NORTON CYBERSECURITY INSIGHTS REPORT

*Get informed about the truths of **online crime** and the personal impact it has on you*

Table of Contents

INTRODUCTION

Why should we care about the human impact of online crime?

Online crime has become a fact of life.

348
MILLION
IDENTITIES EXPOSED

In 2014, more than 348 million identities were exposed when identity thieves **hacked** several trusted institutions.

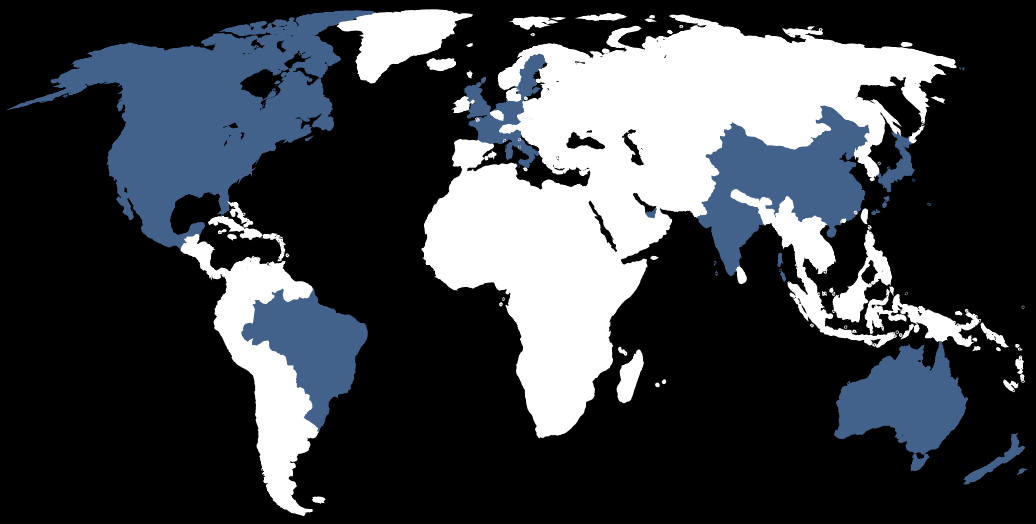
SOURCE | 2015 ISTR.

While many people have seen these high-profile data breaches in the news, know someone who has been impacted, or have been impacted themselves, they still haven't taken the actions needed to adequately protect themselves.

Our research explores the personal impact of online crime. Our hope is that the findings will move people from general awareness online of the threats to a clearer sense of what's at risk and why they should care—and take action.

WE KNOW THE RISK FOR ONLINE CRIME IS HIGH

Consumers globally are feeling the danger of cybercrime.



594
MILLION

AFFECTED BY CYBERCRIME **GLOBALLY**

While many of those consumers impacted by online crime might have been victims of a large data breach or other scam, the majority of victims are not confident in how to handle online crime.

Somewhat troubling, many of those who live in high risk countries are least likely to feel personally responsible when online crime occurs.

Interestingly, Americans are more inclined to take personal responsibility after an online crime than the average of the 17 nations surveyed, with **40%** saying they feel personally responsible after they have been a victim.

AND WE KNOW — AND DREAD — THE CONSEQUENCES

> **“CONSUMERS AROUND THE WORLD LOST AN AVERAGE OF 21 HOURS AND $358 PER PERSON OVER THE PAST YEAR DEALING WITH ONLINE CRIME”**

Once a person has been the victim of online crime, the impact on their life can be extensive. Cybercrime has costs that go beyond financial. Consumers around the world lost an average of 21 hours (for perspective that’s the entire next season of Arrested Development) over the past year dealing with the fallout from online crime, and nearly **$358 on average per person, enough for a year of home security monitoring.**

And because so much of our business is conducted online—bill payments, shopping, and trading, for example—the inconvenience of dealing with the impact of having financial information compromised can be almost painful.

Nearly half (**41%**) report feeling furious after becoming a victim of online crime and **81%** say they’d feel devastated if their personal financial information was compromised.

70% of U.S. consumers would rather cancel dinner plans with a best friend than have to cancel their debit/credit card.

63% would rather go on a bad date than have to deal with customer service after a security breach.

BUT WE'RE ALL FAIRLY CERTAIN IT WON'T HAPPEN TO US

When it comes to our own personal security online, we think we've got it covered. Consumers consistently award themselves a solid A when it comes to grading their online security behaviors, but most of what we do leaves us vulnerable.

In reality, most of us are failing the most basic requirement of online security: **Passwords 101.**

Of those using passwords, less than half of consumers "always" use a secure password.

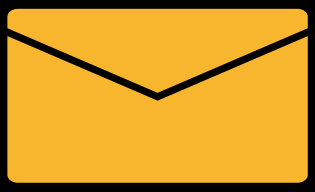
One in three do not have a password on their smartphone or desktop computer at all!

WE OVERSHARE OUR MOST VULNERABLE INFORMATION

****

MORE THAN 1/3 (36%) OF THOSE SHARING PASSWORDS IN THE U.S. **HAVE SHARED THE PASSWORD TO THEIR BANKING ACCOUNT!**

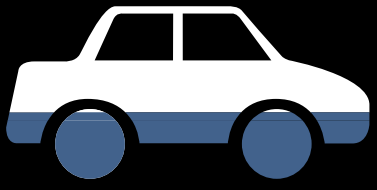
Of those sharing passwords across the globe, people have shared on average their passwords for two accounts, mostly email **(55%)**, TV/media **(29%)** and social media (43%).



55%

29%

43%

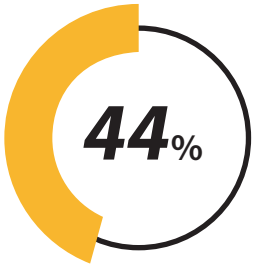


Two in three believe it is riskier to share their email password with their friend than lend them their car.

MILLENNIALS

Surprisingly, overly confident, digital-native Millennials are the most vulnerable to online crime

Of the generations that spend the most time online, Millennials are the most likely to throw caution to the wind. While they work, conduct business and socialize online, 44 percent of U.S. Millennials have been a victim of online crime in the last year.

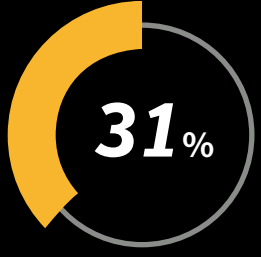


U.S. Millennials are the least likely to take responsibility for their personal security, and:

NEARLY HALF

RELY ON BANKS AND CREDIT CARD COMPANIES

to protect them after a hack.



Globally, Millennials are also the most likely to share passwords at **31%**.

ACROSS THE GLOBE: MILLENNIALS VS. BABY BOOMERS

Baby Boomers are more tech-savvy than expected

42% of Baby Boomers using passwords, use secure passwords

ONLY **15%** of Baby Boomers have shared their passwords

ONLY **16%** of Baby Boomers globally have experienced online crime in the past year

Although they didn't grow up in the digital age, Baby Boomers are savvier than expected: While **40%** of all US consumers (and **56%** of those 55+) feel older generations are most vulnerable to online crime, this group actually reports safer online behavior than younger generations:

They are less likely to share passwords (only **15%**) and the most likely to always use secure passwords (**44%**).

As a result, only **16%** of Baby Boomers have experienced online crime in the past year.

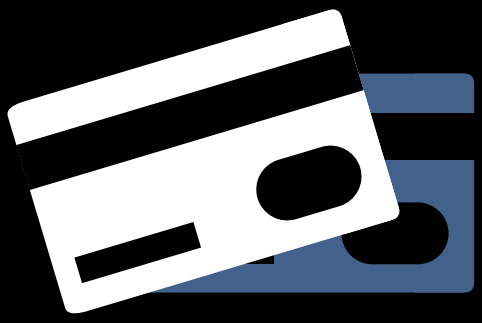
WHAT WE FEAR

We're nearing the point where online risks scare us more than our physical-world fears

Up until today, people often did not approach the Internet with the same heightened sense of danger as we do in threatening situations in real life. Director of the FBI, James Comey, called the Internet, "the most dangerous parking lot imaginable," and warned people to be just as aware of scams, compromised websites, malware and other threats as they would be of a physical theft.

Luckily, folks are wising up and becoming more conscious of the riskiness of online behavior:

Six in 10 consumers believe using public Wi-Fi is riskier than using a public restroom.



Consumers around the world believe they are nearly twice more likely to have their credit card information stolen online than from their wallets.

Four in five worry about being an online crime victim.

61% believe identity theft is more likely than ever before.

JUST OVER HALF

of U.S. consumers (**51%**) think that storing their credit/banking information in the cloud

IS RISKIER THAN NOT WEARING A SEATBELT.

51% of parents around the world see

ONLINE BULLYING

AS MORE LIKELY THAN BEING BULLIED AT SCHOOL OR WORK (49%).

STAYING SMART IN A WORLD OF CHANGING TECHNOLOGIES

You can't always know what's lurking out there in the "shadows," but here are some key tips to keep you safe:

1) Choose a unique, smart, secure password for each account you have online. For tips on how to do this, **click here**.

2) Delete emails from senders you don't know, and don't click on attachments or links on suspicious-looking emails.

3) On social media sites, if an offer sounds too good to be true, it just might be. Avoid clicking on posts that offer that "Free trip to Tahiti!" especially if they don't come directly from a reputable, "official" trusted company page.

4) Always monitor your financial accounts for unusual activity. If you see a charge that you didn't make, report it immediately. Often cybercriminals will charge a small "test" amount before attempting to drain your bank account.

5) Don't put off updating your software. Yes, those update pop-ups are annoying, but those updates often contain important patches for dangerous security holes that cybercriminals could use to access your device.

6) Use a secure backup solution to protect your files and backup regularly so criminals can't hold them for ransom.

7) Don't rely on freeware for cybersecurity. You get what you pay for. And some freeware options that are meant to protect your information are even selling it to make money. Use trusted, multi-layered protection with support and a security guarantee, like **Norton Security**.

For more smart information on how to stay protected, please visit the **Norton Protection Blog** on the Norton Community.

GO BOLDLY, NOT BLINDLY