RBC Dominion Securities Inc.

Wealth Management Matters

Wealth Management
Dominion Securities

March 2019

Chinner Wealth Management Group

RBC Dominion Securities Inc.

Dennis Chinner, FMA
Vice President & Investment Advisor
dennis.chinner@rbc.com
403-317-4308

Sylvia Chinner
Associate Advisor & Financial Planner
sylvia.chinner@rbc.com
403-317-4322

Tania Tytula
Associate
tania.tytula@rbc.com
403-317-4316

410 – 7th Street South
Suite #202
Lethbridge, AB
www.dennischinner.com
1-800-555-6789

*Please contact us if you would like more information about the topics discussed in this newsletter.

We are all concerned about the safety of our personal and financial information. RBCDS Chinner Wealth Management employs rigorous security and technological safeguards, and **you can help too**. Here's how!

Top 10 tips for safe computing and online privacy:

1. Protect your personal information.
Do not respond to unsolicited requests for confidential information.

2. Choose effective passwords.
Choose passwords that are difficult to guess but easy for you to remember. Use multiple passwords, and change them frequently.

3. Verify a message before you take any other action.
Do not click on a link, call a phone number, wire money or take any requested action unless you have first verified that the request is legitimate. Verify it using information from a source other than from within the message itself.

4. Limit the online information that you make available about yourself.
Be careful about including personal information online, on social networking sites in chat rooms and in unencrypted email as fraudsters may try to get at your information for their own benefit.

5. Be cautious in your online activity.
Use caution when accessing new sites.

6. Be wary of pop-up windows.
Don't click on any action buttons within a suspect pop-up window.

7. Maintain a suite of security software products.
This should include a reputable personal firewall, anti-virus, anti-spam and anti-spyware, all necessary to provide online protection for your computer and your information.

8. Keep your computer healthy.
Take advantage of automated updates for your computer or regularly check the applicable websites for required software patches and updates.

9. Remember to log off.
Ensure you properly log off and close your browser to prevent others from being able to view your information later.

10. If it looks too good to be true, it probably is!
Be cautious of emails and websites that promise incredible deals and monetary windfalls.

10 tips to safeguard your assets

1. Keep your personal information safe.
An identity thief will pick through your garbage or recycling, so be sure to shred receipts, copies of credit applications, insurance forms, etc.

2. Keep personal information confidential.
Do not give out personal information on the phone, in an email or over the Internet unless you initiated the contact and know who you're dealing with.

3. Be aware of billing and statement cycles.
If your bills or statements don't arrive on time, follow up immediately to ensure they have not been fraudulently redirected. Request electronic statements.

4. Protect your mail. Bring in your mail daily.
Forward or re-route it if you move, change your mailing address or are away.

5. Protect your PIN and passwords.
Do not reveal your PIN or passwords to anyone, including employees of RBC, family and friends. Always shield the keypad when entering your PIN.

6. Limit your risk.
Sign all credit cards as soon as you receive them. If they are lost or stolen, report it immediately.

7. Unusual transactions.
Beware of "too good to be true" or unexpected offers or requests such as, "You've inherited a large sum of money. To claim it, send us a deposit first." Never agree to conduct financial transactions on behalf of strangers.

8. Review your transactions.
Regularly review your financial statements to ensure that all transactions are authorized, and report any missing or fraudulent ones. Review your credit bureau file annually.

9. Limit your exposure.
Only carry credit cards you use. Don't carry your birth certificate and social insurance card when you don't need them; instead keep them in a safe place.

10. Contact the authorities.
If you suspect you are a victim of fraud or theft, contact the authorities immediately.

Common Fraud Scams

Romance Scam – fraudsters present false romantic intentions toward a victim in order to gain their trust and affection. They do this to obtain the victim's money or access to their bank accounts or credit cards. Most romance scams begin via social media sites or online dating sites. *Exercise caution with any admirer you meet or reconnect with via social media.

Grandparent Scam – fraudsters contact potential victims posing as a family member in urgent need of cash. *Always take measures to verity the requestor's authenticity before you forward any money.

Bank/CRA information Scam – fraudsters send a text or email requesting you verify your information. This information could then be used to commit fraudulent activity in your name. *Visit rbc.com/privacysecurity to learn more about how to spot email scams. **Financial Institutions and CRA will never request your information via email or text message.**

THANK YOU!

Tania, Wesley & the PeeWee AA Lethbridge Hurricanes White would like to say thank you to Dennis & Sylvia at Chinner Wealth Management for their support this year. Wesley and his team had a great season!