COMPASS
CYBER SECURITY

5 TIPS TO DETECT PHISHING EMAILS

One of the most common forms of social engineering is the phishing attack. Phishing is the attempt to electronically collect sensitive information by pretending to be a trusted entity. Typically this is in the form of an email from an organization that the recipient believes is legitimate. In reality the email is from a hacker trying to gain access to sensitive information that may include personal or business data. **To keep your data safe from these attacks, here are some tips to help identify and report phishing emails.**

1. **Check the sender email address for variations (jhill@company.com vs jhill@company.net).** Hackers often attempt to impersonate someone you trust by creating an email address similar to theirs.

2. **Look for spelling and grammar errors within the email.** Many phishing emails are sent from overseas. As a result, you can find spelling and grammar mistakes that can set off alarms.

3. **If an email is requesting information such as account numbers, contact information, etc., call the sender to validate the request before providing any information.** Verbal confirmation is a great way to ensure that you're communicating with the right person. Also, be sure to confirm that the number listed in the email is the same as the one you have on file.

4. **Do not open attachments or click on links embedded in emails unless they are from a validated or known source.** If you do not know the sender of an email, you should not assume the attachments and links are legitimate.

5. **When in doubt, contact the IT department for verification.** Your IT department is a resource for all of your cyber security questions. Representatives can help you verify the legitimacy of an email and, if you believe you have already clicked on a malicious link, they can help wipe your device so that your sensitive information does not fall into the wrong hands.

Managers also find success in routine mock-phishing exercises. These exercises simulate a phishing email and help employees identify whether the messages is legitimate or fake.

For more information on phishing emails and cyber security best practices, contact Matt Flora at mflora@compasscyber.com or 667-401-5108.

(ISC)² cpe Submitter

COMPASSCYBER.COM