PHISHING AWARENESS

Wor-Wic Information Technology Department

5/9/2024

Understanding The Threat: Phishing Attacks

Phishing attacks are a significant concern for academic institutions, especially given their vast user networks and open access. Phishing emails are social engineering attacks often disguised as legitimate communications and are used to steal personal information from their victims.

Here are some common phishing scenarios:

- **Impersonating the IT Department:** Cybercriminals send emails pretending to be from the institution's IT department, asking recipients to verify their credentials or update their passwords.
- **Fake Tuition Payment Portals**: Fraudulent emails mimic tuition payment portals, tricking students into revealing sensitive information.
- **Bogus Scholarship Announcements**: create fake scholarship announcements, enticing students to click on malicious links.

Recognize The Signs Of A Phishing Email

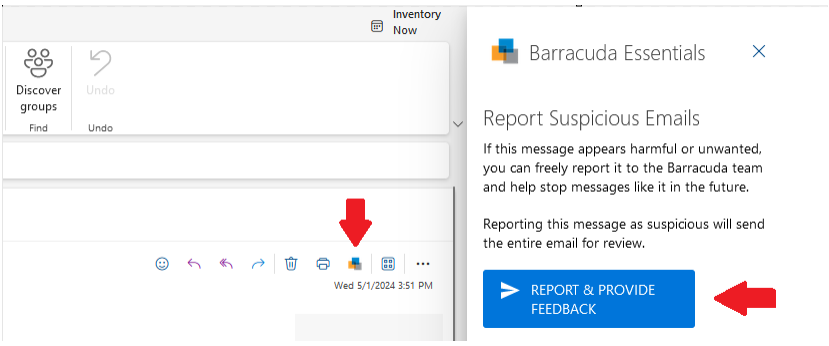
- Be wary of unfamiliar greetings or tones.
- Watch out for grammar mistakes and spelling errors.
- Be cautious if the email creates a sense of urgency.
- Did someone you know send a message, but it seemed odd or usual?
- Check for inconsistencies in email addresses such as web links or QR codes.
- Be skeptical of unusual requests or alerts claiming you've won something.
- Never give anyone your passwords. Wor-Wic IT, faculty, and staff would never ask for passwords through email or text messages.

The following awareness video provides additional information on how to catch and avoid phishing messages.

SANS Security Awareness: Email and Phishing — https://www.youtube.com/watch?v=sEMrBKmUTPE

Reporting Suspicious Emails

Click the **Barracuda Essentials** message button in the Outlook desktop app or



Outlook Online to quickly and easily report suspicious emails to the IT Department.

Any questions or concerns about suspicious emails can be sent to **infosec@worwic.edu**.

Stay Informed, Stay Secure Fins!