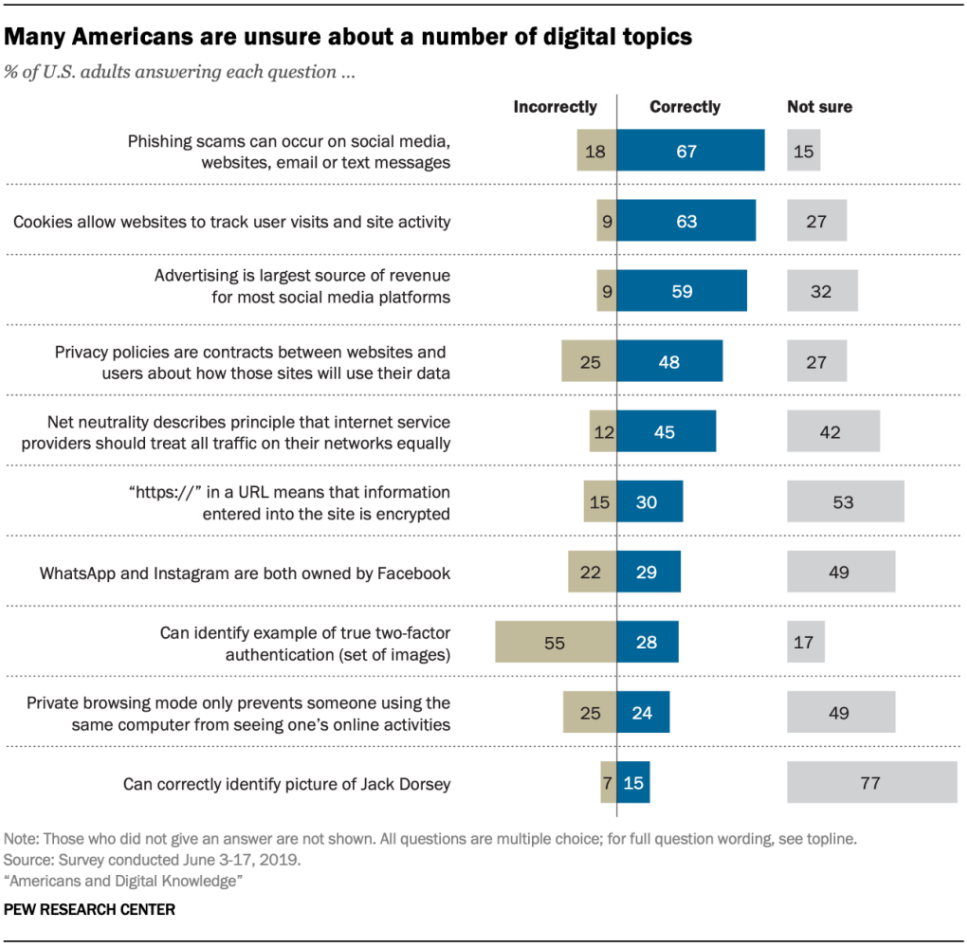
STRONGBOX WEALTH

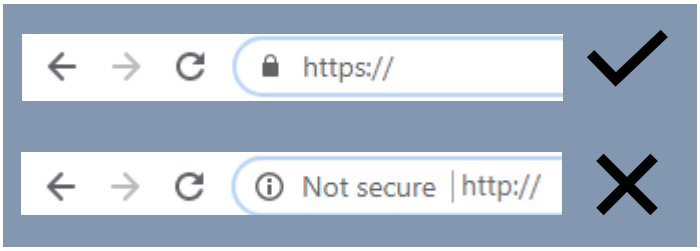
Working from Home: Digital Security Basics

Since the start of the COVID-19 pandemic, millions of workers have begun to work from home. Before this massive transition to remote work, Americans spent an average of 6.42 hours on the internet every day. 36% of internet users in the USA between ages 16-64 were using mobile banking or financial services apps every month, and 20% of internet users in the USA between ages 16-64 use mobile payment services every month.[i] These metrics have likely increased over the last few months, which is a perfect reminder to consider digital security best practices.



While many assume they are up to speed on basic internet security topics, the chart at the left from Pew Research suggests that there are still significant gaps in common understanding of best practices while working or browsing online[ii]. In particular, the chart reveals how a significant percentage of the public is uncertain or uninformed about crucial cybersecurity topics, such as encryption of websites with https://, or two-factor authentication.

Encrypted Browsing



Multi-Factor Authentication

Credit: NIST/Natasha Hanacek

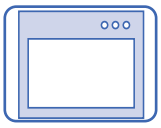
Constant internet connectivity is a very useful resource, but it can also make us more vulnerable to a number of risk factors often taken advantage of by malicious actors. Technology also makes everyone more efficient, including cyber criminals. One study found that 64% of Americans have been impacted by some form of data theft.[iii] Following a few basic procedures in your online life can significantly reduce exposure to cyber-attacks.

Home Network Security

When you first contacted an internet service provider (ISP) to set-up your WiFi and cable, you likely considered the internet speed you needed, what cable channels you wanted, and how much these services would cost. But, once you were connected, did you ask your ISP how to change your router's default password (not to be confused with your WiFi Password)?

Internal Router Administrative Password: Used to access the internal router configuration. All online activity passes through your router before connecting your computer to your ISP, and the internet. Most routers come preconfigured with a default password. These passwords are easily searchable online (for example, at routerpasswords.com) so it is important to change the password to a unique, strong password.

WiFi Network (SSID) Password: Used to access and connect to a wireless network. Change both your SSID and password to something unique. Avoid using your home address or your name, which are also easily guessable. When configuring your wireless network, select a strong encryption method. It is recommended to use WPA2 or WPA3 encryption.



Internet Service Provider (ISP) Password: Create a strong password to manage account settings, internet services, billing details, and device controls on your ISP's customer website.

Firewalls: Firewalls add an extra layer of security to your network by helping to identify and block malicious traffic from unauthorized devices. Many basic ISP packages include firewall protection, which can be configured through your router or with your ISP.

*** Contact your ISP if you need help configuring any of the above.**

Password Best Practices

While configuring your home WiFi, you should have created at least three separate, unique passwords, before creating any passwords for your different devices and applications. According to industry-leading password management firm LastPass, weak or compromised passwords cause approximately 80% of data breaches. Remember to follow the below password basics and avoid reusing the same password across multiple accounts.

Length:

The primary factor that makes a password harder to guess. 8 to 12 characters is the recommended standard, according to CIS and FINRA.

Multi-Factor Authentication:

MFA adds another obstacle for hackers to overcome before they can gain access to one of your accounts.

Password Manager:

Software that stores account credentials in an encrypted, cloud environment, and has the added convenience of remembering your usernames and passwords for you.

Randomness:

Combine words to create longer passphrases, and use a mix of upper-case letters, lowercase letters, numbers, and special characters. For example: Cyb3r$ecur!tyIsGr3at

Phishing Attacks and Social Engineering

Phishing is a cybercrime in which malicious actors attempt to gain access to sensitive personal data by posing as legitimate organizations or people.

According to the FBI, their Internet Crime Complaint Center (IC3) has received and reviewed hundreds of complaints related to COVID-19 phishing scams alone.

Phishing emails are often crafted to appear as if they were sent from health organizations, financial institutions, social media sites, or retailers. Often, phishing emails include suspicious links or attachments that try to trick you into you into taking an action or visiting a website that is against your own best interest.

To stay vigilant against phishing:

Look for spelling and grammar errors both in the content of the email and the sender's address. However, keep in mind that hackers have also learned how to steal and use legitimate email addresses.

Don't click on links until you can verify that they lead to a legitimate website. Hovering over a hyperlink in an email with your cursor will reveal the web address where the link leads, before you click through. If you receive an email that appears to be from a known contact (such as a client, friend or company) and you are unsure if the email, a link, or an attachment is authentic, contact the sender by phone or a separate email (don't just "reply" or "forward") to verify.

Never share your email address, passwords, or any other sensitive personal information via email unless you are absolutely certain of the sender's authenticity and of how the information will be used. Be skeptical of language implying urgency or immediate need. When in doubt, pick up the phone and call to share such personal details for any reason.

Managing Devices

Software Updates: A Pew Research study indicated that more than 50% of smartphone owners update operating systems only when it is convenient and 14% never even bother with updates.[iv] Manufacturers like Apple and Samsung release updates to patch security vulnerabilities, so it's important to update your software, applications, browsers, and firewall protection to the latest versions available. Consider enabling automatic updates for your convenience.

Protecting the Data on Your Device: Survey results indicate that 28% of smart phone owners do not lock their phones with a passcode.[v] Would you leave your home unlocked when you leave for work or an errand? Always lock your devices when you are not using them. Even if one of your devices is lost or stolen, password protection can help protect your data against theft or unwanted access.

Wireless Configurations: Public Wi-Fi networks, like the one in your local Starbucks, don't offer the same security as your private home or work network, yet 20% of internet users report completing financial transactions on public networks.[vi] It is always safest to assume that public networks do not offer any protection to your browsing. Consider configuring your devices so they do not automatically join detected networks (with your private home or work networks as the only exceptions).

Resources and Further Reading

National Institute of Standards and Technology (NIST):

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-114r1.pdf

Center for Internet Security (CIS):

https://www.cisecurity.org/white-papers/cis-controls-telework-and-small-office-network-security-guide/

FINRA:

https://www.finra.org/investors/insights/online-security-tips

---

[i] "Digital 2020". We Are Social. 2020.
https://wearesocial.com/digital-2020
[ii] "Americans and Digital Knowledge". Pew Research Center, Washington, D.C. 2017.
[iii] "Americans and Cybersecurity". Pew Research Center, Washington, D.C. 2017.
https://www.pewresearch.org/internet/2017/01/26/americans-and-cybersecurity/
[iv] "Americans and Cybersecurity". Pew Research Center, Washington, D.C. 2017.
https://www.pewresearch.org/internet/2017/01/26/americans-and-cybersecurity/
[v] Ibid.
[vi] Ibid.