McLeod Lake Indian Band

General Delivery, McLeod Lake, BC V0J 2G0
Main Office (250) 750-4415 Fax: (250) 750-4420

April 29, 2020

To all McLeod Lake Indian Band Members,

During this time of uncertainty, when people are turning to technology, there are people of the world are trying to take advantage of the situation. These people are developing new ways of trying to scam ordinary citizens.
Over the last several weeks, there has been an increase in these scams, whether they be by email text or phone.
BC Hydro has asked we share the following statement with the Membership:

BC Hydro is warning customers about an increase in scams targeting customers. Since March, they've received a 350% increase in scams reported. Fraudsters are using sophisticated technology to reach customers over the phone, email and text message by indicating customers are eligible for a refund or threatening disconnection and requesting immediate payment. Here's what you should know:
• BC Hydro has suspended all disconnections for non-payment during the COVID-19 pandemic.
• They don't collect credit card or bank account information over the phone, by email or text.
• They don't accept payment from pre-paid cash or credit cards, or bitcoin ATM.
• They don't offer refunds or credits through Interac e-transfer.
If you receive a suspicious communication, please call 1 800 BC HYDRO (1 800 224 9376) or check your MyHydro account. Learn more at https://tinyurl.com/yap8re8y.

MLIB Administration would like to remind everyone, there are ways of protecting yourself:

- **Be alert to the fact that scams exist.** When dealing with uninvited contacts from people or businesses, whether it's over the phone, by mail, email, in person or on a social networking site, always consider the possibility that the approach may be a scam. Remember, if it looks too good to be true, it probably is.
- **Know who you're dealing with.** If you've only ever met someone online or are unsure of the legitimacy of a business, take some time to do a bit more research. Do a Google image search on photos or search the internet for others who may have had dealings with them. If a message or email comes from a friend and it seems unusual or out of character for them, contact your friend directly to check that it was really them that sent it.
- **Do not open suspicious texts, pop-up windows or click on links or attachments in emails – delete them:** If unsure, verify the identity of the contact through an independent source such as a phone book or online search. Don't use the contact details provided in the message sent to you.
- **Don't respond to phone calls about your computer asking for remote access – hang up** – even if they mention a well-known company such as Telstra. Scammers will often ask you to turn on your computer to fix a problem or install a free upgrade, which is actually a virus which will give them your passwords and personal details.

McLeod Lake Indian Band

General Delivery, McLeod Lake, BC V0J 2G0
Main Office (250) 750-4415 Fax: (250) 750-4420

- **Keep your personal details secure.** Put a lock on your mailbox and shred your bills and other important documents before throwing them out. Keep your passwords and pin numbers in a safe place. Be very careful about how much personal information you share on social media sites. Scammers can use your information and pictures to create a fake identity or to target you with a scam.
- **Keep your mobile devices and computers secure.** Always use password protection, don't share access with others (including remotely), update security software and back up content. Protect your WiFi network with a password and avoid using public computers or WiFi hotspots to access online banking or provide personal information.
- **Choose your passwords carefully.** Choose passwords that would be difficult for others to guess and update them regularly. A strong password should include a mix of upper and lower case letters, numbers and symbols. Don't use the same password for every account/profile, and don't share your passwords with anyone.
- **Review your privacy and security settings on social media.** If you use social networking sites, such as Facebook, be careful who you connect with and learn how to use your privacy and security settings to ensure you stay safe. If you recognize suspicious behavior, clicked on spam or have been scammed online, take steps to secure your account and be sure to report it.
- **Beware of any requests for your details or money.** Never send money or give credit card details, online account details or copies of personal documents to anyone you don't know or trust. Don't agree to transfer money or goods for someone else: money laundering is a criminal offence.
- **Be wary of unusual payment requests.** Scammers will often ask you to use an unusual payment method, including preloaded debit cards, gift cards, iTunes cards or virtual currency such as Bitcoin.
- **Be careful when shopping online.** Beware of offers that seem too good to be true, and always use an online shopping service that you know and trust. Think twice before using virtual currencies (like Bitcoin) - they do not have the same protections as other transaction methods, which means you can't get your money back once you send it. Learn more about online shopping scams.