CYBER SECURITY

Topic: Phishing Awareness Training

Presented by: Sawan S Khadsan

PHISHING ATTACKS: DON'T GET HOOKED!

Welcome, everyone!

We are at the forefront of defense against constantly evolving threats. Today, we will focus on phishing attacks, a common cybercrime that aims to steal valuable information. We will prepare to identify and prevent these sneaky attempts, keeping our sensitive data safe and protecting our useful information.

WHAT IS PHISHING?

- Phishing is a type of cybercrime that involves using deceptive emails, websites, or social engineering techniques to illegally obtain personal information.
- Cybercriminals pretend to be legitimate entities, such as banks, social media platforms, or trusted contacts, to trick individuals and organizations into revealing sensitive information.
- The stolen data is then used for malicious activities like identity theft, financial fraud, or data breaches.

Phishing is like a fisherman using bait to trick victims into revealing personal information. Understanding how it works is crucial for better protection.

HOW PHISHING WORKS : THE PHISHING EMAIL

Phishing emails often display the following traits:
- Communicate a sense of urgency or threat (e.g., "Your account will be suspended!")
- Contain grammatical errors and typos
- Use generic greetings ("Dear Customer")
- Request immediate action
- Include links to fake websites that mimic legitimate ones

Phishing emails are designed to make you feel panicked or rushed. They may contain spelling or grammar mistakes, typos, or generic greetings to look less professional. They often push you to respond fast by saying your account is in danger or offering something that seems too good to be true. Be careful with emails that make you feel rushed or ask you to click on dubious links.

HOW PHISHING WORKS : THE PHISHING WEBSITE

Please keep in mind the following:

1. Check the website URL for inconsistencies. Legitimate URLs should match the company website.
2. Look for spelling or grammar errors on the website.
3. Legitimate websites have a security certificate, which appears as a padlock icon in the address bar.
4. Be careful with websites that pressure you to download files or provide personal information.

Be cautious of fake websites, check the URL for inconsistencies, watch for typos or grammatical errors, look for a padlock icon for security, and avoid entering personal information on unverified websites.

BEYOND EMAILS: SOCIAL ENGINEERING TACTICS

- Social engineering utilizes human psychology to manipulate individuals.
- Attackers may impersonate trusted sources (e.g., IT support, colleagues), offer enticing rewards or incentives, and instill fear or urgency.

Remember this: Social engineering manipulates our emotions and our wish to help or gain something valuable. Attackers may pretend to be someone we trust, like IT support or a colleague, to earn our trust. They might offer appealing rewards or incentives to get us to click on a link or divulge personal information. They may also use fear or urgency to pressure us into acting without thinking critically.

HOW TO AVOID PHISHING ATTACKS - BE VIGILANT!

- Beware of clicking on links or attachments in suspicious emails.
- Verify the sender's email address and avoid entering personal information on unverified websites.
- Be cautious of unsolicited calls, messages, or pop-ups creating a sense of urgency or offering unbelievable rewards.

it's important to be extra cautious. Avoid clicking on links or attachments in suspicious emails. Verify the sender's email addresses before entering personal information or navigating to a website. Be wary of unsolicited messages and pop-ups, especially those creating a sense of urgency or offering unbelievable rewards. If it seems too good to be true, it probably is.

WHEN IN DOUBT, VERIFY AND REPORT!

- If you receive a suspicious email, don't click on anything.
- Forward the email to your organization's IT security team for investigation.
- Most email providers offer a way to report phishing attempts. Utilize this functionality to help protect your organization and others.

"If you receive a suspicious email, do not click on any links or attachments. The safest action is to delete the email. If you are unsure about the email, forward it to your organization's IT security team for investigation. Most email providers have a way to report phishing attempts directly on their platform. Use this feature to protect your organization and others from similar attacks. Reporting phishing attempts helps to identify and stop malicious campaigns before they can cause widespread damage."

EDUCATE YOUR TEAM: BUILDING A CULTURE OF SECURITY AWARENESS

- Regularly conduct security awareness training for your team.
- Educate employees on how to identify phishing attempts.
- Emphasize the importance of reporting suspicious emails and social engineering tactics.
- Encourage a culture of open communication where employees feel comfortable raising security concerns.

Building a strong security culture is crucial in defending against phishing attacks. Regularly train your team to identify phishing attempts and report suspicious emails and social engineering tactics. Encourage open communication for a more secure environment.

STAY INFORMED, STAY SECURE!

- Phishing attacks are constantly evolving. Stay informed about the latest phishing tactics by following reputable cybersecurity resources.
- There is no foolproof solution to phishing, but by following these best practices and remaining vigilant, we can significantly reduce the risk of falling victim to a phishing attack.

The field of cybersecurity is in a constant state of flux, with phishing tactics evolving continuously. It is crucial to stay abreast of the latest phishing scams and trends by following reputable cybersecurity resources. Although there is no fail-safe solution to phishing, adhering to the best practices outlined in this presentation and maintaining a vigilant stance can substantially mitigate the risk of falling prey to a phishing attack. It is essential to remember that exercising caution can avert a significant security breach within your organization. We appreciate your attention to this matter. Thank you.

THANK YOU FOR YOUR ATTENTION