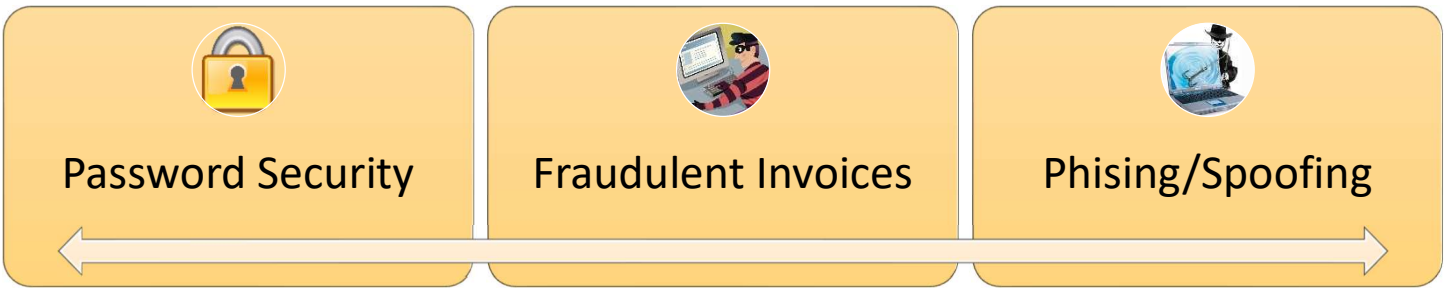
There are Plenty of "Phish" in the Sea: Don't Get Caught Up in the Scam

Since government orders that respond to the COVID-19 crisis have disrupted many businesses and have resulted in many of your employees working remotely, including from their homes, we wanted to bring Cybersecurity Awareness to your attention. Cybersecurity is the protection of computer systems and networks from the theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide.

It's imperative to be aware of the latest scams in order to help maintain your company's data security and integrity.

Important Topics



Tips to spot a scam:

- Misspelled words
- Strange or big requests
- Website is "off" and bare-boned:
  - Website is "unsecure"
  - Missing footer and navigation
  - Misspelled words
  - No contact information

How to avoid these attacks:

- Above all else: Don't click the link
- Be skeptical and ask a follow-up question or clarification
- Be careful about the info you share on social media, oversharing can be used to target you
- Keep software up to date

Remember your passwords need to be:

- Alphanumeric
- At least 8 characters
- And never give your passwords to anyone.

Fraudulent Invoices/Gift Card Request

Scam artists often aim fake invoices and requests at employees hoping to trick them into paying for products or services that they did not order. Many of these "invoices" appear at first glance to be legitimate bills and may include threatening or confusing legal jargon to create a false sense of urgency to pressure recipients to make quick payments.

“Phishing” scams are a very popular tactic hackers use to trick users into thinking they received an email or text (SMiShing = SMS phishing) from a reputable company. They will use logos, fake but realistic-looking email addresses and contacts, and other tactics to trick you into clicking a malicious link that could compromise your security.

Other iterations:

- “Spear-phishing” is a subset of phishing that is more personalized — the hacker will pose as someone you know to gain your trust.
- “Whaling” refers to a type of phishing that targets individuals who have high-level access to data, funds and information (i.e. business owners, CFOs, etc.).

Do not click links from emails that you weren’t expecting, raise any sort of suspicion or from contacts not already in your contact list. Hover over the link to see the URL and even if it still looks normal, type the domain into your browser using https. Remember your supervisor Bob will never ask you to buy several $100 gift cards and email him the security codes to bobLovesFishing325202@aol.com

Thank you for taking the time to read through this and help keep your company’s data safe and secure.