From the Big Chair

It is often said that watching the news on television is depressing. Recently I was watching the suppertime news and was beyond depressed; I was disturbed. The story was about technology being used to capture a snippet of a conversation by a performer. Using the technology, that snippet was then used to create a song by that artist, one that the artist never recorded. The related Music Association was upset by this and was calling for this misuse of technology to be stopped immediately. As the CEO of the local credit union, this story disturbed me as it drove home two training sessions I participated in recently. The sessions were all about cyber-crime and the many ways it can be carried out – phishing, compromising accounts, hacking, artificial intelligence (AI), pretending to be someone else, scamming, harassing, and coercing, to name a few.

The reason I was disturbed by the news story was it highlighted how careful we need to be as a financial institution. Throughout their history, local credit unions have been proud of the fact that "we know our members". As our memberships increase and our members use our services in new ways, "knowing our members" becomes more difficult. If we serve our members using technology and not as often in person, we lose that personal connection including knowing members' voices. If technology can now "dub" voices, we can no longer rely on that avenue as we have done in the past. I remember an incident where I was asked to describe a member who was trying to complete a transaction at another institution. At the time, I asked the service rep to let me talk to the member on the phone as I would be able to recognize her voice. I am not sure we will have that luxury anymore.

So what does all this mean? How does it affect you as a member? What does it mean for employees of the credit union?

With new staff, and staff being new to the community, we may not know you like we did when we had longer term staff. Regardless of who is serving you, we have an obligation to protect the privacy of your information and to protect your funds from fraudsters. If we do things differently than we have in the past, we ask you to understand our reasoning and not be insulted or upset by the changes. We are doing things differently in order to protect you and your funds. If we ask to see identification when you come into the branch, it may be because we do not know you, like we did in the past, and we want to ensure you are you. If we ask you a series of "security" questions when you phone in, we are ensuring we are talking to you and not a hacker. If we ask you about your transaction, we are wanting to be sure you are not being coerced into doing something you do not normally do. If you wire money, we will ask questions to ensure you are not sending funds to a scammer. If we receive text or email instructions from you to complete a transaction, do not be surprised if we contact you using phone numbers we have on file to ensure you are the one requesting the transaction and not a fraudster. If we regularly ask you to verify your address, email and or phone numbers, we are wanting to ensure we have correct and up-to-date contact information in case we need to get in touch with you if we ever have concerns about your accounts or transactions.

On a daily basis, we receive reports of members across the country being hacked, scammed, compromised, taken advantage of or being pressured to do something they would not normally do. We used to say "buyer beware" and "if it seems too good to be true, it probably is". These cautions apply today more than ever due to the ways members can be misled and encouraged to part with funds for all types of fraudulent reasons. The "bad guys" are good at what they do. The ability to scam large sums of money away from unwary members gives them plenty of incentive to be good.

To help protect yourself from cyber-crime, we recommend:

- Use caution when opening unknown, unfamiliar or unusual emails.
- Do not click any links in emails you were not expecting.
- Do not allow anyone access to your computer and/or online banking applications.
- When in doubt, take time to think about what is being asked of you. If still in doubt, contact a family member, neighbour or friend that you trust to discuss the situation or call Unity Credit Union directly.

If you are being asked to send money to someone you do not know or are unsure of, consider if you would send money to someone you know who lives down the road if they called and asked you to send them money right away. If you wouldn't send funds to someone you know, why would you send money to someone you do not know and who is pressuring you to send it right away, especially if they call you repeatedly about it?

Cyber security is a significant concern. Institutions need to be aware and take steps to protect their members and their member funds. But members need to be aware and protect their funds as well. We are in this together. We need to work together. For that reason, we ask for your patience and understanding if we ask you more questions than we have in the past, regardless of how you do business with us. We would love to still rely on "knowing our members", but the risks have increased and so we must change to do what we can to protect you.

Vigilant but Concerned,
Gerald Hauta
Chief Executive Officer

UNITY Credit Union

Unity Credit Union
120 - 2nd Avenue East
P.O. Box 370
Unity, SK S0K 4L0

Phone: 306-228-2688
Fax: 306-228-2185

Monday - Friday
8:30 a.m. - 4:30 p.m.

www.unitycu.ca
Email: info@unitycu.ca