Integration of Social Engineering to Propagate the Spread of Malware Throughout Networks

Maxwell Derella, Samuel Sharivker, Rafael Aldana-Diaz

Abstract

In recent years, a significant number of viruses have spread due to social engineering as opposed to being very sophisticated on a technical level. Malware can spread across networks by infiltrating different layers of the OSI network model to find new targets. A common question throughout our research is, "Why do so many viruses get transmitted through phishing attacks?". It is critical to address this question and the topic at hand because increasing education on internet safety can prevent billions of dollars in damage. Throughout our research, we also conducted an anonymous survey among middle school students at NYU regarding social engineering and malware. Although our initial hypothesis was that most participants would be unable to detect the phishing email, 74.4% of participants successfully detected the phishing email. Our survey has also found that an increasing number of younger people are gaining some cyber security knowledge. However, our independent research has found that very few high school students receive any cybersecurity education, which is alarming due to the damage that has been done in recent years, as mentioned earlier. Despite the successful performance of our survey participants, we have found that there is still a significant knowledge gap in cybersecurity.

1 Introduction

No matter how secure one's network is, there is always one common weakness. The password? The firewall? The answer is, surprisingly, nothing technological but us. No matter how many security protocols one company or network uses, people are the most vulnerable because they are susceptible to manipulation through social engineering. Social engineering targets individuals or groups of people and gets them to reveal sensitive information or steal data. Social engineering is a critical concept to understand because although it may seem that it takes significant vulnerabilities for unethical hackers to break into a network, all it takes is one compromised individual to cause billions of dollars in damage, as seen in the "ILOVEYOU" Virus mentioned later in our case study. A virus is a type of malware, which is malicious code that attempts to damage or steal data from a computer. Viruses come in several different forms and are able to spread on their own over networks. Networks are when two or more computers are connected and able to communicate with each other. Networks transfer data through different protocols and layers which also allows malware to infect different layers of the network.

In addition to our research, we also conducted an anonymous survey at NYU among middle school students. The survey had topics in the field of social engineering to evaluate the knowledge students have. We conducted this survey because, throughout our research, we saw how a lack of awareness of how malware spreads led to the most significant damage. Our survey aimed to identify if our fellow students were part of the gap or to see how their education affected their judgments despite being at a young age. Although our initial hypothesis that a majority of the survey participants would choose the incorrect option was wrong, when further researching the demographics of our survey, our results became more explicit.

Our study is significant because although we surveyed middle school students, it is essential to acknowledge that these children are future members of the working class and society. In addition, an increasing number of children are getting access to technology at younger ages, so it is critical to assess their knowledge of internet safety now so that they have more time to gain knowledge and experience.

2 Case Study

One of the most notorious viruses was the "ILOVEYOU" virus of 2000. What initially seemed like just a normal email attachment caused over 15 billion dollars worth of dam-

age [2]. The virus originated in the Philippines from two college students and spread through phishing emails. When someone would click the link their system would get infected which resulted in significant performance degradation. The virus would then spread to the victim's contacts and email itself to continue the spread. Although the actual virus wasn't very complex on a technical level, its ability to spread on its own is what made it the most dangerous. This was a perfect example of how "curiosity killed the cat" and how a lack of knowledge leads to catastrophic damage.

Another example of a virus that wreaked widespread havoc was the "WannaCry" ransomware. The origins of this virus trace back to a hacking group believed to be working under the North Korean government, called Lazarus Group. The attack exploited a vulnerability in Microsoft's Windows operating system, which was simply called EternalBlue.

EternalBlue is an exploit written by the U.S. National Security Agency. It exploits a vulnerability in the Server Message Block protocol, which Windows computers use to communicate with each other over a network [10]. Early in 2017, a group of hackers named the Shadow Brokers leaked a set of NSA hacking tools, including EternalBlue, to the public. It gave hackers a powerhouse tool to exploit unpatched Windows systems worldwide.

WannaCry took advantage of this vulnerability, specifically being designed to exploit SMB vulnerability using EternalBlue. Once it had infiltrated a vulnerable system, it downloaded ransomware to encrypt the user's files, subsequently demanding that a ransom be paid in Bitcoin for their decryption. However, what made WannaCry so dangerous was it's ability to spread like a worm (similar to ILOVEYOU). Following the infection of one computer, it was able to search the local network and the internet for other systems with this same vulnerability, propagating infection rapidly and without requiring further user interaction.

In addition to the infamous "ILOVEYOU" virus and the "WannaCry" ransomware, another notable malware that caused widespread damage is the Zeus Trojan. Zeus (also know as Zbot) first emerged in 2007 quickly becoming one of the most well-known banking Trojans in history [4]. Unlike the other two mentioned above, this wasn't a malware designed to replicate itself and spread to as many computers as possible, nor was it meant to create visible damage to the infected systems. On the contrary, it worked silently, with specific orientation toward financial information.

How exactly Zeus propagated itself and spread to so many computers was through the use of social engineering, such as the usage of phishing emails, much like the propa-

gation methods employed by ILOVEYOU, or as part of drive-by downloads from compromised websites. Downloaded on a user's computer, Zeus would run in the background and log the user's activities online while it captured login credentials, mostly those used for online banking. The information would then be sent back to command-and-control servers operated by the attackers, who would use this information to drain bank accounts [4].

What made Zeus particularly dangerous was it' s customizability, allowing it' s capabilities to expand beyond stealing financial data. For example, Zeus could be configured to create a botnet using the infected computers that can be remotely controlled to complete various tasks such as deploying DDoS attacks.

Although one of Zeus' s largest and most dangerous variant (Gameover Zeus) would eventually be taken down by international law enforcement agencies (such as the FBI) during 2014 [4], as a result of the official source code being leaked in 2011 numerous variants and copycats continue to exist and spread chaos in the digital cyberspace, illustrating how the impact of such malware can persist long after its initial defeat.

3 Experiment and Result

Our survey consisted of questions, with the one we were most interested in being question 6. Question 6 consisted of 2 images, with the objective being the students correctly guessing which email was phishing. We hypothesized that most students would guess wrong due to their young ages. 92.3% of our survey takers fell between the ages of 10 to 13 years old. However, to our great surprise, 74.4% of the survey participants correctly guessed that option 2 was the phishing email. Even more shocking because when asking the students to rate their confidence in detecting a phishing email on a scale of 1 to 10, where 1 is "No clue" and 10 is "Very confident," 25.6% of students chose 1. Although 12.8% of students did choose between 9 and 10, the 25.6% that had no clue is still the most significant percentage. One might look at these statistics and automatically assume that the students must have guessed. However, the students' responses to the other questions indicate that they most likely got the correct answer because of the education they received.

One question that immediately supported the result of the phishing email success rate was question 3, which asked students if they knew what a phishing email was. 71.8% of students have heard of a phishing email, and 61.5% said they understood the concept

enough to explain it to someone else. This figure is significant because, in many cases in the real world, one truly understands something if they can explain it to someone else and teach them. While further diving into the survey results, 28.2% of students answered that they did not know what a phishing email was, and coincidentally, or not coincidentally, 25.6% of students got the phishing email question wrong. This statistic indicates a significant correlation between students' understanding of phishing emails and their ability to detect them.

Although some might question how these survey participants performed so well in the first place, it is critical to understand that children are getting access to technology at a younger age. According to studies such as the one conducted by "Common Sense Media," almost 80% of children in the United States have access to a tablet, which can give them access to the internet [9]. There are some negative drawbacks to children getting access to technology at a younger age, such as negatively impacting social and behavioral skills as well as lowering attention span [15]. However, at the same time, we have seen from the results of the survey that this can also build children's education and technical skills in cybersecurity which can help keep them safer and avoid scams.

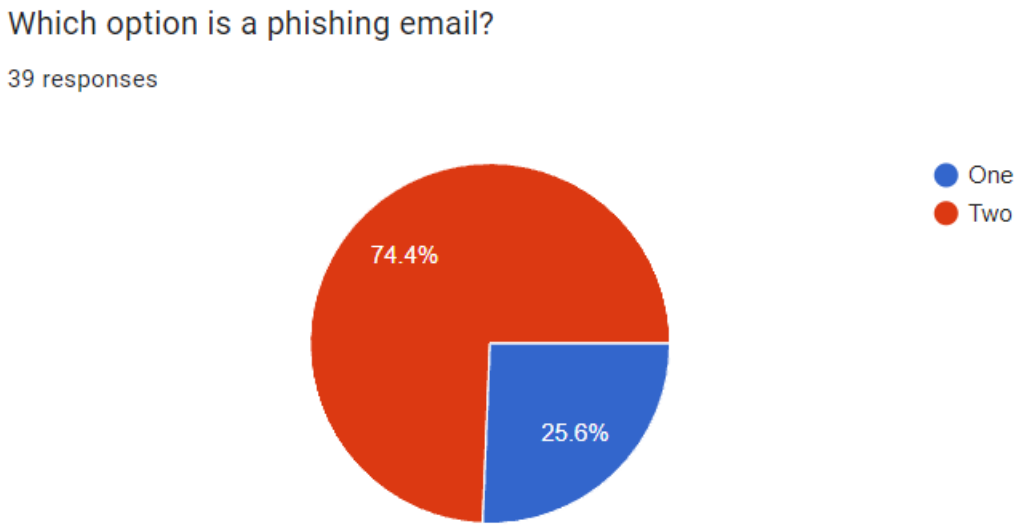

Figure 1: A pie chart that displays the results of survey showing that 25.6% picked the wrong image and 74.4% picked the right image for the phishing email

On the other hand, there is still a way to go on educating children on cybersecurity. Although only 7.7% of survey participants would plug in an unknown USB drive, only 12.8% understand social engineering well enough to explain it to someone else. Concerning because although only 20.5% have been peer pressured to give someone infor-

mation or access, this statistic is due to their limited experience. Phishing emails are just one of the many techniques that unethical hackers use. Some researchers have found that over 85% of high schools do not educate students on cybersecurity concepts [1]. Imagine the lack of knowledge that younger students are experiencing. With the right virus, it only takes a couple of individuals to cause billions of dollars in damages, leading to malware.

4 What is Malware?

What is malware? Malware generally refers to malicious software. It could be any program or file whose purpose or intention may be to cause damage, disrupt, or destroy any computer, network, or user. Malware also comes in a variety of different forms, such as worms, trojans, ransomware, adware, and spyware. Each of these forms of malware transmits through various means and releases different types of payloads, however, the core concept that connects the method in which they are spread is through social engineering. Social engineering plays the crucial role of manipulating humans into interacting with seemingly safe and legitimate entities, such as emails, websites, or phone calls, which are actually deceptive in nature and designed to compromise security by tricking individuals into divulging sensitive information or performing actions that aid the attacker.

4.1 How Does Malware Work?

Malware operates in a series of steps that results in the final outcome, beginning with initial infection of the device. This is typically occurs because of delivery through phishing emails, drive-by downloads from compromised websites, exploitation of software vulnerabilities, or by means of infected removable media like USB drives [11]. Once malware has reached the system, execution is the next step. Either it will be done automatically by the result of an exploit, or because of user action, for example, opening a malicious file.

Right after execution, it starts looking for a way to ensure persistence. Basically, this means being able to remain operative even if the system is rebooted. For this, it could be through the addition of itself to startup programs, changing system settings like adding entries to the Windows registry, or creating scheduled tasks [14]. After providing the means for persistence, the malware exposes its payload. This may involve data theft, file

encryption for ransom, turning the infected machine into a botnet to be used for building a remote-controlled device, or simply leading to direct file destruction and system integrity.

Also, many types of malware are designed to propagate, that is, copy themselves to other systems. This may be achieved via network port scanning in search of vulnerable devices; emailing or messaging copies via social media; or infecting shared files. Many types of malicious code use obfuscation and evasion techniques to try to avoid detection and removal [11]. It can include code obfuscation, where malware disguises its real nature; polymorphism—that is, self-modifying code at each infection to avoid signature-based detection—or even rootkits used to conceal its presence inside the system.

Some malware communicates with a C2 server, which allows attackers to send various commands, update malware, or exfiltrate data that has been previously stolen by the malware. Secondarily, it can spread laterally across a network, infecting other machines, or download other types of malware. It can finally erase logs, remove traces of its activity, or even uninstall itself in a bid to cover up and attempt to prolong the presence[11]. However, if the malware has built persistence mechanisms, it could get back into the system even following its seeming removal. This whole process has demonstrated the sophistication and danger of today's malware, which is capable of getting in, propagating, and inflicting damage while eluding detection and removal.

Malware as mentioned in this beginning comes in a variety of different forms, each with their own unique methods of infection, execution, and impact. These forms include:

4.1.1 Viruses

Actually, viruses are a subset of malware. A virus is a piece of malicious software that spreads from host to host by executing its code when it is attached to a document or file, usually one that allows macros. When a virus is downloaded, it won't wake up until the file is opened and used. The goal of viruses is to interfere with a system's ability to function. Viruses can therefore result in significant operational issues and data loss[3].

4.1.2 Worms

A worm is a kind of malware that spreads throughout all of the devices linked to a network by rapidly replicating itself. It differs from a virus in that it operates independently of any host program. Essentially, a worm gains access to a device by downloading a

file or link via a network, at which point it begins to multiply and spread exponentially. Worms, like viruses, can result in data loss and slow down the device's operation[3].

4.1.3 Trojans

Trojan horses lurk in software applications that seem helpful. However, as soon as a user downloads it, a Trojan virus gains access to the private information and is able to alter, remove, or block it. The device's performance may suffer greatly as a result. Trojan viruses are not made to replicate themselves, in contrast to other types of viruses and worms[3].

4.1.4 Spyware

Malicious software that operates covertly on a computer and reports back to a remote user is referred to as spyware. Spyware is a kind of malware that primarily targets sensitive data and provides remote access to predators, as opposed to interfering with device operations. The primary purpose of spyware is to steal personal or financial data. A term used to describe one kind of spyware is keylogger. This implies that it logs every keystroke you make, disclosing passwords and other private data[3].

4.1.5 Adware

Adware is a kind of malware that tracks your computer usage habits and displays relevant adverts in your browser. While most adware is not dangerous, certain types of adware may cause issues for your system. In addition to possibly containing Trojan horses and spyware, it has the ability to reroute your browser to dangerous websites. Additionally, a large amount of adware dramatically reduces system speed. Since not all adware is harmful, protection that can detect this kind of software intelligently and continuously is necessary[3].

4.1.6 Ransomware

Malware known as "ransomware" takes control of a system, encrypts any sensitive data it finds, and then demands a ransom to unlock the data. The majority of ransomware arrives as an attachment from a spearphishing attempt. The ransomware is downloaded after the user clicks a bogus link. After that, some information is encrypted so that only a mathematical key that they know can decrypt it. The data is unlocked after the attacker receives payment[3].

5 How Does Malware Infiltrate the OSI Model?

Malware, which comes in worms, Trojans, ransomware, adware, and spyware, poses one of the major threats to computer systems and networks. Each type of malware represents a malicious program capable of exploiting any vulnerability up and down the OSI Model to do all sorts of damage, disrupt operations, or steal sensitive information. This means that through social engineering, malware convinces users to interact with what seems to be a legitimate entity and then allows it to make very adverse security breaches. From the Physical Layer up to the Application Layer, each layer of the OSI Model demonstrates the possibility of its exploitation by malware, rendering great importance to strict security measures in every phase of network communication.

The OSI Model forms how one's computer communicates with other computers. It forms a universal language between different computer systems. Had it not been for the OSI model, all these different devices would not have been able to communicate with each other. There are seven layers, all of which make up the communication system. Each of these layers also has its protocols, a checklist that must be completed to finalize specific tasks. These seven layers are as follows: Physical, Data Link, Network, Transport, Session, Presentation, and Application. We will describe the use of each layer and its protocol before explaining the vulnerabilities that can be exploited to inject malware into each [6].

5.1 Physical Layer

The Physical Layer of the OSI Model is concerned with physically connecting devices using mediums like Ethernet cables. It is in charge of transmitting raw bits and handling bit-rate control, which is fundamental to running a network. Modems, cables, and hubs are some of the devices at this layer. Due to its physical nature, this layer has some weaknesses against specific attacks. This is accomplished through physical tampering, where a device on the network could be accessed, or cable splicing is done, disrupting operations or data compromise. Attackers may also use passive Ethernet taps to eavesdrop on network traffic without changing it. Other environmental threats like fire or water damage might impair the network's physical components. Every organization should be able to ensure that risks from vulnerabilities get mitigated through robust physical security, good cable management practices, regular inspections, and protection of hardware from tampering. However, mitigating these vulnerabilities is critical to network integrity and avoids expensive disruptions or security breaches.

5.2 Data Link Layer

The Data Link Layer is responsible for framing data packets; it controls access to the physical transmission medium, which is done with the help of devices like switches and bridges. This layer, though, has many attacks against it. Common threats include MAC spoofing, which involves an attacker changing a device's MAC address to reroute data, and ARP spoofing, an exploit of the Address Resolution Protocol that enables traffic to be redirected to the attacker's device. VLAN hopping occurs when poorly configured trunk ports are used to access several VLANs unauthorizedly. DHCP spoofing involves rogue devices that act like DHCP servers, capturing the traffic. Furthermore, rogue access points, like those constructed with the WiFi Pineapple, invite the user to associate and connect through unauthorized networks, capturing sensitive information in the process. Best practices should include turning off dynamic trunking and setting BPDU guards on necessary interfaces. Staff can be made aware of such possible threats to help maintain the security and integrity of the network.

5.3 Network Layer

The Network Layer, Essential for internet access, operates much like the process of posting a letter. It's responsible for identifying the address of the destination and routing packets to the destination address in the most efficient way possible. This layer uses IP addresses to trace and direct packets to their intended destinations, ensuring they take efficient routes. A key part of this process is ARP, Address Resolution Protocol, which the Network Layer uses to map IP addresses onto the MAC addresses within a local network. However, there have been several attacks against the network layer. The most crucial threat is a man-in-the-middle attack, in which the attacker acts as an intermediary, listening to communications between two parties and maybe even modifying them [13]. The second of the standard attacking methods is ARP spoofing, which involves sending false ARP messages to trick a system into redirecting packets meant for another to the attacker's device. It provides security measures that hide network activities, creating a baseline of regular network traffic to compare incoming traffic against anomalies using packet sniffers, among other strategies in defending against network attacks. These attacks that focus on the Network include IP spoofing, routing table overwriting, ICMP redirects, TCP/UDP floods, SYN floods, and smurf attacks. The intricacy of securing this network layer comes out, providing scope for implementing security measures beyond that provided by an operating system.

5.4 Transport Layer

The Transport Layer is responsible for segmenting large messages from the Application Layer into small portions, or segments, for transmission over the Network Layer and then reassembling those segments back into the original message upon reaching the destination [7]. This layer allows both connection-oriented services via TCP, or Transmission Control Protocol, which provides reliable communication with acknowledgments that ensure the integrity of the data transferred, as well as connectionless services via UDP, or User Datagram Protocol, which offers quick, though less reliable, transmission of data as is suitable for applications such as streaming. The Transport Layer performs error detection and correction, flow control, and adds source and destination port numbers, allowing data to reach a device's correct applications. It handles these features, providing for the correct segmentation of data, its transmission, and reassembly—an essential interface between the Application and Network Layers. The Transport Layer is also vulnerable to several security threats. Mainly, lateral movement is hazardous: the attackers do network vulnerability scans, exploit them, and thereby move from device to device, which increasingly extends the scope of compromise and, consequently, the cost of restoration [5]. Other Layer 4 attacks include TCP/UDP port scanning, which involves sending packets to specific ports to identify vulnerabilities and, through the responses received, try to know the result. It also includes DNS poisoning, a corruption of data on DNS servers that enables the redirection of queries to malicious destinations, and TCP/UDP floods, which overwhelm a target device's ports with too many packets for it to handle and allow the handling of legitimate traffic. Effective prevention of these threats requires proper strategies to limit lateral movement and concurrently implement network segmentation with robust monitoring and defensive measures.

5.5 Session Layer

The Session layer is essential in managing the connection establishment, maintenance, and termination between processes to enable them to communicate with each other. It manages synchronization by inserting checkpoints into the data stream; in case of an error, it eliminates all data sent following a checkpoint. Half-duplex, which describes two-way but not simultaneously, and full-duplex, which describes two-way communications simultaneously, are supported at this layer. In the TCP/IP model, all functions of the Session Layer get rolled into the Application Layer, which is home to protocols like NetBIOS and PPTP. NetBIOS provides a method for applications to communicate over a local network; PPTP creates secure, encrypted VPN tunnels over the Internet. For instance, the

Session Layer of a messaging application sends compressed, encrypted data by formatting it into bits. The Session Layer is vulnerable to many different types of threats. Session hijacking, probably the most important, means attackers usually intercept active sessions due to malware-infected sites or applications that enable the attacker because of a stolen session cookie. This could be due to exploiting session privileges or bypassing security controls like VPNs, NAC, and WAF by vulnerabilities or credential compromises. Finally, enforcement may occur at the network ports, endpoint agents, cloud environments, or control appliances for new security technologies such as SSE, SASE, ZTNA, network overlays, and micro-segmentation. Another attack involves an adversary-in-the-middle attack, a modern variation of man-in-the-middle attacks wherein communications get hijacked, and the attacker assumes some employee identity to get access to protected data. Entailing protection of the session layer through identity and access management platforms like Okta, BeyondTrust, and CyberArk, coupled with passwordless technologies such as HYPR, Trusona, and Auth0—defending user identities and securely managing access controls.

5.6 Presentation Layer

The Presentation Layer gets data from the Application Layer ready for transfer over a network; this it achieves by dealing with some of the very important functions, including translation of data formats between systems, usually from ASCII to EBCDIC and vice versa. It also encrypts and decrypts data for security purposes, plus compressing data for efficient transfer. ASCII is a standard 7-bit encoding that shows text in 128 characters, while EBCDIC is an 8-bit standard developed by IBM, supporting 256 characters used in old legacy mainframes. Common protocols and formats at this layer include JPEG, MPEG, and GIF. The Presentation Layer itself, however, is also vulnerable to several forms of attack, including the cracking of encryption methods in order to reveal protected data; injection attacks, which extract data or execute malicious commands, such as SQL and command injection; file inclusion vulnerabilities from poorly coded applications; cross-site scripting (XSS) attacks that inject malicious scripts into websites; and cross-site request forgery (CSRF), where users are tricked into creating, updating, or deleting something in their accounts [8].

5.7 Application Layer

Application Layer is the topmost layer of the OSI Model and is responsible for managing the execution of network applications and transmitting the data involved. It provides the

interface for applications to access network information and present it to the user. Examples include Web browsers and messaging applications like Skype. Also known as the Desktop Layer, this layer supports many well-known protocols such as SMTP for email transmissions, Network Virtual Terminal to log into other hosts, File Transfer Protocol (FTP) to manage files, and Directory Services to access distributed databases. While the OSI Model is a conceptual framework, real-world internet deployment relies on the TCP/IP model.

Because the Application Layer is the closest to the user, it is a preferred target of hackers. Examples of such common attacks include viruses, which corrupt or steal data; worms that copy themselves and shut down systems; keyloggers track keystrokes to secure credentials; and backdoors that open up entry points for unauthorized access. SQL injection and cross-site scripting exploit defects in the code, while bugs can cause interruptions in operation. A Trojan appears as a regular program and executes malicious activity [5]. Knowing these threats is, therefore, fundamental to the implementation of adequate security measures to protect information systems and end-users.

6 Social Engineering

Social engineering is attempting to gain access to unauthorized information through social manipulation. As mentioned throughout the paper, social engineering techniques were responsible for most of the spreading of malware in recent years. The main danger of social engineering is that no matter how many protections one uses, anyone becomes the most significant vulnerability without adequate knowledge, and people are easy to manipulate. Three significant social engineering techniques are phishing, baiting, and peer pressure. Phishing is similar to impersonation. Phishing attacks commonly use fake emails or links to attempt to gain control of a user' s device or steal information. Phishing emails will commonly impersonate a company and try to get a user to click a link or download a malicious attachment, which can spread malware. There are four types of phishing: Spear, Whaling, Vishing, and Email Phishing [12]. Spear phishing is a phishing attack that targets a specific group or individual. Whaling is similar. However, the targets are higher-ups with significant power or control, such as the CEO or other executives. The goal of a vishing attack could be the same as a Spear or Whaling attack; however, the attack is through a call instead of a text message or email. Email phishing is widespread and has the same goals as Spear or Whaling attacks, but the attack is through emails. Typically, the user must download malware through malicious links or

email attachments. Baiting is a social engineering attack typically carried out through hardware, such as malicious HID devices, also known as human interface devices. Baiting attacks are frequently carried out through fake USB drives. These fake drives get left in a place the target has access to, and then, they will eventually get curious and plug the drive into their device. The drives have a payload that executes when plugged in and can perform various tasks depending on how they are programmed. One of the most famous drives for baiting attacks is the USB Rubber Ducky developed by Hak5. These drives have payloads programmed in a ducky script. They are particularly dangerous because the drives will appear on the target's operating system as a standard USB drive, which grants them more permissions and makes it harder for antiviruses to detect them. Peer pressure is the pressuring someone to do something or reveal information they otherwise would not. Peer pressure can be found in both the technological and physical worlds and can be equally damaging. Peer pressure is frequently present in chat and game servers. For example, one player might ask the administrator, who is most likely their friend, for higher permissions on their server. The administrator might grant the user higher access because they are friends; however, this is now a security vulnerability and is a failed example of the least privilege principle. The least privilege principle is the concept of granting users the least amount of privileges possible to prevent security vulnerabilities. Peer pressure can also result in downloading files or going to a website that one might not otherwise go to just because someone close to them instructs them. It is critical to avoid falling into peer pressure for increased network security.

7 Conclusion

Social engineering is an overwhelming contributor to the spread of malware across networks. Despite the lack of education on cybersecurity taught to students in school, it is critical to change this to reduce the damage of malware in the future. Research has shown that the different layers of the OSI network model are responsible for security; however, the most critical vulnerabilities are always people. Through surveying fellow students, we have found that the younger generation is growing more aware of cyber threats despite the lack of education. We acknowledge that our survey has limitations due to the survey pool and assuming that no participants just unthinkingly guessed. However, our findings still suggest that we need to develop cybersecurity education to prevent the spread of malware mentioned throughout the paper. We recommend that readers of this paper take the time to properly educate themselves on network security after reading about the harm in recent years. We urge more schools to educate their stu-

dents on network security to ensure the next generation is safe and that they can spread their knowledge to older generations. We want to leave our readers with a quote from Mahatma Gandhi, "Be the change you wish to see in the world." We urge our readers to take responsibility for their new knowledge and help educate their friends and family to make the world safer.

References

[1] Anon. "Most high schools don't teach cybersecurity. This Pitt program aims to change that." In: *University of Pittsburgh* (2023). URL: https://www.pitt.edu/pittwire/features-articles/cybersecurity-gencyber-teachers.

[2] Anon. "The History and Impact of the ILOVEYOU Virus". In: *Goldsky Security* (2023). URL: https://www.goldskysecurity.com/the-history-and-impact-of-the-iloveyou-virus/.

[3] Anon. "What is malware?" In: *Cisco* (n.d.). URL: https://www.cisco.com/site/us/en/learn/topics/security/what-is-malware.html#jump-anchor-4.

[4] Kurt Baker. "The Zeus Trojan Malware —Definition and Prevention". In: *Crowdstrike* (2023). URL: https://www.crowdstrike.com/cybersecurity-101/malware/trojan-zeus-malware/.

[5] Byos. "How Cyber Adversaries Attack Each of the OSI Layers 1-7". In: *BYOS* (2023). URL: https://www.byos.io/blog/types-of-cyber-attacks-osi.

[6] Cloudflare. "What is the OSI Model?" In: *Cloudflare* (2024). URL: https://www.cloudflare.com/learning/ddos/glossary/open-systems-interconnection-model-osi/.

[7] James Edward and Richard Bramante. "Introduction to Computer Networking". In: *Google LLC* (2017). URL: https://www.google.com/books/edition/Introduction_to_Computer_Networking/uqI7DgAAQBAJ?hl=en&gbpv=1&dq=Introduction+to+Networking&printsec=frontcover.

[8] GeeksForGeeks. "What is OSI Model? –Layers of OSI Model". In: *GeeksForGeeks* (2017). URL: https://www.geeksforgeeks.org/open-systems-interconnection-model-osi/.

[9] Eloise Hendy. "iPad Kids Are Getting Out of Hand". In: *Vice* (2023). URL: https://www.vice.com/en/article/93k8kv/ipad-kids-gen-alpha-childhood-development.

[10] Kaspersky. “What is WannaCry ransomware?” In: *Kaspersky.com* (2019). URL: https://usa.kaspersky.com/resource-center/threats/ransomware-wannacry.

[11] Etay Maor. “Diagnosing the Details of a Malware Infection”. In: *Security Intelligence* (2015). URL: https://securityintelligence.com/diagnosing-the-details-of-a-malware-infection/.

[12] Trend Micro. “What Are the Different Types of Phishing?” In: *Trend Micro* (2022). URL: https://www.trendmicro.com/en_us/what-is/phishing/types-of-phishing.html.

[13] Pooja Rawat. “Common Security Attacks in the OSI Layer Model”. In: *InfosecTrain* (2023). URL: https://www.infosectrain.com/blog/common-security-attacks-in-the-osi-layer-model/.

[14] Cisco Talos. “DarkGate switches up its tactics with new payload, email templates”. In: *Cisco Talos Blog* (2024). URL: https://blog.talosintelligence.com/darkgate-remote-template-injection/.

[15] National University. “The Negative Effects of Technology on Children”. In: *National University* (2021). URL: https://www.nu.edu/blog/negative-effects-of-technology-on-children-what-can-you-do/.