OLD NATIONAL BANK

Wire Transfer Scams—Don't Get Hooked!

IMPORTANT PHISHING INFORMATION

- An increasing number of companies are falling victim to business email compromise scans, with the average per-wire transfer loss exceeding $80,000 per attack.[1]
- 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 and purchasing controls can help protect company assets.

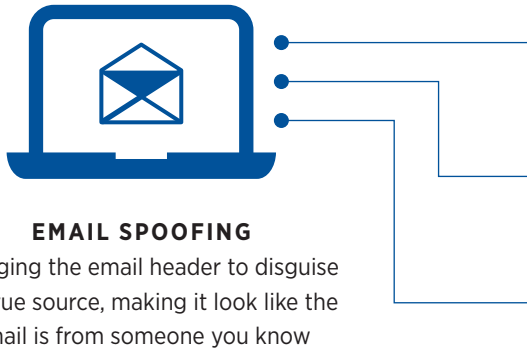
Prevention is key. Recouping stolen cash is rare.

Controls can help stop these scams in their tracks. Promote a culture that encourages a questioning mindset, especially when it comes to investigating unusual or unexpected requests.

1. **STOP** before you click. Ask yourself "Is **ANY** part of this email suspicious?"
2. **BE SUSPICIOUS OF...**
   - Urgent requests
   - Unfamiliar/Unusual requests
   - Links in emails
   - Pop up ads
   - Requests for password changes
   - Unsolicited email with attachments
3. **DO NOT CLICK ON** pop up ads or links/attachments in suspicious e-mail.

Understanding emails scams and educating key employees is critical.

Scammers are successfully targeting companies with email scams that lead to wire transfer fraud. Common methods include:



EMAIL SPOOFING

Changing the email header to disguise the true source, making it look like the email is from someone you know

Spoofed email to employee allegedly from CEO or CFO asking for an emergency wire transfer

Spoofed email to employee allegedly from CEO or CFO citing a "confidential deal" and asking employee to contact an outside "attorney" for further instruction

Spoofed email to employee (often in AP) allegedly from a vendor asking to change the vendor's address and payment information in the system

Whatever the method, employees—especially those who have the authority to request, approve, or execute wire transfers—need to be on guard.

Why is this scam so successful?

Those committing these frauds frequently research employees' responsibilities—they know who to target and often gather information to make the wire transfer request as believable as possible. *Example: The executive's schedule is researched using public data or making inquiries of the executive's assistant with the goal of sending fraudulent wire requests when the executive is out of town and cannot be easily reached for verification.*

Some fraudulent requests are for millions of dollars but they are often for smaller amounts. Many companies have stricter controls (like dual approvals) for amounts over certain dollar thresholds so the scammers often send lower dollar requests hoping the looser controls will raise the success rate of their scam. Once a preliminary request is successful, they may continue to submit requests until detected.

[1]*Source: "Phishing Activity Trends Report", Anti-Phishing Working Group, 2020, www.apwg.org*