Cybersecurity Risks in Remote Work and Learning Environments and Methods of Combating Them

Sanjana Mandadi[1], Sarada Prasad Gochhayat[#], Virgel Torremocha[#] and Jothsna Kethar[#]

[#]Advisor

ABSTRACT

In a post-pandemic world, more and more people are opting to work from home or use personal devices for work and learning. These trends correspond to a greater rate of cyber attacks, as remote work makes it harder for companies to protect their employees and their data. In this paper, the cybersecurity risks of remote work are outlined, followed by possible means of protection and preventing attack. Some of the former include unsecured networks and expanded attack surfaces, while the latter includes enhanced endpoint management and the use of the Zero Trust model. However, it was concluded that the most important way to minimize cyber attacks in an age of remote work is to educate the public on the best security practices and the ways in which they can spot threats.

Introduction

In recent years, public awareness of the modes and capabilities of cybersecurity threats has become more and more crucial for ensuring data protection and privacy. This is primarily due to world events that have led to a greater reliance on technology that is outside the scope of corporate protection. Even in a post-pandemic era, companies and K-12 school districts alike have chosen to more frequently permit practices that may unintentionally increase risks to their security. For the former, the option to continue working remotely is still widely available, and employers and employees alike are unsure of how to proceed in the face of changing values in the labor force. For the latter, a greater general reliance on technology has forced schools to either provide monitored devices or allow the use of personal devices which, even if only an issue for a small minority, poses serious threats to young, uneducated students.

The issue extends to a global scale when considering India's cybersecurity concerns with regards to remote working in a post-COVID world. In 2021, just one year into the pandemic, respondents from India reported a 40% increase in the number of cybersecurity attacks compared to the year before. Most commonly, attacks occur by malware, ransomware, phishing, and credential stuffing. What's more, nearly half of respondents reported that their infrastructure was not prepared to handle the risks posed by remote work [7]. Another survey reports that Indian educational institutions are one of the biggest targets of cyber attacks, as students and faculty are seriously advised to avoid clicking on suspicious links and emails and create strong passwords. Currently, India is ranked the sixth country with the worst cyber security [3].

On a national scale, another pressing concern is cyber or digital literacy and lack thereof. Results from surveys done by Kenneth Olmstead and Aaron Smith [17] suggest that Americans have a relatively good understanding of general cyber safety practices and can properly explain the more basic topics with ease. These include avoiding public Wi-Fi when possible, knowing how to choose a secure password, and understanding that turning off GPS does not prevent all location tracking. However, when it came to more technical topics, a greater percentage of people were found to be unsure. Such topics included the difference between HTTP and HTTPS, identifying multi-factor authentication, and, perhaps most relevant, the benefits of a VPN. These knowledge gaps only serve to hinder employee cyber security in remote working environments, as they must rely more heavily on their individual knowledge than the safety of their company.

Finally, on a more local scale, threats and concerns match those that exist at a larger perspective. One specific incident from November of 2023 in New Jersey involved the health care organization, Capital Health. Capital Health reportedly experienced network outages, system disruptions, and unavailable services, all of which endanger both the health and privacy of their patients. They now believe it to have been a cyber attack, and it is just one of many that happen every single day. In particular, healthcare facilities are at high risk of cyber attacks due to their size, which leaves them vulnerable, and their sensitive data [11]. All such attacks have increased in an especially drastic manner since the pandemic, and continue to do so in an upward trend as remote work remains as a dominant option.

This paper addresses in detail the enumerable threats to cyber security posed by remote work and learning environments. It also provides prevention methods that highlight the necessity of educating both employers, employees, *and* students about the full scope of their security measures. In doing so, the paper will potentially alleviate the risks that have pervaded nearly every industry in the age of remote work.

Types of Attacks

Listed below are the most common types of cyber attacks experienced by remote workers and students. Many of them are interconnected and overlap with each other, or they may be used simultaneously by hackers.

Malware

Malware, also known as malicious software, is very broad terminology that describes any software designed to intrude computer systems and steal data, damage infrastructure. Attacks can extend to computers, tablets, mobile devices, etc. Most often, cyber criminals install malware through corrupted files, unsecure downloads or installations from unknown providers, browsing of hacked sites, and legitimate sites with malicious ads. Signs of malware include slowed computer operations, an inundation of pop-ups and unwanted advertisements, system crashes, loss of access to files or the entire computer, and changes to browser settings. Under the blanket term of “malware”, the most frequent threats to remote workers include ransomware, spyware, and Trojan viruses [12].

Ransomware

Ransomware is a type of malware in which a cyber criminal will encrypt specific files on a device, blocking the original owner from accessing them. They will then demand a ransom for the files’ decryption and return. In recent years, it has become one of the most common forms of malware, as it is popular with hackers for its profitability. Most companies and organizations threatened by ransomware have no choice but to pay the ransom in order to ensure the safe return of their files. The popularity of ransomware particularly began to rise after the WannaCry attack in 2017, which targeted Microsoft Windows users globally, demanding a Bitcoin ransom. Since 2020, remote work has only increased the vulnerabilities that allow for installations of ransomware. In the age of remote work alone, 71% of companies have experienced ransomware attacks [21].

<u>Double Extortion</u>: A type of ransomware in which not only are files encrypted, but data is stolen with the threat of leaking if the ransom is not paid.

<u>Triple Extortion</u>: This type of ransomware extends the double extortion technique with a third threat to their victims. Oftentimes, this may be a distributed denial-of-service attack.

Locker Ransomware: The victim is locked out of their entire computer until the ransom is paid rather than just specific files.

Crypto Ransomware: A ransomware attack in which the criminal specifically demands cryptocurrency as ransom (similar to the WannaCry attack).

Spyware

Spyware is another type of attack listed under malware in which information about the victim is collected and distributed to third parties with malicious intent and implications. The information may include personal data, a user's web activities and location, logins and passwords, banking information, etc., all of which is a serious violation of privacy. There is a gray area within spyware, however, as many large corporations share their users' information and track their online activities for advertisement and data collection purposes with little legal consequence [9].

Trojan Horse Attack

A Trojan horse virus is a type of malware disguised as legitimate software. This can be in the form of seemingly innocuous emails, links, files, attachments, and more. Trojans are used in many of the other listed attacks, with a broad range of purposes from stealing and modifying data to damaging computer systems. The name itself comes from the ancient Greek epic, *The Odyssey*, by Homer, and it is a symbol of disguise and deceit. Oftentimes, Trojan attacks are executed through social engineering, which involves exploiting human emotions and psychology in order to gain leverage and expose vulnerabilities. This is especially an issue in remote work, as victims may be outside the scope of protection of large companies that are less subject to social engineering [4].

Phishing

Phishing is a very common cyber crime in which the victims are contacted either via email or text message by a seemingly legitimate source (see: Trojan Horse Attack). Such messages will lure victims into sharing sensitive information including passwords and banking and credit card details. In 2023, an estimated 3.4 billion phishing emails were sent every day [20], and in 2022, about 83% of businesses in the UK reported that phishing was their most frequently encountered cyber attack [6]. Phishing is especially dangerous when directed towards educational institutions because younger students are less likely to differentiate between legitimate and illegitimate email addresses.

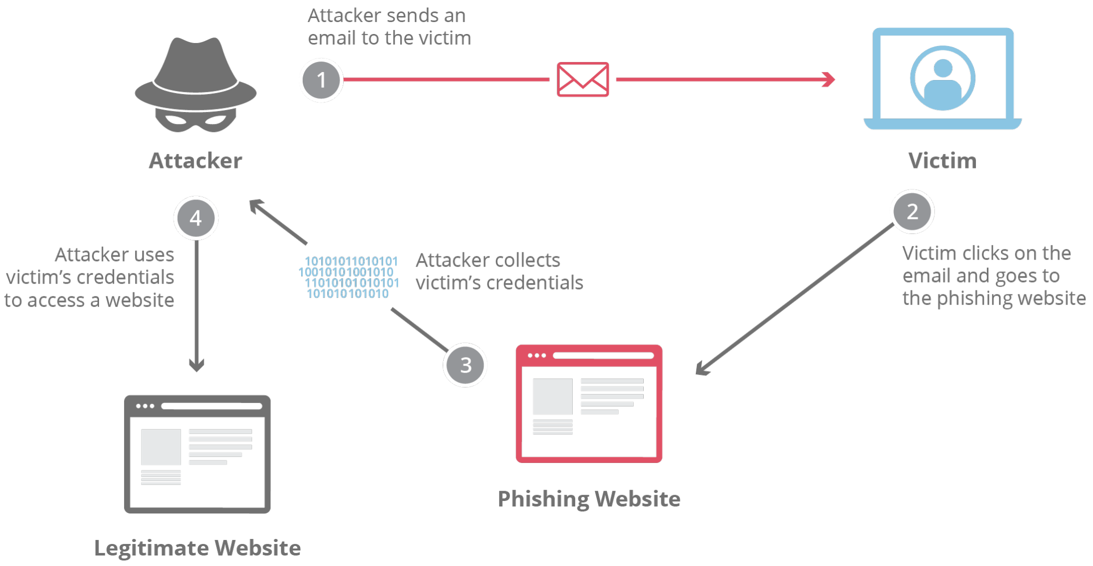
Attacker sends an email to the victim
1
Attacker
Victim
4
2
Attacker uses victim's credentials to access a website
Attacker collects victim's credentials
Victim clicks on the email and goes to the phishing website
3
Phishing Website
Legitimate Website

Figure 1. The full process of phishing [5].

Camfecting

Camfecting is the process of hacking into someone's webcam and activating it. Typically, this happens through Remote Access Trojans (RATs), which allow criminals to control their victim's entire device remotely. RATs work the same way as other Trojan attacks and are deployed in the same way as well. Another method of camfecting is by exploiting the vulnerabilities in software created by human error. Hackers will slip through these cracks, which are far more commonplace on personal networks used for remote work, and seize control of cameras. Camfecting does not only impact webcams. The risks extend to home security cameras as well, oftentimes through password stealing. One indication of camfecting is when the victim's camera light comes on even when they haven't activated their camera [18].

(Distributed) Denial-of-Service

Denial-of-service is a type of attack in which a user's network or other online services are forcibly shut down. This is typically done by flooding the network with requests and other traffic, causing it to exceed its maximum capacity and be rendered unusable. Such attacks tend to be difficult to track, as they may occur slowly and subtly. A distributed denial-of-service attack specifically is done across multiple computers or devices, which all contribute to flooding a network. These types of attacks are even harder to track because they come from multiple sources. They degrade bandwidth, use up resources, steal information, etc. Denial-of-service attacks are especially detrimental for corporations with websites that are user/customer based, as those organizations will experience a loss of trust in their software [10].

Zero-Day

A zero-day attack is simply a term for any cyber attack that occurs due to a hole in the system's security that is unknown to its developers. The idea is that they have "zero days" to recover from the attack and protect their systems, as it is already in motion. Such holes in security are known to appear more frequently in companies that have remote workers, partially because of decreased collaboration between those in charge of developing a system, which leads to less overall thoroughness. Zero-day attacks can be paired with any of the other listed attacks, as the nature of this classification is more broad and does not define the specific actions of the attacker [2].

Code Injection

Code injection, like the name suggests, is when malicious code is placed, or injected, in a website or application. The malicious code runs like all of the other code in the application, allowing for its easy exploitation. Viruses and worms can be loaded onto computers using this method, which can lead to data theft and a full loss of system control. One specific type of code injection is SQL injections, which target information within databases. This is one of the most common types of cyber attacks [19].

Supply Chain

A supply chain attack is one in which cyber criminals go after the third parties that provide support for the target network's application functionality. The target has what is known as a dependency with these third parties, often unknowingly, as they rely on specific programs in order for their own to be maintained. In order to carry out a supply chain attack, criminals start by infiltrating these third party systems, which is called an upstream attack. Once the attacker has control of the third party, they begin what is known as the downstream attack. This is when they actually go after their true intended target, typically by altering the third party's code or injecting viruses and other malware [16].

Man-in-the-Middle

A man-in-the-middle attack is one in which a hacker inserts themself in the "conversation" between a user and an application. This attack is used to gain sensitive information either about the user or the application itself. There are a number of different reasons why this is done, ranging from selling data to identity theft. The general process of man-in-the-middle attacks begins when the hacker has infiltrated a target user's network. After that, they must decrypt any information without either party noticing. This is done with a variety of methods, including SSL stripping, where HTTPS connection is downgraded to HTTP, and SSL hijacking, where forged authentication keys are used by both parties without either knowing [15].

Watering Hole

A watering hole attack is when a target's most frequently visited websites or applications are tracked, and then those sites are infected by the attacker. The next time the target uses any of those sites, they too will be infected by the malware. Watering hole attacks, although comparatively rare, are highly sophisticated and are often successful. The attacker must do a lot of research and profiling of targets, looking for the people who are easiest to exploit and know the least about how to protect themselves. Remote workers, who lose some of the protection offered by their companies when working in person, are more likely to be prime targets for these types of attacks [13].

Risks

There are many risks associated with remote work. Listed below are the most important ones, as they are both common and dangerous.

Unsecured/Unprotected Networks

While companies typically have secure WiFi networks within their designated buildings, this access does not extend past such areas. Remote workers are therefore required to use their own WiFi if they must access the Internet, and it may not have the same levels of protection. Remote workers may also use free WiFi, which is even more dangerous, as it is often unencrypted or weakly encrypted, leaving personal and company data potentially exposed to hackers with malicious intent. The same goes for school children, who, when using free WiFi, are vulnerable to any number of cyber attacks. In fact, students may be more willing and likely to use free WiFi if they do not have a data plan or if it is simply more convenient. With regards to securing WiFi networks, there are four general security protocols, all with different degrees of protection.

WEP

Wired Equivalent Privacy, or WEP, began being used in the late 1990s, and was the first security protocol. It uses basic static keys and symmetric key encryption, meaning that under any given network, the same key is used to send and receive encrypted messages. This is almost never a safe practice, as it means that anyone using the WiFi network can use the static key to decrypt messages or traffic meant for another device using the same network. In order for this to be safe, an unrealistic amount of trust is required in both the competence and integrity of all of the network's users. Furthermore, modern computers typically have the computing power to find the encryption relatively quick and easy. It is therefore not recommended that WEP be used to secure WiFi networks.

WPA

WiFi-Protected Access, or WPA, was introduced in the early 2000s and starts to fix the encryption issue found in WEP. Rather than a static key, WPA uses the Temporal Key Integrity Protocol (TKIP), which creates a new encryption key every time an exchange is made on a network. This makes it more difficult for intruders to infiltrate a network. However, criminals have since been able to attack WPA, which has led to newer generations of the protocol.

WPA2

WPA2 improves upon WPA and is largely considered to be the standard for the security protocols. It uses the Advanced Encryption Standard (AES), which is a more secure encryption standard overall. It also verifies encrypted packages to ensure that they are safe. WPA2 has two modes: personal and enterprise. With the personal mode, all devices use a single password to access a WiFi network. This is generally preferred for household use. With the enterprise mode, each device gets its own separate password to use the WiFi network. This is generally recommended for businesses.

WPA3

WPA3, released in 2018, is the most secure protocol. It has even stronger data encryption than WPA2 and also uses longer keys, making them extremely difficult to crack. For WPA3, AES is implemented using the Simultaneous Authentication of Equals (SAE) protocol, which has greater protection against password-guessing, brute-force attacks, and other decryption algorithms. Although WPA is the best of the four security protocols, it is not as commonly used as WPA2 simply because the former is not yet compatible with most devices.

Any device using a WiFi network that is unsecured or uses WEP or WPA is at risk of being hacked into. This is a serious issue with remote working and learning, as most people are not familiar with different WiFi security protocols and may not realize that they are vulnerable to attack [8].

Expanded Attack Surfaces and Insecure Endpoints

The attack surfaces are all of the points at which hackers can gain unauthorized access to a company's systems. It is inevitable that people use a wider range of devices when working remotely, creating new endpoints for the company to handle. This can be through personal computers or even cell phones that are used to access company information and networks, which give hackers a larger number of entry points to attack their targets. These extra devices also may not be as well protected, leading to the same issues with unprotected networks. An expanded attack surface can also be more difficult and costly to maintain in general, and with more and more personal devices being used in place of company-issued devices, security becomes ignored for the sake of functionality [22].

Insufficient System and Security Updates

Unless strictly enforced by employers, workers in general may neglect to update their software due to it being inconvenient or simply because they forget to do so. From the comfort and safety of one's home it is easy to forget that cyber security is important, causing remote workers to more frequently ignore system and security updates. There is also often less oversight of remote workers by IT departments that are in charge of such updates. However, cyber criminals will seek out outdated systems to target because they are easier to exploit. By failing to keep their security up to date, remote workers invite the risk of more attacks both upon themselves and their companies.

Prevention

The methods of protecting corporations from cyber attacks have evolved greatly over the last few decades. As cyber criminals continue to work around these barriers, new protection must continually be created. Listed below are some effective prevention methods, some older and some more modern.

Enhancement of General Security Practices

It is important for organizations to emphasize the necessity of good cyber security practices for their employees, as a few simple actions can greatly reduce the risk of attack. Listed below are some of the easiest and most helpful practices.

Creating Strong Passwords

Having strong passwords is an important step in safeguarding accounts and network access. The stronger the password, the less likely a criminal is to guess it. There are three components to a strong password. The first is that it should be long, at least 8-16 characters. Longer passwords have greater variability which makes them more difficult for others to access. Along with that, the second component is that passwords should be random. It is best if they do not contain the user's name or anything commonly affiliated with them. It is also best to use numbers, letters, and special characters. The final component of a strong password is that it should only be used to protect a single account. Having unique passwords for different purposes ensures that even if one password is stolen by an attacker, they will not have access to all of the victim's accounts and information [21].

Using a VPN

As long as it is not prohibited by employers, workers should use a VPN, or a virtual private network, in order to enhance their privacy and protection. VPNs allow users to encrypt data like emails and payment information, which is an added layer of protection on top of the company's security protocols. They also allow remote workers to easily access company resources that they are authorized to from anywhere, without compromising the company's security. The only caveat is that VPNs typically mask a user's IP address, which can hinder other security measures like threat prevention. Many companies will choose to ban personal VPNs for this reason and opt to rely on their own security measures instead [23].

Using an Up-to-Date Router

As mentioned previously, a serious issue for remote workers is using unsecured WiFi networks. In order to negate this, it is important to be aware of how well-protected any network is and be mindful of accessing a company's data and resources when the security protocol is not appropriate. It is also important to keep personal routers up to date. Generally, they should be replaced once every five years in order to ensure the standard of the security. This can go a long way in filling in any gaps in security that are unreachable by the employer's security measures.

Endpoint Management

Endpoint security is exactly what it sounds like – it is the process of protecting all endpoint devices in a company, regardless of whether they are connected to the network or have any physical proximity to company premises. The most current approach to endpoint security is management that happens completely through the cloud, which allows administrators to protect remote endpoints. This allows companies to maximize their security in a way that goes beyond conventional security measures like antivirus solutions that cannot reach remote endpoints.

An antivirus can be downloaded on computers typically in order to prevent, detect, and eradicate viruses or other malware. However, it does this by keeping a database of known malware signatures, and when a potential threat arises, it must check that database in order to recognize that it is malware. A novel virus, which would not be in the system, can therefore bypass a traditional antivirus undetected and cause serious issues. Advanced endpoint security, on the other hand, uses what is known as next-generation antivirus (NGAV). Instead of only checking malware signatures, NGAV uses artificial intelligence and behavioral modeling to predict and identify malware. It examines other aspects to detect viruses, including IP addresses and URLs. Moreover, antivirus solutions must be installed individually on every device, while endpoint security extends to any device under a specific network.

Another useful element of endpoint management is that it provides a continuous, real time view of what is happening with all endpoints from a security standpoint. This helps speed up the pace of detection and incident investigation, should an attack occur. It makes patching up security holes much simpler as well. It also allows administrators to process security updates for all devices using a network instead of having workers manually install their updates, reducing the risk of error.

Enhancing endpoint security is more cost-effective than other methods, as it prevents major and detrimental loss and saves money in the long run [24].

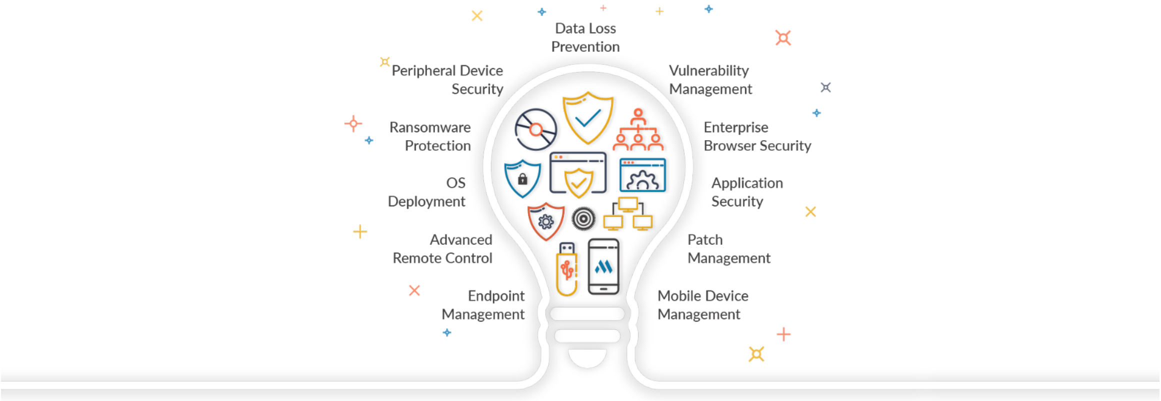

Figure 2. The main components of endpoint management and security [14].

Zero Trust Access

The idea behind Zero Trust is that no one – no matter the person, no matter the device, regardless of whether they belong to the network – can be trusted without identity verification. Zero Trust applies to workers that are both within and outside the scope of the company's network. Therefore, it applies equally to remote and in-person employees. The assumption that attackers can exist both inside and outside of the network is incredibly important because even if a user is verified once, their device cannot be 100% trusted permanently. It is common for attackers to move within a network after gaining access to it. This is called lateral movement, and it can be hard to detect without Zero Trust access.

Within the Zero Trust model is the idea of least-privilege access. This means that users and their devices are only given access to what they need rather than the entire network of data. By doing so, more sensitive information can be better protected, as the pool of access to it is narrowed.

The key characteristic of Zero Trust access is the use of multi-factor authentication. This is when more than one piece of evidence is required in order to verify a user's identity. What this comes down to is that the use of a single password is not enough to prove one's identity. This can make it dramatically more challenging for unauthorized devices to access sensitive data, as password stealing is not sufficient [1].

Educating Employees and Students

By far the most important and fundamental prevention method is educating employees and students. Those who are aware of the different kinds of cybersecurity risks as well as different types of attacks are more well equipped to recognize red flags. They are also better prepared to handle attacks if and when they come. Those that are educated can properly incorporate good safety practices into their own work, and they can ensure that their company or school is also taking the right steps to protect them. Those who understand threats to cybersecurity will be more careful with the information that they share, as the consequences can be dire. Organizations that take the steps to educate their users make the long-term investment of enhancing the protection of their networks as a whole.

Discussion and Conclusion

When working remotely, people have a far more limited interaction with their coworkers. Perhaps the only chance to communicate in real time is during phone and video calls, which are typically reserved for more formal meetings. In other words, those who work remotely may not get the chance to socialize with peers in their field often. Because of this, there are two important cognitive impacts of remote work that are relevant to cyber security. The first is that security is just not taken seriously by the average person, even more so when they are working at home. Why would anyone bother making dozens of unique, random passwords that they will never remember? From a student perspective, why pay more for an expensive WiFi when it is free at coffee shops? Yes, it provides better protection, but that is simply not at the forefront of people's minds when they work remotely. The second impact of remote work is that people learn less from their peers when they see them infrequently. This is especially important for something like cybersecurity, which is an ever-changing field. Remote workers have fewer opportunities to learn about the latest antivirus technology from their peers. They don't get a chance to mimic their coworkers' safe security practices in an environment where rules about security are likely stricter.

These issues are most prevalent in remote work, and moving back to full, in-person work would be ideal with regards to cyber security. However, the reality is that our post-pandemic society will likely continue to heavily rely on remote working for many years to come. The challenge is to continue to develop new methods of protection and strengthen the barriers already in place.

This paper discussed various cyber attacks most commonly seen by or seen because of remote workers. It addressed the risks that remote work poses as well as potential methods of prevention. In doing so, it emphasizes a need for employers, employees, and students to be educated on how to handle their own cyber security. After all, nothing can stop a cyber criminal when the doors to a network are left wide open, unprotected and unsecured.

Acknowledgments

I would like to thank my family and friends for their continued support throughout this journey. I would also like to thank my mentors from Gifted Gabber, Dr. Sarada Prasad, Professor Virgel Torremocha, and Coach Josthna Kethar, for their help in this process.

References

1. Assunção, P. (2019). A zero trust approach to network security. In *Proceedings of the Digital Privacy and Security Conference* (Vol. 2019). Porto Portugal.
2. Bilge, L., & Dumitras, T. (2013). Investigating zero-day attacks. *Login*, *38*(4), 6-13.
3. Bischoff, P. (2024, January 10). *Which countries have the worst (and best) cybersecurity?* Comparitech. https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country/
4. Bridges, L. (2008). The changing face of malware. *Network Security*, *2008*(1), 17-20. https://doi.org/10.1016/s1353-4858(08)70010-2
5. *The full process of phishing* [Photograph]. (n.d.). Cloudflare. https://www.cloudflare.com/learning/access-management/phishing-attack/
6. Griffiths, C. (2024, February). *The latest 2024 phishing statistics*. AAG. https://aag-it.com/the-latest-phishing-statistics/
7. *Indian businesses continue having cybersecurity concerns with remote working, one year into pandemic, finds thales*. (2021, August 18). Thales. https://www.thalesgroup.com/en/india/press_release/indian-businesses-continue-having-cybersecurity-concerns-remote-working-one

8. Indira Reddy, B., & Srikanth, V. (2019). Review on wireless security protocols (WEP, wpa, wpa2 & WPA3). *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 28-35. https://doi.org/10.32628/cseit1953127
9. Jonasson, D., & Sigholm, J. (2005). What is Spyware?. *TDDC03 Projects, Department of Computer and Information Science, Linkopings University, Sewden*. Chicago
10. Kaur, P., Kumar, M., & Bhandari, A. (2017). A review of detection approaches for distributed denial of service attacks. *Systems Science & Control Engineering*, *5*(1), 301-320. https://doi.org/10.1080/21642583.2017.1331768
11. Kekatos, M. (2023, November 30). *New Jersey health system says outages are likely result of cyber attack*. ABC News. https://abcnews.go.com/Health/new-jersey-health-system-outages-result-cyber-attack/story?id=105270813
12. Kramer, S., & Bradfield, J. C. (2009). A general definition of malware. *Journal in Computer Virology*, *6*(2), 105-114. https://doi.org/10.1007/s11416-009-0137-1
13. Krithika, N. (2017). A study on wha (watering hole attack)–the most dangerous threat to the organisation. *Int. J. Innov. Sci. Eng. Res.(IJISER)*, *4*, 196-198.
14. *The main components of endpoint management and security* [Photograph]. (n.d.). ManageEngine. https://www.manageengine.com/products/desktop-central/endpoint-management-solutions.html
15. Mallik, A. (2019). Man-in-the-middle-attack: Understanding in simple words. *Cyberspace: Jurnal Pendidikan Teknologi Informasi*, *2*(2), 109-134. Chicago
16. Martínez, J., & Durán, J. M. (2021). Software supply chain attacks, a threat to global cybersecurity: SolarWinds' case study. *International Journal of Safety and Security Engineering*, *11*(5), 537-545. https://doi.org/10.18280/ijsse.110505
17. Olmstead, K., & Smith, A. (2017, March 22). *What the public knows about cybersecurity*. Pew Research Center. https://www.pewresearch.org/internet/2017/03/22/what-the-public-knows-about-cybersecurity/
18. Poojary, P. S. (2021). Techniques to avoid webcam hacking. *International Research Journal of Modernization in Engineering Technology and Science*, *3*(1).
19. Ray, D., & Ligatti, J. (2012). Defining code-injection attacks. *ACM SIGPLAN Notices*, *47*(1), 179-190. https://doi.org/10.1145/2103621.2103678
20. Recognizing and reporting phishing. (n.d.). *Information Technologies | Secure UD Threat Alerts*. https://sites.udel.edu/threat/2023/10/02/recognizing-and-reporting-phishing/
21. Require strong passwords. (n.d.). Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/secure-our-world/require-strong-passwords
22. Richardson, R., & North, M. M. (2017). Ransomware: Evolution, mitigation and prevention. *International Management Review*, *13*(1), 10.
23. What is a VPN? (n.d.). Microsoft Azure. https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-vpn
24. Zeng, S., Adam, C., Wu, F., Guo, S., Ruan, Y., Venugopal, C., & Puri, R. (2014). Managing risk in multi-node automation of endpoint management. *IEEE Symposium on Network Operations and Management*. https://doi.org/10.1109/noms.2014.6838295