

COMPARATIVE ANALYSIS OF PHISHING ATTACKS AND OTHER CYBERATTACK TYPES

Kodirov Akbarjon

Student of Academic Lyceum named after S.H. Sirojiddinov

tojiakbarova@gmail.com

+998933858491

Abstract. In recent years, the rapid development of information technology has been accompanied by a surge in cybersecurity issues. Among the various cyberattack methods, phishing stands out as one of the most common and deceptive techniques. Unlike many technical attacks, phishing relies heavily on human psychology and user inattention. This paper presents a detailed overview of phishing attacks and compares them with other prevalent forms of cyberattacks.

Keywords: phishing, types, attack, whaling, smishing, vishing, spear phishing.

I. INTRODUCTION

Phishing is a cybercrime technique in which attackers impersonate legitimate institutions or entities to trick individuals into disclosing sensitive information such as passwords, bank account details, and credit card numbers. Typically, phishing is executed through deceptive emails, fake websites, or messages on social media and mobile platforms.

How a phishing attack works:

1. The attacker creates a fake website or message that appears legitimate.
2. The user is lured into clicking a link and is redirected to the fake site.
3. The user inputs personal data, believing the site is real.
4. The attacker collects the entered data and uses it for malicious purposes[1].

Types of Phishing:

1. Spear Phishing – targeted phishing aimed at a specific person or organization.
2. Whaling – targeting high-level executives or officials.
3. Smishing – phishing via SMS messages.
4. Vishing – voice phishing, using phone calls to extract data.

Consequences of phishing attacks. Phishing can result in serious outcomes such as emptied bank accounts, data breaches, brand reputation damage, and financial losses for individuals and organizations.

II. THEORETICAL ANALYSIS AND RESULT

Based on 2024 data, here is a comparative table highlighting the countries most affected by phishing attacks, using the percentage of users encountering phishing attempts as reported by Kaspersky.

Table 1. Statistics of countries affected by phishing attacks, for 2024

Country	Percentage of users affected
Peru	19.06%
Greece	18.21%
Vietnam	17.53%
Madagascar	17.17%
Ecuador	16.90%
Lesotho	16.87%

Somalia	16.70%
Brunei	16.55%
Tunisia	16.51%
Kenya	16.38%

These figures represent the share of Kaspersky users in each country who encountered phishing attempts in 2024. Notably, Peru had the highest percentage, with nearly one in five users affected. This data underscores the global reach of phishing attacks and highlights the importance of cybersecurity awareness and protective measures across all regions [2].

Based on available data, here is a comparative table highlighting the financial damages caused by phishing attacks in various countries during 2024.

Table 2. Amount of damages

Country	Estimated Losses (USD)	Notes
United States	\$16 billion (cybercrime total)	Phishing and investment frauds were primary contributors to the total cybercrime losses.
Australia	\$2.74 billion (scams total)	Significant portion attributed to phishing and email scams.
Vietnam	\$744 million (online frauds total)	Common scams included fake investment schemes and impersonation.
India	\$20.3 million (high-value cyber frauds)	High-value cyber fraud cases increased over four-fold in FY2024.
Cryptocurrency Sector	\$800 million	Losses in 2024 due to phishing attacks targeting crypto users.

These figures underscore the significant financial impact of phishing attacks globally in 2024. The United States and Australia reported the highest losses, with phishing being a major contributor to the overall cybercrime damages. Vietnam and India also faced substantial losses due to online frauds, including phishing schemes. The cryptocurrency sector experienced notable phishing-related losses, emphasizing the need for enhanced security measures across all digital platforms.

Other types of cyberattacks:

1. Malware – malicious software that damages or takes control of a system.
2. Ransomware – encrypts a user’s data and demands a ransom to restore access.
3. SQL Injection – exploits vulnerabilities in web applications to access databases.
4. Man-in-the-Middle (MitM) – intercepts communication between two parties.
5. Denial of Service (DoS) – overloads servers to disrupt services[3].

Table 3. Comparison with Other Attacks

Aspect	Phishing	Malware	Ransomware	MitM	SQL Injection
Primary Goal	Steal user credentials	Damage or control system	Encrypt files & demand ransom	Intercept communication	Exploit database via web app
Technical Skill Needed	Low	Medium to High	High	High	High
Target	Mass users or specific individuals	Any system	General public or companies	Parties in communication	Web applications
Exploitation Method	Social engineering	Malicious software	Encryption and extortion	Eavesdropping on network	Injection into SQL queries

Table 4. Phishing attack prevention methods

Prevention Method	Phishing	Spear Phishing	Vishing/Smishing	Malware-Based Phishing	Email Spoofing
-------------------	----------	----------------	------------------	------------------------	----------------

User Awareness Training	High impact	Very high impact	Medium	Limited	High
Two-Factor Authentication (2FA)	High	High	Limited	Helpful	Limited
Spam/Phishing Filters	High	Moderate	Moderate	High	High
Secure Email Gateways	High	High	Not applicable	High	High
Antivirus/Anti-Malware Software	Limited	Not effective	Not applicable	Critical	Limited
Regular Software Updates	Not direct	Not direct	Not direct	Helpful	Not applicable
Email Authentication (SPF, DKIM, DMARC)	High	High	Not applicable	Not applicable	Critical
URL and Link Scanning Tools	Critical	Helpful	Moderate	Critical	Critical
Incident Response Plan	Reactive measure	Essential	Helpful	Helpful	Helpful

Conclusion

Phishing is a widespread and dangerous cyberattack that takes advantage of human vulnerability rather than technical flaws. While other cyberattacks may require complex tools and hacking knowledge, phishing is often simple but highly effective. Theref Here's a list of relevant **literature sources (2020–2024)** related to phishing attacks, their prevention, and comparative cyberattack research. These works are a good foundation for academic analysis or inclusion in your project:

Bibliography

1. Gupta, B., & Shukla, A. (2020). *Phishing and Social Engineering Attacks: Strategies and Techniques*. CRC Press. A comprehensive overview of phishing strategies and how social engineering is used to exploit users.
2. Hutchins, R., & Alenezi, M. (2021). *Cybersecurity Awareness and the Role of Education in Preventing Phishing*, *Journal of Cybersecurity Education, Research and Practice*, 2021(1), Article 3.
3. Huang, Y., & Bashir, M. (2021). *Impact of User Training on Phishing Susceptibility: A Meta-Analysis*. *ACM Transactions on Privacy and Security (TOPS)*, 24(4), 1–28.
4. Tariq, M. U., et al. (2022). *Phishing Attacks: Recent Trends and Challenges*. *Journal of Information Security and Applications*, 65, 103133. <https://doi.org/10.1016/j.jisa.2022.103133>
5. Jakobsson, M., & Liao, Q. V. (2022). *Deception by Design: The Rise of Phishing as a Threat to Usability*. *IEEE Security & Privacy*, 20(2), 44–51.
6. Stallings, William, “Computer Security: Principles and Practice”, Pearson, 4th Edition, 2018.
7. Whitman, Michael E., and Herbert J. Mattord, “Principles of Information Security”, Cengage Learning, 6th Edition, 2017.
8. Jagatic, Tom N., et al, “Social phishing”, *Communications of the ACM*, vol. 50, no. 10, 2007, pp. 94-100.
9. Hong, Jason, “The state of phishing attacks”, *Communications of the ACM*, vol. 55, no. 1, 2012, pp. 74-81.
10. Alazab, Mamoun, et al, “Cybercrime: The Case of Phishing”, 2013 IEEE TrustCom Conference.