TN Department of Finance & Administration | Strategic Technology Solutions

Cybersecurity and Privacy Bulletin

The Dangers of Phishing

Phishing

When an internet fraudster impersonates a business to trick you into giving out your personal or work information, its called phishing. Don't reply to email, text, or pop-up messages that ask for your; state credentials, personal or financial information. Don't click on links within them either – even if the message seems to be from an organization you trust. It isn't. Legitimate businesses don't ask you to send sensitive information through insecure channels.

No State of Tennessee agency or division, along with F&A, Edison and STS will ever ask you to send or share your passwords!!!

No one representing your credit card company or bank, any reputable company, or a governmental agency is going to email you to "verify" your personal financial information. Be aware also, that if an email of this nature contains a link to a Web site, that site may be a deceptive mirror of a real company's website. The phony site has been constructed just for you -- to steal your identity. Look up the company's websites address or if known, type the URL manually.

Take a closer look at the email

Does the email:

1) Address you in vague terms, such as “Dear Sire or Madam”
2) Ask for personal information, such as your online banking login details or your date of birth
3) Ask you to click on link in the email or download an attachment
4) Come from an organization you don’t normally deal with
5) Contain odd ‘sp3lling’, have poor grammar or use ‘CaPiTals in strange places

(Phishing emails do this in an attempt to avoid spam filter software)

Security threats from Phishing

Phishing emails or any other unsolicited message could be used to convince an end-user to reveal sensitive information about themselves or internal computer systems. A message posing as an online survey could ask recipients for their password. The survey could also ask for other information which may allow an attacker targeting a specific organization to gain valuable intelligence prior to launching another type of cyber-attack.

Examples of Phishing Subject lines

- Security Alert
- Revised Vacation & Sick Time Policy
- A Delivery Attempt was made
- All Employees: Update your Healthcare Info
- Change of Password Required Immediately
- Password Check Required Immediately
- Unusual sign-in activity
- Urgent Action Required

The subject lines reported here have actually made it through some corporate email filters and into the inbox of an employee. If the phishing email is created correctly, the right type of message can pass all of the defenses because it is playing into the human nature of wanting to receive something you didn’t know about, or needing to intervene before something is taken away. Ultimately this means that a company’s ‘human firewall’ is an essential element of organizational security because people truly are the last line of defense.”

Examples of Phishing Messages

- "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.”

The senders are phishing for your information so they can use it to commit fraud.

How to Deal with Phishing Scams

- Delete email and text messages that ask you to confirm or provide personal information (credit card and bank account numbers, Social Security numbers, passwords, etc.). Legitimate companies don't ask for this information via email or text.

- The messages may appear to be from organizations you do business with – banks, for example. They might threaten to close your account or take other action if you don’t respond.

- Don’t reply, and don’t click on links or call phone numbers provided in the message, either. These messages direct you to spoof sites – sites that look real but whose purpose is to steal your information so a scammer can run up bills or commit crimes in your name.

- Area codes can mislead, too. Some scammers ask you to call a phone number to update your account or access a "refund." But a local area code doesn’t guarantee that the caller is local.

- If you’re concerned about your account or need to reach an organization you do business with, call the number on your financial statements or on the back of your credit card.

You can take steps to avoid a phishing attack:

Use these computer security practices.

- Don't email personal or financial information. Email is not a secure method of transmitting personal information.
- Only provide personal or financial information through an organization's website if you typed in the web address yourself and you see signals that the site is secure, like a URL that begins https (the "s" stands for secure). Unfortunately, no indicator is foolproof; some phishers have forged security icons.
- Review credit card and bank account statements as soon as you receive them to check for unauthorized charges. If your statement is late by more than a couple of days, call to confirm your billing address and account balances.
- Be cautious about opening attachments and downloading files from emails, regardless of who sent them. These files can contain viruses or other malware that can weaken your computer's security.

- The best policy is to refrain from downloading files or clicking through links in a strange email, unless you trust the source. Malware, viruses, and other types of malicious material can be easily downloaded to your server or computer through attachments or malicious links

Reporting Phishing Emails

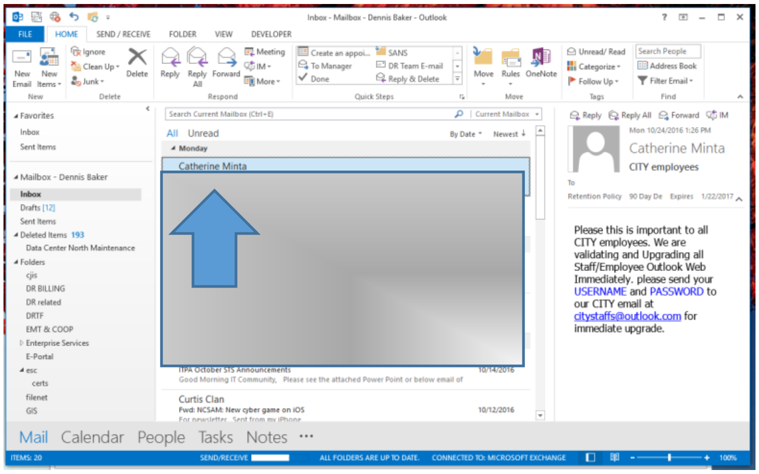
If you receive an email that you think is a phishing attempt or you do not trust the sender, you should forward that email as an attachment to Spam.Abuse@tn.gov

- ***Important****! Please make sure that you use the "Forward as attachment" option. Just merely forwarding the attachment does not give us enough information.*

How to Forward a Message as an Attachment in Outlook

Select Email - On your Microsoft Outlook main page, select the Email you want to forward as an attachment.

Report Phishing Emails - *continued*



Catherine Minta

ITPA October STS Announcements 10/14/2016
Good Morning IT Community, Please see the attached Power Point or below email of

Curtis Clan
Fwd: NCSAM: New cyber game on iOS 10/12/2016
For newsletter Sent from my iPhone

Reply Reply All Forward IM

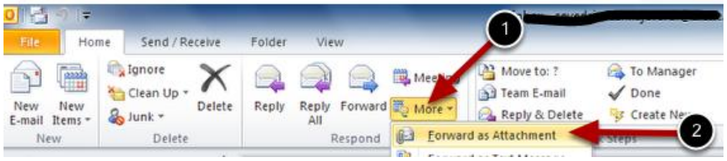
Mon 10/24/2016 1:26 PM
Catherine Minta
CITY employees
To
Retention Policy 90 Day De Expires 1/22/2017

Please this is important to all CITY employees. We are validating and Upgrading all Staff/Employee Outlook Web Immediately. please send your USERNAME and PASSWORD to our CITY email at citystaffs@outlook.com for immediate upgrade.

Click on the Home tab & then Forward as Attachment

(1) Choose "More" from the Respond subcategory.

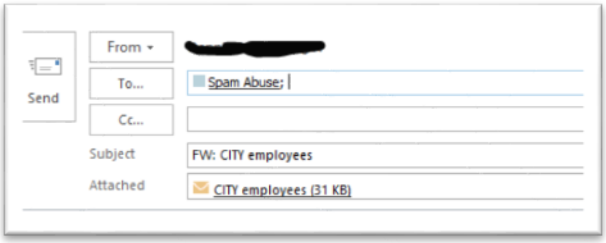
(2) Click on "Forward" as Attachment



Fill out Recipients

(3) Fill out the "To" section with "Spam Abuse"

(4) Click "Send"



From [redacted]

To... Spam Abuse;

Subject FW: CITY employees

Attached CITY employees (31 KB)

Following these suggestions can help you avoid being 'phished' and help the State of Tennessee remain safe.

The information provided in the Monthly Security Tips Newsletter is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall cyber security posture. This is especially critical if employees access their work network from their home computer. Organizations have permission and are encouraged to brand and redistribute this newsletter in whole for educational, non-commercial purposes.

MS-ISAC MULTI-STATE Information Sharing & Analysis Center™

STOP | THINK CONNECT™

TN