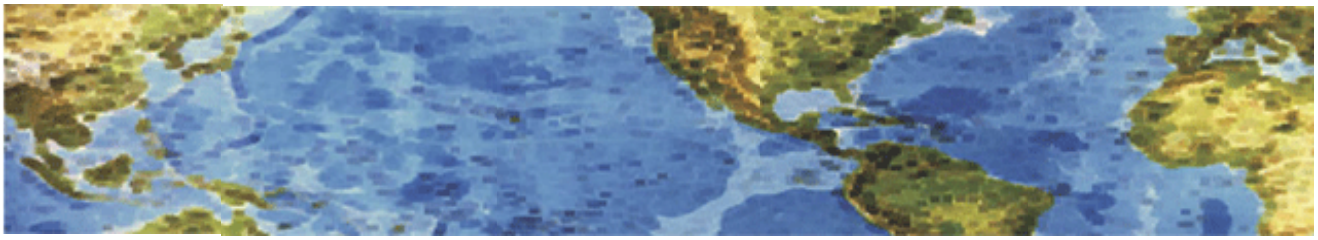
HALL ASSOCIATES



Risk-Based Decision Making Commentary
5 September 2013 Newsletter

How Online Bank Fraud Could Destroy Your Business

In the past 10 years, online banking has exploded, with millions of customers checking their balances and moving money around through Web browsers. Such activity has created a goldmine for cybercriminals, who hack into online bank accounts and transfer large sums to accounts they control. Under federal law, private, or "retail," customers in the United States are largely insured against such fraud. But no such protections apply to commercial clients, whose huge losses can lead to bankruptcy. **Yet many owners of small and medium-size businesses are unaware of the risks of online banking.** Here's how to avoid being the next victim.

Understand the risks - Cybercriminals target small and medium-size businesses for two important reasons. First, many business owners often have a limited understanding of Web-based threats and fail to implement the necessary protections. Second, small and medium-size businesses generally have far more money in their bank accounts than consumers do. Limited protection, combined with high account balances, makes such businesses an attractive target for cybercriminals. Business owners are generally unaware of three key points regarding to online banking. Highly sophisticated malware, often in the form of banking Trojans, is being used to compromise hundreds, if not thousands, of business bank accounts; the measures many banks have in place don't effectively protect businesses against these types of attacks; and in many cases, banks will hold business customers liable for online fraud losses.

How to guard against risks - There are several large risks for businesses that use online banking services: Phishing scams, particularly those related to the email account tied to the online business bank account; "Man-in-the-middle" attacks that can intercept, redirect or reformat communications between the customer and the bank, without either party's knowledge; Fraudulent or corrupted websites, which can silently infect Web browsers; and Public or unsecure Wi-Fi networks, which can result in banking-session hijacks.
To best protect your business from potential online-banking dangers, **First manage your risks:** Small and medium-size businesses need to move beyond the mindset that they are too insignificant to be targeted by criminals. Business accounts are perfect targets for criminals because the cash balances are higher than those of retail banking accounts. Nearly half of small-business owners have no protocols in place for securing data, and have no one directly responsible for managing data security. **Second use a browser that's not on the hard drive:** Extending fraud prevention to the computer in the form of a secure browsing platform can dramatically reduce fraud-related losses and is relatively inexpensive and easy to set up. Such a hardened browser, typically stored and run from on a USB drive, creates a protected connection to the financial institution's website. Since transactions can only take place via the hardened browser and a secure proxy server, any malware that exists on the user's computer is "blind" to the exchange of customer information. Essentially, the device turns the user's computer into a dedicated machine for online banking that isolates critical data from the cybercriminal's prying electronic eyes.

For serious security, boot the computer from a "live" Linux distribution burned to a CD and use the included browser to access the online account. Malware can't write to or otherwise alter a burned CD. **Third keep your software updated:** Many forms of malware can sneak into a computer through old or unpatched Web browsers, which present a serious risk to users.

Even when a software vendor has issued a fix for a vulnerability, the end user will often need to be reminded to install it. Take the guesswork out of the equation: Set up your PC and its applications to automatically load and install software updates. **Fourth dedicate a computer to online banking:** To prevent online fraud, the FBI and the American Bankers Association recommend designating a single computer that handles only online banking activities. Because emailing and Web surfing account for nearly all infections, those activities should not be allowed on that machine. A dedicated PC is not a practical recommendation for retail banking, but in the commercial sector, it's a powerful technique used to prevent or mitigate the risks associated with online banking. If your business can't spare the space or the hardware, consider booting a PC from a live CD, using a USB-based browser or setting aside a seldom-used browser, such as Opera or Maxthon, to be used only to access online bank accounts.

http://www.technewsdaily.com/18541-online-banking-dangers.html

Online Banking Thieves Pose as Victims In 2 New Scams

It's not every day that online crooks come out from behind the computer, but when they do, they can make an ordinarily preventable scam much more potent, especially when your bank account is at stake. Two new online bank fraud cons have been identified, both of which require the hacker to demonstrate not only technical talent, but interpersonal skill as well, and even puts the hacker face to face with police officers who unknowingly facilitate the fraud. One attack employs a Trojan called "Gozi" to hijack a victim's international mobile equipment number (IMEI) when they log in to their online banking website. Once the crooks have the IMEI number, which is unique to each device, they call the victim's wireless carrier, report the phone as lost or stolen, and ask for a new SIM card. With the victim's SIM card in their own phone, the hackers are then able to use the stolen IMEI number to hijack the one time password (OTP) sent to the phone's rightful owner as a means of authorizing legitimate online banking transactions. This particular scam is intricate, but in terms of pure boldness, it pales in comparison to another banking scheme identified.

In this case, the criminals use traditional phishing pages or browser exploits to siphon victims' online banking credentials, as well as their name, phone number and other personally identifiable information. Instead of calling the victim's wireless carrier, the cybercriminals, in a gutsy but calculated move, go directly to the police. Using the harvested personal information to impersonate the victim, they obtain a police report confirming the phone has been stolen. With the police report in hand, the crooks, after calling the victim and telling them their service will be out for 12 hours, go to the wireless carrier's retail outlet and present the police report. The carrier then deactivates the victim's SIM card, issues the fraudster a new one, and from there, the perpetrator is able to authorize all the fraudulent banking transactions and reap the benefits.

The one common threat in both schemes is that they are made possible by compromising the Web browser with a MitB [man in the browser] attack to steal the victims' credentials.

http://www.technewsdaily.com/7601-online-banking-hijack-accounts.html