Royal Canadian Mounted Police | Gendarmerie royale du Canada

May 7th, 2027

Cranbrook Chamber of Commerce,

This letter is to advise the Chamber of Commerce and its membership of a fraud trend currently targeting businesses using corporate email systems, particularly Microsoft 365 portals.

Our detachment is currently investigating multiple incidents involving the same method of fraud and is concerned that further victims may exist but have not yet reported losses.

Overview of the Fraud

In the incidents reported:

- Cybercriminals gained unauthorized access to a business's Microsoft 365 email portal, including accounts protected by two-factor authentication.
- Once access was obtained, the fraudsters sent emails from the legitimate business email address to that company's clients.
- These emails requested payment of outstanding invoices but directed the funds to a different bank account than normally used.
- The fraudulent emails appeared legitimate, as the perpetrators had access to accurate invoice information and exact payment amounts.
- Email replies from clients were intercepted or re-routed, preventing the business from seeing the responses and delaying detection of the fraud.

Because the communications originate from trusted email addresses and contain correct billing details, recipients often have no immediate indication that the request is fraudulent.

Important Warning to Businesses and Clients

Any request to change payment instructions or redirect funds to a new bank account should be treated with caution and independently verified before payment is made.

Recommended Verification Steps

Before sending payment to a different account:

- Verify the request by calling a trusted and known contact at the business using previously established contact information.
- Do not rely solely on email for confirmation of banking changes.
- Where possible, verify the request in person.

Protective Measures for Businesses

- Inform staff and clients about this fraud trend.
- Implement internal controls requiring verbal or in-person confirmation for all banking or payment changes.
- Regularly review email security settings, access logs, and forwarding rules.
- If suspicious activity is identified, contact your financial institution immediately and report the matter to police.

The Cranbrook RCMP encourages Chamber members to share this information within their organizations and with clients where appropriate. Increased awareness and verification remain critical in preventing financial loss. We will be sending out a media release to the public as well.

Businesses that believe they have been targeted or victimized by this type of fraud are asked to report the incident to the Cranbrook RCMP via our non-emergency line.

Please do not hesitate to contact our Community Engagement Coordinator, Kristin Galanov, should you have any questions or require assistance.

Sincerely,

S/Sgt. Darren Kakuno
Acting Detachment Commander, Cranbrook RCMP
250-489-3471
cranbrookrcmp@rcmp-grc.gc.ca