



Powered by

## Cybercrooks stalk small businesses that bank online

By Byron Acohido, USA TODAY

A rising swarm of cyber-robberies targeting small firms, local governments, school districts, churches and non-profits has prompted an extraordinary warning. The American Bankers Association and the FBI are advising small and midsize businesses that conduct financial transactions over the Internet to dedicate a separate PC used exclusively for online banking.

The reason: Cybergangs have inundated the Internet with "banking Trojans" — malicious programs that enable them to surreptitiously access and manipulate online accounts. A dedicated PC that's never used for e-mail or Web browsing is much less likely to encounter a banking Trojan.

And the bad guys are stepping up ways to get them onto PCs at small organizations. They then use the Trojans to manipulate two distinctive, decades-old banking technologies: Automated Clearing House (ACH) transfers and wire transfers.

ACH and wire transfers remain at the financial nerve center of most businesses. ACH transfers typically take two days to complete and are widely used to deposit salaries, pay suppliers and receive payments from customers. Wire transfers usually come into play to move larger sums in near-real time.

"Criminals go where the money is," says Avivah Litan, banking security analyst at Gartner, a technology consulting firm. "The reason they're going here is the controls are antiquated, and a smart program can often get the money out."

Internet-enabled ACH and wire transfer fraud have become so acute that the FBI, which is usually reticent to discuss bank losses or even acknowledge ongoing cases, has gone public about the scale of the attacks to bring attention to the problem. The FBI, the Federal Deposit Insurance Corp. and the Federal Reserve have all issued warnings in the past two months.

The FBI says it has investigated more than 200 cases, mostly in 2008 and 2009, in which cyber-robbers executed fraudulent transfers totaling about \$100 million — and successfully made off with \$40 million.

The victims are mostly small to midsize organizations using online bank accounts supplied by local community banks and credit unions, FBI analysis shows. "The bad guys are still out there breaking into customers' computers," says Steven Chabinsky, deputy assistant director of the FBI's Cyber Division.

Banking and tech security experts say many more cases of ACH and wire transfer fraud are going unreported mainly because the attacks are new and there are no laws setting forth the rights of online business account holders, the way consumer-rights laws protect accounts held by individuals. The result: Many cases end in civil disputes in which small businesses often lose.

"Our nation's legislators are not doing their job in affording the same protections for business account holders that they do for consumer account holders," says Litan.

### Risky business

Several developments make this new form of fraud irresistible for cybercriminals. In a race to win more online business customers, many banks offer high limits on ACH and wire transfers, even though their systems lack modern technologies for detecting fraud, says Terry Austin, CEO of security firm Guardian Analytics.

"Many banks rely heavily on their online channels but fail to implement the necessary protections," says Austin. "Cybercriminals are capitalizing on this opportunity."

Meanwhile, stealthy, malicious programs borne by corrupted Web links lurk everywhere on the Internet: in e-mails, social-network postings, online ads, even search query results. Click on a tainted link, and you could get infected by a cyber-robbert's banking Trojan. Hundreds of new banking Trojan variants appear on the Internet every day. The number should top 200,000 in 2009, up from 194,000 in 2008, according to PandaLabs.

The likelihood of any ordinary person getting his or her PC infected by a banking Trojan is so great that Gartner's Litan tells acquaintances who run small businesses to switch from commercial online accounts to an individual consumer account.

That's because consumer-protection laws require banks to fully reimburse individual account holders who report fraudulent activity in a timely manner. However, banks have taken to invoking the Uniform Commercial Code — a standardized set of business rules that have been adopted by most states — when dealing with fraud affecting business account holders. Article 4A of the UCC has been interpreted to absolve a bank of liability in cases where an agreed-upon security procedure is in place and a theft occurs that can be traced to a compromised PC controlled by the business customer.

"It's time for small business to wake up and understand the true risk of online banking," says Litan. "If the bank thinks you were negligent, they do not have any obligation to pay you."

back."

The Western Beaver County School District in Pennsylvania, for one, is testing this stance. It is suing ESB Bank for executing 74 unauthorized cash transfers totaling \$704,610 over four days during Christmas break a year ago. Court records show cash moved into 42 receiving accounts in several states and Puerto Rico. The bank retrieved \$263,413 but did not recover \$441,197.

ESB's attorney, Joseph DiMenno, says the bank is confident it will be "fully exonerated" but declined to discuss the lawsuit in detail. In a court filing, the bank denied any liability and said the district's "failure to secure and protect" its computers and network were to blame for any damages.

"They were able to reverse some of the transfers, but for others, the money apparently was already gone," says the district's attorney, Brian Simmons, of the Pittsburgh law firm Buchanan Ingersoll & Rooney. "We're not entirely sure who ended up with the funds. But the school district would like its money back."

So, too, would officials in Bullitt County, Ky. Over seven days in June, unauthorized transfers totaling \$415,989 were moved out of the payroll account the county kept at First Federal Savings Bank of Elizabethtown. In a resolution authorizing a lawsuit against First Federal, county officials noted that "\$105,813.06 of the people's money" had been recovered, while "\$310,176.11 remains in the hands of the thieves throughout the country and abroad."

Gregory Schrecke, the bank's president, said in an interview that Bullitt County's "net loss" was actually \$299,684. He said the bank stands by its decision not to make the county whole.

"No, we are not going to give it back," says Schrecke. "The county's network did not have an effective firewall, its virus protection software was woefully out of date and the county's treasurer and (chief) executive did not follow internal controls that would have prevented the unauthorized transfers."

The county's attorney, Larry Zielke, says First Federal should have stopped payroll transfers to other states and countries, something Bullitt County, population 75,000, never does. "Customers shouldn't have to protect the banks," says Zielke. "Banks should protect their customers."

Banking analyst Litan says it is unrealistic for the banking industry to promote Internet banking as safe based on the expectation that account holders will continually secure their PCs against cyberintrusions. "Banks should at least put a large disclaimer on their home Web pages advising customers that they bank online at their own risk," she says.

Indeed, any organization that cannot survive a sudden five- or six-figure loss should consider shunning Internet banking altogether, says Amrit Williams, chief technical officer of security firm BigFix. "Online is a very dangerous place for any small organization to be right now," he says. "The guidance for most of them should be, 'Don't bank online unless you absolutely have to.' It is too risky, and there are too few controls to support you if you fall prey to a malicious incident."

#### Getting the cash

The banking industry acknowledges that online banking is risky and is doing all it can to address those risks without impairing development of electronic banking, says Doug Johnson, senior risk management adviser at the American Bankers Association. He says small businesses should heed the ABA's advice to use a dedicated PC for online banking.

"The fraudulent transactions represent a very small portion of the millions of safe and successful ACH transactions conducted daily by businesses across the country," says Johnson.

The ABA's position is that each bank sets its own policy for how much liability to assign to business account holders when unauthorized transfers occur. In general, "Banks urge business customers to be aware of their responsibility to keep computers used for online banking free of malicious programs," Johnson says.

Meanwhile, cyber-robbers continue to orchestrate online heists of increasing sophistication. Getting the money out is not easy; it requires careful planning and meticulous coordination. According to interviews with law enforcement officials and security researchers, here's how a typical theft unfolds:

First, a researcher spends some time on Google locating the public Web pages of small businesses, local agencies and smaller organizations in the habit of posting names — and sometimes e-mail addresses — of a comptroller or a senior executive. Next, a graphic designer crafts an official-looking message purporting to come from the IRS or a shipping company addressed to the targeted employee. This is what's known as "spear phishing," a ruse to get the employee to click on a tainted Web link. Clicking on the link swiftly and silently installs a banking Trojan.

One spear-phishing template in wide circulation purports to come from the target's own tech department, says Amit Klein, CTO of security firm Trusteer. It instructs the recipient to click on a link to ensure continued access to the company's Outlook e-mail system. "It's well-crafted and very effective," says Klein.

Banking Trojans can be simplistic. One common variety readily for sale on the Internet installs keystroke loggers that record banking account log-ons typed by the PC user. The robber later uses the log-on to access the account. Others are intricate, crafted to defeat the single-use PIN codes, smart cards, security certificates and biometric scanners some banks require for ACH transfers and wire transfers.

One such Trojan discovered by Trusteer set up a special chat channel to alert the attacker whenever the victim began to type in a key-fob-issued PIN code, which remains valid for 60 seconds. Acting quickly, the robber would then log on and set up a transfer, undetected, while the employee carried on other banking transactions.

"The problem is growing, and the sophistication is increasing," Klein says.

#### Micropayments

Randy Vanderhoof counts himself lucky. The executive director of Smart Card Alliance, a Princeton Junction, N.J., non-profit advocacy group, moved quickly when he noticed suspicious wire transfers from the group's Bank of America online banking account in July.

The first two transfers were two micropayments, for 95 cents and 31 cents, that went to the same account at ING Direct, an online-only bank. That was followed two days later by a transfer of \$25,000 into the ING account, followed by three more transfers for \$25,000 and one of \$24,800 in the ensuing four days, one transfer a day.

Vanderhoof alerted Bank of America quickly enough for it to recover all of the transfers. He figures the micropayments were tests and that the subsequent big transfers indicate that the robber was being frustrated in attempts to convert the deposits into cash.

He figures ING probably had the account under surveillance. But he doesn't know because he says the banks did not satisfy his requests for a detailed explanation. ING declined to comment. Bank of America follows industry practice of not discussing customer cases, says spokeswoman Tara Burke. The bank takes security seriously and offers customers a wide array of security tools and services, she says.

Vanderhoof closed the breached account and opened a new one, begrudgingly agreeing to pay Bank of America \$125 more a month in fees for a service that permits transfers only from pre-approved parties. The service recently has blocked unapproved transfers of 12 cents, 25 cents and 38 cents.

He concludes would-be cyber-robbers have obtained the log-on details to the new account and are testing whether the bank will make unauthorized transfers.

"Our account is still out there, still getting hit with these probe transfers," he says. "I guess the only thing the bad guys haven't figured out is that they're not on our approved list."

**Find this article at:**

[http://www.usatoday.com/tech/news/computersecurity/2009-12-30-cybercrime-small-business-online-banking\\_N.htm](http://www.usatoday.com/tech/news/computersecurity/2009-12-30-cybercrime-small-business-online-banking_N.htm)

Check the box to include the list of links referenced in the article.

Copyright 2009 USA TODAY, a division of Gannett Co. Inc.