IT Security Notice

Telephone Scam Reported

Enterprise Security Services has been made aware of unsolicited telephone calls asking users to verify their emails as a lure to send malicious email for users to look at which could install software to gain access to your system.

Callers may represents themselves as Microsoft, IBM, or other IT Company offering support, however, major IT Companies do not make unsolicited phone calls (also known as cold calls) about your computer security or software fixes. Communication typically has to be initiated by you. Simply hang up.

Recommendations:

There are a few simple actions you can take to protect yourself against unsolicited scams:

- Watch for vishing: Be suspicious of unsolicited phone calls asking for confidential information like account information, passwords, or asking you to open an email they have sent you.
- Watch for phishing: 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.
- Maintain up-to-date software, including operating systems, applications, and anti-virus software.
- Utilize strong passwords and never reuse passwords across multiple accounts or use generic passwords such as your birth date, 'password123', 'YourName123', etc.
- Use Multifactor Authentication (MFA) whenever possible as a 2nd form of verification to access accounts.
- Avoid sending sensitive information over email or texts
- Reduce the information you share online (e.g. phone numbers and extensions for employees)
- 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
- Use a PIN or passphrase to protect your mobile devices.
- Review organization policies and guidelines to ensure you are using information and assets properly

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 ServiceDesk@eHealthsask.ca 1-888-316-7446

We appreciate your help in protecting the Saskatchewan health network.