Best Business Practices to Prevent or Reduce the Risk of Wire Transfer Fraud

Article
Amundsen Davis Cybersecurity & Data Privacy Alert
June 14, 2023

Cyber fraud has been around as long as the internet itself, but cyber criminals are more sophisticated than ever. While any experienced email user can spot a phony "Nigerian Prince" a mile away, even the most vigilant businesses are vulnerable to business email compromise (called "BEC") attacks by the new breed of internet fraudsters.

A pattern we have seen repeated time and again is a "man in the middle" attack leading to a fraudulent wire transfer. In this scenario, the fraudster infiltrates an employee's email account, uses that access to learn when one business is about to make a large payment—or series of payments—to another business, and then sends bank information for the *fraudster's account* to the payer, pretending it is new banking information for the intended recipient.

Bad actors accomplish this email access in a variety of ways, such as a brute force attack in which a bot is used to try millions of possible passwords, or by using a "spoofed" email address to send a phishing email wherein the fraudster impersonates your legitimate business partner and forwards a malicious link. Regardless of how the bad actor obtains a foothold in the email system, the result is that the payer sees what appears to be a "simple" change in bank account information and sends payment using the bank account information for an account the fraudster has set up. The parties eventually figure out that the business expecting the payment never received it. You sent the money—just not to your business partner's actual bank account.

Frequently, by the time everyone figures out what happened, the funds have been transferred to a bank account in Eastern Europe or elsewhere. That means clawing the money back presents a real challenge. There is a small but developing body of law regarding how to allocate losses in scenarios like these, but the bottom line is that nobody "wins" except for the fraudster. The best way to minimize the losses from these kind of attacks is to stop them before they start.

Even with a robust cybersecurity system and other best practices, vigilance is necessary to avoid this kind of attack. What makes man-in-the-middle attacks particularly challenging is that you and your business could be a victim *even if*

PROFESSIONALS

Molly A. Arranz
Partner

Ronald Balfour
Partner

RELATED SERVICES

Cybersecurity & Data Privacy

Data Privacy in the Workplace

your email system is never infiltrated. If someone gains access to a business partner's system and uses that to communicate with your employees, you could unwittingly fall victim as well.

Fortunately, we have learned a few lessons along the way that we can pass along.

Best Business Practices to Prevent or Reduce the Risk of Wire Transfer Fraud

1. **Pick up the phone.** NEVER – EVER – rely on email alone when sending money. And **don't call the number on the signature block of the email.** No matter how confident you are that the bank account information you're looking at is legitimate, always confirm it with a phone call to the *known number* of your business partner before sending money via wire, and make sure your employees are trained to do the same.
2. **Implement technological protections.** While motivated cybercriminals can find holes in any system, there are certain protections you can implement to harden as many of those vulnerabilities as possible. Best practices in this regard include implementing multifactor authentication and requiring passwords to be complex in order to minimize the vulnerability to a brute force attack. Regular resetting of passwords—that cannot be "recycled"—is also a must. Providing a Virtual Private Network for employees to use if they need to work outside of the office should be required.
3. **Train your employees.** Even the most technologically-protected and sophisticated email system can be infiltrated through social engineering, where the fraudster tricks an employee into giving them access. Plus, employees may be checking emails on their handheld devices (where the text is even smaller) and/or responding to multiple emails a day. While employees are human and *will* make mistakes, mistakes can be minimized by training that emphasizes good cyber hygiene practices. Those practices include avoiding links from unknown accounts, confirming that communications are received from legitimate email accounts by viewing the full email address instead of relying on display names alone, and avoiding unsecured wireless networks. Coaching employees to "take a beat", i.e., to pause and think before acting, is a great strategy. Employees should be extremely wary of email communications that combine a sense of urgency and payment of monies, even if it appears to come from a trusted business partner, as this tone or tenor in an email is a favorite pressure point used by the bad actors.
4. **React quickly and contact law enforcement.** With man-in-the middle and other BEC attacks becoming more prevalent and clever, even the precautions outlined above may not be enough to prevent an attack. If your business has been the victim of this cyber incident, acting quickly is critical. Ensure employees know that escalating this issue immediately is highly valued so they don't react with embarrassment or attempt to sweep the misstep under the rug. Contact law enforcement and the rest of your incident response team to position yourself in the best way to find and freeze the funds that were transferred before they disappear forever. To avoid additional legal consequences, ensure your incident response team starts an investigation and ensures a clean environment. Along the same lines, make sure to have

an incident response team in place *before* the incident occurs – once it happens, there is no time to waste.

With more data being created every day, and more ways to access that data, credential theft and wire fraud are not going away anytime soon. It's important to take steps to minimize the risk of wire transfer fraud.

Best Business Practices to Prevent or Reduce the Risk of Wire Transfer Fraud