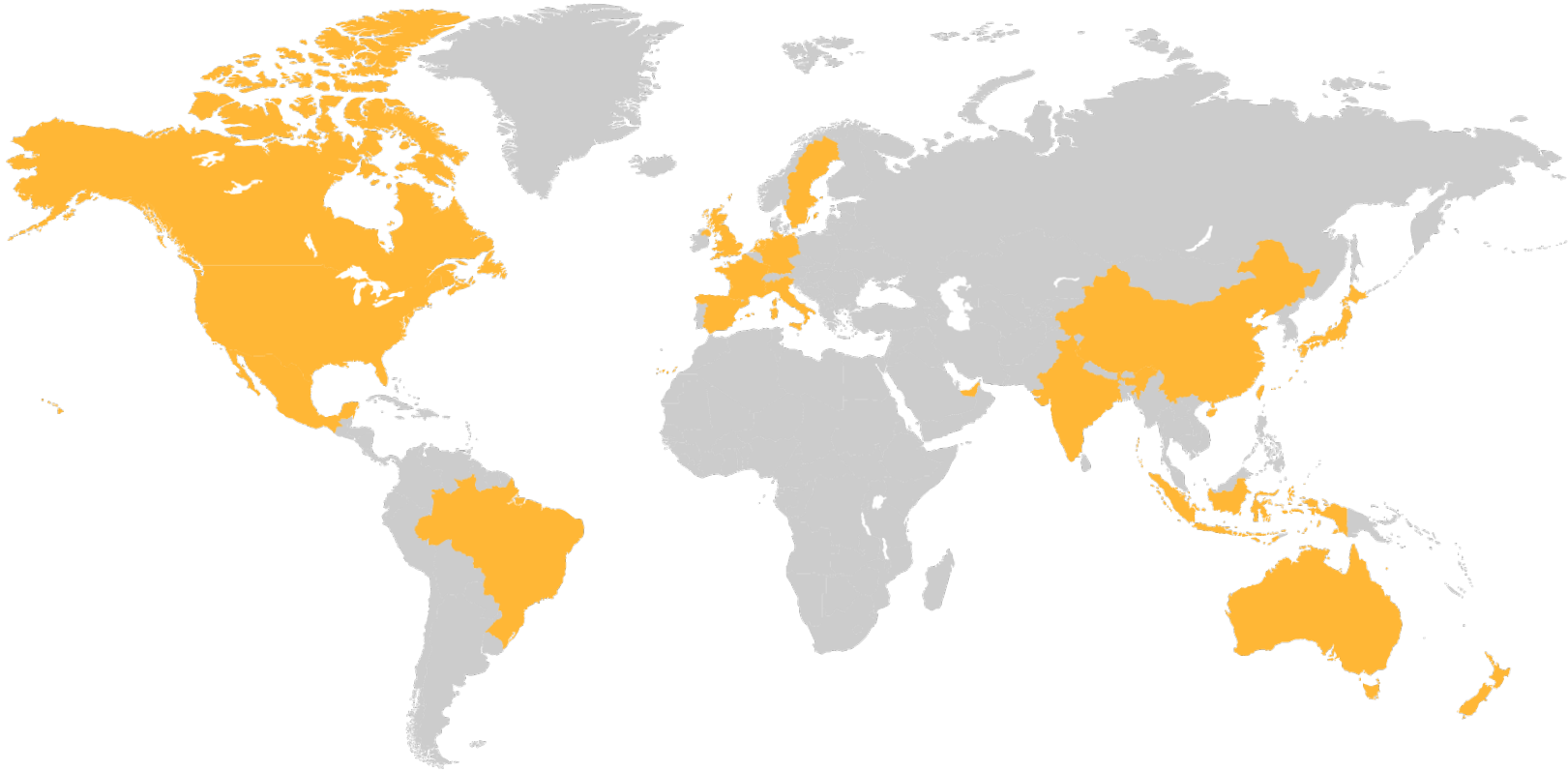
Norton by Symantec



2017

Norton Cyber Security Insights Report United States Results

Table of Contents

1. Key Findings 3 – 9
2. Cybercrime by the Numbers 10 – 16
3. Portrait of a U.S. Cybercrime Victim 17 – 20
4. Consumers' Contradicting Beliefs 21 – 24
5. State of Consumers' Trust 25 – 26
6. About the 2017 Norton Cyber Security Insights Report 27 – 30

Copyright © 2018 Symantec Corporation

Key Findings

Copyright © 2018 Symantec Corporation

Key Findings

When it comes to cyber security, consumers are overconfident in their security prowess, leaving them vulnerable and enabling cybercriminals to up the ante this year, which has resulted in record attacks.

143 million Americans were affected by cybercrime in 2017. This is more than half the US adult online population. Nearly eight in ten people (77%) report either experiencing or know some who has experienced cybercrime. Most common cybercrimes include:

- Having a device infected by a virus or other security threat (57%)
- Experiencing debit or credit card fraud (54%)
- Having personal information involved in a data breach (54%)
    - Note: Americans were 80% more likely to have their personal information involved in a data breach, compared to the global average (30%)
- Having an account password compromised (40%)
- Encountering unauthorized access to or hacking of an email or social media account (40%)
- Making a purchase online that turned out to be a scam (33%)
- Clicking on a fraudulent email or providing sensitive (personal/financial) information in response to a fraudulent email (34%)

As a result, American consumers who were a victim of cybercrime lost $19.4 billion – an average of $96 per victim – and nearly 20 hours (19.8 hours) dealing with the aftermath.

Copyright © 2018 Symantec Corporation

Key Findings

Cyber security concerns do not always seem to translate to good behaviors as many consumers put themselves at risk in their day-to-day lives. This leads us to a startling cybercrime confession: those who emphasize the importance of online security, generally contradict themselves through their actions, and as a result, are more likely to fall victim to cybercrime.

Cybercrime victims share three common traits:

- **Overconfident in Cyber Security Prowess:** While 58% of consumers have personally experienced cybercrime in the past year, more than a third of victims gained trust in themselves to manage their data and personal information (37%) and more than a quarter think they're at a low risk of becoming victim (28%).
- **Favor Multiple Devices:** 46% of U.S. cybercrime victims own a smart device for streaming content, compared to about one quarter of non-victims. They're also three times as likely to own a connected home device as non-victims.
- **Dismiss the Basics:** U.S. cybercrime victims practice new security techniques such as such as fingerprint ID (45%), voice ID (14%), pattern matching (21%), facial recognition (16%), personal VPN (19%), and two-factor authentication (16%). Yet, nearly a quarter of victims use the same online password across all accounts (24%) and 60% share their passwords for at least one device or account with others. Additionally, 41% write their passwords down on a piece of paper and are almost twice as likely to use different passwords and save their password to a file on their computer/smartphone than non-victims.

Copyright © 2018 Symantec Corporation

Key Findings

From Millennials to Baby Boomers, to the parents in between, everyone leaves their virtual door open when it comes to cyber security.

- Confession: While Millennials are the most technologically savvy – owning the most devices and adopting security practices such as pattern matching, face recognition, VPN, voice ID and two-factor authentication – they're the most likely to make simple security mistakes and become a victim, with 69% experiencing a cybercrime in the last year alone:
  - One in three (39%) Millennials use the same password for all accounts, compared to 7% of Baby Boomers
  - 73% of Millennials have shared at least one or more of their passwords with another person, compared to 34% of Baby Boomers
- Confession: Baby Boomers are generally the safest, though they make faux pas as well:
  - Nearly 69% of Baby Boomers use different passwords, but 45% of Baby Boomers write those passwords down on a piece of paper. Baby Boomers were also less likely to back up their devices, with 12% of Baby Boomers failing to back up any devices versus 4% of Millennials.
- Confession: Parents are worried about many things when it comes to their child and the Internet – but fewer act. 95% of parents worry about their children and the Internet, yet only 29% of parents always supervise their children online when using social media, and less than a third always supervise their children online when they are playing online games or watching videos, streaming movies or TV shows online. Meanwhile, 9% of parents do not take any actions to protect their children online.

Copyright © 2018 Symantec Corporation

Key Findings

Consumers' boundaries skewed between cybercrime and "real life"

- Confession: While 81% of consumers think a cybercrime should be treated as a criminal act, 41% believe it's sometimes acceptable to engage in morally questionable online behaviors in certain instances:
  - One fourth (28%) say reading someone's emails without their consent is sometimes acceptable
  - 20% believe using a false email or someone else's email to identify their self online is sometimes acceptable
  - 18% believe that accessing someone's financial accounts without their permission is sometimes acceptable
- Interestingly, victims of cybercrime were more likely to think it's acceptable to commit cybercrime than non-victims:
  - 32% say reading someone's emails without their consent is sometimes acceptable compared to 14% of non-victims
  - 22% believe using a false photo or someone else's phone to identify themselves online is sometimes acceptable
  - 21% believe that accessing someone's financial accounts without their permission is sometimes acceptable compared to 9% of non-victims

Copyright © 2018 Symantec Corporation

Key Findings

Despite this year's cyberattacks, consumers generally continue to trust the institutions that manage their data and personal information. However, they are not as trusting of some institutions and organizations.

- Consumers have gained or maintained trust in the following institutions to manage their data and personal information:
    - 71% in identity theft protection services
    - 74% in email providers
    - 76% in internet service providers
    - 76% in financial institutions

- Concerningly, however, 53% of consumers lost trust in their government

Copyright © 2018 Symantec Corporation

What to Do?

Stick to the basics. The realities of cybercrime can feel daunting, but practicing basic behaviors, such as proper password hygiene will go a long way. While new technologies such as facial recognition and voice ID are effective, it all starts with basic security measures such as:

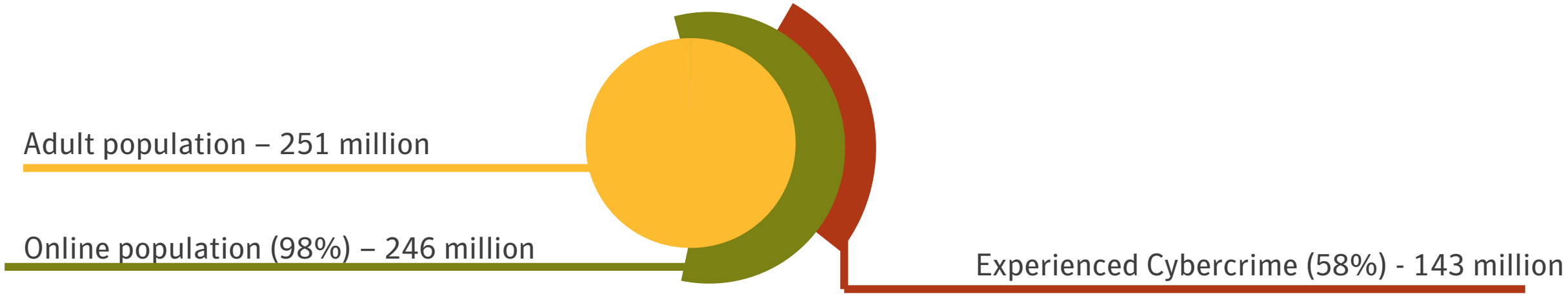
- **Craft a strong, unique password** using a phrase that consists of a string of words that are easy for you to memorize, but hard for others to guess. Don't tie your password to publicly available information as it makes it easier for the bad guys to guess your password. The longer, the better! Additionally, if your account or device enables it, consider two-factor authentication for an additional layer of security. Finally, once you've created a strong password, stick with it until you're notified of a security breach. If you feel overwhelmed, use a password manager to help!
- Using unprotected Wi-Fi can leave your personal data vulnerable to eavesdropping by strangers using the same network so **avoid anything that involves sharing your personal information when connected to an open Wi-Fi network**. If you do use public Wi-Fi, consider using a Virtual Private Network (VPN) to secure your connection and help keep your information private.
- Make it a habit to **change default passwords on all network-connected devices**, like smart thermostats or Wi-Fi routers, during set-up. If you decide not to use Internet features on various devices , such as with smart appliances, **disable or protect remote access as an extra precaution**. Also, **protect your wireless connections with strong Wi-Fi encryption** so no one can easily view the data traveling between your devices.
- **Think twice before opening unsolicited messages or attachments**, particularly from people you don't know, or clicking on random links.
- **Protect your devices** with a robust, multi-platform security software solution to help protect against the latest threats.

Copyright © 2018 Symantec Corporation

Cybercrime by the Numbers

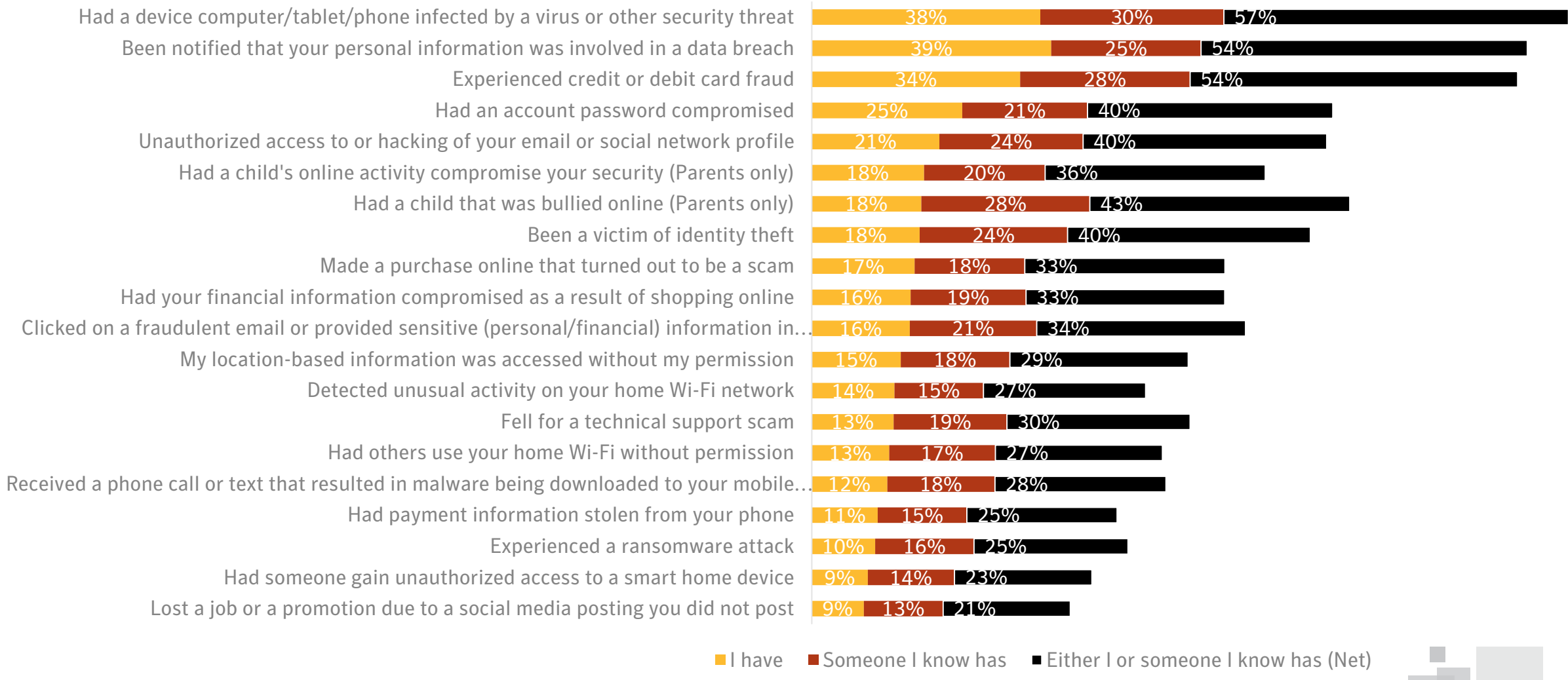
Copyright © 2018 Symantec Corporation

Within the last year, 143 million people in the US experienced cybercrime



Copyright © 2018 Symantec Corporation

Nearly eight in ten Americans (77%) report either experiencing or know someone who has experienced cybercrime



Copyright © 2018 Symantec Corporation

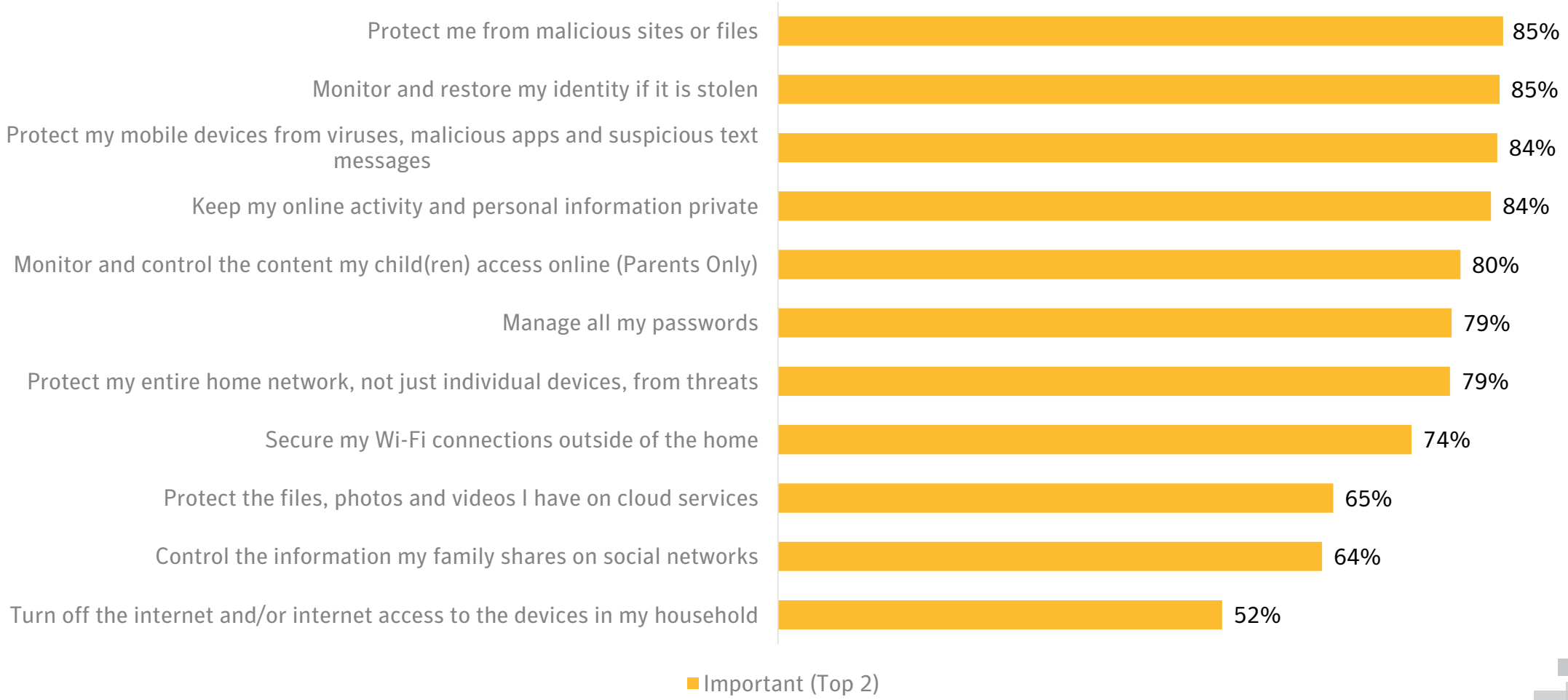
Cybercrime victims spent nearly $19.4 billion dealing with the consequences

Copyright © 2018 Symantec Corporation

The average cybercrime victim spent 19.8 hours dealing with the aftermath

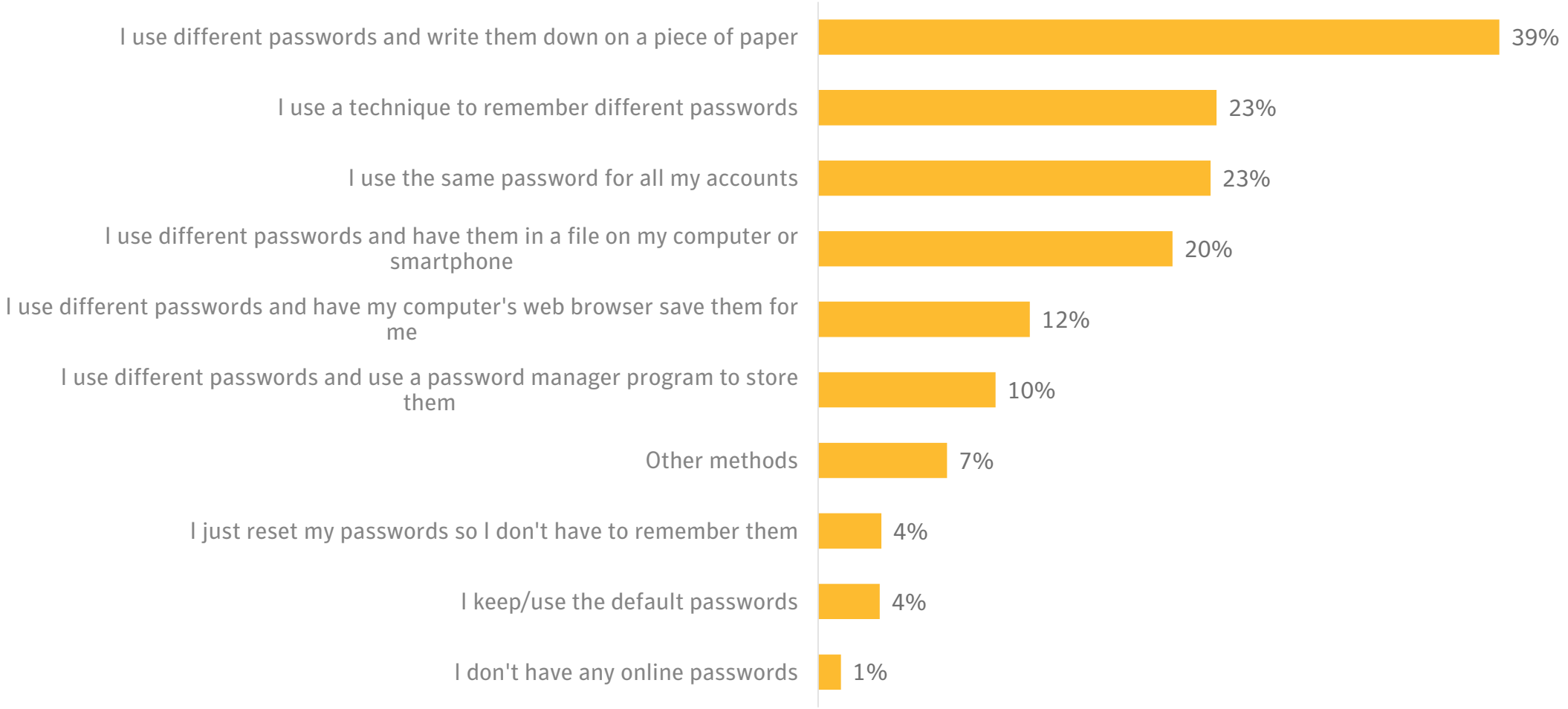
Copyright © 2018 Symantec Corporation

Americans emphasize the importance of online security



Copyright © 2018 Symantec Corporation

Yet, one-third store their passwords insecurely and more than one in five use the same password for all accounts.

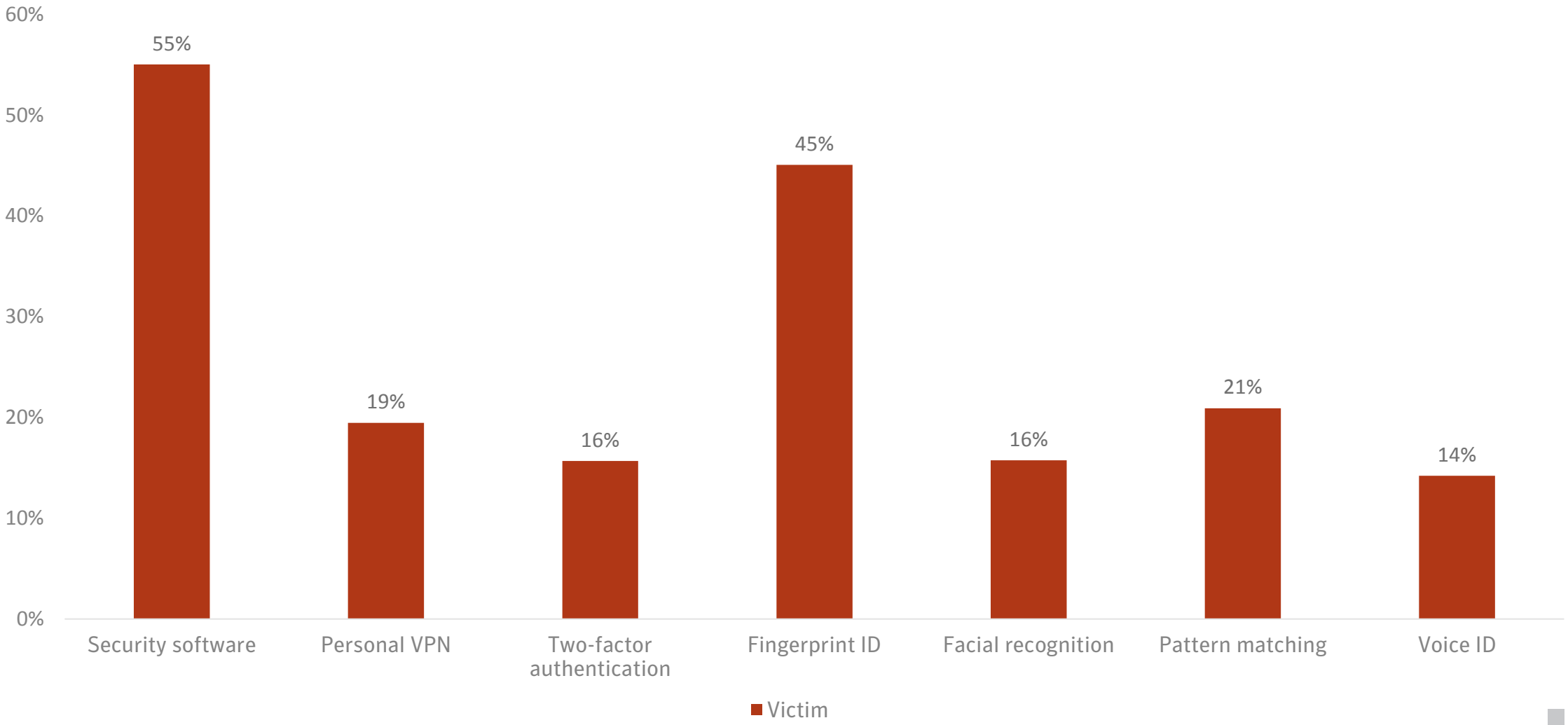


Copyright © 2018 Symantec Corporation

Portrait of a U.S. Cybercrime Victim

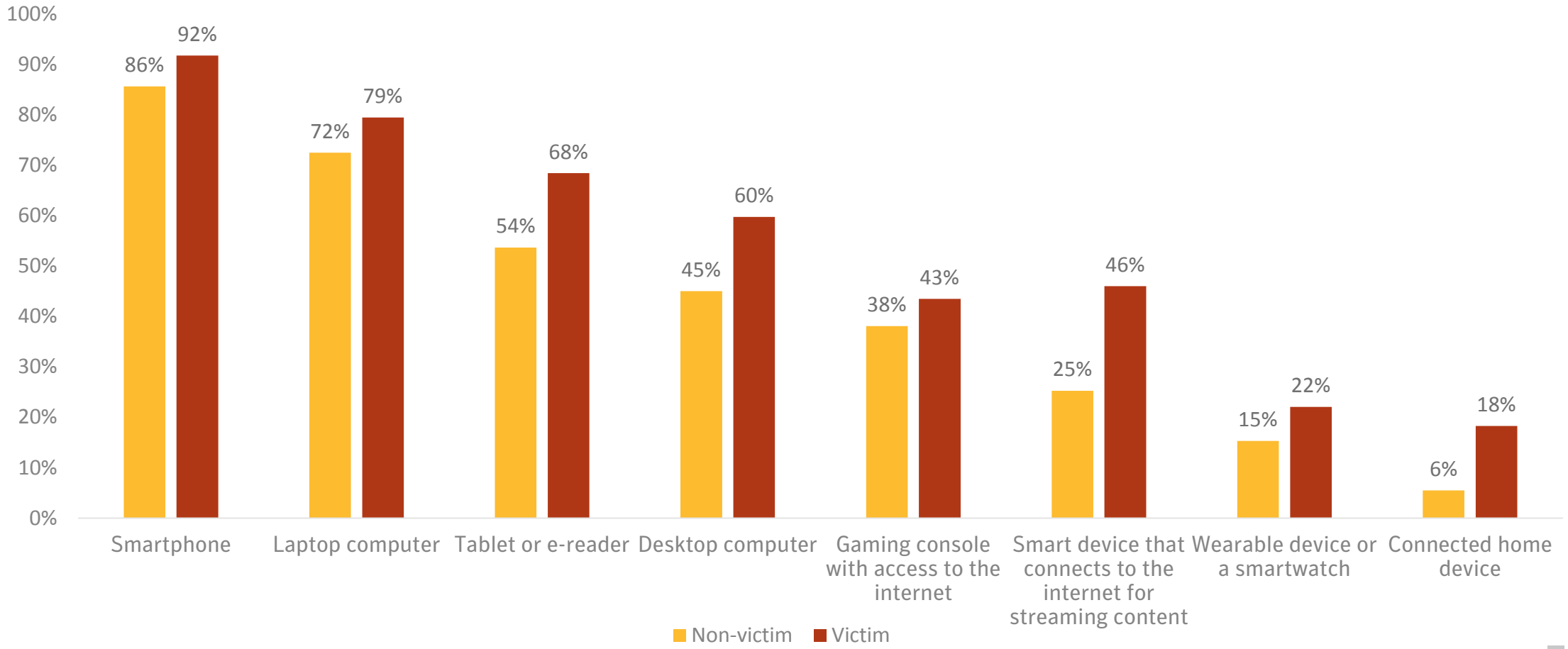
Copyright © 2018 Symantec Corporation

They’re adopters of newer security techniques



Copyright © 2018 Symantec Corporation

They're 3x as likely to own a connected home device than non-victims.



Copyright © 2018 Symantec Corporation

They're more likely to use the same online password across all accounts and share their device or online account passwords with others than non-cybercrime victims.

60%

Of cybercrime victims shared their passwords for at least one device or account with others

24%

Nearly a quarter of U.S. cybercrime victims use the same online password across all online accounts

However, **only 17% of non-cybercrime victims** reuse passwords and **37% share their passwords** with others.

Copyright © 2018 Symantec Corporation

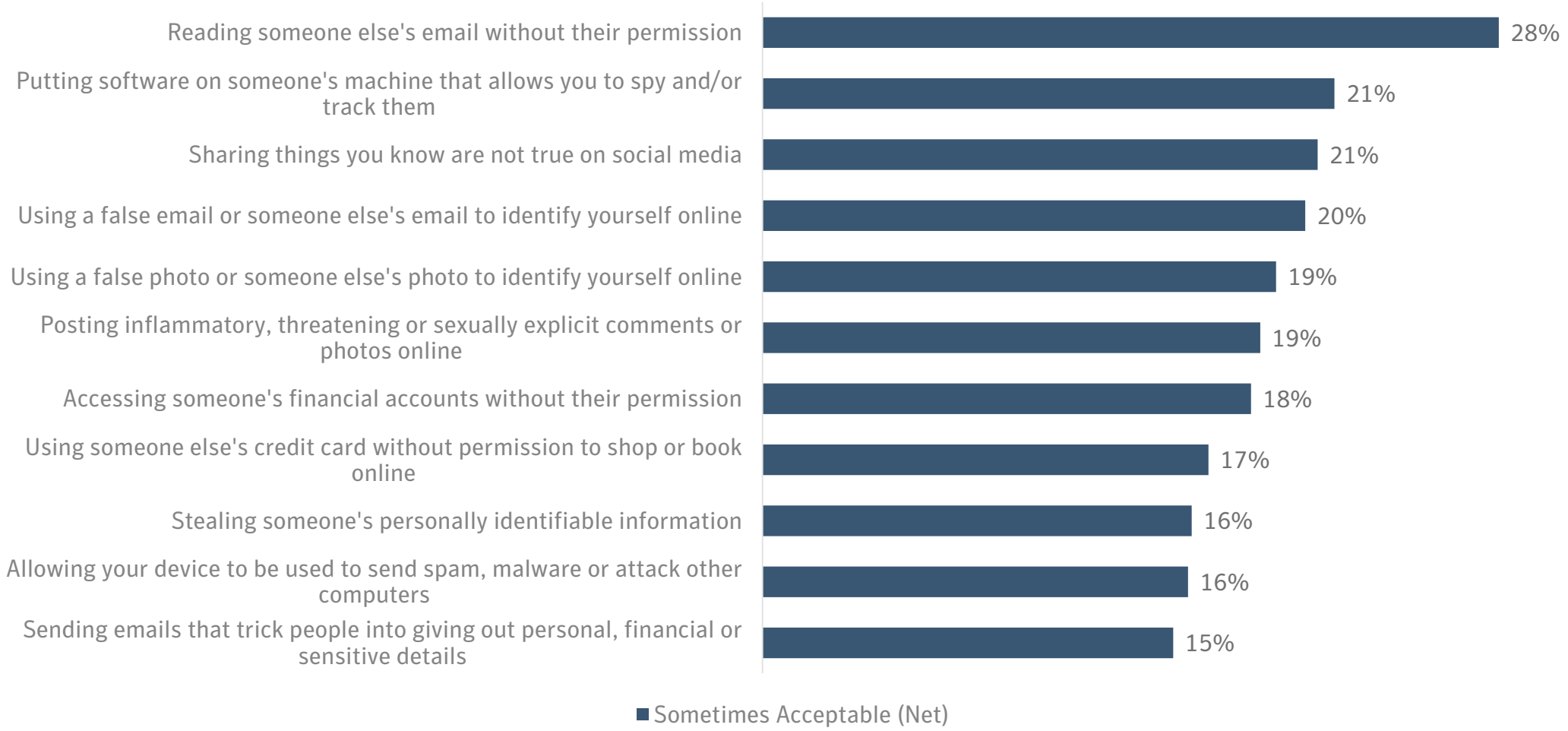
Consumers' Contradicting Beliefs

Copyright © 2018 Symantec Corporation

Consumers believe cybercrime is wrong and should be treated as a criminal act

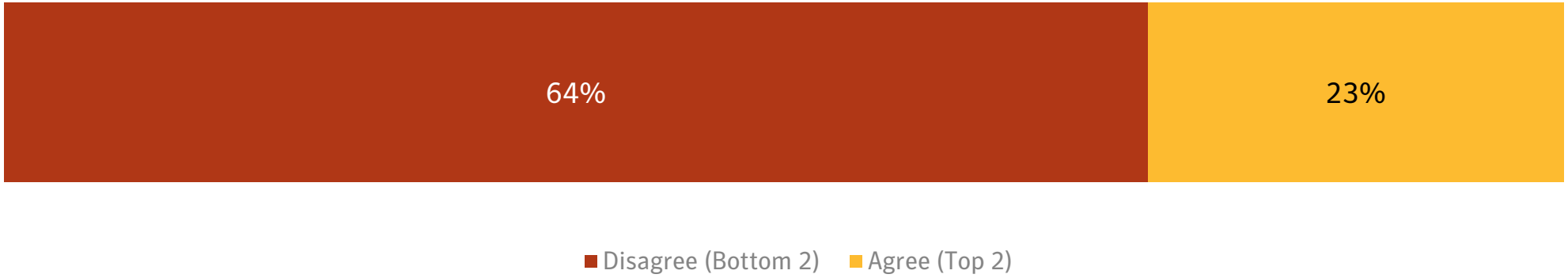
Copyright © 2018 Symantec Corporation

Yet, 41 percent of U.S. consumers believe it's sometimes acceptable to commit morally questionable online behaviors



Copyright © 2018 Symantec Corporation

And nearly one in four believe stealing information online is not as bad as stealing property in ‘real life’

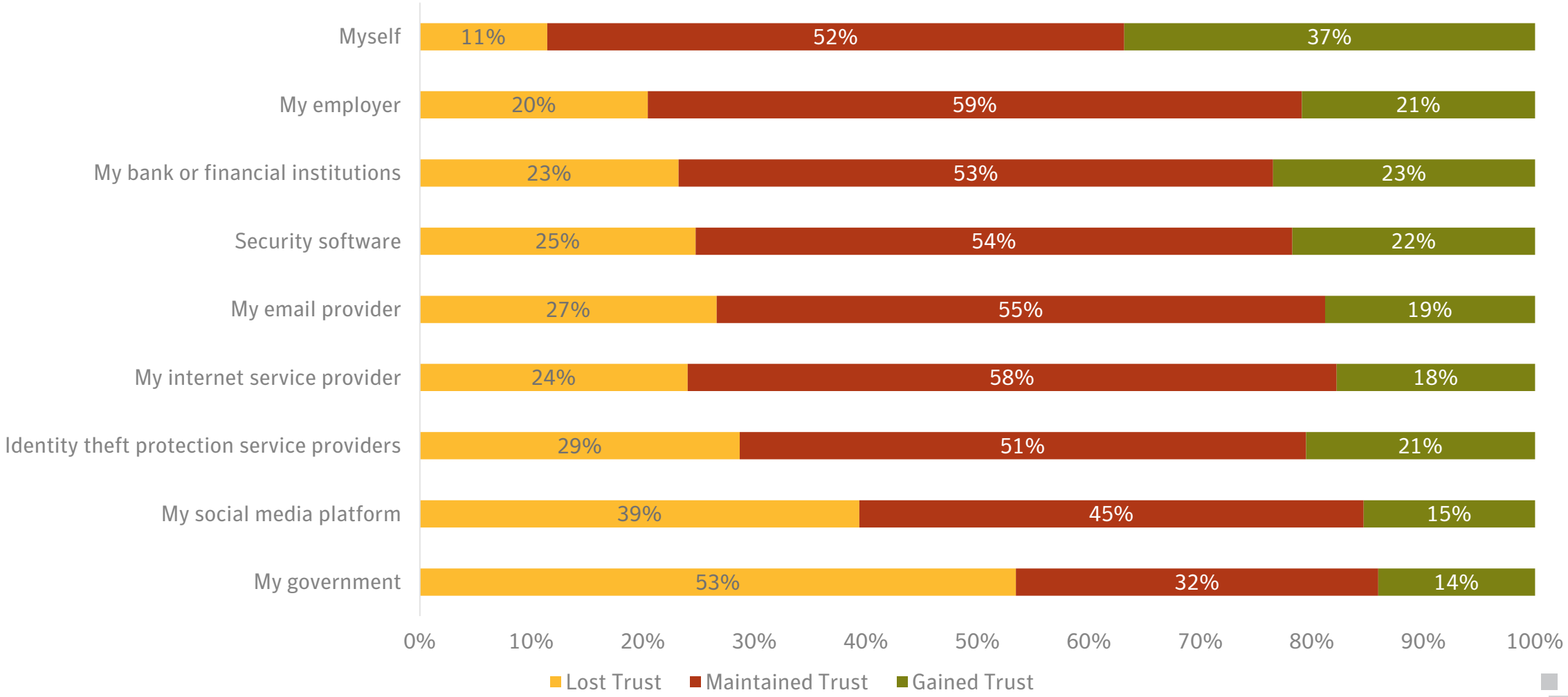


Copyright © 2018 Symantec Corporation

State of Consumers' Trust

Copyright © 2018 Symantec Corporation

Americans generally continue to trust the institutions that manage their data and personal information



Copyright © 2018 Symantec Corporation

About the 2017 Norton Cyber Security Insights Report

Copyright © 2018 Symantec Corporation

About the 2017 Norton Cyber Security Insights Report

The Norton Cyber Security Insights Report is an online survey of 21,549 individuals ages 18+ across 20 markets, commissioned by Norton by Symantec and produced by research firm Reputation Leaders. The margin of error for the total sample is +/-.7%. The U.S. sample reflects input from 1,003 U.S. adults ages 18+. The margin of error is +/- 3.1% for the total U.S. sample. Data was collected Oct. 5 – Oct. 24, 2017 by Reputation Leaders.

Markets: 20

North America	Canada, USA
Europe & Middle East	France, Germany, Italy, Netherlands, Spain, Sweden, UAE, UK
Asia Pacific	Australia, China, Hong Kong, India, Indonesia, Japan, New Zealand, Singapore
Latin America	Brazil, Mexico

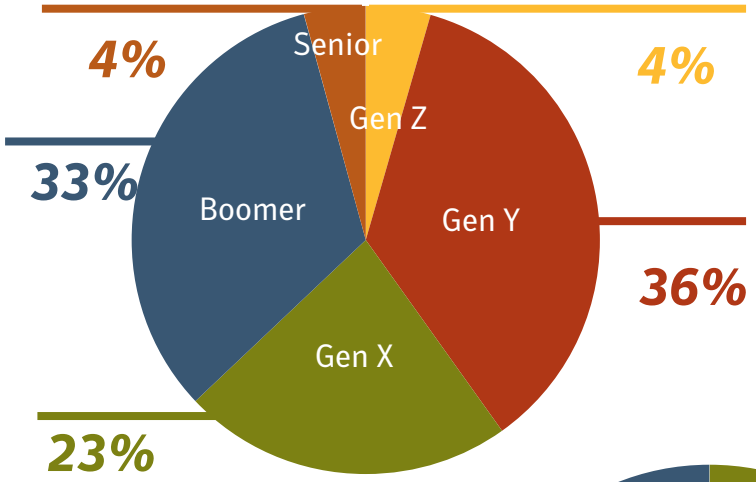
Copyright © 2018 Symantec Corporation

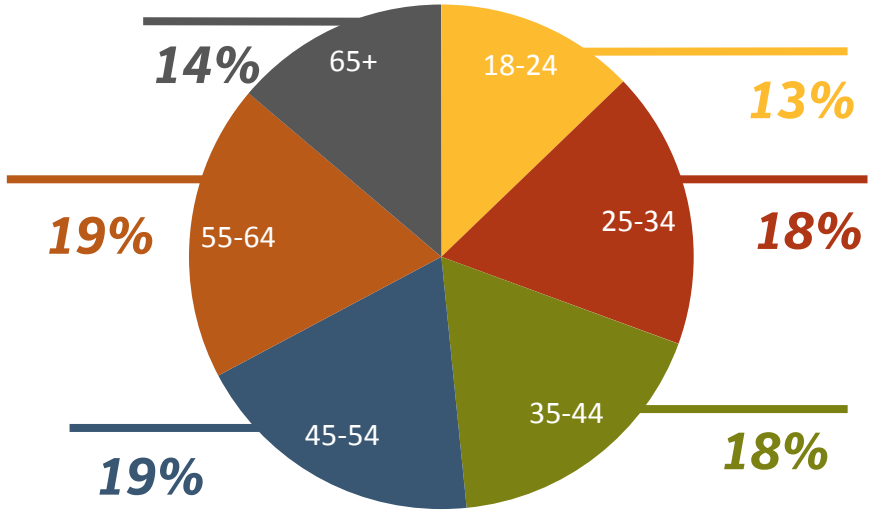
How We Define Cybercrime

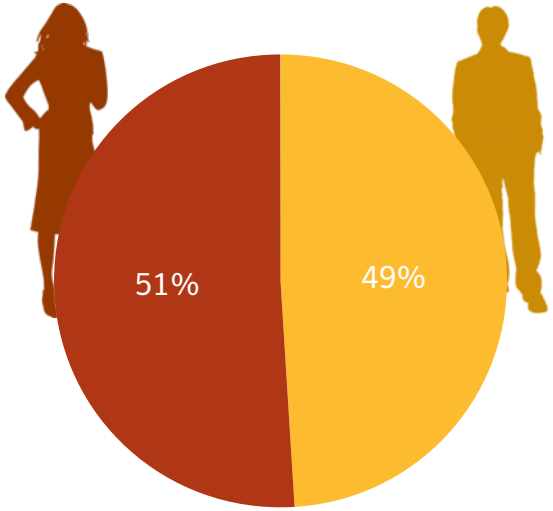
The definition of cybercrime continues to evolve as avenues open up that allow cybercriminals to target consumers in new ways. Each year, we will evaluate current cybercrime trends and update the report's methodology as needed, to ensure the Norton Cyber Security Insights Report provides an accurate snapshot of the impact of cybercrime as it stands today. In the 2017 Norton Cyber Security Insights Report, a cybercrime is defined as, but not limited to, a number of specific actions, including identity theft, credit card fraud or having your account password compromised. For the purposes of this report, a cybercrime victim is a survey respondent who confirmed one or more of these incidents took place. Visit https://www.symantec.com/about/newsroom/press-kits to learn more.

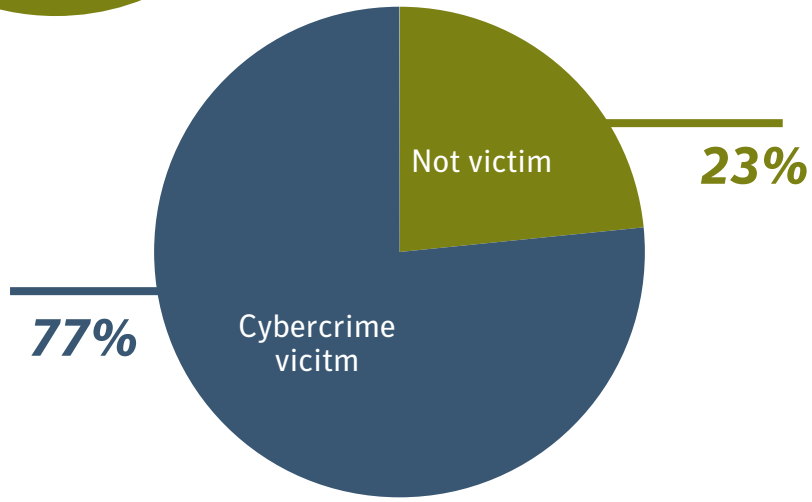
Copyright © 2018 Symantec Corporation

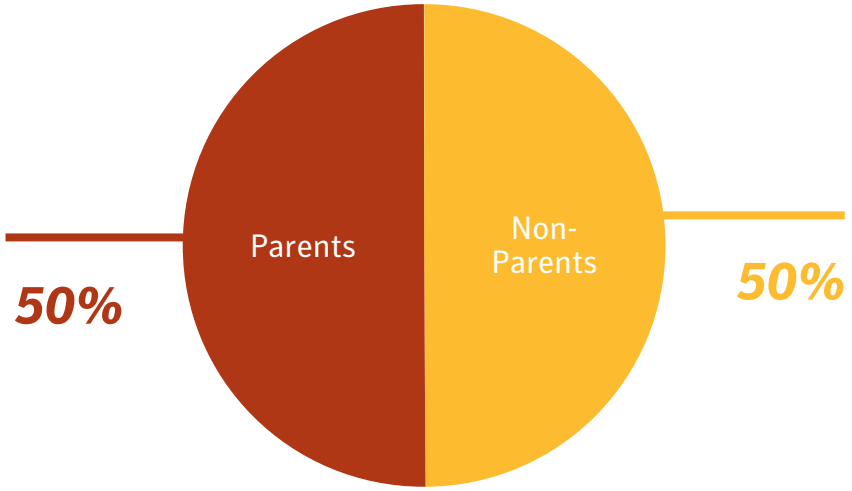
Demographics Breakdown











Copyright © 2018 Symantec Corporation