Phishing Attacks: Don't Get Hooked!

Learn to recognize and avoid phishing emails, websites, and social engineering attacks.

CodeAlpha

...so what are we learning today???

What is Phishing?

How Phishing Works

Types of Phishing

Phising Tactics

Identifying Phising Attepts

Protecting Yourself

What if you are already Phished?

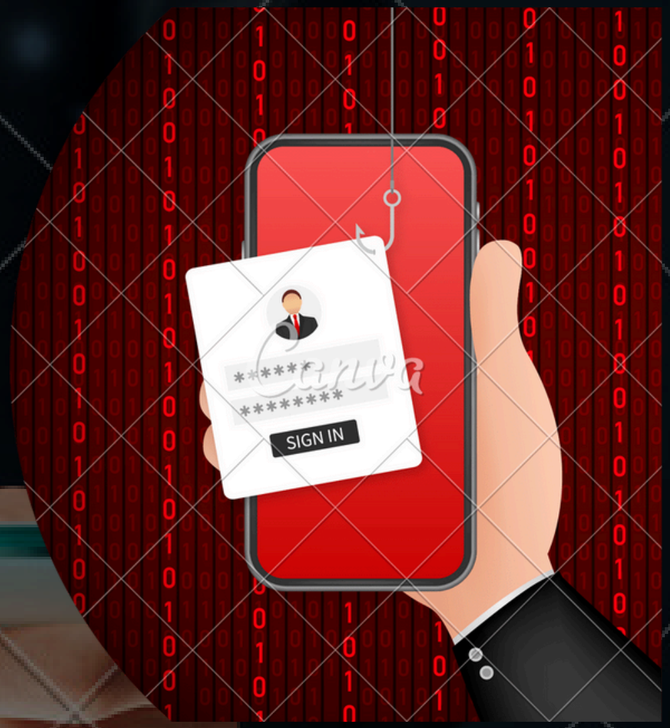
...fun facts

What is Phishing?

Phishing is a fraudulent attempt to obtain sensitive information such as usernames, passwords, and credit card details by disguising as a trustworthy entity in an electronic communication.

How Phishing Works

- Phisher sends a deceptive email or message.
- Victim clicks on a malicious link or opens an attachment.
- Malicious software is installed or personal information is stolen.



Types of Phishing

- **Email Phishing:** Common examples, such as fake bank emails, fake lottery wins, etc.
- **Smishing:** Phishing via SMS
- **Vishing:** Phishing via voice call

Phishing Tactics

- **Urgency:** Creating a sense of urgency to prompt immediate action.
- **Fear:** Using threats or scare tactics to manipulate victims.
- **Greed:** Offering unrealistic rewards or prizes.
- **Curiosity:** Arousing curiosity with unexpected or intriguing messages.

Identifying Phishing Attepts

- Check the sender's email address: Look for typos or suspicious domains.
- Hover over links before clicking: Verify the actual link destination.
- Be wary of urgent requests for personal information: Legitimate companies won't ask for sensitive information via email.
- Check for spelling and grammar errors: Phishing emails often contain mistakes.

Protecting Yourself

- Strong passwords: Use complex and unique passwords for different accounts.
- Enable two-factor authentication: Add an extra layer of security.
- Keep software updated: Install security patches to protect against vulnerabilities.
- Be cautious with social media: Avoid sharing personal information online.
- Educate yourself: Stay informed about the latest phishing scams.

Already Phished???

- Change passwords immediately.
- Monitor your accounts for suspicious activity.
- Report the phishing attempt to your email provider or the relevant authorities.

#FUNFACTS

- Phishing is big business: Cybercriminals make billions of dollars annually from phishing scams.
- Speed is key: The average time it takes for a user to fall for a phishing email is less than 60 seconds.
- Social media is a goldmine: Many phishing attacks start with information gathered from social media profiles.
- Phishing isn't just email: It can also happen through text messages (smishing), phone calls (vishing), and even social media platforms.
- Even the experts get fooled: Studies show that a significant percentage of IT professionals fall for phishing attempts.
- Phishing is constantly evolving: Cybercriminals are always coming up with new and creative ways to trick people.

THE END

Thank YOU