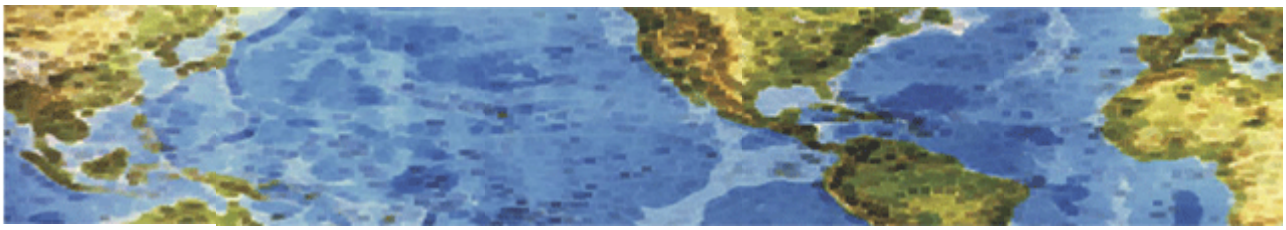
HALL ASSOCIATES



Risk-Based Decision Making Commentary
20 Oct 2013 Newsletter

New Security Threat: Cash Register Skimmers

Crooks who steal credit and debit card numbers have found a devious new way to snag this information. They're using a small, relatively cheap piece of off-the-shelf technology to compromise computerized store cash registers. We know about this because a band of brazen thieves was caught on security cameras installing these high-tech skimmers on cash registers at the Nordstrom store in Aventura, Fla., two weeks ago.

The skimmers are built into standard PS/2 cable connectors that plug into the back of a computer where customers can't see them. They're only about an inch long—and look so innocuous that even if employees saw them they might not suspect anything. The skimmer is a little piece of plastic, usually purple, that fits into the port where your keyboard connects to your computer. It intercepts any data that is sent on that communication channel, whether it's keystrokes or somebody swiping a card through a terminal. PS/2 keystroke loggers have been available for years. They sell for as little as $40 and are marketed as "professional surveillance products, however this seems to be the first time they have been used to skim card information from a retailer. Nordstrom confirmed that it had found and removed "unauthorized devices on a small number of cash registers" at its Aventura store.

Krebs obtained a copy of an information sheet prepared by the Department's Crime/Intel Analysis Unit that says Nordstrom located a total of six skimming devices attached to registers. The alert outlined what was seen on the retailer's surveillance footage. The thieves, all men, worked in teams of three. Two men distracted the sales staff while a third took pictures of the register, then removed its rear access panel and took additional photos. Several hours later, three different men entered the store. Again, two of them distracted the sales staff while the third removed the register's back panel and installed the skimmer. The police memo described the device: It captures all track data from credit card transactions and stores it on the device, similar to a USB drive. The connector was made to match the connections on the back of the register to include color match. Therefore, no one would have detected it unless there was a problem with the register.

It is unlikely customer card information was compromised in this case, as the devices were discovered before the crooks could retrieve them and download the information they had recorded. But for as little as $135 they could have purchased keystroke loggers capable of sending the stolen information over a local wireless network.

This scheme, involving smaller, harder-to-detect skimming devices, puts the onus on businesses to heighten their security efforts. Many retailers have card readers that connect to cash registers via PS/2 connections. These are now vulnerable to this kind of skimming attack and need to be secured. The bottom line is that we all need to be aware of the potential for this sort of identity theft. It can happen no matter how hard you try to protect yourself. So you need to remain vigilant.

That's why it's so important to continually review all the transactions on your credit card and bank account statements. If you spot charges that aren't yours, report them right away. And if you're at a store and see someone tampering with a register, say something to a store employee.

http://www.cnbc.com/id/101115205?goback=.gde_4387290_member_579678179174228787 5#!

HALL ASSOCIATES

Scared of an Online Password Hack? Here's How to Help Prevent It

Password hacks are becoming more common as people's online accounts contain more sensitive personal data. Even big, trusted sites like LinkedIn, LivingSocial, and Dropbox suffered password breaches in the past. And because 78% of people reuse their passwords, it becomes more likely that a password hacked on one site can open accounts on other sites. Here's how to prevent your data from being compromised in 5 easy [albeit non-exhaustive] steps:

1. Stay away from English-language passwords

One of the biggest mistakes that internet users make is using English words in their passwords. English words make hacking passwords far easier for a potential hacker. Given that there are only approximately 500,000 words in the English language and that there are approximately 70 typable characters available on an English keyboard, that means that for password of 8 characters in length, there are 9,440,350,920 combinations available for an 8 letter password. That number skyrockets once you create even longer passwords. Clearly, there is significantly more diversity in using characters rather than just English words.

2. Create fake security answers

Web sites ask questions like Which street did you live on when you were ten? What is your mother's maiden name? **STOP. DO NOT SUPPLY THE CORRECT ANSWERS.** Think about it: if you give the correct answers to these questions, you're giving companies and potential hackers even more extensive information about yourself. Plus anyone can find these answers on data broker websites for only a few dollars, so they're hardly secure. Giving the wrong answers to these questions, even answers that aren't actual words, can add another layer of protection.

3. Have a favorite poem or song?

One of the easiest ways to create strong passwords is to use something that you've already committed to memory. Many articles have been published about using a "base password" to remember all other passwords by, and simply adding the name of a website to the end, such as for Amazon.com: passwordAMAZ. Any song, poem, or even sentence that you have memorized can be used.

One of the most important reasons as to why this method works so well is because it always functions on those websites that don't allow special characters in passwords. Also, remember that this method could always be combined with numbers/special characters for increased security (such as spaces (_) or symbols (*,&,#,@,$,%, etc.).

http://www.abine.com/blog/2013/scared-of-an-online-password-hack-heres-how-to-prevent-it/