All Bout *ishing
(Phishing Smishing & Vishing)

Phishing has been and continues to be one of the most common methods cyber attackers use, it’s effective and too often successful. Phishing is a simple attack vector that enables cyber attackers to scale their attacks, easily customizing for intended targets. While there are technical controls to help, cyber attackers continue to adapt, with the Human Element responsible for the majority of all breaches.

Smishing can be thought of as SMS+Phishing, a cyber attack using misleading text. Texting has become increasingly popular as many phones lack much filtering capability, which means the scams and attacks are far more likely to bypass any security controls. Also, since text messages tend to be much shorter with little context, it’s much harder to confirm what is legitimate versus what is an attack.

Vishing would be Voice+Phishing, an attack by phone, which can appear to be calling from a familiar area code or a recognizable organization. The cyber attacker’s goal here is to get the victim to call a phone number. Once the victim is on the phone, cyber attackers will use stories and emotion to pressure people into taking actions, such as giving up their passwords, purchasing gift cards or transferring money from their bank accounts to accounts controlled by the attacker.
Whether it’s phishing, smishing or vishing, the indicators and clues this might be a malicious attack are similar:

- **Urgency**: Any email or message that creates a tremendous sense of urgency, trying to rush you into making a mistake. An example is a message from a credit card company stating that your payment is overdue, and if you don’t pay your account will be closed and reported.

- **Pressure**: Any email or message that pressures an employee to ignore or bypass company policies and procedures.

- **Curiosity**: Any email or message that generates a tremendous amount of curiosity or too good to be true, such as an undelivered UPS package or you are receiving an Amazon refund.

- **Tone**: An email or message that appears to be coming from a co-worker or leader, but the wording does not sound like them, or the overall tone or signature is wrong.

- **Generic**: An email coming from a trusted organization but uses a generic salutation such as “Dear Customer”. If FedEx or Apple has a package for you, they should know your name.

- **Personal Email Address**: Any email that appears to come from a legitimate organization, vendor or co-worker, but is using a personal email address like @gmail.com.

- Companies and government agencies you do business with should never ask for your account information, credit card numbers or password in an email. If you have any questions about a communications you receive that supposedly came from your financial institution or service provider, find their number on their website and call them.

- When a major news event happens, cyber criminals will take advantage of the incident and send phishing emails with a subject line related to the event. These phishing emails often include a link to malicious websites, an infected attachment or are a scam designed to trick you out of your money. For example, think back to global disasters; cyber attackers were keen on topics that pulled on our emotions.

- **CEO Fraud / BEC** is a type of targeted attack. It commonly involves a cyber-criminal pretending to be your boss or senior executive and then tricking you into sending the criminal highly sensitive information, buying gift cards or initiating a wire transfer. Be highly suspicious of any emails demanding immediate action and/or asking you to bypass any security procedures.

- If your role and responsibilities require enhanced privileges continue to be vigilant, and carefully examine all things *ishing.

- Remember – common sense is your best defense.