Friday, May 5, 2017 / Volume 109 / Number 87

THE DAILY RECORD

WESTERN NEW YORK'S SOURCE FOR LAW, REAL ESTATE, FINANCE AND GENERAL INTELLIGENCE SINCE 1908

Title TRACK

Cybersecurity threats evolving to be more sophisticated

By DAVID GUTMANN
Daily Record Columnist

Unless you are not connected online or don't watch television, you know that cybersecurity is a huge problem these days. Anyone or any organization that has any type of sensitive data is susceptible to having that information stolen or compromised. Cybercriminals have a number of ways that they use to access that information. In addition, it's not just information or data that they are after, but your money, and they have a number of creative ways to take it from you.

Think of the movie "The Sting." It's a con job … only happening online. The crooks are out there trying to trick you into doing something that you wouldn't otherwise do. By now everyone has probably become at least somewhat familiar with the various types of cyber attacks and their terminology, i.e., malware, ransomware, phishing, spear phishing, etc. Below are a couple of the more highly used attacks, one of which has a new twist to it.

CEO fraud has become very common. The basic idea with this type of fraud is the attacker is pretending to be the CEO, or some other high-level officer, of a company and sends an email to an employee to trick them into releasing sensitive data or wiring funds. The employee being duped can often be another high-level officer such as the CFO or head of the HR department. Many of the reported cases have involved the transfer of funds via wire to the fraudster's account. The attack goes something like this.

Email from criminal posing as CEO to CFO:

"Phil, I need a favor. Vendor called me last night and complained that they haven't received payment yet on their latest invoice. He said that they wouldn't complete any more orders for us unless he gets his payment by 3:00 this afternoon. Will you please immediately wire $10,000 to his account below? I would take care of this myself but I will be stuck in meetings all day today. I will check with you when I get back in the office tomorrow."

The criminals at this point have already done their homework. They have researched companies online to find an appropriate company to target. They research the CEO and CFO or other employees that will be targeted, including searching social media. The attacks employ a sense of urgency. They also rely on the fact that the email is from the CEO, a trusted authority figure in the company. And they sometimes use a script of several emails back and forth with the targeted employee to make sure that they have bought into the scam. In order for the email address to look legitimate the criminals will often spoof the company's domain name, or use a slightly misspelled address that at quick glance looks the same (CEO@example.com will become CEO@examp1e.com).

The second type of attack has targeted real estate closing transactions attempting to obtain escrowed funds from a closing attorney or escrow agent. Once again the criminals have done their homework. They have become familiar with how real estate transactions work, and the various parties to (or involved in) the transaction. They have been able to hack into the email account of the attorney or escrow agent and have monitored email traffic waiting for the appropriate time to act. And they usually strike late in the day just before a weekend, and when possible, just before a holiday weekend. One scenario goes something like this:

A residential real estate purchase transaction occurs on a Friday. Late in the day the paralegal (Mary) at the lender's attorney's office gets an email from the criminal purporting to be the seller's attorney. The email says "Mary, my client just contacted me and asked if you could wire his proceeds to his new account. The wire instructions are below." Mary knows that she shouldn't rely on an email changing wire instructions at the last minute, so she calls the seller's attorney using his actual phone number from her file. Unfortunately, the secretary at the seller's attorney's office says that he has already left the office and cannot be reached as he is headed out of town for the weekend. Mary doesn't want to hold up sending the sale proceeds until Monday and makes the decision to wire to the new account. Naturally, on Monday she gets a call from the seller's attorney saying that his client called and is upset that he hasn't received his funds yet. Mary indicates that she followed the attorney's instructions for wiring to his

Continued on next page

Continued from previous page

client's new account. Of course, the attorney says that he never sent any such email.

This scenario is from an actual wire fraud case. It turns out that the criminal actually hacked into the seller's attorney's account and was able to use his actual email address. The dollar amount of the misdirected funds was in the neighborhood of $100,000. Ultimately, the seller's attorney and the lender's attorney split the loss.

The newest twist on the above fraud scenario is where the criminal calls the office that he just convinced to direct the sale proceeds elsewhere, posing as the receiving bank for the wired funds. The criminal indicates that the funds were wired to an account that the bank has flagged as suspicious, and assures the office that the funds will be returned within a few days. Often the caller ID is spoofed so that the call appears legitimate. The purpose is to prevent the closing office from contacting their bank after they discover the fraud, and possibly providing the criminal additional time to move the funds out of reach. Usually to an overseas account.

Cyber criminals are becoming smarter and more sophisticated. When faced with a situation that just doesn't seem right, verify. Do not rely on incoming phone calls as the caller ID can be spoofed. Initiate call-back procedures using phone numbers that you know are correct to verify information. Set up procedures and let parties know in advance that you don't allow changes to wiring instructions at the last minute. Be wary of any last-minute requests (especially late in the day on a Friday) that require immediate action or that have a sense of urgency. Make sure that your computer systems are up to date with the latest anti-virus software and firewall protections.

As they used to say every week on Hill Street Blues: "Let's be careful out there."

David Gutmann is Executive Vice President and Managing Counsel of Rochester Equity Partners, Inc., also operating as WebTitle Agency and Customized Lenders Services.