**Lesson 3: Phishing**

An article about a common cyber threat— phishing, including its signs and ways to combat it. Because phishing attacks are so common (a whopping 90% of cyberattacks start with a phishing email), an important element of staying cybersecure is knowing how to recognize and protect yourself against those types of attacks.

**What is Phishing**

To review, **phishing** is when a cybercriminal sends a fraudulent message, designed to look legitimate, that tricks a user to expose personal sensitive information or deploys malicious software on the user's system. These messages can be sent via email, social media, or text, and could contain malicious links that attackers urge the user to click.

For example, a cybercriminal might conduct their phishing attempt by posing as a seemingly trustworthy credit card company. They might take advantage of current events or stoke fear by creating a problem that leaves the user feeling forced to give up their account details. Once the user responds to the attacker with their information, the attacker now has access to the user's account and data.

A computer with a hook and a paper on it

Description automatically generated

**Signs**

To prevent yourself from falling victim, look out for the following signs in a message that might indicate a phishing scam:

* **Spelling** **errors, poor grammar, and layout inconsistencies**: A lot of phishing emails are sent by foreign nationals. A legitimate email would not have those errors because reputable institutions have teams that proofread customer correspondence.
* **A spoofed email address**: The sender's address tries to imitate that of a real company, omitting or altering select characters to trick the receiver by closely resembling (but not exactly matching) a reputable source. Examples include LinkedIn to Linkedln, Amazon to Amaz0n, Google to Go0gle
* **Suspicious attachments**: An attacker creates a false sense of urgency to persuade the receiver to click on or download an attachment. If the user happens to click on the attachment in a phishing email, their system might be exposed to malware.
* **Spoofed and suspicious links**: The text display for websites most likely hides that link's true destination. Try hovering your cursor over all links in an email to see if the text matches up with the actual hyperlink. Also, verify that hyperlinks don't have a different domain (.com vs .net) or variation in spelling to a legitimate site. If they do, that link is spoofed and is probably malicious.
* **Generic introduction and conclusion line**: Generic greetings and signatures like "Sir," "Ma'am," or "Valued Customer" and a lack of contact information all point to the high chance that that email is a phishing scam. A legitimate business would address receivers by their actual name and give contact information.
* **Incorrect information**: If the sender is telling you that you did something (like purchase an order), even though you never did it, that is a strong indicator of phishing.
* **A sense of urgency**: In a phishing scam, a cybercriminal will most likely use a false sense of urgency or importance to persuade the receiver to click on a link or attachment or send their information.

Here is an example of a phishing scam. Notice where the signs described above are present in this email:

A screenshot of a computer

Description automatically generated

If you fall for a phishing message and reveal personal details (such as account information) to a cybercriminal, you might become a victim of identity theft as well. The malicious hacker who carried out that phishing attack against you could use your information to commit fraud and other crimes. Additionally, if you click on any links or attachments in a phishing email, you may compromise your username and password for the account, expose your system to **malware** and malicious code, or be targeted by a **ransomware** attack.

**Actionable Steps**

That's why it is so important to stay vigilant against phishing. Recognize the common factors of a phishing scam in a message and/or email and be suspicious of any unsolicited lines of communication. When in doubt, contact the legitimate company directly to verify if an email request is legitimate or not. Remember-- never provide personal or financial information or click on links unless you are absolutely sure that the sender is reputable, legitimate, and trustworthy. To ensure your safety (even against realistic-looking phishing emails), it is smart to install **anti-malware/virus software**. This software protects your device from cybercriminals' harmful code if you ever click on a phishing link.

If the event that you have been compromised by a phishing attack, change the passwords and usernames that you revealed to the attacker (on all accounts that you used them) and monitor your account for any changes in activity. Contact appropriate institutions and organizations to report the incident, too.

To reiterate, always think before you click and give away personal information!