TOIRMA Update

By Jim Donelan TOIRMA Executive Director

Protect Your Network – Red Flags

Anyone that has a personal computer, laptop, or smartphone has received unwanted emails or spam. I spend at least five to ten minutes every morning cleaning out my inbox. Some emails are self-inflicted due to me opening an account at a retail site, and I just can't get myself to unsubscribe due to the possibility of missing out on a good deal. However, some of these messages are phishing emails. Phishing is the most common form of "social engineering." According to Google Dictionary, "social engineering is (in the context of information security) the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes. 'People with an online account should watch for phishing attacks and other forms of social engineering.'" Township officials are vulnerable to social engineering, in particular phishing emails.

Phishing is best described as an email that looks legitimate but is NOT. The email appears to be from a sender or organization you may know or trust. Unfortunately, the message is from a malicious sender, or hacker. These individuals are targeting local governments, businesses, and recipients looking for personal and organizational information. This may be your township's computer that has information such as employee data, intellectual property, financial account information, and credit card or payment data. If one elected official or employee falls for a phishing attack, your township's entire system may be compromised.

Again, phishing emails look legitimate and appear to be from a reliable company, organization, or even other townships officials or employees. Phishing emails often have the following characteristics:

- Ask you for your username and password, either by replying to the email or clicking on a link that takes you to a site where you're asked to input the information;
- Look like they come from your human resource or information technology (IT) personnel;
- Have grammatical errors.

Please refer to the "Social Engineering Red Flags" on the following page.

eRiskHub – Cybersecurity Services Available to TOIRMA Members

TOIRMA members have access to our cyber partner's, DUAL Cybersecurity, website www.eriskhub.com/dual, containing information and resources designed to assist in the prevention of network, cyber and privacy losses, and support in the timely reporting and recovery of losses if an incident occurs. eRiskHub is an internet-based service featuring news, services from leading practitioners in risk management, computer forensics, forensic accounting, crisis communications, legal counsel, and other highly specialized segments of cyber risk.

To obtain access to eRiskHub, please contact Carla Hilligoss at chilligoss@ccmsi.com (217) 444-2111 or Danielle Smith at dsmith@ccmsi.com (217) 444-1204.

Thank you for your attention to these matters.

As always, if you have any additional questions, please feel free to contact me toll-free at (888) 562-7861 or by email at jdonelan@toirma.org.

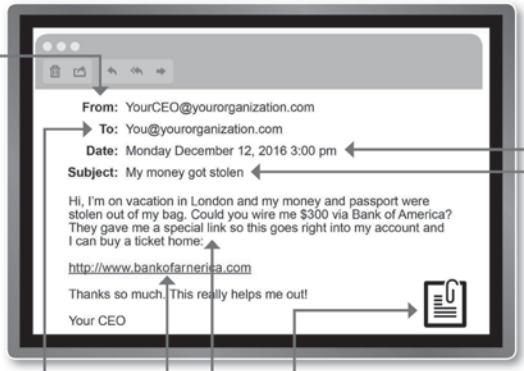
Think Safe … Drive Safe … Work Safe

toirma.org

Social Engineering Red Flags

FROM

- I don't recognize the sender's email address as someone **I ordinarily communicate with**.
- This email is from **someone outside my organization and it's not related to my job responsibilities**.
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner and is **very unusual or out of character**.
- Is the sender's email address from a **suspicious domain** (like micorsoft-support.com)?
- **I don't know the sender personally** and they **were not vouched for** by someone I trust.
- **I don't have a business relationship** nor any past communications with the sender.
- This is an **unexpected or unusual email** with an **embedded hyperlink or an attachment** from someone I haven't communicated with recently.



DATE

- Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time** like 3 a.m.?

SUBJECT

- Did I get an email with a subject line that is **irrelevant** or **does not match** the message content?
- Is the email message a reply to something **I never sent or requested**?

TO

- I was cc'd on an email sent to one or more people, but **I don't personally know** the other people it was sent to.
- I received an email that was also sent to an **unusual mix of people**. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.

ATTACHMENTS

- The sender included an email attachment that **I was not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly **dangerous file type**. The only file type that is **always safe to click on is a .txt** file.

HYPERLINKS

- I hover my mouse over a hyperlink that's displayed in the email message, but the **link-to address is for a different website**. (This is a **big** red flag.)
- I received an email that only has **long hyperlinks with no further information**, and the rest of the email is completely blank.
- I received an email with a **hyperlink that is a misspelling** of a known web site. For instance, www.bankofarnerica.com — the "m" is really two characters — "r" and "n."

CONTENT

- Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence** or to **gain something of value**?
- Is the email **out of the ordinary**, or does it have **bad grammar** or **spelling errors**?
- Is the sender asking me to click a link or open up an attachment that **seems odd** or **illogical**?
- Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a **compromising or embarrassing picture** of myself or someone I know?

KnowBe4
Human error. Conquered.