# Phishing Attacks

EDWIN MATHEW

Kennesaw State University

Atlanta, Georgia
Emathew9@students.kennesaw.edu

IKHELOWA ADEJI

Kennesaw State University

Atlanta,Georgia
Iadeji@students.kennesaw.edu

RYAN SHAH

Kennesaw State University

Atlanta, Georgia
rshah20@students.kennesaw.edu

## ABSTRACT

Phishing has become a major cybersecurity concern in the digital age, harming people, and companies all over the world. This study project explores the complexity of phishing assaults by looking at their methods, evolution, and attackers' varied strategies. We classify and examine the distinct features and techniques of phishing assaults, such as spear phishing, email phishing, whaling, smishing, vishing, and pharming.

[1].

## General Terms

***Keywords—phishing attacks, formatting, style, styling, insert** (key words)*

## 1. INTRODUCTION

Phishing attacks can occur through various channels such as social media, text messages, emails, and even phone calls. Ramzan (2010) [2] postulates that the term "phishing" is a play on the word "fishing," as attackers use bait to try to hook their victims into providing sensitive information. In this case, the bait is often a seemingly official-looking message from an organization like a bank or an email service. A phishing assault, targeting Facebook in 2018, exposed the private data of millions of users. The attackers posed as a research company and sent messages to users, asking them to install a browser extension that gave the attackers access to the user's Facebook accounts and personal information [3].

Phishing attacks typically involve several stages. The first stage is the creation of the bait, which is typically an email or other message that appears to come from a legitimate source [3]. The attacker will often use social engineering techniques to make the message seem urgent or important, to increase the likelihood that the victim will take action. The second stage is the delivery of the bait. The attacker will typically send the message to many potential victims, in the hopes that at least a few of them will take the bait; the message may contain a link to a fake website, or it may ask the victim to reply with sensitive information [4].

Once the victim has taken the bait, the attacker will collect the sensitive information and use it for their own purposes. This may involve accessing the victim's accounts, stealing their identity, or selling the information on the black market. For instance, in 2016, Snapchat suffered a phishing attack that resulted in the leak of sensitive employee information. The attackers posed as Snapchat's CEO and sent an email to the company's payroll department, requesting employee data [3]. The department was tricked into providing the information, which included Social Security numbers and salary details.

Attackers typically go to considerable lengths to make their phishing bait look authentic, making it difficult to spot. They may use logos, graphics, and other elements that are identical to those used by legitimate source [3]. They may also use domain names that are very similar to the legitimate source, in an attempt to trick the victim into thinking that they are on a legitimate website.

For protection from phishing attacks, it is important to be cautious of unsolicited messages, particularly if they ask provision of sensitive information. It is required that the legitimacy of the sender before taking any action. This may involve contacting the legitimate source directly, rather than clicking on any links in the message. Enabling two-factor authentication, which requires the input of a code or biometric verification in addition to a password, increases the security of accounts [3]. This can help protect your accounts even if an attacker has your password. Gupta added that it is also important to keep software up to date, as attackers often exploit software vulnerabilities to gain access to systems or steal information. [4] add Thus, keeping operating systems, web browsers, and other software up to date to minimize the risk of exploitation is critical.

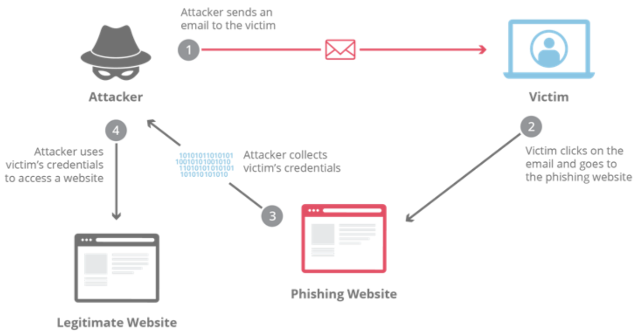

Attacker sends an email to the victim
1
Attacker
Victim
4
Attacker uses victim's credentials to access a website
Attacker collects victim's credentials
2
Victim clicks on the email and goes to the phishing website
3
Phishing Website
Legitimate Website

*Figure 1: Phishing attack diagram*

## 2. Type of phishing attacks

### 2.1 Spear Phishing

Spear phishing is a type of phishing attacks that targets a specific individual organization or business through malicious emails to seek unauthorized access to sensitive information. [7]

Hackers customize their emails with the target's name, number, and additional information to trick victims into believe that this is a legit source. The goal of this attack is to get the victim to click the malicious link. [8]

### 2.2 Whaling Phishing

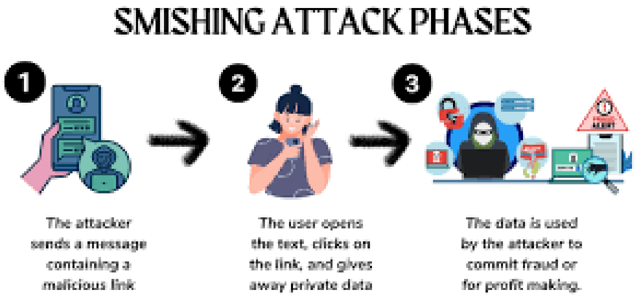
Similar to a spear phishing attack, a whaling attack targets high-level executive where attackers pose as legitimate emails. Victims of this attack are referred to as “Whales” or “Big Phish”. This type of attack is digitally enables fraud through social engineering, designed to encourage victims to initiate a wire transfer. [9]

Attackers use multiple methods to carry out whaling attacks:

- Emails
- Phone
- Pretexting
- Baiting

### 2.3 Smishing

Smishing attack is a form of phishing attacks that utilizes SMS on mobile phones to solicit victims into sending private information and/or sending private information. [10]


SMISHING ATTACK PHASES
1
2
3
The attacker sends a message containing a malicious link
The user opens the text, clicks on the link, and gives away private data
The data is used by the attacker to commit fraud or for profit making.

Attackers use a variety of methods to trick users into sending private information. They may use basic information such as the victim's name and address to convince them that the message is coming from a trusted source. [10]

### 2.4 Deceptive Phishing

Deceptive phishing is the most common and well- known type of phishing attack.[11]

Cybercriminals impersonate a recognized sender to gain personal information and/or login credentials. This type of attack will trick targets into sending information by asking them to verify their account information, change passwords or make a payment. [11]

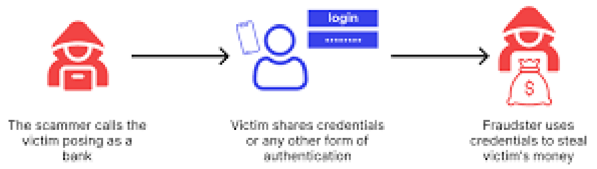
### 2.5 Clone Phishing

Clone phishing is a newer type of cyberattack where the attacker clones/replicates a legitimate email with the intention of gathering sensitive information and spreading malware, installing rootkits, and ransomware to compromise a user's device. [12]

Clone phishing is very successful because victims receive an email from a legitimate email address as opposed to a standard phishing attack. [12]

### 2.6 Vishing

Vishing is a type pf phishing attack that uses fraudulent phone numbers, voice-altering software, text messages and social engineering to trick targets into revealing personal information. [13]

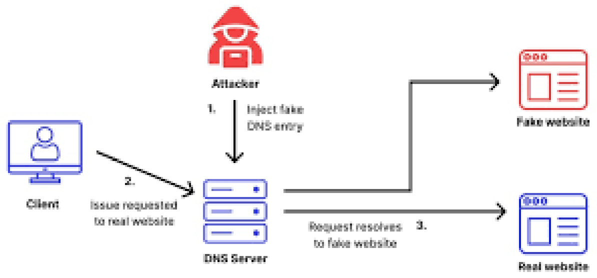

login
The scammer calls the victim posing as a bank
Victim shares credentials or any other form of authentication
Fraudster uses credentials to steal victim's money

There are multiple methods that vishers use to gain potential targets:

- A visher might send a text message to potential victims in high volume from different phone numbers. [13]
- A visher might create an automated message and robo-dial potential victims, where they use a computer-generated voice message to remove accents and build trust. [13]

### 2.7 Pharming

Pharming is a type of social engineering phishing attack that involves cybercriminals redirecting users from legitimate websites to fake websites to steal username, passwords and financial data. [14]



There are two types of pharming:

- *Pharming malware,* also known as DNS changers/hijackers, infects victims computers and stealthily make changes to their host files [14]
- *DNS poisoning:* Takes advantage of exploits in user’s software that controls the DNS servers in order to hijack the servers and reroute web traffic. [14]

### 2.8 Angler Phishing

Angler phishing is a new type of phishing attack where attackers pose as a customer service agent on social media to convince users to provide personal information and/or money. [15]

Users use social media as a way to express or complain about their experience with a store or product. Customer service agents tend to respond quicker on these platforms as opposed to traditional methods. Attackers tend to see a user’s complaint and contact them with a direct message.

## 3. Impact and Consequences of Phishing Attacks

There are multiple impacts and consequences that a phishing attack can have on personal, business and organizational sectors of people's lives. Many falls victim, costing them a significant loss of money and resources. Some ways phishing attacks can specifically affect the victim are by financial losses, damage to reputation, and loss of personal information. All this is the result of a successful phishing attack.

Also, you should not just worry about the cost of the breach but also the cleaning up coast as well.

The following are ways in which phishing attacks can affect their targets:

*Financial Loss:* Phishing attacks can cause immediate financial loss if a user is deceived into sharing their financial information. Attackers can use this information to steal money from the victim's bank account or make unauthorized purchases with their credit card.

*Loss of Personal Information*: Personal information, such as usernames, passwords, and social security numbers, can be compromised in a phishing attack. This can lead to identity theft or other types of fraud. Damage to Reputation: If sensitive information is leaked as a result of a successful phishing attack, it can harm an individual or organization's reputation, eroding customer or client trust.

*Downtime and Business Disruption*: A phishing attack can cause significant downtime and business disruption if an organization's network is compromised. This may necessitate shutting down systems or services to contain the breach and prevent further damage.

*Regulatory and Legal Penalties*: Inadequate protection of data and customer information can result in regulatory and legal penalties, such as fines under the GDPR or CCPA.

*Psychological Impact*: Phishing attacks can also have a psychological impact on their victims, causing anxiety and distress due to feelings of violation and loss of trust. In conclusion, phishing attacks can have far-reaching effects on individuals, businesses, and organizations. It is important to be aware of the risks and to take proactive measures, such as using strong passwords, enabling two-factor authentication, and exercising caution when receiving emails from unknown sources. In times like these, large-scale privacy attacks are unacceptable as they put many people at risk of harm through their personal information.

## 4. PHISHING ATTACKS

**These are some of the phishing attacks that has happened in the past few years:**

1. In 2017, a phishing scam that impersonated Google Docs was circulated via email. The email asked recipients to click on a link that directed them to a fake Google login page, where they were prompted to enter their login credentials. The attackers were then able to access users' Google accounts, potentially compromising sensitive information.

2. Business Email Compromise (BEC) attacks are a type of phishing attack that targets businesses and organizations. In a recent example, cybercriminals posed as a subcontractor and sent fraudulent invoices to a US defense contractor, using BEC tactics to defraud them out of $500,000. The invoices were paid without proper verification.

3. In 2021, phishing scams related to the COVID-19 pandemic were on the rise. One example was a phishing email that claimed to offer early access to the COVID-19 vaccine in exchange for a fee. The recipients were directed to a fake registration page where they were prompted to enter personal and financial information.

4. In a recent PayPal phishing scam, attackers sent emails claiming that the recipient's PayPal account had been suspended. The email contained a link to a fake PayPal login page where the victim was prompted to enter their login credentials. The attackers then used this information to access the victim's PayPal account and make unauthorized purchases.

## 5. BEST PRACTICES FOR AVOIDING PHISHING ATTACKS

Phishing attacks are becoming increasingly sophisticated and harder to detect. They can cause significant harm to individuals and organizations alike. Fortunately, there are several best practices that can be followed to minimize the risk of falling victim to a phishing attack:

1. Be cautious of unsolicited emails or messages: Phishing attacks often involve unsolicited emails or messages that request sensitive information or prompt the recipient to click on a link. It is important to be cautious when receiving such emails or messages, particularly if they are from unknown senders or appear to be from a legitimate organization.
2. Verify the sender: Before responding to an email or message, verify the sender's identity. Look for any signs of spoofing or impersonation, such as a slight variation in the sender's email address or domain name. If in doubt, contact the sender directly through a known, secure channel to confirm the authenticity of the message.
3. Exercise caution when clicking on links: Phishing attacks often use links to direct the victim to a fake website or to download malware. It is important to exercise caution when clicking on links, particularly those that appear to be from a trusted source. Hover over the link to view the URL and check for any signs of spoofing or impersonation.
4. Use strong passwords: Using strong, unique passwords for each account can help minimize the risk of a successful phishing attack. Avoid using common words, phrases, or personal information as passwords. Instead, use a combination of upper and lowercase letters, numbers, and symbols.
5. Enable two-factor authentication: Two-factor authentication provides an additional layer of security by requiring a second form of authentication, such as a code sent to a mobile device or fingerprint verification. This can help prevent unauthorized access to accounts, even if the password has been compromised.
6. Keep software up to date: Software updates often include security patches that address known vulnerabilities. Keeping software up to date can help minimize the risk of a successful phishing attack.

7. Educate employees: Educating employees about the risks of phishing attacks and providing regular training on how to identify and respond to suspicious emails or messages can help minimize the risk of a successful attack.

In conclusion, phishing attacks are a serious threat that can cause significant harm to individuals and organizations. By following these best practices and remaining vigilant, it is possible to minimize the risk of falling victim to a phishing attack.

## 6. CONCLUSION

With the world become more digital, phishing attacks have been at an all-time high. Phishing attacks can be either fraudulent emails, SMS, phone calls or fake sites to trick individuals into downloading malware or spyware and sharing personal information. Throughout the years, hackers have been successful in targeting high-level businesses. These attacks have caused financial, psychological, regulatory, reputational damage to a company, organization, and user. It important that consumers are educated on what phishing attacks are and how to prevent them from happening in the future. It's crucial to confirm the sender's credibility, usually by contacting the organization directly through official means or double-checking email addresses. Furthermore, stay away from downloading documents or opening links from unidentified or dubious sources as they could be shady websites set up to steal personal information. As these simple techniques can not only safeguard your information, but the people around you as well.

# References

[1] Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science*, *3*, 563060.

[2] Alsharnouby, M., Alaca, F., & Chiasson, S. (2015). Why phishing still works: User strategies for combating phishing attacks. *International Journal of Human-Computer Studies*, *82*, 69-82.

[3] CNN. (2016).Snapchat employee fell for phishing scam. Retrieved from https://money.cnn.com/2016/02/29/technology/snapchat-phishing-scam/index.html

[4] Gupta, B. B., Tewari, A., Jain, A. K., & Agrawal, D. P. (2017). Fighting against phishing attacks: state of the art and future challenges. *Neural Computing and Applications*, *28*, 3629-3654.

[5] Ramzan, Z. (2010). Phishing attacks and countermeasures. *Handbook of information and communication security*, 433-448.

[6] The New York Times. (2018). Facebook Security Breach Exposes Accounts of 50 Million Users. Retrieved from https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html

[7] M. E. Shacklett and C. Bedell, "spear phishing," *Security*, Aug. 2021, [Online]. Available: https://www.techtarget.com/searchsecurity/definition/spear-phishing

[8] "6 Common Phishing Attacks and How to Protect Against Them," *Tripwire*. https://www.tripwire.com/state-of-security/6-common-phishing-attacks-and-how-to-protect-against-them

[9] "Whaling: how it works, and what your organisation can do about it." https://www.ncsc.gov.uk/guidance/whaling-how-it-works-and-what-your-organisation-can-do-about-it

[10] "What Is Smishing? Examples, Protection & More | Proofpoint US," *Proofpoint*, Mar. 27, 2023. https://www.proofpoint.com/us/threat-reference/smishing

[11] Helixstorm, "12 Types of Phishing Attacks to Watch Out For," *Helixstorm*, Feb. 2021, [Online]. Available: https://www.helixstorm.com/blog/x-types-of-phishing-attacks-to-watch-out-for/

[12] "What Is Clone Phishing? - Definition, Examples & More | Proofpoint US," *Proofpoint*, Mar. 27, 2023. https://www.proofpoint.com/us/threat-reference/clone-phishing

[13] "What is Vishing? Definition & Protection | Proofpoint US," *Proofpoint*, Apr. 06, 2023. https://www.proofpoint.com/us/threat-reference/vishing

[14] "Pharming - What is it and how to prevent it? | Malwarebytes," *Malwarebytes*. https://www.malwarebytes.com/pharming

[15] "Yahoo is part of the Yahoo family of brands." https://finance.yahoo.com/news/mimecast-angler-phishing-know-relatively-000500281.html#:~:text=Angler%20phishing%20is%20an%20online, media%20platforms%20to%20target%20victims.

[16] M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989