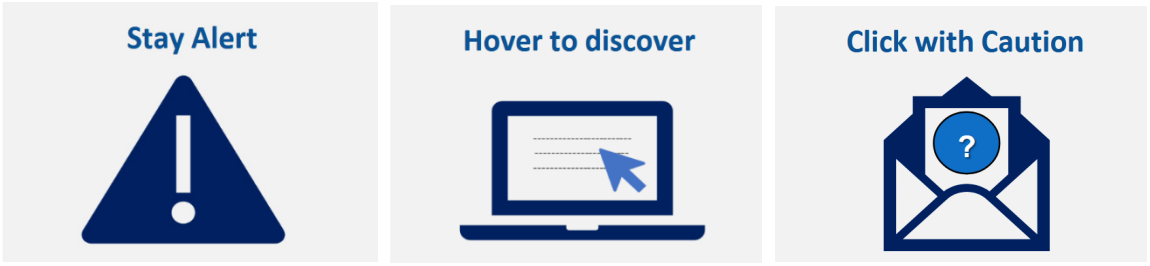
COVID-19 Phishing Awareness Alert

Shared Health has seen an increase of phishing attacks attempting to take advantage of COVID-19 uncertainty.

What is a phishing attack?

A phishing attack is an email message that attempts to steal confidential user information such as usernames, passwords, and credit card information. This message is often unexpected, urgent or comes from an unknown sender.



KEY ACTIONS YOU CAN TAKE

Stay Alert

- Be suspicious of unexpected email messages, especially messages that seem urgent or try to instill fear.

Hover to Discover

- Often, the scammer appears to be someone you know, but when you hover over the sender's name or email address you may notice the sender is not really who they say they are. If you receive an email from someone you know but the email address is not one you recognize, follow-up with a phone call.

Click with Caution

- If you receive any suspicious email messages that contain links or attachments, do not click on the links or open the attachments. Instead, report the email.

Report you have received a phishing message

- If you receive an email message that seems suspicious, call the Service Desk at 204-940-8500 or forward the email as an attachment to ServiceDesk@sharedhealthmb.ca and phish@access.ironport.com

COVID-19 Phone Scam

There have been reports of multiple phishing scams related to Covid-19 asking people for credit card information to provide medication following a positive test result. This is not a call that Manitobans would receive from public health officials.

Manitobans are advised to not provide any financial data, hang up on the call and to report to their local law enforcement agency.