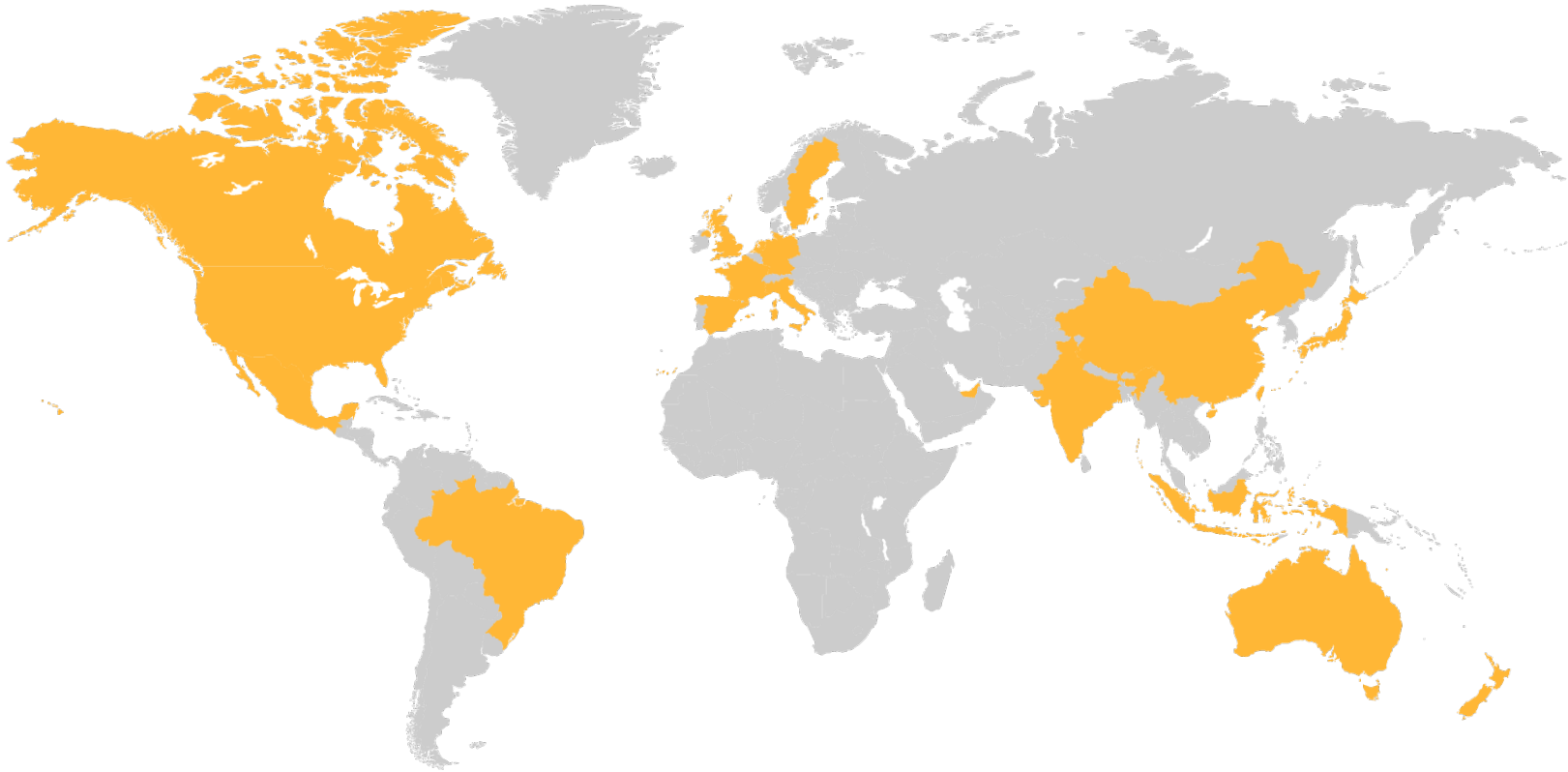
Norton by Symantec



2017

Norton Cyber Security Insights Report Global Results

Table of Contents

Key Findings

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.

- 978 million people in 20 countries were affected by cybercrime in 2017.
- 44% of consumers were impacted by cybercrime in the last 12 months.
- The most common cybercrimes experienced by consumers or someone they know include:
  - Having a device infected by a virus or other security threat (53%)
  - Experiencing debit or credit card fraud (38%)
  - Having an account password compromised (34%)
  - Encountering unauthorized access to or hacking of an email or social media account (34%)
  - 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 (32%)
- As a result, consumers who were a victims of cybercrime globally lost $172 billion – an average of $142 per victim – and nearly 24 hours globally (or almost three full work days) dealing with the aftermath.

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 Cybersecurity Prowess:** Consumers who've fallen victim to cybercrime, emphasize the importance of online security more than non-victims, yet they're more likely to contradict their efforts through simple missteps. While 44% of consumers have personally experienced cybercrime, 39% of cybercrime victims globally report gaining trust in their ability to hold and protect their personal information and data and 33% believe they're at a low risk of becoming a cybercrime victim.
- **Favor Multiple Devices:** Consumers who adopt the newest technologies and own the most devices are also more likely to be victims of cybercrime. More than one third (37%) own a gaming console and smart device, compared to 28% of non-victims. They're also almost twice as likely to own a connected home device than non-victims.
- **Dismiss the Basics:** They practice new security techniques such as fingerprint ID (44%), facial recognition (13%), pattern matching (22%), personal VPN (16%), voice ID (10%) and two-factor authentication (13%). Yet, 20% of cybercrime victims globally use the same password across all online accounts and 58% shared at least one device or account password with others. By comparison, only 17% of non-cybercrime victims use the same password across all online accounts and 37% share their passwords with others.

Key Findings

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

- Confession: Millennials are the most technologically savvy – owning the most devices (four devices on average) and adopting advanced security practices (32%) such as pattern matching, face recognition, VPN, voice ID and two-factor authentication, yet they make simple security mistakes such as bad password management (70%) and become a cybercrime victim, with 60% globally experiencing a cybercrime in the last year alone. :
  - One in four (26%) of Millennials use the same password for all accounts, compared to 10% of Baby Boomers.
  - 63% of Millennials globally have shared at least one or more of their passwords with another person, compared to 36% of Baby Boomers.
- Confession: Baby Boomers and Seniors are generally the safest age groups, though they make faux pas as well:
  - 61% of Baby Boomers and two-thirds of Seniors globally use different passwords, but 39% of Baby Boomers and 49% of Seniors write those passwords down on a piece of paper.
  - Globally. Seniors are least likely to back up their devices, with 16% failing to back up any devices.
  - Notably, Baby Boomers globally lost an average of $167 – the highest of all age groups and 15 percent higher than the global average.
- Confession: Parents are worried about many things when it comes to their child and the Internet – but few act. 96% of parents globally worry about their children and the Internet, yet only a third of parents always supervise their children online when they are playing online games, using social media or surfing the internet. Meanwhile, 11% of parents globally do not take any actions to protect their children online.

Key Findings

Consumers' boundaries skewed between cybercrime and "real life"

- Confession: While 81% of consumers globally think a cybercrime should be treated as a criminal act, 43% believe it's acceptable to commit morally questionable online behaviors in certain instances:
  - One fourth (26%) of consumers globally say reading someone's emails without their consent is sometimes acceptable
  - 21% of consumers globally believe using a false email or someone else's email to identify their self online is sometimes acceptable
  - 15% of consumers globally believe that accessing someone's financial accounts without their permission is sometimes acceptable
- Interestingly, 53 percent of cybercrime victims globally were more likely to think it was acceptable to commit morally questionable online behavior than non-victims (32%):
  - 31% of cybercrime victims globally say reading someone's emails without their consent is sometimes acceptable compared to 18% of non-victims
  - 25% of cybercrime victims globally believe falsely identifying themselves is sometimes acceptable compared to 14% of non-victims
  - 18% of cybercrime victims globally believe that accessing someone's financial accounts without their permission is sometimes acceptable compared to 10% of non-victims

Key Findings

Despite this year's cyberattacks, consumers continue to trust the institutions that manage their data and personal information; though, they have lost trust in their government.

- Consumers globally have gained or maintained the same level of trust in the following institutions that manage their data and personal information:
  - 76% in identity theft protection services
  - 80% in internet service providers
  - 80% in email providers
  - 82% in financial institutions
- Concerningly, however, 41% of consumers globally lost trust in their government to manage their data and personal information.

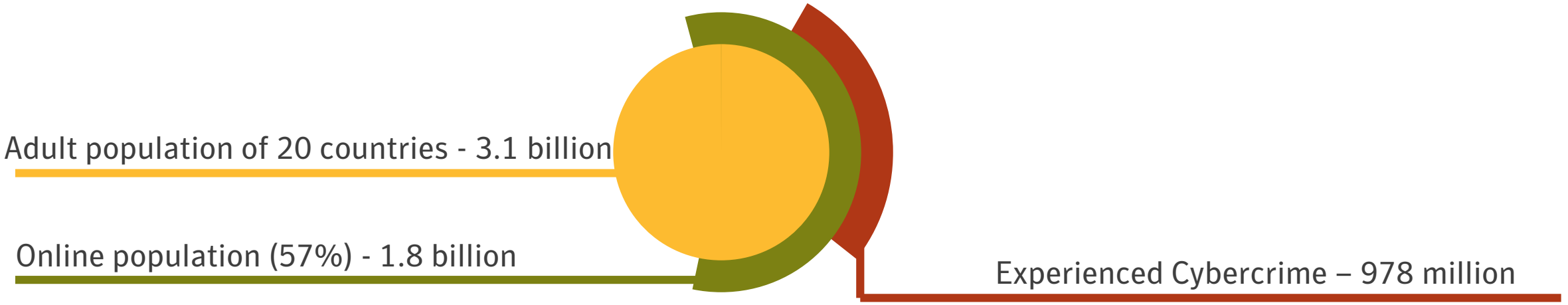
What to Do?

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 the perfect password:** Don't tie your password to publicly available information as it makes it easier for the bad guys to guess your password. Be sure to use a phrase that consists of a string of words that are easy to memorize but hard for anyone else to crack. The longer your password, the better it is. Additionally, if your account or device enables it, consider two-factor authentication for an additional layer of security. That way, if your password is compromised, it's harder for the hacker to access your account. Finally, once you've created a strong password, stick with it until you're notified of a security breach. If you still feel overwhelmed, use a password manager to help!
- **Know the ins and out of public Wi-Fi networks:** Accessing personal information on unprotected public Wi-Fi is like broadcasting your entire screen on TV – everything you do on a website or through an app, could potentially be exposed. Avoid anything that involves sharing your personal information (paying a bill online, logging in to social media accounts, paying for anything with a credit card, etc.). If you must access the information over public Wi-Fi, consider using a Virtual Private Network (VPN) to secure your connection and help keep your information private.
- **Don't keep a (dis)connected home:** When installing a new network-connected device, such as a router or smart thermostat, remember to change the default password. If you don't plan on using the Internet feature(s), such as with smart appliances, disable or protect remote access when not needed. Also, protect your wireless connections with strong Wi-Fi encryption so no one can easily view the data traveling between your devices.
- **Don't go on a phishing expedition:** Think twice before opening unsolicited messages or attachments, particularly from people you don't know, or clicking on random links. The message may be from a cybercriminal who has compromised your friend or family member's email or social media accounts**.**
- **Be in control when online:** Protect all your devices with a robust, multi-platform security software solution to help protect against the latest threats.

Cybercrime by the Numbers

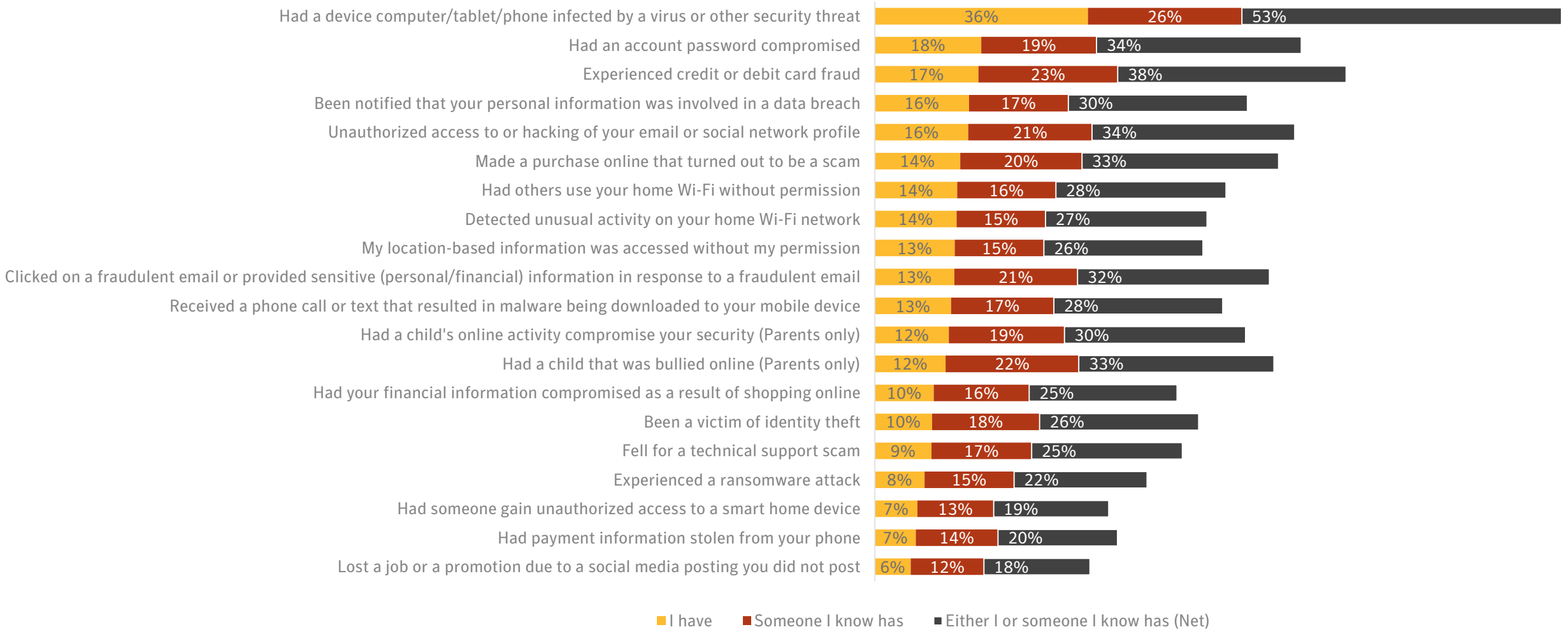
Within the last year, more than 978 million adults in 20 countries globally experienced cybercrime



Millions unless noted:

	Australia	Brazil	Canada	China	France	Germany	Hong Kong	India	Indonesia	Italy	Japan	Mexico	Netherlands	New Zealand	Singapore	Spain	Sweden	UAE	UK	USA
2017	6.09	62.21	10.14	352.70	19.31	23.36	2.41	186.44	59.45	16.44	17.74	33.15	3.43	1.14	1.26	16.20	2.09	3.72	17.40	143.70

53% of consumers experienced cybercrime or know someone who has



Consumers who were victims of cybercrime globally lost $172 billion

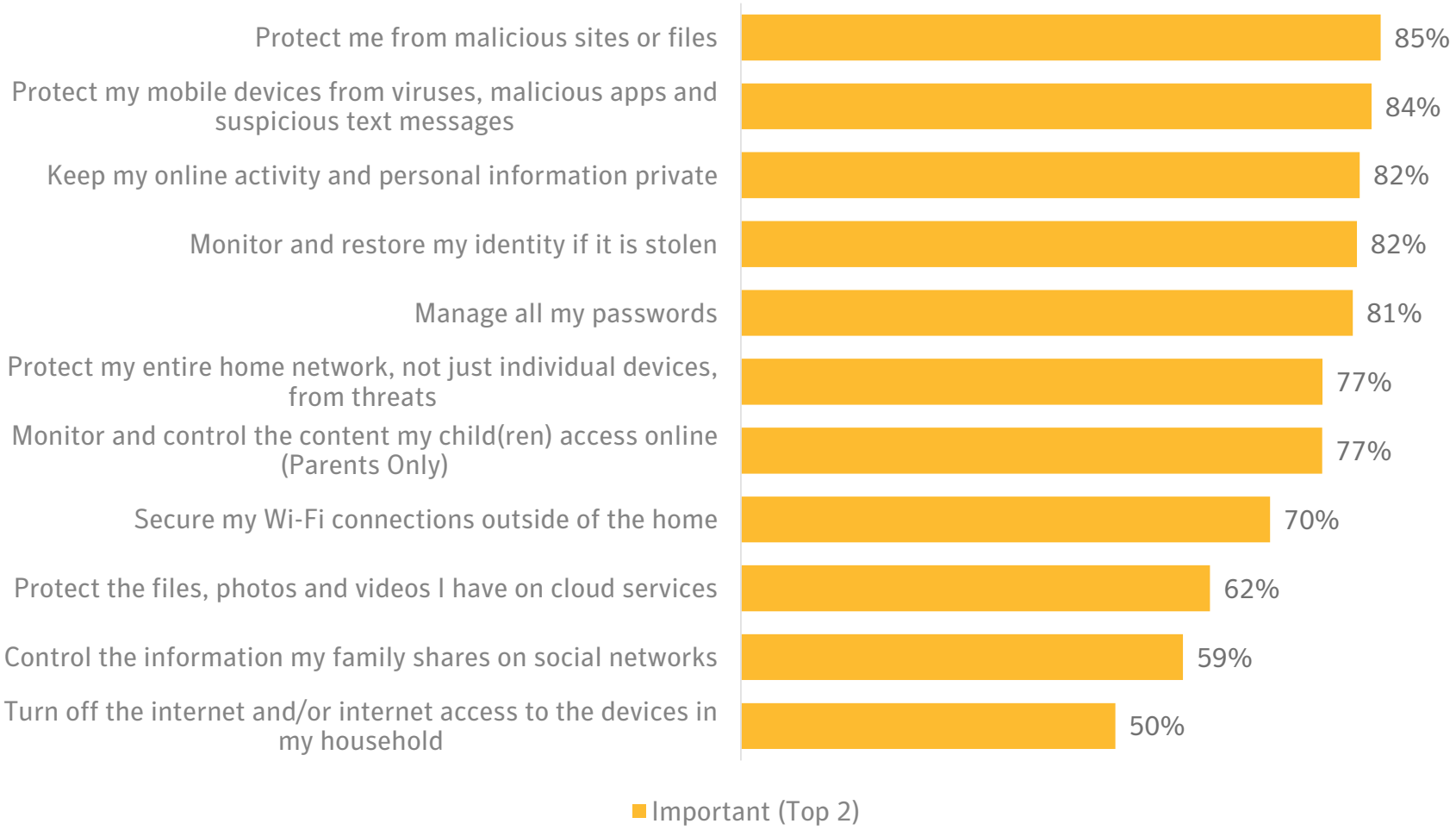
Figures represented in billions (USD):

	Australia	Brazil	Canada	China	France	Germany	Hong Kong	India	Indonesia	Italy	Japan	Mexico	Netherlands	New Zealand	Singapore	Spain	Sweden	UAE	UK	USA
2017	$1.9	$22.5	$1.5	$66.3	$7.1	$2.6	$0.1	$18.5	$3.2	$4.1	$2.1	$7.7	$1.6	$0.1	$0.4	$2.1	$3.9	$1.1	$6.0	$19.4

The average cybercrime victim spent nearly **24 hours (23.6 hours) globally (or almost three full work days)** dealing with the aftermath

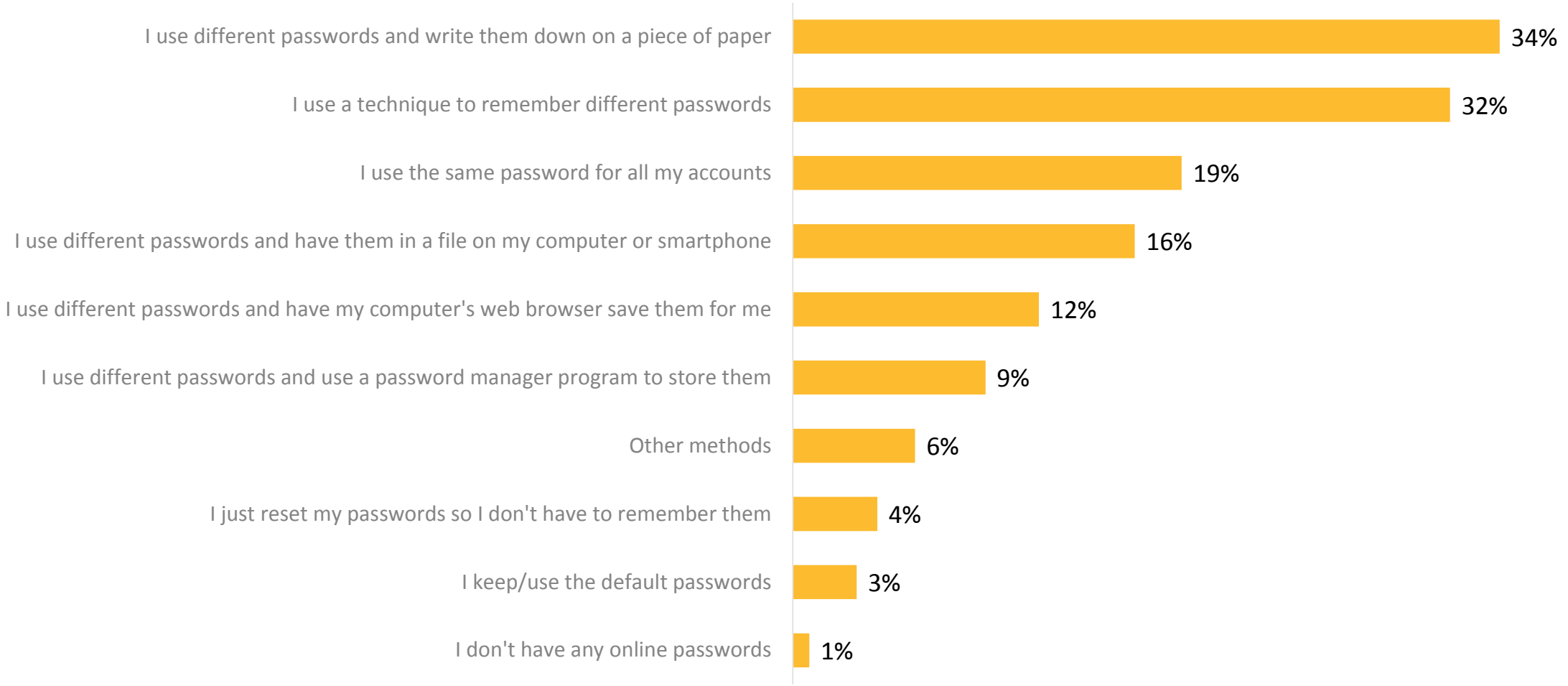
	Australia	Brazil	Canada	China	France	Germany	Hong Kong	India	Indonesia	Italy	Japan	Mexico	Netherlands	New Zealand	Singapore	Spain	Sweden	UAE	UK	USA
2017	16.2	33.9	10.3	28.3	16.0	14.6	18.9	50.7	34.1	19.2	5.6	55.1	5.6	9.0	14.6	22.1	22.0	47.9	14.8	19.8

Consumers emphasize the importance of online security



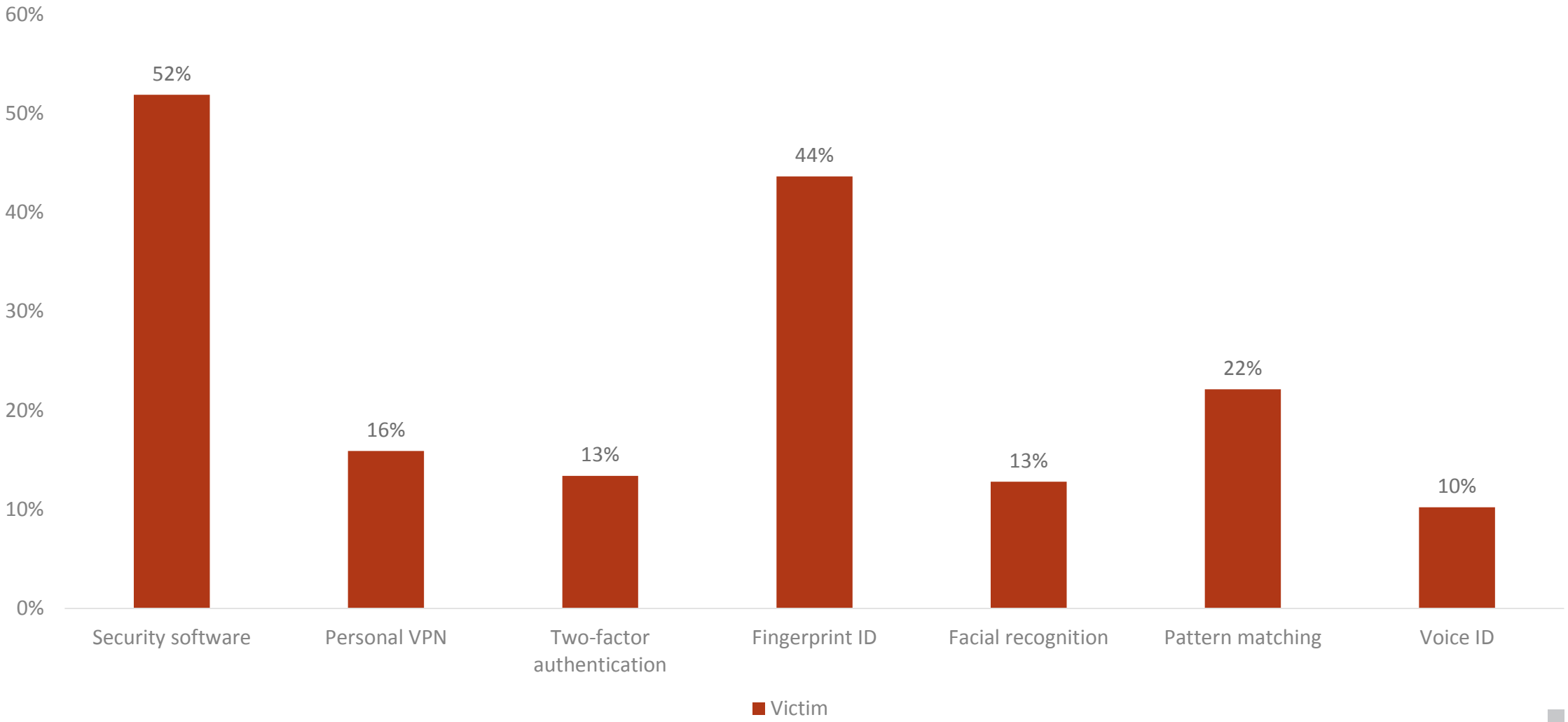
PROTECTION from malicious threats is the biggest concern

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

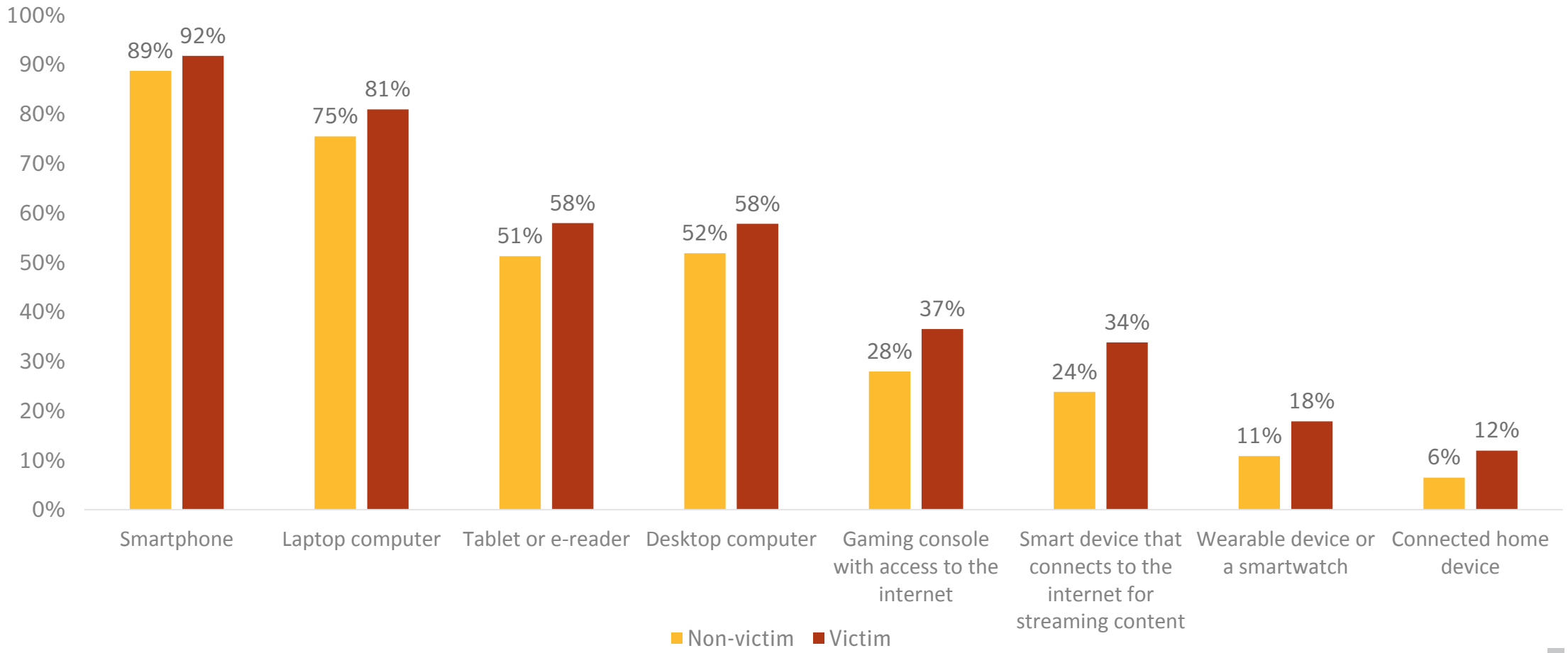


Portrait of a Cybercrime Victim

They’re adopters of newer security techniques



And almost 2x as likely to own a connected home device than non-cybercrime victims.



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.

20%

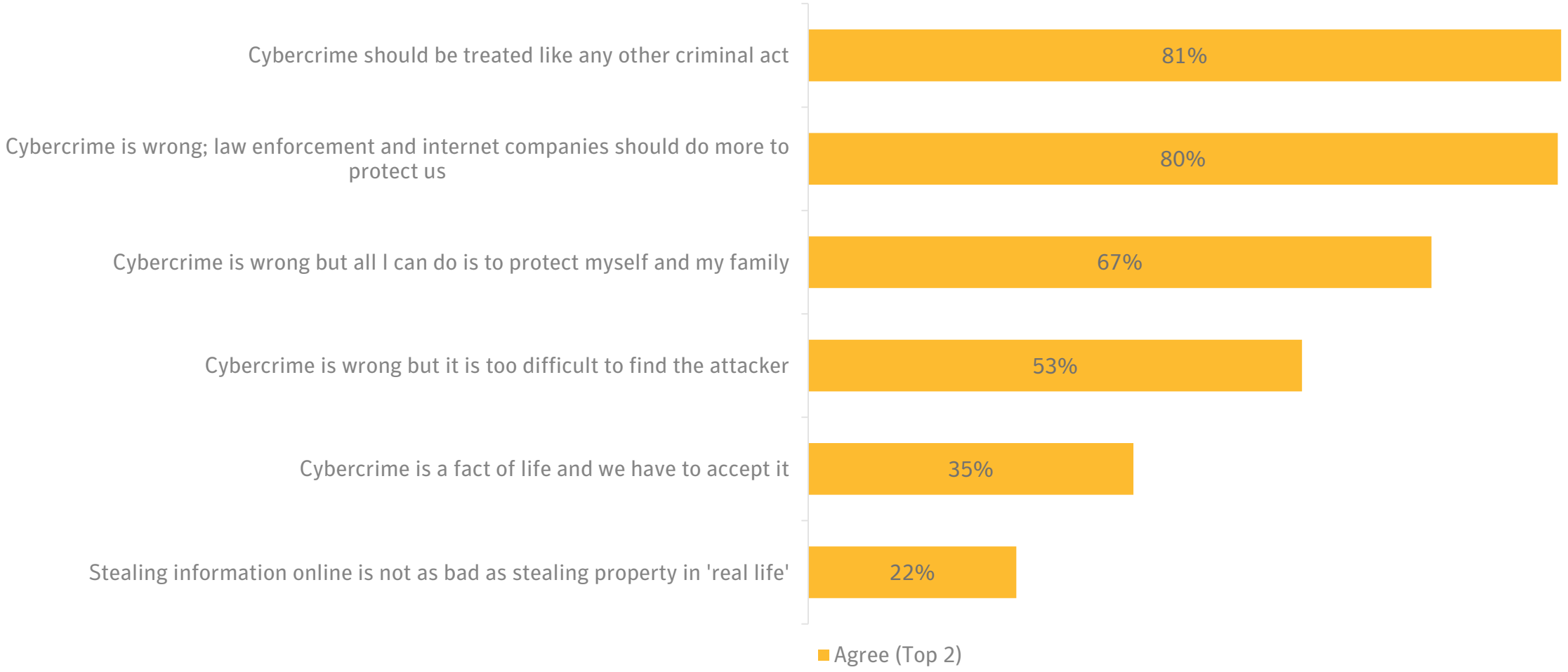
of cybercrime victims globally use the same online password across all online accounts

58%

of cybercrime victims shared at least one device or account password with others

Consumers' Contradicting Beliefs

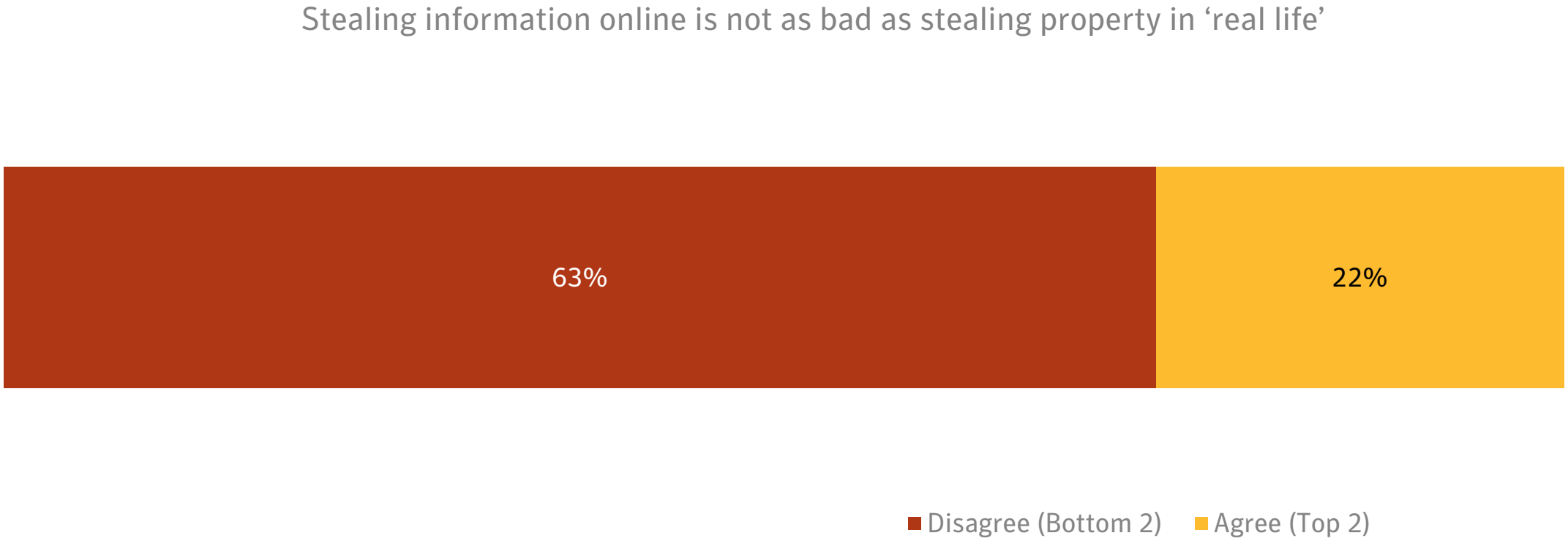
Consumers believe cybercrime is wrong and should be treated as a criminal act



Yet 43 percent believe it's sometimes acceptable to commit morally questionable online behaviors in certain instances

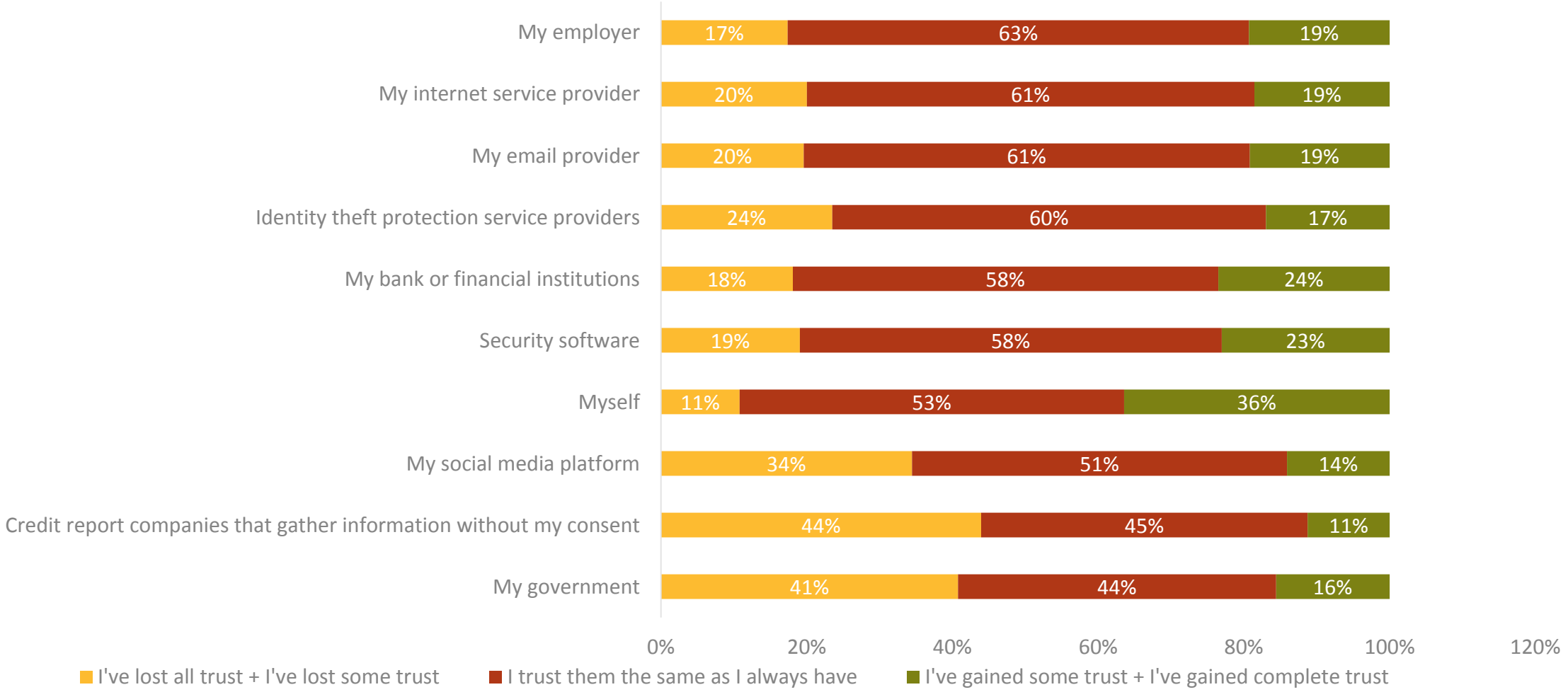
43%
believe at least one type of cybercrime is always or sometimes acceptable

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



State of Consumers' Trust

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



About the 2017 Norton Cyber Security Insights Report

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%. Data was collected Oct. 5 – Oct. 24, 2017 by Reputation Leaders.

Markets: 20

North America	Canada, United States
Europe & Middle East	France, Germany, Italy, Netherlands, Spain, Sweden, United Arab Emirates, United Kingdom
Asia Pacific	Australia, China, Hong Kong, India, Indonesia, Japan, New Zealand, Singapore
Latin America	Brazil, Mexico

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.

Demographics Breakdown