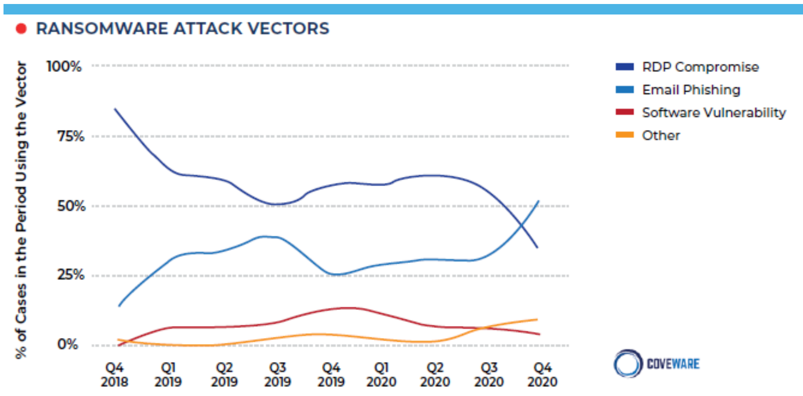
eHealth Saskatchewan

Enterprise Security Services

Ransomware increases through email phishing



IMAGINE IF YOUR FILES GOT ENCRYPTED AND YOU MUST PAY $200 TO UNLOCK YOUR COMPUTER.

What would you do if your computer and files were taken hostage? Would you have to pay to get them back? How much time and resources would you waste on fixing that issue?

Cybercriminals use ransomware to extort money from organizations and individuals by holding computers, phones and files hostage. Countless organizations have been paralyzed by such attacks.

Adopt safe behaviors and reduce the impact of a ransomware attack or even better, prevent it from happening in the first place.

Think Twice!

Always back up your files as it is nearly impossible to decrypt ransomed files.

Be the strong link!

☑ Never click on links and buttons in unexpected or suspicious emails or text messages. This is how ransomware is delivered.

☑ Only install approved software and applications, and only download from a trusted source.

☑ Never modify or disable antivirus software installed on your computer. It only protects you if it is enabled and updated!

☑ If you fall victim to a ransomware attack, do not contact the cybercriminal, and do not pay the ransom.

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.