eHealth Saskatchewan

Enterprise Security Services

Business Email Compromise Scams Cost Millions

Can you recognize a legitimate email from our senior management?

Have you ever received an email from an executive asking you to transfer money for an urgent transaction?

This is an elaborate phishing-based scam designed to get funds transferred directly into accounts held by the fraudsters. The CEO fraud, where a fraudster impersonates a senior executive by email, is a very common and costly scenario. Millions of dollars are extorted annually.

If you frequently perform wire transfers, you are at greater risk of being targeted by these scams.

Think Twice!

If a request makes you uncomfortable, pause and ask yourself:

- Does this person usually write to me?
- Am I really the person to fulfill this request?

Be the strong link!

- ☑ Be suspicious of urgent request of large transfer of funds in an unusual manner, especially if the sender pretends to be unreachable or demands secrecy.
- ☑ Watch out for sudden unexpected changes in business practices, like a change in contact or banking information.
- ☑ Never bypass the policies, procedures and controls in place for substantial transfers and payments.
- ☑ Before providing sensitive information by email or telephone, verify the identity of the individual requesting it and confirm the legitimacy of his or her request.

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.