Privacy Experiences & Attitudes Survey

2015 Nationally Representative Online Survey

Prepared by CR Survey Research Department

February, 2015

Consumer Reports | Digital Lab

2015 Consumer Reports Privacy Experiences and Attitudes Survey

Introduction

The findings from this survey describe American behaviors, experiences, and attitudes toward current events and trends as they occur online, including internet privacy, cyberbullying, and the continued emergence of smart health and lifestyle monitors. As consumer products and consumers themselves move toward a complete integration with wireless networks, Consumer Reports needs to be there to ensure the best interests of the consumer are represented. The survey was fielded online in January of 2015 to a nationally representative sample of 3,004 Americans.

Highlights

- Most Americans (91%) have access through some medium to the internet, including a device attached to a home internet connection, smartphone, or tablet.
- Within the past year, almost 29% of Americans were told or discovered on their own that their personal information was compromised by a business, agency or organization. For those Americans who were notified of a data breach, breaches came most frequently from brick and mortar retailers (47%) and/or from a bank or financial institution (46%).
- Over one in four Americans (28%) report they store some type of private personal information in the cloud, including documents, financial records, passwords, medical records, and more. Furthermore, about 31% of Americans report that they access their personal health information records online, most commonly through either websites maintained by their doctor (47%) or health insurance company (37%), or through mobile apps (10%).
- One in five smartphone owners have used mobile check deposit within the past year. Using a mobile phone as a ticket for public transportation (14%) and making purchases at retail stores (12%) are the second most common class of financial activities we asked about for which a smartphone was used. Still, 58% of smartphone owners do not commonly make any purchases on their phone, deposit checks, or use their phone as a ticket or pass.
- Only 3% of smartphone owners lost their phone or had it stolen within the past year. Although commonly available at no cost, only 10% of consumers report actively installing software that can remotely erase the content of their smartphones.
- Over half of parents (52%) worry most about their child viewing adult-oriented material while online. Only 4% of parents report that their child has been bullied online in some way.
- Only 10% of Americans have used the emerging wearable devices—such as sleep trackers, smart clothing, smart glasses, wearable activity monitors, or smartwatches—in the past year. A higher percentage of Americans (33%) have some type of device in their home that can be controlled by a smartphone, tablet, or computer.

Findings

Most Americans (81%) have access to an internet connection in their home, and many Americans are also free to roam outside, with 62% owning a smartphone and 38% owning a tablet. **In fact, only 9% of Americans report not having access to either a home internet connection or at least a smartphone or tablet through which they can likely access the internet**. The near universality of internet connectivity may mean that many populations without it, seniors for example, are at risk for becoming disenfranchised from information and social interaction that has moved online.

The results of the survey are discussed below and organized within the information themes captured by the survey, specifically data security, smartphone safety, social media and cyberbullying, and the smart lifestyle.

Data Security

2014 has been called "the year of the massive data breach," leaving the information of millions of Americans vulnerable to attack.[1] The number of breaches in 2014 was staggering: over 700 in total, an increase of over 27% from 2013, according to the Identity Theft Resource Center. From credit card numbers and social security numbers to health and financial data, the information stolen has impacted all types of organizations and businesses, including eBay, the Montana Department of Public Health and Human Services, P.F. Chang's, Home Depot, Michaels Stores, Target, and JPMorgan Chase.

In our nationally representative survey, **almost 29% of Americans experienced a situation where they were told or discovered on their own that their personal information was compromised within the past year** (Table 1). One in five Americans were notified of the data breach, specifically by a company, financial institution, government agency, or other organization. Furthermore, about 9% of Americans report that an unauthorized person placed charges on card accounts, while only 3% reported money had been taken from another type of existing account, such as a bank account.

[1] http://www.idtheftcenter.org/ITRC-Surveys-Studies/2014databreaches.html; http://www.pcworld.com/article/2453400/the-biggest-data-breaches-of-2014-so-far.html

Table 1. Data Breach Experiences among Americans	
Experience	**% Endorsed**
I was notified by a company, financial institution, government agency, or other organization that my personal information was possibly part of a data breach	20%
An unauthorized person placed charges on one of my existing credit card accounts	9%
An unauthorized person placed charges on or took money from an existing account OTHER THAN a credit card account (e.g., bank account)	3%
An unauthorized person opened NEW credit card accounts, bank accounts, or other accounts using my personal information	1%
An unauthorized person used my personal information for some other fraudulent purpose (e.g., gave my information to the police when they were charged with a crime; applied for government benefits, medical care, or a job; rented a home)	1%
Other	1%
I have not had my personal information compromised in the past 12 months	71%
Base: All survey respondents	***2959***

So, where do these breaches occur? As shown in Table 2, **for those Americans who were notified that their personal information was compromised, about half were notified by a brick and mortar retailer (47%) and/or a bank or financial institution (46%) that a breach occurred. Only 18% of these individuals reported that notifications came from an online retailer, suggesting everyone is truly at risk for a data breach, not just online shoppers.** Nonetheless, Americans with home internet are significantly more likely (31% vs. 19%) to report having been a victim of a data breach or fraud within the past year than individuals without access to home internet. Americans are not commonly affected by data breaches at government agencies, email providers, medical or health facilities, and employers.

Table 2. Source of Data Breach Notification	
Business Type	**% Endorsed**
A brick and mortar retailer	47%
Bank or financial institution	46%
Online retailer	18%
Government agencies	5%
Email provider (e.g., Yahoo)	4%
Medical or health facility	3%
Employer or former employer	3%
Other (please specify)	8%
Base: Notified of date breach	***593***

Half of Americans who are notified or impacted in some way by data theft or fraud do not change their online behavior at all as a result of the breach (Table 3). The other half protect themselves in a variety of ways, but no single behavior dominates. About 10% or more of Americans impacted by a

breach choose to either reduce use of the internet for sending personal information (15%), stop registering or entering personal information on websites (15%), purchase or sign up for an identity protection service (14%), and/or stop using the affected website or business (10%). A common "other" write-in response is changing passwords for accounts.

Table 3. **Self-Reported Online Behavior Changes After Data Breach**	
Online Behavior	**% Endorsed**
Reduced use of the Internet to send personal information	15%
Stopped registering or entering my personal information on websites	15%
Purchased or signed up for an identity theft or fraud protection service	14%
Stopped using the website or business that was part of the data breach	10%
Reduced or eliminated use of cloud-based services (e.g., Apple iCloud, Dropbox)	7%
Stopped purchasing items online	6%
Used cookies/tracking blocker software or browser plug-ins (e.g., Ghostery, Disconnect)	4%
Encrypted my e-mails	3%
Used privacy-oriented search engine (e.g., DuckDuckGo, StartPage)	2%
Used privacy-oriented e-mail service (e.g., StartMail)	2%
Used a Virtual Private Network (e.g., Astrill)	2%
Other	9%
I have not changed my online behavior as a result of the data breach	50%
Base: Impacted by data breach or fraud	848

Consumers may contribute to breaches in data security themselves by disclosing personal information to unauthorized parties. This can occur during phishing attempts when fraudulent emails or websites that appear to come from reputable companies or organizations solicit account information or other sensitive materials. In the past year, only 2% of Americans report submitting personal information in response to a fraudulent email, while 94% had not. Approximately 4% of Americans were unsure if they had done so. Even though 2% is a small proportion, this number represents hundreds of thousands of Americans falling victim to these phishing schemes, which are often inexpensive to produce and difficult to trace and prosecute. Fortunately, for the population that do fall prey to a phishing scheme, 68% do not report any major negative consequences such as fraudulent transactions, losing money from a bank account, or being forced to close an account. Members of popular social networking sites, particularly Google+, Twitter, and Instagram, are more likely to be a victim of a phishing attack (2.9% vs. 1%). They are also more likely to have been a victim of a data breach (32% vs. 22%). Overall, having more social networking accounts is associated with an increased risk of data breach or successful phishing attack, but that does not necessarily mean that information submitted to these sites was exposed or used by a third party. This may merely indicate that this group has a higher level of internet activity, which can make them more vulnerable to attacks; the cause of this association is still unclear.

As the sheer amount of information we store on our computers grows, data breaches may be of particular concern for those who use a cloud-based service to handle the overflow. **Over one in four Americans (28%) report they store some type of private personal information in the cloud (Table 4), which could include documents, financial records, passwords, medical records and more.** Photographs

are one of the more common file types stored in the cloud (21% of Americans do so). This is almost twice as many Americans as those who store documents (11%). The storage of photographs, one of the more common file types backed up in the cloud by Americans, may appear to be low risk; however, smartphones and many cameras geotag photos, which allows third parties to easily identify when and where a photo was taken. If provided access to enough photos, your entire schedule and the whereabouts of your family, friends, and valuable commodities appearing in the photographs can be ascertained.

Medical and financial records are least commonly stored in the cloud, but **about 31% of Americans report that they access their personal health information records online, most commonly through either websites maintained by their doctor (47%), health insurance company (37%), or through mobile apps (10%).** Consumers may not realize that this medical information, although not personally stored in the cloud by the patient, is in a cloud maintained by a third party.

Table 4.
Storage of Personal Information in the Cloud

Information Type	**% Endorsed**
Photographs	21%
Documents (e.g., text, spreadsheets, presentations)	11%
Videos	8%
Passwords	4%
Financial/tax records	2%
Medical records	2%
Other (please specify)	1%
I have not stored any PRIVATE PERSONAL INFORMATION on a cloud-based service during the past twelve months	72%
Base: All survey respondents	***2952***

People unknowingly share data every day, and many do it with the best intentions hoping to increase their security. For example, many cloud-based backup services, like Carbonite®, will by default store all files on your computer in a cloud accessible to you anywhere online. Unfortunately, this can presumably give hackers full access to your files should they obtain the username or password to your account. Individuals may also not understand that all email is stored in the cloud, including any sensitive documents attached to emails sent or received. Even though only 16% of Americans are either somewhat or very willing to allow websites and mobile apps access to personal information and online activity to personalize content and provide advertising, a greater number of consumers may nonetheless be making this information available unknowingly. Overall, Americans who store information in a cloud-based service are significantly more likely (30% vs. 17%) to have been a victim of any data breach or fraud within the past year.

Smartphone Safety

Most Americans now own a smartphone, and every year the potential uses for smartphones in commerce and daily activities increase. The advent of mobile payment services in particular have transformed the smartphone into a virtual wallet, partially freeing consumers from the clutter of paper

bills, credit cards and change. Frequent visits to the bank teller are also a thing of the past for many people who now deposit checks over their phone. In fact, depositing checks was the most frequent of six uses we asked American smartphone owners about. **One in five smartphone owners has submitted a mobile check deposit within the past year** (Table 5), potentially limiting traffic to banks for smaller transactions. Oddly enough, the number of bank branches (now over 95,000) isn't dropping dramatically just yet, as banks still feel the need to personally connect with customers.[2]

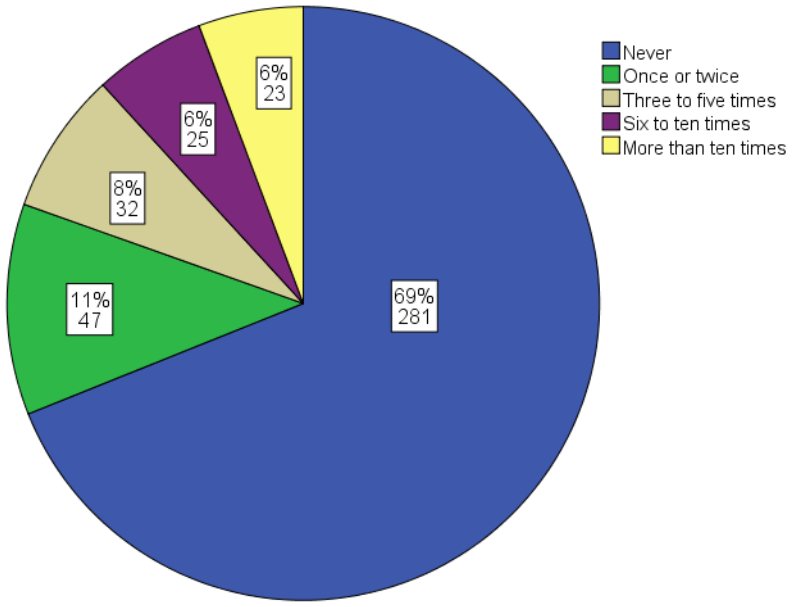
Table 5. **Smartphone Feature Usage within the Past Year**	
Feature Use	**% Endorsed**
Deposited a check by scanning it with the phone	21%
Used phone as a boarding pass or ticket for an airplane, train or other form of public transportation	14%
Made purchase(s) at a retail store (e.g., grocery store, electronics store, clothing store, etc.)	12%
Used phone as a ticket for a sporting event, concert, movie, performance, festival or play	10%
Made purchase(s) at a coffee shop	9%
Made purchase(s) at a restaurant	7%
Made other type of purchase with smartphone (please specify)	6%
None of the above	58%
Base: Smartphone owners	***1834***

Slightly over one in 10 smartphone owners use a mobile phone as a ticket for public transportation (14%) and/or make purchases at retail stores (12%). Food and beverage purchases are also made on smartphones by many owners, although slightly less commonly. Still, **58% of smartphone owners do not typically make purchases on their phone, deposit checks, or use their phone as a ticket or pass.** Overall, smartphone owners who use their phone to make payments are significantly more likely (40% vs. 31%) to have been a victim of any data breach or fraud within the past year.

Although many consumers make purchases of some sort on their smartphones, most Americans do so the more traditional way: entering a credit card or using a PayPal-type service at checkout. That said, many of the nearly one-third of Americans who have tried mobile payment services, such as Apple Pay, end up using these services on a recurring basis throughout the year (Figure 1).

[2] http://www.biztimes.com/article/20141208/MAGAZINE03/312059979

Figure 1.
Frequency of In-Person Transaction Mobile Payment Use (e.g., Apple Pay) Among Smartphone Shoppers



Even though smartphones have not yet become the ubiquitous modern-day credit card, smartphones still may contain a significant amount of sensitive information including locations, browser history, passwords, or other information stored by their owners. Thus, keeping smartphones in a secure location and enabling security features is important for keeping information safe. Most Americans have been successful at keeping track of their phone: **only 3% of smartphone owners lost or had their phone stolen within the past year.** However, over one-third of these owners never found their phone.

Carelessness in terms of the physical storage of a smartphone is certainly a risk factor reducing data security due to the increased likelihood of losing the phone or being a victim of theft. But even beyond that, smartphone owners who have their phone stolen are twice as likely (66% vs. 33%) to be a victim of data breach or fraud as well as phishing attacks (15% vs. 3%)[3], which may suggest that these people are negligent in other ways. Keeping track of one's smartphone is necessary but not sufficient to keep sensitive information safe. Other strategies are also important, and include screen locks, data backups, antivirus software, and remote locking or data wiping applications. Unfortunately, one in three smartphone owners do not report having taken any of these measures to protect their device in the past year, and no one method is used by most consumers (Table 6). Overall, Americans who own a smartphone or tablet are significantly more likely (33% vs. 19%) to have been a victim of data breach or fraud within the past year.

[3] Please note that although there is a statistical relationship between individual phone theft and fraud victimization, this does not indicate that the theft was a cause of the separate case of fraud. This is also the case with other cross-tabulations and correlations presented in this report.

Table 6. Smartphone Security Measures Taken	
Security Measure	**% Endorsed**
Set a screen-lock with a 4-digit PIN	36%
Backed-up your data (e.g., photographs, contacts and other files) to a computer and/or online service	33%
Set a stronger screen-lock measure, such as a PIN longer than 4-digits, a password, fingerprint, or an unlock pattern	21%
Installed software that can remotely locate and secure your smartphone	17%
Installed an antivirus app	16%
Used security features of the phone other than a screen-lock (e.g., encryption)	11%
Installed software that can remotely erase the contents of your smartphone	10%
Other	1%
I have not taken any security measures to protect my smartphone from loss or unauthorized access	34%
Base: Smartphone owners	***1831***

The most common smartphone security measures taken by owners include setting a four-digit screen lock (36%) and backing up phone data to a computer or using an online service (33%). Stronger screen lock security measures, such as a PIN longer than four digits or a fingerprint, are only used by one in five smartphone owners. **Although commonly available at no cost, only 10% of consumers report they have actively installed software that can remotely erase the content of their smartphones.** It is also possible they do not know that their phone may come with software installed for this purpose (e.g., Find my iPhone, Android Device Manager). There does also appear to be a relationship between tech-savviness and security behaviors. Smartphone owners who have used their phone to make purchases are more likely to take security precautions such as using a screen lock with a 4 digit pin (46% vs. 33%).

Social Media and Cyberbullying

According to our survey, over two-thirds (71%) of American adults belong to one of the top six popular social networks, including Facebook, LinkedIn, Google+, Twitter, Pinterest, and Instagram, and have maintained an active membership within the past 12 months. It is no wonder, then, that parents may be rather lenient when it comes to restricting their own children's internet use. In fact, **almost half (46%) of parents who provide internet access to their children via a computer, tablet, smartphone, or iPod Touch report that one of those children is under 11 years old (Table 7).**

Table 7. Age Breakdown of Children with Access to the Internet*	
Age of Child	**% Endorsed**
10 or younger	46%
11 or 12	26%
13	12%
14	12%
15	11%
16	11%
17	14%
None of the above	3%
Base: Parents with children <18 who are given internet access	***668***

*Note: Percentages are not based on total number of children, but rather: among the parents who reported that at least one child has access to the internet, what percentage had at least one of a given age with access.

Nonetheless, parents still experience some concern about their children's online behavior, but what about? **Over half of parents (52%) worry most about their child viewing adult-oriented material while online (Table 8). Among the other top worries include meeting or interacting with strangers (49%) and being distracted from schoolwork or other responsibilities (46%).** More than twice as many parents are concerned about their child getting bullied (26%) than bullying others (11%). In fact, bullying others was the least common concern among parents.

Table 8. Parents Top Concerns about Children's Internet Use	
Parental Concern	**% Endorsed**
View adult-oriented material	52%
Meet or interact with strangers	49%
Be distracted from their school work or other responsibilities	46%
Share things you don't want them to	38%
View aggressive or violent material	35%
Incur charges from websites or apps	27%
Get bullied on social networking websites	26%
Learn information that contradicts what they've been taught	16%
Bully others on social networking websites	11%
Other	2%
I do not worry when my children are online	18%
Base: Parents with children <18 who have internet access	***667***

Only 4% of parents report that their child has been bullied online in some way but 9% of parents were unsure. For those children who did suffer cyberbullying, most parents (70%) reported that it occurred on a social networking site, rather than a news media site, gaming site, or other location.

The Smart Lifestyle

Devices that are not internet-enabled may one day go the way of the cassette, giving their owners the nostalgic feeling of being disconnected. Those days are not yet here, however, and **only 10% of Americans have used the emerging wearable devices such as sleep trackers, smart clothing, smart glasses, wearable activity monitors, or smartwatches in the past year** (Table 8). This reticence to engage is not likely to be short lived; about nine in 10 Americans have no intention of purchasing these devices in the near future. The internet-enabled device that Americans are most likely to purchase in the near future is a wearable activity monitor such as a pedometer or Fit Bit. Only 6% of consumers are interested in this device, however.

Table 8.
American Use of Wearable Internet-Enabled Electronic Devices

Wearable Internet-Enabled Device	**% Endorsed**
Wearable activity monitor (e.g., pedometer; Fitbit, Smart jewelry)	6%
Sleep tracker (that may or may not be attached to an activity monitor such as Fitbit)	4%
Smart glasses (e.g., Google Glass)	1%
Wearable computer/Smartwatch (e.g., Pebble Watch)	1%
Smart clothing (to monitor heart rate, etc.)	1%
Wearable electronics for pets	0%
Other	0%
I have not used any wearable internet-enabled devices in the past twelve months	90%
Base: All survey respondents	***2983***

Desire for internet-enabled devices in the home is somewhat higher, as they allow users to interface with their home appliances and electronics for reasons that range from safety to convenience. Unlike wearable electronics, the smart home devices do not necessitate a nontraditional appearance (e.g., donning smart glasses) or a keen interest in personal health. Also, these devices have been around for purchase for a longer time period. **As such, a higher percentage of Americans (33%) have some type of device in their home that can be controlled by a smartphone, tablet, or computer** (Table 9).

Table 9. Internet-Enabled/Controllable Devices in the Home	
Home Internet-Enabled Device	**% Endorsed**
Television	13%
Gaming console (e.g., Xbox)	5%
Alarm system	5%
Radio	4%
Thermostat	3%
Indoor camera/monitor (e.g., a nanny cam)	2%
Lighting system/bulbs	2%
Garage door opener	2%
Door lock	2%
Outdoor camera	1%
Washer and/or dryer	1%
Smoke and/or carbon monoxide detector	1%
Kitchen appliance(s)	1%
Baby Monitor	1%
Water meter	1%
Power meter	0%
Generator	0%
Other (please specify)	2%
There are no such devices in my home	77%
Base: All survey respondents	***2919***

The most popular smart device owned by Americans is a television. Interestingly, a TV would not necessarily be controlled outside the home by a mobile device, unless it was to schedule the recording of programs, in which case it would be the DVR that would be internet-enabled. Many uses presumably involve changing channels or using smart features of the television that often are used when the owner is still in the home.

Predictors of Data Breach and Phishing Victimization

To better identify online behaviors that are uniquely associated with data breaches and phishing victimization, we utilized a form of predictive modeling known as forward regression. Several unique characteristics and behaviors were associated with both the profile of a consumer who had been the victim of a data breach and, separately, a phishing attack. Please note that in many or most instances, the data breach is no fault of the consumer, and associated characteristics do not indicate cause. Additionally, specific online behaviors related to data breach or phishing victimization may simply serve as a proxy for increased internet or mobile technology usage and not result from the identified behavior.

Demographically, victims of a data breach were more likely to be:

- older
- female
- higher household incomes
- higher levels of education

Online behaviors associated with increased likelihood of data breach included:

- using a phone as a boarding pass or ticket for transportation
- having had their phone stolen
- storing photographs in the cloud
- accessing health information online (particularly from websites maintained by a health insurance company)
- being familiar with the terms *deep* or *dark web*
- intending to purchase wearable internet-enabled devices
- having smart home devices
- having children under 18 with access to the internet

Consumers who were **not** part of a data breach were more likely to have:

- set a four-digit pin screen lock on their phone

On the other hand, victims of a phishing attack are more likely to be:

- younger
- less educated
- lower household income
- male

Online behaviors associated with increased likelihood of a phishing attack included:

- made a purchase at a restaurant with a smartphone
- stored videos, passwords, and financial records (but not documents) in the cloud
- access their health information electronically
- be open to websites and apps collecting information for marketing purposes
- fear their children getting bullied on social networking websites relative to other parental concerns

Consumers who were **not** a victim of a phishing attack were more likely to have:

- set a stronger screen-lock measure on their smartphone (such as a fingerprint)

Overall, both data breaches and phishing attacks appear to have some selectivity with regard to which populations they impact. Data breaches appear to adversely impact higher socioeconomic (SES) individuals who are more engaged in mobile and wireless technologies. Phishing attacks also target those highly engaged online, but in this case, the Americans are typically of lower SES.

Methodology

This survey was administered online from January 15, 2015 to January 23, 2015 to a nationally representative sample of 3,004 American adults managed by the GfK Group. To qualify for the main survey, a panel member must have been age 18 or older. Panel members were randomly recruited through probability-based sampling, and households were provided with access to the Internet and hardware if needed.

A post-stratification weight was computed to adjust for any survey non-response as well as any non-coverage or under- and over-sampling resulting from the study-specific sample design. Demographic and geographic distributions for the non-institutionalized, civilian population ages 18+ from the most recent U.S. Census Current Population Survey are used as benchmarks in this adjustment and included gender, age, race, ethnicity, education, household income, census region, metropolitan area, and internet access.

Key demographic characteristics (after weighting was applied) of this sample are presented below:

- 52% female
- Median age of 47
- 66% White, non-Hispanic
- 29% 4-year college graduates
- 60% have a household income over $50,000

Sampling error for this cohort was 2% at a 95% confidence level. Findings presented in this report represent analyses of data after weighting was applied to respondent data to approximate population-based estimates. Please note that any subsets of the sample ("bases") that fall below 384 have a margin of error that exceeds +/-5% at a 95% confidence level which makes differences in responses falling within this range difficult to interpret. Aggregate tabulations have been provided separately so that trends can be reviewed. Only statistically significant inferential analyses were reported. Please contact the Survey Research Department with any questions.