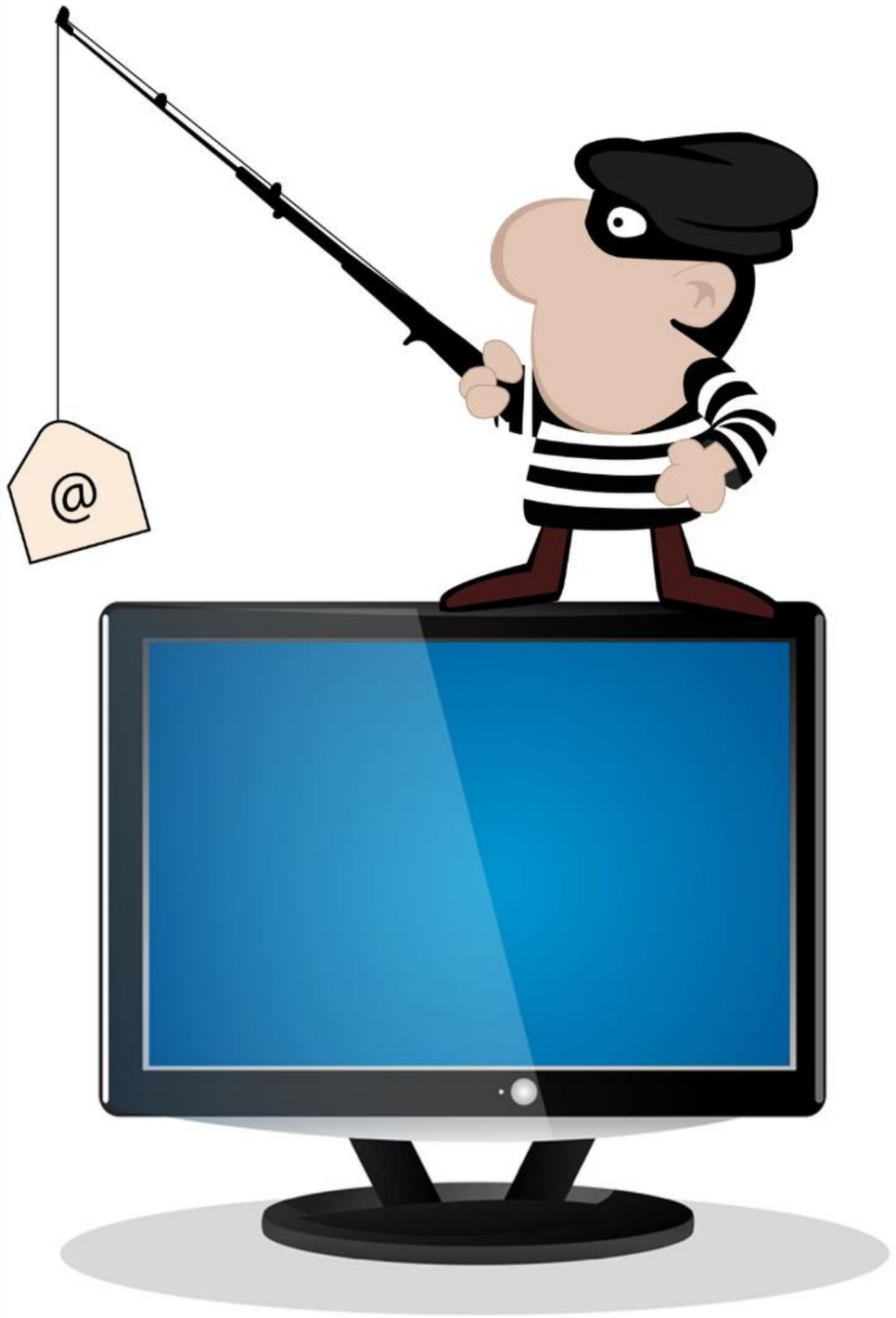
Phishing Awareness

This presentation covers phishing awareness, including what phishing is, types of phishing attacks, examples, and tips to protect yourself from phishing emails and phone calls.

By Marwane Andjar, Computer Science Student



What Is Phishing?

Phishing email messages, websites, and phone calls are designed to steal money or sensitive information. Cybercriminals can do this by installing malicious software on your computer, tricking you into giving them sensitive information, or outright stealing personal information off of your computer.

1. ## Steal Money

   Phishing attempts often aim to steal financial information or directly access funds.

2. ## Obtain Sensitive Data

   Cybercriminals seek to acquire personal or confidential information through deception.

3. ## Install Malware

   Some phishing attacks involve installing malicious software on the victim's computer.

4. ## Identity Theft

   Stolen personal information can be used for identity theft and fraud.

Types of Phishing Attacks

Social Engineering

Cybercriminals use information from social media profiles like Facebook or LinkedIn to craft convincing phishing messages. They gather details such as name, date of birth, location, workplace, interests, hobbies, skills, relationship status, telephone number, email address and favorite food to make their attacks more believable.

Link Manipulation

Most phishing methods use deception to make links in emails appear legitimate. Common tricks include misspelled URLs or using subdomains. Many email clients or web browsers show link previews when hovering over them, which can help identify suspicious links.

Spear Phishing

These are targeted attacks directed at specific individuals or companies. Attackers gather personal information to increase success rates. This is the most successful technique, accounting for 91% of attacks.

More Types of Phishing Attacks

Clone Phishing

This attack uses a legitimate, previously delivered email as a template. The attachment or link is replaced with a malicious version, and the email is sent from a spoofed address appearing to be the original sender.

Voice Phishing (Vishing)

Voice phishing uses social engineering over the telephone to gain access to personal and financial information. It's typically used to steal credit card numbers or other information for identity theft schemes.

Mass Phishing

These attacks target large groups of people simultaneously, often using generic greetings and urgent language to prompt immediate action.

Whaling

This type of phishing specifically targets high-profile individuals like executives or politicians, often with highly customized and sophisticated approaches.

Examples of Phishing Attacks

1. ## Spear Phishing Example

   An email claiming to be about a "Valdosta Upgrade" from a ucla.edu address, with greyed out To/Cc fields and a suspicious external link.

2. ## Clone Phishing Examples

   Emails mimicking legitimate eBay or PayPal communications, with generic sender addresses and links to external sites attempting to steal credentials.

3. ## Link Manipulation Examples

   Emails from spoofed valdosta.edu addresses or generic "Admin Team" senders, using urgent subject lines and links to external sites instead of legitimate valdosta.edu addresses.

4. ## Social Engineering Example

   Targeted messages on social media platforms like Facebook, using information from user profiles to craft convincing phishing attempts.

Identifying Phishing Emails

1

Check the Sender

Verify if the email is from someone you know or an expected sender. Only IT members will email about accounts.

2

Examine the Subject Line

Be wary of subject lines in all caps or with multiple exclamation marks trying to create urgency.

3

Look for Hidden Recipients

Phishing emails often hide the To: or Cc: fields to conceal that it's a mass email.

4

Hover Over Links

Before clicking, hover over links to see the actual destination. Legitimate emails from Valdosta State will use valdosta.edu addresses.

5

Check for Generic Signatures

Be cautious of emails with vague or generic sign-offs that don't identify a specific sender.

Protecting Yourself from Phishing

Never Share Passwords

IT will never ask for your password over email. Be wary of any such requests.

Be Cautious with Attachments

Be careful about opening attachments, especially unexpected ones. Call to verify if unsure.

Check for HTTPS

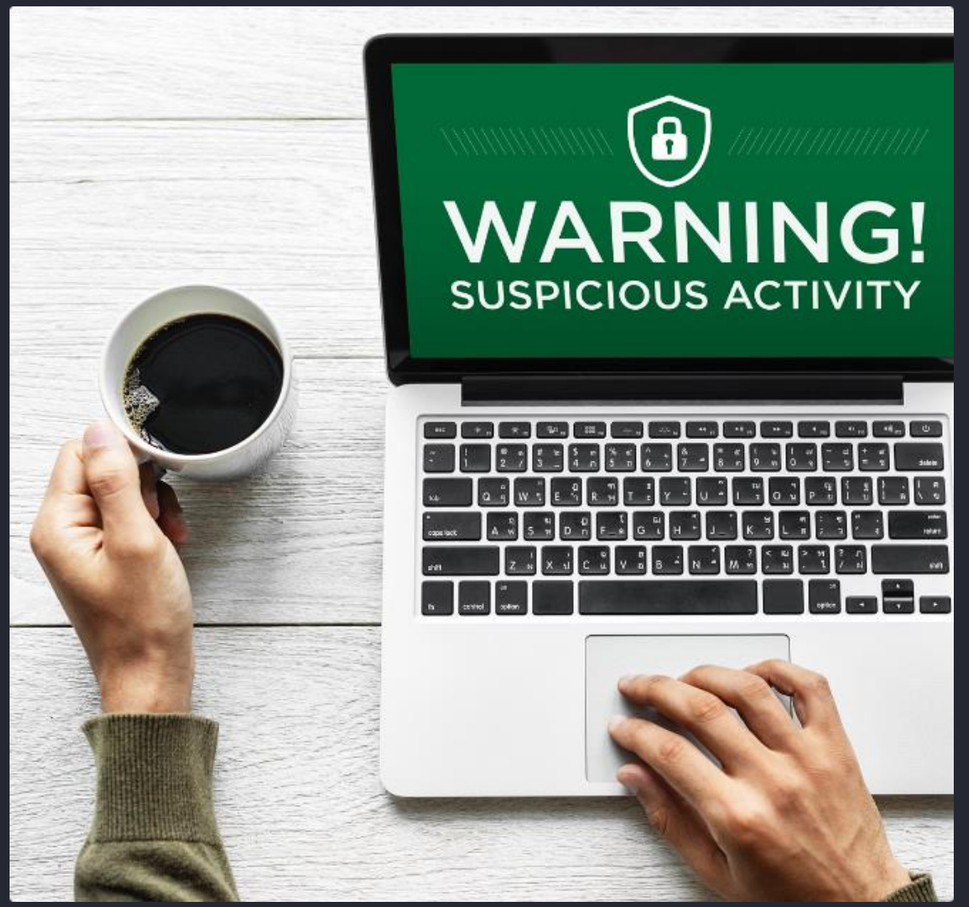
Look for 'https://' and a lock icon in the address bar before entering private information on a website.

Scrutinize Email Content

Look for spelling errors and bad grammar, which are common in phishing attempts.

Handling Suspicious Communications

Suspicious Emails	Suspicious Phone Calls
Do not click links or download attachments	Be wary of pressure to make immediate decisions
Forward to abuse@valdosta.edu	Never give out personal or financial information
Call sender to verify if attachment is expected	Research unfamiliar companies before transacting
Report to IT if you suspect a compromised account	Report abusive callers to FTC at 1-877-FTC-HELP



Sources

http://phishme.com/phishing-social-media-infographic/

http://en.wikipedia.org/wiki/Phishing

Additional resources

http://www.fraudwatchinternational.com/phishing-alerts

http://phishme.com/ http://www.onguardonline.gov/phishing

http://www.consumer.ftc.gov/articles/0076-phone-scams

http://www.fbi.gov/scams-safety/fraud