


Phishing Awareness Program

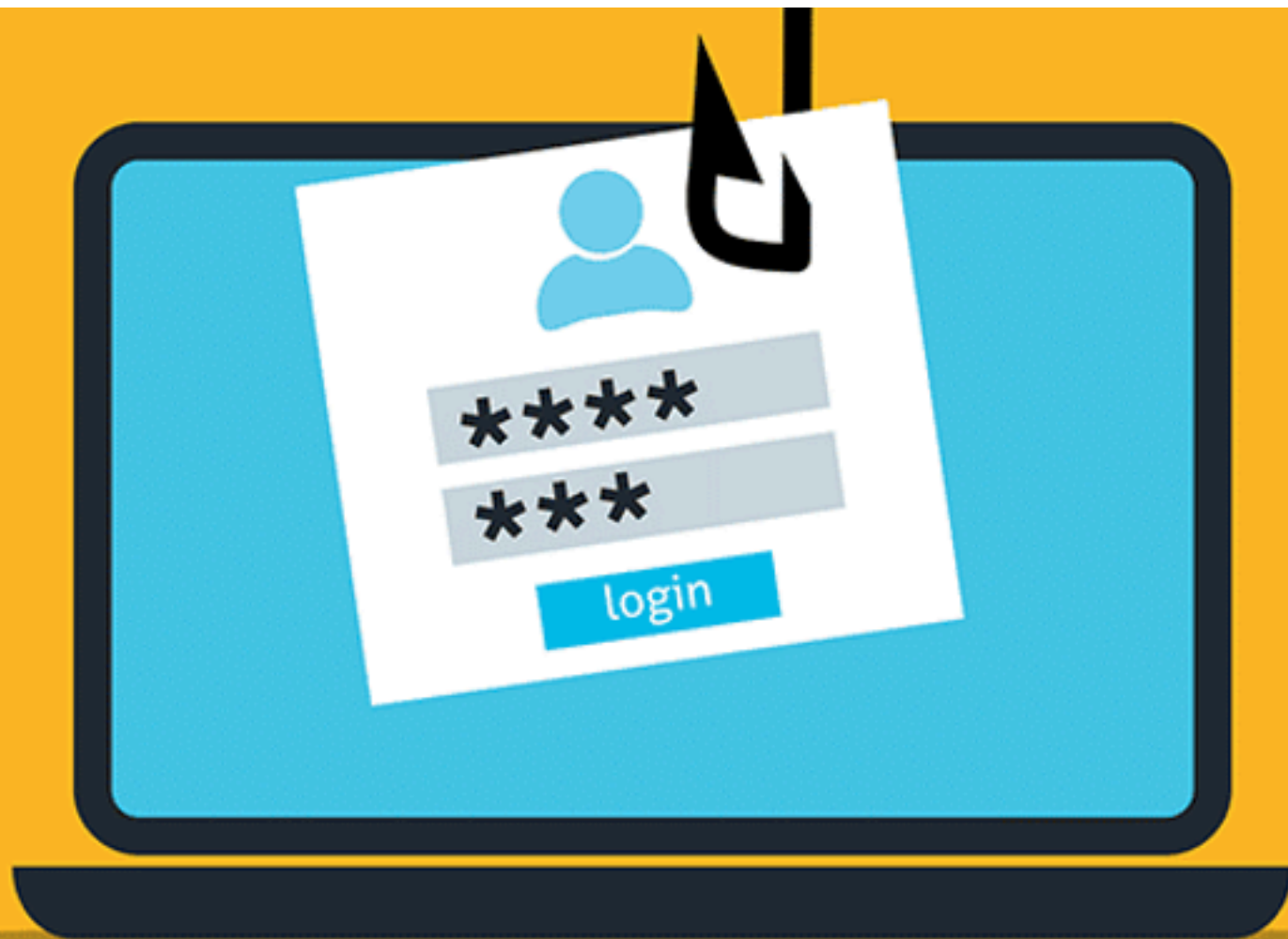


Introduction To Phishing Attacks

Presented by

January, Favour Chioma

CodeAlpha Internship Program



What is phishing?



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 Attacks

1. Email Phishing: This is a type of phishing attack in which an attacker uses a fake Email as a legitimate one so as to obtain vital information from its victim.
2. Spear Phishing: This is a personalized attacks targeting specific individuals.
3. Whaling: Whaling attacks targets high-profile executives or important employees.
4. Vishing: This is a voice phishing attack carryout via phone calls.
5. Smishing: This is a phishing carryout through SMS messages.

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."