KeyBank
Use the red key.

Cybersecurity Threats: How Companies Can Protect Against Wire Fraud

The term “cybersecurity threats” conjures images of IT systems being brought to a standstill and corporate data being expropriated and misused. There’s another type of cybercrime, however, that’s pretty close to regular crime: wire fraud.

While we’ve all heard of cases of consumers being scammed into wiring money to fix non-existent IRS bills or pyramid schemes, such scams dupe a surprising number of corporate executives as well.

According to Core Title, “The FBI claims that the number of wire fraud scams reported by title companies spiked 48%” in recent years.

Countering such schemes relies on employee education, some safeguards and new policies for dealing with wire transfers. The solution isn’t complex, but it requires a firm commitment and follow-through.

How scams work

Wire fraud hinges on a fake identity. Fraudsters usually figure out how to spoof a company email address and other ID markers or figure out a password and hack into the real account of a CEO or upper management executive within the company. They might also impersonate a trusted vendor. If they have access to emails, they might learn to mimic the writing style of the person they are pretending to be. Tell-tale signs of hacking, like misspelled words and poor grammar, aren’t as common as they used to be, so these emails can be very convincing. Close scrutiny might reveal that the hacker has made subtle changes in the email address, like substituting a country domain for “.com.”

Once the fraudster has convinced the recipient that they’re actually the CEO or another executive, then the impostor asks for a wire transfer, which might be for an urgent matter or merely to pay a vendor. Sometimes the scammer poses as a longtime supplier and sends a phony invoice with instructions to send payment. They might also up the ante by calling to ask why they haven’t received the money yet and take advantage of disruptions in the calendar during three-day weekends. Companies that work with suppliers abroad and regularly wire them payments are particularly susceptible to this type of scam. To make matters worse, insurance often doesn’t cover wire fraud. If a business loses money, it has no way to recoup it.

Remember, if the email asks for personal information, includes a too-good-to-be-true offer, or closes with an odd salutation it may be a phishing scam. When it comes down to it, if something doesn’t feel right, don’t act on it.

How to fight wire fraud

Unlike other types of cybersecurity threats, wire fraud is more of a con than a direct attack. As with other types of cons, the best way to counter wire fraud is to educate employees that such attacks exist. Changing company policy to get more than one sign-off on a wire transfer can also help defend against wire fraud, especially if employees are trained to be skeptical about communication around wire transfers.

Communicate to your staff that they should exercise extra care when handling sensitive information and be careful not to click on any suspicious links.

Additionally, companies can closely monitor every wire transaction the company makes and execute random in-depth reviews to look for any fraudulent transactions.

Depending on the number of wire transfers a business regularly sends, it might be advisable to check every wire transfer request by placing a phone call (using the number on file) with the intended recipient to verify the request. Finally, companies may opt to discontinue wiring money on all occasions and opt for more secure methods of transferring money.

While that's an extreme measure, this is a case where such measures are warranted. As the rate of wire fraud attempts keeps increasing, companies need to do all they can to protect themselves.

Let's talk about your business.

For more information on KeyBank's capabilities, contact your KeyBank Relationship Manager.

KeyBank
Use the red key.®