eHealth Saskatchewan

Enterprise Security Services

Spotting Suspicious Email Messages

Have you ever seen a link that looks a little off?

Phishing attacks can take the form of emails, texts, or phone calls, but more than 90% of successful cyber-attacks start with a phishing email.

Given our desire to trust (and the number of emails we receive daily), it can be easy to believe the content we read in these emails, click on embedded links, or open attachments.

However, the attachments may contain malicious software, and the links may direct you to malicious websites.

Think Twice!

Even if an email comes from someone you know, you should always think twice before clicking links or opening attachments.

Be the strong link!

- ☑ Never provide personal information in response to unsolicited messages and leave suspicious websites immediately.
- ☑ Watch for unrecognizable names, email addresses or phone numbers. When in doubt contact the sender by another means (e.g. phone call) to confirm they contacted you.
- ☑ Look for spelling or grammar errors, requests for personal or confidential information, urgent requests with a deadline, or offers that are too good to be true.
- ☑ Always access sites the way you usually do and never through a link provided in a unsolicited email or text message.

If you suspect you've received a suspicious email, forward it (as an attachment) to emailsecurity@eHealthSask.ca and delete it from your inbox. Report any security-related incidents immediately to ServiceDesk@eHealthSask.ca

We appreciate your help in protecting the Saskatchewan health network.