Texas Council Risk Management Fund

Fraudulent Transfers, Business or Vendor Email Compromise

Business Email Compromise (BEC), Vendor Email Compromise (VEC), and Fraudulent Funds Transfer (FFT) might not be the most common online crimes, but they are some of the most financially damaging because it usually involves a significant amount of funds. The emergence of Artificial Intelligence (AI) is also assisting bad actors with this type of attack. Often, the victim doesn't even realize AI was utilized so it never gets reported to claims that AI was involved.

What makes this kind of fraud particularly damaging for businesses is the fact that it's almost impossible to recover the funds that were stolen. The fraudster sets up fake accounts and exercises several money laundering techniques, and by the time an entity realizes they were spoofed, the money is long gone, and the bank accounts are closed. Any public entity, no matter if they're small or large, can fall victim to fraud like this.

A BEC or VEC represents one of the most common methods for executing fraudulent funds transfer. This kind of compromise usually starts with a social engineering attempt or a phishing attack wherein cybercriminals exploit human vulnerabilities to access a company's network. Once access is granted, the attackers can orchestrate fraudulent transactions, resulting in financial losses.

In a social engineering attack, the criminals assume the identity of one of the entity's executive staff to instruct an employee from the financial department to transfer money to their fraudulent account. They will send an email to the employee, urging them to transfer funds into the provided account. Without any process of next-level approval or confirming the transfer by another method first, an employee could take this email seriously and approve the transaction for processing.

Another common business email compromise scenario happens when the criminals steal login information for their victim's account through phishing attacks. The threat actors create websites and login pages that look authentic, where employees provide their credentials, unaware that they're being stolen, when attempting to log into their accounts. The criminals later use their stolen credentials to create fake invoices and send them to the entity's clients, who end up transferring funds into the fraudulent account the criminals provided.

These types of incidents do not typically involve costly data restoration, system recovery, business interruption or breach response efforts that are commonly required following ransomware attacks.

While ransomware continues to be a dominant risk, we are seeing tactics change, including the rise of other forms of extortion as well as business email compromise, vendor email compromise, or fraudulent funds transfer. This serves as a reminder to all

security leaders that cybersecurity is fluid, and attackers will shift their methods, even revisiting old tactics, so long as they continue to reap financial benefits.

Fraudulent Funds Transfer Prevention Steps to Take:

To prevent fraudulent fund transfers, you should:

1. Educate your employees on anti-fraud, social engineering, phishing, business e-mail compromise, and other related cyber scams on, at least, an annual basis.
2. Before processing a request, confirm the instructions via a method other than the original means of instruction first (i.e., if the instruction is received by email, call or walk down the hall and ask to confirm).
3. Avoid sending wire transfer details through email as it can easily be intercepted by threat actors.
4. Be cautious of anything that creates a sense of urgency or demands for immediate action.
5. Implement and enable Multifactor Authentication (MFA) for your organization, including on banking accounts to add an extra layer of security.
6. Use caution with new contacts and when dealing with new business partners or individuals requesting wire transfers.
7. Consider using dual control and ensure there are, at least, two people in the business transaction approval process.
8. Implement two-step verification to add an extra layer of approval such as verification of a driver's license or other means as proof of identity.
9. Verify the request by phone and call the recipient to confirm the wire transfer request before sending the funds. Be very cautious with phone numbers listed in an email.
10. Regularly monitor accounts and review bank statements along with online transactions to identify any suspicious activity.
11. Test your automated and online systems regularly to ensure they are in compliance.
12. Implement advanced security features that are offered by the bank such as transaction limits or alerts for large transfers.
13. Contact the bank immediately if you suspect a fraudulent transfer along with law enforcement.

The TCRMF Cyber Risk Services Advisor is ready to schedule Cyber Risk Assessments, Incident Response Plan Tabletop Testing visits, and Cyber Presentations for members. To get on the schedule, email Lee.Cain@sedgwick.com or call Lee at 512-619-1437.