TOIRMA Update

By Jim Donelan TOIRMA Executive Director

Cyber Liability & Phishing

On June 1, 2017, TOIRMA began offering its members Cyber Liability Coverage. This coverage is designed to cover claims relating to (a) Information Security and Privacy Liability, (b) Privacy Breach Response Services, (c) Regulatory Defense and Penalties, (d) Website Media Content Liability, (e) PCI Fines and Penalties, and (f) Cyber Extortion Loss. The portion of the coverages this article will focus on is the Cyber Extortion Loss or sometimes referred to as "ransomware."

Cyber extortion is a threat to breach computer security, destroy or corrupt data, or interrupt computer systems. For example, a computer virus is installed on a computer and encrypts the files. The hacker then makes a demand for payment in exchange for a decryption key (i.e. a password to unlock your computer and data).

The most common method for corrupting computers is through a malicious/infected email which includes an attachment or hyperlink. Known as "phishing," these messages look like legitimate emails but have malicious content designed or intended to provide a hacker access to your computer and data. Although TOIRMA's Cyber Liability Coverage aids townships in these types of situations, it is a very unpleasant process that can be prevented.

The following questions and answers relate to what phishing emails are and how to spot them.

Question: *What is phishing?*

Answer: Phishing emails look like they came from a person or organization you trust, but in reality, they're sent by hackers to get you to click on or open something that will give the hackers access to your computer.

Question: *Why are you at risk?*

Answer: Hackers have been targeting businesses and local governments because they have information that is valuable to their organizations. Specifically, hackers may be interested in township's computer information such as residents and employee data, intellectual property, financial account information, and credit card or payment data. If one employee falls for a phishing attack, your township's entire system can potentially be accessed.

Question: *How to spot a phishing email?*

Answer: Hackers have gotten clever in how they design the emails they send out to make them look legitimate. They may even look like they come from your township supervisor or other officials and employees. Phishing emails often have the following characteristics:

Your assistance is needed ...

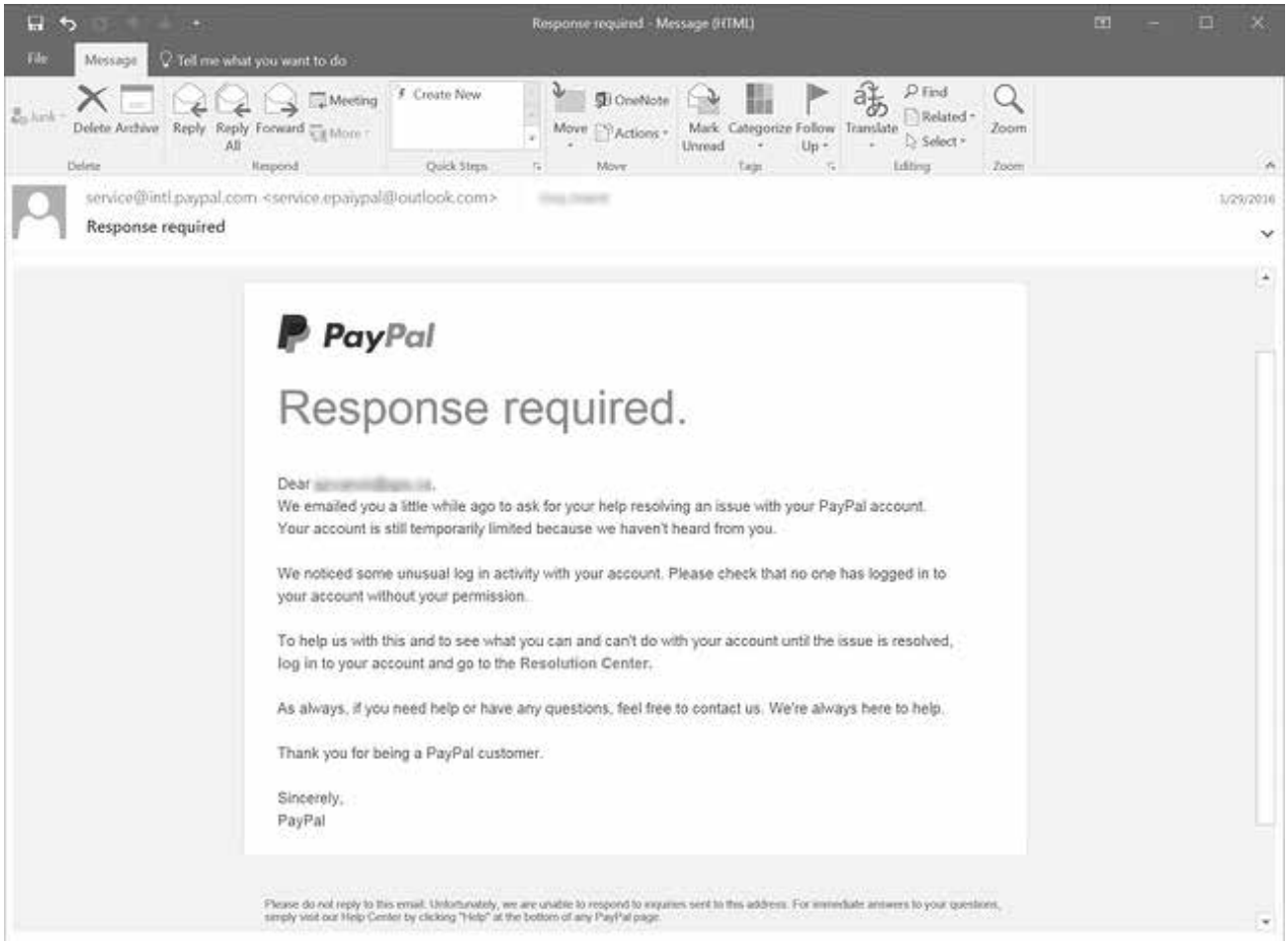
To make sure that you, or the officials in your township, receive their issue of *Township Perspective*, please make sure that TOI is notified when there is a change of official or address. We are receiving several address changes from the postal service and sometimes is after we have already sent out another mailing.

Please call the TOI Office toll free at 1.866.897.4688 and ask for Pam or Kayla, or email your change to pam@toi.org or kayla@toi.org.

Your assistance is much appreciated!

- 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;
- Contain email addresses that don't match between the header and the body, are misspelled (like @gmaill.com), or have unusual formats (@company-othersite.com);
- Have links or email addresses that show a different destination if you hover over them; and
- Try to create a sense of urgency about responding

Here is an example of what a phishing email looks like.



Question: *What you should do if you get a suspicious email?*

Answer: If you suspect that an email is a phishing email:

- Do not open any links or attachments in the email
- Notify your IT personnel
- **If you've already opened a link or attachment, disconnect your computer from the internet but do not turn it off, and then immediately call IT**

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