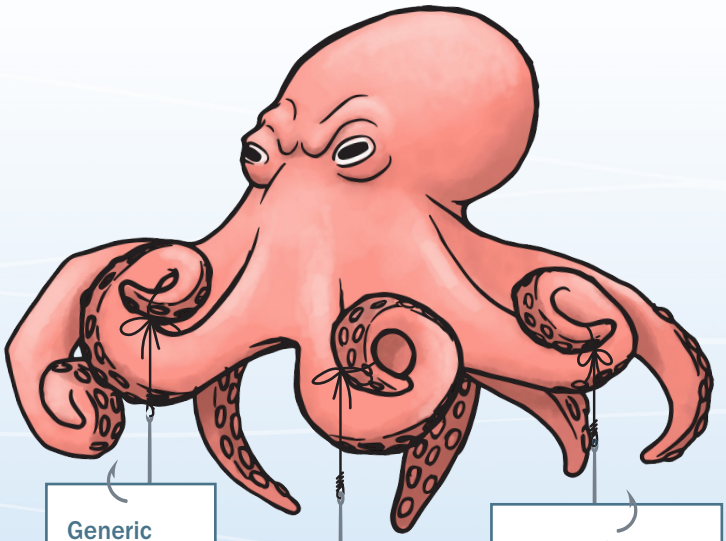
Beware of BAIT!

How to Spot a Phishing Scam

"Phishing" emails attempt to trick people into sharing information that helps criminals access an organization's information technology (IT) network, distribute malicious software, or commit identity theft. Healthcare organizations are common targets; 42% of all data breaches in the past year involved email as a breach location (HHS "Breach"). Phishing scams are increasingly sophisticated and threaten privacy and security of protected health information, accuracy of clinical information, and continuity of care.

Signs of phishing include the following:



Generic greetings

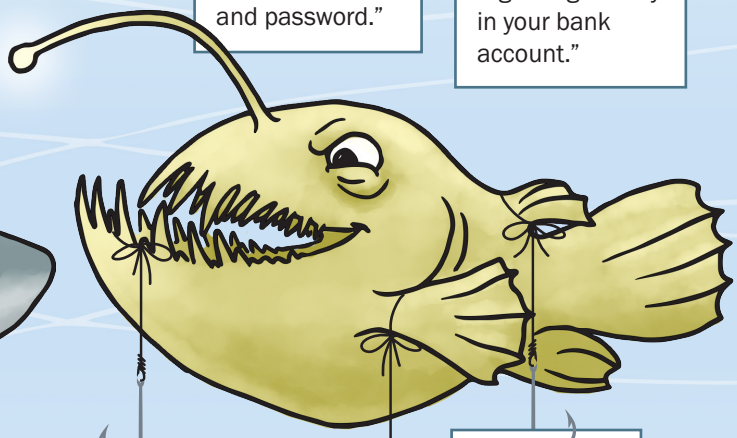
"Dear User,"

Request for login credentials

"Please confirm your username and password."

Abuse of trust by impersonating a real website

"We are contacting you regarding activity in your bank account."



Poor spelling and grammar

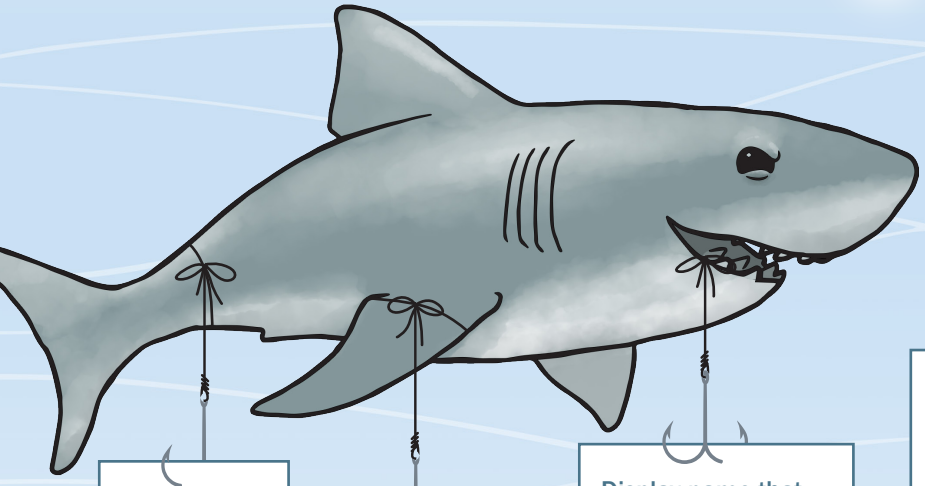
"u must rspnd ASP"

Small errors in links

A11health instead of Allhealth

Altered domain names

JohnJones@ggmail.com



Creating fear or urgency

"Your account has been hacked!"

Unexpected attachments

"Please review the attached contract."

Display name that doesn't match email address

From: Mary Smith
Email Address: gotcha@phishing.net

Don't take the bait!

Everyone plays a part in protecting information security.

Remain vigilant and use the following strategies to combat phishing:

- Hover over links in emails before clicking to verify destination and confirm that the link begins with https://
- Validate unexpected attachments by calling the sender at a known telephone number
- Ask your organization's IT department about any suspicious emails
- Change your password and call IT immediately if you think you have been phished

Disclaimer: This infographic is not intended to take the place of individual health center information security policies.

ECRI Institute Resources

- The HIPAA Privacy Rule: https://www.ecri.org/components/PPRM/Pages/RS5.aspx
- The HIPAA Security Rule: https://www.ecri.org/components/PPRM/Pages/RS5_1.aspx

Sources

Cofense.com. How to spot a phish. 2018 [cited 2019 Aug 8]. https://cofense.com/wp-content/uploads/2016/07/phishme-how-to-spot-a-phish.pdf

KnowBe4, Inc. Social engineering red flags. 2018 [cited 2019 Aug 8]. https://cdn2.hubspot.net/hubfs/241394/Knowbe4-May2015-PDF/SocialEngineeringRedFlags.pdf

Securitymetrics.com. 7 ways to recognize a phishing email: email phishing examples. [cited 2019 Aug 12]. https://www.securitymetrics.com/blog/7-ways-recognize-phishing-email

Staysafeonline.org. 5 ways to spot a phishing email. 2018 Aug 22 [cited 2019 Aug 12]. https://staysafeonline.org/blog/5-ways-spot-phishing-emails/

US Department of Health and Human Services Office for Civil Rights. Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information. [cited 2019 Aug 14]. https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

US Department of Health and Human Services Office for Civil Rights. Phishing. 2018 Feb [cited 2019 Aug 8]. https://www.hhs.gov/sites/default/files/cybersecurity-newsletter-february-2018.pdf

US Department of Health and Human Services Office for Civil Rights. Train your workforce, so they don't get caught by a phish! 2017 Jul [cited 2019 Aug 8]. https://www.hhs.gov/sites/default/files/july-2017-ocr-cyber-newsletter.pdf