TN Department of Finance & Administration | Strategic Technology Solutions

2021 NCSAM National Cybersecurity Awareness Month

Week 2 - Do Your Part
Fight the Phish!
#BeCyberSmart

Can you always spot phishing attempts? It's cybersecurity awareness month and we'll show you how to spot potential phishing attempts that can result in ransomware or other malware. Reduce your chances of falling victim to phishing attacks by reporting or deleting suspicious activities!

Always Keep Your Guard Up:

- Protect your credentials. If you're asked for sensitive information, don't be afraid to ask why. No reputable company will ask for sensitive information via email, text message, or phone.

- Beware of attachments and links. E-mail attachments and links are commonly used to send malicious software. When you get a message with an attachment or link, verify that it is legitimate - before clicking.

Check the sender's email address:

- If you don't know the sender, check the sender's e-mail address before replying or clicking on links. Since emails can be spoofed, float your cursor over addresses before replying to make sure they are legit. Any correspondence from an organization should come from an organizational e-mail address.

Your Public profile:

- Limit your public information. Attackers use personal, public information about you to lure you into responding. The less you share about yourself, the smaller the target you are for a social engineering attack. Cybercriminals use information you post online to learn how to gain your trust.

The bad guys use pressure:

- Don't be pressured. Emails that create urgency and fear are usually fake. Take your time, look at the whole email and be skeptical: double check the "from" address to see if it's legitimate.

- Stop and review. Look at the email before replying. Is it unexpected? Does the request make sense? When in doubt, reach out to the sender, separately, by phone or directly emailing them (not replying to the email).

Report it!

- (As outlined above) Be on the lookout for emails or text messages from unknown senders that contain strange links or attachments. Learn how to recognize these types of messages and think before you click.

- If you receive a suspicious email, but haven't opened the attachment or clicked on a link, please forward that email to spam.abuse@tn.gov as an attachment. The Spam Abuse account is monitored around the clock by the customer care center staff, who will notify and engage the appropriate operations and incident response staff.

You are a part of cybersecurity.

Cybersecurity is how we protect information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction in order to provide confidentiality, integrity and availability.

Cybersecurity is achieved through implementing technical, management and operational controls designed to protect the confidentiality, integrity and availability of information. Your continued investment in participating in this year's information security training class, will help drive the actions and activities that will help to sustain a culture of cybersecurity here at the state.

Remember: always trust your instincts. If an email, phone call or an attachment seem suspicious, don't let your curiosity put your computer at risk! If you see or hear something cyber suspicious, please contact the STS Customer Care Center at 615-741-1001.

Best regards to all,

Curtis

TN Department of Finance & Administration | Strategic Technology Solutions
Curtis Clan | Chief Information Security Officer, CISSP
p. 615-741-9109