IT Security Notice

QR Code Phishing Text Messages Reported

Enterprise Security Services has been made aware of possible QR Code related phishing SMS (text) messages that may be circulating in Saskatchewan. If you receive an inquiry from the member of the public wondering if eHealth has sent them a QR code, kindly advise them that eHealth would not send them a QR code directly and suggest they delete the message.

Mobile devices are attractive targets that provide unique opportunities for threat actors intent on gathering information because they contain vast amounts of sensitive and personal information. A compromised device has the potential to allow unauthorized access to your organization's network, placing not only your own information at risk, but also that of the organization.

Recommendations:

There are a few simple actions you can take to drastically reduce the risk of exposing sensitive or personal information:

- Do not reply to suspicious messages or spam messages. Doing so will only confirm your address is valid resulting in more spam.
- Be suspicious of unsolicited emails, links or attachments. Even if they appear to be from someone you know. If there is any doubt, don't open or click them.
- Avoid sending sensitive information over email or texts
- Maintain up-to-date software, including operating systems and applications.
- Use a PIN or passphrase to protect your device.
- Use Multifactor Authentication (MFA) on all possible business and personal accounts as a second form of verification requirement in order to access an account.
- Reduce the information you post online (e.g. phone numbers and extensions for employees)
- Do not reuse passwords across multiple accounts or use generic passwords such as your birth date, 'password123', 'YourName123', etc.
- Do not use "Remember Me" features on websites and mobile applications – always type in your username and passphrase or password to log in.
- Avoid joining unknown, unsecured, or public Wi-Fi networks.
- Disable features not in use, such as GPS, Bluetooth, or Wi Fi.
- Do not jailbreak (e.g. disable security measures imposed by device manufacturer) your device

If you suspect you've received a suspicious email, forward it (as an attachment) to emailsecurity@eHealthsask.ca and delete it from your inbox. Please report any security-related incidents immediately to to ServiceDesk@eHealthsask.ca 1-888-316-7446

We appreciate your help in protecting the Saskatchewan health network.