You can guard against wire fraud when you can see it coming.

Spectrum®

What is fraudulent wire transfer?

This happens when two banks transfer funds due to a fraudulent electronic communication. And it occurs when a scammer pretends to be a trusted source, like a vendor, company or family member, and requests an immediate transfer of money.

Digital connectivity has helped make your business more efficient. And it's created convenience for your customers. But with fewer in-person interactions, verifying a person's identity can be a challenge. And that's opened the door for more cyber crime, such as wire fraud. According to The Deposit Account Fraud Survey Report, bank deposit accounts are the target of more than $1B in wire fraud attacks every year.[1] The threat to businesses is real.

Examples of Actual Fraudulent Wire Transfer Events

Rerouting: A company uses Microsoft's remote desktop protocol (RDP) to connect to the systems of a branch location. However, it didn't have the right security in place, so their system could be accessed by anyone on the internet. In other words, they left the door open. This made it easy for a cyber attacker to exploit a vulnerability and get into the company's finance records and monitor their email. The attacker saw that a large wire transfer was going to an overseas manufacturer. He changed the bank information for the manufacturer in the company system. More than $1.5M was sent, or rerouted, to a fraudulent account. No one knew there was a theft until the manufacturer called looking for their money.

Fake Check for Return Payment: A scammer sends you a fake cashier's check, personal check or money order with instructions to cash the check and send the money back. The check is often accompanied with a congratulatory letter advising you've won a prize, are the beneficiary of an inheritance or have an offer to work from home. Sometimes, the check is for something you're selling online. Generally, the check amount is for more than what the scammer is asking in return. This is explained by advising that the overage is a processing fee, or the difference is an error. These checks are fake and shouldn't be cashed.

Direct Deposit Information Update Request: A business gets a request via email to change direct deposit information for a supplier. The request looks legitimate, so the change is made. Once the business starts depositing funds, it finds out the new account isn't their supplier's account.

Fraudulent Communications Request for Automated Clearing House (ACH) Transfer: A scammer emails a business a series of fraudulent invoices, changing the routing numbers on the invoices and bills of lading. The business doesn't see a small change in the email address the invoices originate from. They make multiple automated clearing house (ACH) payments, which total thousands of dollars, to a fraudulent account.

Confirmation Code Before Withdrawing Funds: If you're asked for a confirmation code or a money transfer control number (MTCN) to access money that was wired to you, it's a red flag that the request is fraudulent.

Unexpected Request for Wiring Money: Scammers are skilled at making you believe your relatives are asking for money. A scammer may call from a familiar phone number and disguise his voice claiming to be sick or use an email address or name you recognize. They could also use information from your social media account to try and convince you the request is real. Calls from the IRS are also often scams. Fake IRS representatives will threaten you with arrest or other consequences if you don't pay them. If you think you might owe money to a government agency, contact the agency directly to confirm.

Phishing Attack to Access and Control an Internal Email Address:
The loan officer at a bank was targeted as part of a phishing scam.* With access to the loan officer's computer, a scammer was able to create fraudulent fund transfer requests and bank approvals.

* Phishing is a type of social engineering. An attacker sends a fraudulent message to trick a person into revealing sensitive information or to deploy malicious software on the victim's infrastructure like ransomware.

What can you do?

Start by checking out our Fraudulent Wire Transfer Best Practices here.

Contact your agent today.

The Hartford

[1] The Deposit Account Fraud Survey Report, released in 2017, by the American Banking Association (ABA).