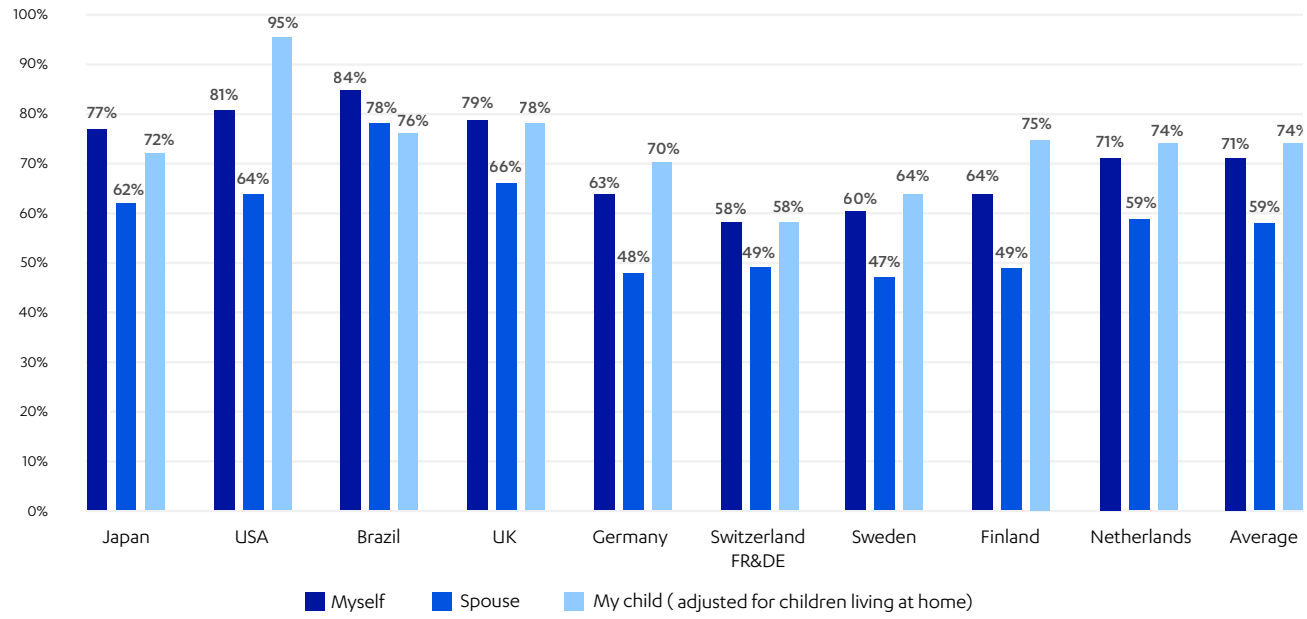
WHICH COUNTRIES ARE MOST WORRIED ABOUT ONLINE THREATS



Given that more than three in four Brazilians have had a personal experience with cyber crime, it makes sense that nearly nine in ten of them are worried about online threats.

About half the respondents in Switzerland, the United Kingdom and the United States expressed similar fears. Dutch and German internet users should share their cyber security secrets with the world. Only about one in three are worried about online threats.

LIKELIHOOD OF BECOMING A VICTIM OF A CYBER CRIME OR IDENTITY THEFT



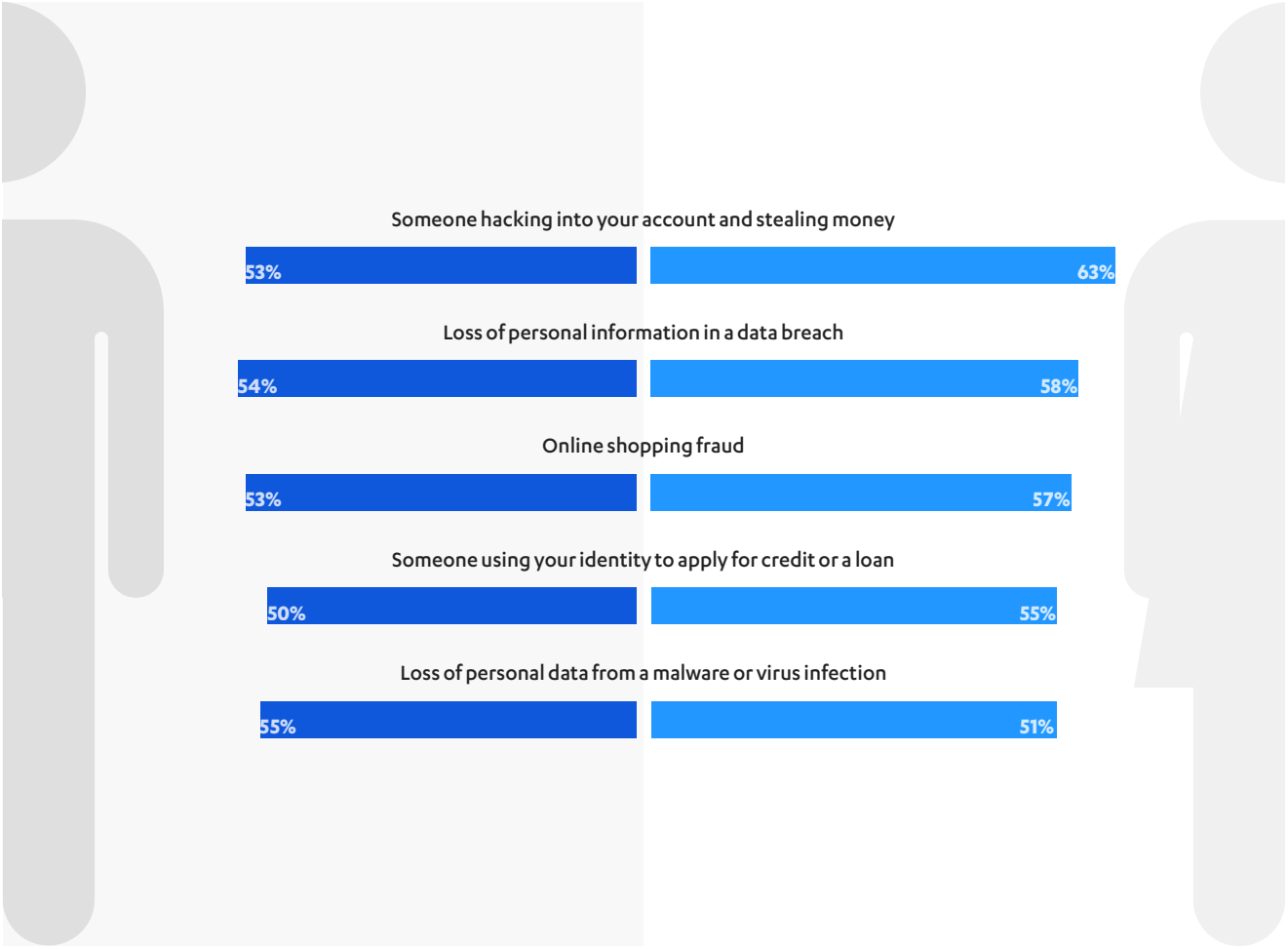
Included responses: Moderately likely - Very likely
Excluded: Unlikely and Not at all likely

In every country surveyed, most respondents expressed at least a moderate fear that they would endure some sort of cyber crimor identity theft (71%).

However, parents' fear that their children would have to deal with these scourges rose above concern about their individual online safety in eight of the countries surveyed – the exceptions were Japan (77% Myself v. 72% My child) and Brazil (84% Myself v. 76% My child).

In the United States, 19 out of 20 parents (95%) expressed significant fears that their kids would have suffering inflicted upon them through criminals using the internet.

CONTRASTING MEN AND WOMEN



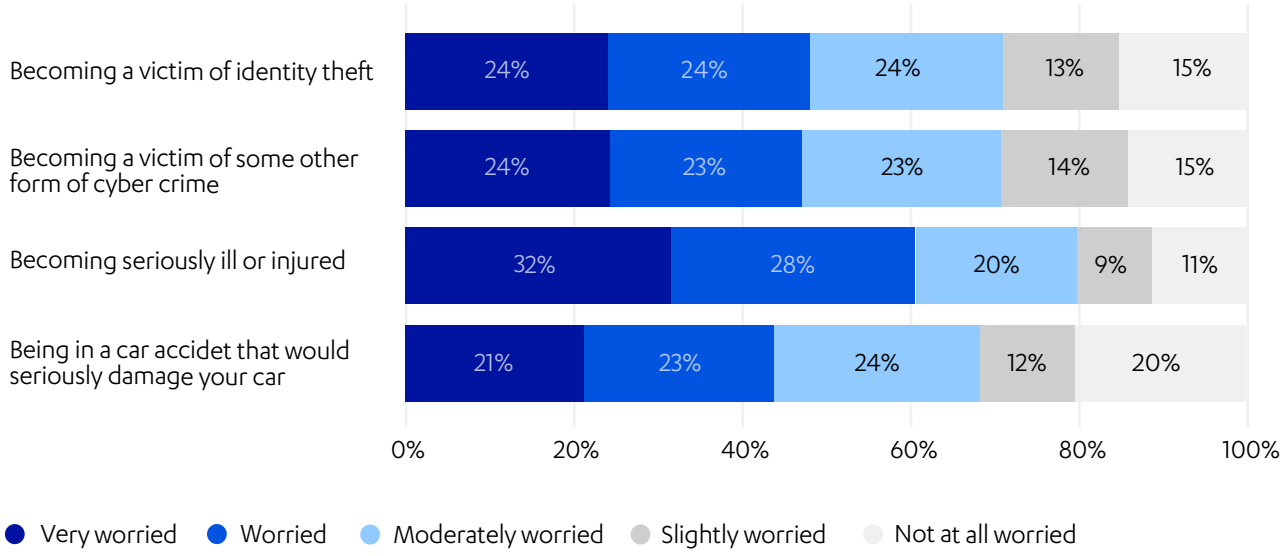
The data in this chart represents only the respondents who expressed they were worried and very worried, excluding those who said they were somewhat worried.

While at least 50% of both women and men are worried or very worried about many of the biggest risks associated with identity thefts, women are more worried about all of these risks, with the biggest gulf being that 10% more women (63%) worry about someone hacking into their bank account to rob them than men (53%).

The percentage of women who are worried or very worried about identity theft and cyber crime is 47-48%, higher than 44% who expressed similar concerns about a car accident that damages the vehicle.

Women

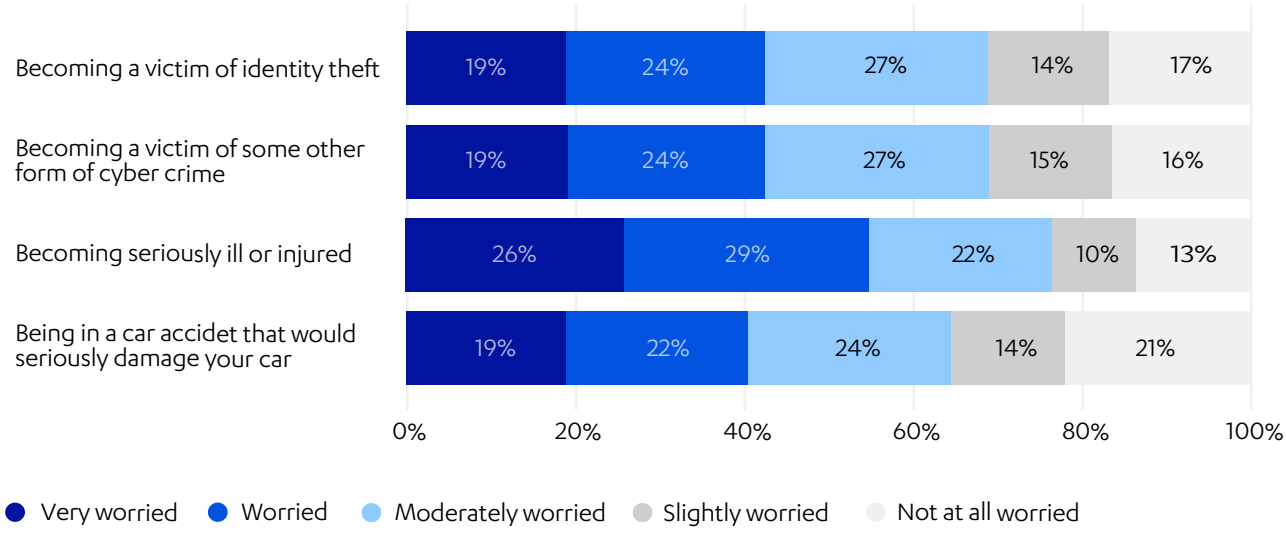
WORRIED ARE YOU ABOUT EACH OF THE FOLLOWING STATEMENTS? 1,855 Responses



Men, again, are less worried in general with 43% reporting they are worried or very worried about identity theft and cyber crime.

Men

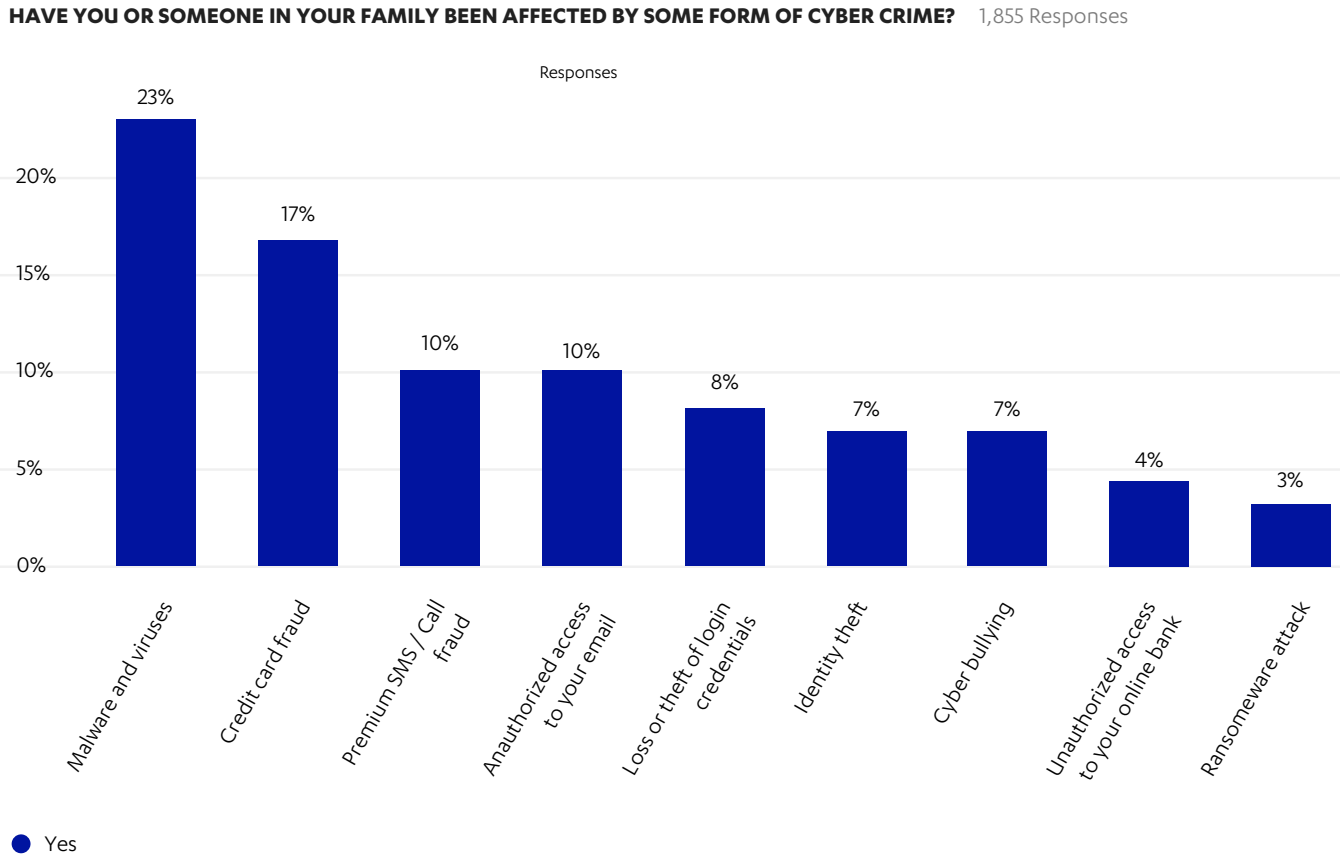
WORRIED ARE YOU ABOUT EACH OF THE FOLLOWING STATEMENTS? 1,745 Responses



Women

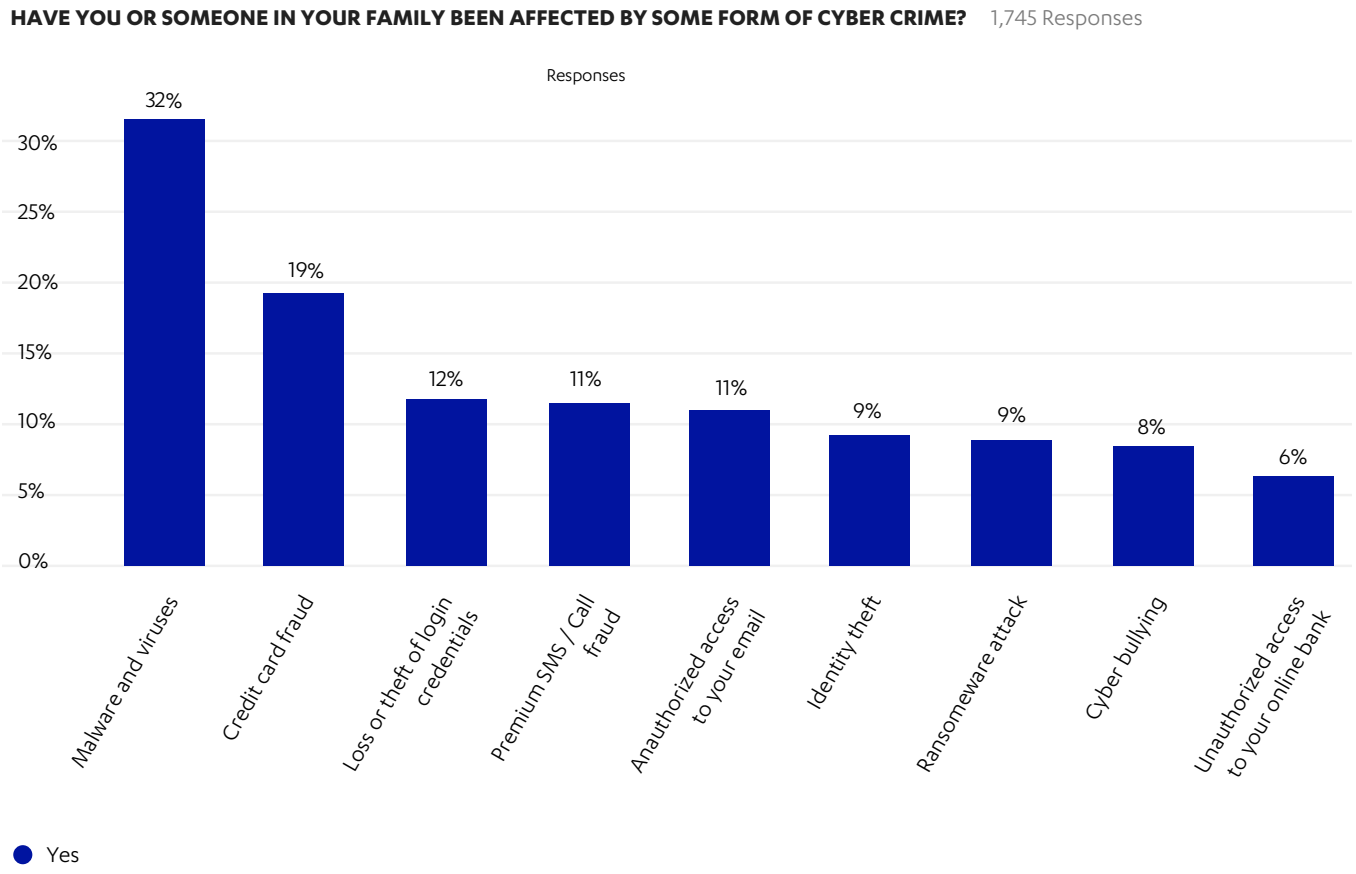
Here's the fascinating thing.

While they may express more concern, women were less likely to report having been a victim of some form of cyber crime.



Men

68% of men offer similar worries about identity theft or cyber crime with only 42% of men with children saying they have these fears for their kids.



CONCLUSION

Human beings are not known as excellent evaluators of risks.

We may tense with fear as an airplane takes off, though we're more likely to suffer a fatal accident when we jump into a car, which isn't subject to a rigorous regime of regulations and inspections once it leaves the assembly line.[14]

Men report more experience with online threats than women, yet worry less about them. And though the costs of cyber crime go up every year, the average internet user still spends about as much time online as they do at work.

Yet when it comes to the risks that come from using the internet consumers seem to understand that our risks extend far beyond our devices.

The era where securing your PC was enough to prevent most of the harm that comes from being online is long over. Now securing dozens of accounts, including credentials for our credit cards, bank accounts, social media accounts, loyalty programs and more is necessary in order to protect our identities.

While malware and viruses still threaten our computers and our files, the risks that come from an attack spilling over into our "real lives" continue to mount as our digital footprints continue to grow.

Cyber crime is a real concern but the fraud and long-term damage that come from stolen identities seems to be what's keeping consumers up at night. The damages that come from identity theft can be expensive and long lasting. Expert help to both prevent these crimes and deal with the consequences promptly could reduce that anxiety.

What should you do about it?

Most of the cyber security advice that began circulating in the early days of the web is still relevant today. You should still keep your software updated. Clicking on unexpected attachments is still a bad idea. Running top-notch security software is still smart.

However, no matter how well you secure your devices, you can't secure your data when it's stored inside someone else's networks.

Data breaches don't just expose our personal information; they expose our dependency on companies around the world.

The good news is that there are some simple things you can do right now to help secure your online identity.

Forget your passwords

If you can remember your passwords, they're probably not strong enough to protect your accounts. So what do you do with more than a dozen passwords you cannot remember? The solution to this problem is a reliable password manager.

Secure all your accounts with two-factor authentication

The best password in the world can still be compromised if it is not properly secured by the site you've trusted it with. That's why you should use two-factor authentication to secure your accounts wherever it is available. But keep in mind that it is possible to bypass multi-factor authentication by accessing emails and mobile phone messages. So for extra security, use an app like Google Authenticator as your second factor.

14 Which Is Safer: Airplanes or Cars? https://fortune.com/2017/07/20/are-airplanes-safer-than-cars/

Check how exposed you are now

Lists of breached user credentials often circulate among scammers who collect them in order to turn this information into some sort of attack that monetizes your data. This can include phishing, spam, and the spreading of malware. And since the attack can be targeted, it is far more likely to be successful than typical spam. How can you know how vulnerable you are? Consult a reliable service that helps you identify if your information is available somewhere on the dark web.

What should you do if you think you're a victim of identity theft?

If you think your identity has been stolen in any way, remember you are not alone. It happens to more than a million people every month,[15] compared to the about 10,000 cars that were stolen every month worldwide in 2017.[16] Fast action is key.

The Federal Trade Commission (FTC) recommends a few steps to help you react to a breach

1. Call the fraud departments at companies where you know the fraud occurred to freeze your accounts. Changes the logins, pins and passcodes of all affected accounts.
2. Call the major credit bureaus to place a fraud alert and get a copy of your credit. Fraud alerts with Experian, TransUnion and Equifax are free. The alert requires all new creditors to verify your identity and can be renewed after a year.
3. In the United States, report your identity theft to the FTC by calling 1-877-438-4338 or contacting the agency online.
4. You can file your report with your local law enforcement. You will likely need government issued ID, proof of address and any proof you have of the theft. In the US, you will need your FTC Identity Theft report.

15 Facts + Statistics: Identity theft and cybercrime https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime
16 Interpol: Vehicle Crime https://web.archive.org/web/20181103162315/https://www.interpol.int/Crime-areas/Vehicle-crime/Vehicle-crime

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/business | twitter.com/fsecure | linkedin.com/f-secure

F-Secure