Members BSIT 4-C

Macky Mar Layao
Kent Jun Gil
Mhel Jhon Leones
Alexandra May Pis-ing

This infographic entitled " CYBER SECURITY AWARENESS" recognizes and preventing phishing cyber threats are becoming increasingly sophisticated, with phishing attacks being one of the most common and dangerous forms of cybercrime. Phishing refers to fraudulent attempts by cybercriminals to deceive individuals into revealing sensitive information, such as passwords, credit card numbers, or personal identification details. This infographic aims to raise awareness about phishing attacks, helping you recognize the warning signs and providing tips on how to prevent falling victim to these malicious tactics. Stay informed, stay secure, and protect yourself from potential harm in the digital world.

Phishing Awareness

Phishing is a common scam where hackers trick you into sharing personal information. Learn how to spot and avoid these scams to protect yourself

COMMON PHISHING SIGNS

Urgent Requests: These often claim that your account will be closed if you don't act immediately. Such messages are designed to pressure you into responding quickly without thinking

Too Good To Be True: Phishing scams often offer free money or prizes to tempt you. These offers are designed to trick you into sharing personal information or clicking on harmful links.

Suspicious Links: Be careful with links in emails or messages. Hover over them to check if the web address looks correct if it doesn't match the sender or seems strange, avoid clicking on it.

Actions to Take if You're Caught in a Social Media Phishing Scam

Change Your Passwords: Immediately change the passwords for your social media accounts and any linked accounts, like email or bank accounts.

Enable Two-Factor Authentication: Set up two-factor authentication on your accounts for added security.

Report the Incident: Report the phishing attempt to the social media platform so they can take action against the attacker.

Check for Suspicious Activity: Look through your account for any changes or posts you didn't make and delete them.

Warn Others: Inform your friends or followers about the phishing attempt so they can avoid falling for it too.

Beginner's Guide 🔍

TO
CYBERSECURITY AWARENESS

Recognizing and Preventing Phishing Attacks

Phishing Awareness 🔍

Phishing is a common scam where hackers trick you into sharing personal information. Learn how to spot and avoid these scams to protect yourself.

Common Phishing Signs

Urgent Requests 🔍

These often claim that your account will be closed if you don't act immediately. Such messages are designed to pressure you into responding quickly without thinking.

Too Good To Be True 🔍

Phishing scams often offer free money or prizes to tempt you. These offers are designed to trick you into sharing personal information or clicking on harmful links.

Suspicious Links 🔍

Be careful with links in emails or messages. Hover over them to check if the web address looks correct if it doesn't match the sender or seems strange, avoid clicking on it.

Actions to Take if You're Caught in a **Social Media Phishing Scam**

- **Change Your Passwords:** Immediately change the passwords for your social media accounts and any linked accounts, like email or bank accounts.
- **Enable Two-Factor Authentication:** Set up two-factor authentication on your accounts for added security.
- **Report the Incident:** Report the phishing attempt to the social media platform so they can take action against the attacker.
- **Check for Suspicious Activity:** Look through your account for any changes or posts you didn't make and delete them.
- **Warn Others:** Inform your friends or followers about the phishing attempt so they can avoid falling for it too.