



BUSINESS EMAIL COMPROMISE & SOCIAL ENGINEERING

How cyber criminals exploit trust and what your business can do to help reduce risk

Business Email Compromise (BEC) is one of the most common forms of cyber fraud affecting businesses today and can result in significant financial losses. Rather than relying solely on technical vulnerabilities, these attacks often exploit trust, human behaviour, and business processes by impersonating trusted individuals such as executives, vendors, clients, lawyers, or accountants. The goal is often to redirect payments, obtain sensitive information, or gain access to business systems.

Canadian authorities continue to report significant losses from BEC and spear phishing incidents, and experts believe actual losses may be substantially higher due to underreporting¹.



COMMON BUSINESS EMAIL COMPROMISE TACTICS

Cyber criminals continually adapt their methods, but common BEC schemes include:

- **Executive impersonation:** A fraudster poses as a senior leader and requests an urgent, confidential payment or transfer. These requests often create a sense of urgency and discourage verification.
- **Vendor payment fraud:** Attackers impersonate a supplier or contractor and provide “updated” banking details or remittance instructions, causing legitimate payments to be redirected to fraudulent accounts.
- **Payroll diversion:** Fraudsters impersonate employees and request changes to payroll or direct deposit information to divert funds.
- **Professional advisor impersonation:** Attackers may pretend to be lawyers, accountants, or investment advisors to encourage unauthorized transfers or disclosure of sensitive information.

Other social engineering techniques

Business email compromise is often supported by broader social engineering tactics², including:

- Phishing, spear phishing, smishing (text message phishing), and vishing (voice phishing)
- QR-code and document-sharing scams

- Advanced phishing attacks designed to capture passwords and authentication information
- Fake consent requests and email rule manipulation used to hide fraudulent activity or redirect communications

Watch for warning signs

- Requests involving urgency or secrecy
- New banking or payment instructions
- Requests to bypass normal approval procedures
- Messages that contain unusual language, tone, formatting, or grammar
- Requests received while a contact is travelling, unavailable or difficult to verify

PRACTICAL ACTIONS TO HELP REDUCE RISK

Strengthen payment and payroll controls

Strong internal processes can help prevent BEC-related losses. Consider:

- Verifying all banking or payment changes by calling a trusted phone number already on file
- Requiring dual approval for significant transactions and account changes
- Implementing a maker-checker process for vendor and payroll updates
- Establishing documented procedures for payment changes and wire transfers

Use multi-factor authentication (MFA)

MFA remains one of the most effective controls for reducing unauthorized access³. You should consider enabling MFA for:

- Email accounts
- Banking applications
- Cloud services
- VPN and remote-access tools
- Administrative accounts

Finance personnel, executives, and IT administrators should consider stronger phishing-resistant MFA methods where available³.

Strengthen email security

Because BEC often begins with email compromise, you should evaluate your email security controls. Key measures include:

- Implementing email authentication controls such as Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting and Conformance (DMARC) to help verify legitimate senders, and reduce the risk of phishing, and email spoofing

- Reviewing forwarding rules, delegated email access, and email security settings regularly
- Monitoring unusual email account activity, messaging behaviour, and sign-in activity, including logins from unfamiliar locations, devices, or times of day.

Educate employees

Many BEC incidents succeed because they appear legitimate. Awareness training can help your employees recognize and respond to suspicious activity. Training should focus on:

- Payment fraud schemes
- Payroll scams
- Phishing attempts
- MFA fatigue attacks
- Impersonation tactics
- Suspicious links and attachments

Maintain strong cyber hygiene

Strong cyber hygiene practices can help reduce exposure to a range of cyber risks, including fraud, ransomware, and email compromise. Key practices include:

- Using strong and unique passphrases
- Keeping operating systems and software up to date
- Deploying antivirus or endpoint detection and response (EDR) solutions
- Limiting administrative privileges
- Performing regular vulnerability reviews
- Encrypting sensitive data
- Maintaining secure, regularly tested backups, to help protect critical data and support recovery from cyber incidents. This may include cloud-based, offline, immutable backups that cannot be altered or deleted without authorization, helping organizations recover more quickly from ransomware attacks.
- Testing backup restoration procedures regularly

If you suspect fraud, act quickly

Prompt action may help reduce the impact of a cyber incident and financial losses. Consider:

1. Contacting your financial institution immediately to attempt a payment freeze or recall
2. Resetting potentially compromised credentials and MFA settings
3. Reviewing email accounts for unauthorized forwarding rules or access

4. Reporting the incident to the appropriate authorities, including the Canadian Anti-Fraud Centre and the National Cybercrime Coordination Centre (NC3)
5. Validating vendor and payment information before resuming transactions

HOW WE CAN HELP

Northbridge Insurance offers cyber insurance solutions and Cyber Assist services designed to help businesses **strengthen their cyber resilience** and **prepare for potential incidents**. Eligible customers also have access to tools such as vulnerability scans, self-assessments and incident simulations.

For more information on making your business safer, contact our Risk Services team at **1.833.692.4111** or visit us at **www.northbridgeinsurance.ca**.



Northbridge Insurance, Northbridge Insurance Logo and Risk Insights are trademarks of Northbridge Financial Corporation, licensed by **Northbridge General Insurance Corporation** (insurer of Northbridge Insurance policies). This Risk Insight is provided for information only and is not a substitute for professional advice. We make no representations or warranties regarding the accuracy or completeness of the information and will not be responsible for any loss arising out of reliance on the information.

¹ Royal Canadian Mounted Police (RCMP), 2025;

² Canadian Centre for Cyber Security, Government of Canada, 2024-2025;

³ Canadian Anti-Fraud Centre, Government of Canada, 2025. [5078-001-ed04E | 09.2026]