Commercial Bank

The Evolving Threat of Email Scams

Look-alike and hacked emails are helping fraudsters steal billions of dollars. While awareness is growing, the scams are also evolving and there are a few common misconceptions that are leaving businesses vulnerable.

Nic White
Global Head of
Fraud Prevention,
Citi Commercial Bank

For the last five years, companies around the world have been suffering from a fraud scheme known as a Business Email Compromise (BEC). The scam sees a cybercriminal pose as a known business contact and send a forged email requesting their victim to make a payment to a new beneficiary. While the attacks may sound simplistic, more than $12.5 billion in fraud losses have been attributed to this type of fraud globally,[i] making BEC the most lucrative form of cybercrime seen to date.

During a typical BEC attack, a cybercriminal will use a hacked or look-alike email account to impersonate an Executive within your company or one of your existing suppliers. Before they send the email, the attacker will spend many months studying your business, so the timing, content and tone of the message will often appear normal.

Because these types of attacks have been around for a few years, awareness of the scam has increased, and businesses have started to strengthen their defences. But as businesses have evolved, the scam has too, and fraudsters are changing their tactics to try to avoid detection. Here are three of the most common misconceptions about BEC, which are based upon earlier versions of the scam:

1. Executive impersonation is the primary risk
During the early years, most BEC cases involved the attacker impersonating a CEO, CFO or another internal Executive. While this threat has not completely gone away, the overwhelming majority of BEC cases now see the attacker pose as one of your existing suppliers. As you already make regular payments to your vendors, the attacker no longer has to convince their victim of the need for the payment, they simply need to create a good reason for the payment to be sent to a new bank account.

2. The emails will be unsolicited and easy to spot
Many people assume that a BEC attempt will arrive via a new email request, much like cold calling over the telephone. While this may previously have been true, the attackers now try to intercept and manipulate an existing email conversation, rather than initiating a fresh request. In the supply chain scenario, the attackers will hijack an email about an existing order (regularly after the down-payment has already been made) and then ask that their payment details be updated.

3. The attackers will try to avoid prolonged dialogue
In the Executive scenario, the fraudsters would often send a single payment request, together with a reason why they couldn't be contacted – such as being in an important meeting or about to board a flight. These standalone (and normally ad-hoc) requests often looked suspicious and so the fraudsters have started to refine their approach. It is now common to see numerous emails between the fraudster and victim, which are designed to build rapport, develop the cover story and even create the opportunity for a second or third attempt. In the supplier scenario, we have even seen cases where the fraudster is having simultaneous conversations with both the supplier and buyer (in both cases impersonating the other party), which allows them to gather additional information, answer any questions and improve the credibility of the request.

While the attacks have continued to evolve, the most effective controls to combat BEC have remained consistent. If you want to protect your business, there are three simple steps which will help reduce your susceptibility to an attack:

1. Call Backs – If you ever receive an email requesting a payment to be sent to a new beneficiary, pick up the telephone and call the sender back to confirm the request. It's important to use a previously known telephone number, rather than using any numbers that are given in the body/signature of the email.

2. Dual Approval – Whenever you need to add a new payee, or change existing payment details, configure your systems to require an approver/checker. An extra set of eyes significantly improves your chances of spotting anything untoward.

3. Training – Ensure your staff is aware of risk. Most people have naturally good instincts, but need to understand what BEC is, before they are able to look out for it.

If you suspect you have fallen victim to BEC, contact your Citi Service Representative as quickly as possible so we can help to protect your account and attempt to recover any lost funds. Your security is our priority.

Click here to see an infographic about BEC

[i] https://www.ic3.gov/media/2018/180712.aspx

1758628 10/18