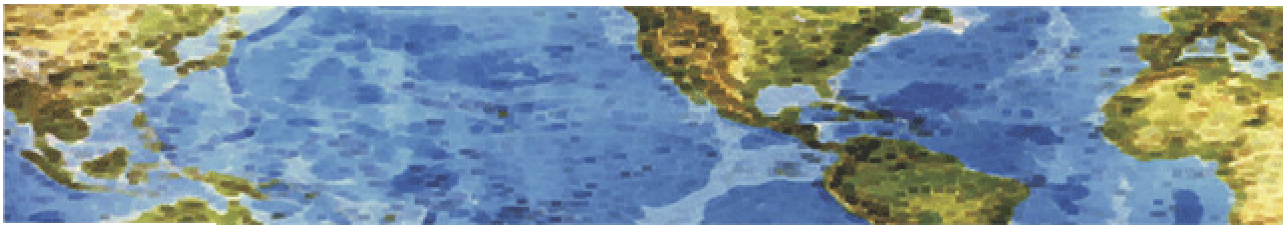
HALL ASSOCIATES



Risk-Based Decision Making Commentary
1 May 2013 Newsletter

What Does the Internet Know About You?

The Internet is a place for people, companies and criminals to pick up more information about you. That includes your address, gender, date of birth and, with a little sleuthing, your Social Security number and credit history. That's been made clear in a recent spate of "doxing" (document tracing) of celebrities that revealed, for example, that Microsoft CEO Bill Gates had an outstanding debt on his credit card. But none of this information comes from hacking. It's either already public or accessible by, for example, paying an online people-finding service to get a Social Security number, and then running a credit check.

Then there's all the data that gets poured into social media sites such as Facebook, Twitter, Tumblr, Instagram, Foursquare and others. Now employers can fire workers for expressing opinions they don’t like, strangers can stalk you with mobile apps, cybercriminals can steal your identity or company accounts and college administrators can judge the quality of applicants by the number of drinking photos posted to their account. **People need to understand** that their information has secondary or tertiary uses. The issue isn’t so much that information is out there and people can see it. The issue here is when that information gets used in new and different ways. **It's all public.**

Many gun owners felt a secondary use of private information when they saw an interactive map published by the Journal News of White Plains, N.Y., that listed the name and addresses of everyone in two New York state counties with a gun permit. However, the records are all public. There is no current law against publishing them either in print or online, even if it makes some uncomfortable. Of course, some states are rushing to create laws against this practice **for some information.**

When real estate search site Zillow.com first came out, many people were shocked at the amount of information on it — including their physical address, aerial house photos and the price paid for their homes. Last year, Zillow began listing homes going through the foreclosure process, which caused another firestorm of people looking to opt out. But all the information comes from public records. Zillow says it doesn’t list names, only properties; and it does not allow those with foreclosed property to "opt out” of being published.

Social oversharing

The Electronic Frontier Foundation cautions about the use of Facebook Graph Search, which allows users to search information from news feeds of friends and those users with settings set to public on Facebook. Now anyone can look for, for example, single women living in San Francisco who share their taste for tapas and perhaps find a phone number and email address. Who needs Match.com anymore?

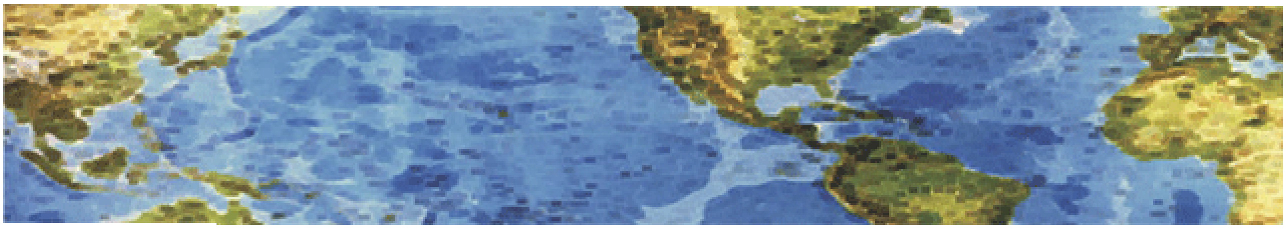
Today, people's futures are in peril every time their boss or college admissions office looks on the Internet. That means users shouldn't post photos of themselves with an alcoholic drink in their hand or espouse extreme political views, because it can lead to a value judgment. You can still go online and say what you want, but be aware that anything electronic is forever and could go viral. Another problem today is social networks becoming a larger part of one's life. To comment on articles, people frequently log into a Facebook account first. Others are finding that their Google+ social account is being attached to their Gmail account and will be needed to comment on apps or games on Google Play. Google+ accounts are also used to sign into YouTube and other Google sites. Many social networks are seemingly trying to end anonymous posting. To preserve privacy, a person would have to walk away from Google or Facebook. Recently Facebook Home was launched on Android devices, and many noticed that the interface logged online purchases and visits, although Facebook said that it doesn't assign names to the information. Facebook is using customer loyalty cards' information and public records to sell to advertisers and marketers. However, Facebook Home isn't hunting anyone down to do this; people themselves are opting to use an Android phone with the Facebook skin on it.

What you can do

Long-term solutions could be legal, regulatory or even codes of conduct for companies. Meanwhile, users can save themselves some headaches **by understanding that whatever they place online will stay online.** Nothing online is temporary; instead, it's more like an Internet tattoo. Keep all social networks set to the highest privacy settings even if you have to manually approve follow requests. If posting to a forum or other online database, don't use your real name or email address (or at least one you don't mind people seeing). **Never give out** your date of birth, phone number or physical address if you can help it. **Never give out** your Social Security number. Many colleges, banks, brokerage houses and other companies now have alternative login IDs to use provided you ask for one. (However, not even colleges or banks are immune to hackers, so always monitor your credit for suspicious activity.) Remember that what you post can be seen by others. Be careful of what you say and which photos are posted because it could potentially be seen by millions of people.

http://www.technewsdaily.com/17886-what-does-internet-know-about-you.html?cmpid=520751

HALL ASSOCIATES



Risk-Based Decision Making Commentary
1 October 2013 Newsletter

Mobile Browsing - Is Your Company at Risk?

This infographic gives a quick visual representation of some of the key findings of a recent Webroot research report on web security in the US and UK. As cybercriminals increasingly exploit vulnerabilities in mobile browsers and apps, companies with mobile workforces (or those that allow employees to use their own mobile devices to access the company network) face new challenges in protecting users and customers data. And the impacts of failing to protect against mobile browsing threats can be severe.

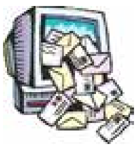
Among the key points:

50% of companies in the US estimate that web-borne attacks cost from $25,000 to $1 million in 2012

90% of respondents agree that managing the security of remote users is challenging

50% of firms with remote workers had a website compromised

Mobile Threats Experienced in 2013 by Companies



9% lost data

24% got Malware

45% lost devices

Mobile Threat Impacts

53% reported business activities were significantly disrupted

61% required additional resources to manage mobile security

56% had reduced employee productivity

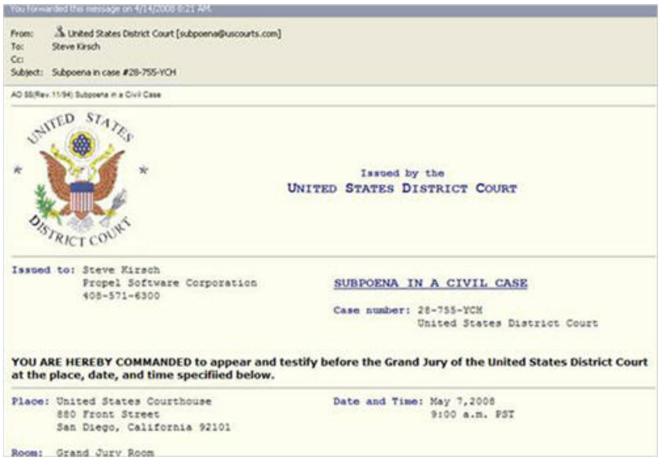
What can you do to minimize these kind of impacts if your employees use their own mobile devices?

1. Establish and enforce device control policies.
2. Require YOUR device level security to be used by any personal mobile device
3. Provide mandatory mobile workforce security training.

Social Engineering Example – Spear Phishing

These phishing emails are typically targeted to individuals at companies that are high ranking officials, possibly CXOs. The contents of the email will usually include personally identifiable information of the victim to build confidence in the email. This might include full name, telephone number, position, etc. This is possibly one of the best examples of a targeted spear phishing attack.

Thousands of high-ranking executives across the country have been receiving e-mail messages this week that appear to be official subpoenas from the United States District Court in San Diego. **Each message includes the executive's name, company and phone number, and commands the recipient to appear before a grand jury in a civil case**.   A link embedded in the message purports to offer a copy of the entire subpoena. But a recipient who tries to view the document unwittingly downloads and installs software that secretly records keystrokes and sends the data to a remote computer over the Internet. This lets the criminals capture passwords and other personal or corporate information. Another piece of the software allows the computer to be controlled remotely. According to researchers who have analyzed the downloaded file, less than 40 percent of commercial antivirus programs were able to recognize and intercept the attack. An example image (courtesy of the New York Times blog by John Markoff) of the article is show below:



You forwarded this message on 4/14/2008 8:21 AM.

From: United States District Court [subpoena@uscourts.com]
To: Steve Kirsch
Cc:
Subject: Subpoena in case #28-755-YCH

AO 88(Rev.11/94) Subpoena in a Civil Case

Issued by the
UNITED STATES DISTRICT COURT

Issued to: Steve Kirsch
Propel Software Corporation
408-571-6300

SUBPOENA IN A CIVIL CASE

Case number: 28-755-YCH
United States District Court

YOU ARE HEREBY COMMANDED to appear and testify before the Grand Jury of the United States District Court at the place, date, and time specifiied below.

Place: United States Courthouse
880 Front Street
San Diego, California 92101

Date and Time: May 7,2008
9:00 a.m. PST

Room: Grand Jury Room

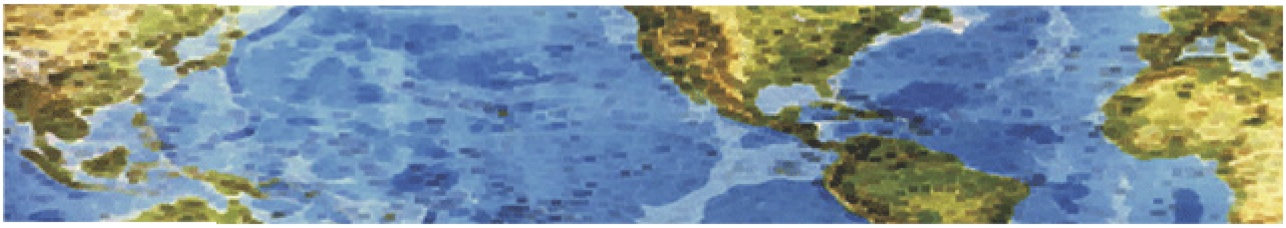
So how can someone avoid responding to this type of e-mail phishing? **Obviously, the number one thing is user awareness**. Unfortunately, the security community has been pushing user awareness for a decade, and the attackers just get less blatant and obvious about their attacks, making it more difficult for users to avoid this type of attack. There are two things to drum into potential targets of these type of attacks:

One – No Government agency would send this type of alert via e-mail. There are phishing e-mails supposedly from the Justice Dept, the FTC, the FBI, the IRS and numerous other agencies.

Two – ***Never*** click on a link in an e-mail without checking on it first. I recommend calling the agency and asking if they sent this.

http://www.zdnet.com/blog/security/targeted-spear-phishing-attacks/1032

HALL ASSOCIATES



Risk-Based Decision Making Commentary
1 September 2013 Newsletter

Recent Retail Breaches Connected

A malware attack that exploited a point-of-sale software vulnerability within systems used by a select group of Kentucky and Southern Indiana retailers has now been linked to attacks against grocery chain Schnuck Markets Inc. and four other merchants. The attacks that breached Point Of Sale systems and networks at Schnucks, as well as retailers in Kentucky and Southern Indiana, share a number of characteristics. The Secret Service has determined that the malware used in the attacks and the methods of entry all trace back to a single hacker using an overseas IP address. The tethering of these attacks illustrates why it's so critical for banking institutions to regularly communicate with card brands about the fraud trends they are detecting.

Common Attack Patterns

Recent breaches that followed similar attack patterns include the malware attacks against supermarket chain Bashas' Family of Stores and convenience store chain MAPCO Express, as well the cyber-attack against retail tool store chain Harbor Freight Tools, and a suspected breach at supermarket chain Raley's Family of Fine Stores. In all of these attacks, card numbers were targeted and compromised. And although the type of malware used in the attacks has not been revealed publicly, issuers say they suspect most of these attacks likely resulted from a single or similar strain. All of these cards were compromised and sold in a forum. **Within 72 hours of the breaches, cards were being used**, so the fraud occurred very quickly.

Impact on Issuers

Evidence of fraud linked to the Kentucky-Indiana breach as well as the still-under-investigation Raley's breach continues to trickle in, but the attack against Kentucky and Southern Indiana retailers resulted in fraud losses that were five times greater than any other previous breach in the region. MasterCard and Visa released alerts about the merchants that had been affected. The local reseller who provided the remote-access software, which the malware exploited, has not been identified in those alerts.

Retail malware attacks are plaguing banking institutions because it's challenging to trace to the source. It's been a long line of succession this year, and a predominant amount of the attacks have been at grocery stores. But one thing banks and credit unions need to be aware of is when we have inconclusive evidence, it may be challenging to find a common point of compromise. Sometimes it's a processor breach, which may not lead them to a specific retailer.

http://www.govinfosecurity.com/recent-retail-breaches-connected-a-6022/op-1

Malicious software pretends to be your friend, hijacks your Facebook account

Next time your friend appears to send you a strange video link, **think twice about clicking on it -- it could infect your computer**. According to the New York Times, Facebook is being used to spread malicious software that acts like a message or email to gain access to your account and browser information. The software masquerading as an email or Facebook message notifies users that they have been tagged in a post and includes a link in the message. The link then directs you to a website where it asks to install a browser extension in order to play a video.

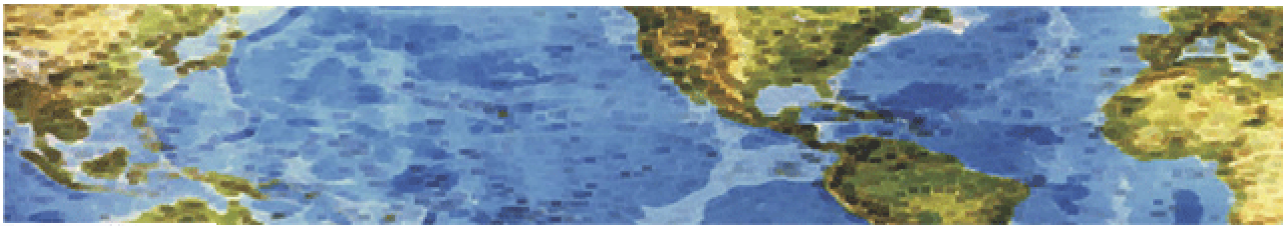
If the browser extension is installed, it can gain access to any sensitive information stored in your browser including passwords and log-in information. And once the extension is installed, it is tough to remove because it blocks user access to browser settings. According to researchers who discovered this Facebook malware, it is affecting as many as 40,000 users per hour and has infected 800,000 people so far. The malware was originally designed to specifically target users of Google Chrome, but has since spread to Mozilla Firefox as well.

Attacks through social network messages are fairly common and once someone has been infected, they often become a carrier of the malware for their friends. Receiving a message from a friend through a social network doesn't raise as many flags as messages from unknown users and while the message might seem strange, **people tend to be more apt to click the link**.

These kinds of attacks also take advantage of a user's apathy towards computer permissions, since unsuspecting people will often click "accept" to a prompt without thinking about it. Facebook is aware of the malware and is blocking and clearing the links wherever they are found. Google has already disabled the extension in their Chrome browser. While this particular malware is being addressed, the tactic is common enough that it will most likely come up again. Luckily, these kinds of malicious software require a level of participation in order to be effective**. To protect yourself from being fooled, make sure to never allow an extension to be installed that you didn't specifically want, and always be suspicious of strange messages, even if they are from people you normally trust.**

http://central.gdgt.com/2013/08/27/malicious-software-pretends-to-be-your-friend/?icid=maing-grid7|main5|dl19|sec1_lnk2%26pLid%3D364449

HALL ASSOCIATES



Risk-Based Decision Making Commentary
3 July 2013 Newsletter

Cybercriminals Improve Android Malware Stealth Routines with OBAD

We have been seeing apps that exploit vulnerabilities in Android, with most of them attempting to gain higher privileges on user devices. In recent days, a stronger and far more advanced Android malware named ANDROIDOS_OBAD has come into play.   ANDROIDOS_OBAD is found to be **equipped with ability to avoid being uninstalled** from devices and triggers more malicious code.

This new malware family has overall stealth and anti-reverse methods for both normal users and security researchers. When installed, it asks for root privileges and activates the device administrator. Because of ANDROIDOS_OBAD's gaining root privilege, the malware takes complete control of the device and may allow an attacker to utilize this fully. If the user does not activate as instructed, the malware displays frequent pop-up messages when the device restarts. Additionally, if users press the back button, pop-ups appear once again. If the home button is pressed, the pop-ups appear any time later. Here, users will finally have the chance to uninstall it, but if device administrator is activated, the malware will instead run fully in stealth mode.

Still, you can carefully distinguish the malicious app from the mixed Android system apps under Apps Management. However, you won't be able to uninstall it because it's a device admin app. The "anti-uninstall" tricks also work on Android's vulnerability by hiding itself from Device Administrator management view.   This malware is capable of the following behavior:

- **Hiding the launcher, and run as a background service with the highest priority.**
- **Automatically try to open Wi-Fi connections and connect to a remote server.**
- **Collect user's contacts, call log, SMS inbox and installed apps.**
- **Download, install and uninstall apps (with root privileges, this can be done silently).**
- **Distributing malware to other phones via Bluetooth.**

ANDROIDOS_OBAD shares similar features with that of its predecessor ANDROIDOS_JIFAKE. The latter is a fake app installer that tricks user into installing and executing them, after which it will silently register as a service connecting to remote servers as it waits for commands. The remote server can then **trigger sending premium text messages** and do the same "anti-uninstall" tricks.

The anti-uninstall trick is exploited through Android's Device Administration feature. If one app is installed and enabled as the device admin application, it will be entrusted with more power to constrain user's device, including enforcing security policy, lock or wipe user's device. Under this level, an app cannot be easily uninstalled, which contributes much for the anti-uninstall tricks.

http://blog.trendmicro.com/trendlabs-security-intelligence/cybercriminals-improve-android-malware-stealth-routines-with-obad/?goback=.gde_1765567_member_249721248

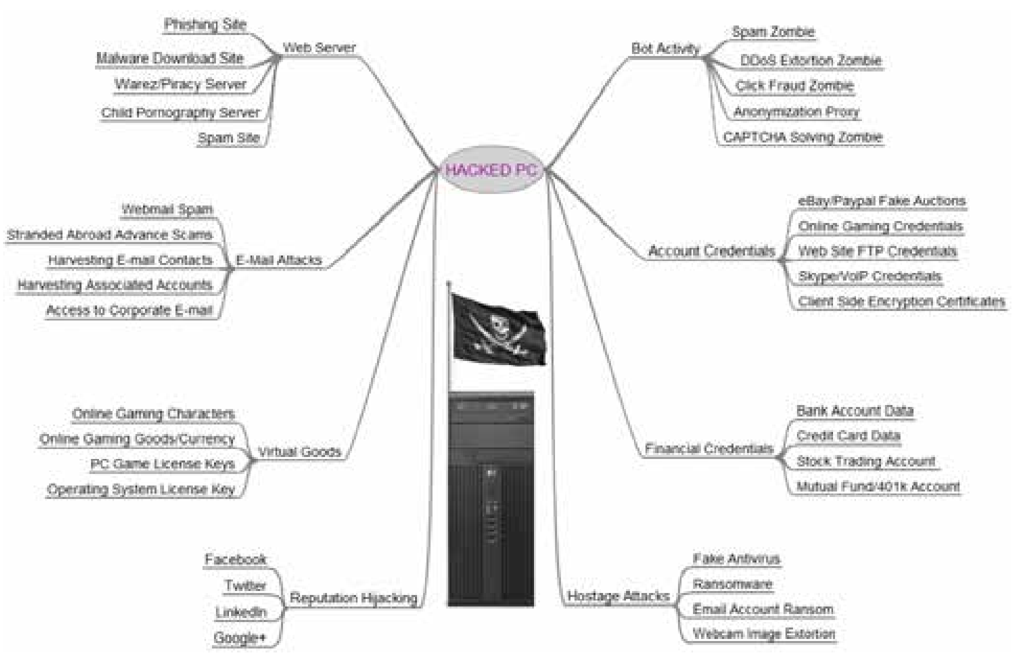
Two Middle TN Mapco stores at risk in data breach

More details have emerged about a data security breach that Brentwood-based convenience store operator Mapco Express Inc. disclosed a month ago. The accounts of consumers who used their debit or credit cards at any of the company's 373 locations from March 19 through March 25 might have been affected, according to an updated FAQ on Mapco's website..
Also, card transactions at two specific Middle Tennessee locations – 1301 Dickerson Road in Goodlettsville and 6624 Charlotte Pike in Nashville – on April 14 and 15 and at certain, undisclosed stores on April 20-21 also might be at risk.

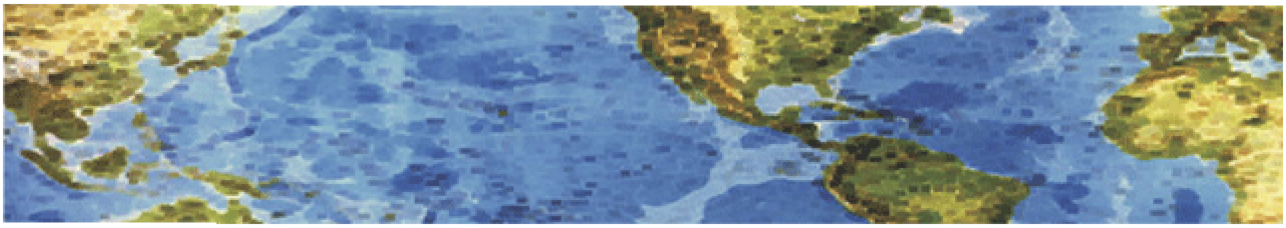
That's because malware installed on Mapco's payment card processing system might have been active at those times and locations, the company said. Those are the first details that have been released since Mapco disclosed the breach on May 6. At the time, the company identified only the dates but gave no details about potentially affected locations. A spokesman said Friday that the company had no comment, citing an ongoing investigation. The company previously said that private security experts and the FBI also were looking into the breach. The hackers who installed the malware targeted systems that transmit certain card information needed for transaction approval, potentially stealing information that could be used to initiate fraudulent purchases, the chain previously said. The malware since has been disabled.
http://blogs.tennessean.com/business/2013/06/10/two-middle-tn-mapco-stores-at-risk-in-data-breach/

The Various Ways That Criminals Can Monetize Hacked PCs

The following graphic was designed to explain simply and visually to the sort of computer user who can't begin to fathom why criminals/hackers would want to hack into his/her/their PC. "I don't bank online, I don't store sensitive information on my machine! I only use it to check email. What could hackers possibly want with this hunk of junk?," http://krebsonsecurity.com/2012/10/the-scrap-value-of-a-hacked-pc-revisited/



HALL ASSOCIATES

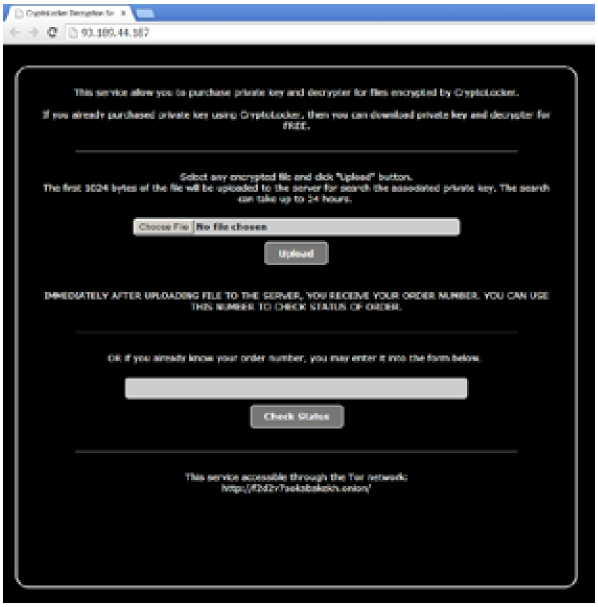


Risk-Based Decision Making Commentary
3 November 2013 Newsletter

CryptoLocker Ransomware – A Global Threat

CryptoLocker infections have been found across most regions, including North America, Europe, the Middle East, and Asia Pacific. **Almost 64% of the victims are in the US.** There are several different ways an organization or an individual can handle the CryptoLocker threat, but there is no known tool to decrypt any files encrypted by CryptoLocker. So you need to always have good backups of ALL your data and files. Some antivirus products now address some of the various CryptoLocker versions, so also be sure your antivirus and system software is up-to-date.

Yesterday there was an article in the Hacker News (see article URL below) about how the criminals behind CryptoLocker have launched a dedicated CryptoLocker Decryption Service website (using a Russian-based hosting server) that allows victims to purchase the decryption key for their encrypted files.



This service allow you to purchase private key and decrypter for files encrypted by CryptoLocker.

If you already purchased private key using CryptoLocker, then you can download private key and decrypter for FREE.

Select any encrypted file and click "Upload" button.
The first 1024 bytes of the file will be uploaded to the server for search the associated private key. The search can take up to 24 hours.

Choose File: No file chosen

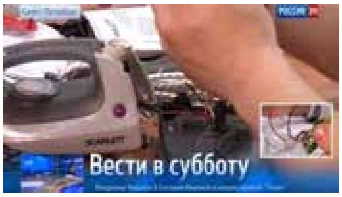
IMMEDIATELY AFTER UPLOADING FILE TO THE SERVER, YOU RECEIVE YOUR ORDER NUMBER. YOU CAN USE THIS NUMBER TO CHECK STATUS OF ORDER.

OR if you already know your order number, you may enter it into the form below.

This service accessible through the Tor network:
http://f2d2v7sokzbakxkh.onion/

Currently almost all antivirus companies are on Red Alert about CryptoLocker and they are releasing updates that can detect and remove the malware or the registry keys from your system. These are needed to actually pay the ransom and get the decryption key. So when this happens, the victim cannot get the decryption key **nor will the criminals get paid**. So, to get their ransom, the criminals have launched a site that looks like a customer support site for CryptoLocker victims. Using this site requires the victim to upload one of their encrypted files to generate an order number. You can then purchase your private key by paying 10 Bitcoins or $2,200. Once the payment is made, the victim can download the private key and a decrypter tool. If you have already paid the ransom, they will provide the key free of additional cost.

http://thehackernews.com/2013/11/CryptoLocker-Ransomware-Decryption-service-malware-keys.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TheHackersNews+%28The+Hackers+News+-+Security+Blog%29&utm_content=Yahoo!+Mail&_m=3n.009a.389.wb0ao05fi9.8cr



“Intelligent Devices” Being Used to Spy

There has been lots of discussion about the rise (and increasing use) of intelligent devices – the Internet of Things. Now hidden chips have actually been found in some devices that enable them to be exploited for illegal activities. Currently only state-sponsored groups are using these, but the threat will expand in the future to criminals and thieves. It turns out that China is planting microchips in numerous manufactured electrical devices. These microchips are equipped with a little microphone and can connect to any unprotected Wi-Fi network within 200 to 600 feet. Mostly these chips are being used to spread malware and spam as well as spying on the surrounding environment but they can be turned to other things. Currently these chips have been found in electric irons, electric kettles, gaming consoles, chargers, network devices, mobile phones and car dashboard cameras.

http://thehackernews.com/2013/11/russia-finds-spying-microchips-planted_1.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TheHackersNews+%28The+Hackers+News+-+Security+Blog%29&utm_content=Yahoo!+Mail&_m=3n.009a.389.wb0ao05fi9.8db

Insurance: Irresistible to Cyber Criminals ?

As insurers aggressively move into new online territory through agency portals, online policy applications, Web-based claims-management systems and mobile apps, they introduce new vectors of Cyberfraud risk. Cyber threats against financial institutions have increased exponentially in the last year and are expected to grow relatively unchecked. The world's biggest data breaches involve millions of records and subject consumers to identity theft risk for years to come. More and more, insurance consumers expect carriers to interact through online channels.

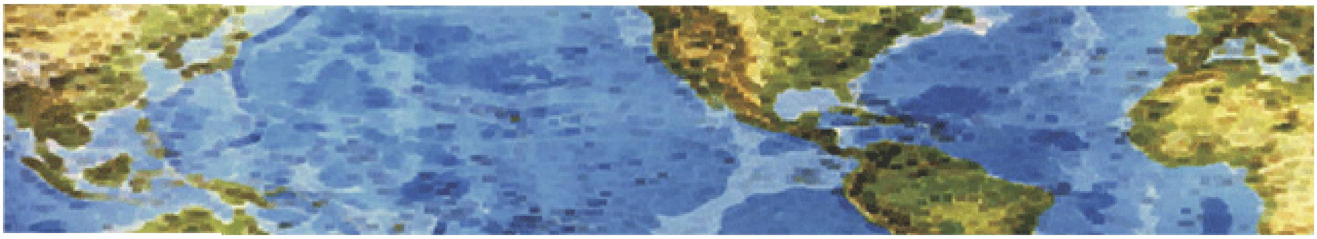
Insurers house a remarkable amount of personal information that identity thieves find irresistible. In October 2012, the insurance industry saw firsthand how intent hackers were on accessing this information when Nationwide suffered a major data breach. Hackers stole names, Social Security numbers, driver's license numbers and dates of birth for more than 1 million individuals – including policyholders as well as individuals seeking quotes.

Technologies and threats are rapidly evolving. In order to keep pace, response strategies also need to evolve. Many cyber threat mitigation programs are reactive – involving forensic analysis after a breach has occurred. More frequently, organizations are doing proactive penetration testing to look for vulnerabilities. But even this methodology is an increasingly outdated approach as it fails to keep pace with the scale and complexity of the cyber threats they are meant to prevent. **In the industry, there is a growing realization that cybersecurity must involve a broader, risk-based approach and move away from being seen as purely a technical problem.**

There are only two types of insurers: those that have been targeted and those that will be. As insurance companies continue to acquire vast amounts of sensitive information, they should reprioritize cybersecurity and data protection as mission-critical business objectives.

http://www.insurancetech.com/security/insurance-irresistible-to-cyber-criminal/240163420?goback=.gde_4387290_member_5803152437833392131#!

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

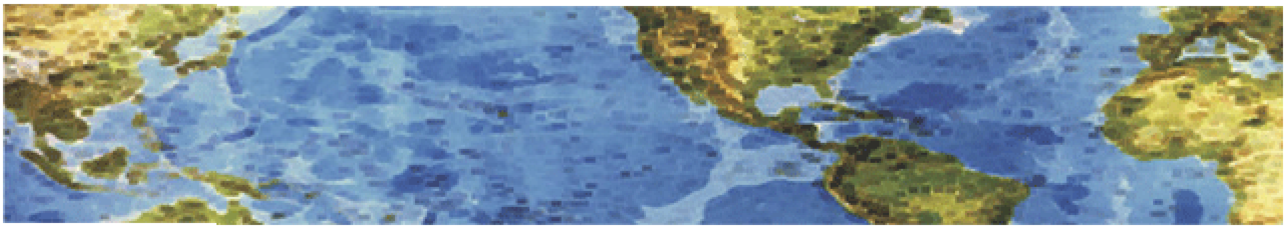
It's not every day that online crooks come out from behind the computer, but when they do, they can make an ordinarily preventable scam much more potent, especially when your bank account is at stake. Two new online bank fraud cons have been identified, both of which require the hacker to demonstrate 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

HALL ASSOCIATES



Risk-Based Decision Making Commentary
8 May 2013 Newsletter

Android Anti-Virus Software Easily Fooled

Anti-virus software made by 10 of the biggest Android security providers can be bamboozled by an embarrassingly easy malware disguise, according to a new report. Android phones are known for being more vulnerable to malware than their Apple peers, but they also come with lots of anti-virus options such as those provided by Symantec, AVG, Kaspersky Lab, Trend Micro, ESET, ESTSoft, Lookout, Zoner, Webroot and Dr. Web. Unfortunately, the Android anti-virus software made by all these companies is easily fooled by a simple trick, according to a report from researchers at Northwestern University and North Carolina State University.

Mobile anti-virus products don't provide real security value to users, given how easy they are to bypass. However, not installing a mobile anti-virus app is still a bad thing but users need to understand that an antivirus app will not protect at all times. Most anti-virus software works by checking potential malware against a list of known "signatures," or essential lines of code that can help identify a program's function. Scammers can evade these security measures by subtly tweaking their malware's code just enough to change its signature without affecting its function. This is called polymorphism.

Polymorphic malware has been a problem on desktop computers for years, and anti-virus companies have developed many solutions to combat it. In the past year, polymorphic malware has also begun cropping up on mobile devices. So researchers from Northwestern University's computer science department decided to see how well Android-specific anti-virus programs could handle polymorphic code. The researchers developed a program that could automatically take a malware's code and apply very basic polymorphic changes. They then ran these "disguised" types of malware through the Android anti-virus programs. In nearly all of the trials, the anti-virus programs failed to identify the disguised malware as a threat.

These findings are serious, but not surprising — mobile security is still a new field, and has far to go before it catches up to desktop. So users should be extremely careful about what they put on their Android phones/tablets. Be sure to at least encrypt your data and use the best antivirus/antimalware apps.
http://www.technewsdaily.com/17982-android-antivirus-serious-weakness.html?cmpid=525478
The full report is at this URL. http://list.cs.northwestern.edu/mobile/droidchameleon_nu_eecs_13_01.pdf

What security secrets might an attacker unearth about your business on Dropbox?

The recent "life hack" of journalist Mat Honan has demonstrated the degree to which many technology-savvy consumers **have tied together numerous online services, including Gmail, Twitter, Amazon, and Apple iCloud.** Due to rampant password reuse, however, attackers have been able to take passwords used on one site, and reuse them to log into a person's account on another site. In the case of Dropbox, that means that any corporate secrets stored there could be easily accessed. An example of such an exploit came to light this month, owing to a Dropbox employee having stored an unencrypted document on the service that contained Dropbox users' email addresses. An attacker logged into the Dropbox employee's account, using a password that the employee had reused on another--compromised--site, obtained a copy of the document, then used the email addresses to unleash a flood of spam at Dropbox users. Any business with employees using Dropbox should:

1. Monitor Dropbox use
2. Compare Cloud service security
3. Beware of lackluster Cloud security service practices
4. Treat Dropbox as a public repository
5. Make sure you can detect insider theft using Dropbox.

http://www.informationweek.com/security/management/5-dropbox-security-warnings-for-business/240005413

Malicious Flash Player Updates Hosted on Dropbox

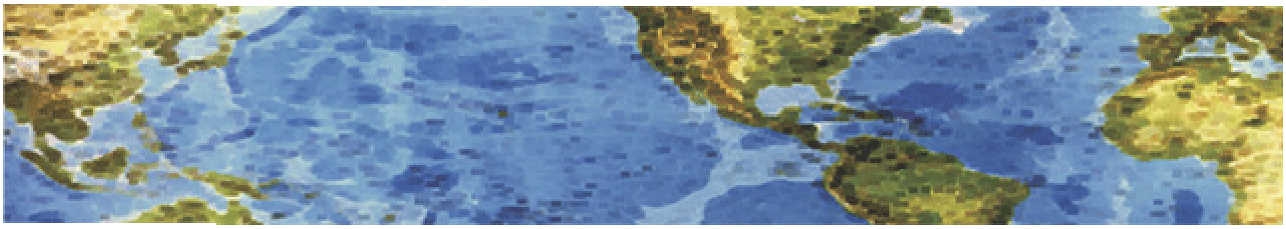
Cybercriminals often disguise malware as updates for Flash Player. An interesting example has been analyzed recently by security experts from Zscaler. The attack starts with a number of websites that redirect their visitors to click-videox.com. Once victims land on this site, they're urged – in English or Turkish – to update their Adobe Flash Player in order to see a video. The interesting thing about this particular attack is that the malicious Flash Player update is actually stored in a Dropbox account. Once executed, the malicious files try to **disable the Windows UAC, the firewall, the antivirus and other security features**. Ultimately, a variant of the notorious Sality virus is dropped onto victims' PCs. While the malware itself is flagged by most antivirus solutions, the initial .exe files are detected only by a handful of products. The campaign appears to be highly successful. Zscaler found that the malicious **website was visited by over 1,400 users in a single day**.

http://news.softpedia.com/news/Malicious-Flash-Player-Updates-Hosted-on-Dropbox-351239.shtml

New Yahoo Accounts Have Dropbox

This is a notice I got yesterday about turning on Dropbox within my Yahoo account.

"Have you noticed yet? Your Yahoo! Mail now has Dropbox built in! Now you can attach stuff from Dropbox to emails you send (even if they're over 25 MB), or save the attachments you receive back to Dropbox. Happy emailing, The Dropbox Team"



Risk-Based Decision Making Commentary
8 October 2013 Newsletter

Vulnerabilities in Microsoft Word Could Allow Remote Code Execution

Multiple vulnerabilities have been discovered in Microsoft Word that could result in remote code execution. Exploitation of these vulnerabilities may occur **if a user opens a specially crafted Word file** using Word in Microsoft Office 2003, Word in Microsoft Office 2007 or Microsoft Office Compatibility Pack SP3. Successful exploitation of these vulnerabilities could result in the **attacker gaining the same rights as the logged on user.** Depending on the privileges associated with the user, an attacker could then install programs, view, change, or delete data, or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

RISK:

Government:

- For Large and medium government entities: **High**
- For Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- View emails in plain text.
- Remind users not to open e-mail attachments from unknown users or suspicious e-mails from trusted sources.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.

https://technet.microsoft.com/en-us/security/bulletin/ms13-086

HALL ASSOCIATES

Cumulative Security Update for Internet Explorer

Multiple vulnerabilities have been discovered in Microsoft's web browser, Internet Explorer, which could allow an attacker **to take complete control of an affected system**. The systems affected are Internet Explorer 6, Internet Explorer 7, Internet Explorer 8, Internet Explorer 9, Internet Explorer 10 and Internet Explorer 11. Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

RECOMMENDATIONS:

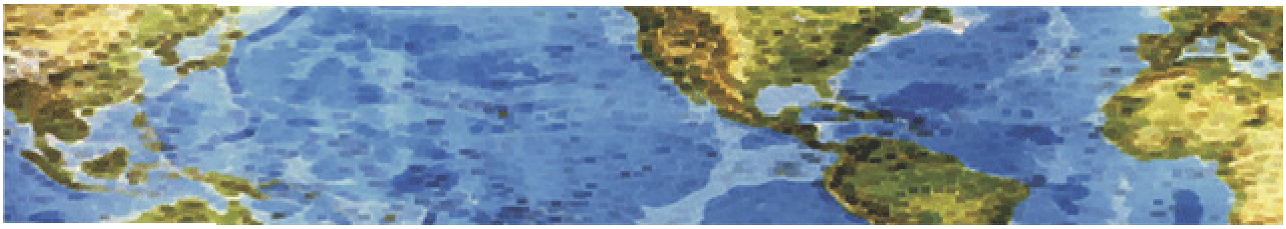
The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.

REFERENCE:

https://technet.microsoft.com/en-us/security/bulletin/ms13-080

HALL ASSOCIATES



Risk-Based Decision Making Commentary
9 August 2013 Newsletter

California Escrow Firm Shuttered after Losing $1.5 Million

A California escrow firm has been run out of business and its 9 employees laid off after a remote access Trojan planted on its computer system drained it of $1.5 million.   The funds got transferred in three fraudulent wire transfers. The first one, about $430K, went to Moscow and the other two, totaling $1.1 million, went to the Chinese province of Heilongjiang. The problems at this firm began in December 2012 with the first transfer. **Now, whatever money the firm has left is under the control of a court-appointed state receiver, who plans to sue the victimized company's bank in an effort to claw back the stolen funds.** The firm got the money sent to Moscow back, but has been unable to recover the funds sent to China.

When the firm reported the crime to California State regulators (required by state law), it was given 3 days to scrape together enough to replace the looted amount. When they were unable to do so, the state stepped in and closed it down. And up until a few weeks ago, all remaining funds have been locked up in a state-established conservatorship. The receiver is asking why the bank did not slam the brakes on the out-of-character overseas transfers. This firm had never sent wires overseas before, so why did the bank not pick up a phone and confirm the requested transactions? More information is available at nakedsecurity.sophos.com/2013/08/08.

Cybercriminals and nation-states attacking small businesses through their financial/accounting systems is indicative of a major trend over the past few years. Several security firms and the federal government has developed numerous "Banking Best Practices for Businesses". I have noted some of them below.

1. **Use a dedicated system to access your financial institution's site.** This machine should be restricted from visiting all but the handful of sites necessary to interact with a financial institution and manage your finances. This approach **ONLY** works if you access your financial institution's site **ONLY** from a locked-down, dedicated machine. Making occasional exceptions or using your smartphone undermines the whole purpose of this approach.
2. **Remove any unneeded software from your dedicated machine/system**. In particular, unneeded plugins such as Java should be eliminated.
3. **Use a bookmark to access your financial institutions site.** Avoid manually typing the address into a browser since a fat-fingered keystroke might send you to a look-alike phishing site or one that contains malware.
4. **If offered, take advantage of ACH Positive Pay.** Any item that fails to meet the criteria you set up will cause you to be notified via e-mail or text message before it is completed.
5. **Require two people to sign off on every transaction**. This is a fundamental anti-fraud technique.

HALL ASSOCIATES

MALWARE:

THE HIDDEN THREAT TO YOUR BUSINESS

Whether it's a Trojan horse, a worm, or a virus, battling computer malware is a full-time profession for software epidemiologists. Despite the fact that they are highly sophisticated, there are simple steps you can take to safeguard your business and your data from infectious software. Take a look at recent trends in computer infection and see how a little malware can cost you more than just a little lost productivity.

A cyber-attack that hit Harbor Freight Tools and likely exposed card data processed at all 400 of its retail tool stores could rank among one of the biggest retail breaches this year. Card fraud linked to retail breaches is a growing concern for banking institutions. Attacks on retailers ranked among the top two most common reasons for card-related fraud losses in the last 12 months.

Although Harbor Freight has not stated the number of cards potentially affected by the attack that hit its corporate network, three separate card issuers have confirmed that fraud linked to the tool store breach is growing, with new advisories about possible compromised card numbers coming out from card brands on a nearly daily basis. One issuer says more than 10,000 of its cardholders have so far been impacted; another issuer estimates more than 20,000 of its cardholders have been affected.

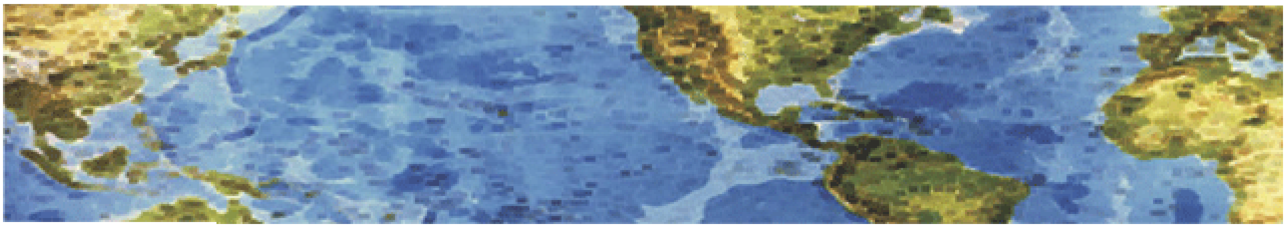
In a July 20 statement about the cyber-attack, the Harbor Freight President said the breach was "similar to attacks being reported by other national retailers," apparently making reference to **malware** attacks that have targeted other merchants, such as **Schnucks, Raley's**, upscale restaurant chain **Roy's Holdings Inc.** and convenience store chain **MAPCO Express**.

Now, one card fraud expert, who also asked to remain anonymous, says it seems, based on forensics details being revealed by various sources, that Harbor Freight's corporate network was attacked **<u>by three different strains of malware - two of which had never been seen before.</u>** All of the malware strains were equipped with built-in security features to prevent reverse-engineering detection.

The Harbor Freight breach affected transactions conducted between June 14 and July 20, according to advisories from Visa and MasterCard shared with Information Security Media Group. Issuers say they believe the breach many have occurred sooner. Another issuer says fraudulent transactions linked to the breach have ramped up within the last two weeks, signaling that the compromised numbers were likely sold in an underground forum. "We haven't necessarily experienced a large loss yet, but I think we are just at the beginning of this thing," that issuer notes. And a third issuer points out that fraudulent transactions associated with cards compromised in the Harbor Freight attack **<u>are showing up throughout the world.</u>** "We have seen significant attempts linked to Harbor throughout the world, as their aggressiveness in using the cards is increasing," that issuer points out.

<u>The Harbor Freight incident is one in a growing series of cyber-attacks affecting retailers</u>. For additional information, check out http://www.bankinfosecurity.com/new-retail-breach-among-2013s-biggest-a-5970/op-1.

HALL ASSOCIATES



Risk-Based Decision Making Commentary
April 10 2013 Newsletter

Secure Your Facebook Timeline

The new Facebook Timeline is supposed to make your profile look newspaper like and let you look at your older information instantly. Looking at the security and privacy implications of any new Facebook (or any social media application/feature) is essential and a couple of actions are recommended.

This new feature lets your friends, and depending on your privacy settings, complete strangers view and navigate with ease a comprehensive history of your (or your kids or employees) life as posted on Facebook. While most of your existing privacy settings are maintained in Timeline, there are three actions that you may want to consider to make it more secure.

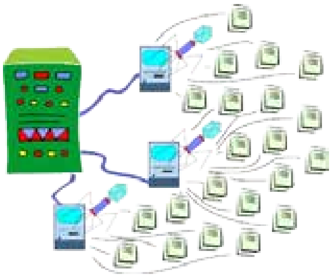
First, you can make all your past posts accessible to Friends only. When you first started using Facebook, you may have had more relaxed privacy settings than you do now. As a result, some of your older posts *(remember that everything you send/post is forever in this digital age)* may be more public than they should be. Timeline lets everyone navigate your older posts with ease. To cover this Facebook has a feature called “Limit the Audience for Past Posts”. This will change past posts from whatever their current state is to “Friends Only”. However, if friends are tagged in them, then friends of friends may still be able to see them. *And do you know who your friends have friended*?

Second, set your default privacy setting for future Timeline posts. You should customize your default setting for all future posts in the privacy settings menu so only your friends can see them.

Third, consider enabling the Timeline Review and Tag Review feature. Since there are things that you would never want posted on your Facebook page, it is useful that you can review and decide if something will appear on your Timeline before it is published. With the Timeline Review and Tag feature, you can review and decide if you want a post to be published prior to it showing up on your timeline.

http://netsecurity.about.com/od/securityadvisorie1/a/How-To-Secure-Your-Facebook-Timeline.htm

The http://netsecurity.about.com/od/newsandeditorial1/u/Protect-Mobile-Devices-Smart-Phones-Ipad-Mp3-Players-Etc.htm website provides a lot of information about how to protect your social network accounts and mobile devices.



vSkimmer Botnet Targeting Payment Card Terminals Connected to Windows

McAfee has shared details of a new botnet circulating on criminal forums, mostly out of Russia, which targets payment card terminals connected to Windows systems. The botnet, named **vSkimmer**, has been around since February and appears to be an ongoing project for the person selling it.

vSkimmer seems to be the successor to Dexter. Dexter is the financial malware responsible for the loss of nearly 80,000 credit card records and the successful breach of payment card data at scores of Subway restaurants in 2012. vSkimmer has more functionality when compared to Dexter. In a forum post, vSkimmer is pitched as an advanced tool that will capture credit card data from systems running Windows that host payment processing software. vSkimmer is supposed to detect card readers and capture all of the track data collected, encrypt the data and ship it off to a control server for later retrieval. It uses a whitelisting routine to look for actionable processes, by checking each process run on the system that isn't on the ignore list and using pattern matching to extract the card's Track 2 data. Track 2 is where the card number, three-digit CVV code, and expiration date are stored on your card.

If present in the terminal software, vSkimmer says it will also ferret out any additional data, including names and PINs. This botnet is particularly interesting because it directly targets card-payment terminals running Windows. Like Dexter, vSkimmer is said to be completely undetectable on the compromised host.

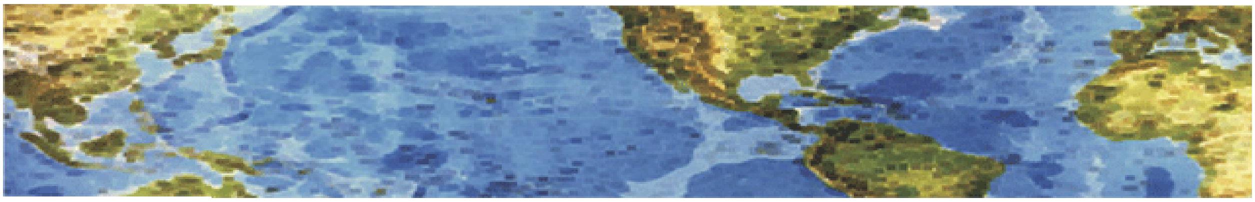
http://www.securityweek.com/vskimmer-botnet-targeting-payment-card-terminals-connected-windows

Spear-Phishing Attack Targeting Android Devices

This is part of an emerging trend – phishing attacks using Trojans that can compromise not just mobile devices, but also the PCs and Macs that these devices connect to. This particular attack involved an APK – a program for the Android operating system that allows users to download G-mail attachments. This malware has the ability to secretly report back information about the user to a server and could harvest information such as contacts, call logs and SMS/text messages stored on your device. Having access to contacts is one of the things a scammer needs to make a spear phishing campaign successful. Scammers are increasingly gathering information about mobile and online users through groups they are affiliated with and social media channels (see the above Facebook note).

http://www.govinfosecurity.com/interviews/spear-phishing-goes-mobile-i-1877

HALL ASSOCIATES



Risk-Based Decision Making Commentary
11 June 2013 Newsletter

Can Your Car Be Hacked??

You might be behind the wheel, but increasingly, computers control your car's every function. Microprocessors direct braking, acceleration and even the horn these days. There can be anywhere from 30 to 40 microprocessors in most cars and even up to 100 different ones running different functions in some vehicles. But could a hacker compromise these systems? Recently, several news reports have raised the issue of car-hacking risks, including:

Vehicle disablement. After a disgruntled former employee took over a Web-based vehicle-immobilization system at an Austin, Texas, car sales center, more than 100 drivers found their vehicles had been disabled or their horns were honking out of control.

Tire pressure system hacking. Researchers from the University of South Carolina and Rutgers University were able to hack into tire pressure monitoring systems. Using readily available equipment and free software, the researchers triggered warning lights and remotely tracked a vehicle through its unique monitoring system.

Disabling brakes. Researchers at the University of Washington and University of San Diego created a program that would hack into onboard computers to disable brakes and stop the engine. The researchers connected to onboard computers through ports for the cars' diagnostic system.

Is your car at risk? Most of the danger right now may come from hackers who want to demonstrate their prowess and enhance their reputations. And the increased reliance on wireless systems makes your car more vulnerable to these attacks.

Protect your car from hacking. Security is largely in the hands of auto manufacturers, who are working to address concerns. In the meantime, you can take these steps to protect your vehicle:

1. Ask about wireless systems. Familiarize yourself with the wireless systems if you're purchasing a new car. For a car you already own, you can review your manual or check online. Find out if any of the systems can be operated remotely.

2. Go to reputable dealers and repair shops. It's possible for unscrupulous garages to manipulate your car's computer systems, making it appear you need repairs that aren't actually warranted. Don't cut corners when it comes to choosing a dealer or repair shop.

3. Protect your information. Of course, locking your car is always wise. And if you use OnStar -- the GM-owned auto security and information service -- make sure you don't leave OnStar-related documents or your password in the car. Since OnStar can remotely shut off your engine if you report the vehicle stolen, there's the potential for mischief if your password falls in the wrong hands.

4. Be cautious about after-market devices. After-market car systems may not be as rigorously tested or designed, opening you to vulnerabilities.

You can compare the use of computers in cars to the development in our use of personal computers. Hacking exploded when the Internet evolved, making it easy to access computers via networks. Wireless connections mean your car is no longer a closed system. Once you have connection to vehicles, you have an entry point for people to try to access. The only thing standing in their way now is a standardized piece of software. It's a concern we need to address. ***http://us.norton.com/yoursecurityresource/detail.jsp?aid=car_computer***

5 Social Media Scams

We’re wired to be social creatures. Facebook draws 175 million logins every day. But with this tremendous popularity comes a dark side as well. Virus writers and other cybercriminals go where the numbers are -- and that includes popular social media sites. To help you avoid a con or viral infection, we’ve put together this list of five social media scams.

5. Chain Letters

You’ve likely seen this one before -- the dreaded chain letter has returned. It may appear in the form of, "Retweet this and Bill Gates will donate $5 million to charity!" But hold on, let’s think about this. Bill Gates already does a lot for charity. Why would he wait for something like this to take action? Answer: He wouldn’t. Both the cause and claim are fake. So why would someone post this? Good question. It could be some prankster looking for a laugh, or a spammer needing "friends" to hit up later. Many well-meaning people pass these fake claims onto others. Break the chain and inform them of the likely ruse.

4. Cash Grabs

By their very nature, social media sites make it easy for us to stay in touch with friends, while reaching out to meet new ones. But how well do you really know these new acquaintances? That person with the attractive profile picture who just friended you -- and suddenly needs money -- is probably some cybercriminal looking for easy cash. Think twice before acting. **In fact, the same advice applies even if you know the person.** Picture this: You just received an urgent request from one of your real friends (or a relative) who "lost his wallet on vacation and needs some cash to get home." So, being the helpful person you are, you send some money right away, per his instructions. But there’s a problem: Your friend never sent this request. In fact, he isn’t even aware of it. His malware-infected computer grabbed all of his contacts and forwarded the bogus email to everyone, waiting to see who would bite. Again, **think before acting**. Call your friend or relative/family member. Inform them of the request and see if it's true. **Next, make sure your computer isn't infected as well**.

3. Hidden Charges

"What type of STAR WARS character are you? Find out with our quiz! All of your friends have taken it!" Hmm, this sounds interesting, so you enter your info and cell number, as instructed. After a few minutes, a text turns up. It turns out you’re more Yoda than Darth Vader. Well, that’s interesting … but not as much as your next month’s cell bill will be. You’ve also just unwittingly subscribed to some dubious service that charges $9.95 every month. As it turns out, that "free, fun service" is neither. **Be wary of these bait-and-switch games.**

2. Phishing Requests

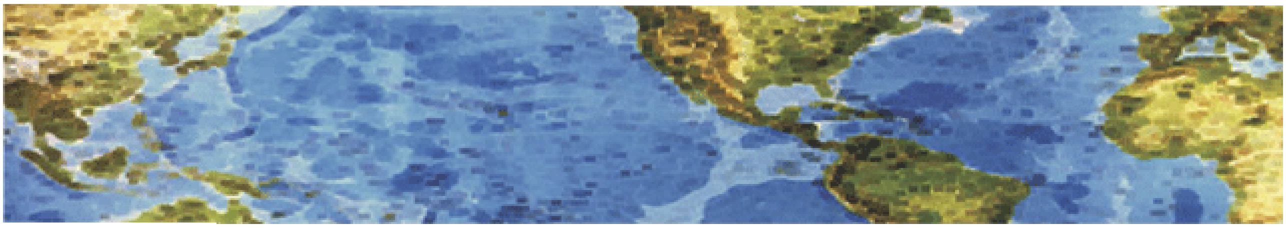
"Somebody just put up these pictures of you drunk at this wild party! Check 'em out here!" Huh?? Immediately, you click on the enclosed link, which takes you to what looks like your Twitter or Facebook login page. There, you enter your account info -- and a cybercriminal now has your password, along with total control of your account. So both the email and landing page were fake. That link you clicked took you to a page that only looked like your intended social site. You've just been had. To prevent this, make sure your Internet security includes antiphishing defenses and think before you act. Only go to your social media page by typing in the URL or using your favorites link. Don’t click on an e-mail link.

1. Hidden URLs

Beware of blindly clicking on shortened URLs. You'll see them everywhere on Twitter, but you never know where you're going to go since the URL hides the full location. Clicking on such a link could direct you to your intended site, or one that installs all sorts of malware on your computer. URL shorteners can be quite useful. Just be aware of their potential pitfalls and make sure you have real-time protection against spyware and viruses. Bottom line: **Sites that attract a significant number of visitors are going to lure in a criminal element, too.** If you take security precautions ahead of time, such as using antivirus and anti-spyware protection, you can kinda defend yourself against these dangers.

http://us.norton.com/yoursecurityresource/detail.jsp?aid=social_media_scams

HALL ASSOCIATES



Risk-Based Decision Making Commentary
12 December 2013 Newsletter

With each new year, comes a new round of cybersecurity risks – and most of the old ones are still risks also.

What we are doing is not working. We need to review what we are doing and why. We need to re-evaluate everything, from passwords to pentests to firewalls to DLP. We have to stop doing the same thing over and over again and expecting different results each time. Companies and individuals need to start looking for alternative security technologies to augment or outright replace many of the technologies and policies that have failed time and time again. To help businesses and individuals prepare for the year ahead with appropriate risk mitigation and response solutions several companies and security individuals have identified cybersecurity trends that indicate a changing tide in cyber standards. Responding appropriately to these trends will require all size organizations and individuals to take stronger actions and safeguards to protect against reputational, financial and legal cybersecurity risks.

The new cybersecurity issues for 2014 will include:

National Institute of Standards and Technology (NIST) and similar security frameworks will become the de facto standards of best practices for all companies: Cybersecurity strategies largely designed for companies that were part of the "critical infrastructure" will become more of an expectation for everyone, from conducting an effective risk assessment to implementing sound cybersecurity practices and platforms. Organizations that don't follow suit may find themselves subject to lawsuits by individuals and companies, actions by regulators and other legal repercussions.

As new laws are passed that reflect the NIST guidelines and look more like the EU privacy directive, all size U.S. companies will find themselves ill-prepared to effectively respond to the regulations, if they even know them. To minimize your risk, companies will have to get smart on these standards and make strategic business decisions that give clients and customers confidence that their information is protected.

The data supply chain will pose continuing challenges to even the most sophisticated companies: It is not unusual for companies to store or process the data they collect by using third parties. However, the security that these third parties use to safeguard their client's data is frequently not understood by companies that hire them until there is a breach. Companies need to vet their subcontractors closely and get specific as to the technical and legal roles and responsibilities of these subcontractors in the event of a breach. This requires technical, procedural and legal reviews.

The malicious insider remains a serious threat, but will become more visible: Information technology has simply made the insider’s job easier. In 2014, a significant number, almost half, of data breaches will come at the hands of people on the inside. However, as the federal government and individual states add muscle to privacy breach notification laws and enforcement regimes, these hidden insider attacks will become more widely known. Thwarting an insider threat requires collaboration by general counsel, information security and human resources.

Corporate boards (and individual CEOs) need to take a greater interest in cybersecurity risks and the organization's plans for addressing them: With more and more data breaches covering more and more people- from theft of trade secrets to loss of customer information - in the headlines, management should focus on the connection between cybersecurity and an organization's/individual's financial well-being. For example, what are your strategic plans for protecting non-public information? Management also needs to look at risk-mitigation plans for responding to a possible breach. As corporate boards carry out their fiduciary responsibilities, they must also protect the company from possible shareholder lawsuits (and lawsuits and class action lawsuits for those caught up in the data breach) that allege the company's cybersecurity wasn't at a level that could be reasonably viewed to be 'commercially reasonable' and that incident response plans weren't in place to mitigate the risk. The challenge management faces is determining what is a reasonable level of security and response, and who should make that call. Is it their IT team, an industry expert, an independent third party?

Sophisticated tools will enable smart companies to quickly uncover data breach details and react faster: Management must realize that even the best firewalls and intrusion detection systems cannot stop all attacks. But technological progress that occurred over the last 12 months will enable companies to unravel events and see with near–real-time clarity what's happened to their data and how much damage has been done. Most organizations have invested in preventative security technologies, but remain unprepared to launch an effective response to a leak or intrusion. Without the right tools and policies in place beforehand, they find themselves suddenly under intense pressure to investigate, track and analyze events.

New standards related to breach remediation are gaining traction and will have a greater impact on corporate data breach response: Credit monitoring will no longer be the gold standard in breach remediation in 2014, as lawmakers, consumer advocates and the public at large continue to raise questions about the relevancy and thoroughness of this as a stand-alone solution. These parties will demand a more effective alternative. While no legal guidelines currently exist for consumer remediation, the FTC and states like California and Illinois are already offering guidance that suggests a risk-based approach to consumer remediation will be the way of the future.

As cloud and BYOD adoption continues to accelerate, implementing policies and managing technologies will require greater accountability: The development and evolution of cloud services and BYOD have moved at a whirlwind pace, leaving IT departments scrambling to get out in front of the technologies and employee usage. In 2014, IT leaders will need to work closely with senior leadership and legal counsel to adapt policies in a way that addresses changing legal risks, while effectively meeting the needs of the organization. Organizations must realize that even if they don't want to deal with this, they're not going to have much choice.

Expect to see a sharp increase in attacks against end-users and administrators who are accessing and controlling cloud-based services (both public and private clouds). Much of the focus is on the security of the cloud itself but very often the end-users are left to their own while connecting from less secure public networks. Administrators in particular will be targeted as they hold the keys to the cloud-based kingdom.

Expect to see large increases in attacks (i.e. Cryptolocker) against individuals and individual computers in networks. Once such ransomware gets into any computer, the entire network it may be attached to is at risk.

This will be the year for advancements in authentication. Even though good multi-factor authentication systems have existed for years, most organizations and individuals have relied on passwords to the exclusion of these other technologies despite clear demonstrations that usernames and passwords just aren't enough.

With the continued development and proliferation of intelligent portable electronic devices (smartphones, tablet computers, etc.), we will see a significant rise in account compromises resulting from the credentials for those accounts being stored on unsecured devices. While the user may have selected a password of sufficient length, when it's stored on an unsecured device it may be easily recoverable by an attacker.

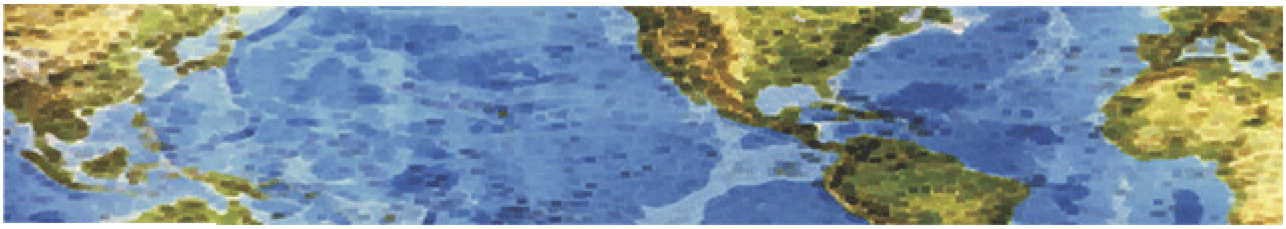
The Internet of Devices will become security critical: Up to now, the internet connected mostly people. The end point of an internet connection was usually implemented using a PC, a server or more lately tablets and phone. But foremost, a person was operating and using the device connected to the network. In parallel to this "internet for people" we always had an "internet for devices": Small control systems and embedded devices that delivered metrics and control to other devices or larger control networks. Up to now, the proliferation of these devices was limited to specialized networks and environments. However, in particular the advent of IPv6, and the continuation of Moore's law to deliver cheaper and more powerful devices, will make it much easier to deploy devices ubiquitously. We already see a surge in internet controlled home automation and alarm systems. Cars with not one but several IP addresses, sub $50 "servers" as implemented in the Raspberry Pi project and projects like Androino to deliver sensory and control capabilities to the masses. These technologies frequently take advantage of cloud computing to supplement their limited computing capacity and heavily rely on commodity networks for data exchange. We have seen successful attacks against these devices by exploiting unsecured communication networks and will see an explosion in such attacks. Later on, complete takeover of the device by injecting exploit code into the insecure communication stream may be achieved.

The new HTML5 web specification has device geolocation baked in. With just a few lines of code, any website can now enable geolocation features, potentially leaving geo-artifacts on any device with a web browser. The recent US Supreme Court case, U.S. vs. Jones, demonstrates how interested law enforcement has been in geolocation monitoring. There will be a much wider range of investigators, both public and private, beginning to take advantage of geo-artifacts present on nearly every computer and mobile device, giving the ability to put the device at a particular place at a particular time.

Financial institutions will increasingly deploy mobile and cloud technologies and integrate their partners, suppliers and customers, so that their data perimeters are becoming much harder to define. As a result, they will have to essentially redefine the concept of a network perimeter. They should do this by developing a much more dynamic cyber security approach that includes customer training, outside connections cybersecurity audits, actionable threat intelligence, advanced adversary hunting as well as data protection and access controls developed at a much greater degree of granularity.

Can find additional information at the following:
http://www.businessnewsdaily.com/5563-7-cybersecurity-risks-for-2014.html
http://www.sans.edu/research/security-laboratory/article/2140
http://www.boozallen.com/media-center/press-releases/48399320/booz-allen-releases-annual-cyber-security-trends-for-2014

HALL ASSOCIATES



Risk-Based Decision Making Commentary
12 May 2013 Newsletter

7 Ways to Protect Your Small Business (or any business) from Fraud and Cybercrime

How secure are your small business assets from fraud, identity theft and cybercrime?
According to the Association of Certified Fraud Examiners (ACFE), **companies with less than 100 employees lose approximately $155,000 as a result of fraud each year.** Small businesses also have a higher fraud rate than larger companies and non-business owners. One of the most frequent sources of fraud is credit card abuse – largely due to the fact that few business owners actually take the time to go through every line item on their bill or choose to mingle business and personal accounts. Other sources of fraud stem from an overall lack of security across the business – such as inadequate network and computer security and a lack of background checks when hiring employees.

Don’t be a victim! Here are some tips you can take to better protect your business from some common forms of fraud and cybercrime.

Protect Your Credit Cards and Bank Accounts

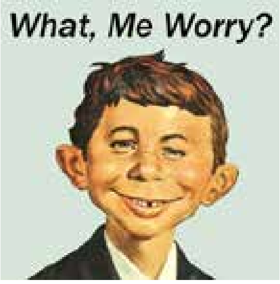
Since this is a common area of fraud for everyone from sole proprietors to employee-based firms, this one goes at the top of the list. Start by separating your personal banking and credit cards from your business accounts – this will ensure fraudsters don’t get their hands on ALL your money. Separating your accounts will also make it easier to track your business expenses and report deductions on your tax return. Be sure to check your online banking every day for suspicious activity.

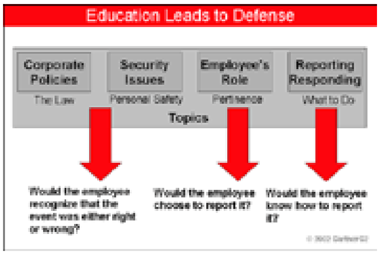
Secure Your IT Infrastructure

Every business owner should invest in a firewall as well as anti-virus, malware and spyware detection software. Backing-up is also a must and will make it a lot easier for you to continue working in the event of a cyber attack.

Use a Dedicated Computer for Banking

Use a dedicated computer for all your online financial transactions and, ideally, make sure it’s one that isn’t used for other online activity such as social media, email and web-surfing which can open up the machine to vulnerabilities. Avoid mobile banking if you can.





Education Leads to Defense

Topics

- Corporate Policies – The Law
- Security Issues – Personal Safety
- Employee's Role – Pertinence
- Reporting Responding – What to Do

Would the employee recognize that the event was either right or wrong?

Would the employee choose to report it?

Would the employee know how to report it?

Have a Password Policy

Another easy step you can take to protect your IT systems is to institute a password policy.
Make sure you and your employees change them regularly (every 60 to 90 days is good rule)
Set rules that ensure passwords are complex (i.e. contain one upper case letter, one number and must be a minimum of eight characters). Use different passwords for different online and system accounts.

Educate Your Staff

Employees are perhaps your biggest point of vulnerability when it comes to fraud, but they are also your first line of defense. **Hold regular training sessions on basic security threats** (online and off) and prevention measures – both for new hires and seasoned staff. Enforce the training by instituting policies that guide employees on the proper use and handling of company confidential information, including financial data, personnel and customer information.
For ideas on what to include in your training, check out the resources offered by small business groups like your local Small Business Development Center or Women's Business Center (find one near you here), you could also look out for free online webinars from security organizations and businesses.

Consider Employee Background Checks

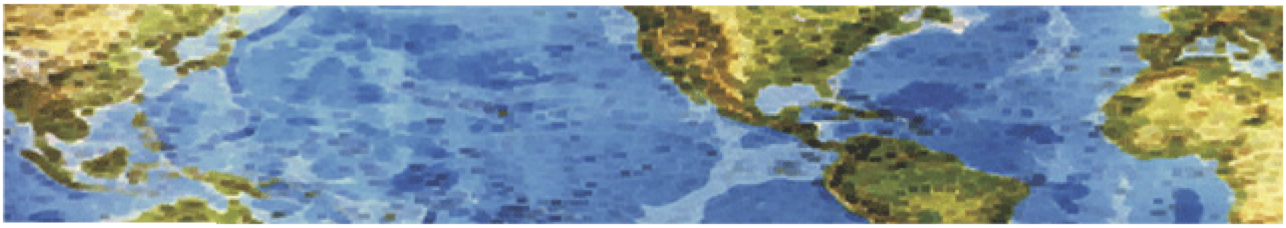
One of the first steps to preventing fraudulent employee behavior is to make the right hiring decision. Basic pre-employment background checks are a good business practice for any employer, especially for those employees who will be handling cash, high-value merchandise, or have access to sensitive customer or financial data. This blog offers tips on which background checks you can legally pursue and some tips for doing your own detective work: Conducting Employee Background Checks – Why Do It and What the Law Allows.

Insure Your Business

Fraud and cybercrime does happen; however, you can still seek to cover your damages by purchasing an insurance policy that protects you against any losses that you may incur from crime or fraud. Remember, your normal Errors and Omissions and Liability insurance DOES NOT cover cybercrimes, breaches and identity theft. You need special cyber insurance for that. Likewise, find out what your bank is willing to do to help you out if your credit card or business account is compromised.

http://www.sba.gov/community/blogs/7-ways-protect-your-small-business-fraud-and-cybercrime

HALL ASSOCIATES



Risk-Based Decision Making Commentary

13 November 2013 Newsletter

The Second Operating System Hiding In Every Mobile Phone

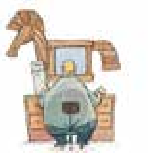
Every smartphone or other device with mobile communications capability (e.g. 3G or LTE) actually runs not one, but two operating systems. Aside from the operating system that we as end-users see (Android, iOS, PalmOS), it also runs a small operating system that manages everything related to radio. Since this functionality is highly timing-dependent, a real-time operating system is required. This operating system is stored in firmware, and runs on the baseband processor. This baseband RTOS is always entirely proprietary, handling everything from USB to GPS.

The problem here is clear: these baseband processors and the proprietary, closed software they run are poorly understood, as there's no proper peer review. You may have the most secure mobile operating system in the world, but you're still running a second operating system that is poorly understood, poorly documented and proprietary. These operating systems have a complicated codebase written in the '90s - complete with a '90s attitude towards security and barely any exploit mitigation, so exploits are free to run amok. What makes it even worse, is that **every baseband processor inherently trusts whatever data it receives from a base station** (e.g. in a cell tower). Nothing is checked, everything is automatically trusted. Lastly, the baseband processor is usually the master processor, whereas the application processor (which runs the mobile operating system) is the slave. So, each smartphone has a complete second operating system with very little exploit mitigation, which automatically trusts every instruction, piece of code, or data it receives from the base station you're connected to. What could possibly go wrong?

You can do some crazy things with these operating systems using exploits. For instance, you can turn on auto-answer. This uses a command language for modems designed in 1981, and it still works on modern baseband processors found in smartphones today. The auto-answer can be made silent and invisible, too. While we can maybe assume that the base stations in cell towers operated by large carriers are "safe", the fact of the matter is that base stations are becoming a lot cheaper, and are being sold on eBay. There are even open source base station software packages. Such base stations can be used to target phones. **Put a compromised base station in a crowded area -** or even a financial district or in a conference center - and you can remotely turn on microphones, cameras, place rootkits, place calls/send SMS messages to expensive numbers, and so on.

It's kind of a sobering/scary thought that the mobile communications we all use actually pivots around software that is of dubious quality, poorly understood, entirely proprietary, and wholly insecure by design. Another reason to ensure that you encrypt all data on mobile devices and be very careful about using mobile devices for important work or connecting to your networks.

http://www.osnews.com/story/27416/The_second_operating_system_hiding_in_every_mobile_phone



Online Banking Best Practices for Businesses

The best way to avoid becoming a victim of a cyberheist **is not to let computer crooks into the computers you use to access your organization's financial accounts online.** The surest way to do that is to maintain a clean computer: Start with a fresh install of the operating system and all available security updates, or adopt a "live CD" approach.

Use a dedicated system to access the bank's/financial institution's site. The dedicated machine should be restricted from visiting all but a handful of sites necessary to interact with the financial institution and manage the organization's finances. This can be done using custom firewall rules and hosts files, or services like OpenDNS. Remember that the dedicated system approach **only works if you only** access your financial institution's site from locked-down, dedicated machines. Making occasional exceptions undermines the whole purpose of this approach.

If possible, use something other than Microsoft Windows. Most malware only runs in a Microsoft Windows environment, so using a different operating system for the dedicated machine is an excellent way to drastically reduce the likelihood of becoming a cyberheist victim. A "live CD" is a free and relatively painless way to temporarily boot a Windows PC into a Linux environment. The beauty of this approach is that even if you fail to maintain a clean Windows PC, malicious software can't touch or eavesdrop on your banking session while you're booted into the Live CD installation. Your IT support can let you know how to set up a Live CD session.

If you must use a multi-purpose machine where you will check email, **avoid clicking links in email** (see some of my previous newsletters). Also, set email to display without HTML formatting if possible.

If you installed it, patch it. Keep the operating system and all applications up-to-date with patches. It's important to update the third-party software on your system, especially browser plugins. One leading cause of malware infections are exploit kits, which are attack tools stitched into hacked Web sites that exploit unlatched or undocumented vulnerabilities in widely-used browser plugins.

Remove any unneeded software from dedicated systems used to access the financial institution's site. In particular, unneeded plugins (such as Java) should be junked.

Avoid opening attachments in email that you were not expecting. Be particularly wary of emails that warn of some dire consequence unless you take action immediately.

Use a bookmark to access the financial institution's site. Avoid "direct navigation," which involves manually typing the bank's address into a browser; a fat-fingered keystroke may send you to a look-alike phishing Web site or one that tries to foist malicious software.

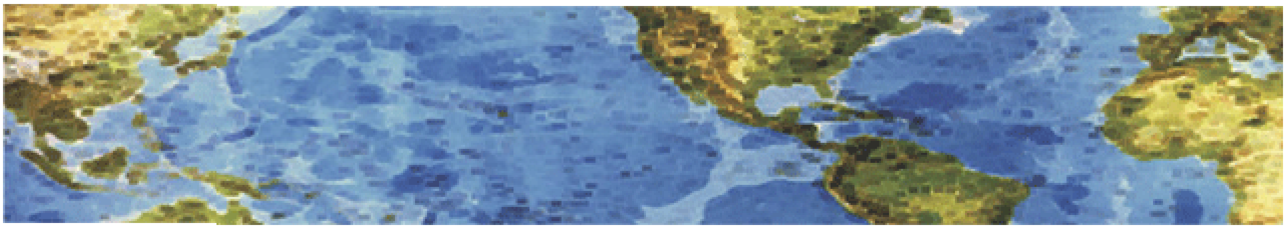
Remember that antivirus software is no substitute for common sense. A majority of today's cyberheists begin with malware that is spread via email attachments. Many of these threats will go undetected by antivirus tools in the first days/weeks. Be aware of social engineering.

If your financial institution offers it, consider taking advantage of ACH Positive Pay. Any item that meets the criteria you establish will automatically post to your account. Your company will be notified via email and/or text message of any rejected electronic item(s) that do not meet your filter criteria. Upon receipt of the rejected items, you can then return them or conveniently add filter criteria for future electronic transactions.

Require two people to sign off on every transaction. This fundamental anti-fraud technique can help block cyberheists (and employee fraud).

http://krebsonsecurity.com/online-banking-best-practices-for-businesses/

HALL ASSOCIATES



Risk-Based Decision Making Commentary
14 October 2013 Newsletter

Open Enrollment Is Phishing Season
Fraudsters Target Those Signing Up for Health Insurance

Open enrollment has begun for Obamacare as well as for health insurance plans offered by many employers. And that means it's prime time for fraudsters to target consumers with phishing scams, disguised as official-looking open enrollment messages, in an attempt to steal personal information. **Privacy and security experts stress the need to remind those participating in open enrollment about the dangers of phishing, including avoiding clicking on links in suspicious e-mails that bring individuals to fake websites designed to gather information.**

Health Benefits Ploy

The open enrollment scams typically involve e-mails that purport to be official communications about health insurance but link the user to a fake employee or government web portal designed to collect personal information that can be used to commit fraud. In some cases, simply clicking to open the e-mail or a link it contains can lead to an immediate malware infection.

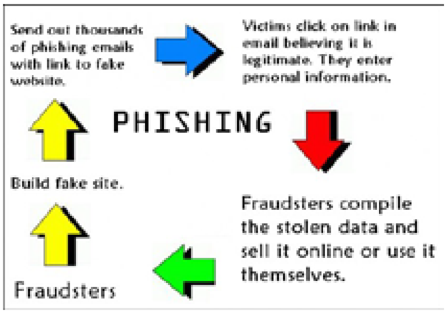
In addition to spear-phishing e-mails targeting employees at specific companies during open enrollment season, scammers are also targeting consumers who are interested in shopping for insurance on new state health insurance exchanges and seniors looking for supplemental Medicare plans. Even before new state health insurance exchanges under Obamacare launched on Oct. 1, scammers began sending consumers spam containing the terms "Medicare," "enrollment" and "medical insurance." The spam contained links taking users to nefarious websites containing surveys asking for personal information in exchange for a chance to win prizes, such as iPhones.

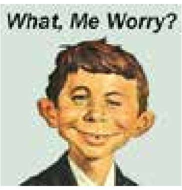
Steps to Take

To prevent employees from becoming victims of these scams, organizations must educate them to avoid opening e-mail from unrecognized senders and refrain from opening attachments or clicking on links that look suspicious. Employers also should take the extra step of alerting employees in advance that the company, or its outside benefits contractor, will be sending employees messages about open enrollment information. Alert employees to notify company officials when they receive suspicious e-mails.

http://www.bankinfosecurity.com/open-enrollment-phishing-season-a-6135

HALL ASSOCIATES


Send out thousands of phishing emails with link to fake website.
Victims click on link in email believing it is legitimate. They enter personal information.
PHISHING
Build fake site.
Fraudsters compile the stolen data and sell it online or use it themselves.
Fraudsters



Recent Spear-Phishing Incident

A recent healthcare-related spear-phishing incident at St. Louis University demonstrates that the scams can hit at any time. The scam e-mail about a systems update sent to 180 SLU employees, including physicians at the university's medical group, contained a link to a fake site that looked like the SLU's employee portal. Several employees were fooled into entering personal information related to their direct deposit accounts.

The phishing e-mail contained the university's logo and was well-written. However, a keen eye would have noticed that the link in the e-mail contained an incorrect URL for the university's employee portal. The university's investigation found that 10 employees had direct deposit information changed, although no unauthorized financial transactions had occurred. However, the university also learned that the incident resulted in unauthorized access to about 20 SLU e-mail accounts that contained personal health information for approximately 3,000 individuals. and Social Security numbers of about 200 people. SLU is offering affected individuals a year's worth of free credit monitoring and identity theft protection services. As a result of the phishing incident, SLU is ramping up employee education.

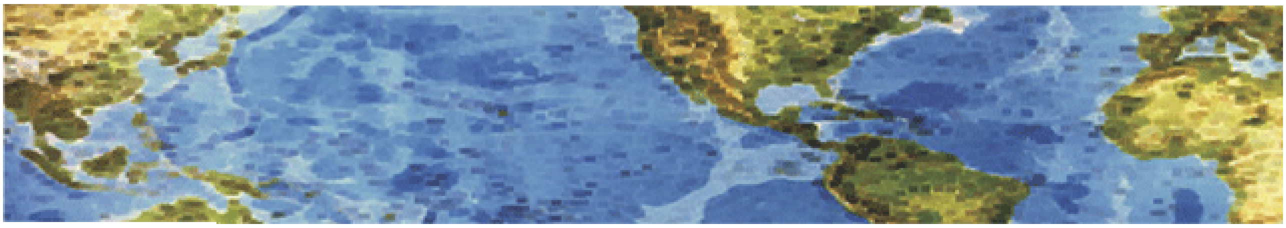
http://www.govinfosecurity.com/open-enrollment-phishing-season-a-6135/op-1

Breaches: Holding Retailers Accountable

The Vermont Attorney General's $30,000 settlement with a breached retailer is significant because it demonstrates that states can play a role in holding retailers accountable for losses associated with card fraud, one banker says. As a result of this case, more banking institutions may ask state attorneys general to conduct investigations after card fraud is linked to a retailer. That's because attorneys general enforce state laws, which may call for timely breach notification and establish security requirements, including compliance with the Payment Card Industry Data Security Standard.

Last month, the Williston, Vt.-based grocery chain Natural Provisions agreed to pay a $15,000 fine to settle allegations that it failed to promptly notify customers of a breach dating back to 2012. Natural Provisions also agreed to spend $15,000 on security upgrades to its point-of-sale system. According to Vermont Attorney General William Sorrell, Natural Provisions' lax security contributed to the breach that resulted in tens of thousands of dollars in fraud losses linked to compromised cards. In the settlement with Natural Provisions, Sorrell claims Natural Provisions failed to address, in a timely manner, security weaknesses that allowed its payments network to be compromised and an undetermined amount of card data was stolen.

http://www.bankinfosecurity.com/breaches-holding-retailers-accountable-a-6138



Risk-Based Decision Making Commentary
16 August 2013 Newsletter

At $1.2M, Photocopy Breach Proves Costly

The U.S. Department of Health and Human Services has settled with Affinity Health Plan, a New York-based managed care plan, for HIPAA violations to the tune of $1,215,780 **after a photocopier containing patient information was compromised.** Affinity filed a breach report with the HHS Office for Civil Rights on April 15, 2010, as required by the HITECH Breach Notification Rule.

Affinity officials were informed by CBS Evening News that, as part of an investigatory report, the television network had purchased a photocopier, previously leased by Affinity, that contained confidential medical information on its hard drive. Affinity estimated that up to 344,579 individuals may have been affected by this breach. An HHS Office for Civil Rights investigation indicated that Affinity impermissibly disclosed the protected health information of these affected individuals **when it returned multiple photocopiers to leasing agents without erasing the data contained on the copier hard drives**. Moreover, the investigation revealed that Affinity failed to incorporate the electronic protected health information stored on photocopier hard drives in its analysis of risks and vulnerabilities as required by the Security Rule, and failed to implement policies and procedures when returning the photocopiers to its leasing agents.

This settlement illustrates an important reminder about **any equipment** designed to retain electronic information: **Make sure that all personal information is wiped from hardware before it's recycled, thrown away or sent back to a leasing agent.** HIPAA covered entities are required to undertake a careful risk analysis to understand the threats and vulnerabilities to individuals' data, and have appropriate safeguards in place to protect this information. In addition to the $1,215,780 payment, the settlement includes a corrective action plan requiring Affinity to use its best efforts to retrieve all hard drives that were contained on photocopiers previously leased by the plan that remain in the possession of the leasing agent, and to take certain measures to safeguard all PHI.

The HIPAA Privacy Rule requires that covered entities apply appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information. That means, "reasonable safeguards to limit incidental, and avoid prohibited, uses and disclosures of PHI, including in connection with the disposal of such information.“ Additionally, it requires covered entities to address "the final disposition of electronic PHI and/or the hardware or electronic media on which it is stored, as well as to implement procedures for removal of electronic PHI from electronic media before the media are made available for re-use.“ For electronic media that means "clearing (using software or hardware products to overwrite media with non-sensitive data), purging (degaussing or exposing the media to a strong magnetic field in order to disrupt the recorded magnetic domains), or destroying the media (disintegration, pulverization, melting, incinerating, or shredding)."

http://www.healthcareitnews.com/news/12m-photocopy-breach-proves-costly give some more detail on this settlement and http://www.healthcareitnews.com/news/old-it-new-tricks?single-page=true discusses dealing with old equipment in a HIPPA-compliant way.

Cyber Sextortion – Something to warn our kids and employees about

Newly crowned Miss Teen USA Cassidy Wolf is allegedly the latest victim of sextortion. According to the LA Times, the FBI confirmed on Wednesday that it's investigating claims by Wolf and other women who say that their webcams were hacked, photos or video were taken surreptitiously, and that the hacker or hackers then demanded money in exchange for keeping the photos out of public disclosure.

19-year-old Ms. Wolf has told reporters that prior to being crowned, she received an anonymous email from someone who claimed to have nude photos of her, taken via the webcam on her computer. Wolf told Today News that about four months ago, Facebook notified her about somebody trying to log into her account from another state. She then received an email saying that the person had photos of her taken in her bedroom via her computer's hacked webcam. The person, who hasn't been named in the ongoing federal investigation, tried to extort her in exchange for keeping the photos from being made public.

As if everyday webcam hacking weren't shocking enough, this case apparently involves a webcam that was hacked without the telltale camera light coming on to indicate that it was recording. This is how Ms Wolf tells it: "I wasn't aware that somebody was watching me [on my webcam]. The [camera] light didn't even go on, so I had no idea.“ Note that Some laptops allow you to turn the light on and off in software, others only work physically. So this is certainly possible, if unlikely. But if it's unlikely to suffer a webcam hacking that manages to turn off the camera's "on" light, plain old vanilla webcam hacking that leaves the light on isn't very unlikely at all.

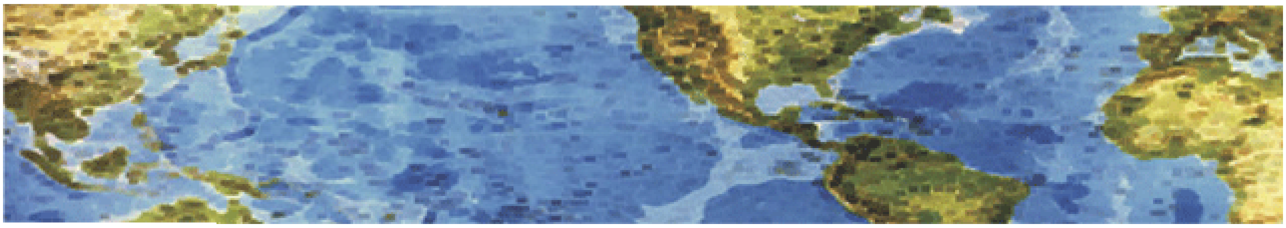
In fact, as the BBC reported in June, there's a thriving black market for access to computers whose webcams have been compromised. Stolen webcam video of females cost $1 per "slave," as they're called. Stolen video of male slaves goes for $1/100 slaves.

If you have a webcam on your computer or tablet, keep an eye on the light. That, evidently, won't stop remote hackers of webcams who manage to turn off the camera light via accessing its software.

But given that such a hack is less likely than one turning on the light, it's still **a good idea to keep an eye on the light. Better still, cover it with a patch - a tiny piece of black tape, say, or a sticker or bandage - when you're not using the camera.** Also make sure your security applications (really, all applications and programs) are up-to-date, routinely clear your browsing history and change passwords into something difficult to guess.

http://nakedsecurity.sophos.com/2013/08/15/miss-teen-usa-2013-says-sextortionist-hacked-webcam-to-snap-bedroom-photos/?utm_source=Naked+Security+-+Sophos+List&utm_medium=email&utm_content=Yahoo%21+Mail&utm_campaign=b434c846c1-naked%252Bsecurity&utm_term=0_31623bb782-b434c846c1-454959897
http://www.latimes.com/local/lanow/la-me-ln-fbi-investigating-sextortion-case-targeting-miss-teen-usa-20130814,0,4440441.story

HALL ASSOCIATES



Risk-Based Decision Making Commentary
16 November 2013 Newsletter

Cyber Monday and Online Shopping Season: What You Need to Know to Protect Yourself

Online holiday shopping continues to grow in popularity. According to American Express, for the first time, more people are expected to shop online on Cyber Monday than visit brick and mortar stores on Black Friday. Shoppers are expected to spend nearly $62 billion online throughout the holiday season this year, up more than 15% from 2012. The use of mobile devices for online shopping is projected to reach almost $10 billion for the 2013 holiday season, as more consumers are using these devices to compare prices, research products, locate stores, and make purchases to a larger degree than ever before.

Whether you'll be conducting transactions from your desktop, laptop or mobile device, keep these tips in mind to help protect yourself from identity theft and other malicious activity on Cyber Monday, and throughout the year:

1. **Secure your computer and mobile devices.** Be sure your computer and mobile devices are current with all operating system and application software updates. Anti-virus and anti-spyware software should be installed, running, and receiving automatic updates. Ensure you use a strong password and unique password, which is not used for any other accounts. Set a timeout that requires authentication after a period of inactivity.
2. **Use mobile applications with caution.** As devices such as smartphones and tablets, continue to gain popularity for online shopping, so too will the volume of attacks against them. Malware could be downloaded onto the device from seemingly legitimate shopping apps that can steal credit card and other sensitive information for transmission to cyber criminals. Update all apps when notified and disable Bluetooth and Near Field Communications when not in use to reduce the risk of your data—such as credit card number—being intercepted by a nearby device.
3. **Know your online merchants.** Limit online shopping to merchants you know and trust. Only go to sites by directly typing the URL in the address bar. If you are unsure about a merchant, check with the Better Business Bureau or the Federal Trade Commission. Confirm the online seller's contact information in case you have questions or problems.

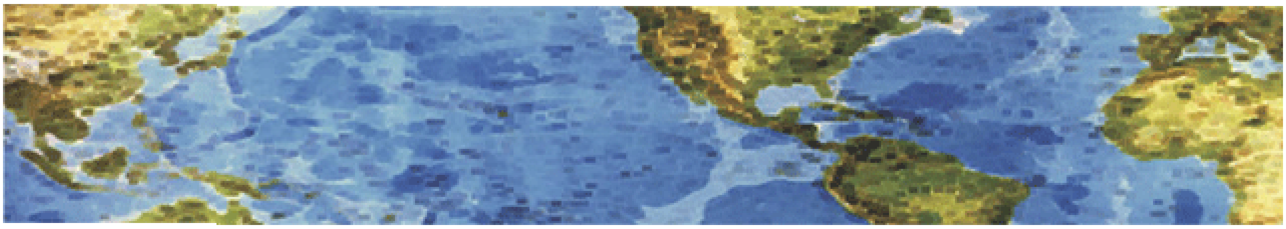
HALL ASSOCIATES

4. **Consider using an online payment system or credit card.** Where available, you may want to use online payment services, which keep your credit card information stored on a secure server, and then let you make purchases online without revealing your credit card details to retailers. If you do pay online directly to the retailer, use a credit, not debit card. Credit cards are protected by the Fair Credit Billing Act and may reduce your liability if your information is used improperly.
5. **Look for "https" before you click "Purchase."** Before you submit your online transaction, make sure that the webpage address begins with "https." The "s" stands for secure, and indicates that communication with the webpage is encrypted. A padlock or key icon in the browser's status bar is another indicator. Also, make sure your browser is current and up-to-date.
6. **Do not respond to pop-ups.** When a window pops up promising you cash, bargains, or gift cards in exchange for your response to a survey or other questions, close it by pressing Control + F4 on Windows devices, or Command + W for Macs.
7. Do not use public computers or public wireless access for your online shopping. Public computers and Wi-Fi hotspots are potentially insecure. Criminals may be intercepting traffic on public wireless networks to steal credit card numbers and other sensitive information. Care should be taken that the settings on your computer or device prevent it from automatically connecting to Wi-Fi hotspots.
8. **Secure your home and business Wi-Fi.** Make sure you control who has administrative access, and that any users on your network authenticate with a strong password. Encryption settings should be enabled and strong - using WPA2 is recommended.
9. **Be alert for potential charity donation scams.** Cyber criminals try to take advantage of people's generosity during the holiday season and can use fake charity/donation requests as a means to gain access to your information or computer/device. Think before clicking on emails requesting donations. Don't give your financial or personal information over email or text. Contribute by navigating to the trusted address of the charity, never through a link in an email. To check if an organization is eligible to receive tax-deductible charitable contributions, visit the IRS website. **Note that charity and donations for the Philippines typhoon and the mid-west tornados are already being used to scam people.**

For additional information about safe online shopping, you can check with the following sites:

- US-CERT www.us-cert.gov/cas/tips/ST07-001.html
- OnGuard Online www.onguardonline.gov/articles/0020-shopping-online
- Microsoft www.microsoft.com/security/online-privacy/online-shopping.aspx
- Privacy Rights Clearinghouse www.privacyrights.org/Privacy-When-You-Shop
- Internet Crime Complaint Center www.ic3.gov/media/2010/101118.aspx
- Internal Revenue Service www.irs.gov/Charities-&-Non-Profits/Exempt-Organizations-Select-Check

HALL ASSOCIATES



Risk-Based Decision Making Commentary
16 Oct 2013 Newsletter

Helping Companies Understand The Risks of Handling Credit Cards

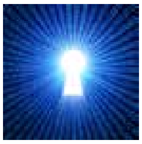
These days, the vast majority of businesses selling goods and services are dependent on being able to accept credit cards as the primary form of payment, whether on location, online, or even over the phone. Few, however, seem to realize that the processing of thousands, sometimes millions, of customer credit card records carries a range of different financial risks, one of which is compliance with the Merchant Services Agreement, a contract at the heart of being able to accept credit payments.

This certainly appears to have been the case with Cicero’s, a small restaurant located in Park City, Utah. Cicero’s has sued its bank and the affiliated payment processor alleging, amongst other things, that they failed to inform Cicero’s of its obligations under a merchant agreement to accept credit card payments. (Cicero’s Inc. vs. Elavon Inc., Third Judicial District Court, Summit County, Utah) According to the complaint, Cicero’s incurred claims against them exceeding $90,000 as well as other significant costs due to a potential breach of payment card information from its computer system. The good news is, by better understanding loss exposures associated with payment card information, a merchant’s general obligations under common Merchant Services Agreements, and insurance options available, insurance agents and brokers can assist their clients to fully understand and manage the risks associated with handling credit cards.

Determining Payment Card Exposures

To help a client determine the severity of a credit card exposure, the agent or broker needs to assess how the merchant processes credit card transactions and also review the exact terms of the Merchant Services Agreement. Many small merchants may simply swipe the credit card through a special electronic box. The “swipe box” will capture and transmit the card information to the payment processor, but will not retain the card information. The card information gets transmitted directly to the processor via a direct telecommunications line. Because the information is not retained to the merchant’s computer system, merchants using this type of system generally have a low exposure to the risks of losing payment card information.

Payment card exposures, however, are highest for merchants that process credit card transactions directly through a Point of Sale (POS) system. Typically, this is the case when the merchant swipes the payment card via a reader directly affixed to the POS system which stores the card information on the merchant’s computer systems. Many merchants mistakenly believe that because a POS system encrypts card information as the card is swiped, or because the POS system is certified as “PCI Compliant,” there is little to no exposure to loss.



Unfortunately, hackers have been able to circumvent these protections and Merchant Service Agreements do not protect the merchant in these cases. Payment card exposures are also significant for online merchants that process credit card payments directly on their websites, and possibly even retain the information in their computer systems to facilitate easy ordering for future orders.

The Merchant Services Agreement

Clearly, there is a range of ways a merchant can process credit card information, which will dictate the merchant's level of exposure to loss. Because there are so many different ways of handling credit card transactions, the best way to determine a client's exact exposure to loss is to examine their obligations under a Merchant Services Agreement. The Merchant Services Agreement is not based on obligations imposed by statutory or common law, but through obligations imposed under contract. Most notably, the Merchant Services Agreement requires the merchant to maintain compliance with the Payment Card Industry Data Security Standards (PCI DSS), as well as accept certain obligations in the event of payment card information breach. The PCI DSS is a set of standards promulgated by the Payment Card Industry Security Standards Council composed of all the major credit card brands. The extent of a merchant's responsibility to demonstrate compliance with the PCI DSS is based on the number of transactions that a merchant handles annually.

Specifically, merchants handling less than six million transactions a year are generally required to complete a Self-Assessment Questionnaire (SAQ). Merchants handling more than six million transactions a year are required to supply a Report on Compliance (ROC) from an approved IT-security expert. Most merchants are also required to obtain a quarterly network scan of their computers systems from an approved provider. In addition to demonstrating compliance with PCI DSS, the Merchant Services Agreement will place obligations on the merchant when a payment card company suspects that the merchant is a source of a breach. If suspected to be the source of a breach, the merchant is often required to obtain a computer forensic audit (at the merchant's expense) from a forensic auditor that has been approved by the PCI Security Standards Council. If the forensic auditor finds that the merchant is the source of a breach, the merchant may be held accountable for fines and penalties (if not in compliance with PCI DSS standards) as well as for the costs incurred to re-issue cards to consumers. As demonstrated in the Cicero's case, these costs and assessments may be substantial.

Risk Management

Once an assessment of a merchant's payment card exposures has been completed, good risk management requires implementation of appropriate risk controls as well as appropriate risk financing techniques. Note that no set of risk controls can guarantee that a loss will not occur. As such, the company should consider the use of insurance, or other risk financing techniques, to finance recovery from a loss that cannot be prevented. Careful adherence to the PCI DSS will provide a basic level of risk control, but insurance may be needed for higher exposures. Companies often fail to recognize the significant risks they carry when accepting credit card payments. This is especially true when they don't understand or properly comply with Merchant Service Agreements.

http://www.insurancejournal.com/magazines/features/2013/09/09/303861.htm?goback=.gde_4387290_member_5794770072438329348#!

http://www.zdnet.com/blog/security/targeted-spear-phishing-attacks/1032