Phishing Awareness

Think Before You Click!

What Is Phishing?

Phishing is the most common form of social engineering for stealing an individual’s personal information like IDs or passwords, or for installing malware which can be used for various purposes including ransomware attacks.

Why Is Phishing a Problem?

Phishing is a significant problem because it is easy, cheap, and effective for cybercriminals to use. Phishing tactics, particularly email, require minimal cost and effort, making them widespread cyber-attacks.

94%

Of malware on computers found their way there via phishing email.

67,5%

Of individuals that click on a phishing link are likely to enter their credentials on a phishing website.

2 Million+

Phishing sites have been found and registered as malicious by Google as of January 2021.

How Does Phishing Work?

Phishing emails often appear to be from legitimate sources like banks, social media platforms, or even friends and family.

Phishers frequently use tactics like fear, curiosity, a sense of urgency, and greed to compel recipients to open attachments or click on links.

The emails contain malicious links or attachments that, when clicked, can steal your information or infect your device with malware.

Phishing Techniques

01 **Malicious Web Links**

02 **Malicious Attachments**

03 **Fraudulent Data Entry Forms**

Different Types of Phishing Attacks

Email Phishing

An email sent with the intention of deceiving you to act, such as updating a password or clicking on an attachment. **96%** of all phishing attacks come via email.

Smishing

Phishing via text. The fraudulent text may appear to come from a reputable business but is designed to trick you into revealing personal information.

Vishing

Also known as voice phishing occurs via phone. It is a fraudulent phone call or voice message designed to obtain sensitive information such as login credentials

Angler Phishing

Targets social media users. Bad actors will direct message disgruntled customers, pretending to be customer service agents, to obtain personal information or other account credentials.

Different Types of Phishing Attacks

Spear Phishing

Targets specific individuals instead of a wide group of people. That way, the attackers can customize their communications and appear more authentic. It is often the first step used to penetrate a company's defenses and carry out a targeted attack.

Whaling

When attackers go after a "big fish" like a CEO, business executives, and high-net-worth individuals. The account credentials of these high-value targets typically provide a gateway to more information and potentially money.

Evil Twin Hotspots

Fraudulent Wi-Fi access points designed to trick users to connect to them so they can steal sensitive information or redirect links to malicious sites.

Pop-up Phishing

Fraudulent messages that “pop up” on otherwise legitimate websites that have been infected with malicious code and entice you to click on them to corrupt your device or data.

Evil Twin Phishing

Click with caution!

Phishing tips to protect you

- ⚠ Avoid unknown senders. Check names and email addresses before responding.
- ⚠ Don’t trust links or attachments in unsolicited emails.
- ⚠ Be suspicious of emails marked “urgent.”
- ⚠ Beware of messages with mistakes in spelling or grammar.

Phishing tips to protect you

- Don't be lured by “deals”. They are usually too good to be true.
- Be wary of generic greetings, such as dear sir or ma’am.
- Never give out personal or financial information based on an email request.
- When receiving email from known institutions (government, banks, your doctor), go directly to the source instead of clicking on links in the email.

Thanks!

Do you have any questions?
mariettesamir7@gmail.com

in/mariettesamir

CodeAlpha Remote Internship