FIGHT THE PHISH

Do Your Part. #BeCyberSmart.

CYBERSECURITY AWARENESS MONTH 2021

Phishing Detection Tips

Look for suspicious "From" addresses. Check received e-mails for spoofed or misspelled From: addresses. For example, if your organization is "ACME" and you receive an e- mail from user@AMCE.com, do not open the e-mail without verifying that it is legitimate. You can check by hovering over the sender's name. Does the mail address match what is in the "From" field?

Check embedded links. Validate that the URL of the link matches the text of the link itself. This can be achieved by hovering (not clicking) your cursor over the link to view the URL of the website to be accessed.

Be cautious with "too good to be true" messages. If you receive an unexpected message about winning money or gift cards, do not open the e-mail or take any action without verifying that it is legitimate.

Be cautious with "urgent" messages. If the e-mail message requires immediate action, especially if it includes a request to access your e-mail or any other account, do not open the e-mail or take any action without verifying that it is legitimate.

Subject: URGENT: New password management tool FREE for a limited time!

From: Karen Realperson <karen.realperson@AMCE.com>
To: John Doe <john.doe@ACME.com>

Hi John!

We have an amazing new tool to help manage all your usernames and passwords, but we need professionals like you to test it for us and provide feedback. For this limited time, testers can use our tool for FREE! Don't miss out!

Click >>>>>>>HERE<<<<<<< to submit your current log-in information to your healthcare's database system and we'll set up your FREE account.

DON'T MISS THIS AMAZING OPPORTUNITY!!! FREE ACCOUNTS ARE LIMITED!!!

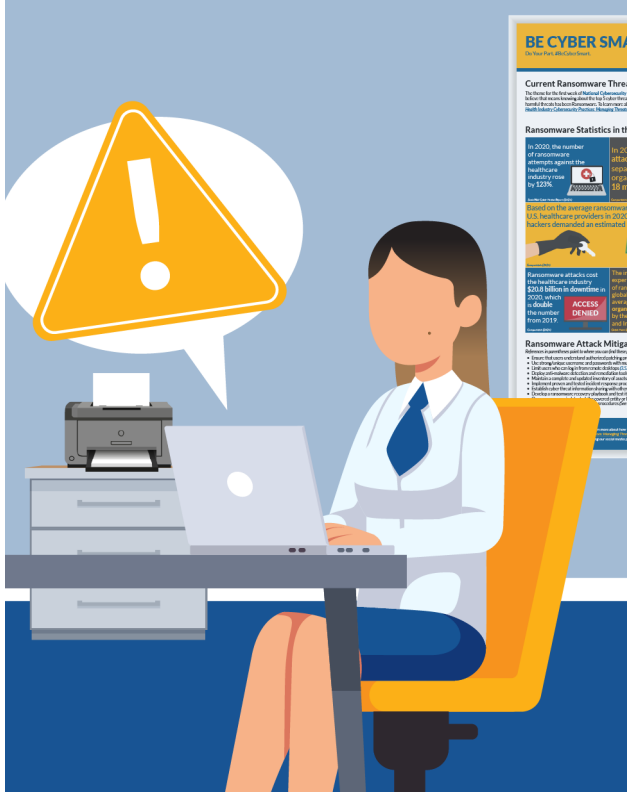
Thank you for your input!
Sincerely,
Karen Realperson
Head of HR, ACME Inc.

Best Line of Defense: Phishing Training for Employees

Train your employees to be careful when sending and receiving emails that contain personally identifiable information (PII) and protected health information (PHI). Ensure that you know your organization-specific protocols for sending PII and PHI. As a general rule, enable encryption when sending any PII or PHI information to outside stakeholders.

Train your employees on your process for encrypting email messages that are sent to external partners. This will minimize the risk of information being intercepted by hackers.

Train your employees on the protocol for reporting suspicious emails to your cybersecurity department. The earlier security personnel become aware of a phishing attack, the faster they can execute HICP Cybersecurity Practice #8: Security Operations Center and Incident Response.



HHS 405(d)
Aligning Health Care Industry Security Approaches

To learn more about how you can protect your patients from cyber threats check out the Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients publication. Check out the available resources 405(d) has to offer by visiting our social media pages: **@ask405d** *on Facebook, Twitter, LinkedIn and Instagram!*