#SeeYourselfInCyber

Phishing

What is Phishing?

Phishing is when a criminal poses as a trusted source and sends fraudulent digital messages, such as emails, with the intent of manipulating individuals into revealing personal information and gaining unauthorized access to a system through a download or link.

Phishing emails may appear to come from a real financial institution, e-commerce site, government agency, or any other service, business, or individual. The email may also request personal information such as account numbers, passwords, or Social Security numbers. When users respond with the information or click on a link, attackers use it to access users' accounts.

Phishing attacks are some of the most commonly successful types of criminal attacks.

How Criminals Lure You In

The following messages are examples of what attackers may email or text when phishing for sensitive information:

- "We suspect an unauthorized transaction on your account. To ensure that your account is not compromised, please click the link below, and confirm your identity."

- "During our regular verification of accounts, we couldn't verify your information. Please click here to update and verify your information."

- "Our records indicate that your account was overcharged. You must call us within 7 days to receive your refund."

Simple Tips

- **Go slow with strangers.** Links in email and online posts are often the way cybercriminals compromise your computer. If you're unsure who an email is from even if the details appear accurate — do not respond, and do not click on any links or attachments found in that email. Be cautious of generic greetings such as "Hello Bank Customer," as these are often signs of phishing attempts. If you are concerned about the legitimacy of an email, call the company directly.

- **Think before you act.** Be wary of communications that implore you to act immediately. Many phishing emails attempt to create a sense of urgency, causing the recipient to fear their account or information is in jeopardy. If you receive a suspicious email that appears to be from someone you know, reach out to that person directly on a separate secure platform. If the email comes from an organization

but still looks “phishy,” reach out to them via customer service to verify the communication.

- **Protect your personal information.** If people contacting you have key details from your life—your job title, multiple email addresses, full name, and more that you may have published online somewhere—they can attempt a direct spear-phishing attack on you. Cyber criminals can also use social engineering with these details to try to manipulate you into skipping normal security protocols.

Submitting suspected Phishing Emails

- (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. The following examples will submit those emails to the spam.abuse@tn.gov account

Using the Office 365 Client

Using the Office 365 Web Portal

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.

Remember: always trust your instincts. If an email, phone call or an attachment seems suspicious, don't let your curiosity put your computer at risk, and try to avoid hurriedly going through your email because that’s when you might click before thinking!! If you see or hear something cyber suspicious, please contact the STS Customer Care Center at 615-741-1001.

Our hope is that this year’s campaign will help tighten your cybersecurity at home and across communities and businesses alike. We need your help and the help of your peers in protecting the state of Tennessee, businesses and other communities, and your personal and professional assets. This year’s campaign has shared ways to increase your resilience against cyber-attacks, and has provided easy-to-use tools to lock down private data, and to keep those assets secure from criminals, terrorists and foreign entities.

Best regards to all,

Curtis Clan | Chief Information Security Officer, CISSP

You May Also Be Interested In:

CyberSafeTN

NCSAM Tips and Advice

Security & Risk Mitigation Resources

STS Security Services Policy Documentation