Phishing Awareness

Created by

YMUKUNDWA DELPHINE

What is Phishing?

Definition of Phishing

Phishing is a type of cybercrime where attackers disguise themselves as trustworthy entities to deceive individuals into revealing sensitive information, such as passwords and financial data

Common Phishing Methods

Common phishing methods include deceptive emails, fake websites, and messages that prompt users to click on malicious links or download harmful attachments.

Spoofing and

Phishing often involves spoofing legitimate organizations or individuals, creating a false sense of trust to manipulate victims into taking actions that benefit the attackers.

Types of phishing attacks

Spear phishing

Spear phishing targets specific individuals instead of a wide group of people. Attackers often research their victims on social media and other sites. That way, they can customize their communications and appear more authentic. Spear phishing is often the first step used to penetrate a company's defenses and carry out a targeted attack.

Pharming

Similar to phishing, pharming sends users to a fraudulent website that appears to be legitimate. However, in this case, victims do not even have to click a malicious link to be taken to the bogus site. Attackers can infect either the user's computer or the website's DNS server and redirect the user to a fake site even if the correct URL is typed in.

Deceptive phishing

Deceptive phishing is the most common type of phishing. In this case, an attacker attempts to obtain confidential information from the victims. Attackers use the information to steal money or to launch other attacks. A fake email from a bank asking you to click a link and verify your account details is an example of deceptive phishing.

- **Whaling** will be shown in the example on the next later slide

Common Phishing Techniques

Social Engineering Tactics

Social engineering tactics manipulate human behavior to trick individuals into divulging confidential information. Attackers exploit factors like trust, urgency, and curiosity to deceive users into compromising security.

Email Spoofing

Email spoofing is a technique used in phishing where attackers falsify the sender's address to make it appear as if the email is from a trusted source. This can deceive recipients into believing the email is legitimate and trick them into taking action.

Deceptive URLs

Phishing attacks often use deceptive URLs that resemble legitimate websites. These URLs may redirect users to malicious websites designed to steal sensitive information such as login credentials or financial details.

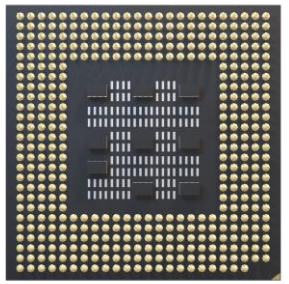
Phishing Examples

Real-Life Phishing Scenarios

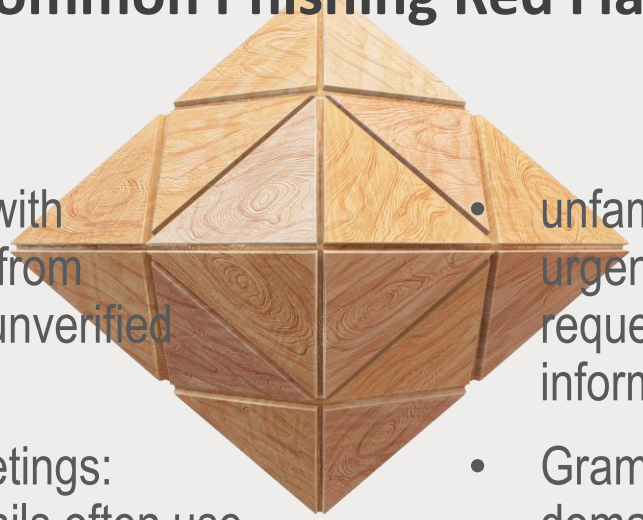
FACC, an Austrian manufacturer of aerospace parts, also lost a significant amount of money to a BEC scam. In 2016, the organization announced the attack and revealed that a phisher posing as the company's CEO instructed an employee in the accounting department to send $61 million to an attacker-controlled bank account.

This case was unusual in that the organization chose to fire and take legal action against its CEO and CFO. The company sought $11 million in damages from the two executives due to their failure to properly implement security controls and internal supervision that could have prevented the attack. This lawsuit demonstrated the personal risk to organization's executives of not performing "due diligence" with regard to cybersecurity.

Signs of a Phishing Attempt



Common Phishing Red Flags



- Be cautious with attachments from unknown or unverified sources.
- Generic Greetings: Phishing emails often use generic greetings like "Dear Customer“ instead of your name
- unfamiliar senders, urgent language, requests for personal information,
- Grammatical error in the domain name , suspicious link

Photos provided by Unsplash

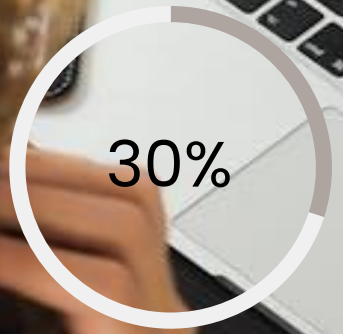
Protecting Against Phishing

Tip	Description
Use Multi-Factor Authentication	Add an extra layer of security by requiring a second form of verification, such as a code sent to your phone.
Keep Software Updated	Regularly update software to patch vulnerabilities that cybercriminals exploit for phishing attacks.
Employee Training	Educate staff on phishing awareness, how to spot suspicious emails, and the importance of data protection.
Monitor Account Activity	Regularly review account activity for unusual behavior or unauthorized access attempts.

Impact of Phishing

Financial Loss

Victims of phishing attacks can suffer significant financial losses through unauthorized transactions or identity theft.



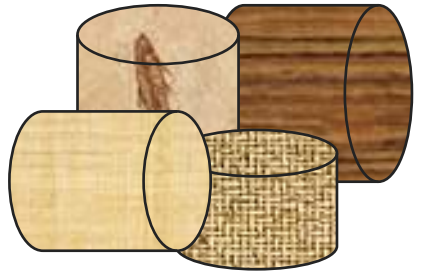
Data Breach

Phishing attacks can lead to data breaches, compromising sensitive information, and causing reputational damage to individuals and organizations.

Identity Theft

Identity theft is a common consequence of phishing attacks, where cybercriminals use stolen information for fraudulent activities.

Phishing Prevention Strategies



Email Security Practices

Implement email security protocols like SPF, DKIM, and DMARC to verify email authenticity and reduce the risk of domain spoofing.

Incident Response Plan

Develop a comprehensive incident response plan to mitigate the impact of a successful phishing attack, including containment, investigation, and recovery procedures.

User education

One way to protect your organisation from phishing is user education. Education should involve all employees. High-level executives are often a target. Teach them how to recognize a phishing email. Simulation exercises are also key for assessing how your employees react to a staged phishing attack.

Concluding remarks

- *Stay vigilant, always verify, and report suspicious activities.*