October Cyber Security Month Tips

October isn't just about Halloween- it's Cyber Security Awareness Month! Let's stick to treats and remember to stay clear of tricks all year long, especially those in the form of phishing scams.

Phishing is when cyber attackers use email or a messaging service (like those on social media sites) to trick or fool you into taking an action, such as clicking on a link, sending sensitive data, or opening an infected email attachment. By falling victim to such an attack, you risk having highly sensitive information stolen and/or your computer infected.

Attackers work hard to make their phishing emails convincing through various methods, including adding logos of reputable companies and businesses or forging an email address to make it look like it came from someone or something you know.

Here are some common indicators of a phishing attack to look out for:

- The message is directed to "Dear Customer" or some other generic greeting.
- Some immediate action is required, creating a sense of urgency, such as threatening to close down your account.
- The sender claims to be from an official organization, but grammar and spelling mistakes are present, or it comes from a personal email address, such as @gmail.com, @yahoo.com, or @hotmail.com.
- The sender is requesting highly sensitive information, such as passwords, department files, or payment information.
- The message looks like it came from someone you know, but the tone of the message does not sound like him or her. Call the sender on a trusted phone number to verify they sent it.

Here are some best practices to avoid becoming a victim of a phishing attack:

- **NEVER** click on a link you do not trust:
  - Links can easily be disguised to make them appear trustworthy when they actually lead to malicious sites. Avoid clicking on links you were not expecting to receive or were sent from someone you do not recognize.
- **NEVER** open an email attachment you did not expect:

- Infected email attachments have become a very common attack method. If you receive and email with an attachment you were not expecting, avoid opening the attachment.

- **NEVER** enter credentials or sensitive information into a website you do not trust:
- Oftentimes, malicious links will take you to a fake website designed to collect login credentials and other sensitive information. It is best to avoid entering any credentials into a website that you may not trust or used a malicious link to navigate to.