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 (HTTP://WWW.PEWINTERNET.ORG/AUTHOR/KOLMSTEAD/) **AND AARON SMITH** (HTTP://WWW.PEWRESEARCH.ORG/STAFF/AARON-SMITH/)

(jmiks/iStock.com)

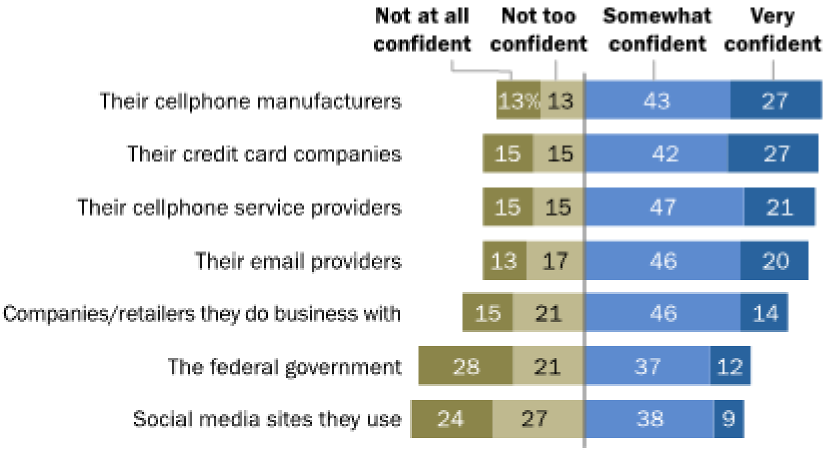
Cyberattacks and data breaches are facts of life for government agencies, businesses and individuals alike in today's digitized and networked world. Just a few of the most high-profile breaches in 2016 alone include the hacking and subsequent release of emails (http://www.cbsnews.com/news/us-has-high-confidence-russian-intelligence-agency-hacked-dnc-dccc/) from members of the Democratic National Committee; the release of testing records of dozens of athletes (https://www.theguardian.com/sport/2016/nov/25/fancy-bears-hack-again-with-attack-on-senior-anti-doping-officials) conducted by the World Anti-Doping Agency; and the announcement by Yahoo (http://venturebeat.com/2016/12/14/yahoo-reveals-another-hack-where-unauthorized-third-party-stole-data-from-1-billion-accounts/) 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 (http://www.armed-services.senate.gov/hearings/17-01-05-foreign-cyber-threats-to-the-united-states) 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 (http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/) of their personal information and many worry (http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/) whether government agencies and major corporations can protect the customer data they collect. As part of this ongoing series of studies (http://www.pewinternet.org/topics/privacy-and-safety/) 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

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

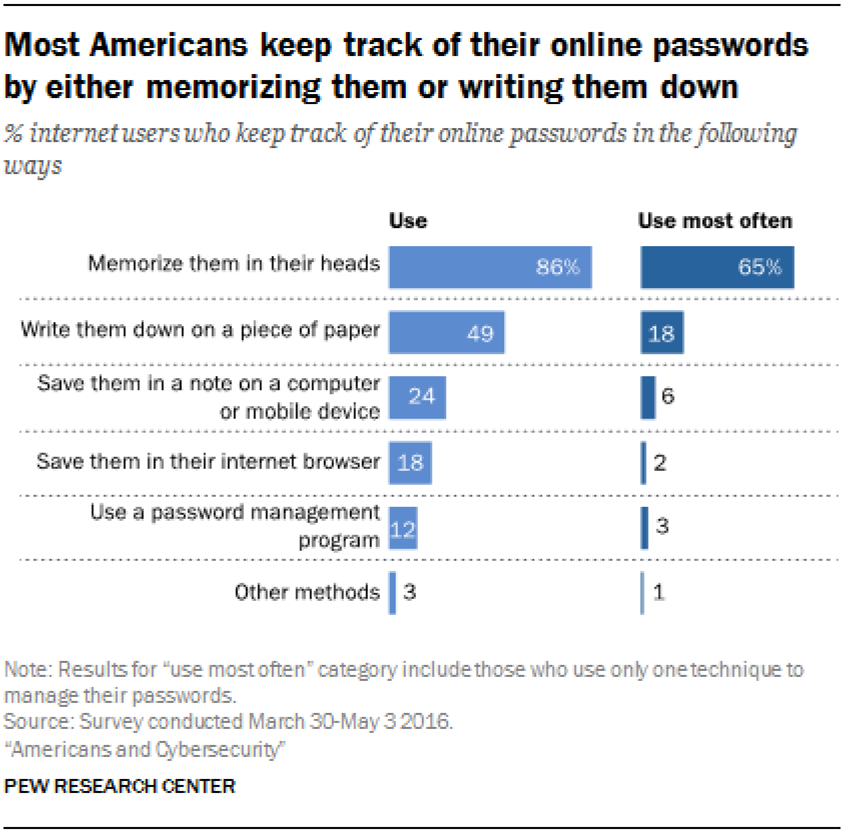
(http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/pi_01-26-cyber-00-02/) Data security is a personal issue for many Americans: The survey finds that a majority of the public has noticed or been notified of a major data breach impacting their sensitive accounts or personal data. The survey 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.

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



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

(http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/pi_01-26-cyber-00-01/) 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.

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.

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 (https://staysafeonline.org/)

Consumer information on online security from the Federal Trade Commission (https://www.consumer.ftc.gov/topics/online-security)

Top-10 safe computing tips from Information Systems and Technology at MIT (https://ist.mit.edu/security/tips)

Password management:

7 password experts on how to lock down your online security (https://www.wired.com/2016/05/password-tips-experts/)

PC Magazine: The best password managers of 2017 (http://www.pcmag.com/article2/0,2817,2407168,00.asp)

Using public Wi-Fi:

How to stay safe on public Wi-Fi (http://fieldguide.gizmodo.com/how-to-stay-safe-on-public-wifi-1779464400)

If your account has been hacked:

FBI Internet Crime Complaint Center (https://www.ic3.gov/default.aspx)

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 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).

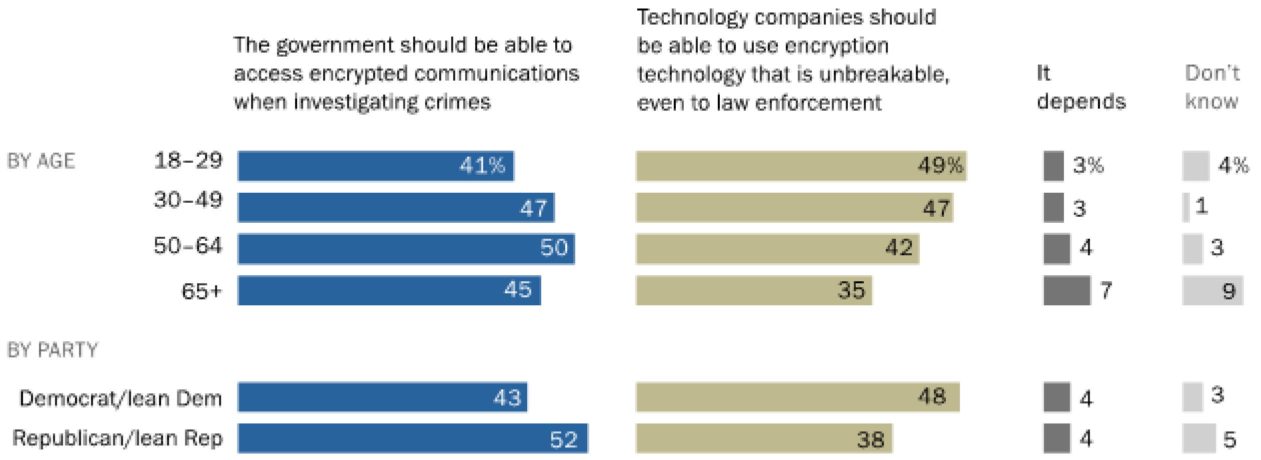
More broadly, a substantial majority of Americans anticipate major cyberattacks in the next five years on our nation's public infrastructure (70% expect that this will happen) or banking and financial systems (66%). Yet a majority of Americans feel that the U.S. government is at least somewhat prepared 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