10 TIPS TO DETECT PHISHING SCAMS

01 Check the Sender’s Email Address

- Look out for subtle spelling changes in the domain name.
- Verify if the email is coming from a trusted source, even if the name appears familiar.

02 Spot Typos and Grammatical Errors

- Be cautious of emails with spelling mistakes and awkward phrasing.
- Phishing emails often contain errors, which could signal a scam.

03 Beware of Urgency Tactics

- Phishers create a sense of urgency to force quick actions (e.g., "Immediate action required!").
- Never share personal information under pressure or with vague requests.

04 Hover Over Links (But Don’t Click)

- Hover over links to check if the displayed URL matches the actual link.
- Avoid clicking on suspicious or mismatched links.

05 Be Careful with Attachments

- Hover over attachments to confirm they lead to a legitimate location.
- Don’t open attachments if you’re unsure of the sender's authenticity.

06 If It Sounds Too Good to Be True...

- Phishing scams often promise unrealistic rewards (e.g., lottery winnings or prizes).
- Always question offers that seem too enticing or out of the ordinary.

07 Keep Devices and Software Updated

- Ensure your device’s operating system and antivirus software are up to date.
- Regular updates help protect against new phishing techniques and security threats.

08 Monitor Your Accounts Regularly

- Review your accounts frequently to detect unusual or unauthorized activity.
- Knowing what’s normal for your accounts makes spotting phishing attempts easier.

09 Don’t Share Sensitive Information Over Email

- Legitimate companies never ask for personal or financial information via email.
- If in doubt, call the company directly to verify requests for sensitive information.

10 When in Doubt, Reach Out

- Inform your cybersecurity team or manager if you suspect a phishing attempt.
- Always double-check with trusted sources before taking action on suspicious messages.

Visit www.ampcuscyber.com or reach out to us at letsconnect@ampcuscyber.com