TransForm
SHARED SERVICE ORGANIZATION
Leading Innovation. Improving Healthcare.

Communiqué

TO: **All Member Hospital Staff**

DATE: 29 October 2020

FROM: Mazen Joukhadar, Vice President, Chief Information, Privacy & Security Officer

RE: **Latest Phishing Campaigns - Vigilance**

Please be advised there are several new reports of a spike in ransomware attacking hospitals in the United States. The FBI and two federal agencies have issued an alert to all U.S. healthcare providers, however this ransomware campaign threat could also affect Canadian hospitals and so we are requesting heightened vigilance.

TransForm is reminding all hospitals and staff to be extra cautious of these attacks. If you receive a suspicious email, text message, or phone call, or if you receive a COVID-19 e-mail from any external party, do NOT open any attachments or click on any links. Please log a ticket with tech support indicating the 'subject' of the e-mail and the 'sender' e-mail address (use the TransForm Support Portal or contact the TransForm regional IT/IM service desk at 519-973-4411, extension 7771).

Please delete the concerning e-mail from your mailbox and/or text message from your phone.

As always, please restrict Internet surfing to business and clinical applications and continue to be vigilant when clicking on links or opening attachments from unexpected or suspicious emails addresses.

In most circumstances, a good general principle to follow if an email request seems suspicious or questionable whether you know the sender or not, is to **NOT OPEN** attachments, follow web links or respond to the email. If you know the sender, follow up personally, (not replying to the email) before taking action and always follow normal operating procedures. If the sender is unknown, delete the email.

Below are some tips on how to identify fraudulent emails and how to avoid becoming a victim.

What to look out for:

- Spelling and bad grammar - Cybercriminals are not known for their grammar and spelling. If you notice mistakes in an email, it might be a scam.
- Email Links - Rest your mouse (but don't click) on the link to see if the address matches the link that was typed in the message.
- Threats - Cybercriminals often use threats that your security has been compromised. They may indicate your account will be closed if you do not respond.
- Generic Emails - phishing emails are usually generic, for example Dear First Bank user. If you don't see your name, be suspicious.

Spoofing popular websites or companies - Scam artists use graphics in email that appear to be connected to legitimate websites but actually take you to phony scam sites or legitimate-looking pop-up windows.