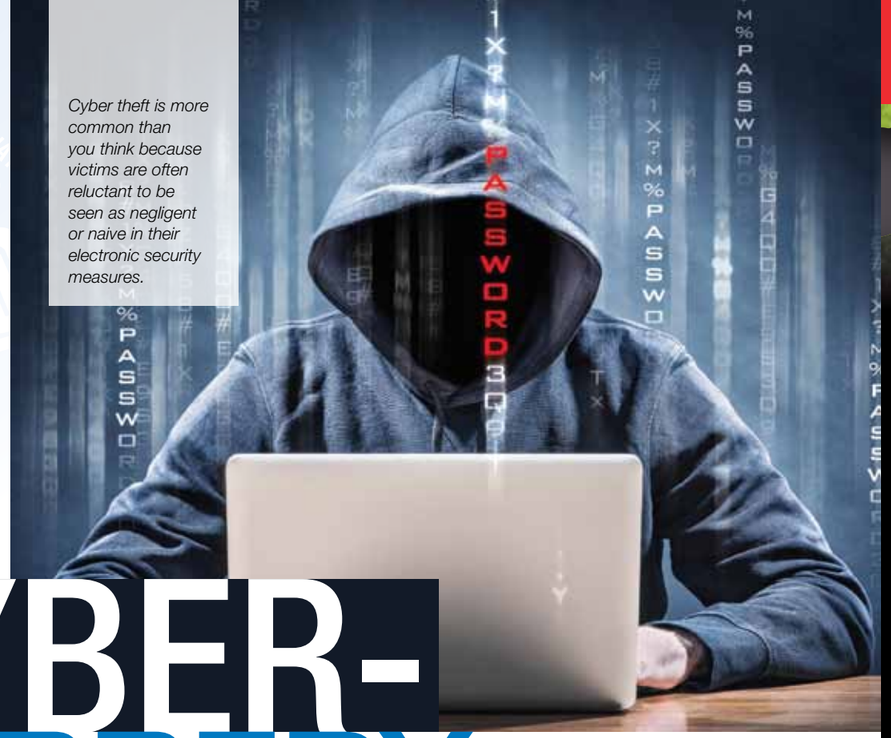

Cyber theft is more common than you think because victims are often reluctant to be seen as negligent or naive in their electronic security measures.

CYBER-ROBBERY

YOUR BUSINESS BANK ACCOUNT EMPTIED ELECTRONICALLY

by Robert. J. **Rebhan**

Criminal hackers can infiltrate just about any company, dropping bank accounts and other assault tools behind fire walls. After a three-day weekend, Connie Delgado logged into her bank's website from her desktop computer at the Phoenix business she owns with her husband. Payroll was due and suppliers needed to be paid. Suddenly she looked stricken. Her assistant Carole thought Connie was having a heart attack.

"Phone 911," Connie gasped. "We've been robbed."

Over the weekend, cyber thieves had cleaned out Phoenix Alloy's bank accounts to the tune of $60,000. They also tapped into Alloy's line of credit. The losses totaled $130,000.

Gathering her wits, Connie alerted her husband Dave, and then she called the bank. The bank manager told her that investigators would be on their way to the bank and also to Phoenix Alloy's office. They suspected Phoenix Alloy's computers had been compromised. Connie's correct bank account log-in credentials had been used to make the withdrawals.

REBHAN

MODERN BANK ROBBERY

The cyber robbery was something referred to as an "Account Takeover," and it has been happening frequently across the country. Merely using the office's computers for legitimate internet searches can open the electronic door to the criminals.

Connie began to have second thoughts about reporting the incident to the police. After all, her reputation was at stake.

Two things could take her down, she thought: Loss of the working capital and bad press. Her clients could flee, thinking their business or personal information might have been breached.

CONTINUED ON PAGE 78

WHEN AND WHERE

Robert J. Rebhan, international expert on identity theft and financial crimes, will explore the "Cyber Attacks & Business Data Protection" on **Sunday, Nov. 8** from **1:00 - 2:30 p.m.** and again from **3:00 - 4:30 p.m.**

PHOTO: FRANK PETERS

The bank had the same issue with the potential damage from publicity. They could deal with the monetary loss, but not the loss of confidence within the community. Like Connie, they felt it might be easier to fill in the financial gap than it would be to restore a good name. A decision was made on both fronts not to go public. Although computer crimes against businesses are common, they have gotten little media coverage because they are often hushed up by the parties involved.

A week after the theft, Connie and her husband negotiated a settlement with the bank. Some $70,000.00 had been recovered by shutting down transactions before the money left the country, but the rest of the cash had been successfully moved to a foreign account in Madrid, Spain.

The subsequent investigation revealed that the bank's system failed to recognize unusual transaction from Phoenix Alloy's accounts. And Phoenix Alloy's server, as well as every desktop, was riddled with spyware.

Connie and her husband walked from the bank with a 50/50 split. She felt relieved to get away with a $30,000 loss. Like most victims of the account takeover fraud, Connie and Dave knew their system administrator had failed them and it was of critical importance to reconfigure the office's computer security.

THE ULTIMATE PRIZE

In Phoenix Alloy's case, the malware's ultimate prize would be Connie's log-in credentials for the bank.

While the stealthware was working in Phoenix Alloy's office in Phoenix, criminal website developers in a place called Ramnicu Valcea, Romania, (referred to as "Hackerville" by Interpol and "Cybercrime Central" by others), were busy planning other aspects of the heist. They created a legitimate looking website that mimicked the site of a genuine worldwide charity.

In a setup that rivaled a Hollywood script, the thieves created the illusion they were the financial wing which processed funds for the global charity.

Back in the United States they started an advertising campaign, enticing people to respond to ads about work-from-home jobs. In the Phoenix Alloy case, they hired Barry Sands, who was living in Pensacola, Fla. He was one of more than more than 10 unwitting co-conspirators or "mules" who were part of the team selected to assist the international charity. As directed, Barry opened a new bank account and he started opening e-mail attachments

ALTHOUGH COMPUTER CRIMES AGAINST BUSINESSES ARE COMMON, THEY HAVE GOTTEN LITTLE MEDIA COVERAGE BECAUSE THEY ARE OFTEN HUSHED UP BY THE PARTIES INVOLVED.

MECHANICS OF THE STING

The investigation revealed that for many months, cyber thieves from Europe had been scheming to transfer Phoenix Alloy's financial assets to Rome. The robbers first penetrated when the one of the Phoenix Alloy's sales agents began searching for office supplies on his company computer. He unknowingly logged onto a legitimate website that had unknowingly been infected with malicious code, and this code stealthily infected his computer with malware.

The virus found a vulnerability to exploit in Phoenix Alloy's network and installed a program that allowed the criminals to remotely collect information on Phoenix Alloy and its employees. The rogue program attached itself to interoffice e-mails and thus began transferring from desktop to desktop. While blocking antivirus software updates, it enabled the thieves take control of every desktop, from his new employers. He was told he would be able to keep five percent of donation transfers.

Back at Phoenix Alloy, every keystroke made by Connie on her keyboard was captured by the cyber thieves. Eventually, they got the log-in credentials to Phoenix Alloy's bank account. All the pieces for the scheme were now in place. The fraudulent wire transfers began.

When Barry Sands received his first wire transfer into his new bank account, it wasn't a transfer from Phoenix Alloy. The first deposit of $4,000 was from one of several other businesses that had been compromised by the crime ring. Phoenix Alloy's money arrived the following day and just like the previous day, using the routing and account numbers provided by the thieves, Barry and the other mules, unknowingly pulled the trigger blasting currency through several accounts until the final deposits were made in Rome.

WHEN YOU POINT YOUR FINGER

Bank security and law enforcement officials call these slow and deliberate cyber assaults, "Advanced Persistent Threats." Behind the scenes, not only is the electronic mugging done with painfully tedious stealth, but banking officials and law enforcement are agonizingly slow to reveal to the public about just how bad the situation is.

When determining who is liable for this type of intrusion, courts have issued judgments for the plaintiff businesses, but sometimes judges have sided with the banks, citing, "Their security was commercially reasonable."

Experts like cyber security consultant Kashminder Chahil say that these persistent, lengthy, ***cyber account takeovers usually start with negligence or technical insecurity at the business***. "That can easily be fixed by choosing the right data security person," he tells his clients. He further recommended these steps to protect your business from cyber robbery:

- Reconfigure your office computing network to isolate sensitive functions and limit access to as few employees as possible.
- Ensure all systems and softwares are updated. Old software is easier to hack.
- Frequently change passwords.
- Educate your employees about cyber security.
- Keep financial accounts offline from other business operations.
- Ask your financial institution about additional protections they can provide. Keep in mind these services may come with added fees. CS

Robert J. Rebhan is an internationally renowned expert on financial crimes. He served 22 years with the Los Angeles Police Department and directed a fraud-prevention program for the American Express Company. He is currently a government agent.

At the request of the victims, the names of those involved in the incident have been changed.