SECURE
Your Online Accounts

Being aware of fraudulent techniques and taking preventive measures can significantly reduce the risk of your personal information being stolen.

USE STRONG PASSWORDS more than eight characters in length and containing a combination of capital letters, lowercase letters, numbers, and at least one symbol. Don't use passwords that can be easily guessed such as birthdates, phone numbers, addresses, children's or pet's names, etc.

REGULARLY UPDATE YOUR PASSWORDS and security questions (at least once per year).

NEVER USE THE SAME USERNAME OR PASSWORD TWICE, as it could allow a fraudster to access multiple accounts just by compromising one.

NEVER USE YOUR EMAIL ADDRESS AS YOUR USERNAME unless it's required.

DON'T WRITE YOUR PASSWORDS DOWN on paper or save them in your phone's notes application, a word document saved on your computer, or in your computer's browser.

CONSIDER USING A PASSWORD MANAGER, an application that can store all your usernames and passwords, making it easier to maintain different usernames and passwords for each of your accounts. Which password manager you use is a personal decision; information can be found online to help you select the one that's best for you.

NEVER SHARE YOUR USERNAMES AND PASSWORDS with anyone including family members, friends, co-workers, supervisors, and financial advisors. Your financial advisors should never need to access your personal online account.

ALWAYS REGISTER ONLINE ACCOUNTS ASSOCIATED WITH YOUR FINANCIAL PRODUCTS.

- **Take full advantage of all security measures** offered with your online account(s).
    - **Always enable Multi-Factor Authentication (MFA)**, a security feature that requires multiple forms of verification to confirm a user's identity. A common MFA method is the use of a one-time passcode (OTP). OTPs can be codes sent to your phone or email after you enter your password when logging into an online account or be obtained using an Authenticator Application loaded on your phone or computer.
    - **Never provide your OTP to anyone** unless you initiated the call or transaction.

ALWAYS SIGN UP FOR TRANSACTION ALERTS that send you a text or email when an update is made to your account or a transaction is requested.

REPORT SUSPICIOUS ACTIVITY IMMEDIATELY if you receive any transaction alerts, a password reset, an account lockout notification, or notice any account updates or changes you didn't request.

1013-2024

LIMRA LOMA
Navigate With Confidence