Cyber Security

How to protect yourself from scams while navigating the internet, using email, and moving money

By Linnea Lundberg
Wilmette Public Library Digital Services
llundberg@wilmettelibrary.info
digital@wilmettelibrary.info

Presentation Overview

Terminology
Spam, Scams and Phishing
Navigating the Internet
"How can I be more secure with my technology and accounts?"
What to do if your private information might have been compromised
Watchdog groups and proactive community resources and organizations online
Cited Sources

Terminology

The terms you'll be looking at here are not particularly discrete in practice. They're often lateral processes; they work side-by-side with each other.

Identity Theft is the illegal use of someone else's personal information in order to obtain money or credit.[5]

- There are other reasons why people behave maliciously online, but theft (financial theft, identity theft) and fraud are the most harmful.

Spam is electronic junk mail or the abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages.[2]

Malware is synonymous with 'malicious code.' It is hardware, firmware, or software that is intentionally included or inserted in a system for a harmful purpose.[2]

Spyware is software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious code.[2]

Viruses are computer programs that can copy themselves and infect a computer without permission or knowledge of the user. A virus might corrupt or delete data on a computer, use email programs to spread itself to other computers, or even erase everything on a hard disk. [2]

Ransomware is a type of malicious software, or malware, that prevents you from accessing your computer files, systems, or networks and demands you pay a ransom for their return.[1]

Bots are short for robot. They are software programs that perform automated, repetitive, pre-defined tasks. Bots typically imitate or replace human user behavior. Because they are automated, they operate much faster than human users. They carry out useful functions but they can also come in the form of malware. Internet bots can also be referred to as spiders, crawlers, or web bots. [4] Malicious automated tasks can include the 'crawling' or 'scraping' of webpages for sensitive information in an effort to send malware or spam to users. A lot of websites filter bots out using captchas, "I am not a robot" check boxes to click, or a picture where you select all sections that have cars, street lights, or crosswalks in them.

Phishing schemes are emails, ads, and websites that attempt to collect one's personal and financial information or infect their machine with malware and viruses.[3] Phishing schemes often use spoofing techniques to lure you in and get you to take the bait. These scams are designed to trick you into giving information to criminals that they shouldn't have access to.[6]

Spoofing is when someone disguises an email address, sender name, phone number, or website URL—often just by changing one letter, symbol, or number—to convince you that you are interacting with a trusted source.[6]

Scams & Phishing

How to spot and avoid scam and phishing schemes

"Cybercriminals use sophisticated techniques to appear legitimate; they pose as friends or family members, banks, charities, mortgage vendors, and even healthcare and low-cost prescription providers to steal information in order to conduct identity theft, phishing schemes, credit card fraud, and more."[5]

As described by the FBI's Internet Crime Complaint Center[8], some major scams include:

Tech support scam: Criminals pose as technology support representatives and offer to fix non-existent computer issues. One method they have, is to direct you to download remote access software which gives them complete control over your computer including all your saved passwords and saved files.[11]

Romance/family scam: Criminals pose as interested romantic partners on social media or dating websites. Family/caregiver scam where perpetrators can pose as a relative like a child or grandchild and claim to be in immediate financial need.

Government impersonation scam: Criminals pose as government employees and threaten to arrest or prosecute victims unless they agree to pay.

Sweepstakes/charity/lottery scam: Criminals claim to work for a charitable organization to gain victims' trust, or claim victim has won a foreign lottery or sweepstake, which they can collect for a "fee."

Home repair scam: Criminals appear in person and charge homeowners in advance for home improvement services they never provide.

TV/radio scam: Criminals target potential victims using advertisements about services, such as reverse mortgages or credit repair.

Investment scam: Criminals offer unsuitable investments, fraudulent offerings, and unrecognized products which can result in the theft or misappropriation of funds.

Phishing Trademarks include messages like…[6]

- An important "technical update." Calling the listed number in the email can lead you to straight into a tech support scam.
- "New lower pricing!"
- Fill out this fun survey! First pet's name? First street name? Favorite animal? Year you graduated high school? College?
- Messages from a sender you don't recognize, whose title and email suggests you're good friends or family
- Messages that claim you've won any prizes or money. Requesting your participation in raffles or bids for free things.
- Messages with bad spelling or grammar asking for your charity or financial help

URGENCY!

- Call the police immediately if you feel there is a danger to yourself or a loved one.
- Resist the pressure to act quickly. Many scammers send messages (emails, texts, phone calls, etc) that try to get their victims scared so they'll make irrational decisions and volunteer their information in an effort to stop a fictitious disaster
    - Red letters, exclamation points, words in capitals that effect fear and worry
    - Deadlines and daunting consequences: "you have only 24 hours to do this or you will lose so much money!"

Beware: Pandemic-related scams are soaring, reports Market Watch on September 28th, 2021.[31]

"During the pandemic, we witnessed new scams that involved masks, non-FDA approved medical supplies, immunity boosting products, and equipment through online purchase scams relating to COVID19," says Vee Daniel, president and chief executive officer of the Better Business Bureau (BBB) of upstate South Carolina. But that's just the tip of the iceberg.

Testifying before Congress last week, she said "We have also seen fake websites, phishing emails that involved stimulus checks, price gouging,

scammers impersonating government agencies like Medicare, and promoting fake vaccines. We have also seen an increase in romance scams during COVID-19."

Example of a Malicious Email[32]

The exact email crvdgi@comcast.net is not legitimate, Undisclosed recipients indicates an email sent out to a large number of people, 'Dear member' – there's a capitalization error and any message indicating something so serious would address their 'member' with their actual name. Formatting issues – bolding and small letters for 'Please sign in to your account.' A hyperlink that takes you to a totally different website URL, and another punctuation error, using a comma instead of a period.

Scams and Phishing: Best Practices[3]

Never reveal personal or financial information in an email

Never follow links inside an email requesting personal or financial information from you

Never download attachments in an email unless you are positive you know and trust the sender

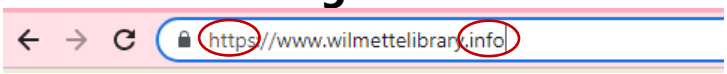
Never reply to emails soliciting personal or financial information from you
Never call the help numbers provided in the email
Never use the information or links provided in the email
Always try to verify the email by contacting the company directly. To find verified and trustworthy contact information to reach the company directly, use the information provided on

- An account statement
- Their official website
- On the back of a credit card
- Look the company's details up on the Better Business Bureau[10] website, https://www.bbb.org
- Report spam and scam emails to your own email provider - google, yahoo, etc.

Navigating the Internet

Passive browsing, sharing, and moving money

Passive Browsing: look at the URLs



HTTPS

The strongest privacy and integrity protection currently available for public web connections is HTTPS, which stands for "HyperText Transfer Protocol Secure"
Where a plain HTTP connection can be easily monitored, modified, and impersonated, an HTTP**S** connection offers the following:

- Confidentiality. The visitor's connection is encrypted, obscuring URLs, cookies, and other sensitive metadata.
- Authenticity. The visitor is talking to the "real" website, and not to an impersonator or through a person-in-the-middle.
- Integrity. The data sent between the visitor and the website has not been tampered with or modified.[20]

Domain suffixes

Website urls that end with ".edu", ".gov", ".org" are educational institutions, government websites, and non-profit organizations, respectively. They are usually safe, reliable sources of information.
Websites with ".info" like the Wilmette Library's usually indicates the site's purpose is to provide users with information. These websites rarely have ads in them.
Website urls that end with ".com" refers to 'commercial.' Many safe, reliable websites are commercial businesses like banks, department stores, etc. but beware of advertisements.[25]
Whenever you're not sure about the business, look it up on bbb.org, The Better Business Bureau[10]

Passive Browsing: Frequent Flyers

Advertisements often lead you to illegitimate websites that may deliver malware, spyware, or viruses to your computer. Be wary of ads on the Internet offering downloadable antispyware—in some cases these products may be fake and may actually contain spyware or other malicious code. It's like buying groceries—shop where you trust. They also might seem like legitimate small-scale sellers of t-shirts, for example, only for you to discover they scam buyers.[12]
Click-bait is when something (such as a headline) designed to make readers want to click on a hyperlink especially when the link leads to content of dubious value or interest. [14]
Toolbars are an example of PUPs, Potentially Unwanted Programs that occur when you download a program you *want* but bundled along with that program, are programs you *don't want*. These programs can just be bloatware or they can be malicious. Either way, monitor your web browser extensions and apps. Also include PUPs as content to scan and remove with your security software.[19]
Browser Extensions. A browser extension is essentially a small piece of software that performs a function or adds a feature to a web browser. Since

extensions are given special authorizations within the web browser, they are attractive targets for attackers.[21]

HTTPS Everywhere, designed by the Electronic Frontier Foundation, www.eff.org, a non-profit that "defends digital privacy, free speech, and innovation." HTTPS Everywhere can be added as an extension to the web browsers Firefox, Chrome, and Opera. It redirects any HTTP websites to HTTPS, thereby encrypting your communications with your websites, making your browsing more secure.[23]

Ad-blocking extensions like uBlock Origin, AdBlock, AdGuard, Ghostery, etc. are great extensions to help you avoid clicking bad content by accident[22]

Sharing: Be careful[9]

The internet is p u b l i c !

The internet is a public resource. Avoid putting anything online that you do not want the public to see or that you may want to retract.[9]

The Internet Archive, aka The Wayback Machine, is a federal U.S. 501(c)3 non-profit whose mission is to preserve and archive important websites and pages all over the internet. There is no barrier for entry. Sign up with your email and start saving and archiving important websites & webpages exactly as you see them. Remember though: people can save the sites and pages *you've* shared your information on using Archive.org too. This is why you must always be careful what information you post onto the worldwide web.[24]

"You cannot take it back. Once you publish something online, it is available to other people and to search engines. You can change or remove information after something has been published, but it is possible that someone has already seen the original version. Even if you try to remove the page(s) from the internet, someone may have saved a copy of the page or used excerpts in another source. Some search engines "cache" copies of web pages; these cached copies may be available after a web page has been deleted or altered. Some web browsers may also maintain a cache of the

web pages a user has visited, so the original version may be stored in a temporary file on the user's computer. Think about these implications before publishing information—once something is out there, you cannot guarantee that you can completely remove it.

View the internet as a novel, not a diary. Make sure you are comfortable with anyone seeing the information you put on blogs, social networking sites, and personal websites—write it with the expectation that it is available for public consumption and that people you have never met will find your page."

Sharing: Pseudonyms

Like many novelists, consider pseudonyms if you want to share or 'publish' opinions or information publicly online without revealing your real name or your real email account.

Pseudonyms are very popular and many websites such as social media and news platforms do not ask for legal credentials, they only ask for valid email addresses, so giving a made-up email address of your *pseudonym* instead of your legal name, is a great extra layer of security.

An example would be to create a new email like marktwain@gmail.com and use that email for anything and everything that *doesn't* require legal credentials (and usually, the only sites that need your legal credentials involve banking or payment).

Remember to write the details of your pseudonym email down so you don't lose access to it.

Sharing: Privacy Settings[17]

Definitely use them, but don't trust them

Sites with Graduated Privacy Settings/Security like Facebook, Skype, LinkedIn, NextDoor, etc. Use those privacy settings and only establish and maintain connections with people you know and trust. Review your connections often. Keep your email concealed from public view. Don't allow the semi-public nature of these sites lull you into a false sense of security: it is still public and bad actors in these social media accounts can still screenshot whatever information you've posted and pass it along to anybody.

This is why it would be best to assume that ANYONE can see any information about your activities, personal life, or professional life that you post and share.

Moving Money: Networks[30]

Use trusted networks.

- The most trusted networks are the ones you've paid for as an individual. The internet connection you have at home is by far the most secure place to move money. Your router has a name, and a very long password string that probably means nothing to you. This means it is very secure
- Your smart phone's internet data plan is another safe, secure way to access the internet. However, it is still ill advised to move money on your phone while in public.

Don’t use public wifi.

Public wi-fi is any wireless internet connection that is open to you as a member of the public (and other members of the public)

- Don’t use public wi-fi to access sensitive information. Don’t enter and submit sensitive information over public wi-fi networks.
- Don't bank over public wi-fi whether it's in a library, a coffee shop, or an airport, or sign into any accounts that hold sensitive information about you (or others). Don't make large purchases, or enter your credit card information over public wi-fi connections.

At the Library

- Library Hotspot, the library’s public wifi, is open to all without a password. It is not secure. If you must move money or submit sensitive data over a public wifi connection like this, ALWAYS check and make sure the URL says ‘HTTPS’ as it encrypts and secures that data. It is “the strongest privacy and integrity protection currently available for public web connections.”
- Patron computers are connected to the internet via Ethernet cords which makes wireless infiltration impossible. Additionally, after a patron ends their session, the computers are set to automatically wipe and

erase everything the patron might have done or saved onto the computer during their time on it. It is very secure.
- Using Mobile Hotspots that have their own lengthy password, meaning there's a very secure wireless connection. You can borrow wifi hotspots at the circulation desk.

Website Security

Even when you're at home, use HTTPS!

The strongest privacy and integrity protection currently available for public web connections is HTTPS, which stands for "HyperText Transfer Protocol Secure"

Where an plain HTTP connection can be easily monitored, modified, and impersonated, an HTTPS connection offers the following:

- Confidentiality. The visitor's connection is encrypted, obscuring URLs, cookies, and other sensitive metadata.
- Authenticity. The visitor is talking to the "real" website, and not to an impersonator or through a person-in-the-middle.
- Integrity. The data sent between the visitor and the website has not been tampered with or modified.[20]

How to be More Secure

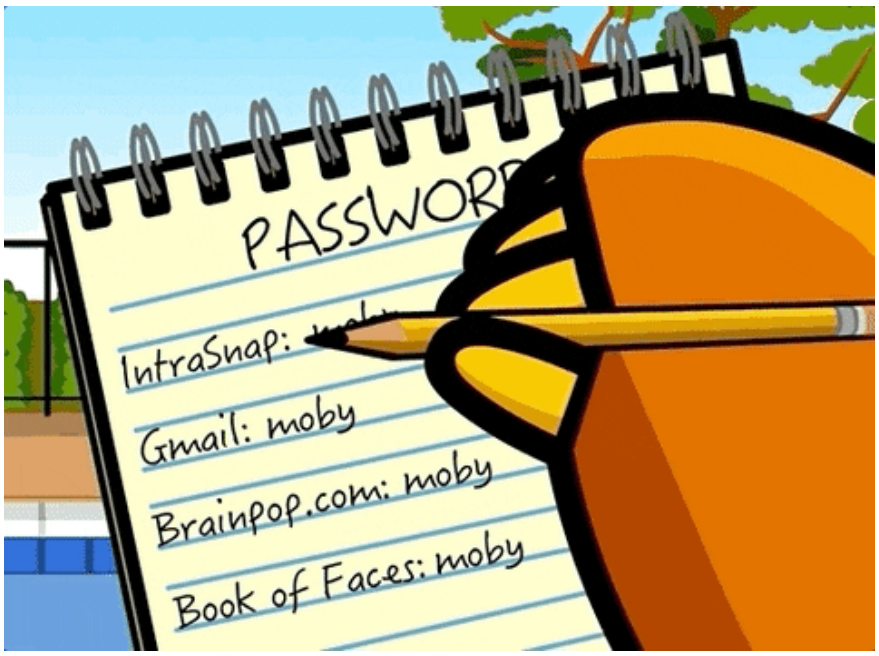
Passwords, updates, and security software

Passwords. Passwords are a common form of authentication and are often the only barrier between you and your personal information. There are several programs attackers can use to help guess or crack passwords. By choosing good passwords and keeping them confidential, you can make it more difficult for an unauthorized person to access your information.[15]

How to get yourself some great passwords!

- Use the longest password or passphrase permissible by each password system. Include upper and lowercase letters, numbers, and special characters
- Do not use passwords that are based on personal information that can be easily accessed or guessed

- Do not use words that can be found in any dictionary of any language. Develop mnemonics to remember complex passwords
- Use different passwords on different systems and accounts
- Consider using a password manager program to keep track of your passwords



In the presentation, this was an animated clip of a robot scratching out the same easy password 'moby' and instead creating unique passwords that use a variety of letters, numbers, special characters, and capitalizations. This robot is doing a great job.
Example: gu$$s9SS8!

How to be more secure? MFA

Multiple Factor Authentication, sometimes referred to as two-factor authentication or 2FA, is a security enhancement that allows you to present two pieces of evidence – your credentials – when logging in to an account. It is a more secure method of authorizing access.[26]
It requires two out of the following three types of credentials: something you know (e.g., a password or personal identification number [PIN]), something you have (e.g., a token or ID card), and something you are (e.g., a biometric fingerprint). [16] [26]
Because one of the required credentials requires physical presence, this step makes it more difficult for a threat actor to compromise your device.[26]

While MFA might be inconvenient, it ensures a great level of security to you and your information.

How to be more secure? Security Software[27]

Forbes' article "Best Antivirus Software Of 2021"[27] lists the following security software (many of which are free - or have free versions - and available to download on their official

Antivirus, antimalware software programs like these run frequent scans on your computer to find any dangerous or potentially dangerous files or data on your computer. Many will also provide a quality rating on whatever websites you're on, as well as scan any new content you've downloaded from the internet to make sure it's clean and safe to open and use.

How to be more secure? Update!

Whenever you see the opportunity to update anything, click 'update'! Updates improve security and privacy of all software on internet-connected devices such as PCs, smartphones and tablets. Updates patch any recently discovered vulnerabilities as well as fix bugs that emerge in the software over time.

Keep all of your personal electronic device software current. Manufacturers issue updates as they discover vulnerabilities in their products. Automatic updates make this easier for many devices—including computers, phones, tablets, and other smart devices—but you may need to manually update other devices. Only apply updates from manufacturer websites and built-in application stores—third-party sites and applications are unreliable and can result in an infected device. When shopping for new connected devices, consider the brand's consistency in providing regular support updates.[26]

Take care especially to update your security software.

Also use and update your PC's firewall. Firewalls provide protection against outside cyber attackers by shielding your computer or network from malicious or unnecessary network traffic. Firewalls can also prevent malicious software from accessing a computer or network via the internet. Firewalls can be configured to block data from certain locations (i.e., computer network addresses), applications, or ports while allowing relevant and necessary data through. [13]

What to do if you think your private information has been compromised[3]

Don't panic

There are very simple steps to take

- Disconnect your computer from the internet and use your security software to scan your computer for malware. At the same time, tell everyone in your household or network. They can be alert for any suspicious or unusual activity.
- If you believe your financial accounts may be compromised, contact your financial institution immediately and close the account(s).
- Watch for any unauthorized charges to your account.
- Consider reporting the attack to your local police department, and file a report with the Federal Trade Commission. The Federal Trade Commission handles scam & spam phone calls, mail, and emails at https://reportfraud.ftc.gov
- Consider filing a report to The Internet Crime Complaint Center, aka the IC3. The IC3 is a division of the FBI and validates reports for those who believe they have been the victim of an internet crime or if they want to file on behalf of another person they believe has been such a victim."[7]
- If you're a senior, an additional resource created by the U.S. Department of Justice (DOJ), Office for Victims of Crime, is the National Elder Fraud Hotline and can be reached at (833) 372–8311. They will walk you through the steps you may have to take.

Watchdog Groups and proactive community Resources and organizations online

Anti-Phishing Working Group (APWG)[28] is an international coalition unifying the global response to cybercrime across industry, government and law-enforcement sectors and NGO communities.

The Better Business Bureau (BBB)[10] is a private, nonprofit organization founded in 1912 focused on advancing marketplace trust. Its vision is "an ethical marketplace where buyers and sellers trust each other" and can be used to find businesses, brands, and charities they can trust. Millions of people turn to BBB each year to view BBB Business Profiles and Charity Reports all available for free on BBB.org. The BBB has a 'Scam Tracker' page that allows consumers to search for and learn more about scams in their area.

The Federal Trade Commission's Pass It On Campaign[18] enlists people 65 and older in an effort to recognize and report fraud and other scams. Topics include imposter scams, identity theft, charity fraud, health care scams, paying too much, and "you've won" scams.

The U.S. Cybersecurity and Infrastructure Security Agency (US-CISA): Current Activity[29] webpage is a regularly updated summary of the most frequent, high-impact types of security incidents currently being reported. Subscribe by email in the footer of their website homepage, https://us-cert.cisa.gov

Have I Been Pwned is a website created by Troy Hunt, a cyber security expert and developer at Microsoft. You navigate to the website, enter your e-mail address, and find out whether your e-mail address has been mentioned in major data breaches. If results pop up, you know it's time to change your e-mail's password as well as the passwords to all the company accounts listed. https://haveibeenpwned.com[33]

Thank You!
Feedback and questions would be greatly appreciated.
You can contact me at llundberg@wilmettelibrary.info or digital@wilmettelibrary.info
Have a wonderful rest of your day.

Works Cited

1. "Cyber Crime". *Federal Bureau Of Investigation*, 2021, https://www.fbi.gov/investigate/cyber.
2. "Glossary". *Computer Security Resource Center*, 2021, https://csrc.nist.gov/glossary.
3. "Spam And Phishing". *Stay Safe Online*, 2021, https://staysafeonline.org/stay-safe-online/identity-theft-fraud-cybercrime/spam-and-phishing.
4. "What Are Bots? – Definition And Explanation". *Kaspersky Lab*, 2021, https://www.kaspersky.com/resource-center/definitions/what-are-bots.
5. "Stop.Think.Connect. Older American Resources". *U.S. Cyber Security and Infrastructure Security Agency*, 2021, https://www.cisa.gov/publication/stopthinkconnect-older-american-resources.
6. "Spoofing And Phishing". *Federal Bureau Of Investigation*, 2021, https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/spoofing-and-phishing.
7. "Internet Crime Complaint Center (IC3)". *Internet Crime Complaint Center*, 2021, https://www.ic3.gov.
8. "Elder Fraud". *Federal Bureau Of Investigation*, 2021, https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/elder-fraud.
9. "Guidelines For Publishing Information Online". *U.S. Cyber Security and Infrastructure Security Agency*, 2021, https://us-cert.cisa.gov/ncas/tips/ST05-013.

10. "BBB: Start With Trust® | Better Business Bureau®". *The Better Business Bureau*, 2021, https://www.bbb.org.
11. Rober, Mark. *Glitterbomb Trap Catches Phone Scammer (Who Gets Arrested)*. Youtube, 2021, https://youtu.be/VrKW58MS12g?list=RDCMUCY1kMZp36IQSyNx_9h4mpCg.
12. "On The Internet". *Federal Bureau Of Investigation*, 2021, https://www.fbi.gov/scams-and-safety/on-the-internet.
13. "Understanding Firewalls For Home And Small Office Use". *U.S. Cyber Security and Infrastructure Security Agency*, 2021, https://us-cert.cisa.gov/ncas/tips/ST04-004.
14. "Clickbait". *Merriam-Webster Dictionary*, 2021, https://www.merriam-webster.com/dictionary/clickbait. Accessed 23 Sept 2021.
15. "Choosing And Protecting Passwords". *U.S. Cyber Security and Infrastructure Security Agency*, 2021, https://us-cert.cisa.gov/ncas/tips/ST04-002.
16. "Back To Basics: What'S Multi-Factor Authentication - And Why Should I Care?". *National Institute Of Standards And Technology*, 2021, https://www.nist.gov/blogs/cybersecurity-insights/back-basics-whats-multi-factor-authentication-and-why-should-i-care.
17. "Social Media Identity Awareness, Protection, and Management Guide". *Department of Defense*, 2021, https://www.robins.af.mil/Portals/59/documents/Social%20Media/Identity%20Awareness,%20Protection%20and%20Management%20Guide%20-%20March%202021.pdf
18. "Consumer Information - Pass It On". *Federal Trade Commission*, 2021, https://www.consumer.ftc.gov/features/feature-0030-pass-it.
19. "PUP Reconsideration Information: How Do We Identify Potentially Unwanted Software?". *Malwarebytes Inc.*, 2021, https://www.malwarebytes.com/pup.
20. "The HTTPS-Only Standard". *Federal Chief Information Office*, 2021, https://https.cio.gov.

21. "Browser Extensions: How To Vet And Install Safely". *Berkeley University*, 2021, https://security.berkeley.edu/education-awareness/browser-extensions-how-vet-and-install-safely.
22. "The Best Ad Blockers In 2021". *Tom's Guide*, 2021, https://www.tomsguide.com/round-up/best-adblockers-privacy-extensions.
23. "HTTPS Everywhere". *Electronic Frontier Foundation*, 2021, https://www.eff.org/https-everywhere.
24. "Internet Archive: Digital Library Of Free & Borrowable Books, Movies, Music & Wayback Machine". *Archive.Org*, 2021, https://archive.org.
25. "Library Guides: Savvy Info Consumers: Internet Domains". *University of Washington*, 2021, https://guides.lib.uw.edu/research/evaluate/domains.
26. "Good Security Habits | CISA". *U.S. Cyber Security and Infrastructure Security Agency*, 2021, https://us-cert.cisa.gov/ncas/tips/ST04-003.
27. Roach, Jacob. "Best Antivirus Software Of 2021". *Forbes Advisor*, 2021, https://www.forbes.com/advisor/business/software/best-antivirus-software.
28. Group, Group-IB, and PhishFarm: Blacklists. "APWG | Unifying The Global Response To Cybercrime". *Apwg.Org*, 2021, https://apwg.org.
29. "Current Activity". *U.S. Cyber Security And Infrastructure Security Agency*, 2021, https://us-cert.cisa.gov/ncas/current-activity.
30. "How To Safely Use Public Wi-Fi Networks". *The Federal Trade Commission*, 2021, https://www.consumer.ftc.gov/articles/how-safely-use-public-wi-fi-networks.
31. Brandis, Paul. "Beware: Pandemic-Related Scams Are Soaring". *Market Watch*, 2021, https://www.marketwatch.com/story/beware-pandemic-related-scams-are-soaring-11632794455. Accessed 6 Oct 2021.
32. Wallace, Fred. "Bad Emails." *Wilmette Public Library*, 2016.
33. Hunt, Troy. 2021, https://haveibeenpwned.com.