**National College of Computer Studies**

Paknajol, Kathmandu

**Research Paper:**

**Phishing Attack**

**Submitted By:**

Niraj Maharjan

Programme: Bsc CSIT 1st Semester

Roll: 15

Email: maharjanniraj87@gmail.com

**Submitted To:**

Mr. Dadhi Ram Ghimire

Lecturer (TU)

**ABSTRACT**

Phishing attacks are the practice of sending fraudulent communications that appear to come from a reputable source. Attacks can facilitate access to your online accounts and personal data, obtain permissions to modify and compromise connected systems. Phishing is a type of cyber-attack that everyone should learn about in order to protect themselves and ensure email security throughout an organization.

A phishing attack starts with a fraudulent message, which can be transmitted via email or chat applications. Even using SMS conversations to impersonate legitimate sources is known as smishing, which is a specific category of phishing attacks. Irrespective of the manner of transmission, the message targets the victim in a way that coaxes them to open a malicious link and provide critical information on the requisite website. More often than not, the websites are designed to look as authentic as possible. Once the victims submit information using the link, be it a password or credit card details, the data is sent to the hacker who designed the email and the fake website, giving him complete control over the account whose password was just provided. Often carried out in campaigns where an identical phishing mail is sent to thousands of users, the rate of success is relatively low but never zero.

The report comprises of the detailed information regarding the phishing attack, its types and history, statistics, prevention measures and what are the steps to be taken by the victim.

Table of Contents

[1. Introduction 1](#_Toc108356984)

[1.1. What is Phishing? 1](#_Toc108356985)

[1.2. Etymology 1](#_Toc108356986)

[1.3. History of Phishing 2](#_Toc108356987)

[1.4. Where it happens? 2](#_Toc108356988)

[2. Types of phishing attacks 3](#_Toc108356989)

[Spear Phishing 3](#_Toc108356990)

[Email Phishing 3](#_Toc108356991)

[Whaling 4](#_Toc108356992)

[Smishing and vishing 4](#_Toc108356993)

[Angler Phishing 5](#_Toc108356994)

[3. What are the signs of phishing? 5](#_Toc108356995)

[4. Most targeted industries 6](#_Toc108356996)

[5. Most impersonated brands 6](#_Toc108356997)

[6. Phishing Kit 6](#_Toc108356998)

[7. Phishing Statistics 7](#_Toc108356999)

[8. Phishing protection measures for organizations 8](#_Toc108357000)

[8.1 Employee awareness training 8](#_Toc108357001)

[8.2 Deploy proactive phishing tools 8](#_Toc108357002)

[8.3 Limit user access to high value systems and data 8](#_Toc108357003)

[9. Prevention measures for individuals 9](#_Toc108357004)

[10. What to Do If You’ve Fallen Victim 9](#_Toc108357005)

[11. References 10](#_Toc108357006)

Table of Figures

[Figure 1: Phishing 1](file:///C:\Users\nicolson's%20PC\Desktop\Term_paper.docx#_Toc108357021)

[Figure 2: Spear Phishing 3](file:///C:\Users\nicolson's%20PC\Desktop\Term_paper.docx#_Toc108357022)

[Figure 3 : Smishing 4](file:///C:\Users\nicolson's%20PC\Desktop\Term_paper.docx#_Toc108357023)

[Figure 4: phishing kit 6](file:///C:\Users\nicolson's%20PC\Desktop\Term_paper.docx#_Toc108357024)

[Figure 5: % of phishing hosted on HTTPS 7](file:///C:\Users\nicolson's%20PC\Desktop\Term_paper.docx#_Toc108357025)

# Introduction

## What is Phishing?

Phishing is a cyber attack whose aim is to obtain the sensitive or personal information like username, password, bank details etc using fake website, email, message etc which looks original. It is a type of cyber security attack in which target or targets are contacted by telephone, email, or text message by someone pretending to be a trusted person or entity. It lures the individual into performing actions like installing a malicious file or clicking a malicious link. Phishing is a general term used to describe attempts to manipulate or trick computer users. Social engineering attacks, like phishing, are often combined with other threats, such as malware, code injection, and network attacks.

## 1.2. Etymology

The term “phishing” came about in the mid-1990s by hackers stealing American Online accounts and passwords. By analogy with the sport of angling, these Internet scammers were using e-mail lures, setting out hooks to "fish" for passwords and financial data from the "sea" of Internet users. There is a good reason for the use of “ph.” in place of the “f”. Some of the earliest hackers were known as phreaks. Phreaking refers to the experimenting and study of telecommunication systems. Phishing emails try to lure people in and get them to take the bait. And, once they are hooked, both the user and the organization are in trouble [5].



Figure 1: Phishing

## 1.3. History of Phishing

According to Internet records, the first time that the term “phishing” was used and recorded was on January 2, 1996. Back then American Online (AOL) was the number one provider of internet access. Each day millions of people logged on to the service and its popularity made it a neutral choice for those who had less than pure motives. It was this community which made the first move to conduct phishing attacks.

In the beginning phishers conducted attacks by stealing users’ passwords and using algorithms to generate randomized credit card numbers. While fortunate hits have been few and a long way between, they struck the jackpot regularly sufficient to reason numerous damages. These random credit card numbers were then used to create AOL account, further spamming other users and for a wide range of other things. These processes were simplified the special programs like AOHell. Later AOL was forced to include the warning messages on its email and instant messenger clients to prevent users from providing sensitive information through such methods [4].

## 1.4. Where it happens?

In your personal life:

* Money stolen from bank accounts
* Lost access to the personal data like photos, videos
* Tax returns filed in a person’s name
* Fraudulent charges on credit cards
* Fake social media posts made in a person’s accounts

At Work:

* Loss of corporate funds and company value
* Access to confidential files and system by outsiders
* Files become inaccessible
* Exposed personal information of customers and co-workers
* Financial fines from compliance violations

# Types of phishing attacks

## Spear Phishing

It is a type of phishing that involves targeting a specific individual within an organization. In this phishing, attacker has some or all of the following information regarding the victim [2]:

* Name
* Place of employment
* Email address
* Job title
* Trusted colleagues, family members, or other contacts, and samples of their writing
* Specific information about their job role

Example:

An attacker tried to target an employee of NTL World, which is a part of the Virgin Media company, using spear phishing. The attacker claimed that the victim needed to sign a new employee handbook. This was designed to lure them into clicking a link where they would have been asked to submit private information [3].

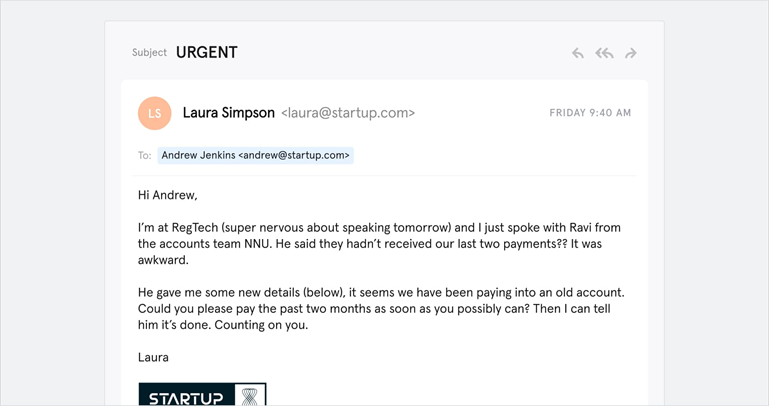


Figure 2: Spear Phishing

## Email Phishing

Most phishing attacks are sent by emails. The attacker registers a fake domain names that mimic genuine organizations and send thousands of generic requests. The fake domain often includes character substitution, use of sub-domains and use of trusted organization’s name as the email username [2].

Example:

Hackers used LinkedIn to grab contact information from employees at Sony and targeted them with an email phishing campaign. They got away with over 100 terabytes of data [3].

## Whaling

A whaling attack is a phishing attack that targets a senior executive or other highly privileged roles. Although the ultimate goal of whaling is same as the other types of phishing, the technique is often crafty. Due to their highly targeted nature, whaling attacks are often more difficult to detect and prevent than standard phishing attacks. They leverage highly personalized messages using information they discover in their research about the victim. For example, whaling attackers commonly use bogus tax returns to discover sensitive data about the victim, and use it to craft their attack [2].

Example:

A founder of Levitas, an Australian hedge fund was the target of a whaling attack that led the individual to a fake connection using a fraudulent Zoom link. After following the link, they had malware installed on their system, and the company lost $800.000 [3].

## Smishing and vishing

Smishing and vishing are two types of fraud that use SMS (smishing) and voice (vishing) to trick people into giving up money or personal information.

Smishing often contain a link encouraging the users to take urgent actions, for example:

* Claiming a prize
* Claiming a tax refund
* Confirming and rescheduling a delivery
* Locking their online banking account

In vishing attack, the victim will receive a phone call or voicemail from a scammer, pretending to be a trusted person. A vishing attack often starts with a automated text message. Attackers use a wide range of attacking techniques, including:

* Faking caller ID, so it appears that the call is coming from a trusted number
* Utilizing “war dialers” to call large numbers of people
* Using synthetic speech and automated call processes

Example:

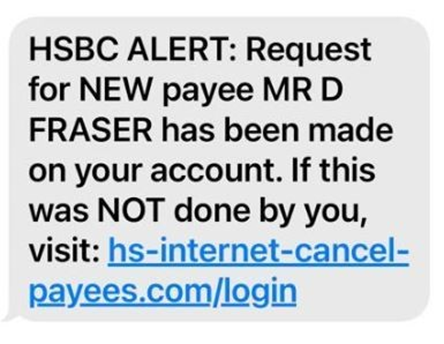
Hackers pretended to be from American Express and sent text messages to their victims telling them they needed to tend to their accounts. The message said it was urgent, and if the victim clicked, they would be taken to a fake site where they would enter their personal information [3].

Figure 3 : Smishing

## Angler Phishing

These attacks use fake social media accounts belonging to well-known organizations. They use the same profile picture as the real company account. Attackers take advantage of consumers’ tendency to make complaints and request assistance from brands using social media channels. During their interaction, the attacker might request the customer to provide personal details or click a link to resolve the issue. Once the victim clicks the link, they’re redirected to a fake site asking them to input their personal details [2].

Example:

Hackers pretended to represent Domino's Pizza on Twitter, fielding the concerns and comments of customers. Once they engaged with a customer, they would use their situation to try to get their personal information—using the guise of trying to get them a refund or a reward [3].

# What are the signs of phishing?

* Threats or sense of urgency

Emails, calls or text messages that threaten negative consequences should be treated doubtful. Also, attackers often use urgency to demand immediate action in a sense by reading a mail in hurry, they will not thoroughly audit the content and will not discover the inconsistencies.

* Message styles

An immediate indication of phishing is that a message is written with inappropriate language or tone. Recipients of the message should check for anything else that could indicate a phishing message. Other signs of phishing emails are misspellings and grammatical misuse. Most companies have set up spell checking in their email clients for outgoing emails. Therefore, emails with spelling or grammatical errors should raise suspicion, as they may not originate from the claimed source.

* Inconsistencies in web addresses

The easy way to identify the phishing attack is to look out for mismatched link, email addresses and domain names. Recipients should always hover over a link in an email before clicking it, to see the actual link destination. If the email is believed to be sent by Bank of America, but the domain of the email address does not contain “bankofamerica.com”, that is a sign of a phishing email.

* Request for Credentials, Payment Information or Other Personal Details

In most of the phishing attacks, attackers create a fake login pages that appear to be original in order to fetch the personal details of the users. The fake login page typically has a login box or a request for financial account information.

# Most targeted industries

* Online stores (ecommerce).
* Social media.
* Banks and other financial institutes.
* Payment systems (merchant card processors).
* IT companies.
* Telecommunication companies.
* Delivery companies

# Most impersonated brands

* Google
* Microsoft
* Amazon
* Chase
* Wells Fargo
* Bank of America
* Apple
* LinkedIn
* FedEx
* DHL

# Phishing Kit

A collection of various software utilities like HTML, code and images that allows cybercriminals to launch a phishing attack is called phishing kit. It enables people with less or no knowledge of phishing create phishing pages and attack larger users. Hackers use phishing kits to develop the website that trick people into thinking that they are on a official site. They are shortcuts to launch a phishing attack by cloning a well-known organization by mirroring a official website. Phishing kit also includes email templates, graphics and sample scripts.

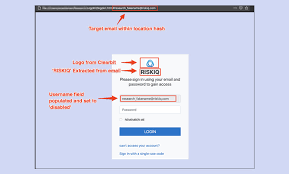


Figure 4: phishing kit

# Phishing Statistics

Phishing is a huge threat and growing more widespread every year. According to the report, the most common type of branded phishing attacks is email phishing, accounting for 44% of attacks. The brands most commonly used by attackers in fake phishing messages were Microsoft, DHL, and Apple.

According to the Tessian research, employees receive an average of 14 malicious emails per year. There’s an uneven distribution in phishing attacks throughout the year. Cisco found that phishing tends to peak around holiday times, finding the phishing attacks soared by 52% in December. In 2021, 83% of the organizations reported experiencing phishing attacks. In 2022, six billion attacks are expected to occur. One in 99 emails is a phishing email. It’s determined that 3.4 billion fraudulent emails are sent daily. 2021 is the costliest year for data breaches in 17 years. The total average cost of a data breach was $4.24 million in 2021, up from $3.86 million previous year [1].

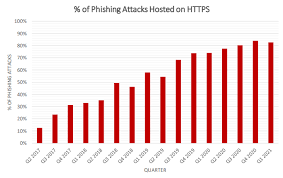


Figure 5: % of phishing hosted on HTTPS

# Phishing protection measures for organizations

## 8.1 Employee awareness training

One of the most effective ways to prevent phishing attacks is to conduct regular cybersecurity awareness training for all employees in your organization. Phishing awareness training will help your employees recognize the various tactics that attackers employ to deceive them into supplying sensitive information. It will also ensure they know what to watch out for and let them understand the importance of reporting such situations early enough. One can also conduct the simulated phishing attack tests.

## 8.2 Deploy proactive phishing tools

The best way to avoid phishing attacks is to prevent phishing attacks. One way to do this is by deploying “ahead-of-threat” attack prevention tools. This proactive approach helps organizations determine malicious domains before scammers will use them during a phishing attack and before the threat becomes visible. Another advantage is that IT leaders in organizations can quickly realize and remedy compromised terminations with this approach and so limit the harm across the network. To more strengthen your endpoint watching capabilities and stop phishing attacks from increasing across the complete network, deploy a sturdy Endpoint Detection and Response (EDR) tool.

## 8.3 Limit user access to high value systems and data

Most phishing methods are designed to trick human operators, and privileged user accounts are attractive targets for cybercriminals. Restricting access to systems and data can help protect sensitive data from leakage. Use the principle of least privilege and only give access to users who absolutely need it.

# Prevention measures for individuals

* People should keep themselves updated with the latest phishing techniques.
* One must think twice before clicking on the suspicious mails and links.
* Install an anti-phishing toolbar provided by many popular web browsers. These toolbars run routine checks on the visited websites and compare them with the known phishing sites in their database. If a user, accidentally or otherwise, navigates to a malicious website, the toolbar alerts them.
* Following things should be checked before supplying vital information to the websites:

1. Ensure that the site’s URL begins with https
2. Look for a closed lock icon near the address bar
3. Check the site’s security certificate

* Internet users must deploy firewalls to keep their systems inaccessible for phishers and attackers.
* Browsers release security patches from time to time. One must download and install the security update, advisably as soon as it is available.
* One must avoid sharing personal or financially sensitive information over the internet.

# What to Do If You’ve Fallen Victim

After the user sent the information to attackers, it is likely to be disclosed to other scammers. Victim will probably receive vishing and smishing messages. Always stay alert for suspicious messages asking for personal details.

Before planning the next step, the first thing you need to do after falling victim to a phishing attack is to take a few deep breaths to calm down and clear your mind. And take the following measures:

* Disconnect device from the internet right away to reduce the risk of the malware spreading to other devices on the network.
* Backup files in case the data gets erased in the recovery process of the phishing attack. The important thing is to protect sensitive information and documents as well as precious files.
* Change the login credentials to ensure the assailant does not inflict further damage.
* It’s a good idea to have the device fully scanned for malwares and viruses.
* Report the incident to the Federal Trade Commission (FTC) for a step-by-step recovery plan.

# References

|  |  |
| --- | --- |
| [1] | K. Hanko, "Startling Phishing Statistics to Be Aware of in 2022," 12 04 2022. [Online]. Available: https://clario.co/blog/phishing-statistics/. |
| [2] | L. Irwin, "The 5 most common types of phishing attack," 24 03 2022. [Online]. Available: https://www.itgovernance.eu/blog/en/the-5-most-common-types-of-phishing-attack. |
| [3] | "19 Types of Phishing Attacks," [Online]. Available: https://www.fortinet.com/resources/cyberglossary/types-of-phishing-attacks. |
| [4] | "History of Phishing," [Online]. Available: https://www.phishing.org/history-of-phishing. |
| [5] | "What is Phishing?," [Online]. Available: https://www.proofpoint.com/us/threat-reference/phishing. |