Business Email Compromise (BEC):

The Costly Scam You've Never Heard Of

Cybersecurity threats make headlines every day, but some of the most damaging attacks don't involve malware or ransomware. Instead, they rely on simple deception. One of the fastest-growing and most costly cybercrimes today is **Business Email Compromise (BEC).**

What Is Business Email Compromise?

BEC is a form of cybercrime where attackers impersonate a trusted person—like a CEO, CFO, vendor, or supplier—through email. Their goal is simple: **trick an employee into sending money or sensitive information.**

Instead of breaking into systems, fraudsters exploit human trust and routine business processes.

How BEC Works

Fraudsters use several tactics to carry out BEC scams:

- **Spoofed Emails**
  Attackers send messages that appear to come from a trusted executive or partner, often with minor changes in the email address that go unnoticed (e.g., john.smith@company.co instead of john.smith@company.com).
- **Compromised Accounts**
  Criminals gain access to a legitimate email account and use it to send convincing instructions internally.
- **Social Engineering**
  Scammers research company structures, employee roles, and supplier relationships, then use this information to craft highly targeted emails.

Common Scenarios

- **Invoice Fraud:** A fake invoice from a "vendor" with new bank account details.
- **CEO Fraud:** An urgent request from the CEO to transfer funds immediately.
- **Payroll Diversion:** Fake HR requests to change direct deposit information.
- **Data Theft:** Requests for employee tax forms or sensitive customer records.

The Bottom Line

Business Email Compromise is not about technical hacking—it's about **tricking people.** That's why awareness, verification, and proactive security measures are key.
At Teleco, we help businesses safeguard their email systems and train employees to recognize scams before the damage is done.

Why BEC Is So Dangerous

- **No malware needed** — traditional security tools may not detect it.
- **Exploits human trust** — employees want to be helpful and follow instructions.
- **Financially devastating** — wire transfers are often irreversible once sent

How to Detect BEC Attempts

Employees should be trained to spot red flags, such as:

- Unexpected requests for payments or sensitive data.
- Urgent or secretive instructions from executives.
- Slight variations in email addresses or domain names.
- Requests to bypass normal approval processes.

Steps to Prevent BEC Attacks

- **Enable Multi-Factor Authentication (MFA):** Protects email accounts from being taken over.
- **Employee Training:** Regular awareness programs on phishing and email scams.
- **Verification Procedures:** Always confirm payment or data requests via a separate channel (phone call, in-person, secure chat).
- **Email Security Tools:** Deploy advanced filtering and domain monitoring solutions.
- **Incident Response Plan:** Have a process in place if a suspicious email slips through.

teleco.ca
sales@teleco.ca

One Partner. One Call. Work securely with Teleco.

1-800-465-3933