WORKING REMOTELY

Tips on how to manage cyber security when you're working remotely.

Do not use an unsecure Wi-Fi.
Use a secure home network and make sure your home router is secure. This prevents man-in-the-middle attacks from remote locations: remember that since you're working from home, the traffic is now flowing over public networks. ***Remember*** to always use the company's VPN.

Lock your screen if you work in shared space.
Lock your computer when not in use – both at home and in public places. An inquisitive child accidentally sending an email to your boss or a customer is easily prevented, as is limiting the opportunity for someone to access the machine while your back is turned in the local coffee shop. ***Remember*** press "CTRL-ALT-DEL" then click "lock"" or "Windows key + L" to lock your computer when you step away or it is not in use.

Look out for phishing emails and websites.
During this time, you should remain vigilant about recognizing phishing emails and exercising caution when opening attachments, or clicking on links from sources they don't know to be trustworthy. Many cyber criminals will take advantage of COVID-19 news and updates and use these email messages to gain unauthorized access to the corporate network. You should review email policies and procedures for when a suspicious email arrives in your inbox. ***Remember*** never click on a link if you think an email is phishing.

Email security
Generally, internal emails sent between employees of credit unions are secure and do not require additional security. Any emails that are sent to recipients outside the employee network and include content that is confidential must have added security. ***Remember,*** if in doubt, use email encryption.

Ransomware
Ransomware is a type of malware that restricts access to your computer or files. A message will display demanding payment for the restriction to be removed. Sometimes a notification will display stating that that the authorities have detected illegal activity and a payment is required to avoid prosecution. ***Remember*** to never click on unverified links or open unexpected email attachments and only download from sites you trust.

Physical security
Physical security is the protection of personnel, hardware, programs, networks and data from physical circumstances and events that could cause serious losses or damage to your organization. ***Remember*** even when working remotely to always follow a Clean Desk Policy ensuring that all corporate assets are secured properly when not working.

Passwords
Company password policies should be enforced and include complexity rules, password expiration, lockouts and minimum lengths. ***Remember*** it is your responsibility to keep your passwords safe, secure and private.

Non-standard software use
No software should be installed without the approval of management and/or your organizations technology department. ***Remember*** you are responsible to ensure that all department software is registered and approved. All software installed must be registered to your organization.

alberta central