MEMO

Date:

To: All Shared Health staff and Service Delivery Organizations

From: Perry Poulsen, Provincial Lead & CIO, Digital Health

Re: **COVID-19 – Cybersecurity threats**

As COVID-19 continues to evolve in Manitoba, Digital Health has seen a marked increase in cybersecurity threats including Ransomware attacks. A number of local and national organizations have been impacted by these threats.

It is extremely important to remain vigilant at this time to minimize the impact of these threats to our organization and our partners.

Digital Health has protocols and security measures in place to minimize risk to our networks and computers from these types of attacks. Given the aggressive and targeted nature of these latest threats, we are reinforcing the importance of scrutinizing emails, links and attachments to ensure they are legitimate.

Be aware of these COVID-19 related scams:

- Local and national health agencies or government departments will never email you for your health details or to sell you a COVID-19 vaccine or test.
- Organizations such as The Canadian Red Cross or the World Health Organization will never email or text you for confidential information.
- Do not trust social media posts or ads promising COVID-19 cures, tests, vaccines or selling masks and gloves.
- National health agencies, local or national government officials will never contact you regarding the latest viruses-related risks, statistics, advisories and safety measures.
- Human Resource departments will never email you asking you to fill out a form with your personal information.

How to Protect yourself

Here are a few simple steps you can take to protect yourself, whether you are using a Digital Health managed device or your own personal device:

- Do not open attachments in unsolicited e-mails, even if they come from people in your contact list.
- Never click on a URL contained in an unsolicited e-mail, even if you even if you think it looks safe. Instead, close out the e-mail and go to the organization's website to confirm its authenticity.
- Make sure you have updated antivirus software on your computer.
- Have strong passwords. Do not use the same passwords for work, personal, shopping, banking. Password Guidance for personal use can be found here: https://cyber.gc.ca/en/guidance/best-practices-passphrases-and-passwords-itsap30032
- Do not plug in USB devices that are not Digital Health issued and secured devices. It is a common tactic for cybercriminals to place USBs around an office. Often these USB devices are used to install malicious software.
- Use the same precautions on your mobile phone as you would on your computer when using the internet.
- Consult the Government of Canada Cyber Safe web site for tools and information to protect your personal devices - https://www.getcybersafe.gc.ca/index-en.aspx

What to do if you have been a target of a Cybersecurity attack

Report any emails that you suspect are "phishing" attempts or contain malicious content as follows:

- Forward the email as an attachment to the Service Desk at: servicedesk@sharedhealthmb.ca
- If you require help doing this, call the Service Desk at 204-940-8500 or 1-866-999-9698
- Delete the email after forwarding to the Service Desk.

If you have questions or require additional information, please contact the Service Desk at servicedesk@sharedhealthmb.ca or call 204-940-8500 or 1-866-999-9698.