Summer Edition

From The Desk Of The CEO - Tom Murray

Re-opening

As the Provincial Government has recently announced their province-wide re-opening plans, so too does NDCU have branch re-opening plans in the works. Any NDCU changes will mirror the timelines and stages contained within the provincial guidelines outlined by the Public Health Office (PHO) last month.

The first change of significance will be to our in-branch service hours:
• Effective July 5 (providing the Provincial Government adheres to their timeframes) we will be open 10:00 am to 4:00 pm.
  o Monday to Friday in Nelson & Rossland,
  o Tuesday, Wednesday and Thursday in Crawford Bay. With Monday and Friday employees offering remote service
• Other changes to our internal Safety Plan, such as mask wearing and branch occupancy capacity, will occur as PHO changes are allowed.

What an experience the past 16 months has been! We are looking forward to less restricted interactions with our members, employees and communities as we enter the summer season.

Please continue to email and phone us for support – we've become very adept at meeting our member needs without the requirement to make a trip down to a branch (although sometimes unavoidable!).

With society moving to more online transactions, we are seeing an increase in fraud attempts against our members. Some important reminders to safeguard yourself:
• Never open attachments or click email links that you didn't expect to receive.
• Never enter your passwords or provide login information for any accounts over the phone or via email.
• Never share your personal information or passwords with anyone by email or phone, especially when not expected.

• Use anti-virus software to keep your computers clean from malware.
• Register for Alerts for online banking and Credit Cards.

It pays to be suspicious – there are some bad actors out there who don't think twice about taking advantage of people. Always contact us if transactions are uncertain or require support adding Alerts.

Your credit union successfully held its 70th Annual General Meeting virtually in April, and I had the chance to review our strong 2020 financial performance with our members. And since the AGM, we're pleased to let you know that we have added two new Directors to our Board:
• Zoe Creighton will fill a Nelson area seat for 1-year term
• Cam Stokes will fill the East Shore area seat for 1-year term.

Welcome aboard Zoe and Cam!

Hope you all have some downtime this summer and a chance to re-charge with family and friends.

Our Branch Hours Are Changing!

We are OPEN

10 - 4
Monday - Friday
in **Nelson and Rossland**

We are OPEN

10 - 4
Tuesday, Wednesday and Thursday
on the **East Shore**, to serve members
in-person, and from 10 - 4 on Monday and
Friday, offering remote service.
*providing the Provincial Government adheres to their timeframes

Protect Yourself

Connecting online has never been easier. You can talk to your grandchild across the country, buy things from around the world or play games with your friends no matter where they are. But if you're active online, you need to make sure that you're being cyber secure with all your online activity.

Multi-factor authentication, VPN's, network security, phishing…all these things can impact your cyber security. But being cyber safe doesn't have to be as complicated as you think. Strong cyber security practices can help limit your screen time to what's important. We're here to help with a few simple things you can do to start making your online activity secure.

Protect your online activity

A breach of any of your accounts can have huge impacts, such as your identity being stolen by cyber criminals. The consequences can be even more serious if you're using the same password for multiple accounts. If your password from one account is stolen, someone can then use it to access any of your other accounts that also use that password. Having strong and unique passwords for each of your accounts can help keep your information safe.

If you're having a hard time keeping all your accounts and passwords organized, a password manager can remember your login information and keep it secure. Some password managers can even help you generate strong and unique passwords for each account and have handy auto-fill options. However, even though it may be convenient, we don't recommend that you use the auto-fill options within your web browser or on your mobile phone.

It's also important to run software updates regularly to keep your devices and applications secure. A great way to do this is to enable automatic updates for all your software. Automatic updates do exactly what the name suggests: they install updates on your devices and software as soon as they become available. This ensures your software has the latest protections in place. Once you turn automatic updates on, you won't have to worry about them anymore and you'll stop receiving those pesky notifications.

These resources provided by the Government of Canada
https://www.getcybersafe.gc.ca/

Watch out for scams

Online scams try to steal your personal data. These scams often look like they come from an official source, such as Netflix, the Canada Revenue Agency or even someone you know personally. It's important to know the signs and watch out for them, so you don't fall victim to an online scam.

Keep an eye out for the red flags of a phishing scam, like a misspelled email address or threatening language in the email body. Phishing scams, a common type of cyber crime, are cleverly designed to trick victims into revealing information they otherwise wouldn't, like credit card numbers and passwords. If anything seems off in an email, link or website, it's best to double check and make sure it's legitimate. You can verify the email's sender through the contact information on their official website instead of clicking on it in the email.

Install anti-virus software

You can use some cyber security tools, like automatic updates, to put your mind at ease and protect your data. Anti-virus software is another tool that you can install to help keep your online activity safe. Anti-virus software scans your device for viruses and harmful malware.

When downloading and installing anti-virus software, you need to make sure that it comes from a legitimate and reputable source. Scammers will try to trick you into believing you're downloading anti-virus software when it's really a virus that will infect your computer. Never click on any ads or links that offer anti-virus software for free, and never download anything unless you know it's safe. It's best to do some research to find the right software for you and then go directly to the vendor's website to download it. Once you've installed anti-virus software and enabled automatic updates, you can rest a little easier knowing that your online activity is more secure.

Conclusion

Being active online means there's lots to explore and discover. While you're enjoying everything the internet offers, it's important to browse safely and make cyber security part of your online activity. This may seem like a big task, but the simple cyber security tips described above make a difference, will help protect you online and will ensure your personal data is safe. And you can get back to spending your time online doing the things you enjoy.