2017 Norton Cyber Security Insights Report
Global Results
Table of Contents

1. Key Findings 3 – 9
2. Cybercrime by the Numbers 10 – 16
3. Portrait of a Cybercrime Victim 17 – 20
4. Consumers’ Contradicting Beliefs 21 – 24
5. State of Consumers’ Trust 25 – 26
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:
  o Having a device infected by a virus or other security threat (53%)
  o Experiencing debit or credit card fraud (38%)
  o Having an account password compromised (34%)
  o Encountering unauthorized access to or hacking of an email or social media account (34%)
  o Making a purchase online that turned out to be a scam (33%)
  o 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. :
  o One in four (26%) of Millennials use the same password for all accounts, compared to 10% of Baby Boomers.
  o 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:
  o 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.
  o Globally. Seniors are least likely to back up their devices, with 16% failing to back up any devices.
  o 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:
  o One fourth (26%) of consumers globally say reading someone’s emails without their consent is sometimes acceptable
  o 21% of consumers globally believe using a false email or someone else's email to identify their self online is sometimes acceptable
  o 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%):
  o 31% of cybercrime victims globally say reading someone’s emails without their consent is sometimes acceptable compared to 18% of non-victims
  o 25% of cybercrime victims globally believe falsely identifying themselves is sometimes acceptable compared to 14% of non-victims
  o 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:
  o 76% in identity theft protection services
  o 80% in internet service providers
  o 80% in email providers
  o 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

Adult population of 20 countries - 3.1 billion

Online population (57%) - 1.8 billion

Experienced Cybercrime – 978 million

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Australia</td>
<td>6.09</td>
<td>6.17</td>
<td>6.25</td>
<td>6.33</td>
<td>6.41</td>
<td>6.49</td>
</tr>
<tr>
<td>Brazil</td>
<td>62.21</td>
<td>62.81</td>
<td>63.41</td>
<td>63.94</td>
<td>64.47</td>
<td>64.99</td>
</tr>
<tr>
<td>Canada</td>
<td>10.14</td>
<td>10.25</td>
<td>10.36</td>
<td>10.47</td>
<td>10.58</td>
<td>10.69</td>
</tr>
<tr>
<td>China</td>
<td>352.70</td>
<td>354.20</td>
<td>355.70</td>
<td>357.20</td>
<td>358.70</td>
<td>360.20</td>
</tr>
<tr>
<td>Germany</td>
<td>23.36</td>
<td>23.44</td>
<td>23.52</td>
<td>23.60</td>
<td>23.68</td>
<td>23.76</td>
</tr>
<tr>
<td>Hong Kong</td>
<td>2.41</td>
<td>2.44</td>
<td>2.47</td>
<td>2.50</td>
<td>2.53</td>
<td>2.56</td>
</tr>
<tr>
<td>India</td>
<td>186.44</td>
<td>187.20</td>
<td>188.00</td>
<td>188.80</td>
<td>189.60</td>
<td>190.40</td>
</tr>
<tr>
<td>Indonesia</td>
<td>59.45</td>
<td>59.71</td>
<td>59.97</td>
<td>60.23</td>
<td>60.49</td>
<td>60.75</td>
</tr>
<tr>
<td>Italy</td>
<td>16.44</td>
<td>16.51</td>
<td>16.58</td>
<td>16.65</td>
<td>16.72</td>
<td>16.79</td>
</tr>
<tr>
<td>Japan</td>
<td>17.74</td>
<td>17.82</td>
<td>17.90</td>
<td>17.98</td>
<td>18.06</td>
<td>18.14</td>
</tr>
<tr>
<td>Mexico</td>
<td>33.15</td>
<td>33.31</td>
<td>33.47</td>
<td>33.63</td>
<td>33.79</td>
<td>33.95</td>
</tr>
<tr>
<td>Netherlands</td>
<td>3.43</td>
<td>3.46</td>
<td>3.49</td>
<td>3.51</td>
<td>3.53</td>
<td>3.55</td>
</tr>
<tr>
<td>New Zealand</td>
<td>1.14</td>
<td>1.16</td>
<td>1.18</td>
<td>1.20</td>
<td>1.23</td>
<td>1.25</td>
</tr>
<tr>
<td>Singapore</td>
<td>1.26</td>
<td>1.29</td>
<td>1.32</td>
<td>1.35</td>
<td>1.38</td>
<td>1.41</td>
</tr>
<tr>
<td>Sweden</td>
<td>2.09</td>
<td>2.12</td>
<td>2.15</td>
<td>2.18</td>
<td>2.21</td>
<td>2.24</td>
</tr>
<tr>
<td>UAE</td>
<td>3.72</td>
<td>3.75</td>
<td>3.78</td>
<td>3.81</td>
<td>3.84</td>
<td>3.87</td>
</tr>
<tr>
<td>UK</td>
<td>17.40</td>
<td>17.53</td>
<td>17.66</td>
<td>17.79</td>
<td>17.92</td>
<td>18.05</td>
</tr>
<tr>
<td>USA</td>
<td>143.70</td>
<td>144.20</td>
<td>144.70</td>
<td>145.20</td>
<td>145.70</td>
<td>146.20</td>
</tr>
</tbody>
</table>
53% of consumers experienced cybercrime or know someone who has

- Had a device computer/tablet/phone infected by a virus or other security threat: 36% (I have), 26% (Someone I know has), 53% (Either I or someone I know has)
- Had an account password compromised: 18% (I have), 19% (Someone I know has), 34% (Either I or someone I know has)
- Experienced credit or debit card fraud: 17% (I have), 23% (Someone I know has), 38% (Either I or someone I know has)
- Been notified that your personal information was involved in a data breach: 16% (I have), 17% (Someone I know has), 30% (Either I or someone I know has)
- Unauthorized access to or hacking of your email or social network profile: 14% (I have), 21% (Someone I know has), 34% (Either I or someone I know has)
- Made a purchase online that turned out to be a scam: 14% (I have), 20% (Someone I know has), 33% (Either I or someone I know has)
- Had others use your home Wi-Fi without permission: 14% (I have), 16% (Someone I know has), 28% (Either I or someone I know has)
- Detected unusual activity on your home Wi-Fi network: 14% (I have), 15% (Someone I know has), 27% (Either I or someone I know has)
- My location-based information was accessed without my permission: 13% (I have), 15% (Someone I know has), 26% (Either I or someone I know has)
- Clicked on a fraudulent email or provided sensitive (personal/financial) information in response to a fraudulent email: 13% (I have), 21% (Someone I know has), 32% (Either I or someone I know has)
- Received a phone call or text that resulted in malware being downloaded to your mobile device: 13% (I have), 17% (Someone I know has), 28% (Either I or someone I know has)
- Had a child’s online activity compromise your security (Parents only): 12% (I have), 19% (Someone I know has), 30% (Either I or someone I know has)
- Had a child that was bullied online (Parents only): 12% (I have), 22% (Someone I know has), 33% (Either I or someone I know has)
- Had your financial information compromised as a result of shopping online: 10% (I have), 16% (Someone I know has), 25% (Either I or someone I know has)
- Been a victim of identity theft: 10% (I have), 18% (Someone I know has), 26% (Either I or someone I know has)
- Fell for a technical support scam: 9% (I have), 17% (Someone I know has), 25% (Either I or someone I know has)
- Experienced a ransomware attack: 8% (I have), 15% (Someone I know has), 22% (Either I or someone I know has)
- Had someone gain unauthorized access to a smart home device: 7% (I have), 13% (Someone I know has), 19% (Either I or someone I know has)
- Had payment information stolen from your phone: 7% (I have), 14% (Someone I know has), 20% (Either I or someone I know has)
- Made a purchase online that turned out to be a scam: 6% (I have), 12% (Someone I know has), 18% (Either I or someone I know has)
- Lost a job or a promotion due to a social media posting you did not post: 5% (I have), 7% (Someone I know has), 12% (Either I or someone I know has)

Copyright © 2018 Symantec Corporation
Consumers who were victims of cybercrime globally lost $172 billion

The average victim lost $142

Figures represented in billions (USD):

<table>
<thead>
<tr>
<th></th>
<th>Australia</th>
<th>Brazil</th>
<th>Canada</th>
<th>China</th>
<th>France</th>
<th>Germany</th>
<th>Hong Kong</th>
<th>India</th>
<th>Indonesia</th>
<th>Italy</th>
<th>Japan</th>
<th>Mexico</th>
<th>Netherlands</th>
<th>New Zealand</th>
<th>Singapore</th>
<th>Spain</th>
<th>Sweden</th>
<th>UAE</th>
<th>UK</th>
<th>USA</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017</td>
<td>$1.9</td>
<td>$22.5</td>
<td>$1.5</td>
<td>$66.3</td>
<td>$7.1</td>
<td>$2.6</td>
<td>$0.1</td>
<td>$18.5</td>
<td>$3.2</td>
<td>$4.1</td>
<td>$2.1</td>
<td>$7.7</td>
<td>$1.6</td>
<td>$0.1</td>
<td>$0.4</td>
<td>$2.1</td>
<td>$3.9</td>
<td>$1.1</td>
<td>$6.0</td>
<td>$19.4</td>
</tr>
</tbody>
</table>
The average cybercrime victim spent nearly 24 hours (23.6 hours) globally (or almost three full work days) dealing with the aftermath.
Consumers emphasize the importance of online security

<table>
<thead>
<tr>
<th>Protection</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protect me from malicious sites or files</td>
<td>85%</td>
</tr>
<tr>
<td>Protect my mobile devices from viruses, malicious apps and suspicious text messages</td>
<td>84%</td>
</tr>
<tr>
<td>Keep my online activity and personal information private</td>
<td>82%</td>
</tr>
<tr>
<td>Monitor and restore my identity if it is stolen</td>
<td>82%</td>
</tr>
<tr>
<td>Manage all my passwords</td>
<td>81%</td>
</tr>
<tr>
<td>Protect my entire home network, not just individual devices, from threats</td>
<td>77%</td>
</tr>
<tr>
<td>Monitor and control the content my child(ren) access online (Parents Only)</td>
<td>77%</td>
</tr>
<tr>
<td>Secure my Wi-Fi connections outside of the home</td>
<td>70%</td>
</tr>
<tr>
<td>Protect the files, photos and videos I have on cloud services</td>
<td>62%</td>
</tr>
<tr>
<td>Control the information my family shares on social networks</td>
<td>59%</td>
</tr>
<tr>
<td>Turn off the internet and/or internet access to the devices in my household</td>
<td>50%</td>
</tr>
</tbody>
</table>

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.

- I use different passwords and write them down on a piece of paper: 34%
- I use a technique to remember different passwords: 32%
- I use the same password for all my accounts: 19%
- I use different passwords and have them in a file on my computer or smartphone: 16%
- I use different passwords and have my computer’s web browser save them for me: 12%
- I use different passwords and use a password manager program to store them: 9%
- Other methods: 6%
- I just reset my passwords so I don’t have to remember them: 4%
- I keep/use the default passwords: 3%
- I don’t have any online passwords: 1%
Portrait of a Cybercrime Victim
They’re adopters of newer security techniques

- Security software: 52%
- Personal VPN: 16%
- Two-factor authentication: 13%
- Fingerprint ID: 44%
- Facial recognition: 13%
- Pattern matching: 22%
- Voice ID: 10%

Victim
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

- Cybercrime should be treated like any other criminal act: 81%
- Cybercrime is wrong; law enforcement and internet companies should do more to protect us: 80%
- Cybercrime is wrong but all I can do is to protect myself and my family: 67%
- Cybercrime is wrong but it is too difficult to find the attacker: 53%
- Cybercrime is a fact of life and we have to accept it: 35%
- Stealing information online is not as bad as stealing property in 'real life': 22%

Agree (Top 2)
Yet **43 percent** believe it’s sometimes acceptable to commit morally questionable online behaviors in certain instances.

<table>
<thead>
<tr>
<th>Behavior</th>
<th>Sometimes Acceptable (Net)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reading someone else's email without their permission</td>
<td>26%</td>
</tr>
<tr>
<td>Sharing things you know are not true on social media</td>
<td>21%</td>
</tr>
<tr>
<td>Using a false email or someone else's email to identify yourself online</td>
<td>21%</td>
</tr>
<tr>
<td>Using a false photo or someone else's photo to identify yourself online</td>
<td>20%</td>
</tr>
<tr>
<td>Putting software on someone's machine that allows you to spy and/or track them</td>
<td>20%</td>
</tr>
<tr>
<td>Changing someone's status, posts or comments on social media without permission</td>
<td>19%</td>
</tr>
<tr>
<td>Posting inflammatory, threatening or sexually explicit comments or photos online</td>
<td>17%</td>
</tr>
<tr>
<td>Accessing someone's financial accounts without their permission</td>
<td>15%</td>
</tr>
<tr>
<td>Using someone else's credit card without permission to shop or book online</td>
<td>15%</td>
</tr>
<tr>
<td>Stealing someone's personally identifiable information</td>
<td>15%</td>
</tr>
<tr>
<td>Allowing your device to be used to send spam, malware or attack other computers</td>
<td>15%</td>
</tr>
<tr>
<td>Sending emails that trick people into giving out personal, financial or sensitive details</td>
<td>14%</td>
</tr>
</tbody>
</table>

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’

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

63%  

22%  

- Disagree (Bottom 2)  
- Agree (Top 2)
State of Consumers’ Trust
Consumers generally continue to trust the institutions that manage their data and personal information

<table>
<thead>
<tr>
<th>Institution</th>
<th>Lost All Trust + Lost Some Trust</th>
<th>Trust Same as Always</th>
<th>Gained Some Trust + Gained Complete Trust</th>
</tr>
</thead>
<tbody>
<tr>
<td>My employer</td>
<td>17%</td>
<td>63%</td>
<td>19%</td>
</tr>
<tr>
<td>My internet service provider</td>
<td>20%</td>
<td>61%</td>
<td>19%</td>
</tr>
<tr>
<td>My email provider</td>
<td>20%</td>
<td>61%</td>
<td>19%</td>
</tr>
<tr>
<td>Identity theft protection service providers</td>
<td>24%</td>
<td>60%</td>
<td>17%</td>
</tr>
<tr>
<td>My bank or financial institutions</td>
<td>18%</td>
<td>58%</td>
<td>24%</td>
</tr>
<tr>
<td>Security software</td>
<td>19%</td>
<td>58%</td>
<td>23%</td>
</tr>
<tr>
<td>Myself</td>
<td>11%</td>
<td>53%</td>
<td>36%</td>
</tr>
<tr>
<td>My social media platform</td>
<td>34%</td>
<td>51%</td>
<td>14%</td>
</tr>
<tr>
<td>Credit report companies that gather information without my consent</td>
<td>44%</td>
<td>45%</td>
<td>11%</td>
</tr>
<tr>
<td>My government</td>
<td>41%</td>
<td>44%</td>
<td>16%</td>
</tr>
</tbody>
</table>
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.