eHealth Saskatchewan

Enterprise Security Services

Social Engineering Exposes Information and Access

Have you ever been manipulated into giving up information?

A social engineering attack needs only one thing to be successful: the trust of the targeted party.

All it takes is a single email, phone call, or text message that appears to come from a trusted source for a cyber criminal to gain access to sensitive information.

Cyber criminals who use social engineering tactics are banking on their victims acting first and thinking later.

Think Twice!

Your alertness to people pretending to be someone else and to manipulation can protect us from social engineering attacks.

Be the strong link!

- ☑ Don't click on unexpected links, even if they come from familiar email senders or organizations. You can be redirected to a website or start a download that can infect your device.
- ☑ Examine all aspects of your incoming messages for suspicious elements, such as a spoofed email address or website URL.
- ☑ Be wary of an urgent tone. Social engineering campaigns typically lean on language that conveys a strong sense of urgency.
- ☑ If you aren't expecting an email from a contact, especially one with a link or attachment that is out of character, verify its legitimacy before opening.

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.