prairie payments
JOINT VENTURE PORTAL

Updated November 3, 2023

Be Cyber Aware!

We are seeing an increase in the number of sophisticated phishing scams out in the financial services industry nationally (large banks and credit unions are experiencing similar issues) where threat actors are requesting that clients/members reset their passwords due to suspected fraud on their account, then compromising this login information. It's important that members are cyber aware of threat actors and all actions they use (phone scams, phishing etc.).

Cyber security is everyone's responsibility!

Remember the following to keep yourself protected:

- *All members are reminded to always pay critical attention to URLs. Ensure you are always using the correct URL for any banking services or other financial transactions that are done online.*
- *Do not communicate or keep a copy of your usernames and/or passwords for any of your financial services (or other secure logins) in your email account. A common way of gaining illegitimate access to a secured account is through the discovery of sensitive information within a compromised email account.*
- *Enable multi-factor authentication (MFA) on your email account, if available, for an added layer of security – for example, so you are prompted to enter a security code sent to your phone whenever you attempt to login to your email from a new device.*
- *Be very cautious of unsolicited emails asking for your login credentials and never click on a link to login from an email you were not expecting.*
- *Even if an email appears to be coming from a legitimate sender, if it involves making changes to login or banking information, verify the legitimacy with the sender via another communication method (e.g., phone call).*
- *Always log out of your secure accounts, such as online banking, when using public or shared computers or devices. If possible, avoid using public wi-fi for sensitive activities.*