Understanding Wire Fraud

How Does it Work?

Email based wire fraud is becoming an increasingly ubiquitous problem for many businesses. Wire fraud is attractive to criminals because funds sent via wire are quickly available for withdrawal after the request is processed. The FBI reported that from 2013-2016, more than $2.3 billion was lost to wire fraud[1]. This is a conservative estimate since only a small fraction of cases get reported.

Wire fraud generally happens in two ways.

The first way is for the cybercriminals to gain access to an email conversation with a common vendor a company uses. They will then make an email address that is almost identical to that of the vendor, but usually with one added or transposed character. For Example, instead of being John@SteelBolts&Screws.com, it might be John@SteelBolts_&Screws.com. Then they send an email to someone at the company with payment authority and request payment of a fake invoice. It will have specific wire instructions and request immediate payment, usually under the guise of avoiding late charges. By the time, the company figures out that the invoice was fake, the money is already gone.

The second way is for the criminals to gain control of an executive level email account such as that of a president or CEO. Once they have access, they will send an email to the payables clerk or CFO, telling them to wire

money to a new vendor.
Although both scenarios seem like they would be easy to catch, countless businesses fall victim to these scams every year.

It's important to understand that cybercriminals gain access to employee emails through targeted phishing attacks. The purpose of phishing is to obtain sensitive information, such as login and password information, in order to access an individual's protected data or company networks. This can be done by embedding a link in an email that takes an employee to a fake site which then prompts them to enter their personal data or by installing a trojan through a malicious email attachment.

Often, recipients of these emails are sent to a site that imitates a software provider of theirs and asks them to enter their password to update to the latest version. These are just a few of the ways phishing can pose a threat to your organization. With the advent of social media sites, it's even easier for them to know exactly who at a company to target.

Common Red Flags

Several things can alert you to potential wire fraud:

1. **Rush Requests** – Be suspicious of any wire request that claims to be an emergency or that needs to be processed as fast as possible to avoid late fees or surcharges.
2. **Abnormal Payment Details** – If your invoices with a certain vendor are always $400, and you suddenly get one for $7,000, then that's reason enough for suspicion. Be wary of anything that's highly unusual with what you've come to expect from a certain vendor. This could be an abnormal amount or instructions that tell you to send the money to a different account than usual.
3. **Unavailable by Phone** – If the person requesting the wire is unavailable by phone and insists only on using email communication. Often, scammers will say that they can't be reached by phone at that time but will assure you that they will call back to verify the transaction at a later time.
4. **Poor Grammar or Spelling** – Be on the look-out for inconsistent spacing and capitalization, strange spelling, bad grammar or awkward word choice. These are all warning signs.
5. **Incorrect Return Email Address** – Always carefully check the return email address to make sure it is legitimate. As stated before, it can be easy to miss if it's off by just one letter.

What Can You Do to Prevent Wire Fraud?

Although email-based wire fraud is a growing issue, preventing it is relatively simple. Here are the most pertinent things to help keep you safe:

- Train your employees to carefully inspect all payment request emails.
- Make sure that all your systems and IT security software are up to date.
- Have employees change email passwords regularly.
- Verify ALL wire requests by phone and implement strong wire verification policies.
- Implement dual controls with wires. Make sure it takes at least two people to carry out a wire transfer.
- Always validate any changes to payment instructions even if they come from an internal email.
- Consider placing restrictions on your bank account that limit which accounts wires can be sent to.

Since phishing attacks are generally what allow cybercriminals the opportunities to commit wire fraud in the first place, educating your employees on phishing and how to avoid it is also important. Here are some things to consider:

- Make sure you have a security policy that includes password expiration and complexity.
- Educate your employees on how to recognize phishing emails and conduct regular training.
- Deploy a web filter to block malicious websites.
- Use a SPAM filter that can detect things like viruses and blank senders.
- Use security products which send test phishing emails to employees and managers to see how well they respond to them.
- Consider investing in cybersecurity liability insurance.
- Install browser add-ons and extensions which can prevent employees from clicking on malicious links.
- Remember that no legitimate website will ever ask for your login/password via email.
- Never click a link in an email. Instead, type the address directly into the address bar.
- Use a short phrase as a password (longer is better) instead of just a few characters.
- Always mouse over links to see if the URL that pops up matches that text of the link.

Cybercrime will almost certainly be a threat to your business at some point. Now is the time to strengthen your company's cybersecurity policies so that you are protected.

Don't Become a Victim

Even the largest companies aren't immune to cyber attacks. In 2013, Facebook and Google fell victim to a massive payment scam that ultimately cost them $100 million. Target fell victim to their now infamous data breach just a year before.

It's important to remember that every employee you have is a potential vector for an attack. If you have 300 employees, then you potentially have 300 different weak points. Your business doesn't have to be a victim. With the proper employee education and procedures in place, you can keep your self from falling victim to this growing threat.

If you feel you have been the victim of wire fraud, please call us at (800) 330-9890 or contact your nearest branch.

[1] "FBI Warns of Dramatic Increase in Business E-Mail Scams." FBI, FBI, 9 Aug. 2016, www.fbi.gov/contact-us/field-offices/phoenix/news/press-releases/fbi-warns-of-dramatic-increase-in-business-e-mail-scams.