Cyber Safety Insights Report
United States (US) Results

Prepared by
The Harris Poll
Survey Method

The research was conducted online in the United States by The Harris Poll on behalf of Norton™ LifeLock™ among 1,004 adults aged 18+ between October 9-30, 2018. Data are weighted where necessary by age, gender, race/ethnicity, education, employment, household income, region, marital status, household size, and internet usage to bring them in line with their actual proportions in the population. Propensity score weighting was also used to adjust for respondents’ propensity to be online. No estimates of theoretical sampling error can be calculated.

Figures on identity theft incidence are from a separate online survey of 5,000 U.S. adults aged 18+ conducted by The Harris Poll on behalf of Norton™ LifeLock™ between January 2-18, 2019.

Cyber crime is defined as having personally experienced a crime committed with devices over the internet, including, but not limited to, detecting unauthorized access on an online account, learning information was exposed in a data breach, and detecting malicious software on a device. Please note, this definition is different than the definition used in past research.
Key Findings
Cyber Crime
Which of the following you are more likely to experience than cyber crime?

85% cyber crime

I am equally or more likely to experience cyber crime

15% home burglarized

I am more likely to have my home burglarized
Majority of Americans Expect to Experience Cyber Crime in Next 12 Months

Expect to Experience in Next 12 Months

65% (% At least somewhat likely to experience cyber crime in the next year)
Have Ever Experienced a Cyber Crime

59% Impacting nearly 152 million US consumers

Experienced in the Past 12 Months

41% Impacting over 105 million US consumers in the past year
### Top 3 Cyber Crimes Ever Experienced

- Detected malicious software on a computer, Wi-Fi network, smartphone, tablet, smart home, or other connected device: 26%
- Learned your personal information was exposed in a data breach: 20%
- Detected unauthorized access on an email account: 14%

### Past Year Impact of Cyber Crime

(among past 12 month victims)

- Average number of hours spent resolving: 3.1*
- For an estimated 324.2 million hours lost
- Almost 2 in 25 needed a week or more to resolve the issue
- An estimated $11.3 billion was lost to cyber crime
Privacy
I am more alarmed than ever about my privacy

Strongly agree: 31%
Somewhat agree: 42%

I accept certain risks to my online privacy to make my life more convenient

Strongly agree: 17%
Somewhat agree: 49%

Consumers are more alarmed than ever, but also willing to accept certain risks

I want to do more to protect my privacy

Strongly agree: 43%
Somewhat agree: 41%

I don’t know how to protect my privacy

Strongly agree: 11%
Somewhat agree: 32%

Consumers want to do more to protect their privacy, but many don’t know how

The Privacy Paradox

Consumers are more alarmed than ever, but also willing to accept certain risks

Consumers want to do more to protect their privacy, but many don’t know how
Consumers Don’t Have a Lot of Trust in Providers to Protect Personal Information

Trust in Managing and Protecting Personal Information
(% trust a lot)

- Healthcare providers/ institutions: 27%
- Financial institutions: 25%
- Retailers/Online shopping sites: 17%
- Government: 12%
- Social media providers: 6%

Of those with a social media account, 28% have deleted one due to privacy concerns in the past 12 months.
Consumers view data protection as a right – not a privilege

% Not Willing to Pay Organizations to Ensure Protection of Personal Information

- Social media providers: 72%
- Retailers/Online shopping sites: 58%
- Healthcare providers/institutions: 57%
- Financial institutions: 56%
Many US Consumers Are Willing to Sell (Or Give Away) Certain Personal Information

<table>
<thead>
<tr>
<th></th>
<th>Internet Search History</th>
<th>Location</th>
<th>Identification Document Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>would give for free</td>
<td>20%</td>
<td>19%</td>
<td>18%</td>
</tr>
<tr>
<td>need to be paid</td>
<td>35%</td>
<td>36%</td>
<td>25%</td>
</tr>
<tr>
<td>would not sell</td>
<td>45%</td>
<td>45%</td>
<td>57%</td>
</tr>
</tbody>
</table>

Copyright © 2019 Symantec Corporation. All rights reserved.
Steps Taken to Protect Personal Information/Online Activities

- Cleared or disabled cookies: 45%
- Limited information shared on social media: 44%
- Read the Terms & Conditions in full before installing or downloading a device or service: 36%
- Stopped using public Wi-Fi: 33%
- Changed default privacy settings on devices: 32%
- Used an identity theft protection service: 24%
- Used something other than full name for social media profiles: 21%
- Used anonymous payment methods: 15%
- Used an encrypted email service: 13%
- Used a virtual private network (VPN) to encrypt information sent to and from devices: 13%
- Other: 3%
- I have not done anything: 14%

86% have taken at least one step
Younger generations are more inclined to take action on social media accounts.

Those with a social media account who deleted one in the past 12 months due to privacy concerns:

- 18-38 years: 33%
- 39-53 years: 31%
- 54+ years: 20%

However, younger generations are more likely than older generations to be willing to sell or give away their personal information:

- Search History:
  - 18-34 years: 67%
  - 39-53 years: 58%
  - 54+ years: 42%

- Location:
  - 18-34 years: 63%
  - 39-53 years: 62%
  - 54+ years: 44%

- ID Information:
  - 18-34 years: 54%
  - 39-53 years: 45%
  - 54+ years: 31%
Control is at the heart of our privacy paradox

Importance In Requiring That Companies & Organizations Give Consumers...

- A way to report misuse of their personal data: 94% (51% Absolutely Essential, 28% Very Important, 15% Somewhat Important)
- The right to find out how their personal data is being used: 93% (50% Absolutely Essential, 27% Very Important, 16% Somewhat Important)
- The right to request that their personal data is erased: 93% (46% Absolutely Essential, 29% Very Important, 18% Somewhat Important)
- The ability to control how their personal data is being used: 93% (49% Absolutely Essential, 28% Very Important, 16% Somewhat Important)
Children and Identity Theft
Nearly 1 in 4 have ever experienced Identity Theft, impacting over 59 million US consumers.

23% experienced Identity Theft in the past 12 months, impacting over 13 million US consumers in the past year.
Most characterize identity theft as an ‘adult problem’

62% of Parents of Minors
Don’t Know That Children Under 18 Are at Risk

Parents’ Concern That Their Child Will Experience Identity Theft...
(among parents of minors)

- Very concerned: 31%
- Somewhat concerned: 24%
- Not very concerned: 25%
- Not at all concerned: 9%

Because of an action their child(ren) has taken:
- 68% Concerned (Net)

Because of an action they have taken:
- 67% Concerned (Net)

Because of an action they have not taken:
- 65% Concerned (Net)

Steps Parents Have Taken to Protect Child’s Identity
(among parents of minors)

- Don’t provide their social security number: 46%
- Limit the amount of information I post about them on social media: 44%
- Limit their access to certain websites and apps: 40%
- Limit the amount of information they can post on social media: 39%
- Review and approve all the apps they download: 32%
- Check to see if a credit rating was established using their name: 22%
- Have identity theft protection for them: 22%
- Freeze their credit report: 18%
- Other: 3%
- Nothing: 13%
Smart Devices
Over Half of US Consumers Own a Smart Home Device; Risks of Unauthorized Access Are Fairly Well Known

57% of consumers own a smart home device

- I do not own any smart... 43%
- Other 5%
- Smart Refrigerator 5%
- Smart Door Locks 5%
- Smart Lighting 7%
- Smart Camera 12%
- Smart Thermostat 12%
- Smart Speaker/Home... 21%
- Smart TV 38%

30% vs. 19%
Interestingly, those who own a smart home device are more likely than those who don’t to believe that smart devices can’t be hacked

25% of consumers don’t know that smart devices can be hacked

Someone can gain unauthorized access to a smart baby monitor to spy on children 77%

Smart Home Device Facts (% Answered Correctly)

Someone can gain unauthorized access to a smart door lock and break into a home 78%

If someone gains unauthorized access to an email account, all the devices that are linked to that email could be accessed 80%
Appendix
How much money would a company need to pay you per month in order to have access to the following types of personal information?

<table>
<thead>
<tr>
<th>Information Type</th>
<th>0 USD</th>
<th>1-10 USD</th>
<th>11-20 USD</th>
<th>21-30 USD</th>
<th>31+ USD</th>
<th>I would not sell this type of information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Search History</td>
<td>20%</td>
<td>9%</td>
<td>9%</td>
<td>12%</td>
<td>13%</td>
<td>45%</td>
</tr>
<tr>
<td>Location</td>
<td>19%</td>
<td>9%</td>
<td>11%</td>
<td>13%</td>
<td>10%</td>
<td>45%</td>
</tr>
<tr>
<td>ID Information</td>
<td>18%</td>
<td>10%</td>
<td>5%</td>
<td>5%</td>
<td>6%</td>
<td>57%</td>
</tr>
</tbody>
</table>
How much would you be willing to pay per month to each of the following to ensure your personal information is protected?

<table>
<thead>
<tr>
<th>Somewhat Important</th>
<th>Willing to Pay</th>
</tr>
</thead>
<tbody>
<tr>
<td>Social Media Providers</td>
<td>16%</td>
</tr>
<tr>
<td>Retailers/Online Shopping Sites</td>
<td>22%</td>
</tr>
<tr>
<td>Healthcare Institutions</td>
<td>21%</td>
</tr>
<tr>
<td>Financial Institutions</td>
<td>23%</td>
</tr>
</tbody>
</table>

- 0 USD
- 1-10 USD
- 11-20 USD
- 21-30 USD
- 31+ USD