off with just a little social engineering and a rudimentary knowledge of technology. But there's good news – simple accounting controls can go a long way in ...

Sep. 15, 2015

Late last month, the FBI issued a warning about business e-mail compromise (BEC) scams that it said have been responsible for $1.2 billion in fraud globally in just the last couple years. Also known as "CEO fraud," this type of scam is surprisingly easy for criminals to pull off with just a little social engineering and a rudimentary knowledge of technology. But there's good news – simple accounting controls can go a long way in helping to prevent your company from becoming the next victim.

There are many ways cyber con artists can execute e-mail scams, and they generally involve assuming someone else's identity. Not any identity, but often the identity of a

person or an organization (or both) that the target would have a reason to believe.

Submitting fake invoices are a common tactic. This could be a real vendor submitting invoices for services never delivered, or a con artist assuming the identity of a real vendor.

And fake invoices can be responsible for significant losses. Did you read the story about how Citi paid $400M in fake invoices at its Mexican subsidiary?

These types of scams are extremely simple to perpetuate – add a few line items to a real invoice, or simply send in an invoice from a legitimate sounding business. Lather, rinse, and repeat. Each year, thousands of businesses fall victim to these scams, and they are often prevented with simple financial controls.

Assuming the Boss's Identity

Another form of e-mail scam exploits the inherent respect that employees often have for a senior person within the company – say the CEO. No complex hacking or other technical wizardry needed: a fraudster simply has to change the "From" address in their e-mail client, and voila! It appears that the urgent request to wire funds (*"now!"*) comes from an important person in the organization. They'll send an email to a CFO, someone else they've identified in the finance department, or maybe even an employee at a company's accounting firm with a quick and simple questions to see if someone takes the bait. Something like, "What do you need from me to send a wire transfer?"

Since the victim of the scam believes they're communicating with their boss, they aren't likely to ask many questions in return. Before long, fraudsters are providing bank account information (usually of intermediate "money mules" and directing the victim to make a significant money transfer.

These scams sound too easy to actually work, but history proves that they do.

Trusting, competent professionals, and their companies, have fallen victim. For

can be just as easy to protect against. From an accounting perspective, a slight procedural change to how payments are approved could go a long way towards ensuring that your company or your client is not the next victim.

Well known practices like segregation of duties and dual payment approvals really work to prevent large losses. It should be a standard practice to ensure that large invoices and payments require dual controls. And simple as they might seem, many organizations whiff when it comes to the consistent use of these controls. Confirming approvals and payments by e-mail unfortunately is not a best practice – e-mail is after all the way in which the fraudsters exploit trusting individuals!

Adding extra processes is never an ideal solution – it creates more work and slows down a company's ability to process AP. But not having these controls is unconscionable! Most growing organizations know this, but are simply reluctant to take the medicine necessary to keep the disease at bay. Most organizations that have taken the steps to implement robust financial controls know that they are well worth it to avoid the risk of becoming the next victim of a business e-mail compromise scam.

A little bit of skepticism is a good thing in any finance-related profession. Especially when it's this easy for thieves to assume a boss or colleague's identity based on what they learn from corporate sites, social media, or news organizations.

Whenever an email seems suspicious, knowing to look for things like a fake invoice, spoofed address, or hacked account is a good first step to stopping these types of email scams. But $1.2 billion in fraud proves that these thieves are very good at going undetected. Accounting organizations need redundancy in place that can help stop them.

———

BC Krishna is President & Chief Executive Officer of MineralTree, which makes mobile and