Protecting Online Investment Accounts

In today's world, it seems like an increasing number of day-to-day businesses we deal with are moving to online billing and account services and away from paper. This is no different in the financial world. While some of my older retired senior clients complain about this shift, it is important that we adapt to the changing world and how we interact with the world, while protecting ourselves. Here are the biggest cybersecurity mistakes clients may make with their investment account when working with their investment advisor:

Not using strong passwords

Clients often use weak, easily guessable passwords to access their investment accounts. They may also reuse the same password across multiple accounts, leaving their sensitive financial information vulnerable to hackers. If having multiple passwords is a challenge for you, consider using a password tracker/keeper app that will make your passwords easily accessible without having to guess what they are or reset them each time you forget one.

.

Failing to enable two-factor authentication

Many clients neglect to enable two-factor authentication on their investment accounts, even when their advisor recommends it. Two-factor authentication adds an extra layer of security beyond just a password

Two-factor authentication (2FA) provides a robust layer of security for clients' investment accounts by requiring two distinct forms of identification before granting access. The first factor is typically something the user knows, such as a password or PIN, while the second factor is usually something the user possesses, like a smartphone for receiving a verification code. This dual-layer approach significantly enhances account security, as even if a hacker manages to obtain the password, they would still need the second factor to gain access. This second factor can still be defeated however, if for example, the user phone is hacked while using public Wi-Fi without VPN protection (most common is while client is on vacation), another reason to avoid public Wi-Fi.

Oversharing sensitive information

Clients sometimes send their advisor payment details, account numbers, or other sensitive information over unsecured channels like regular email. This makes the

information more susceptible to theft by cybercriminals. As many people do use regular email when discussing confidential issues with their advisor, it is better to delete it after and copy / paste important conversations with date / time into a word document (back up all data in the event your computer crashes). The same should be done with online bills you receive in your email (save as a PDF then delete from email).

Regularly update software and apply patches

Keep your computer's software, including security software, up-to-date and apply updates promptly. **Be cautious with emails**

- Be wary of unsolicited emails asking you to click a link or download an attachment, even if they appear to be from a trusted source. Hover over links to check the URL.
- Never enter login credentials or provide sensitive information in response to an email. Contact the company directly if you have concerns.

Use antivirus protection

- Install reputable antivirus and anti-malware software on your devices to detect and block malicious programs.
- Set the software to automatically scan for threats and update its virus definitions regularly.

Monitor account activity

- Regularly review your investment account statements and transaction history for any suspicious activity.

Be cautious on public Wi-Fi

- Avoid accessing sensitive accounts or conducting financial transactions while connected to unsecured public Wi-Fi networks.
- Use a VPN to encrypt your internet traffic, especially when using public Wi-Fi (definitely try to avoid).

Here's how VPNs can help protect investment clients from cybercrime

Encrypt sensitive data and prevent phishing attacks

VPNs encrypt all data transmitted between a client's device and the investment firm's servers. This makes the information unreadable to hackers even if they intercept it, preventing theft of login credentials, account numbers, and other sensitive data.
VPNs can help block phishing emails that try to trick clients into clicking malicious links or entering information on fake websites. The VPN obscures online activity and prevents access to known phishing sites.

By following these basic cybersecurity best practices, investment clients can significantly reduce the risk of falling victim to phishing, malware, and hacking attempts targeting their accounts. Ongoing vigilance and proactive security measures are key to protecting sensitive financial data.

If you want to explore post retirement goals aimed at creating healthy and balanced financial strategies, please contact me at wwoo@researchcapital.com

Wei Woo, Investment Advisor, CIM, EPC
Research Capital Corporation,
Private Client Division
3481 Allan Dr. SW,
Edmonton, AB
T6W -3G9
Cell : 780 – 299 – 0760
Office : 780 – 460 – 6628