Beware of phishing scams — Don’t Take the Bait!

One of the biggest information security risks for most organizations occurs when an associate opens a phishing email and clicks on the link. It only takes one associate clicking a phony link to impact an organization’s cybersecurity efforts.

Why it’s important

Phishing scams are emails that look real but are designed to steal important information. A phishing email with malicious software can allow cybercriminals to take control of your computer and put protected health information (PHI) and personally identifiable information (PII), as well as a company’s confidential and proprietary information, at risk.

It may be a phishing email if it:

- Promises something of value (e.g., “Win a free gift card”).
- Asks for money or donations.
- Comes from a sender or company you don’t recognize.
- Links to a site that is different from that of the company the sender claims to represent.

- Comes from a trusted business partner that has experienced a security incident. All emails sourcing from outside your organization should be scrutinized
- Asks you for personal information, such as your username and password/passphrase.
- Includes misspelled words in the site's URL or subject line.

If you suspect an email may be phishing, here are some tips:

- Do not click any links in the email.
- Do not provide your username and password; you should never share your username or password, even if you recognize the source. Phishing scams frequently mimic well-known companies, such as retailers (like Amazon) or banks.
- Do not reply or forward the email to anyone within your organization.
- Familiarize yourself with your organization's process for reporting suspicious emails. If you suspect an email is a phishing attempt, report it immediately.
- Your organization's information security department may have additional information and guidance on how to protect yourself from phishing scams.