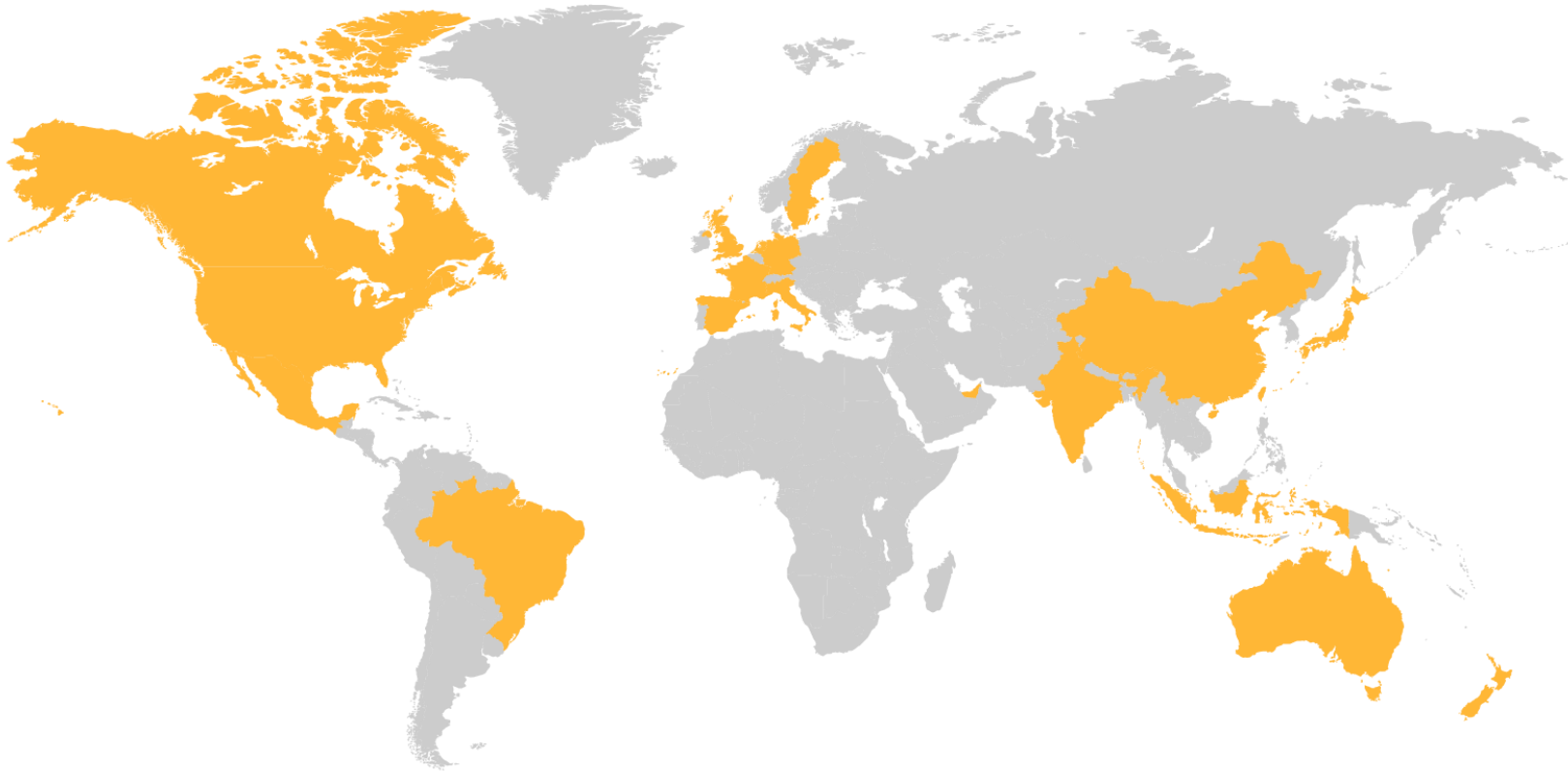
Norton by Symantec



2017
Norton Cyber Security Insights Report Global Results

Key Findings

Key Findings

- **When it comes to cybersecurity, 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**

- **Cybercrime victims share common traits: they are everyday consumers who express confidence and use multiple devices whether at home or on the go, but they have a blind spot when it comes to the basics**

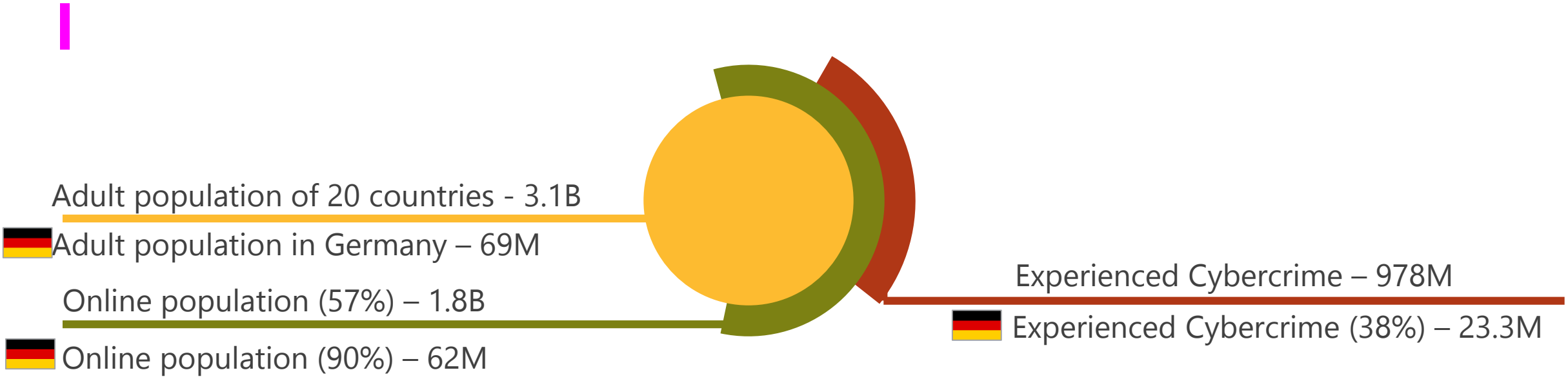
- **Ransomware continues to wreak havoc: despite paying up, many don’t get their digital life back**

- **Consumers’ boundaries skewed between cybercrime and “real life”**

- **With last year’s headline cyberattacks, consumer trust varies in regards to the institutions that manage their data and personal information**

Cybercrime by the Numbers

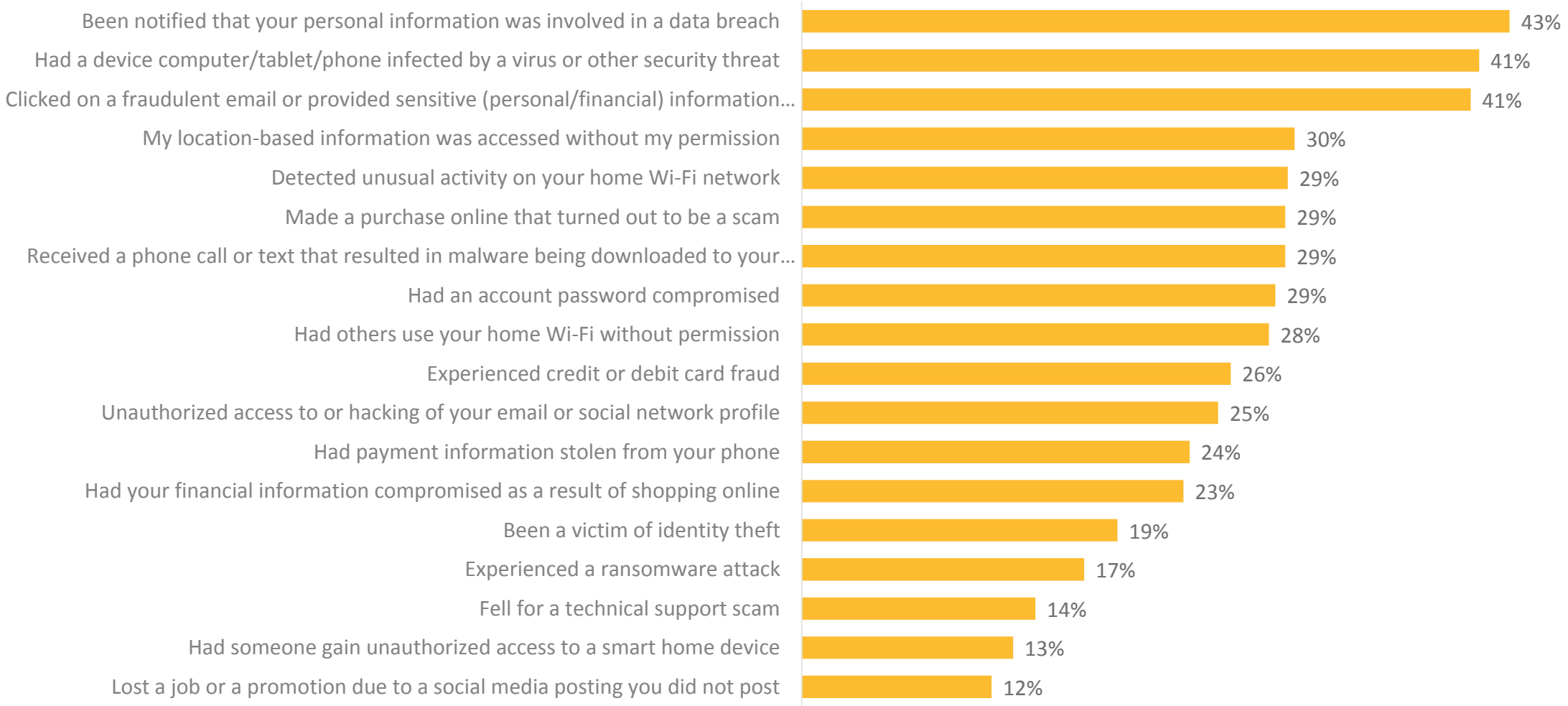
Within the last year, more than 978 million adults in 20 countries globally experienced cybercrime



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

38% of German consumers have personally experienced cybercrime in the past year

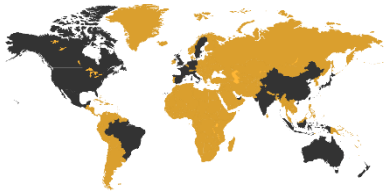


Events experienced in the past year (among those who have ever been impacted by cybercrime)

The total financial cost of cybercrime in Germany totaled more than $2.5B (€2.2B) in the past year, compared to $172B (€146.3B) globally

At least 63% of German consumers' reported financial loss was not reimbursed

Average loss per victim
$54
(€46)

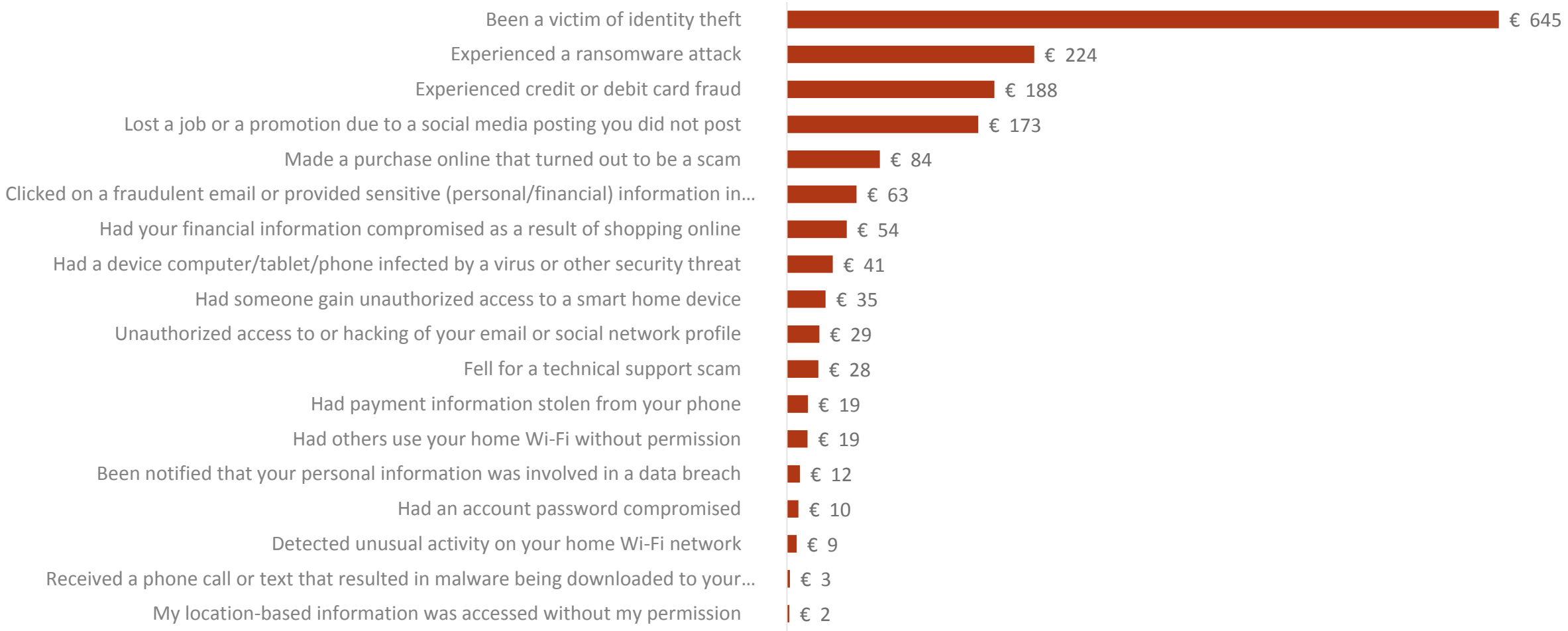


Average loss per victim
$142
(€121)

Total losses per country. Figures represented in billions (USD):

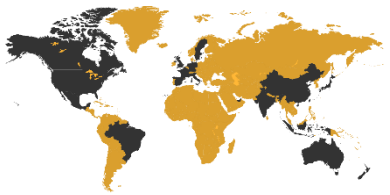
	Australia	Brazil	Canada	China	France	Germany	Hong Kong	India	Indonesia	Italy	Japan	Mexico	Netherlands	New Zealand	Singapore	Spain	Sweden	UAE	UK	USA
2017	$1.9	$22.5	$1.5	$66.3	$7.1	$2.6	$0.1	$18.5	$3.2	$4.1	$2.1	$7.7	$1.6	$0.1	$0.4	$2.1	$3.9	$1.1	$6.0	$19.4

German consumers reported the highest financial loss in the past year after the following incidents



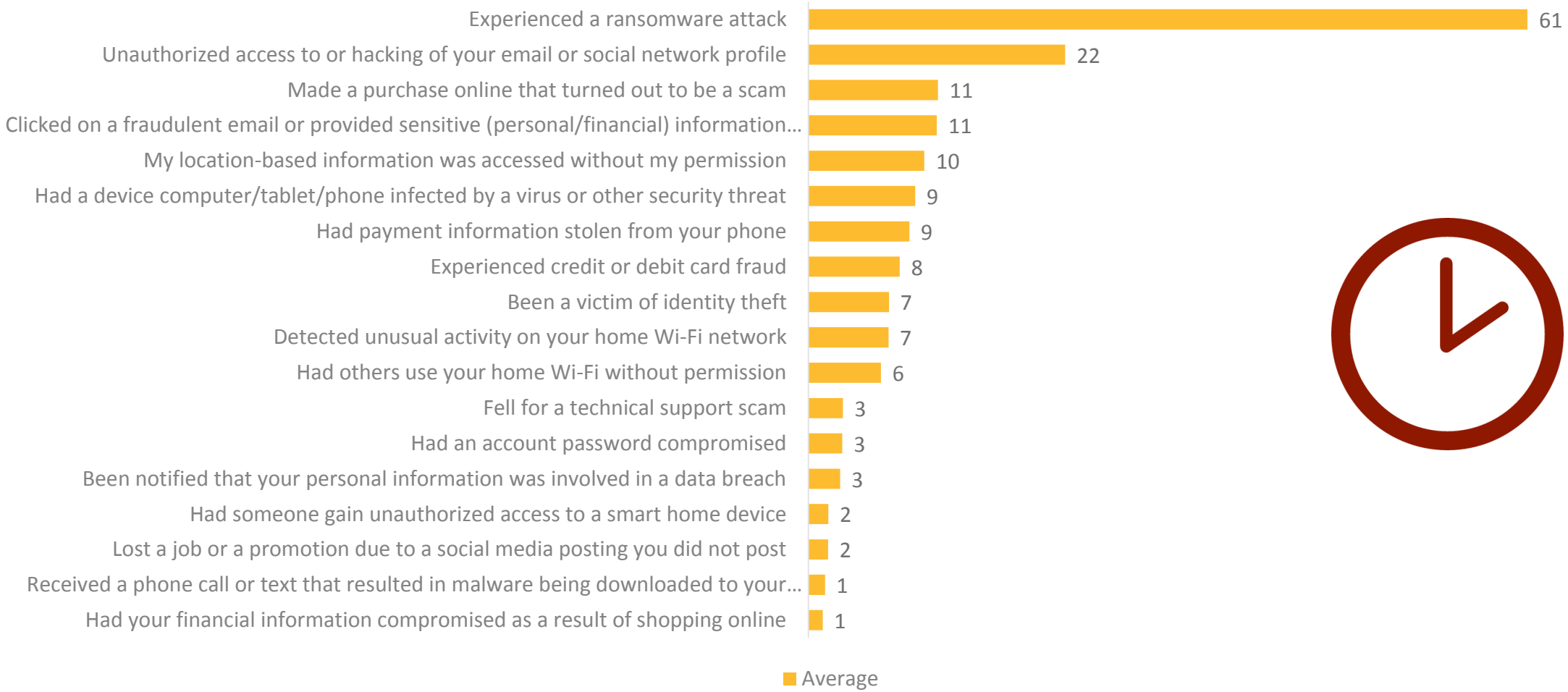
The average German cybercrime victim spent 14.6 hours (nearly two working days) dealing with the aftermath

	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

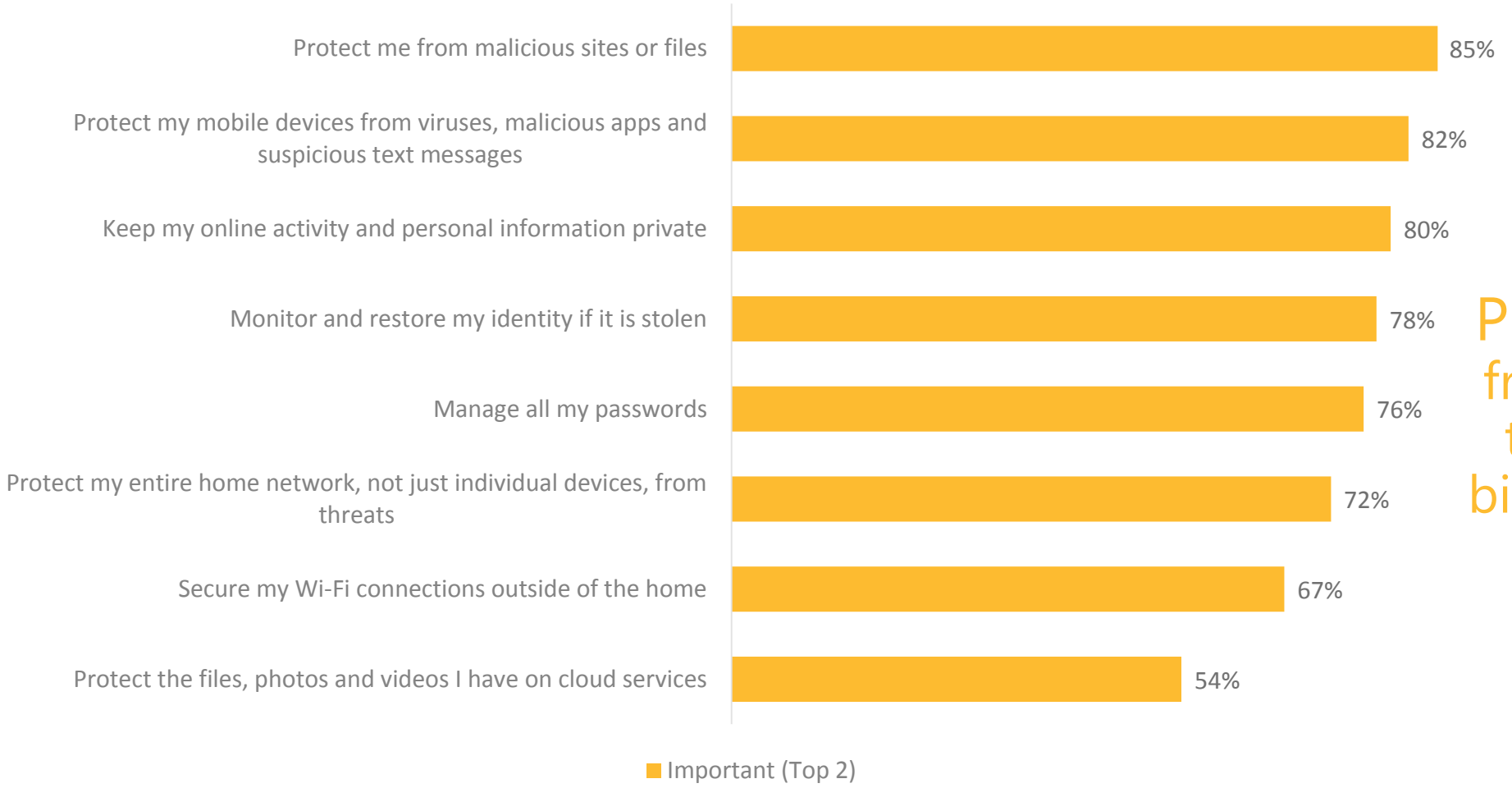


The average global cybercrime victim spent 23.6 hours (nearly three full work days)

Average time lost per incident

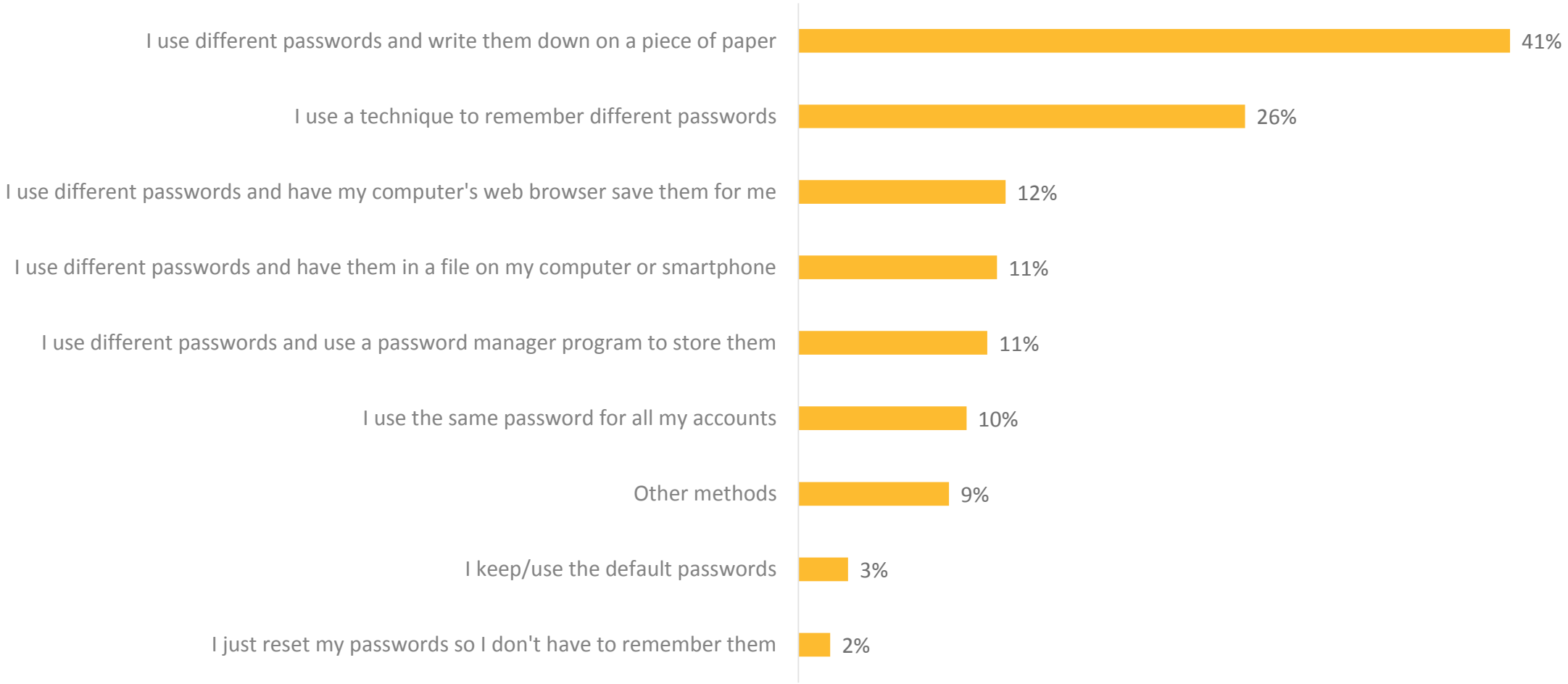


German consumers emphasize the importance of online security



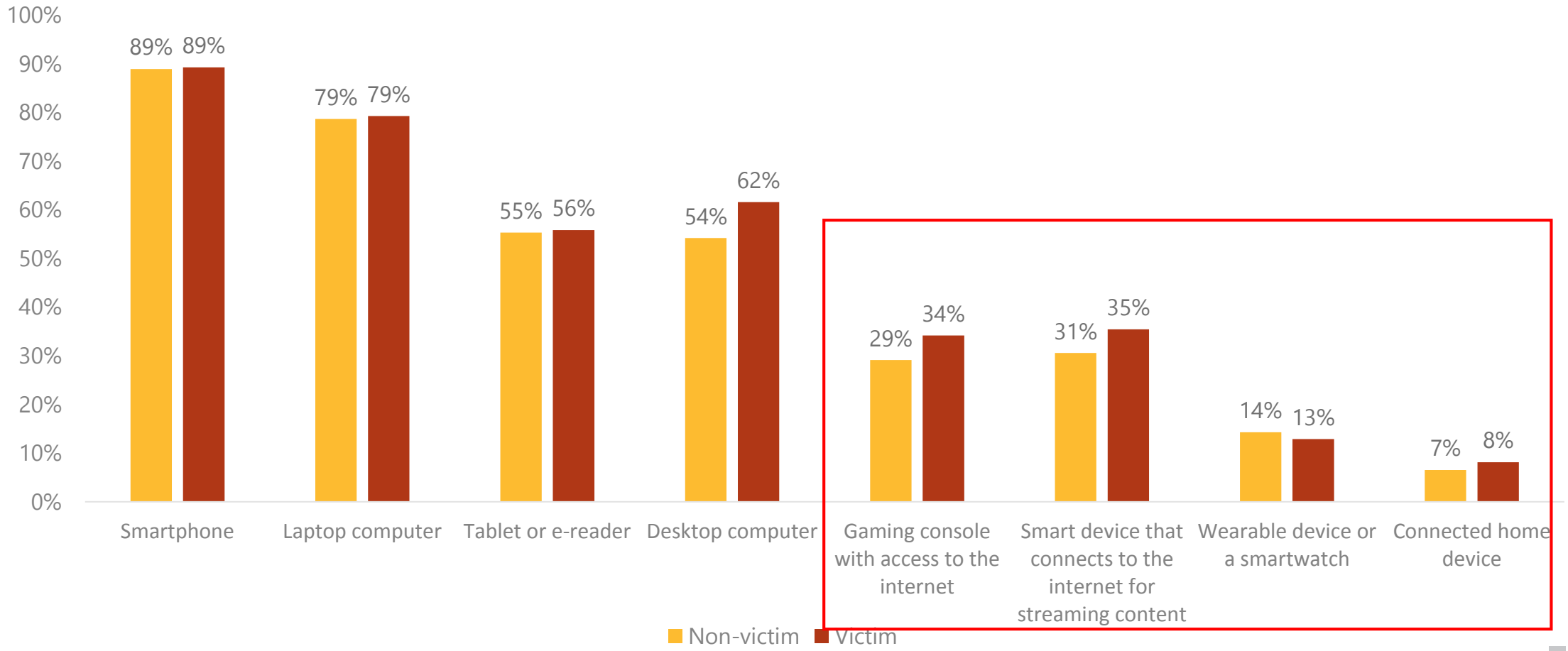
PROTECTION from malicious threats is the biggest concern

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

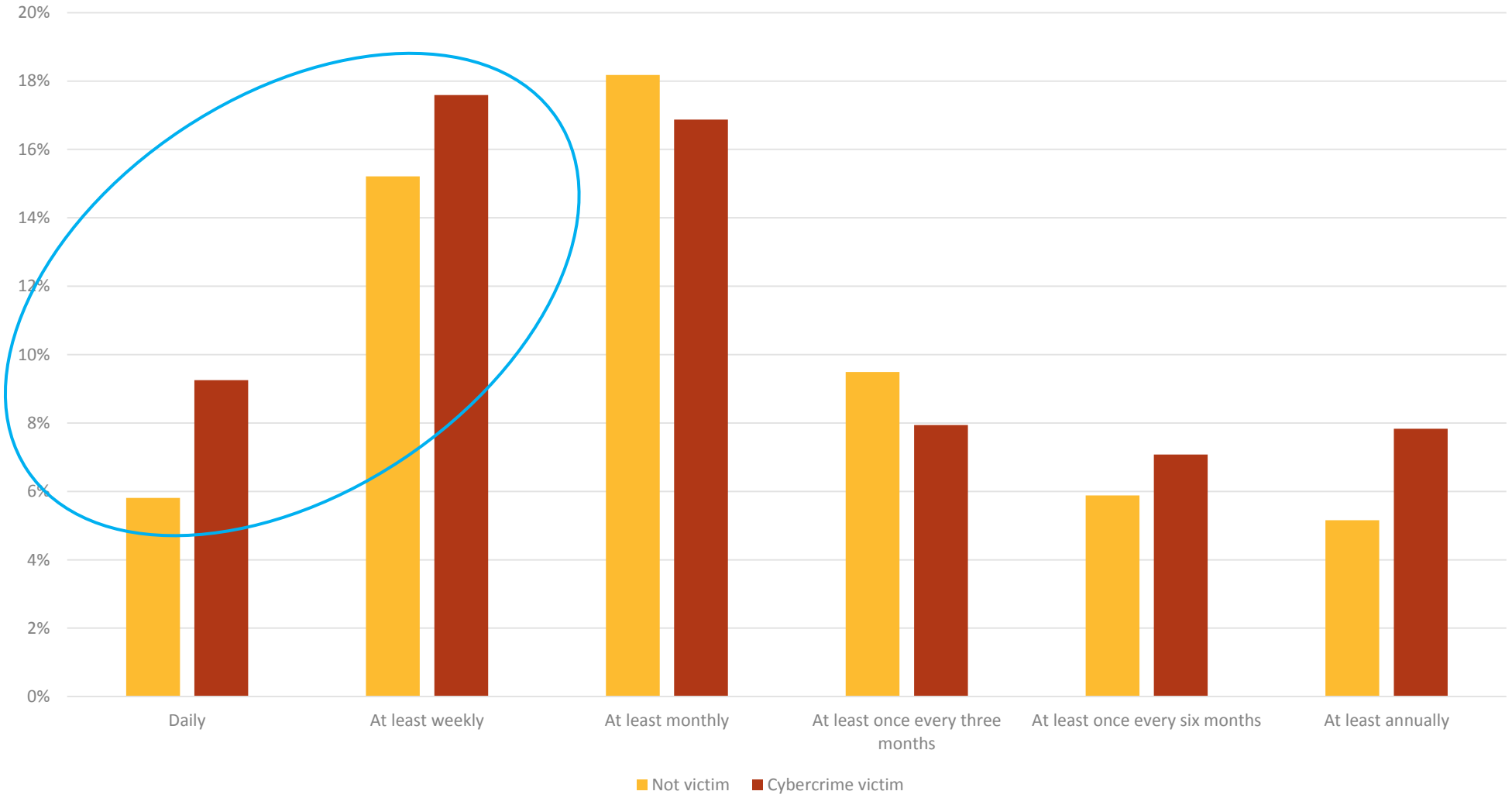


Portrait of a Cybercrime Victim

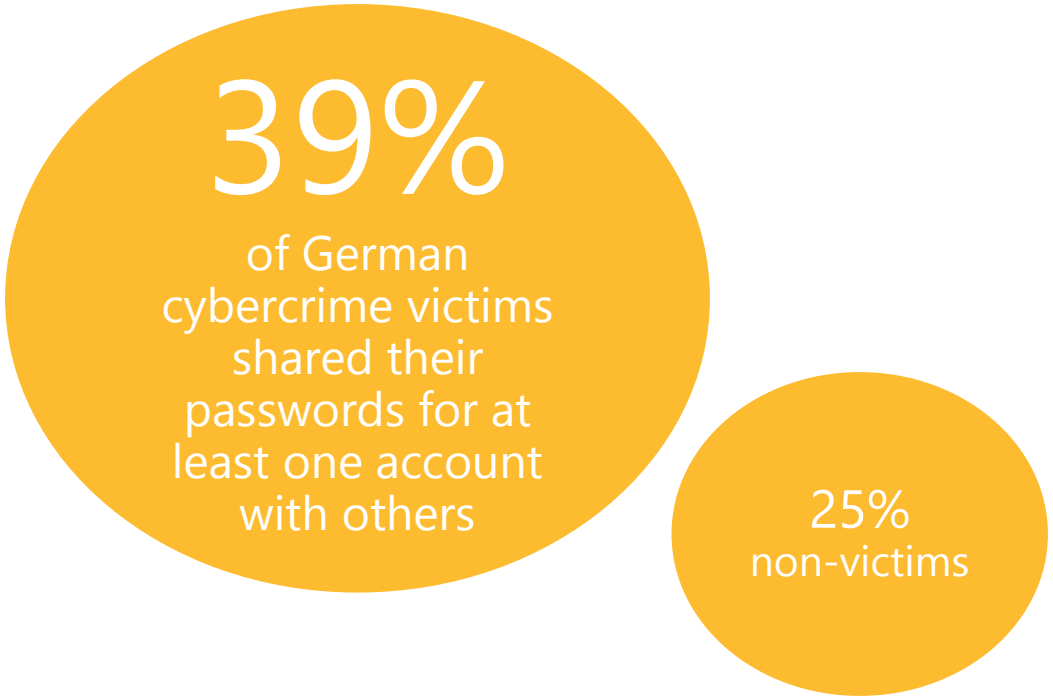
They are technology enthusiasts – more likely to own a connected gaming, or smart devices than non-cybercrime victims.



They also shop via mobile when away from home far more regularly than their crime-free counterparts



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

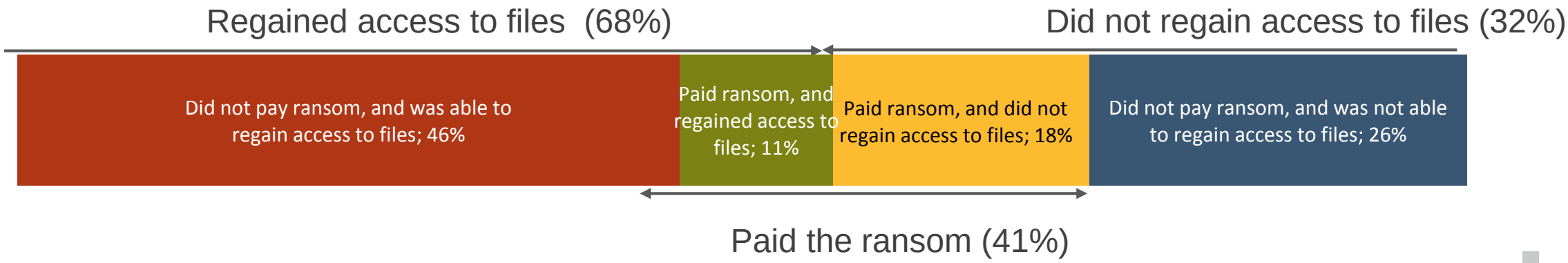


Ransomware Wreaks Havoc

Ransomware Wreaks Havoc: One in fourteen online adults have had their digital files held for ransom

On average, €224 and 61 hours lost following a ransomware attack

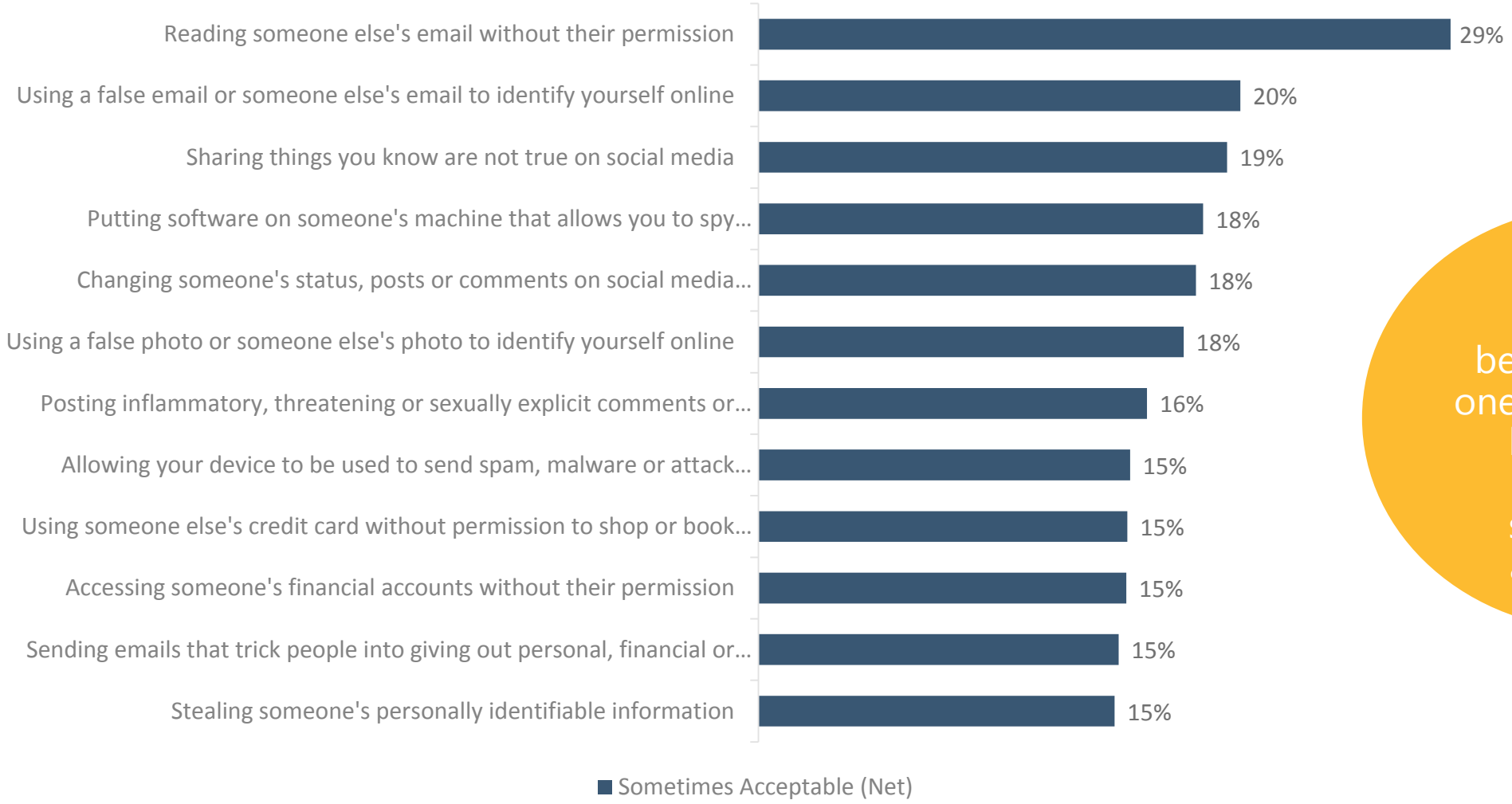
Despite paying up, 1 in 10 did not get their digital life back



Consumers' Contradicting Beliefs

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

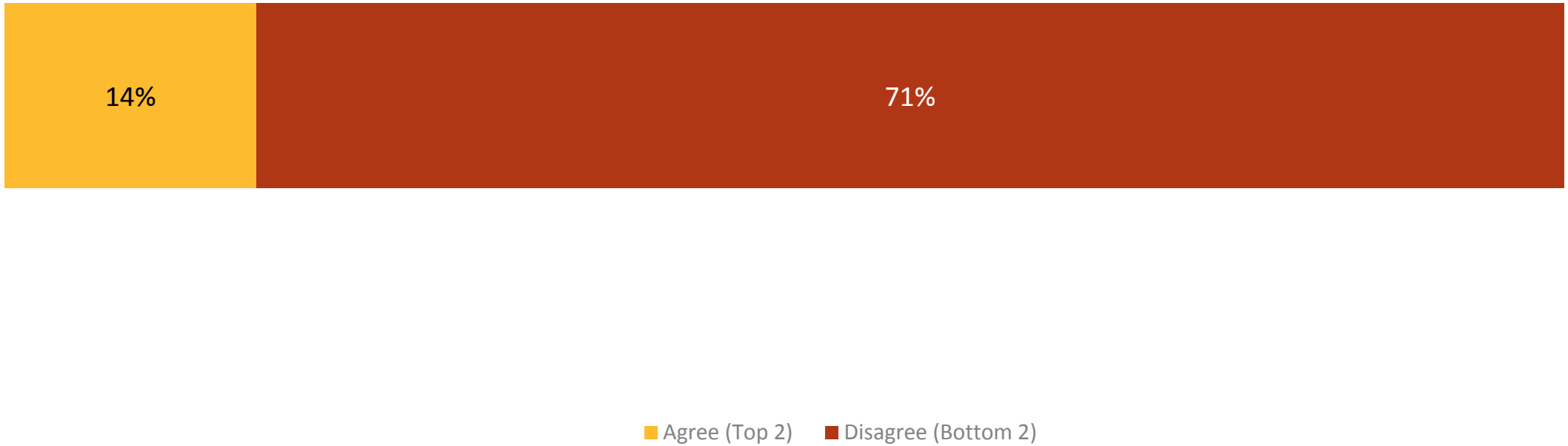
Yet 41 percent believe it's sometimes or always acceptable to commit questionable online behaviors in certain instances



41%
believe at least one questionable behavior is always or sometimes acceptable

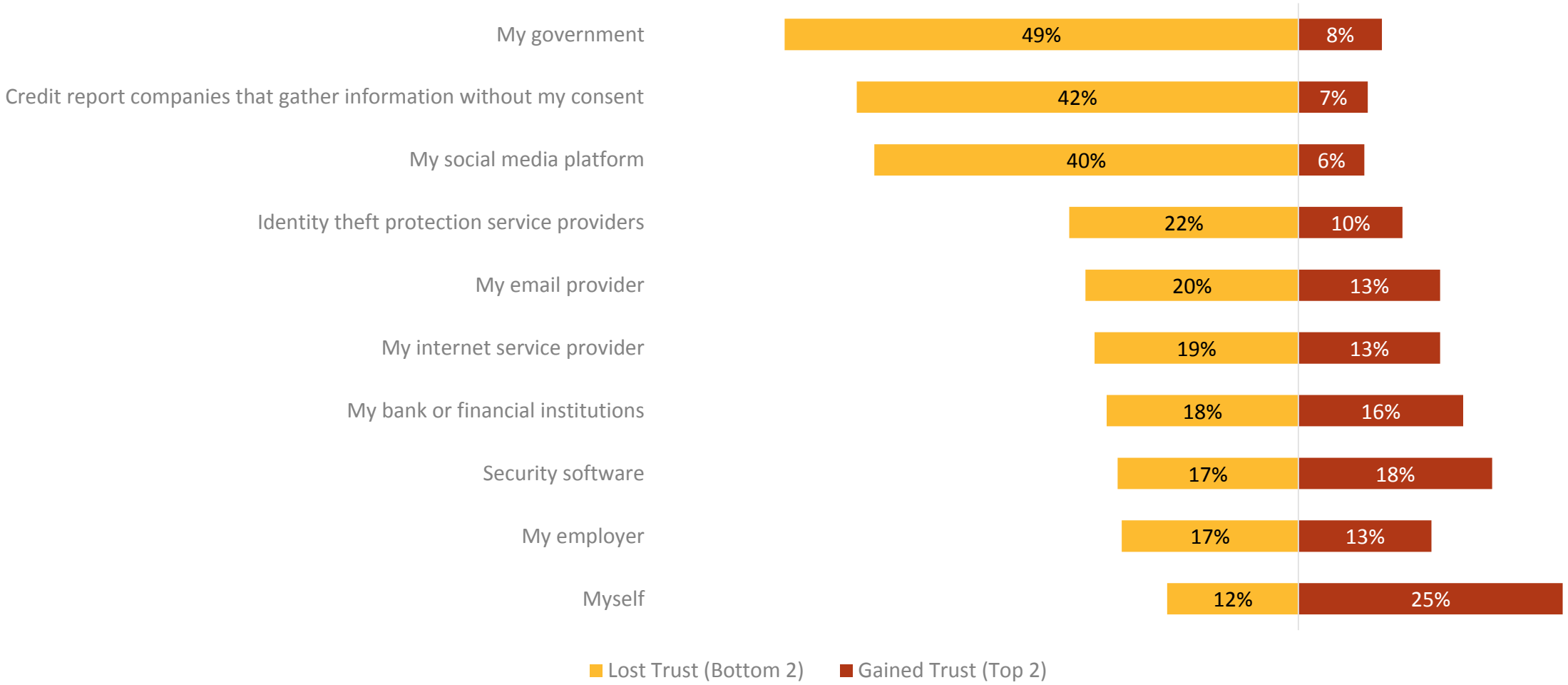
One in seven believe stealing information online is not as bad as stealing property in ‘real life’

Stealing information online is not as bad as stealing property in ‘real life’



State of Consumers' Trust

German consumers' trust varies when it comes to the institutions that 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 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. Consider two-factor authentication for an additional layer of security. 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.

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:

- 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.

Appendix

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, 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

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.