Client Notice – Risk of Email Fraud

Cybersecurity threats continue to be a concern of financial institutions and their clients. The sophistication of cybersecurity attacks continues to increase, as do the costs related to these attacks.

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

Threat actors could use your personal information to seek access your investment and bank accounts. Through methods known as social engineering, spoofing and phishing, fraudsters may 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.

Middlefield Capital Corporation has implemented controls designed to protect client accounts from these cybersecurity threats. To ensure your Middlefield investment account remains protected, we require a collaborative effort between your Registered Representative and accountholders. If any of your electronic devices or email accounts are the subject to a cybersecurity attack, we ask you to immediately contact your Middlefield 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.