PewResearchCenter

NUMBERS, FACTS AND TRENDS SHAPING THE WORLD

FOR RELEASE JANUARY 26, 2017

Americans and Cybersecurity

Many Americans do not trust modern institutions to protect their personal data – even as they frequently neglect cybersecurity best practices in their own personal lives

BY *Kenneth Olmstead and Aaron Smith*

FOR MEDIA OR OTHER INQUIRIES:

Lee Rainie, Director, Internet, Science and Technology Research
Aaron Smith, Associate Director, Research
Dana Page, Senior Communications Manager
202.419.4372

www.pewresearch.org

RECOMMENDED CITATION: Pew Research Center, January, 2017, "Americans and Cybersecurity"

About Pew Research Center

Pew Research Center is a nonpartisan fact tank that informs the public about the issues, attitudes and trends shaping America and the world. It does not take policy positions. The Center conducts public opinion polling, demographic research, content analysis and other data-driven social science research. It studies U.S. politics and policy; journalism and media; internet, science and technology; religion and public life; Hispanic trends; global attitudes and trends; and U.S. social and demographic trends. All of the Center's reports are available at www.pewresearch.org. Pew Research Center is a subsidiary of The Pew Charitable Trusts, its primary funder.

Americans and Cybersecurity

Many Americans do not trust modern institutions to protect their personal data – even as they frequently neglect cybersecurity best practices in their own personal lives

Cyberattacks and data breaches are facts of life for government agencies, businesses and individuals alike in today's digitized and networked world. Just a few of the most high-profile breaches in 2016 alone include the hacking and subsequent release of emails from members of the Democratic National Committee; the release of testing records of dozens of athletes conducted by the World Anti-Doping Agency; and the announcement by Yahoo that hackers had accessed the private information associated with roughly 1 billion email accounts. Finally, in late 2016 and early 2017 U.S. intelligence agencies (the FBI, CIA and Department of Homeland Security) both issued statements and testified before Congress that the Russian government was involved in the hack of the DNC with the aim of influencing the 2016 presidential election.

Previous Pew Research Center studies of the digital privacy environment have found that many Americans fear they have lost control of their personal information and many worry whether government agencies and major corporations can protect the customer data they collect. As part of this ongoing series of studies on the state of online privacy and security, the Center conducted a national survey of 1,040 adults in the spring of 2016 to examine their cybersecurity habits and attitudes. This survey finds that a majority of Americans have directly experienced some form of data theft or fraud, that a sizeable share of the public thinks that their personal data have become less secure in recent years, and that many lack confidence in various institutions to keep their personal data safe from misuse. In addition, many Americans are failing to follow digital security best practices in their own personal lives, and a substantial majority expects that major cyberattacks will be a fact of life in the future. Among the key findings:

A majority of Americans (64%) have personally experienced a major data breach, and relatively large shares of the public lack trust in key institutions – especially the federal government and social media sites – to protect their personal information

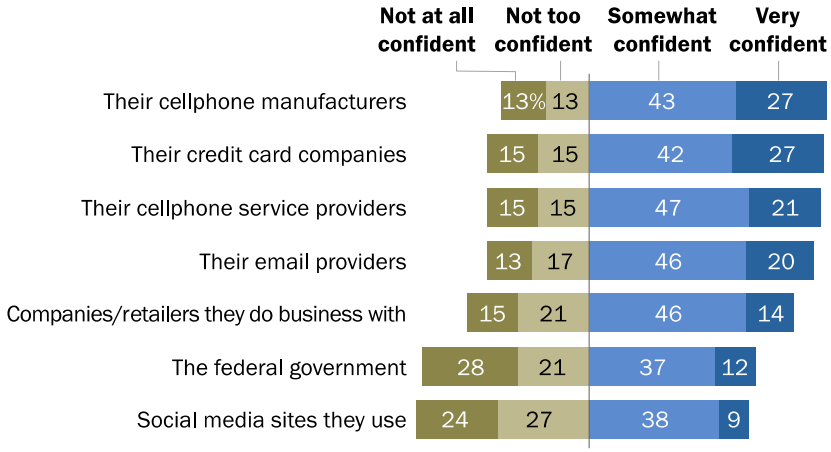
Data security is a personal issue for many Americans: The survey finds that a majority of the public has noticed or been notified of a major data breach impacting their sensitive accounts or personal data. The survey examined several different types of data theft and found that 64% of U.S. adults have been impacted by at least one of them:

- 41% of Americans have encountered fraudulent charges on their credit cards.

- 35% have received notices that some type of sensitive information (like an account number) had been compromised.
- 16% say that someone has taken over their email accounts, and 13% say someone has taken over one of their social media accounts.
- 15% have received notices that their Social Security number had been compromised.
- 14% say that someone has attempted to take out loans or lines of credit in their name.
- 6% say that someone has impersonated them in order to file fraudulent tax returns.

Roughly half of Americans do not trust the federal government or social media sites to protect their data

% of U.S. adults/tech users (see note below) who are ___ in the ability of the following institutions to protect their data



Note: Data on cellphone manufacturers and service providers based on cellphone owners; data on email providers based on internet users; data on social media sites based on social media users. Data for credit card companies recalculated to exclude "does not apply" responses. Otherwise, refusals and "does not apply" responses not included in this chart.
Source: Survey conducted March 30-May 3, 2016.
"Americans and Cybersecurity"

PEW RESEARCH CENTER

And beyond these specific experiences, roughly half of Americans (49%) feel that their personal information is less secure than it was five years ago. Around one-in-five (18%) feel that their information has gotten more secure in recent years, while 31% feel that their information is about as safe as it was five years ago. Americans age 50 and older are especially likely to feel that their personal information has become less safe in recent years: 58% of Americans in this age group express this opinion, compared with 41% of those ages 18 to 49.

In addition, many Americans lack faith in various public and private institutions to protect their personal information from bad actors. They express some level of concern about a variety of entities, ranging from telecommunications firms to credit card companies. But their fears are especially pronounced for two institutions in particular: the federal government and social media platforms. Some 28% of Americans are *not confident at all* that the federal government can keep their personal information safe and secure from unauthorized users, while 24% of social media users lack any confidence in these sites to protect their data. By contrast, just 12% of Americans

(and 9% of social media users) have a very high level of confidence that these entities can keep their personal information safe and secure.

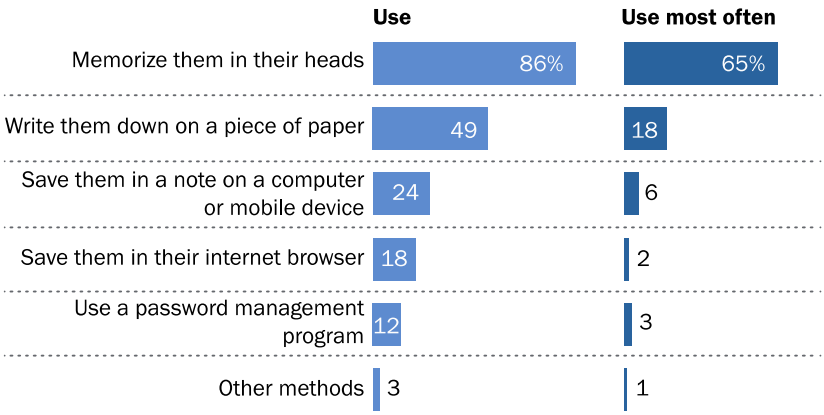
Many Americans fail to follow cybersecurity best practices in their own digital lives

At the same time that they express skepticism about whether the businesses and institutions they interact with can adequately protect their personal information, a substantial share of the public admits that they do not always incorporate cybersecurity best practices into their own digital lives.

This lack of adherence to best practices begins with the ways that Americans keep track of the passwords to their online accounts. Cybersecurity experts generally recommend password management software as the safest and most secure way to track and maintain online passwords.

Most Americans keep track of their online passwords by either memorizing them or writing them down

% internet users who keep track of their online passwords in the following ways



Note: Results for "use most often" category include those who use only one technique to manage their passwords.
Source: Survey conducted March 30-May 3 2016.
"Americans and Cybersecurity"

PEW RESEARCH CENTER

Still, just 12% of internet users say that they ever use password management software themselves – and only 3% say that this is the password technique they rely on most. Instead, roughly two-thirds (65%) of internet users say that memorization is the main or only way they keep track of their online passwords – and another 18% rely primarily on writing their passwords down on a piece of paper. In other words, fully 84% of online adults rely primarily on memorization or pen and paper as their main (or only) approach to password management.

A substantial share of Americans are taking steps or following password protection strategies that experts recommend against:

- 41% of online adults have shared the password to one of their online accounts with a friend or family member.
- 39% say that they use the same (or very similar) passwords for many of their online accounts.
- 25% admit that they often use passwords that are less secure than they'd like, because simpler passwords are easier to remember than more complex ones.

The survey also finds that Americans are not always vigilant in the context of mobile security. For instance, 28% of smartphone owners report that they do not use a screen lock or other security features in order to access their phone, while around one-in-ten report that they never install updates to their smartphone's apps or operating system. Meanwhile, 54% of online adults report that they utilize potentially insecure public Wi-Fi networks – with around one-in-five of these users reporting that they use these networks to perform sensitive activities such as e-commerce or online banking.

To be sure, the story of cybersecurity is far from universally negative. For instance, roughly half of online adults (52%) report that they use two-step authentication on at least some of their online accounts. And majorities indicate that they do in fact take recommended steps such as utilizing different passwords from site to site or placing a security feature on their smartphones. But overall, the way that users treat and manage their online passwords and their overall digital security can be described as mixed at best.

Cybersecurity resources

Cybersecurity experts recommend a number of "best practices" and resources for consumers to minimize their exposure to security breaches.

General information on cybersecurity:

National Cyber Security Alliance StaySafeOnline.org

Consumer information on online security from the Federal Trade Commission

Top-10 safe computing tips from Information Systems and Technology at MIT

Password management:

7 password experts on how to lock down your online security

PC Magazine: The best password managers of 2017

Using public Wi-Fi:

How to stay safe on public Wi-Fi

If your account has been hacked:

FBI Internet Crime Complaint Center

Cybersecurity is not a top-of-mind worry for most Americans

Despite their concerns and experiences, most Americans do not express profound worries about cybersecurity in their personal lives or in their expectations for various public institutions.

In the context of their personal lives, fully 69% of online adults say they do not worry about how secure their online passwords are – more than double the share (30%) that admits to having worries about their personal password security. And Americans who have personally experienced a major data breach are generally no more likely than average to take additional means to secure their passwords (such as using password management software).

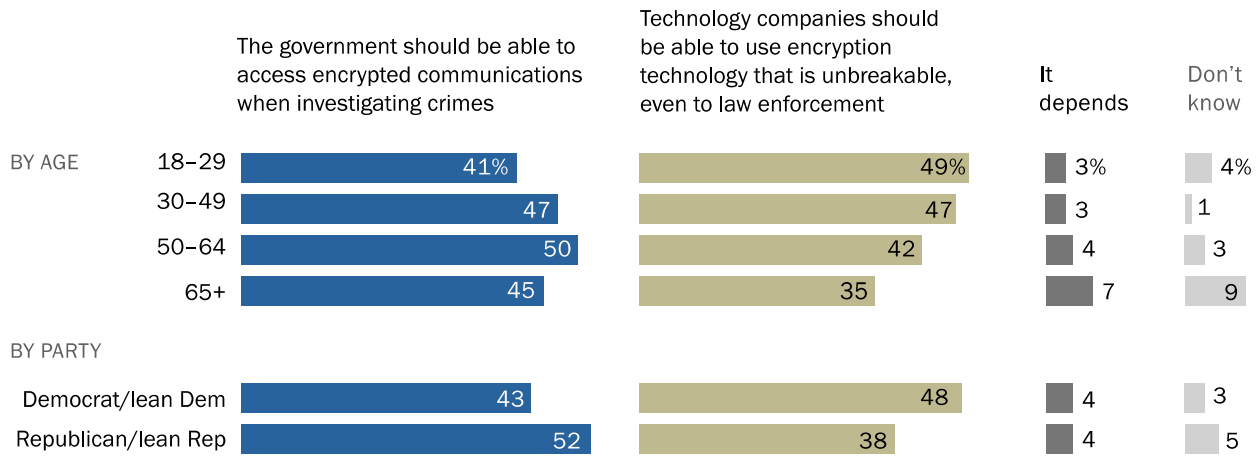
More broadly, a substantial majority of Americans anticipate major cyberattacks in the next five years on our nation's public infrastructure (70% expect that this will happen) or banking and financial systems (66%). Yet a majority of Americans feel that the U.S. government is at least somewhat prepared to handle cyberattacks on our public infrastructure (62%) or government agencies (69%), while 61% have some confidence that U.S. businesses are prepared to handle attacks on their own systems. However, it is worth noting that this survey was fielded prior to the revelations of some more recent, high-profile data breaches, including the hacking of the DNC email system and the breach of email accounts of Yahoo customers.

Americans continue to be highly divided on the issue of encryption

Americans remain divided on the issue of encryption: 46% believe that the government should be able to access encrypted communications when investigating crimes, while 44% believe that technology companies should be able to use encryption tools that are unbreakable even to law enforcement. Democrats and younger adults tend to express greater support for strong encryption, while Republicans tend to express greater support for encryption protocols that can be accessed by law enforcement in the context of criminal investigations.

Younger Americans express elevated support for unbreakable encryption standards

% of U.S. adults who agree with each statement



Source: Survey conducted March 30-May 3 2016.
"Americans and Cybersecurity"

PEW RESEARCH CENTER

1. Americans' experiences with data security

Virtually any digital action that internet users may take – from using credit cards to logging into social media sites – creates data that is stored by companies, governments or other organizations. And when those data are stored, they present opportunities for theft or misuse. This chapter examines the basic contours of the cybersecurity environment for individuals, including: the types of online accounts Americans have, their experiences with various types of data theft, and their overall concerns about the safety and security of their digital information.

The survey illustrates the wide-reaching exposure that many Americans have to the world of cybersecurity. Nearly two-thirds of all Americans (64%) have at least one online account that holds their health, financial or other sensitive personal information. And a similar share (64%) have experienced or been notified of a significant data breach pertaining to their personal data or accounts. More broadly, roughly half the public feels their data have gotten less secure in recent years. Any many Americans express a lack of confidence in various institutions – most notably, the federal government and social media platforms – to safeguard and protect their personal information.

64% of Americans have an online account involving health, financial or other sensitive data

All sorts of online services – from email or social media sites to news or e-commerce platforms – require users to create an account in order to take advantage of them. But some of these services compel users to submit highly personal or sensitive information, such as details of users' financial records or medical history. And these highly sensitive records can be especially damaging if others gain access to them and exploit them. The survey asked about four general categories of these "high value" accounts and found that:

- 55% of Americans report having an online account with banks or other financial service providers.
- 36% have an online account with household utility providers.
- 32% have an online account with their healthcare providers.
- 39% have some other kind of online account that involves bill payments or transactions.

All told, 64% of Americans maintain at least one of the online accounts listed above. College graduates and those with higher household incomes are especially likely to report having all four types of online accounts. For example, half or more of Americans with annual household incomes of $50,000 or more indicate having an online account with banks or financial institutions (73%), utility providers (55%), healthcare providers (50%) or some other type of institution with which they make online transactions (54%). Meanwhile, 42% of Americans in households earning less

than $50,000 per year have an online account with banks or financial institutions and only around one-quarter have an account with utility providers (22%), healthcare providers (18%) or other types of service providers (27%).

Similarly, around three-quarters of college graduates (77%) have an online account with financial institutions, while half or more have online accounts with healthcare providers (53%), utility providers (52%) or some other types of service providers (58%).

Nearly two-thirds of Americans have experienced some form of data theft

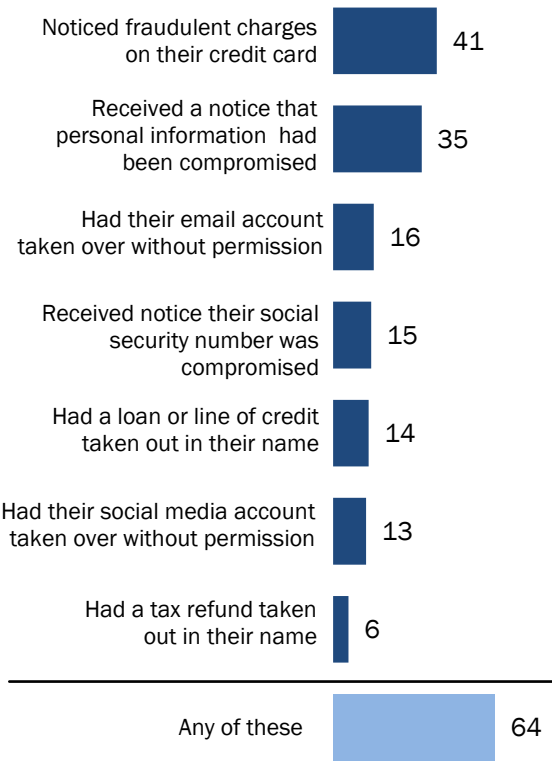
The broader debate over cybersecurity and the safety of Americans' personal data is taking place in an environment where a significant share of the public has personally experienced some type of data theft.

The survey asked about seven different types of identity or data theft that Americans might be exposed to and found that several are particularly widespread. Some 41% of Americans have learned they were the victims of a data breach by seeing fraudulent charges on their credit or debit cards. Around one-third (35%) of Americans have received notices that some sort of sensitive personal information – like an account number – had been compromised, and 15% have received notices that their social security number, specifically, had potentially fallen into the wrong hands.

In other cases, the public experiences data breaches in the context of their major online accounts: 16% of Americans have had someone take over their email accounts without their permission, while 13% say that someone has hacked or taken over one of their social media accounts.

Many Americans have experienced some form of data theft

% of U.S. adults who have ever …



Source: Survey conducted March 30-May 3 2016.
"Americans and Cybersecurity"

PEW RESEARCH CENTER

In addition to these breaches, a notable share of Americans have experienced even more severe forms of data theft. Some 14% of Americans report that someone has attempted to open lines of credit or take out loans using their name, while 6% have had someone impersonate them to try and claim tax refunds. All told, nearly two-thirds of Americans (64%) report that they have experienced at least one of these seven types of data theft.

Americans in their early 30s through mid-60s are especially likely to have encountered many of these forms of data theft. Nearly half (48%) of Americans ages 30 to 64 have noticed fraudulent charges on their credit cards, while around one-in-five (19%) have received notices that their social security number was compromised. Overall, nearly three-quarters of Americans in this age range (72%) have experienced at least one of the seven types of breaches (compared with 55% of those ages 18 to 29 and 50% of those 65 and older). Along with Americans in this age range, college graduates (78% of whom have experienced at least one of these breaches) and those with household incomes of $75,000 or more per year (77%) are also relatively likely to have encountered these various types of data theft.

Many Americans lack trust in key institutions – especially the federal government and social media sites – to protect their personal information

When asked whether they have confidence in various companies and institutions to keep their personal records safe from unauthorized users, Americans' views are decidedly mixed. Some institutions – such as telecommunications firms and credit card companies – inspire relatively broad confidence. In total, around seven-in-ten cellphone owners are very (27%) or somewhat (43%) confident that the companies that manufactured their cellphones can keep their personal information safe; a similar share is very (21%) or somewhat (47%) confident that the companies that provide their cellphone services will protect their information.

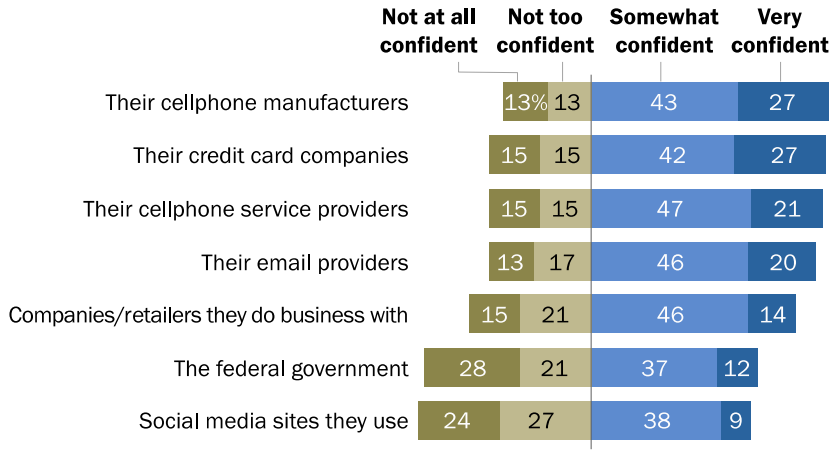
Similarly, around two-thirds of online adults are either very (20%) or somewhat (46%) confident that their email providers will keep their information safe and secure. And roughly six-in-ten Americans are very (23%) or somewhat (36%) confident that their credit card companies can protect their personal information. Other companies and retailers are viewed slightly less confidently: 14% of Americans are very confident (and 46% are somewhat confident) that these entities will keep customers' information safe.

But even as a majority of Americans express at least some confidence in each these institutions, in each instance a notable minority expresses *no confidence at all* in the ability of these entities to protect their personal data.

And some institutions – in particular, the federal government and social media platforms – are viewed with skepticism by a substantial share of the public when it comes to protecting users' personal records. Fully 28% of Americans are *not at all confident* that the federal government can protect their personal information (just 12% are very confident). And 24% of social media users are not at all confident in the ability of these sites to keep their personal information safe – nearly three times the share of social media users (9%) who have a great deal of confidence in these companies.

Roughly half of Americans do not trust the federal government or social media sites to protect their data

% of U.S. adults/tech users (see note below) who are ___ in the ability of the following institutions to protect their data



Note: Data on cellphone manufacturers and service providers based on cellphone owners; data on email providers based on internet users; data on social media sites based on social media users. Data for credit card companies recalculated to exclude "does not apply" responses. Otherwise, refusals and "does not apply" responses not included in this chart.
Source: Survey conducted March 30-May 3, 2016.
"Americans and Cybersecurity"

PEW RESEARCH CENTER

Overall, there is relatively little variation in Americans' attitudes towards these entities based on their demographic characteristics. However, users who have directly experienced certain types of data theft in their own lives tend to have lower levels of confidence in the institutions that were involved in these experiences – particularly when it comes to digital institutions, such as email and social media. Some 22% of Americans who have had their email accounts accessed without their permission are not at all confident in the ability of their email providers to keep their personal information secure – that is double the share (11%) among those who have not directly experienced an email breach themselves. And 40% of those who have experienced a breach of their social media accounts are not at all confident that these platforms can protect their personal information – again double the share (20%) among those who have not had their social media accounts accessed in this way.

On the other hand, Americans' attitudes towards their credit card companies are less strongly correlated with their past experiences with data theft. Among those who have ever noticed fraudulent charges on their credit cards, 13% say they are not at all confident in the ability of these companies to protect their personal information – identical to the share among those who have not experienced this (13%). In fact, one-in-five Americans who have experienced fraudulent charges on their credit cards (22%) indicate that they are *very confident* in the ability of credit card companies to protect their personal information.

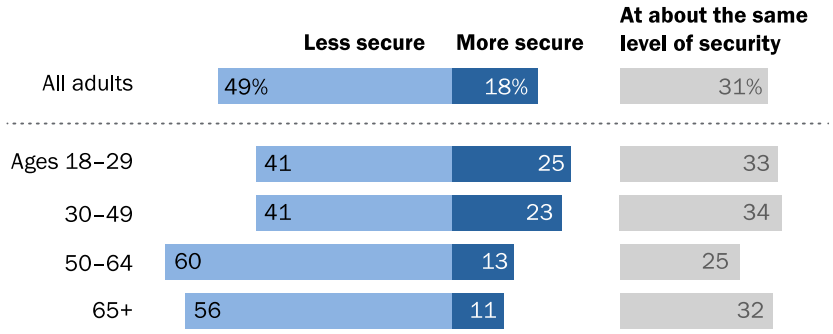
But in the end, relatively few Americans express either blanket confidence or universal concern about the institutions they entrust with their personal information. Just 13% of Americans[1] indicate that they are at least somewhat confident in *all* of these seven institutions, while just 4% indicate that they lack confidence in all of them. The vast majority of Americans fall somewhere in between – they trust some institutions but are skeptical of others.

Roughly half of Americans think their personal data are less secure compared with five years ago

At a broader level, roughly half (49%) of all Americans feel their personal information is less secure than it was five years ago. Around one-third of the public (31%) feels that their data are equally secure now compared with five years ago, while around one-in-five (18%) feel that their data are actually more secure today.

Americans 50 and older express greater concern over personal data security

% of U.S. adults who think their data are ___ compared with five years ago



Source: Survey conducted March 30-May 3, 2016.
"Americans and Cybersecurity"

PEW RESEARCH CENTER

Americans ages 50 and older are especially likely to express concerns that their personal information has become less protected in recent years: 58% of these older Americans feel that their data are less secure than five years ago, while just 12% feel their data are more secure. Americans under the age of 50 tend to express less concern about this issue by comparison: 24% feel that their data are more secure

[1] These figures are based on respondents who answered questions about all seven institutions.

than five years ago. But even so, a plurality of 18- to 49-year-olds (41%) feel their data are less secure now than in recent years.

Outside of age, Americans' attitudes toward this issue do not vary substantially by gender, racial background, household income or educational attainment. However, those who have themselves experienced some sort of data theft or breach express broader concerns about the overall security of their personal information. Roughly half (52%) of Americans who have experienced at least one of the seven types of data theft measured in this survey feel their data are less secure than five years ago, compared with 40% of those who have not experienced any of these forms of data theft.

In addition to these broader concerns about the security of their personal information, Americans express their worries about digital data theft in more concrete ways. Specifically, 69% of online adults report that they have chosen to not open an online account because they were worried about how their personal information would be handled by the site in question. This behavior is largely consistent across a range of demographic groups, although users who have experienced personal data theft themselves are somewhat more wary about signing up for digital platforms. Fully 73% of those who have experienced at least one form of data theft say they have refrained from opening an online account due to their concerns about how their information would be treated, compared with 61% of those who have not experienced any type of data theft.

2. Password management and mobile security

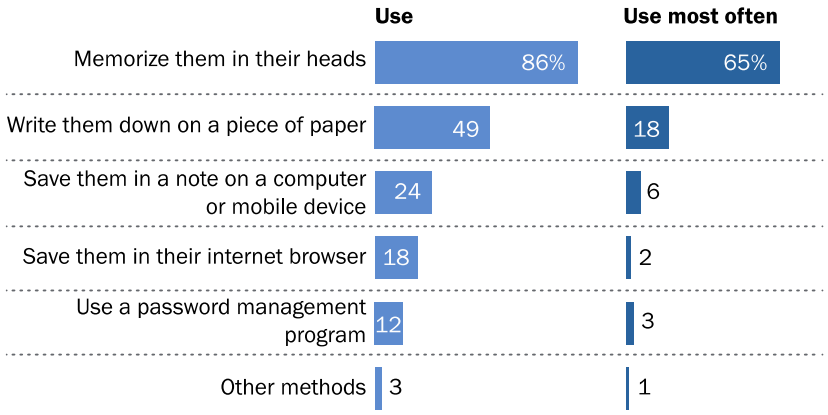
Individuals play a critical role in their own digital security. The weak link in many personal data breaches can be traced back to an overly simple password, an out-of-date smartphone app with missing security patches or the use of an unfamiliar Wi-Fi network. Cybersecurity experts generally recommend a number of steps for users to take in order to reduce their exposure to data theft, such as using a different, complex password for each account; not sharing passwords with others; using some sort of security feature on their smartphones; and always updating their smartphones' apps and operating system to ensure that they have the latest security updates. Although many Americans are utilizing at least some of these steps, this survey finds that less-than-optimum cybersecurity habits are widespread.

Most Americans use memorization or pen and paper as their primary method of keeping track of their online passwords

For average users, creating and storing passwords to their various online accounts is their primary interaction with the world of cybersecurity. Passwords are the first line of defense against unauthorized access to user data, and people's password habits – such as how they manage their passwords, or whether they use passwords that are simple or complex – directly impact their overall security. Many security professionals recommend password management software as the best way to create and store complex passwords. But this survey finds that the vast majority of Americans keep track of their passwords using much more traditional methods – specifically, by memorizing them or by writing them down on a piece of paper.

Most Americans keep track of their online passwords by either memorizing them or writing them down

% internet users who keep track of their online passwords in the following ways



Note: Results for "use most often" category include those who use only one technique to manage their passwords.
Source: Survey conducted March 30-May 3 2016.
"Americans and Cybersecurity"

PEW RESEARCH CENTER

When asked about different ways they might keep track of their online passwords, fully 86% of internet users report that they keep track of them in their heads. Indeed, 65% report that memorization is the method they rely on the most (or is the only method they use) to keep track of their passwords. Around half of online adults (49%) say they keep the passwords to at least some of their online accounts written down on a piece of paper – with 18% saying that this is the method they rely on most heavily. In total, just over eight-in-ten online adults (84%) say that they primarily keep track of their passwords by either memorizing them or writing them down.

Other approaches to password management are far less common. Roughly one-quarter (24%) of online adults keep track of their passwords in a digital note or document on one of their devices (6% say this is the approach they rely on most), while 18% say that they save them using the built-in password saving feature available in most modern browsers (with 2% saying they rely on this technique the most). Most experts agree that saving passwords in browsers is OK if the passwords are unique to each site, however they also agree that password management software outside the browser is preferable. Meanwhile, just 12% of online adults say that they ever use password management software to keep track of their passwords – and only 3% rely on this technique as their primary method for storing passwords.

There are relatively few demographic differences when it comes to how internet users keep track of their passwords. Within every major demographic group, a majority says that memorization is the password management technique they rely on the most – and the differences that do exist on this subject tend to be relatively modest. For instance, those under the age of 50 are more likely than those ages 50 and older to primarily memorize their online passwords (72% vs. 55%), while older users are more likely to say they primarily write their passwords down on a piece of paper (27% vs. 13%). But otherwise, users of all ages manage their online passwords using largely similar approaches.

In addition, the approach to managing password that is most recommended by security professionals – password management software – is used relatively rarely across a wide range of demographic groups. College graduates tend to rely more heavily on these programs than most, but even among this “high usage” group, only 17% use these programs at all – and just 7% indicate that they use them as the sole or primary method for managing their passwords.

Interestingly, users’ personal experiences with data theft are not highly correlated with the steps they take to manage and track their online passwords. Among those who have experienced some type of personal data theft or breach, nearly two-thirds (63%) say that they primarily keep track of their passwords in their head. And although 15% of these users indicate that they use password

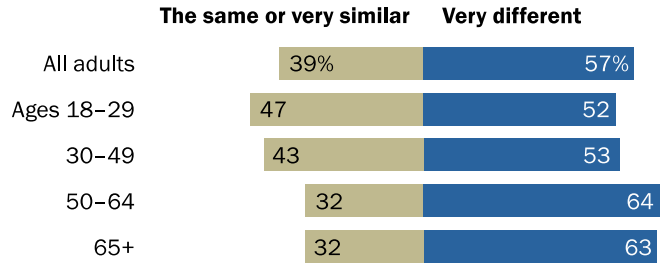
management software for some of their passwords, just 4% say this is the technique they rely on the most.

52% of online adults have used two-factor authentication on their online accounts – but a substantial minority use similar passwords across many sites or share passwords with others

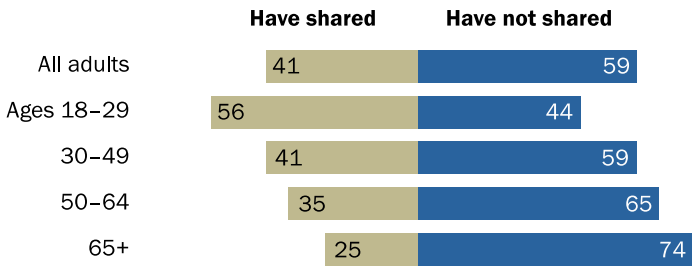
Beyond using password management software, cybersecurity experts recommend a number of other "best practices" to users. These include not using the same passwords across multiple accounts, as well as refraining from sharing passwords with others. When asked about their own behaviors in this regard, a majority of online adults (57%) report that they vary their passwords across their online accounts. However, a substantial minority (39%) indicate that most of their passwords are the same or very similar to one another. In addition, a sizeable minority of online adults (41%) have shared the password to one of their online accounts with friends or family members.

Most online adults say they vary their passwords across sites

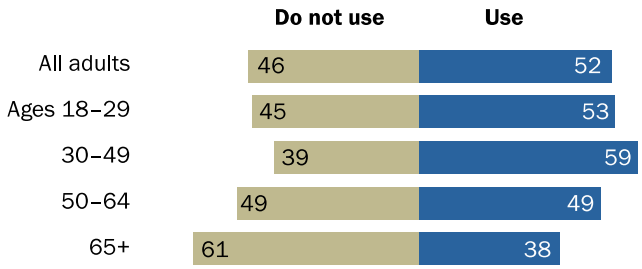
% of internet users who say the passwords they use on their accounts are …



% of internet users who say they ___ passwords with friends or family



% of internet users who say they ___ two-factor authentication



Source: Survey conducted March 30-May 3 2016.
"Americans and Cybersecurity"

PEW RESEARCH CENTER

Those under the age of 50 are especially likely to indicate that their online passwords are very similar to one another: 45% of internet users ages 18 to 49 say this, compared with 32% of those ages 50 and older. And

younger adults are especially likely to share their passwords with others: 56% of 18- to 29-year-old internet users have done so.

Many sites rely on individuals to choose strong passwords as the first line of defense for their online accounts, but there are other technologies that aim to improve – or in some cases replace – the password itself. The first of these techniques is known as "multifactor" or "two-factor" authentication. The "factors" are typically something the user *knows* (such as a password) plus something the user *possesses* (like a code sent to their smartphone). Nearly half of internet users (52%) say that they use this type of multifactor authentication on at least one of their online accounts.

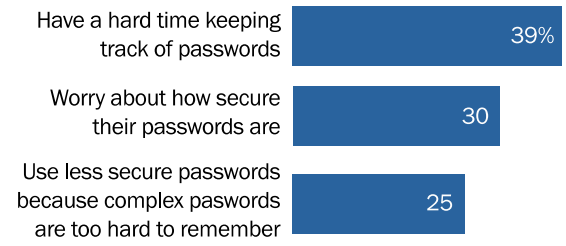
The second of these techniques involves using one's credentials from another site – often a social media platform such as Facebook – to log in to a third party site. Some 39% of social media users say they have logged into another website using the credentials from their social media accounts. Among social media users ages 18 to 29, more than half (56%) have done so.

A substantial minority of online Americans find password management to be a challenge and source of worry

For a relatively substantial minority of online Americans, password management can be a stressful and uncertain process. The survey asked several questions about people's attitudes and concerns about passwords and found that 30% of online adults worry about the overall security of their online passwords, while 25% sometimes use passwords that are less secure than they'd like because remembering more complex passwords is too difficult. For the most part, these behaviors are relatively consistent across different demographic groups.

A substantial minority of online adults express password concerns

% of internet users who say they ever …



Source: Survey conducted March 30-May 3 2016. "Americans and Cybersecurity"

PEW RESEARCH CENTER

In addition, 39% of internet users report that they simply find it challenging to keep up with all of the passwords to their various online accounts. This is relatively common among those in their early 30s through mid-60s: 44% of online adults ages 30 to 64 say they have a hard time keeping track of their passwords, compared with 33% of those ages 18 to 29 and 30% of those 65 and older.

This 39% of the online population that has a hard time keeping track of passwords also expresses concerns about password management in other concrete ways. Compared with the 60% of online adults who do not express difficulties keeping up with their passwords, this "password challenged" group is more likely to …

- Use the same or similar passwords across many different sites (45% vs. 36%)
- Worry about the security of their passwords (44% vs. 22%)
- Use simple passwords rather than complex ones (41% vs. 14%)

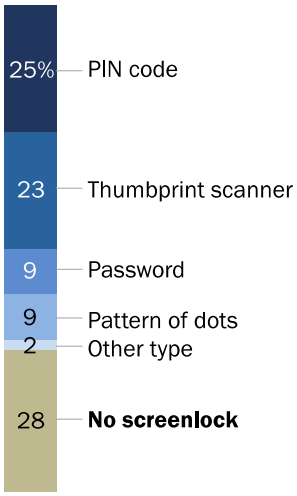
These "password challenged" individuals are also more likely to keep track of their passwords by writing them down on a piece of paper (56% vs. 44%), saving them in a digital note (31% vs. 20%), or by saving them in their internet browser (25% vs. 13%).

More than one-quarter of smartphone owners do not use a screen lock, and many fail to regularly update the apps or operating system on their phones

As smartphones have become increasingly prevalent – and as users engage in a wide range of sensitive behaviors on their phones – these devices have become the latest front in the battle over digital security. In general, smartphones can be compromised in two ways. The first is by gaining possession of the physical phone itself, and security experts recommend the use of a screen lock feature to prevent someone from accessing the contents of a smartphone that falls into the wrong hands. When smartphone owners were asked if they use some form of screen lock on their phones, around one-quarter (28%) reported that they do not.

28% of smartphone owners have no lock screen on their phones

% of smartphone owners who say they access their phones using a ...



Source: Survey conducted March 30-May 3 2016.
"Americans and Cybersecurity"

PEW RESEARCH CENTER

Those smartphone owners who do utilize a screen lock take a wide range of approaches, with numeric PIN codes (used by 25% of smartphone owners) and thumbprint scanners (23%) being the most common. A smaller share uses passwords containing letters, numbers, or symbols (9%), or a connecting pattern of dots (9%).[2]

An especially large share of smartphone owners ages 65 and older (39%) say their devices do not have a lock screen, but it is not uncommon for younger smartphone owners to skip this security step either. Some 28% of smartphone owners ages 18 to 29, 24% of those ages 30 to 49, and 30% of those ages 50 to 64 indicate that their phones do not have any type of screen lock.

Those with lower levels of educational attainment are also relatively likely to forego using a screen lock on their smartphones. Some 80% of smartphone owners with college degrees indicate that they use a screen lock on their phones, but that share falls to 66% among those who have high school diplomas or less.

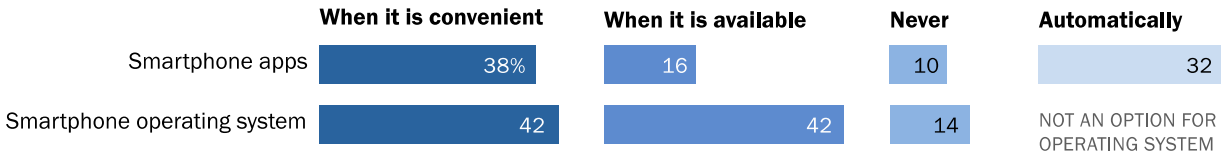
A second way that smartphones can be compromised is through software security flaws – either those that exist in the apps on users' phones or in the smartphone operating system itself. To

prevent this, security experts encourage users to regularly and promptly install updates for their apps and operating system, since these updates often contain important security patches.

But these survey findings indicate that many smartphone owners are slow to update their phones and the apps that come with them – and that in some cases, users are skipping these steps entirely. When it comes to the apps on their mobile devices, around half of smartphone owners indicate that they set them to update automatically (32%) or that they update them manually as soon as a new version is available (16%). However, a comparable share reports that they only update their apps when it happens to be convenient for them (38%) or that they never update the apps on their phones (10%).

Many smartphone owners do not immediately update the apps and operating system on their phones

% of smartphone owners who say they update the apps/operating system on their phone …



Source: Survey conducted March 30-May 3 2016.
"Americans and Cybersecurity"

PEW RESEARCH CENTER

Smartphone owners are similarly divided when it comes to updating the actual operating system on their devices. Some 42% of smartphone owners say that they typically update their operating system as soon as a new version is available, but more than half say that they only update their operating system when it is convenient (42%) or that they never update their phones (14%).

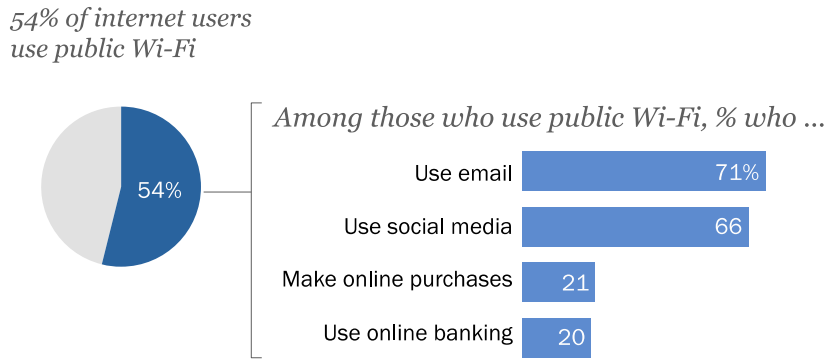
As was the case with screen locks, older smartphone owners tend to update their phones much less consistently than younger users. Some 21% of smartphone owners ages 65 and older say they never update their smartphone apps, while 23% say they never update their operating system. By contrast, just 6% of 18- to 29-year-old smartphone owners never update their apps – indeed, 48% of younger users say they set them to update automatically as they are available – and 13% of these younger users never update their operating system.

Anti-virus software is commonplace on desktop and laptop computers, and the same type of software can be installed on smartphones: 32% of smartphone owners report installing some sort of anti-virus software on their devices.

Just over half of internet users utilize public Wi-Fi networks, including for tasks like online banking or e-commerce

Along with users' passwords and the physical devices they carry, the networks their devices are connected to offer an additional avenue for potential cyberattacks. Public Wi-Fi networks (such as those in cafes, libraries or other public spaces) are an especially common target for hackers. The mechanics behind these attacks vary,[3] and not all public networks are inherently insecure. But in general, security experts recommend that users refrain from performing sensitive activities (such as banking or financial transactions) on public or otherwise unfamiliar Wi-Fi networks.

54% of online adults utilize public Wi-Fi networks



Source: Survey conducted March 30-May 3 2016.
"Americans and Cybersecurity"

PEW RESEARCH CENTER

When asked about their use of public Wi-Fi networks, just over half of internet users (54%) report that they do access Wi-Fi networks in public places. Younger adults are especially likely to do this: 69% of internet users ages 18 to 29 use public Wi-Fi, compared with 54% of those ages 30 to 49, 51% of those ages 50 to 64 and 33% of those 65 and older.

And when asked about some online activities they might engage in while connected to public Wi-Fi networks, most of these users indicate that they have gone online to access their social media accounts (66% of public Wi-Fi users have done this) or to check email (71%). However, around one-in-five of these users have used public Wi-Fi for more sensitive transactions such as online shopping (21%) or banking or other financial transactions (20%).

3 One approach involves hackers reading all of the information being transmitted on an unsecured Wi-Fi network. In a second approach, hackers can create malicious Wi-Fi networks that appear legitimate to unsuspecting users.

3. Attitudes about cybersecurity policy

Cybersecurity does not just impact Americans at an individual level: These issues have potentially profound implications for the U.S. government, law enforcement agencies and the companies and other entities that maintain the nation's infrastructure. On this front, Americans' views and perceptions of the national cybersecurity environment are complex and multifaceted. Although their knowledge of some major cyberattacks that have occurred in recent years is somewhat limited, there is a general public consensus that the coming years will likely see significant attacks on our public infrastructure and financial systems. And the public remains highly divided over the best way to approach issues such as encrypted communications in the context of law enforcement investigations.

A majority of Americans expect significant cyberattacks in the next five years

Many Americans expect that the coming five years will see significant cyberattacks on the country's public infrastructure and financial systems. Fully 70% of Americans expect that the United States will definitely (18%) or probably (51%) experience a significant cyberattack on its public infrastructure (such as air traffic control systems or power grids).

A similar share expects that a significant cyberattack on the country's banking and financial systems will definitely (18%) or probably (48%) happen over the same time frame. Only a small fraction of Americans think that major cyberattacks on our public infrastructure (3%) or financial systems (4%) will *definitely not* occur in the next five years.

Men are somewhat more likely than women to think that there will definitely be major cyberattacks on both our public infrastructure (22% vs. 15%) and financial systems (23% vs. 14%) in the next five years, but otherwise Americans' views on this subject do not differ substantially across demographic groups.

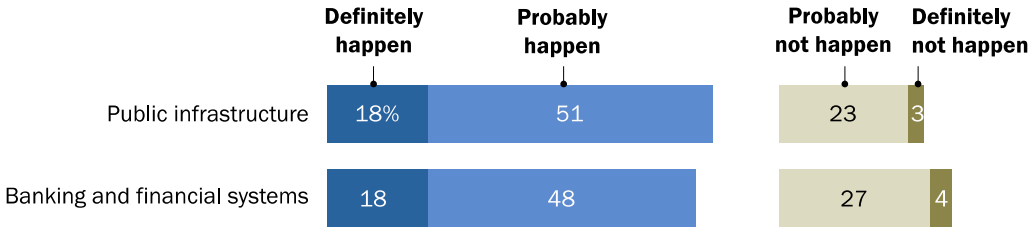
Although a majority of Americans think that significant cyberattacks on our public infrastructure and financial systems are likely in the next five years, they express mixed opinions about the extent to which the government and private industries are prepared to face these attacks.

When it comes to the U.S. government's preparedness to handle these attacks, around six-in-ten Americans feel that the government is very (13%) or somewhat (49%) prepared to prevent a cyberattack on our public infrastructure; a similar share feels that the government is very (18%) or somewhat (51%) prepared to prevent a cyberattack on U.S. government agencies themselves. At the same time, around one-in-ten Americans feel that the government is *not at all prepared* to handle a major cyberattack on public infrastructure (14%) or on government agencies (11%).

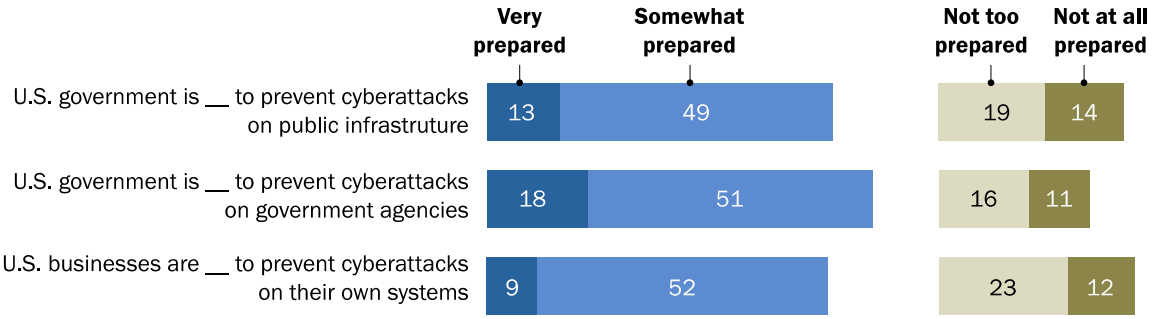
When it comes to their feelings about private industry, roughly six-in-ten Americans feel that U.S. businesses themselves are very (9%) or somewhat (52%) prepared to prevent cyberattacks on their own systems. But 12% think that the private sector is not at all prepared to prevent cyberattacks on their own systems.

Majority of Americans think major cyberattacks will happen in the next five years

% of U.S. adults who think a cyberattack on the following institutions will ____ in the next five years



% of U.S. adults who think the following institutions are ____ to prevent cyberattacks



Source: Survey conducted March 30-May 3 2016.
"Americans and Cybersecurity"

PEW RESEARCH CENTER

Americans' perceptions of how prepared the government and private sector are to defend against cyberattacks are largely consistent across demographic groups. However, those under the age of 50 are somewhat more optimistic than older Americans about the ability of these institutions to withstand future attacks. Those ages 18 to 49 are more likely than older Americans to say that the U.S. government is very prepared to handle cyberattacks on public infrastructure (17% vs. 9%) or

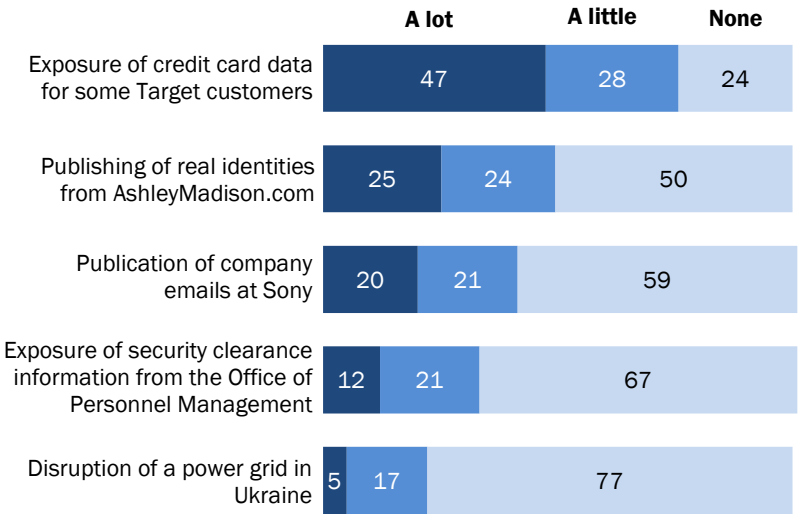
government agencies (24% vs. 12%), and they are also slightly more likely to say that U.S. businesses are very prepared to handle attacks on their own systems (11% vs. 7%).

Americans show widespread awareness of 2011 Target credit card breach, less awareness of some other major cyberattacks

Americans' awareness of a number of high-profile cyberattacks that have occurred in the United States and abroad in recent years is decidedly mixed. The survey asked about five specific attacks and found that Americans are most aware of the breach of credit card data of Target store customers that occurred in 2011 (note: this survey was fielded prior to some more recent high-profile data breaches, including the hacking of the DNC email system and the breach of email accounts of Yahoo customers). A sizeable majority of Americans (75%) have heard at least something about the Target breach, and nearly half the public (47%) has heard a lot about it.

Half of Americans have heard "a lot" about the Target hack, less on other high-profile cyberattacks

% Americans who have heard ___ about each of these events



Source: Survey conducted March 30-May 3 2016.
"Americans and Cybersecurity"

PEW RESEARCH CENTER

Americans are less familiar with two other recent cyberattacks involving private corporations. Around half the public (49%) has heard at least something about the 2015 data breach of the AshleyMadison.com website, with 25% indicating that they have heard a lot about this. And 40% of Americans have some awareness of the 2014 cyberattack on the Sony Corp. that exposed millions of internal corporate emails and documents and damaged the company's internal networks (with 20% indicating that they have heard a lot about it).

The public has much lower awareness of two other attacks that were arguably larger and more dangerous than those discussed above: the 2015 attack on the records of the U.S. government Office of Personnel Management (OPM) and another 2015 attack in which hackers took down a power grid in Ukraine by attacking the grid's computer systems. One-third (33%) of Americans are aware of the OPM attack (with only 12% having heard a lot about it), while around one-in-five (22%) have heard of the Ukraine attack (with just 5% having heard a lot about it). Roughly two-thirds of Americans have not heard anything about the OPM hack, and around three-quarters have no awareness of the Ukraine attack.

Americans remain divided over whether government should be able to access encrypted communications

The issue of encryption – specifically, whether or not the government should legally be able to bypass or decode encrypted communications when investigating criminal cases – has long been a hot-button topic in the ongoing debate over the appropriate balance between individual privacy concerns and the needs of law enforcement in the digital age. This issue again became front page news in 2016, when the FBI obtained a court order to compel Apple to unlock the iPhone of one of the perpetrators of the mass shooting in San Bernadino, California.

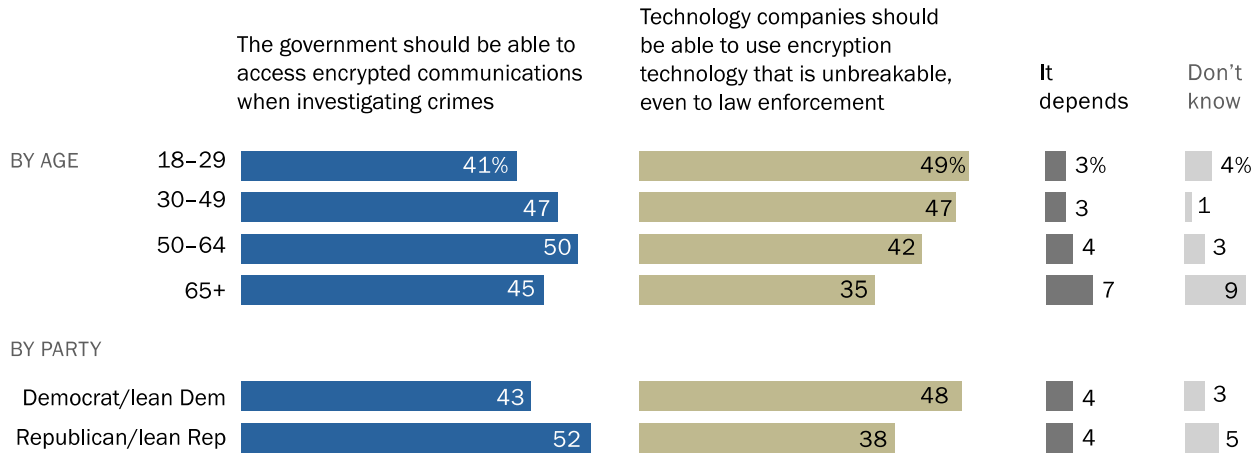
In a Pew Research Center survey conducted at that time, 51% of Americans felt that Apple should be required to unlock the iPhone at the FBI's request, while 38% felt that Apple should not be required to do this.

This survey posed a more general question (with two competing statements) about the tradeoffs between security and privacy, and it finds that Americans' views on this subject remain divided. Fully 46% of Americans agree with the statement: "The government should be able to access encrypted communications when investigating crimes." On the other hand, a comparable share (44%) agrees that "technology companies should be able to use encryption technology that is unbreakable, even to law enforcement." An additional 4% of Americans volunteer that their answer to this question depends on the circumstances.

Men are more likely than women (by a 49% to 39% margin) to say that technology companies should be able to use unbreakable encryption. Conversely, women (51%) are somewhat more likely than men (40%) to support the government's right to access encrypted information when investigating a crime. And although Americans of all ages are somewhat split on this issue, younger adults are more inclined to believe that encryption technologies should be unbreakable even to the government. Roughly half of 18- to 29-year-olds (49%) feel that technology companies should be able to use encryption that is unbreakable to law enforcement, but that figure falls to 35% among Americans 65 and older.

Younger Americans express more support for encryption than older adults

% of Americans who agree with each statement



Source: Survey conducted March 30-May 3 2016.
"Americans and Cybersecurity"

PEW RESEARCH CENTER

There is also a partisan element to these views. Democrats (including independents who lean towards the Democratic party) tend to support the notion that technology companies should be able to use encryption protocols that are unbreakable to law enforcement, although by a fairly close margin (48% vs. 43% who say the government should be able to bypass encryption). Meanwhile, Republicans tend to feel more strongly that the government should be able to access encrypted messages when investigating crimes (by a 53% to 38% margin).

Acknowledgments

This report was made possible by The Pew Charitable Trusts. It is a collaborative effort based on the input and analysis of the following individuals:

Primary researchers

Kenneth Olmstead, *Research Associate*
Aaron Smith, *Associate Director, Research*

Research team

Lee Rainie, *Director, Internet, Science and Technology Research*
Maeve Duggan, *Research Associate*
Monica Anderson, *Research Associate*
Andrew Perrin, *Research Assistant*

Editorial and graphic design

Margaret Porteus, *Information Graphics Designer*
Shannon Greenwood, *Copy editor*

Communications and web publishing

Dana Page, *Senior Communications Manager*
Shannon Greenwood, *Associate Digital Producer*
Travis Mitchell, *Digital Producer*

Methodology

The analysis in this report is based on a Pew Research Center survey conducted from March 30 to May 3, 2016, among a national sample of 1,040 adults, 18 years of age or older, living in all 50 U.S. states and the District of Columbia. Fully 262 respondents were interviewed on landline telephones, and 778 were interviewed on cellphones, including 477 who had no landline telephone. The survey was conducted by interviewers at Princeton Data Source under the direction of Princeton Survey Research Associates International. A combination of landline and cellphone random-digit-dial samples was used; both samples were provided by Survey Sampling International. Interviews were conducted in English and Spanish. Respondents in the landline sample were selected by randomly asking for the youngest adult male or female who was at home. For detailed information about our survey methodology, visit: http://www.pewresearch.org/methodology/u-s-survey-research/

The combined landline and cellphone samples are weighted using an iterative technique that matches gender, age, education, race, Hispanic origin and nativity, and region to parameters from the 2013 Census Bureau's American Community Survey and population density to parameters from the Decennial Census. The sample also is weighted to match current patterns of telephone status (landline only, cellphone only or both landline and cellphone), based on extrapolations from the 2014 National Health Interview Survey. The weighting procedure also accounts for the fact that respondents with both landline phones and cellphones have a greater probability of being included in the combined sample and adjusts for household size among respondents with landline phones. The margins of error reported and statistical tests of significance are adjusted to account for the survey's design effect, a measure of how much efficiency is lost from the weighting procedures.

The margin of sampling error for the complete set of weighted data is ±3.4 percentage points. Results based on the 926 internet users[4] have a margin of sampling error of ±3.6 percentage points.

The following table shows the unweighted sample sizes and the error attributable to sampling that would be expected at the 95% level of confidence for different groups in the survey:

[4] Internet user is defined as those who access the internet or email at least occasionally, or those who access the internet on cellphones, tablets, or other mobile handheld devices at least occasionally.

Group	Unweighted sample size	Plus or minus ...
All adults 18+	1,040	3.4
Men	509	4.9
Women	531	4.8
18-29	170	8.4
30-49	283	6.5
50-64	325	6.1
65+	234	7.3
High school or less	303	6.3
Some college	265	6.7
Bachelor's degree or more	462	5.1

Sample sizes and sampling errors for other subgroups are available upon request.

In addition to sampling error, one should bear in mind that question wording and practical difficulties in conducting surveys can introduce error or bias into the findings of opinion polls. Pew Research Center undertakes all polling activity, including calls to mobile telephone numbers, in compliance with the Telephone Consumer Protection Act and other applicable laws.

Pew Research Center is a nonprofit, tax-exempt 501(c)(3) organization and a subsidiary of The Pew Charitable Trusts, its primary funder.

Topline questionnaire

EMINUSE Do you use the internet or email, at least occasionally?

INTMOB Do you access the internet on a cell phone, tablet or other mobile handheld device, at least occasionally?

	USES INTERNET	DOES NOT USE INTERNET
May 2016	87	13
April 2016	87	13
November 2015	87	13
July 2015	87	13
April 2015	85	15
September 2013	86	14

INTFREQ About how often do you use the internet? [READ]

Based on all internet users [N=926]

	MAY 2016		APRIL 2016	JULY 2015
%	25	Almost constantly	28	24
	50	Several times a day	49	49
	11	About once a day	10	11
	7	Several times a week, OR	7	7
	6	Less often?	6	8
	*	(VOL.) Don't know	*	*
	*	(VOL.) Refused	*	1

DEVICE1a Next, do you have a cell phone, or not?

	YES	NO	(VOL.) DON'T KNOW	(VOL.) REFUSED
May 2016	92	8	0	0
April 2016	92	8	0	0
November 2015	91	9	0	0
July 2015	92	8	*	*
April 2015	92	8	*	0

SMART1 Some cell phones are called “smartphones” because of certain features they have. Is your cell phone a smartphone such as an iPhone, Android, Blackberry or Windows phone, or are you not sure?

Based on cell phone owners

	YES, SMARTPHONE	NO, NOT A SMARTPHONE	NOT SURE/ DON'T KNOW	(VOL.) REFUSED
May 2016 [N=992]	76	17	7	0
April 2016 [N=1,535]	78	16	6	*
November 2015 [N=2,606]	76	17	7	*
July 2015 [N=1,903]	73	20	7	*
April 2015 [N=1,900]	73	21	5	*
September 2013 [N=5,763]	61	32	7	*
August 2013 [N=1,636]	60	33	6	*

SNSINT2 Do you ever use a social media site or app like Facebook, Twitter or LinkedIn?

Based on all internet users [N=926]

	YES	NO	(VOL.) DON'T KNOW	(VOL.) REFUSED
May 2016	74	26	0	*
November 2015	74	26	*	*
July 2015	76	23	*	0
September 2013	74	26	*	0
May 2013	72	28	0	*
December 2012	67	33	*	*
August 2012	69	31	0	*
February 2012	66	34	*	0

ACCT1 Do you have [INSERT ITEMS; RANDOMIZE; 'ANY OTHER ONLINE ACCOUNT' ALWAYS LAST], or not?

Based on all internet users [N=926]

	YES	NO	(VOL.) DOESN'T APPLY / DON'T HAVE THIS ACCT.	(VOL.) DK	(VOL.) REF.
a. Any ONLINE accounts with your bank or financial services provider	64	35	*	1	1
b. Any ONLINE accounts with your health care provider	37	61	*	2	*
c. Any ONLINE accounts with a household utility provider, such as your gas, water, or electric company	41	57	1	1	*
d. Any other online account that involves bill payments or transactions	45	54	0	1	*

ACCT2 Have you ever chosen to NOT use or NOT create an account with an online service because you were worried about how your personal information would be handled?

Based on all internet users [N=926]

	MAY 2016	
%	69	Yes, have done this
	30	No, have not done this
	*	(VOL.) Don't know
	*	(VOL.) Refused

ACCT3 Thinking about some of the companies and organizations that you interact with, how confident are you that they will keep your personal records safe from hackers or unauthorized users? [FOR FIRST TWO RANDOMIZED ITEMS: Thinking about [INSERT ITEMS; RANDOMIZE; ALWAYS ASK ITEMS a AND b TOGETHER AND IN ORDER], how confident are you that these records will be safe from hackers and unauthorized users?

How about…[INSERT NEXT ITEM]? [READ FOR FIRST ITEM THEN AS NECESSARY: Would you say you are very confident, somewhat confident, not too confident, or not at all confident that these records will be safe from hackers and unauthorized users?]

	VERY CONFI-DENT	SOME-WHAT CONF-IDENT	NOT TOO CONFI-DENT	NOT AT ALL CONF-IDENT	(VOL.) DOESN'T APPLY	(VOL.) DK	(VOL.) REF.
Items A-B: Based on cell phone owners [N=992]							
a. The telephone company that provides your cell phone service	21	47	15	15	*	1	1
b. The company that manufactured your cell phone	27	43	13	13	1	3	*
Item C: Based on all internet users [N=926]							
c. Your email provider	20	46	17	13	2	1	*
Item D: Based on social media users [N=665]							
d. The social media sites you use	9	38	27	24	1	*	*
e. The federal government	12	37	21	28	1	1	*
f. Your credit card company	23	36	13	13	15	1	*
g. The companies or retailers you do business with	14	46	21	15	2	2	*

SECUR1 In general, how secure do you feel your personal information is compared with five years ago? Do you think it is [READ] [RANDOMIZE 1-2]

	MAY 2016	
%	49	Less secure
	18	More secure
	31	Or about as secure as it was five years ago
	1	(VOL.) Don't know
	*	(VOL.) Refused

SECUR2 (To the best of your knowledge…) Have you ever…[INSERT ITEMS; RANDOMIZE; ASK ITEMS a AND b TOGETHER IN ORDER]?

	YES	NO	(VOL.) DON'T KNOW	(VOL.) REFUSED
a. Received a notice that your social security number had been compromised	15	84	1	0
b. Received a notice that other sensitive personal information, such as your account number, had been compromised	35	64	1	*
c. Noticed fraudulent charges on your debit or credit card	41	58	*	*
Item D: Based on all internet users [N=926]				
d. Had someone take over your email account without your permission	19	80	1	*
Item E: Based on social media users [N=665]				
e. Had someone take over your social media account without your permission	21	79	*	*
f. Had someone attempt to open a line of credit or apply for a loan using your name	14	84	1	*
g. Had someone attempt to receive a tax refund using your name	6	93	1	*

[READ TO ALL INTERNET USERS:] On a different subject…

HABITS1 Thinking about your online activities, do you ever keep track of your passwords by…[INSERT ITEMS; RANDOMIZE; ASK ITEMS c AND d TOGETHER IN ORDER; 'SOME OTHER WAY' ALWAYS LAST]? How about by…[INSERT NEXT ITEM]? [READ AS NECESSARY: Do you ever keep track of your passwords in this way?]

Based on all internet users [N=926]

	YES	NO	(VOL.) DON'T KNOW	(VOL.) REFUSED
a. Memorizing them in your head	86	14	*	*
b. Writing them down on a piece of paper	49	51	*	*
c. Using a password management program such as Dashlane, Lastpass, or Apple Keychain	12	87	1	*
d. Saving them in a note or document on your computer or mobile device	24	75	*	*
e. Saving them in your internet browser	18	81	*	*
f. Some other way that I haven't already mentioned (SPECIFY)	3	95	1	1

HABITS2 Thinking about the different ways you keep track of your online passwords, which one do you use the MOST? Is it [READ; ONLY INCLUDE "YES" RESPONSES FROM HABITS1; LIST RESPONSES IN SAME ORDER AS HABITS1]?[5]

Based on all internet users [N=926]

	MAY 2016	
%	65	Memorizing them in your head
	18	Writing them down on a piece of paper
	6	Saving them in a note or document on your computer or mobile device
	3	Using a password management program such as Dashlane, Lastpass, or Apple Keychain
	2	Saving them in your internet browser
	1	Some other way
	1	(VOL.) Don't know
	*	(VOL.) Refused
	2	Don't keep track of passwords any of these ways

HABITS3 Thinking about all of the passwords you use to access your various online accounts, would you say that [RANDOMIZE: (most of your passwords are the same or very similar to each other) or that (most of your passwords are very different from each other)]?

Based on all internet users [N=926]

	MAY 2016	
%	57	Most passwords are very different
	39	Most passwords are the same or very similar
	1	(VOL.) Don't know
	2	(VOL.) Refused

[RANDOMIZE HABITS4A THRU HABITS4C]

HABITS4A Do you ever have a hard time keeping track of your passwords, or is this not something that happens to you?

Based on all internet users [N=926]

	MAY 2016	
%	39	Yes
	60	No
	1	(VOL.) Don't know
	*	(VOL.) Refused

[5] Question was asked of respondents who said 'yes' to more than one item in HABITS1. Results shown here have been recalculated to include those who said 'yes' to only one item or said 'no/DK/Refused' to all items in HABITS1.

HABITS4B Do you ever worry about how secure your passwords are, or is this not something you worry about?

Based on all internet users [N=926]

	MAY 2016	
%	30	Yes
	69	No
	*	(VOL.) Don't know
	*	(VOL.) Refused

HABITS4C Do you ever use passwords that are less secure than you'd like because complicated passwords are too hard to remember, or is this not something you do?

Based on all internet users [N=926]

	MAY 2016	
%	25	Yes
	74	No
	1	(VOL.) Don't know
	1	(VOL.) Refused

HABITS5 Have you ever shared a password to one of your online accounts with a friend or family member?

Based on all internet users [N=926]

	MAY 2016	
%	41	Yes
	59	No
	*	(VOL.) Don't know
	*	(VOL.) Refused

HABITS6 Do you use two-factor or two-step authentication for any of your online accounts? [IF RESPONDENT ASKS FOR DEFINITION OF "TWO FACTOR": Two-factor authentication is a feature where you are sent a one-time code via email, text message, or some other method that you would enter after first entering your username and password, and only works for a single login and for a limited amount of time.]

Based on all internet users [N=926]

	MAY 2016	
%	52	Yes
	46	No
	1	(VOL.) Don't know
	1	(VOL.) Refused

HABITS7 Have you ever used your social media account information to log into another website, or have you never done this?

Based on social media users [N=665]

	MAY 2016	
%	39	Yes, have done this
	60	No, have never done this
	1	(VOL.) Don't know
	*	(VOL.) Refused

[READ TO SMARTPHONE OWNER:] Now thinking specifically about your smartphone...

HABITS8 Do you have to use a code, password, or other security feature in order to access your phone?

Based on smartphone owners [N=746]

	MAY 2016	
%	71	Yes
	28	No
	0	(VOL.) Don't know
	1	(VOL.) Refused

HABITS9 What kind of security feature do you use to access your phone? Is it [READ]

Based on those whose smartphone requires a bypass code [N=529]

	MAY 2016	
%	35	A PIN CODE containing only numbers
	13	A PASSWORD containing numbers, letters, or symbols
	12	A pattern of dots you connect with your finger
	32	A thumbprint, OR
	3	Some other kind of screen lock I haven't mentioned yet? (SPECIFY)
	1	(VOL.) Don't know
	5	(VOL.) Refused

HABITS10 Thinking about the APPS on your smartphone, how frequently do you update them? Do you set them to update automatically, do you update them yourself as soon as you are notified that there is a new version available, do you update them yourself whenever it's convenient, or do you never update your apps?

Based on smartphone owners [N=746]

	MAY 2016	
%	32	Set them to update automatically
	16	Update them yourself as soon as a new version is available
	38	Update them yourself whenever it is convenient
	10	Never install app updates
	2	(VOL.) Different settings for different apps
	1	(VOL.) Don't know
	1	(VOL.) Refused

HABITS11 And thinking about the OPERATING SYSTEM on your smartphone, how frequently do you update it? Do you usually update it as soon as you are notified that a new version is available, do you update it whenever it's convenient, or do you never update your smartphone operating system?

Based on smartphone owners [N=746]

	MAY 2016	
%	42	Update as soon as new version is available
	42	Wait until it is convenient
	14	Never update operating system
	1	(VOL.) Don't know
	1	(VOL.) Refused

HABITS12 Have you installed any virus protection apps on your smartphone, or not?

Based on smartphone owners [N=746]

	MAY 2016	
%	32	Yes
	66	No
	2	(VOL.) Don't know
	*	(VOL.) Refused

[READ TO ALL INTERNET USERS:] On a different subject…

WIFI1 Do you ever access public WiFi in places such as airports, cafes, hotels or libraries?

Based on all internet users [N=926]

	MAY 2016	
%	54	Yes
	46	No
	0	(VOL.) Don't know
	*	(VOL.) Refused

WIFI2 Do you ever [INSERT ITEMS; RANDOMIZE] while connected to public WiFi, or not?

	YES	NO	(VOL.) NOT APPLICABLE	(VOL.) DON'T KNOW	(VOL.) REFUSED
Items A-B: Based on internet users who ever access public WiFI [N=502]					
a. Make online purchases	21	78	*	1	*
b. Do online banking or conduct other financial transactions	20	79	0	1	*
Item C: Based on social media users who ever access public WiFI [N=412]					
c. Use social media	80	19	0	1	*
Item D: Based on internet users who ever access public WiFI [N=502]					
d. Use email	71	28	0	*	0

[READ TO ALL:] Next…

POLICY1 Many technology services use encryption of their customers' data and communications. Encryption prevents other people from accessing users' data without their permission, but can also prevent government law enforcement agencies from accessing that data during criminal investigations. Which one of the following statements comes closer to your view, even if neither is exactly right? [READ AND RANDOMIZE]

	MAY 2016	
%	46	The government should be able to access encrypted communications when investigating crimes
	44	Technology companies should be able to use encryption technology that is unbreakable, even to law enforcement
	4	(VOL.) It depends
	4	(VOL.) Don't know
	2	(VOL.) Refused

POLICY2a How likely do you think it is that in the next five years, the United States will experience a significant cyberattack on our public infrastructure, such as our air traffic control system or power grid? Do you think this will definitely happen, probably happen, probably NOT happen, or definitely NOT happen in the next five years?

	MAY 2016	
%	18	Definitely happen
	51	Probably happen
	23	Probably NOT happen
	3	Definitely NOT happen
	4	(VOL.) Don't know
	*	(VOL.) Refused

POLICY2b How likely do you think it is that in the next five years, the United States will experience a significant cyberattack on the banking and financial system? Do you think this will definitely happen, probably happen, probably NOT happen, or definitely NOT happen in the next five years?

	MAY 2016	
%	18	Definitely happen
	48	Probably happen
	27	Probably NOT happen
	4	Definitely NOT happen
	2	(VOL.) Don't know
	*	(VOL.) Refused

POLICY3 How well-prepared do you think the U.S. government is to prevent cyberattacks on our public infrastructure? Is it [READ]

	MAY 2016	
%	13	Very prepared
	49	Somewhat prepared
	19	Not too prepared
	14	Not at all prepared
	4	(VOL.) Don't know
	1	(VOL.) Refused

POLICY4 How well-prepared do you think the U.S. government is to prevent cyberattacks on government agencies? Is it [READ]

	MAY 2016	
%	18	Very prepared
	51	Somewhat prepared
	16	Not too prepared
	11	Not at all prepared
	3	(VOL.) Don't know
	1	(VOL.) Refused

POLICY5 How well-prepared do you think U.S. BUSINESSES are to prevent cyberattacks on their own systems? Are they [READ]

	MAY 2016	
%	9	Very prepared
	52	Somewhat prepared
	23	Not too prepared
	12	Not at all prepared
	4	(VOL.) Don't know
	*	(VOL.) Refused

POLICY6 Thinking about some recent instances of cyberattacks, have you heard anything about [INSERT ITEMS; RANDOMIZE], or is this not something you have heard of? [IF YES, ASK: Have you heard a lot about this, or a little about it?]

Next, have you heard anything about...[INSERT NEXT ITEM]? [IF YES, ASK: Have you heard a lot about this, or a little about it?]

		NET YES, HAVE HEARD	YES, HAVE HEARD A LOT	YES, HAVE HEARD A LITTLE	NO, HAVE NOT HEARD OF THIS	(VOL.) DON'T KNOW	(VOL.) REFUSED
a.	The publication of company emails at the Sony Corporation	40	20	21	59	*	*
b.	The exposure of government security clearance information at the Office of Personnel Management	33	12	21	67	1	*
c.	The exposure of credit card data of customers who shopped at Target stores	75	47	28	24	1	*
d.	The disruption of the power grid in Ukraine	22	5	17	77	1	0
e.	The publishing of the identities of AshleyMadison.com customers	49	25	24	50	1	*