Bank of Tennessee

Carter County Bank

Mountain Community Bank

CARTER COUNTY BANK AND MOUNTAIN COMMUNITY BANK ARE DIVISIONS OF BANK OF TENNESSEE MEMBER FDIC

Breaking Down Wire Fraud

There are countless ways criminals commit wire fraud. Is your company educated on the methods and protected?

The threat of businesses experiencing a financial loss due to wire fraud is growing each year. As a matter of fact, incidents of wire fraud nearly doubled from 14% in 2015 to 27% in 2015.

Companies across the globe lost more than $1 billion from October 2013 through June 2015 as a result of such schemes, according to the Federal Bureau of Investigation. The estimates include complaints from businesses in 64 countries, though most come from U.S. firms.

Companies of all sizes are at risk. According to the 2015 AFP Payments Fraud and Control Survey, 62% of U.S. companies reported that they were targets of payment fraud in 2014. The attack methods vary and are constantly evolving with the use of social engineering and technology. One of the first lines of defense to protect your company is to educate yourself on all the methods criminals use to gain access.

Attack Methods

Many times, employees use the same simple password combinations for multiple systems. So if the criminal is able to hack into an employee's email, chances are good that is the same password for the company's online banking system. Gaining access to email can give the criminal access to many entry points to initiate a crime.

Malware is a general term that includes viruses, spyware and other unwanted software that gets installed on your computer or mobile device without your knowledge or consent. These programs can be used to monitor and control your online activity. Criminals use malware to steal personal information and commit fraud.

Social Engineering is the act of obtaining or attempting to commit fraud by conning an individual into revealing secure information or perform an action.

Usually executed by email, phishing attacks start with an authentic looking email from a credible entity like a vendor or bank and ask the potential victim to provide sensitive information.

Criminals also use the phone and text message to solicit your personal information. The telephone version of phishing is called Vishing and Smishing refers to text messages. Vishing relies on "social engineering" techniques to trick employees into providing sensitive information that can be used to gain access to your company accounts.

Points of Compromise

Each of these entry points are at risk from being taken advantage of by any of the attack methods. Investing in the education and training of your employees is just as important as fire walls and other technology security measures and can help prevent your company from experiencing a substantial financial and reputational loss.

Wire Initiation Methods

The Attack Method that criminals use to gain access or information to perpetuate a crime doesn't mean they will use the same channel to initiate a fraudulent wire. After compromising an email account, they can use Social Engineering to convince an account to initiate a fraudulent wire, or they can obtain online banking credentials from a Call Center and initiate a wire transfer through the company's online banking system.

Common Fraudulent Wire Schemes

Wire fraud is a favorite of many criminals because companies usually use this channel to move large sums of money and, unlike a check, once initiated it is nearly impossible to reverse. Here are some examples of how criminals are able to defeat a company's security measures to steal from companies.

Live Chat with Customer Service

The criminal usually compromises an online banking account or email account of a company employee. They start a live chat session with the company's customer service department or accounting department and say they are having trouble sending a wire. The customer service agent believes the criminal is a legitimate employee. Even if the agent asks for additional information to confirm identity, sometimes the criminal has acquired enough personal information to answer the qualifying questions correctly.

Online Wire Request

The most common schemes start with a criminal compromising an online account and then disabling the security alerts or entering in a new phone number to defeat out-of-band authentication so the employees won't receive an alert that someone has accessed online banking. Then the criminal simply initiates a wire request.

Commercial Account Takeover

There are a couple ways that criminals can take over a commercial account and by pass dual controls that are set in place. The criminal can compromise an online banking administrator's account and create a new user with the authority to approve wire requests. They initiate the wire request from the admin account and then signs in as the "new" user and will then approve the fraudulent wire request. Another method is to gain access to the online banking system and modify the user privileges so that the criminal can initiate and approve wire requests.

Targeting Employees

Using a phishing attack on an employee, the criminal uses malware to gain access to the company's online banking or payment system. The malware allows the criminal to take over the employee's computer, giving him access to submit a wire transfer.

Fake Vendor Invoice

The criminal creates a fake invoice from a known vendor the company would be familiar with that includes payment instructions. If the vendor is one that has done business with the victimized company previously, the accounts payable department may not see or question subtle changes in the invoice and submits payment via wire transfer.

Treasury Management Department

Detra Cleven
Sr. Vice President
Treasury Mgmt Services
423.262.5486

Heather Steele
Treasury Mgmt Sales Officer
Middle Tennessee
615.321.9244

Rod Stent
Treasury Mgmt Sales Officer
Northeast TN / Western NC
423.262.4317

Elizabeth Cox
Treasury Services
Support Specialist
423.262.5487