Email Phishing Tips

- **S L O W D O W N** reading messages. Do not be in a hurry to click without thinking!
- **Read** the entire message before clicking on attachments or links. Reading is Fundamental.
- **Analyze** the From: address. Double-click on the Name / Alias to identify the actual email address. Does it look familiar? What is the domain? The Name / Alias does not always match the email address itself.
- **Lack of personalization**. Did the email use a generic salutation such as 'Dear Customer' or nothing at all? Service providers usually know who you are and typically personalize emails with your name and the last few digits of your account number.
- **Bad spelling and grammar**. Legitimate businesses go out of their way to proofread their email. If an email has lots of spelling mistakes or improperly worded sentences, it's likely a phish. Cyber threat actors are greatly improving their spelling and grammar, though.
- **Hover over all links**. If you hover your mouse over a website link, you will see the actual destination of the website you're about to visit (on some mobile devices you can accomplish the same thing by holding your finger on the link for a second or two). If that location differs from the way the link is written in the email, it's a good indication of an attack. When in doubt – type the URL shown & not the link in the message.
- **Suspicious attachments**. If you don't know the sender, or receive something from a friend that looks suspicious, don't open the attachment. If it is from someone you know, you can always pick up the phone and give them a quick call to make sure they sent the email. Utilize the File "Preview" feature available in most email programs.
- **Requests for sensitive information**. Be suspicious of any request for sensitive information, such as user IDs and passwords, financial account numbers, health information or social security numbers. No legitimate entity will ever ask for that information via email.
- **Unfamiliar sender**. If the sender is unknown, and the email address is one you've never seen before or looks different than it should, be suspicious and look for other clues.
- **Authoritative-sounding sender**. A person representing a company or entity sends an email asking for information they should already have.
- **Blank or "undisclosed" recipients**. Sometimes phishing emails are sent to a lot of people. Other times you see something like "undisclosed recipient list" in the "To:" field. Both are potential red flags.
- **Urgent and immediate call to action**. Messages of an urgent nature, or requesting an immediate call to action, are a common method used to rush people into making mistakes and is another good indicator of phishing.
- **Logos** mean nothing. A logo can easily be cut 'n pasted from the Internet. They offer minimal credibility.
- **Phone numbers** are nearly always included with legitimate business messages. Or use a Search Engine to find the phone number separately. Take the extra time, make a phone call to confirm the legitimacy of the message.

Password & Passphrase Tips

- A **strong** password includes upper- and lower-case letters, numbers, and special characters or symbols. Use the variety of characters.
- **Avoid** using dictionary words, family, friend and pet names, events, locations, license plates, birthdates or teams Adding a number before or after any of these does not make it secure.
- Create **pass phrases** instead of passwords.
- **Longer** is better. A minimum of 8 characters and 12 or more is recommended. The shorter the password, the more frequent it needs to change. The longer the password, the less it needs to change. (See matrix below).
- Always **create** a new password for every app or website. Never reuse a password for more than one application.
- If keeping track of passwords is a challenge, consider using a **Password Manager**.
- Use **Multi-Factor Authentication** whenever possible. Always.
- Keep **private**. Do not share passwords with others, in email or text messages.
- **Alternate** characters by avoiding consecutive identical characters or a string of characters appearing sequentially on the keyboard.
- **Consider** not utilizing the Remember Me option available in many applications.
- **Update** the default password on every device. Never allow the default password to remain.
- **Check** passwords against a list of commonly used, expected, or compromised passwords
- **Immediately** change a password if a site or company is breached.
- **Avoid** password recycling. Use the creativity of the human brain to come up with new ones.
- When using applications on the Internet that require a password, make sure the web address begins with **https://** not http://.
- **Shoulder surfing** can give others your passwords, be aware of password stalkers.
- **Do not** record passwords on paper or in a Word, Excel, or other non-secure file.

Time it takes a Hacker to Brute Force your Password

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15 bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100 bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100tn years	7qd years