CAPITAL MARKETS
HAYWOOD

CLIENT NOTICE – RISK OF EMAIL FRAUD

Cybersecurity threats continue to compound the risk of financial crime and fraud perpetrated on financial institutions and their clients. The sophistication of cybersecurity threat actors continues to increase as do their costs to those affected.

There are multiple methods threat actors use to gain access to electronic devices and email accounts in search of information to commit financial crimes. We strongly encourage our clients to review the information offered at the Government of Canada Get Cyber Safe website for important information about cybersecurity threats and how you can protect yourself from such threats.

If a threat actor accesses your personal information, they will use that information to try to access your investment and bank accounts. Through methods known as social engineering, spoofing and phishing, the fraudster will try to impersonate you over the phone or email, and to trick your financial representative in the execution of transactions and the withdrawal of funds from your investment and bank accounts.

Haywood Securities has implemented security protocols that are designed to protect our client accounts from cybersecurity threats. These protocols include ways and means our Registered Representatives will verify the authenticity of the instructions they receive on client accounts. To ensure the best protection of your Haywood investment account, a team effort between you and your Registered Representative is required. If you are the target of a cybersecurity event on your electronic device or email account, we ask you to immediately contact your Haywood Registered Representative so we may take the necessary actions to safeguard your account.

If you have any further questions on the above, please contact your Registered Representative.