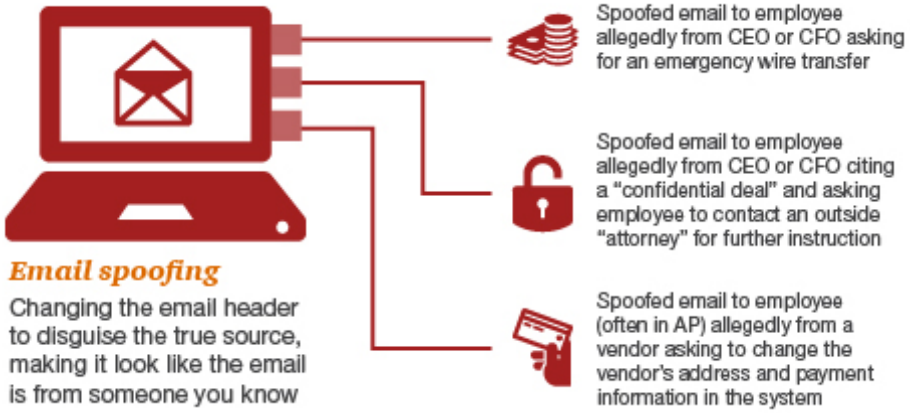
Stop! Did your executive really request that wire transfer?

What you need to know

- An increasing number of companies are falling victim to wire transfer scams, costing victims more than $1 billion in just the last 18 months (per the U.S. Secret Service).
- Scams are being perpetrated through fake emails from senior executives of the company or phony vendor emails.
- Public and private companies of all sizes have been affected by this type of scam. Companies with international business dealings are more likely to be targeted since transfers to overseas banks wouldn't be out of the ordinary.
- Strong IT, treasury, and purchasing controls can help protect company assets.

Understanding emails scams and educating key employees is critical

Scammers are successfully targeting companies with an email scam that leads to wire transfer fraud. Here are some common methods:



Other versions of this scam may use malware installed in the system via an employee clicking on a compromised website link that is emailed to them (phishing), though this method is less common. Whatever the method, employees—especially those who have the authority to request, approve, or execute wire transfers—need to be on guard.

pwc

Training employees to identify spoofing, phishing, and similar techniques can protect against these schemes.

Why is this scam so successful?

The people perpetrating these frauds frequently research employees' responsibilities so they know who to target, and often gather information to try to make the wire transfer request as believable as possible. For example, they may research the executive's schedule using public information or by making inquiries of the executive's assistant with the goal of sending the fraudulent emails when the executive is out of town and cannot be easily reached for verification.

Although some of the fraudulent requests are for millions of dollars, they can just as often be for smaller amounts. Since many companies have stricter controls (like dual approvals) for amounts over a certain dollar threshold, the scammers often submit requests for lower amounts hoping the looser controls will raise the success rate of their scam. If the scammer is successful in a preliminary request, they may continue to submit additional requests until the scam is detected.

Prevention is key since recouping stolen cash is rare

Once funds have been wired, recovering the stolen funds may be possible if the scam is detected within the first 24 to 48 hours, and often only with the help of law enforcement. Controls can help stop these scams in their tracks: IT controls that keep the scammer out of the system, purchasing controls that validate changes in vendor payment information or the setup of new vendors, and treasury controls that require multiple approvals of wire transfers. But a culture that encourages a questioning mindset is also important, especially when it comes to investigating requests from executives that are unusual or unexpected. Encouraging (or requiring) the receiver of a wire transfer request to confirm its validity via phone (using a number they know to be valid, not one that was included in the email) can go a long way toward protecting the company's assets.

What to do if you suspect your company has been scammed

Contact your local FBI or U.S. Secret Service office immediately to report a "business email compromise" scheme. Also contact both your financial institution and the receiving financial institution to request that they halt or unwind the transfer. Seek advice from counsel about any legal obligations or protections you may have related to this situation, such as potential insurance coverage for any loss. Finally, change your controls to minimize the risk of something similar happening again, and don't think you need to sweep it under the rug. Making sure that employees know about the scam, how it was perpetrated, and that they can be a gateway for the scammer is important in motivating employees to remain vigilant.

In the loop

Executive-level insight into today's top financial reporting and regulatory issues

How PwC can help

To have a deeper discussion of how to protect against business email compromise, please contact:

Kristin D. Rivera
415-498-6566
kristin.d.rivera@us.pwc.com

Todd C. Ranta
214-754-4513
todd.c.ranta@us.pwc.com

Beth Paul
973-236-7270
elizabeth.paul@us.pwc.com

For more information
Visit our Forensics webpage at:
www.pwc.com/us/forensics

For more accounting and financial reporting developments, visit www.cfodirect.com