COMPUDATA.CA
What IT can be.

EFT & Wire Fraud Scams are on the Rise.

Tips to help reduce your risk.

What is EFT & Wire transfer fraud?

EFT and Wire transfer fraud occurs when company employees are deceived by fraudsters to send money to a bank account controlled by scam artists.

Cybercriminals typically will use phishing emails to gain insight or access into their target's email account, monitor email correspondence for some time, mimic behaviours and leverage trusted relationships between individuals. The fraudsters will use language that might be specific to the person or the company they're targeting, with invoices and emails often identical to a real one except for the banking details.

Tips on how to prevent EFT & wire transfer fraud:

1. Do not trust emails requesting wire transfers or changes to existing payment accounts. Exercise extreme caution even when a request comes from the email of an existing vendor or trusted contact such as an employee. Confirm email requests by a verified phone or video (Teams/Zoom) call, in case their email has been compromised. Be wary of e-mail-only wire transfer requests involving urgency.
2. Develop a policy and approval process for changing electronic payment accounts within your organization. Compudata has a free MS Word template available for download: https://compudata.link/eft-auth
3. Contact us about setting up Cybersecurity and Phishing Training for your staff. This training can also help with your Cyber Insurance renewal.

Thank you for your business with Compudata.

Please contact us anytime, we are here to help!