Security Bulletin Update – Ransomware Vulnerability Advisory

TransForm
SHARED SERVICE ORGANIZATION
Leading Innovation. Improving Healthcare.

Communiqué

TO: Hospital Employees

DATE: October 4, 2019

FROM: Mazen Joukhadar, Chief Information, Security and Privacy Officer – TransForm SSO

RE: **Ransomware Vulnerability Advisory**

Please be advised that up to three (3) Ontario hospitals have been impacted so far. Those hospitals are in **full disaster recovery** and **MANUAL business continuity** at this time; patient care is impacted.

As an additional preventive measure, we have been informed that LHSC is blocking all MS Word (.doc) email attachments that their staff receive from external sources (Note: LHSC is not one of the impacted hospitals). If you are sharing materials with anyone at LHSC, please contact them to arrange alternate methods to share documents.

TransForm is not at this time taking that same preventive measure, but asks that everyone be extra vigilant. TransForm is again reminding and cautioning hospital employees of ransomware attacks. Ransomware will attack our environment and encrypt files making them not accessible.

Please continue to be vigilant when clicking on links or opening attachments from unexpected or suspicious emails.

If an email is unexpected, seems suspicious or questionable do not open attachments, follow web links or respond to the email immediately. If you know the sender, follow up personally before taking action and always follow normal operating procedures. If the sender is unknown, delete the email.

If you receive a suspicious email or you believe that you have a file which has been encrypted and cannot be accessed, please contact the TransForm regional IT/IM service desk at 519-973-4411, extension 7771 and they will notify TransForm's security team. If calling outside of our normal operating hours (evenings and weekends) simply leave a voicemail message which we will receive the next business day.

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.

For more detailed information on how to protect yourself please view our What You Need To Know About Phishing Document at the link below.

https://www.transformsso.ca/uploads/MemberSite/What%20You%20Need%20To%20Know%20About%20Email%20Phishing.pdf