Aiden Payne

Professor Norman

English 211C

13 April 2024

# Research Piece: CyberSecurity and Cyber Hygiene

The internet has become a staple in the daily lives of billions of people across the world. Since 2005, the internet has grown in users from one billion to about five billion. Nearly three-quarters of the planet uses the internet in some way for their daily lives. With the internet's large population as well as the freedom that comes within cyberspace it's no wonder that cybercrime has also grown tremendously. According to Cisco, cybercrime is an illegal activity that involves the internet and computers (What is cybercrime?). In fact, according to the Federal Bureau of Investigation cybercrime-related losses in the U.S. have gone up by five times since the year 2018 (Petrosyan). With statistics like these, becoming a victim of cybercrime would seem inevitable right? Not exactly, practicing proper cyber hygiene can allow individuals and companies to mitigate cybercrime and financial losses.

Cybersecurity is defined as “the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information”(What is Cybersecurity?). Cybersecurity has become indispensable with internet usage increasing exponentially, and cybercrime becoming a pandemic. With this definition of cybersecurity, we can see the goals of cybersecurity and why it is so important in our daily lives.

The three basic aspects of cybersecurity are known as the CIA triad; this abbreviation stands for Confidentiality, integrity, and availability. Confidentiality refers to measures taken to keep sensitive data out of unauthorized hands or people who shouldn't have the data. Integrity refers to the integrity of data and keeping it unmodified in storage or sending and receiving data. Availability refers to measures taken to keep data and systems available for users at all times.

So why are these concepts important? Using these three concepts of cyber security can help businesses and users create basic cybersecurity frameworks (CIA triad). These principles are the basic foundation of almost every cybersecurity framework. They allow organizations to create frameworks that are tailored to their needs while not becoming too expensive or too much to deal with. Many companies, especially small businesses, might overlook cybersecurity because they see it as too expensive or too complicated. While this may be a decent point, resources like the NIST ( National Institute of Standards and Technology) have created a Cybersecurity framework to help with this issue. The NIST framework "provides guidance to industry, government agencies, and other organizations to manage cybersecurity risks"(The NIST Cybersecurity Framework (CSF) 2.0).

So they are reliable but what about small businesses that are not technologically advanced? The NIST also says the framework "offers a taxonomy of high-level cybersecurity outcomes that can be used by any organization — regardless of its size, sector, or maturity — to better understand, assess, prioritize, and communicate its cybersecurity efforts."(The NIST Cybersecurity Framework (CSF) 2.0). With security in mind, the NIST makes it as easy as possible for all businesses regardless of size to become proficient in cybersecurity and mitigate risks. Cybersecurity allows businesses to utilize the internet while remaining relatively safe and mitigating cyber risks and financial loss. Any company that utilizes the internet for transactions or even simply has a web page will use some sort of cybersecurity to ensure the safety of their business and customers.

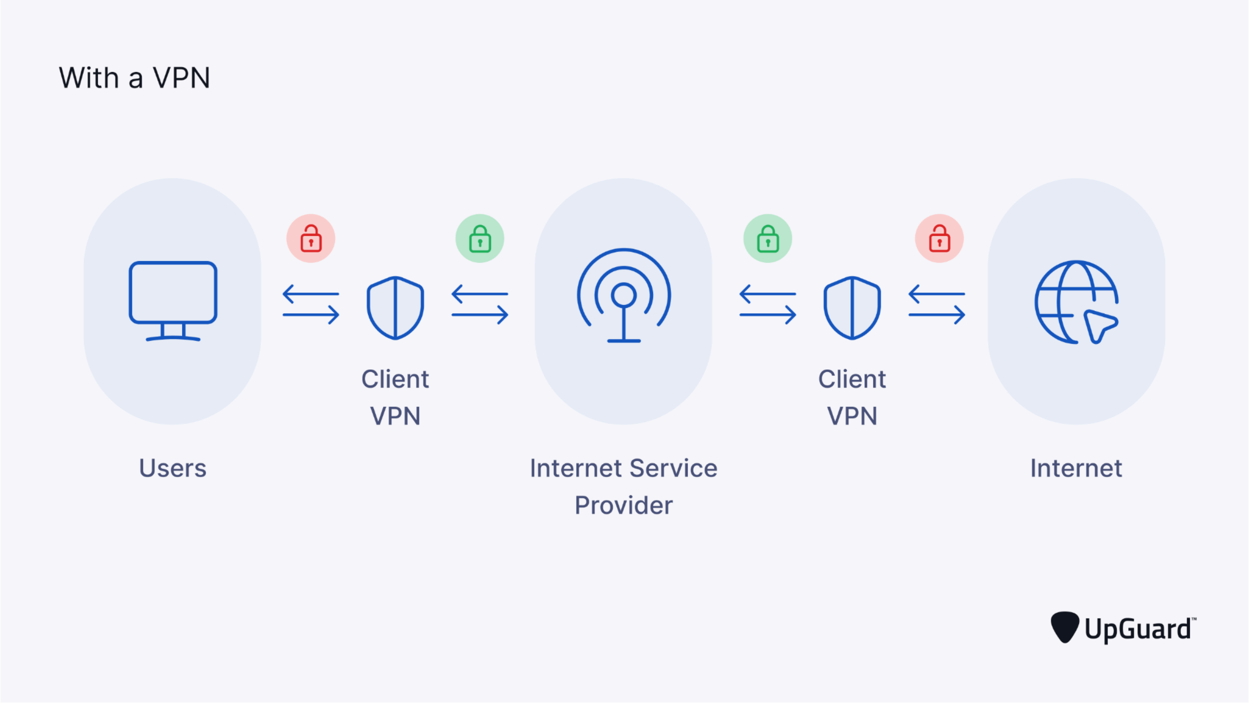
Cybersecurity is essential for business in the modern age, but how does it affect individuals? In 2005 the number of Americans using online banking was 36% and in 2021 the number of Americans is now 73% and continues to grow by the millions each year (Lindner). With the number of users increasing every day, Americans need to understand that cybersecurity is keeping their banks secure and their money safe. Many other industries and platforms, like Infrastructure, careers, and schools, rely on cybersecurity to keep information safe. With all of these industries being essential to life in the United States, the need for cybersecurity is indisputable.

Cybersecurity is imperative because it helps businesses and corporations keep society's information safe. While this is great for businesses, how can the average person protect themselves from day to day? The best way to protect ourselves while we browse online or engage in online purchases is to practice proper cyber hygiene. The idea behind cyber hygiene is that it "relates to the practices and precautions users take with the aim of keeping sensitive data organized, safe, and secure from theft and outside attacks" (Brook). It is argued that proper cyber hygiene is for businesses and corporations; however, everyone needs to practice cyber hygiene to become secure while doing anything online because we are always one malicious link away from becoming a victim of cybercrime. Cyber hygiene is relatively free except for subscription-based protections like VPNs (virtual private networks) and anti-virus software. With the low entry cost, everyone can efficiently practice proper cyber hygiene and significantly reduce their risks while using the internet. Studies show that "Adhering to basic security hygiene can protect against 98% of attacks" (Nguyen). With this statistic alone we can see just how important it is to practice security hygiene. Proper cyber hygiene is important but what does it look like? A very easy way to start becoming secure would be to update the software of systems around the house like phones, computers, and other devices connected to the internet. Keeping these devices up to date ensures that they are up to the latest standards in software security supplied by their manufacturers. Not updating systems can lead them to be unpatched by developers and increase their vulnerability to attacks.

Another way that users can practice proper cyber hygiene is by enabling multi-factor authentication on applications that support it. Multi-factor authentication is the process of gaining authorization by proving identity. Users may log onto applications by using facial recognition, email/text authorization codes, and other devices to prove their identity. MFA(multi-factor authentication) is extremely easy to set up and it won't be needed that often depending on the sensitivity of the information being accessed. Studies have shown that enabling MFA can "help prevent 99.9% of attacks on your accounts."(Nguyen). Within a couple of minutes, users can ensure that almost all attacks on their accounts will be mitigated by simply enabling multi-factor authentication.

How can we remain safe while browsing the internet? Browsing and engaging in malicious links on the internet can be detrimental, but this can easily be avoided. The first way users can avoid malicious websites and links would be to look at the website's link and analyze the protocol and the top-level domain. The protocol is "HTTP" or "HTTPS" and the top-level domain is the websites ".com" or ".org". The difference between the two protocols is that HTTPS uses a form of encryption called transport layer security (TLS) which makes sure the information on HTTPS is encrypted (Why is HTTP not secure? | HTTP vs. HTTPS). Websites with the protocol "HTTPS" ensure that the information being sent between the user and the website is secure and encrypted. This guarantees that the information being shared by the user such as location and information inputs are only viewed by the website and the user. This is important in keeping our information secure when it comes to browsing. Utilizing a VPN (Virtual Private Network) can ensure safety while browsing online. A VPN “establishes a digital connection between your computer and a remote server owned by a VPN provider, creating a point-to-point tunnel that encrypts your data, masks your IP address, and lets you sidestep website blocks and firewalls on the internet.”(What is a VPN?). A VPN allows users to funnel their information through a separate secure web address so they aren't at risk of any cybercriminals or websites collecting the user's information.

Here is a simplified diagram explaining the functions of a VPN.



Between the use of a VPN and ensuring the credibility of a website, users can significantly decrease their chances of becoming a victim of cybercrime. The last main topic of cyber hygiene is to be security-minded when interacting with other people on the internet, either through text, email, or calls. While there is software for protecting users from malicious code there is rarely anything protecting users from their interactions with other people or bots besides their knowledge and safety. Protecting ourselves from phishing attacks and being aware of scams online can significantly reduce the risk we face when utilizing the internet. Phishing is when scammers send fake emails or text messages claiming to be a legitimate company to steal something from the user. A recent study showed that there are around  3.4 billion spam emails sent every day (The latest 2024 phishing statistics). With this amount of phishing emails being sent out every day, it's important to analyze emails very carefully. We can do this by checking over emails for typos, we can also look at the email address to see if there are typos; lastly, we can search the email address on a web browser to see if a legitimate website or company shows up. Another rule to use while communicating online would be a zero-trust policy. Zero-trust entails not trusting anyone until they are proven to be legit in whatever they say they are. Implementing a zero-trust policy within our use of the internet can allow us to be safe to the fullest extent. Proper cyber hygiene is essential to remaining safe online in the current day and when not taken seriously it can have detrimental effects mentally, physically, and financially.

So we know what cybersecurity is and we know what proper cyber hygiene is, but is it the end of the world if we don't utilize these safety measures? Yes, while cyber security may not seem needed in everyday life, there are many examples of companies and individuals who have become victims of cybercrime and have taken massive losses. For example, the colonial pipeline became the next big victim of a cyber attack. In 2021 a group by the name of DarkSide gained access to the company's infrastructure through a retired account. After the group received access they used an attack vector called ransomware to encrypt the data. DarkSide then shut down the pipeline for five days which created serious panic and gas shortages on the east coast. On June 12th the ransom of 75 bitcoin was paid to DarkSide (Kerner). With just this one example we can easily see how the effects of not taking cybersecurity seriously can affect millions of people. The number of cyber-attacks has slightly decreased from 2021-2022 by about 50,000, but the losses due to cybercrime increased by almost 4 billion dollars (USAFacts team). With around 800,000 businesses and individuals victimized by cybercrime each year, the consequences of not taking cybersecurity seriously are obvious (USAFacts team).

In conclusion, as the amount of cybercrime increases the need for taking cybersecurity seriously must also increase to ensure the safety of our businesses, banks, and country's infrastructure. The need for practicing proper cyber hygiene will also continue to grow in importance to ensure that our use of the internet remains safe from the exploitation of cyber criminals. Gaining a basic understanding of how we can implement these into our daily lives will allow cyberspace to become secure one user at a time.

# Works Cited

“Basic Cyber Hygiene Prevents 98% of Attacks.” *TECHCOMMUNITY.MICROSOFT.COM*, 14 Sept. 2023, techcommunity.microsoft.com/t5/security-compliance-and-identity/basic-cyber-hygiene-prevents-98-of-attacks/ba-p/3926856#:~:text=In%20today’s%20digital%20era%2C%20businesses,protect%20against%2098%25%20of%20attacks.

Chris Brook on Saturday May 6, et al. “What Is Cyber Hygiene? A Definition of Cyber Hygiene, Benefits, Best Practices, and More.” *Digital Guardian*, www.digitalguardian.com/blog/what-cyber-hygiene-definition-cyber-hygiene-benefits-best-practices-and-more. Accessed 15 Apr. 2024.

“Cybersecurity Hygiene 101 - Challenges & Checklist for Success.” *Snyk*, 2 Mar. 2023, snyk.io/learn/cybersecurity-hygiene/.

“Cybersecurity Framework.” *NIST*, 8 Mar. 2024, www.nist.gov/cyberframework.

Hashemi-Pour, Cameron, and Wesley Chai. “What Is the CIA Triad?: Definition from TechTarget.” *WhatIs*, TechTarget, 21 Dec. 2023, www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA#:~:text=The%20CIA%20triad%20refers%20to,(infosec)%20within%20an%20organization.

“How Many Cyber-Attacks Occur in the US?” *USAFacts*, USAFacts, 20 Nov. 2023, usafacts.org/articles/how-many-cyber-attacks-occur-in-the-us/.

Kerner, Sean Michael. “Colonial Pipeline Hack Explained: Everything You Need to Know.” *WhatIs*, TechTarget, 26 Apr. 2022, www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know.

Lindner, Jannik. “Online Banking Usage Statistics [Fresh Research] • Gitnux.” *GITNUX*, 16 Dec. 2023, gitnux.org/online-banking-usage-statistics/.

“The Latest Phishing Statistics (Updated April 2024): Aag It Support.” *AAG IT Services*, 8 Apr. 2024, aag-it.com/the-latest-phishing-statistics/#:~:text=Headline%20Phishing%20Statistics,sent%20in%202022%20were%20spam.

Published by Ani Petrosyan, and Apr 15. “Cybercrime: Monetary Damage United States 2023.” *Statista*, 15 Apr. 2024, www.statista.com/statistics/267132/total-damage-caused-by-by-cybercrime-in-the-us/.

Why Is HTTP Not Secure? | HTTP vs. HTTPS | Cloudflare, www.cloudflare.com/learning/ssl/why-is-http-not-secure/. Accessed 15 Apr. 2024.

“What Is a VPN? Why Should I Use a VPN?: Microsoft Azure.” *Why Should I Use a*

*VPN? | Microsoft Azure*, azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-vpn. Accessed 15 Apr. 2024.

"What Are the Main Differences between Proxy Servers & VPNS?: Upguard." *RSS*, www.upguard.com/blog/proxy-servers-vs-vpns. Accessed 15 Apr. 2024.

"What Is Cybercrime?" *Cisco*, 14 Dec. 2023, www.cisco.com/site/us/en/learn/topics/security/what-is-cybercrime.html.

"What Is Cybersecurity?: CISA." *Cybersecurity and Infrastructure Security Agency CISA*, 12 Apr. 2024, www.cisa.gov/news-events/news/what-cybersecurity.