GUARDING AGAINST DECEPTIVE TACTICS:

PHISHING AWARENESS TRAINING

NAME :NITHIAPRABA.B

INTRODUCTION TO PHISHING:

Welcome to **Phishing Awareness Training**. This presentation will help you to gain knowledge and identify and prevent Phishing Attacks. Stay vigilant and protect your organization's data

PHISHING ATTACKS:

Phishing is a form of social engineering that involves communication via email, phone or text requesting a user take action, such as navigating to a fake website. In both phishing and social engineering attacks, the collected information is used in order to gain unauthorized access to protected accounts or data.

HOW DOES PHISHING WORK?

Phishing starts with a fraudulent email or other communication that is designed to lure a victim. The message is made to look as though it comes from a trusted sender. If it fools the victim, he or she is coaxed into providing confidential information, often on a scam website. Sometimes malware is also downloaded onto the target's computer.

DANGERS OF PHISHING ATTACKS

Sometimes attackers are satisfied with getting a victim's credit card information or other personal data for financial gain. Other times, phishing emails are sent to obtain employee login information or other details for use in an advanced attack against a specific company. Cybercrime attacks such as advanced persistent threats (APTs) and ransomware often start with phishing.

COMMON PHISHING TACTICS

Phishing is a cyberattack where attackers trick individuals into providing sensitive information. Common tactics include:

- Email Phishing
- Spear Phishing:

Email Phishing: Fake emails from seemingly legitimate sources urging recipients to click links or download attachments

Spear Phishing: Targeted attacks with customized messages using personal information about the victim to appear legitimate.

Awareness of these tactics can help individuals avoid falling victim to such scams.

SPOTTING PHISHING EMAILS

Suspicious links or unexpected attachments - If you suspect that an email message, or a message in Teams is a scam, don't open any links or attachments that you see. Instead, hover your mouse over, but don't click the link. Look at the address that pops up when you hover over the link.

PROTECTING PERSONAL INFORMATION

Never provide personal financial information, including your Social Security number, account numbers or passwords, over the phone or the Internet if you did not initiate the contact.

REPORTING SUSPICIOUS ACTIVITY

Choose the option Security risk - Spam, phishing, malicious content is selected, and then select Report. Click the Report button

TRAINING RECAP

Congratulations on completing the **Phishing Awareness Training**. Remember to stay alert, be cautious of deceptive tactics and report any suspious activity. Together we strengthen our defence against phishing attacks.

CONCLUSION

Thank you for participating in the **Phishing Awareness Training** . By staying informed and vigilant, we can collectively mitigate the risks of phishing attacks and protect our organization's sensitive information. Stay safe and secure...!