CFO | Daily News

3 COSTLY MISCONCEPTIONS ABOUT BIZ EMAIL COMPROMISE

3 COSTLY MISCONCEPTIONS ABOUT BIZ EMAIL COMPROMISE

An accounts payable clerk for a southern manufacturer receives an email from her CEO urging her to wire funds to a vendor immediately. She complies (it's her CEO after all!) and wires the money to the account info provided.

This company just fell victim to the classic business email compromise (BEC) scam, right?

Not anymore.

There are some potentially costly misconceptions floating around about BEC – and being unaware of them paints a huge target on your company's back.

Take a look at three of the biggest mistaken impressions about BEC today to help your finance department sidestep a costly loss.

MISCONCEPTION 1

How rampant BEC really is... and what it costs

The FBI estimates that BEC cost U.S. companies $1.2 billion last year is nothing to sneeze at for sure. And it certainly serves as a good motivator to be vigilant.

But it turns out it's more like three times that number.

A recently released ***analysis*** by the U.S. Treasury Department estimates BEC costs companies $301 million a month, which would mean more like $3.6 billion in 2018.

And plenty of your peers are getting hit. The Treasury Department says an average of 1,100 businesses fall for this scam each month.

Those numbers should really open some eyes for anyone in your organization who might think a BEC scheme is only a remote possibility for you.

If the FBI can underestimate the toll this fraud is taking on businesses, you can bet that's happening in companies as well.

Use these updated numbers to impress upon everyone from the rest of the c-suite to your front line finance and accounting staffers that the stakes are too high not to devote the time and effort to training, email security factors, etc.

MISCONCEPTION 2

Manufacturing and construction are the main targets

While any company could fall victim to a BEC scam, some industries have felt the brunt more than others. For example, manufacturing and construction accounted for one-quarter of all BEC scams in 2018.

But the targets are shifting.

The report shows that several new industries are being hit hard by BEC, including real estate and commercial services (shopping centers, entertainment facilities and lodging).

First and foremost, this reminds us that anyone is vulnerable. It also underscores how threats are ever-evolving: As one target becomes more aware, and therefore harder to fool, crooks will shift gears quickly.

MISCONCEPTION 3

The primary route in is through a spoofed exec

That goes for the way in, too. This has been considered classic BEC since the fraud came to light: an email posing as the CEO or CFO directs a lower-level employee to urgently move money.

Only trouble? Turns out that's no longer the primary way in.

These days, a phony invoice purporting to be from a legitimate supplier is the No. 1 start to the scam.

The reason: Because it's working! The average transaction amount for BECs impersonating a vendor or client invoice is $125,439, vs. $50,373 when impersonating a CEO, according to the Treasury report.

That's largely because no one's associating that approach with BEC, so more employees are falling for it.

Time to update staffers' vision of what BEC looks like today now … before your money goes out the door.

CFO | Daily News