


# Phishing Awareness Program



---

# **Introduction To Phishing Attacks**

**Presented by**

**January, Favour Chioma**

**CodeAlpha Internship Program**

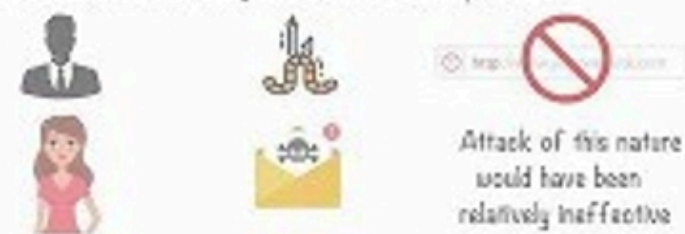
This is a classic example of a phishing attack



# What is Phishing?



It's based on the word fishing, which works on the concept of baits



Smishing

Which is a specific category of phishing

<http://www.yourwebsite.com>



When a hacker launches a phishing attack, **he or she is trying to trick you into believing that the message is from a legitimate source** so that you will click a link or download an attachment.

# **Types of Phishing**

There are various types of phishing, let's explain them.

# Email Phishing

Email phishing is a type of phishing attack in which an attacker sends a fake email to its victim to obtain sensitive information.

Let's see how it works

The attacker sends an email to the victim



Attacker



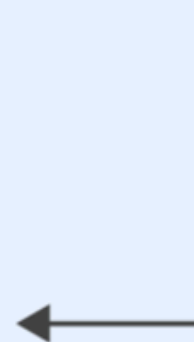
Employee



Real Website



Phishing Website



# Spear Phishing

Spear phishing is a phishing attack that targets a specific individual or an organization.

How does spear phishing works?

During spear phishing, the hacker sends a malicious SMS or Email to a specific users or organization so as to obtain sensitive information.



1

Attacker distributes e-mails with malicious attachments to targeted users



Phishing e-mail

2

Users fail to understand social engineering trick and open the malicious attachment



Targeted users

3

Target system is exploited



Compromised system

4

Malicious code/Trojan is installed on the target system



6

Data is stolen from the compromised machines



5

Malicious code/Trojan is used to gain access to additional systems on the internal network



Data

7

Data is exfiltrated to the attacker



Attacker

# How Spear Phishing Works

# Whaling

Just as spear phishing targets a specific individual or organization, whaling focuses on high-profile employees or executives.

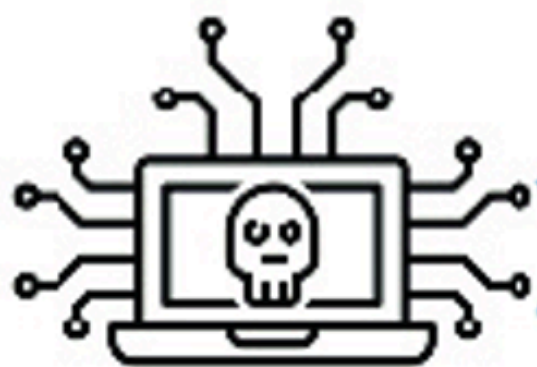
Let's see how whaling works

# INTERNET

Phishing  
attacker



Phishing  
attack



*Personalised email or  
online text message*

*Spear  
phishing*

Selected user  
group



Executives



*Whaling*

# Vishing

During vishing attack, an attacker uses voice calls or messages to obtain sensitive information.

## How Does Vishing works

An attacker poses as an executive of the victims bank or an executive of an organization in which the victim is involved with through phone calls asking for personal or sensitive information.



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

# Smishing

Smishing is a phishing attack through SMS messages.

## How Does Smishing Works

An attacker sends a fake SMS message to its victim with a clickable link so as to obtain there sensitive information when they click on the link.

# SMISHING ATTACK PHASES



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.

# How to Recognize Phishing Attempts

- Suspicious or strange email addresses.
- Urgent language ("Immediate action required!"). Eg An Email requiring to either change your account password to avoid being blocked.
- Links that don't match official websites.
- Unexpected attachments: An attachment you can't remember applying for or have no idea about it, could indicate a phishing attempt.
- Requests for sensitive or financial information.



# How To Identify a Phishing Email

Subject **You've won a \$1000 gift card!**

Too-good-to-be-true offers



Giftcardsdirect.com <g1ftcardsdirect.com to me ▾

Discrepancies between the sender's name and email address



Suspicious links

[Click here to redeem](#)

Deer customer,

Spelling or grammatical errors

You are the winner of our \$1000 gift card giveaway.

Please login below to redeem your prize in the next 24 hours.

Demands urgency

[Log in now](#)

Requests sensitive information



[digital gift card.png](#)

Suspicious attachments

# A Phishing Facebook Website

That's not Facebook's URL

The real page says "Log in" in the title. Ironically, the phishing site is more consistent than Facebook on this



Wrong year in copyright message

Different languages

# How to Protect Yourself From Phishing Attack

Always verify the sender before clicking links.

Never share personal information through email or SMS.

Use strong passwords and multi-factor authentication.

Keep your software and antivirus updated.

# Best Practices for Organizations

Conduct regular cybersecurity training for employees to enlighten them on the emerging phishing attacks from modern technology and how to avoid them.

Implement email filtering and anti-phishing software.

Simulate phishing attacks to test awareness.

Develop a clear incident response plan to take immediate action when such attack occurs.

# What to Do if You Fall for a Phishing Attack

Report the phishing incident to IT/security immediately.

Change your passwords quickly.

Monitor bank and credit card statements.

Alert others to prevent further attacks.

# Key Takeaways:

Stay alert and think critically before you click.

Phishing is becoming more sophisticated every day.

Awareness and caution are your best defense.

Final Tip:

"If something feels off, it probably is."