Staying Safe with Everchanging Technology

Marshall J. Huckins

Department of Information Technology

21FA_INFO_2805_WW: Network and Information Security Basics

Gary Sparks

Nov. 15, 2021

Abstract

During the COVID-19 pandemic, ransomware has increased through phishing email schemes using the Center for Disease Control and World Health Organization as a disguise. Internet security must be a high priority for every company and individual. Websites, emails, and text messages can contain viruses and malware that are designed to steal data from unsuspecting people. How does an individual or a business proactively navigate the current threat scenario and choose an appropriate solution? Using antivirus and antimalware software is a start to protecting sensitive data and personal information. There is a plethora of free and paid services to protect both individuals and enterprises. There are many factors that lead to the correct choice suitable for the user.

Keywords: information technology, information security, staying safe on the internet, protecting your data

Staying Safe with Everchanging Technology

Information security, or Infosec, is commonplace for companies, but what does it mean for the average consumer? Information security pertains to the security of private data such as personally identifiable information, documents, banking information and more (Cisco, 2021). But what can a person do to keep this information secure? Everyone needs to be proactive when it comes to the protection of personal information. The way this can be achieved is through vigilance, firewalls, antivirus software, and password managers.

Using public WIFI might seem like a convenience to many people, but there are hidden dangers that need to be accounted for. Public WIFI is an unsecure network that leaves users vulnerable to attack from hackers. Hackers will position themselves between the user and the access point, allowing them to receive any information sent between the internet and the user to be seen by the hacker (Dolly, 2018). If using public WIFI is unavoidable, there are a few things one can do to increase the safety of their information. The first thing that should be avoided when using public WIFI is not to access any personal information such as online banking websites, online shopping, or any other website that requires personal information (Dolly, 2018). The next way to stay safe is to use a virtual private network, or VPN, if possible.

Virtual private networks provide two key benefits: privacy and security (Johansen, 2020). VPNs work by masking information like internet protocol (IP) addresses, and search history in order to keep others from tracking this information. VPNs provide security by blocking geographical locations so that hackers won't be able to truly see where the user is located (Turner, 2021). VPNs also keep users secure by protecting personal information and other data when it is being transmitted from the user's device to the web or other devices. Virtual private

networks are not the only way to keep sensitive information secure, using a well-equipped antivirus software is a must have for any technology user.

Antivirus software is software designed to defend and protect computers against malicious threats created by hackers and cybercriminals (Wolphin, 2021). Antivirus software works by scanning computers for threats from emails, software downloads, and web surfing. Different versions of antivirus software work in different ways. Some will monitor and alert as soon as a virus is detected during a download, while others will only alert the user when a computer scan is run manually. Most antivirus software has settings that can be set to download updates and run scans automatically, leaving the user to relax while using the computer. When antivirus software detects a virus, it will put the infected files into quarantine to allow the user to visually inspect what file(s) that has been infected. Regularly running an antivirus scan on computers and mobile devices greatly help reduce chances of having personal information stolen and will help keep users safe. Viruses are just one way hackers can steal information, another way is through the use of malware.

"Malware, or malicious software, is any program or file that is intentionally harmful to a computer, network, or server" (Lutkevich, 2020). Malware is designed to infect computer systems and harm devices or users in some way. Having an antimalware software installed alongside an antivirus software is good practice to help keep networks and devices protected from these attacks. Most malicious software is spread without the user's knowledge or approval. There are different types of malware including viruses, worms, trojan horses, ransomware, adware, and keyloggers. Each of these attacks the computer system in a different manner.

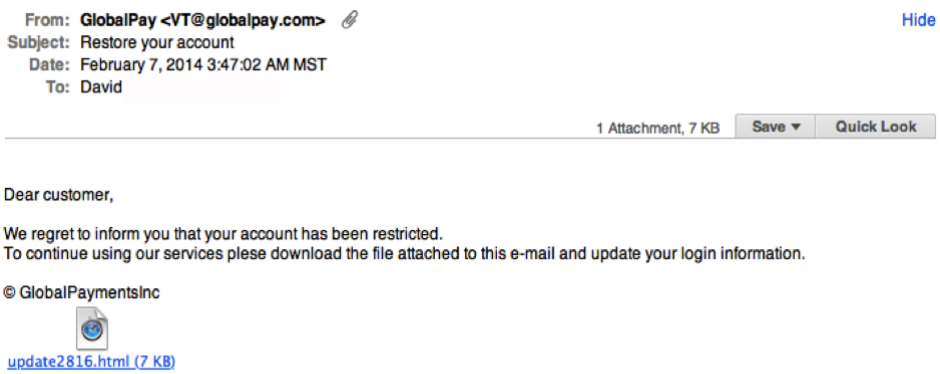
Viruses are the most common form of malware that implements itself and infects other programs or files. Worms generally spread without interaction from the hackers and they can self-replicate. Trojan horses appear as a legitimate software program that is installed and infects the system unbeknownst of the user. Once a trojan horse is installed, the virus can activate their malicious functions to steal information. Ransomeware encrypts the systems information and then the hackers will demand a ransom payment from the victim to decrypt the user's data. Adware is designed to track a web browser's search history with intent to display ads that the user might be interested in making a purchase from. Keyloggers monitor almost everything the user does on their computer, including tracking every keystroke that is made on the device (Lutkevich, 2020). This will give the hacker information such as passwords, credit card information, or any other information that is typed into the computer by the user. Another way to help prevent attacks and keep confidential information secure is to use a firewall.

Firewalls are barriers designed to protect computers and networks from unwanted access. Not only can a firewall be configured to protect devices from unwanted access, but they can also include content filtering to prevent certain websites or connections to other unsavory resources (Cawley, 2020). Firewalls can be either a hardware device or software device. Most home routers have a built-in firewall function that can be programmed to allow certain programs connectivity to the internet. Firewalls are not designed to remove viruses or malware, but rather try and prevent them from being installed in the first place by blocking known malicious programs from reaching devices connected to the network. Using these protections devices is a good start, but it is also up to the consumer to be wary of their activity on the web.

Sometimes, just visiting a website can infect the computer that the user is using. Once it's infected, if there are other devices on the network, they can become infected as well. One good

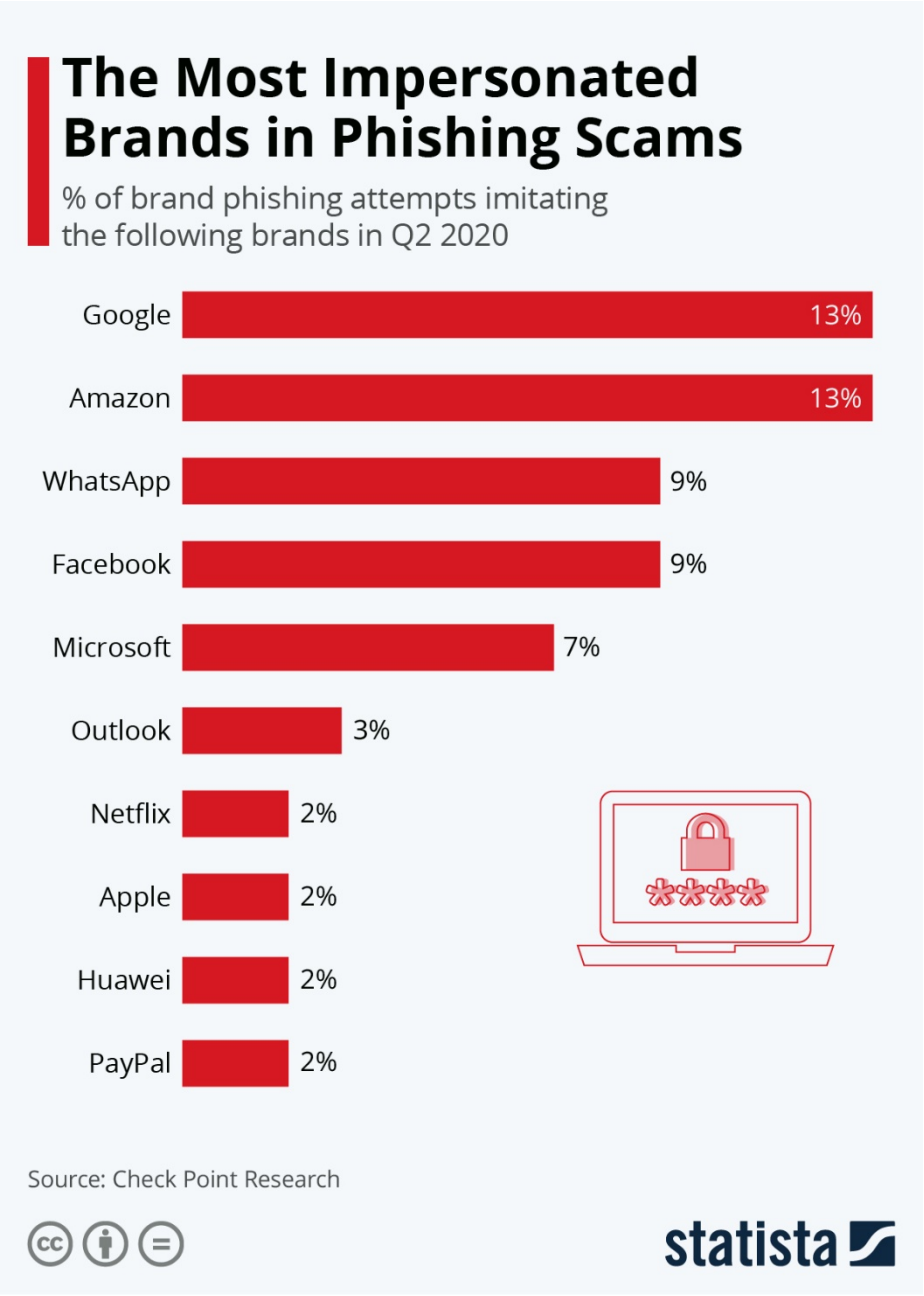
way to tell if a website is secure is to check the address bar. At the beginning of the Uniform Resource Locator, or URL, check to see if there is an “s” following the HTTP word. HTTP stands for Hypertext Transfer Protocol and the accompanying “s” means that the site is secure using a Secure Sockets Layer (SSL) or Transport Layer Security (TLS) certificate (Fruhlinger, 2018). After connecting to a secure website, the next step in preventing data theft is to examine the webpage. Does it look like a legitimate website? If there are a ton of spelling errors or pop-up ads that appear after the page loads, chances are it’s not a legitimate website and the user should disconnect from it. Another reason to raise suspicion is if the website is one the user has been to regularly and knows what it should look like. If, suddenly, the website looks different than normal it is a good idea to verify that the address was typed in correctly and the correct site was accessed. If not, it’s possible the user went to a knock-off website designed to steal information from the user. Websites aren’t the only way to have information stolen, another way is through phishing.

Email phishing is when a hacker imitates a legitimate company to send an email or text message communication to a user in hopes of tricking them into giving out personal information (Ellis). These emails will look legitimate but there are some tell-tale signs that can give away the fact that it is not a legitimate email. This is an example of a phishing email.



It disquises itself as a legitimate email, however no legitimate business will ask to respond with personal information like login information through an email. If the email looks like it is coming from a company that the user normally deals with, it is best to contact the company to find out if it is a legitimate email.

According to Felix Richter with statista.com, Google is the most impersonated company when it comes to phishing scams. This is followed closely by Amazon, WhatsApp, Facebook, and Microsoft. There are many reasons why a hacker might want to steal a users information. The best way to combat these attacks is to read the email address carefully to ensure that it came from the actual business. Some things to look out for include numbers in place of letters. For example, Amaz0n instead of Amazon. Generally, if the email includes a link to a website, it is



best to avoid clicking the link. This can be bait that a hacker hopes the user will click and will take the user to a website that can infect the users computer. Once a hacker has had a chance to infect a computer, they can receive personal information such as a password to a personal account.

Using unique passwords without repeating on multiple websites is a good practice to help prevent theft. If the same password gets used repeatedly on different websites, then hackers only need one password to gain access to all of these sites. “The National Institute of Standards and Technology (NIST) has developed specific guidelines for strong passwords. According to NIST guidance, you should consider using the longest password or passphrase permissible (8–64 characters) when you can (Cisa, 2019).” With having online accounts for all different websites, it can be hard for the average consumer to remember multiple passwords. Using a password manager can help keep passwords strong and remember them for the user.

Some of the benefits of using a password manager include not having to remember multiple unique passwords, having stronger passwords that are harder to crack, and can be faster than having to type the password in manually each time a login is needed (Gray, 2018). A password manager can create a strong password automatically for the user when they are signing up for a new online account or when needing to change a password for the account. Most password managers offer an extension plugin that can be installed right into the web browser. A lot of different password managers also offer cross platform syncing. This means that the user can set it up on multiple devices like their desktop, laptop, cellphone, or tablet. This helps keep a list of passwords secure across all devices without the need to keep a list written down or a file saved to the computer that is susceptible to theft. When the user needs to access their password,

depending on the password manager, the password will automatically fill in the information or it can display the information for the user to copy and paste where it is needed.

Information security is a huge worry for many people today. Private information can range from banking information, identity information like social security numbers or birthdates, or even business account numbers. From viruses to malware to phishing attacks, it's important that the average consumer is aware of how to protect themselves. Antivirus, antimalware, firewalls, virtual private networks, and awareness are all important ways for people to protect themselves.

References

Cawley, C. (2020, August 25). *5 reasons why you should use a firewall*. MUO. Retrieved November 1, 2021, from https://www.makeuseof.com/tag/5-reasons-use-firewall/.

Cisa. (2019, November 18). *Security tip (ST04-002)*. Cybersecurity and Infrastructure Security Agency CISA. Retrieved November 15, 2021, from https://us-cert.cisa.gov/ncas/tips/ST04-002.

Cisco. (2021, September 21). *What is cybersecurity?* Cisco. Retrieved October 17, 2021, from https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html#~how-cybersecurity-works.

Dolly, J. (2018, January 9). *Why you should never, ever connect to public wi-fi*. CSO Online. Retrieved November 1, 2021, from https://www.csoonline.com/article/3246984/why-you-should-never-ever-connect-to-public-wi-fi.html.

Ellis, D. (n.d.). *7 ways to recognize a phishing email: Email phishing examples*. SecurityMetrics. Retrieved November 15, 2021, from https://www.securitymetrics.com/blog/7-ways-recognize-phishing-email.

Fruhlinger, J. (2018, December 4). *What is SSL, TLS? and how this encryption protocol works*. CSO Online. Retrieved November 15, 2021, from https://www.csoonline.com/article/3246212/what-is-ssl-tls-and-how-this-encryption-protocol-works.html.

Gray, K. (2018, April 24). *5 benefits of using a password manager*. 5 Benefits of using a password manager. Retrieved October 17, 2021, from https://blog.envisionitsolutions.com/5-benefits-of-using-a-password-manager.

Johansen, A. G. (2020, August 4). *10 benefits of a VPN you might not know about*. NortonLifeLock. Retrieved October 17, 2021, from https://us.norton.com/internetsecurity-privacy-benefits-of-vpn.html.

Lutkevich, B. (2020, November 3). *What is malware? definition from searchsecurity*. SearchSecurity. Retrieved November 1, 2021, from https://searchsecurity.techtarget.com/definition/malware.

Richter, F. (2020, August 11). *Infographic: The most impersonated brands in phishing scams*. Statista Infographics. Retrieved November 16, 2021, from https://www.statista.com/chart/22528/most-impersonated-brands-in-phishing-attacks/.

Turner, J. (2021, July 29). *Are vpns safe to use? – safe VPNS rated: Tech.co 2021*. Tech.co. Retrieved November 1, 2021, from https://tech.co/vpn/are-vpns-safe.

Wolphin, S. (2021, March 22). *How does antivirus software work?* How Does Antivirus Software Work? Retrieved November 1, 2021, from https://www.usnews.com/360-reviews/antivirus/how-does-antivirus-software-work.