



CYBERSECURITY: EMAIL FRAUD

We've all received junk emails. Buy this. Save that. Click here. While these emails are fairly easy to spot in most cases, law enforcement reports that for every million pieces of junk email sent, roughly 8 people will fall victim to the scam. Not a bad return for a low-cost undertaking from the bad guys point of view.

Like any business however the bad guys are always looking to increase their return on investment. Introducing "CEO Fraud" or Business Email Compromises as the FBI terms it.

These are emails sent by criminals made to look like they are coming from the CEO, other executive or a Director on the Board. The goal is to fool an employee, typically in accounting or HR, into sending wire transfers or providing confidential employee tax information.

The variations of this scam are endless. In Atlantic Canada, a popular version of the scam saw hackers sending email to staff asking them to obtain Gift Cards on behalf of the CEO. Often these emails said the CEO was about to go into an important meeting and not to call and disturb them.

One case I'm familiar with saw email sent out to specific company employees just weeks before Christmas. The Boss was just about to go into a meeting and needed the staffers help on a secret mission to run to the store to pick up some Amazon Gift Cards, fifteen \$100 cards, to be given out as Christmas bonuses to staff.

Unfortunately, one of the staffers fell for it and only realized their mistake after the scammer asked him to scratch off the back of the cards and provide the numbers by email so the CEO could award the "Christmas Bonuses". Calling the Boss to make sure he was providing the correct numbers; he discovered the request was fraudulent and was now out \$1500.

The loss could have been worse. MacEwan University in Edmonton was defrauded \$11.8 million after a staffer fell for a similar trick. Law enforcement reports variations of this scam has netted the bad guys approximately \$2.3 billion, and that is just in reported losses. The number has been estimated to be closer to \$26 billion by some.

Education is key to combatting Cyber Crime. Make sure your staff are aware and alert to such threats. Put a policy in place that staff are to call the reported sender of the email, no exceptions, BEFORE transferring funds or sensitive information, or your organization might become the next victim.

Scott Beck is CEO of the fast-growing cyber security & IT Services firm BeckTek in Moncton New Brunswick. He's a two-time international best-selling author and award-winning speaker, including appearances at NASDAQ and Harvard Club of Boston. Co-star of the Amazon Prime documentary "Cyber Crime", Scott is a frequent celebrity guest expert with appearances on NBC, ABC, Fox and Glob

