International Journal of Electrical, Electronics and Computer Engineering **13**(1&2): 29-34(2024)

ISSN No. (Online): 2277-2626

Cyber Attacks and Prevention through Past Learnings

Vipul Sharma*

Department of School of Computer Science and Engineering

Govt. P.G College Dharamshala, Himachal Pradesh Technical University (HPTU) India.

(Corresponding author Vipul Sharma)*

(Received: 07 January 2024, Accepted: 26 March 2024)

(Published by Research Trend, Website: www.researchtrend.net)

ABSTRACT: Cyber security is a critical matter of concern in today's world, with cyber-attacks posing significant threats to individuals, organizations, and governments worldwide. This research paper explores the landscape of cyber security, focusing on strategies for prevention, challenges faced in implementation, and future directions in the field. By analysis of existing case studies, and emerging trends, this paper aims to provide insights into effective cybersecurity practices and potential areas for further research and development. There are many more ways to enhance cyber security nowadays like some general guidelines, patch updates, etc. But this paper only aims to provide the insides about the past learnings from famous breaches and also how we can save our systems by stepping up with the new technologies.

Keywords: Cyber-attacks, data breach, frameworks.

INTRODUCTION

In today's world, cybersecurity stands as a critical cornerstone for safeguarding our digital assets, privacy, and infrastructure. As technology continues to advance at a rapid pace, the proliferation of cyber threats poses significant challenges to individuals, businesses, and governments worldwide. This research paper aims to delve into the multifaceted realm of cybersecurity, exploring its definition, importance, and the escalating cyber threat landscape. The paper will also outline its impact on various stakeholders, elucidating the purpose and structure of the research to follow.

Definition of Cybersecurity and Its Importance: Cybersecurity involves a set of practices, technologies, and procedures designed to protect digital systems, networks, and data from unauthorized access, use, and misuse. Information security spans many disciplines, including network security, application security, and operational security. The foundation of cybersecurity is to ensure the confidentiality, integrity, and availability of digital assets and protect them from threats such as hackers, malware, phishing attacks, and data leakage. The importance of cyber security cannot be ignored in today's digital age. As businesses increasingly rely on digital technologies to drive innovation, improve operations, and deliver services, they become more vulnerable to cyber-attacks. Cybersecurity breaches can lead to serious consequences such as financial loss, image damage, administrative fines, and liability. Additionally, cyber-attacks can disrupt critical systems, compromise sensitive information, and undermine trust in digital systems, posing a serious risk to national security and public safety.

Cyber Threat Landscape: The cyber threat landscape is constantly evolving, with threat actors employing increasingly sophisticated tactics, techniques, and procedures to exploit vulnerabilities and circumvent security measures. Cyber-attacks come in various forms, ranging from simple phishing scams and malware infections to complex, coordinated cyber campaigns orchestrated by state-sponsored hackers and organized cybercrime groups. With the proliferation of interconnected devices, the Internet of Things (IoT), and cloud computing, the attack surface continues to expand, providing adversaries with new opportunities to target individuals, organizations, and critical infrastructure.

Common Cyber Attacks: Cyber-attacks are perpetrated by threat actors with varying motivations, ranging from financial gain to espionage, sabotage, and activism. Understanding the common types of cyber-attacks is crucial for developing effective cyber security defences. This section provides a detailed examination of prevalent cyber-attacks, including phishing, malware, Ransomware, DDoS attacks, and social engineering. Real-world case studies are presented to illustrate the impact of these attacks and highlight evolving tactics and techniques employed by cybercriminals.

Phishing Attacks: Phishing is the most common form of social networking, which involves tricking, coercing, or manipulating people into sending messages or valuables to unscrupulous individuals. Social engineering attacks rely on human error and manipulation to succeed. The aggressor poses as a person or organization the victim trusts (such as an employee, manager, or company that does business with the victim or the person working with the victim) and creates a crisis that causes the victim to resort to violence. Hackers and scammers use these techniques because it is easier and cheaper to fool people than to infiltrate a computer or network (IBM, IBM, n.d.).

APWG detected 1,077,501 phishing attacks in the 4th quarter of 2023. APWG detected nearly 5 million phishing attacks in 2023, making this the worst year for phishing. Attacks on social media platforms will explode in 2023, accounting for 42.8% of all phishing attacks(APWG, APWG, n.d.).

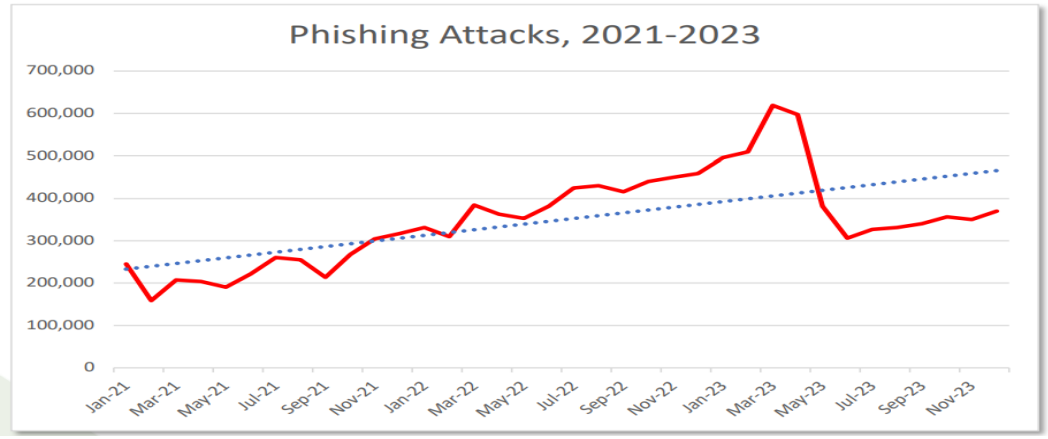


Fig. 1. {(APWG, APWG_TRENDS_REPORT_Q4_2023.PDF, 2023)}.

Malware Attacks: Malware, short for malware, includes many groups of software designed to enter, destroy, or gain unauthorized access to a computer. Basic types of malware includes viruses, worms, Trojans, spyware, and ransomware. Malware can spread through plathora of methods, including mail links, corrupted websites, removable storage devices, and software downloads.

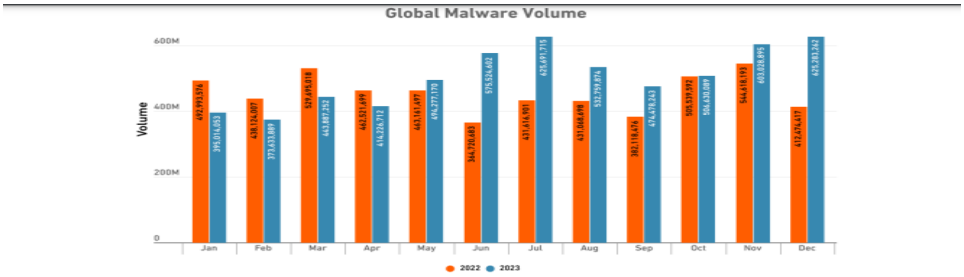


Fig. 2{(IBM, 2024 SONICWALL CYBER THREAT REPORT, 2024)}.

Ransomware Attacks: Ransomware is a kind of malware that encrypts data or locks users out of the system until a ransom is paid. These attacks have become more common in past years, targeting individuals, organisations, &critical systems. Cybercriminals often demand payment in cryptocurrency, making tracking and law enforcement difficult.

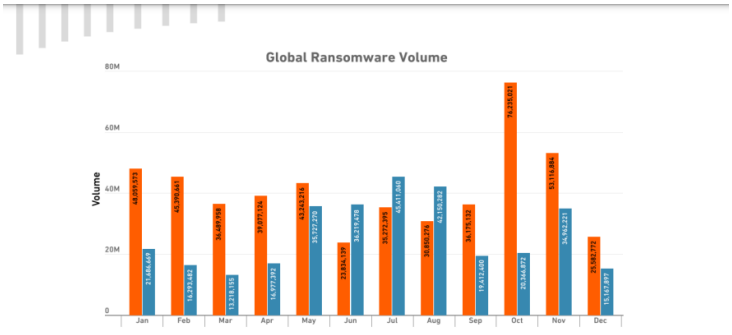
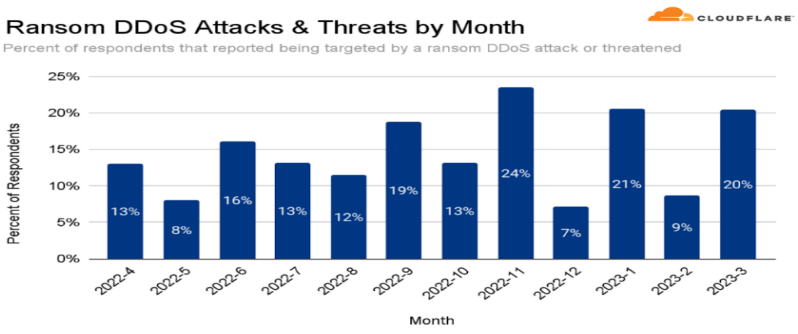


Fig. 3(IBM, 2024 SONICWALL CYBER THREAT REPORT, 2024)

DDOS Attacks: A Conveyed Dissent of Benefit (DDOS) assault may be a pernicious endeavor to disturb activity to a target server, benefit, or organize by flooding the target or encompassing environment with overwhelming Web utilization. DDOS assaults work by having different compromised computers act as endpoints. Pertinent frameworks may incorporate computers and other organize administrations such as IoT gadgets. A high-level DDOS assault is like an startling activity stick on a thruway that anticipates activity from coming to a goal (cloudflare, n.d.).



Percent of users reporting a Ransom DDoS attack or threat, per month

Social Engineering Attacks: Social engineering is a kind of cyber attack in which criminals manipulate victims into providing sensitive information. This is one of the biggest headaches for cyber security professionals today. Attackers will often use information gathered from social media to deceive victims into believing they are trustworthy and then persuade victims to provide information or take actions that affect security. Sometimes these criminals try to trick people into handing over cash or personal information; other times they try to steal corporate information through financial attacks. They are sometimes backed by countries in crisis and seek to destroy important systems or persuade politicians to reveal secrets. However serious damage can occur, as IBM's 2023 Cost of Information Report shows the average cost of a social media attack is $4.76 million(Wollacott, n.d.).

CYBER FRAMEWORKS AND STANDARDS

This is a framework or some set of rules that reduce the chance of the cyber-attack threat and talks about some of the preventive measures. This section explores established cybersecurity frameworks and standards, including the NIST Cybersecurity Framework, ISO/IEC 27001, and CIS Controls. It examines how these frameworks can assist organizations in developing and implementing robust cybersecurity policies and procedures, as well as the challenges and considerations associated with adopting and adhering to cybersecurity standards.

NIST Cybersecurity Framework (CSF): Developed by the National Institute of Standards and Technology (NIST), the NIST Cybersecurity Framework is a voluntary framework designed to help organizations manage and reduce cybersecurity risks. It provides a common language for cybersecurity and a method for evaluating and improving cybersecurity practices. The framework has five main roles: identify, prevent, detect, respond, and recover. Organizations can use CSFs to set cybersecurity priorities, develop risk management strategies, and align cybersecurity with business goals (NIST, n.d.).

ISO/IEC 27001: ISO/IEC 27001 is an worldwide standard for data security administration (ISMS) distributed by the Worldwide Organization for Standardization (ISO) and the Worldwide Electro-Technical Commission (IEC). It gives a way to oversee touchy data and guarantee its secrecy, astuteness, and accessibility. ISO/IEC 27001 indicates necessities for the foundation, usage, support, and ceaseless enhancement of ISMS, counting chance appraisal, chance treatment, and observing and assessment of data security administration. ISO/IEC 27001 is the world's best data security administration (ISMS) standard. It characterizes the necessities that the ISMS must execute. The ISO/IEC 27001 standard guides companies of all sizes and in all ranges of work in making, actualizing, keeping up, and ceaselessly making strides data security administration frameworks. Complying with ISO/IEC 27001 implies that an organization or trade has control over the dangers related with the security of data the company claims or forms which the framework regards all best hones and standards set out in this worldwide standard (ISO, n.d.).

CIS Controls Cybersecurity Centre (CIS) Controls, formerly known as the SANS Top 20 Security Controls, are a key set of cybersecurity best practices developed by an international community of experts. CIS Critical Security Controls (CIS Controls) is a written, clear, and simple collection of best practices that can be used to strengthen your cybersecurity. Today, thousands of cybersecurity professionals from around the world use CIS management and/or contribute to its development through the community consensus process. These controls are divided into three categories: Fundamental, Fundamental, and Organizational. Organizations can use CIS management to identify and implement effective security controls based on their risks, resources, and operations. (CIS, n.d.).

CYBER SECURITY FRAMEWORKS ASSIST ORGANIZATIONS:

1. Risk Management: Cyber security frameworks help organizations identify, assess, and prioritize cyber security risks, enabling informed decision-making and resource allocation.

2. Compliance: Compliance with cyber security frameworks and standards demonstrates an organization's commitment to cyber security best practices and may be required by industry regulations, contractual agreements, or government mandates.

3. Continuous Improvement: Cyber security frameworks provide a structured approach for evaluating and improving cyber security practices over time, fostering a culture of continuous improvement and adaptation to evolving threats.

4. Resource Optimization: By providing guidance on cyber security priorities and best practices, frameworks help organizations optimize their cyber security investments and resources, focusing on areas with the greatest impact on security posture and risk reduction.

CHALLENGES AND CONSIDERATIONS:

1. Complexity: Implementing cyber security frameworks can be complex and resource-intensive, requiring dedicated time, expertise, and resources to develop and maintain effective cybersecurity programs.
2. Scalability: Organizations may face challenges in scaling cybersecurity frameworks to meet the needs of diverse business units, geographies, and operational environments.
3. Integration: Integrating cyber security frameworks with existing business processes, systems, and workflows may require careful planning and coordination to ensure alignment and effectiveness.
4. Sustainability: Maintaining compliance with cyber security frameworks requires ongoing monitoring, assessment, and adaptation to changes in the threat landscape, technology landscape, and regulatory environment.
Cyber security frameworks and standards play a crucial role in helping organizations manage cyber security risks and protect sensitive information. By leveraging established frameworks such as the NIST Cyber security Framework, ISO/IEC 27001, and CIS Controls, organizations can develop and implement robust cyber security policies and procedures tailored to their unique needs and risk profiles. However, adopting and adhering to cybersecurity standards pose challenges that organizations must address through careful planning, investment, and collaboration across business units and stakeholders.

METHODOLOGY

This section presents relevant case studies related to cyber-attacks. Through the analysis of real-world incidents, we are concluding some results that will get to the problem-solving of such problems in future scenarios. Some risks can be found in the time when it occurs. But to deal with cyber security and apply a proactive approach we need to learn from past breaches and also side by side need to be developed in the area of technology. Here I just compared the past attacks with each other to find out some conclusions that will be helpful for the future proactive approach.

Case Study: Equifax Breach

The Equifax data breach in 2017 is a good example of a major cyberattack with major consequences. Hackers exploited a vulnerability in Equifax's website to gain unauthorized access to the personal and financial information of approximately 147 million customers. The company was first attacked through its customer complaint portal, using a useful feature that needed to be fixed, although it was not due to a breach in Equifax's internal processes. Because the systems are not sufficiently isolated from each other, attackers can move from the web portal to other servers and find usernames and passwords stored in the whitepaper, which then allows them to break into many other machines. Attackers extracting data from the web in encrypted form went undetected for months because one of Equifax's internal security tools did not update its encryption certificate. Equifax management waited more than a month after discovering the breach before reporting it. Executives who sold stocks at the time were accused of insider trading. This product led to Equifax's worst and ultimately largest breach (Fruhlinger, 2020).

Case Study: Not Petya Ransomware Attack: Even the Petya ransomware attack in 2017 did not target organizations around the world, including shipping giant Maersk, pharmaceutical company Merck, and FedEx partner TNT Express. Ransomware spreads rapidly through software updates, encrypting data, and disrupting device performance. The attack highlights the interconnectedness of global devices and the vulnerability of critical infrastructure to cyberattacks. Organizations affected by Not Petya face significant financial losses, operational disruptions, and reputational damage. In this paper, we examine the impact of a Russian cyberattack targeting Ukraine and other businesses of the Danish international shipping company A.P. (now known as "Not Petya"). Mäller-Maersk. Maersk is one of many well-known companies involved in the Russian cyber industry. This case study focuses on Maersk's response when its computer systems were quickly breached. He described how various aspects of the company's cybersecurity program were affected by the spread of the Petya malware and how this affected Maersk's operations in the days following the attack. This study specifically highlights the importance of network sharing and effective data recovery as a defense against this attack. Maersk's Not Petya experience also reveals the increasing use of cyber attacks in conflict zones and their potential to disrupt global trade(Burmfield, 2022)(information age, n.d.). Some more case studies related to different cyber-attacks are given here:

Case No 1: Upsher-Smith Laboratories- Even though this incident happened in 2014, it is important because it is one of the classic email examples of the CEO scam category. CEO scams are cyber-attacks by malicious actors who impersonate an organization's CEO and send phishing emails to the organization's employees. In this case, the cyber attacker impersonates an employee of the organization. The company's CEO sent an email to the accounts payable manager of Upsher-Smith Laboratories, a pharmaceutical company in Maple Grove, asking him to follow the instructions of the CEO and the company attorney. The purpose of the instruction was to transfer more than $50 million to the fraudster's account through a nine-line transaction. Although the group managed to prevent one of the changes in the bank, the loss amounted to $ 39 million (PhishProtection.com, n.d.).

Case No. 2-WannaCry: A perfect ransomware storm: WannaCry is a ransomware virus that spread rapidly to many computers in May 2017. After infecting a Windows computer, it encrypts files on the computer's hard drive, making them more accessible, and then demands a ransom in Bitcoins to identify the information. Several factors make the initial spread of Wanna Cry particularly remarkable. It affected many critical and sensitive systems, including much of the National Health Service in the United Kingdom. It used the Windows operating system, which was first

discovered by the US National Security Agency Vulnerability. It was initially linked by Symantec and other security researchers to the Lazarus Group, a cybercriminal organization that may have ties to the North Korean government (CSO, 2022).

Case 3- The Google Attack, 2020: On October 16, 2020, the Google Threat Analysis Group (TAG) published a blog update explaining the threats and how threat actors are changing strategies in response to the 2020 US election campaign. At the end of the report, the company slyly added a note - In 2020, our Security Reliability Engineering team measured data-cracking UDP upgrade halts for several Chinese ISPs (ASN 4134, 4837, 58453, and 9394). This is still the largest bandwidth attack we know of. Three Chinese ISPs' attacks on thousands of Google IP addresses lasted six months and reached 2.5 Tbps! Google Security Reliability Engineer Damian Menscherwrote: Attackers used multiple networks to spoof 180,000 CLDAP, DNS, and SMTP servers exposed at 167 Mbps (millions of packets per second), which the server would then send to us. A flood of responses. This is a testament to the type of attack a successful attacker can perform and that's four times the 623Gbps record set by the Mirai botnet a year ago (Nicholson, 2022).

Case 4: The Attack That Broke Twitter

In middle of July, Twitter announced that hackers used a technique called "phone spear phishing" that allowed attackers to target the accounts of 130 people, including CEOs, renowned peoples, and political learders. Hackers managed to gain control over 45 of these accounts and used them to send tweets promoting Bitcoin scams. Twitter wrote a blog post about the incident, in which hackers called Twitter employees and used fake credentials to trick them into giving up their Details, giving the attackers access to the company's tools and allowing them to reset the password and work. Purpose of use of the account (Greenberg, 2020).

RESEARCH FINDINGS

Empirical research studies have examined the effectiveness and resilience of cybersecurity measures and defense strategies across various industries and organizational contexts. Research findings suggest that organizations with mature cybersecurity programs, strong governance, and proactive risk management practices are better equipped to avoid, detect, and revert back to cyber threats. Key factors contributing to cybersecurity effectiveness include executive leadership, investment in cybersecurity technologies and talent, employee training and awareness, threat intelligence sharing, and incident response preparedness. Moreover, organizations that adopt a holistic and risk-based approach to cybersecurity tend to exhibit greater resilience and adaptability to evolving threats and challenges.

Studies on cyber risk management and mitigation have identified several best practices and strategies for assessing, prioritizing, and mitigating cyber risks effectively. Risk assessment methodologies such as the NIST Cyber security Framework, ISO/IEC 27005, and FAIR (Factor Analysis of Information Risk) provide organizations with structured approaches for identifying, analyzing, and managing cyber risks

The basic result of all these attacks was mostly the systems were not up to date and due to a lack of awareness in the staff they also ignored little things like some of the security checks, ensured data privacy, and even encryption of the data to the safest. All these things led to these breaches. Also, they should conduct a security check by calling some white hat hackers to enhance their system security to the best of their time.

In conclusion, case studies and research findings play a crucial role in advancing our understanding of cybersecurity and informing effective defense strategies and risk management practices. By analyzing real-world incidents and empirical studies, organizations can learn from past mistakes, identify common attack patterns, and implement proactive measures to strengthen their cybersecurity posture and resilience.

CONCLUSION

In the constantly developing area of digital connectivity, concept of cybersecurity stands as a paramount concern for individuals, businesses, and governments alike. This research paper has delved into various facets of cybersecurity, from common cyber threats to emerging trends and technologies, cybersecurity frameworks, case studies, and future directions. As we conclude, it's essential to summarize the key findings and insights derived from our exploration, emphasizing the critical importance of prioritizing cybersecurity efforts to safeguard digital assets and mitigate cyber threats, particularly in the context of the specific challenges and opportunities we've discussed. In the context of our exploration, it's evident that cyber threats will remain thoughtful but still, we have to learn from the experiences and try to evaluate the best out of it to reduce the percentage risk. From phishing and ransomware attacks to emerging threats leveraging AI and quantum computing, the cybersecurity landscape is dynamic and ever-changing. Despite these challenges, our research highlights the importance of proactive cybersecurity measures, robust defense strategies, and a culture of cyber resilience. By adopting these measures our conclusions and established frameworks together we can make an attack-proof security system. Moreover, investing in cybersecurity awareness training, talent development, and incident response planning can empower organizations to detect, respond to, and recover from cyber-attacks more effectively. Looking ahead, it's clear that cybersecurity will remain a pressing concern in the digital age, requiring continued research, collaboration, and innovation to address evolving threats and challenges. Policymakers, industry stakeholders, and cybersecurity professionals must work together to develop comprehensive strategies, policies, and initiatives to strengthen cybersecurity resilience and ensure a secure digital future for all. By embracing a proactive and holistic approach to cybersecurity, we can navigate the complexities of the digital landscape with confidence and resilience, safeguarding our digital

assets and preserving trust in the digital ecosystem. In conclusion, the journey toward cybersecurity excellence is ongoing, but with dedication, vigilance, and collective effort, we can rise to the challenges ahead and build a safer and more secure digital world for generations to come.

REFERENCES

(n.d.). Retrieved from CLOUDFLARE: https://blog.cloudflare.com/ddos-threat-report-2023-q1/

(n.d.). Retrieved from information age: https://www.information-age.com/notpetya-five-years-on-cyber-security-lessons-learned-by-organisations-19999/

(n.d.). Retrieved from PhishProtection.com: https://www.phishprotection.com/phishing/phishing-case-studies-learning-from-the-mistakes-of-others

(n.d.). Retrieved from fortinet: https://www.fortinet.com/resources/cyberglossary/artificial-intelligence-in-cybersecurity

(n.d.). Retrieved from NIST: https://www.nist.gov/cyberframework

(n.d.). Retrieved from ISO: https://www.iso.org/standard/iso-iec-27001-2022-v2

(n.d.). Retrieved from CIS: https://www.cisecurity.org/controls

(2022). Retrieved from CSO: https://www.csoonline.com/article/563017/wannacry-explained-a-perfect-ransomware-storm.html

Allan, K. (2023). Retrieved from cybermagzine: https://cybermagazine.com/articles/the-rapidly-evolving-threat-landscape-of-2024

APWG. (2023). apwg_trends_report_q4_2023.pdf. APWG.

bbc. (2013). phishing attack. bbc news, 2.

Benjamin, N. (2021). Retrieved from ISACA: https://www.isaca.org/resources/isaca-journal/issues/2021/volume-4/how-effective-is-blockchain-in-cybersecurity

Burmfield, C. (2022). Retrieved from CSO: https://www.csoonline.com/article/573049/5-years-after-notpetya-lessons-learned.html

cloudflare. (n.d.). Retrieved from CLOUDFLARE: https://cloudflare.com/learning/ddos/what-is-a-ddos-attack/

fruhlinger, J. (2020). Retrieved from CSO: https://www.csoonline.com/article/567833/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html

Greenberg, A. (2020). Retrieved from WIRED: https://www.wired.com/story/phone-spear-phishing-twitter-crime-wave/

(n.d.). Retrieved from IBM: https://www.ibm.com/topics/phishing

IBM. (2024). 2024 SonicWall Cyber Threat Report.

IBM. (2024). 2024 SonicWall Cyber Threat Report.

Lipman, P. (2021). Retrieved from forbes: https://www.forbes.com/sites/forbestechcouncil/2021/01/04/how-quantum-computing-will-transform-cybersecurity/?sh=153a8bff7d3f

Nicholson, P. (2022). Retrieved from A10: https://www.a10networks.com/blog/5-most-famous-ddos-attacks/

Wollacott, E. (n.d.). Retrieved from Forbes: https://www.forbes.com/sites/technology/article/what-is-social-engineering/?sh=776595ae2281