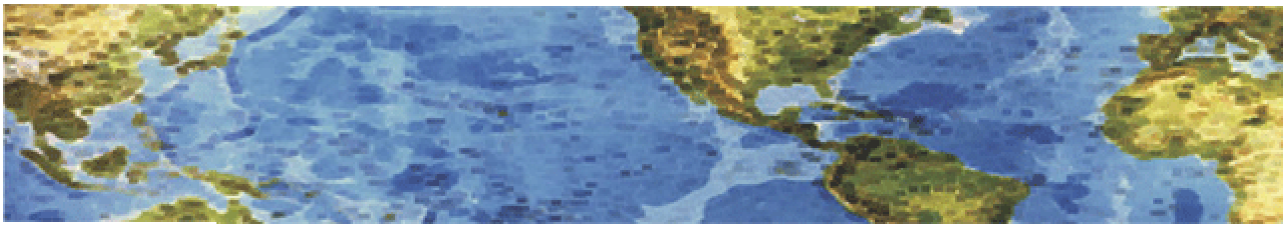
# HALL ASSOCIATES



# Risk-Based Decision Making Commentary
# 17 April 2013 Newsletter

## Scammers Target People With Fake E-Mails About the Boston Explosions

On April 17, 2013, the MS-ISAC became aware of a spam campaign using the Boston Marathon bombings that occurred on April 15, 2013. Users are sent an e-mail that contains a link to a URL hosting an exploit (CVE-2012-1723 – Vulnerability in Java Runtime Environment component) which, if successful, installs malware on the end users system.

**Subject lines used in the spam emails:**

*"2 Explosions at Boston Marathon" ; "Aftermath to explosion at Boston Marathon"; "Boston Explosion Caught on Video"; "BREAKING - Boston Marathon Explosion"; "Video of Explosion at the Boston Marathon 2013"; "Runner captures. Marathon Explosion"; 2 Explosions at Boston Marathon; "Aftermath to explosion at Boston Marathon"; "Arbitron. Dial Global. Boston Bombings"; "Boston Explosion Caught on Video"; "Explosion at Boston Marathon"; "Opinion: Boston Marathon Explosions made by radical Gays? Really? - CNN.com"; "Opinion: Boston Marathon Explosions - Romney Benefits? - CNN.com"; "Opinion: Boston Marathon Worse Sensation - Osama bin Laden still alive!? - CNN.com"; "Opinion: FBI knew about bombs 3 days before Boston Marathon - Why and Who Benefits? - CNN.com"; "Opinion: Osama Bin Laden video about Boston Marathon Explosions - bad news for all the world. - CNN.com".*

**Recommendations:**

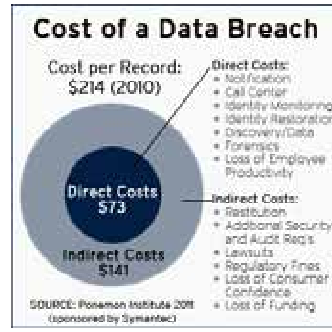
- ***Educate users on spam campaigns which uses recent events or celebrities' names as a lure.***
- ***Encourage users to not click on suspicious links or open suspicious attachments they may receive.***
- Ensure that your IT system has appropriate patches provided by Microsoft, Oracle, Adobe and other third party application providers to vulnerable systems immediately after appropriate testing.

**Reference:** https://isc.sans.edu/diary/Boston-Related+Malware+Campaigns+Have+Begun/

This is the latest in a long, ever-evolving strategy to infect your computer via drive-by malware downloads, which attack computers as soon as your web browser lands on a corrupted site. Previous email scams have used events or celebrities' names to lure users. If you receive an email message from someone you don't know, don't open the link inside without checking to see where they lead. By paying attention to details and treating ALL links with skepticism, you can avoid many of the pitfalls that lead to malware infections.

# HALL ASSOCIATES






**Schnuck's Data Breach Exposes 2.4 Million Credit Cards**

The St. Louis-based supermarket chain was alerted to the breach on March 15 by the company's payment processor, which said there had been fraudulent activity on several cards recently used at Schnucks stores. It wasn't until March 28 that Schnucks, which operates 100 stores in four states, was finally able to locate the security hole. It took another day and a half for the company to contain the breach, which was made public March 30. In a statement yesterday (April 15) updating customers, Schnucks warned that customers who used their cards at 79 different Schnucks stores between December 2012 and March 29 may have been affected. The statement noted that only card numbers and expiration dates had been compromised, and that no names or addresses were attached.

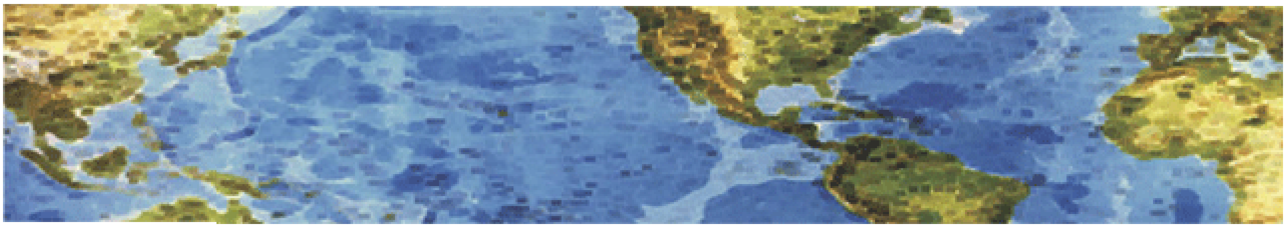
Schnucks hired a breach-mitigation firm on March 19, five days after the supermarket chain had learned of the leak and ruled out an insider or point-of-sale malware as the source. Even then, it took nine days to fix the flaw. While the firm worked to plug the hole, Schnucks' customers' credit-card details continued to be exposed.

Schnucks' statement tried to explain why Schnucks had waited two weeks to notify customers of the data breach. "A cyber-attack is not like a bank robbery where you know immediately when it occurred and who was affected," the statement said. "The investigation of a cyber-attack requires painstaking analysis of digital evidence that takes time in order to determine what happened," it continued. "The forensic investigation firm found the first indication of an issue on March 28, we contained the issue by March 30, and we have been working to identify affected stores and card numbers since then."

**Schnucks' inability to quickly locate and mitigate the leak may be due to increasingly sophisticated methods on the part of cybercriminals, who pose a growing threat to businesses and consumers alike.**

http://www.technewsdaily.com/17765-schnucks-data-breach.html?cmpid=520746

# HALL ASSOCIATES



## Risk-Based Decision Making Commentary
## 17 July 2013 Newsletter



### 11 Really Dumb Things Not To Do With Your E-mail

**http://www.foxbusiness.com/personal-finance/2013/07/03/11-really-dumb-things-do-with-your-email/?intcmp=obinsite**

Our simplest and most common vulnerability to criminals, hackers, spammers and spying eyes is e-mail. Just in the past few months, databases at LivingSocial and Evernote were hacked, exposing roughly 100 million e-mail addresses to identity thieves. Facebook allegedly exposed 6 million users' e-mails to unauthorized users, a "glitch" the company admitted was not detected for a year. All this comes on the heels of mega-breaches like the one at Epsilon, which provides marketing services for more than 2,500 financial and lifestyle companies. Epsilon admitted hackers stole "only" 2% of its customer data. But since its databases may contain upwards of 250 million email addresses, that means "only" 5 million people were placed at risk.

So what's the big deal? E-mail is no longer a convenient secondary conduit for saying hello to friends. It's plugged directly into our lives. Messages sitting in our e-mail accounts can expose not just our address and contact numbers, but also our bank and brokerage account numbers, credit card information, online financial transaction receipts and confirmation of forgotten or changed passwords in all of our other accounts. ***That's why e-mail is now the single most common vector of attack for fraud***, according to the Federal Trade Commission. It's laden with valuable data. And everyone knows their chances of getting caught are slim to none.

***Bottom line: The best way to stay safe is to aggressively protect yourself. No one else can guard your e-mail better than you.*** Here are the top 11 things you can do right now to reduce your risk of getting your e-mail either hacked or scammed.

**1. Never check your e-mail on an unsafe network.** - A computer in an Internet café, library or any other business may be loaded with malware to steal your passwords. Public WiFi systems are vulnerable too, even at places like coffee shops, airports, hotels and conference centers that require passwords, since any ID thief can afford a $3 cup of coffee and get the same password.
**What to do:** Unless the computer and network you're using belongs to you or your employer, don't sign into e-mail.

# HALL ASSOCIATES



**2. Don’t stay signed in.** - Signing into e-mail every time you pick up your phone can be a real pain. Deal with it. By staying constantly signed in, a hacker can gain immediate access to the most important information of your life.
**What to do:** Signing out is inconvenient. Do it anyway.

**3. Don’t repeat use your e-mail login name and password** - Just this year, hackers cracked databases containing the passwords of up to 50 million LivingSocial users, and another 50 million users of Evernote. If the password to your checking, credit card, social media or any other account ends in @gmail.com, @yahoo.com or any other e-mail address, those thieves possess an important piece of your identity puzzle. Since many people mistakenly use the same password or User ID for multiple accounts, identity thieves know the skeleton key that may fit many doors.
**What to do:** Never use your e-mail address and corresponding password for any other accounts. Beyond that, don’t use passwords based on things like your birthday, your kid’s name or your street. The more random, the better.

**4. Not deleting old e-mails properly** - Many people never delete old messages in their inbox, or delete their caches of trashed and sent e-mails (though most e-mail systems purge deleted email after 30 days). Those messages may contain addresses, account usernames and passwords, contact information for all your friends, financial data and a host of other sensitive information.
**What to do:** Delete sent, trashed and old messages. Delete e-mail with any sensitive information (like your tax paperwork, health insurance applications, etc.) immediately after sending it. Better yet, don’t send sensitive information over e-mail. For security, the old-fashioned Postal Service letter is still the best.

**5. Don't fall for a “guaranteed” loan or credit card offer -** If an e-mail promises a loan or credit card worth a guaranteed amount of money at a low interest rate, it’s a scam. Nobody will give you credit without first checking your credit report.
**What to do:** Don’t click on links in these messages, and delete them.

**6. Don’t click on ambiguous e-mails from “friends**. - Since hackers have raided our e-mail contact lists, even messages from our best friends could be vectors of attack. Hackers often pose as friends stuck penniless in Europe or Asia and in need of an immediate wire transfer, or friends imploring us to “Check out this funny video!” with links stuffed with spam or laden with malware. Sometimes the tipoff is an e-mail from a “long-lost friend,” or a close buddy using a very old account. Some of these e-mails come with no text at all… just a link.
**What to do:** Read e-mails from enemies closely, and e-mails from friends even more closely. If you receive a suspicious e-mail from a friend, don’t click on any links or download any files. Delete the e-mail, and call your friend. If it turns out the e-mail was legit, he or she can resend it.

**7. "Verifying" personal information via email** - It looks like your bank or credit card company asking to verify your account information. Or it could be from UPS or FedEx trying to "confirm" your address for a missed delivery. It could even be from the IRS claiming you owe them, or they owe you, money. ***None of these institutions send personalized e-mails, and none ask you to "verify" personal information by email.***
**What to do:** If an institution handles important things like money or packages, it doesn't use e-mail to communicate, and certainly not to confirm personal information. Delete the suspicious e-mail, and call the business or institution in question to inquire about the matter at hand.

8. **Don't e-mail strangers about money** - Many scams involve sending money to people we've never met. There's the "Wall Street insider" with the hot investment tip, the foreign company that needs you to cash a check or process transactions, the marketing company asking you to be a secret shopper or offering an irresistible work-at-home or franchising opportunity, the e-mail chain letter inviting you to "get in early" on a pyramid scheme, the Irish Lottery, even the lawyer of a deposed politician trying to get his money out of the country (this age-old ruse is actually growing more sophisticated, with better-written e-mails and virulent malware). Every one of them is a scam.
**What to do**: If someone you've never met offers you money, delete immediately!

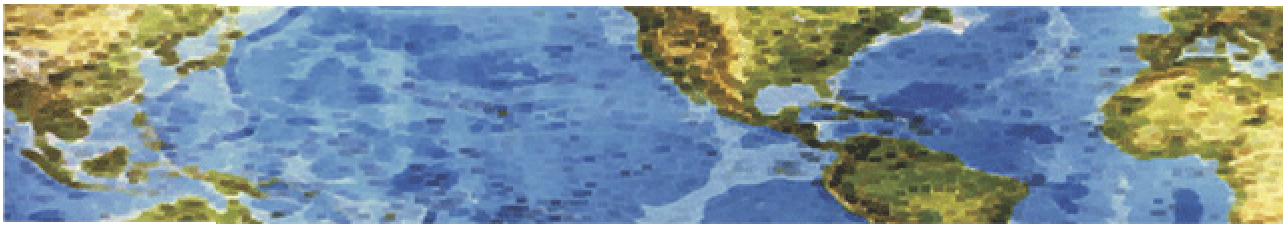
**9. Don't get tricked into thinking your credit card has been stolen** - You may receive an e-mail that says "Thank you for your recent order!" Except — you never ordered anything. You assume your credit card has been stolen and you open the e-mail and click the button that says "Cancel Order." You just became an ID theft target.
**What to do:** Think twice before clicking any button, link or attachment in an e-mail. Even if it's from a business you know, or one from which you have ordered something. If you need to cancel, call the company and cancel, or do so on their website. If you're really worried that you've been victimized, you can check each of your credit reports for free once a year.

1**0. Don't donate to fake charities** - After Hurricane Sandy and the giant tornado in Oklahoma, fraudsters sent e-mails requesting donations for relief efforts. The money went instead to scammers all over the world.
**What to do:** Only donate to established, well-known aid groups, and do so on their website or over the phone. Don't navigate to these sites from e-mails, and don't call the phone number in the e-mail. Look those up.

**11. Don't click on too-good-to-be-true deals** - Many of us receive legitimate e-mails alerting us to cheap flights, hotels and cruises. But when the offers seem just unbelievably low, and they come from companies and e-mail addresses you don't know, don't get sucked into clicking.
**What to do:** What's that old line about something seeming too good to be true? If some new travel site is running a special deal, rather than click a link in an e-mail, search for the deal on the Web. Find out if anyone has reported it as a scam. Make sure it checks out before you click.

There's no silver bullet here even if you do all of these things. It is impossible to completely protect yourself on the Internet. Remember, you are connected to the World, not just your friends. That said, the better you can minimize your exposure and operate cautiously, the longer you can stay safer.

# HALL ASSOCIATES



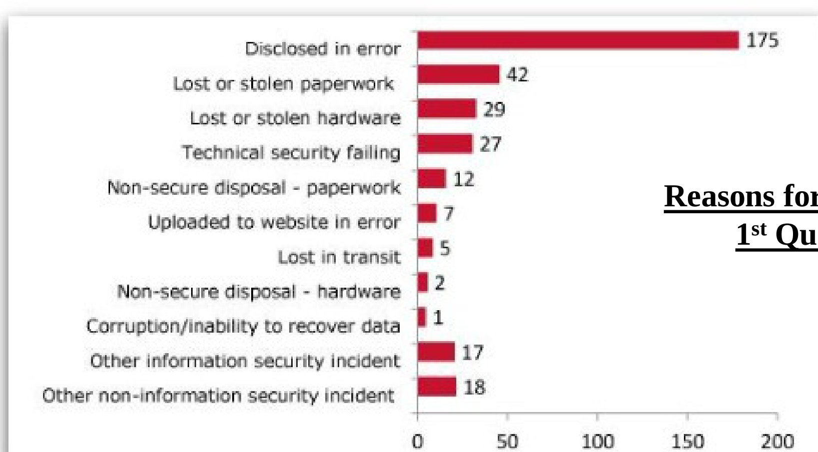
# Risk-Based Decision Making Commentary
# 17 September 2013 Newsletter

## When is Enforcement of Security Policies Effective?

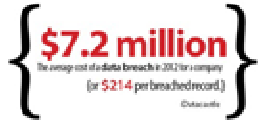
When is enforcement of security policies effective? **When it serves as an enabler of the right behavior.** For that to happen, usually three conditions need to be met. First, enforcement has to be visible, meaning the entire workforce has to be aware of it. Second, it needs to be meaningful, meaning there has to be a real consequence. Third, it needs to be persistent, meaning it has to be visible long enough to shape new behavior.

In recent months, when reading about and talking with folks about security incidents and breaches, a common theme that has repeated itself over and over again is that termination of personnel was often the action taken in response to a data breach. But that action normally only temporarily stemmed the number of incidents. **Terminations have not been as effective as one might expect to effect long-term behavior modification**.

**Is Termination Visible?** For an action to change behavior it must be visible, meaning others must be aware of it - not only that it happened, but the circumstances that led to it. This is problematic because many companies/organizations are hesitant to discuss punitive actions. They are also hesitant to acknowledge that a data breach occurred. As a result, only a few employees may be aware, and depending on their perception, the story told to others may be skewed. Behavioral change is helped by learned retention, and termination has a short shelf-life when it comes to retention.




**Reasons for Data Breaches**
**1st Quarter 2013**


**Is there Meaningful Consequence?** Termination has personal, professional and financial consequences. It alone may actually modify behavior for those aware of what happened. If the goal is long-term change, then termination alone is not likely to achieve that result and might actually be counterproductive.

**Is It Persistent?** Termination eliminates certain awareness opportunities for long-term learning because the person terminated is gone and the people involved don't discuss it. Individuals who have been punished, but remain in the workforce, can testify to others firsthand that certain behaviors are destructive. In fact, individuals that are given a second chance can become positive influences with other personnel - particularly if they perceive the consequences they're handed were fair. Termination is still an appropriate consequence depending upon the circumstances. It should be reserved, though, for the repeat offender, the individual who shows a total disregard for the rules, the person who seeks to harm another, or the most egregious incidents. But it should not be a standard response for every data breach in which an employee had some responsibility. It is also necessary for you to have specific policies stating what an employee can be terminated for.

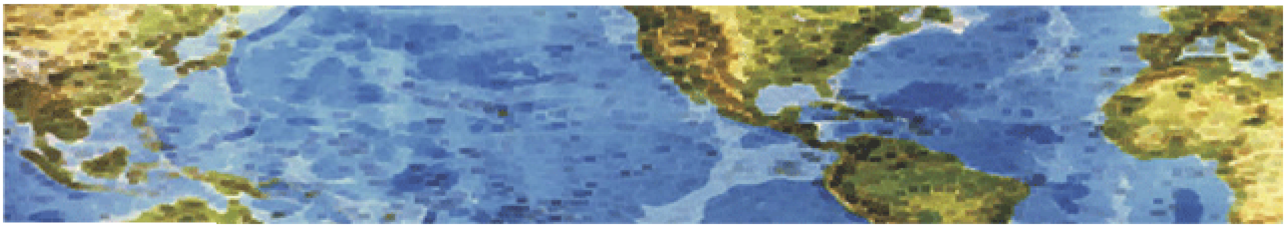
**Privacy and security, both individually and for the company,** are every person's responsibility. You hear this over and over again, yet many companies and organizations seem to be very reluctant to set privacy and security performance criteria for their workforce. **Have you set privacy and security performance criteria for your workforce?** Is data security identified in job descriptions and included as part of performance evaluations? Establishing privacy and security performance criteria for all employees should make everyone in the organization personally aware of their individual and collective responsibility to protect your (and their) sensitive information.

Also note that often companies are held responsible for the actions of their employees in various ways - legal, regulatory, reputational and business. **Everyone needs to provide workforce training and make sure that they emphasize that their personnel's actions have consequences.** The point is that even good workers sometimes make mistakes or have lapses of judgment. That does not necessarily mean they are not good employees or are not capable of doing better. An incident or even a lapse of judgment, depending on circumstance, should not be grounds for automatic dismissal. Sometimes the person who makes the mistake and suffers the consequences, but is not terminated, is far more effective at shaping others' behavior than the one who disappears and is soon forgotten.

Tying privacy and security to individual performance plans and then enforcing it fairly can have a profound effect on behavior, and therefore, culture. It has consequences, it's visible and persistent, and if applied consistently, will be perceived as fair. More importantly, it will contribute to **awareness and learning** and should assist in reducing the number and effects of future incidents.

These links are some useful ideas about establishing and enforcing an effective security policy. There are many, many more available.
http://www.darkreading.com/management/writing-and-enforcing-an-effective-emplo/240142264
http://www.isaca.org/Journal/Past-Issues/2005/Volume-6/Documents/jopdf-0506-creating-enforcing.pdf
http://www.sans.org/reading-room/whitepapers/policyissues/developing-effective-information-systems-security-policies-491?show=developing-effective-information-systems-security-policies-491&cat=policyissues
http://www.cisco.com/en/US/solutions/collateral/ns170/ns896/ns895/white_paper_c11-503131.html

# HALL ASSOCIATES



## Risk-Based Decision Making Commentary
## 19 December 2013 Newsletter

### LOCKER Malware - Yet another new variant of CryptoLocker Ransomware

**Yet another new variant of CryptoLocker Ransomware, a current threat to internet users that continues to grow in popularity with cyber criminals due to its success and monetary potential, has been found in the wild.** This is nothing new and to be expected. There have been many discussions on underground hacking forums about "How to create Ransomware like CryptoLocker malware" or "Malware - hacking tool-kit with ransomware features". Security intelligence provider, IntelCrawler has discovered a new ransomware variant called Locker that demands $150 (£92) to restore files that it has encrypted. Like CryptoLocker, this new ransomware is also nasty because infected users are in danger of losing their personal files forever. **<u>Locker mainly spreads by drive-by downloads from compromised websites, disguised itself as MP3 files</u>** and uses system software vulnerabilities to infect the end user. Once it has infected a system, the malware first checks whether the infected machine has an internet connection or not. Then it deletes any original files from the victim's computer after using AES-CTR for encrypting the files on infected devices and add ". perfect" extension to them. Locker's encryption is based on an open source tool called 'TurboPower LockBox' library. After encrypting all files, the malware places a "CONTACT.TXT" file in each directory, which provides contact details of the author to buy the decryption key and once the ransom is paid, each victim gets a key to unscramble files. The good news is that the researchers are working on the universal decryption software in order to help the victims. It appears that the hackers are simply comparing the list of infected IP addresses of users, along with their host names. **IntelCrawler had discovered 50 different builds of the malware, which are being sold in underground markets for pay-per install programs.** One build had just under 6,000 infected machines. This malware, like CryptoLocker, will encrypt all drives visible on an infected system, **so you must be sure that your backups are stored remotely or in a location that is not simply another drive partition or mapping to another location.** The malware infects users from the United States, Turkey, Russia, Germany and the Netherlands. Users should remain vigilant about their security. D**ouble check the legitimacy of links received in emails and ensure you have your antivirus/antimalware up to date to help protect against such threats. <u>Backing up ALL data daily doesn't hurt, either. But remember, the backups should be separate from your computer or networks or they will be encrypted by the malware at the same time.</u>**

Mohit Kumar, The Hacker News - Friday, December 13, 2013

# HALL ASSOCIATES



## Cyber Hygiene with Critical Security Controls

In this digital age, we rely on our computers and mobile devices for so many aspects of our lives that the **need to be proactive and vigilant to protect against cyber threats has never been greater**. However, in order to be as secure as possible, we need to use good cyber hygiene – that is, making sure we are protecting and maintaining systems and devices appropriately and using cyber security best practices. Many key best practices are outlined in the Top 20 Critical Security Controls, managed by the Council on CyberSecurity (see URL at the end of this article). These Controls assist in mitigating the most prevalent vulnerabilities that often result in many of today's cyber security intrusions and incidents. The Center for Internet Security (CIS) provides free, PDF-formatted configuration guides (Benchmarks) that can be used to implement the Controls and improve cyber security (URL also at the end of this article). **Below are several best practice strategies for strengthening defenses.**

**Update Your Applications, Software and Operating Systems**

Even though you may be diligent in keeping your software up-to-date, you are still at risk from malware infections. Malware can infect your computer from a variety of different vectors, including compromised websites, malicious attachments in email, and infected thumb drives. This is why strong malware defenses are crucial. Anti-virus and anti-spyware will scan your files to see if there’s any malware in the files. It may even tell you if you’re about to download a potentially malicious file. Update your anti-virus software regularly. Keeping applications, software, and operating systems patched will help keep you more secure by providing you with the most recent and secure version. Just remember that as new malware comes out, it requires days to months for the antivirus/antimalware companies to respond with changes.

**Securely Configure Your Systems and Devices**

The “out-of-the-box” configurations of many devices and system components are default settings that are often set for ease-of-use rather than security. This often results in vulnerabilities that offer easy targets for hackers to exploit, often using automated programs that scan for holes. To mitigate risk, systems and devices (especially individual computers and mobile devices) should be configured according to industry-accepted system hardening standards. Remember to encrypt your data – all your data.

**Secure Your Browser and Browser Add-ons**

Cyber attackers search for programming errors and other flaws in web browsers and associated plug-ins in order to exploit them. These vulnerabilities, if successfully exploited, can give cyber criminals access -- and sometimes control over -- your computer system. To minimize these risks, keep your browser(s) updated and patched, and set to auto update. In addition, keep any programs (known as plug-ins) updated and patched as well, particularly if they work with your browser (such as multi-media programs and plug-ins used to run videos, for example), block pop-up windows, as this may help prevent malicious software from being downloaded to your computer and consider disabling JavaScript, Java, and ActiveX controls when not being used. Activate these features only when necessary.

**Back Up Your Data**
Be sure to back up your important data so you can retrieve it if your computer fails or you get caught by malware like CryptoLocker. External hard drives and online backup services are two popular vehicles for backing up files. Remember to back up data (from your computer system and ALL mobile devices) at regular intervals (daily is recommended) and periodically review your backups to determine if all your data has been backed up accurately.

**Secure Your Wireless Network**
Before the days of wireless (Wi-Fi) home networks, it was rather easy to see who was linked into your home network; you could simply follow the wires. You wouldn't allow a stranger to connect to your network, so check to see who is connected to your wireless network. The first step is to lock down your wireless network with a strong password and encryption. This will prevent people who don't have the password from connecting to your network. While there are fewer wires to follow, you can still follow some digital breadcrumbs to see who is connected to your network. Connect to your router (for more information refer to the manufacturer's user guide) to see who the clients (the connected devices) are. Are there more devices connected to your network than you expect? If there are some devices you don't recognize, change your security settings and passwords. Don't forget about your printers, many of which can connect to your network and are Wi-Fi enabled.

**Protect Your Administrative Accounts**
Administrator or "admin" accounts give a user more control over programs and settings for a computer than a typical user account. If an intruder accesses an admin account, he could potentially take over your computer. Non-administrator accounts, or guest accounts, can limit the ability of someone gaining unauthorized access. It is important to change the default password on your admin accounts and to always log on to your computer as a non-administrator or non-admin account. Another aspect to protecting admin accounts is to **change default passwords on your devices**. Many of them are published on the Internet, so be sure to change them to something unique and strong. Default passwords are especially prevalent in routers, wireless access points and other networked devices.

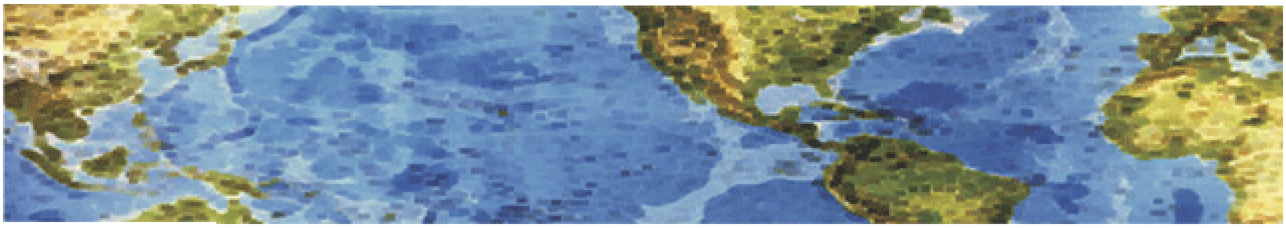
Many computer defaults are set for ease of use, which is convenient not only for us, but also for cyber criminals. Cyber criminals can use weak or unnecessary services as a first step to compromising your computer. Many computers and routers already come with a firewall built in to prevent malicious access to these services. It is recommended that you set the firewall to the securest level you think is appropriate: if this is a laptop you'll use for traveling and connecting to public networks, it is recommended that you choose the strictest level of security and only allow exceptions for services you need. You can always relax the controls if necessary.

**Create, Use and Regularly Change Strong Passwords And <u>Use Different Ones for Different Accounts!!!!</u>**
A strong password is at least eight characters long, does not contain your user name, real name, or company name, does not contain a complete word, is significantly different from previous passwords and contains characters from each of the following four categories: Uppercase letters, Lowercase letters, Numbers and Symbols found on the keyboard (all keyboard characters not defined as letters or numerals) and spaces.

http://www.counciloncybersecurity.org/
http://benchmarks.cisecurity.org/downloads/benchmarks/
http://benchmarks.cisecurity.org/downloads/crosswalk/

Original Article from MS-ISAC , December 2013 Volume 8, Issue 12

# HALL ASSOCIATES



## Risk-Based Decision Making Commentary
## 21 August 2013 Newsletter

### Baby-monitor hacker spies on and swears at sleeping 2-year-old

A hacker took over a baby monitor in a home in Houston, Texas, to spy on a 2-year-old girl, to broadcast obscenities at the child, to swivel the camera so as to watch her shocked parents as they came in, and to then call the parents insulting names. According to ABC News, Marc Gilbert and his wife, Lauren, heard the voice of a strange man with a British or European accent coming from the bedroom of their daughter, Allyson, on 10 August. As the parents approached the room, they heard the hacker call their daughter an "effing moron." The voice also told her to "'wake up, you little sl*t."

When the Gilberts entered the room, the monitor's camera swiveled toward them. The hacker then called Marc Gilbert a "stupid moron" and Lauren Gilbert a "b*tch". Marc Gilbert disconnected the monitor and tried to figure out what had happened, but he couldn't, of course, see the hacker - he could only hear the voice and see that the intruder was controlling the camera. Gilbert told reporters that he believes the hacker hacked his router. The hacker also, apparently, hacked the camera, through which he could see Allyson's name on the bedroom wall above her bed. His router was password-protected, and the firewall was enabled. The IP camera was also password-protected.

ABC News subsequently drove through a neighborhood with a baby monitor video receiver on the dashboard, picking up crystal-clear video feeds left and right. First they found Dominic, playing with his toes in his crib. Next they viewed 14-month old Tally, sleeping in her crib. They found a camera pointed at a bed in one neighborhood, and they viewed a woman making a bed in another.

Baby monitors open the home to invasions by creeps and, potentially, burglars in this manner because they're on fixed frequencies, putting out a signal as long as the device is on. The wireless channels used by the devices can often be picked up outside the home, as demonstrated by ABC News when it scanned neighborhoods to see what it could pick up. The vulnerability of these leaky systems was highlighted in 2009 when a US family in the state of Illinois sued the manufacturer of a baby monitor they purchased at toy retailer Toys R Us. After a month of using the monitor, a neighbor warned the family that its camera was broadcasting its signal into their home, enabling the neighbors to hear entire conversations within the nursery. Of course, devices may well be protected by passwords, but default passwords that haven't been changed are like having no password at all. Video baby monitors can broadcast to TVs, hand-held receivers, or even over WiFi to PCs or smartphones. That means you and sometimes others, can keep an eye on your children from almost anywhere. Be careful with these devices' security. That starts with changing default passwords.

http://nakedsecurity.sophos.com/2013/08/14/baby-monitor-hacker-spies-on-and-swears-at-sleeping-2-year-old/

# HALL ASSOCIATES




## New Android Malware Found

Perkele is a cyber crimeware kit designed to create malware for Android phones that can help defeat multi-factor authentication used by many banks. In this post, we'll take a closer look at this threat, examining the malware as it is presented to the would-be victim as well as several back-end networks set up by cybercrooks who have been  using mobile bots to fleece banks and their customers.  Perkele is sold for $1,000 (remember my newsletter note on the ongoing malware marketplace), and it's made to interact with a wide variety of malware already resident on a victim's PC. When a victim visits his bank's Web site, the Trojan (be it Zeus or Citadel or whatever) injects malicious code into the victim's browser, prompting the user to enter his mobile information, including phone number and OS type.

That information is relayed back to the attacker's control server, which injects more code into the victim's browser prompting him to scan a QR code with his mobile device to install an additional security mechanism.  Once the victim scans the QR code, the Perkele malware is downloaded and installed, allowing the attackers to intercept incoming SMS messages sent to that phone. At that point, the malware on the victim's PC automatically initiates a financial transaction from the victim's account.

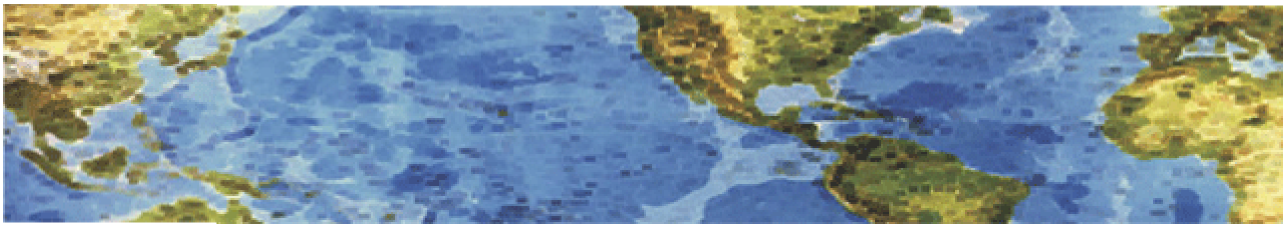
Web site security firm Versafe located a server that was being used to host malicious scripts tied to at least one Perkele operation. The company produced a report (PDF), which delves a bit deeper into the behavior and network activity generated by the crimeware kit.  If you are interested in the technical details, check out  http://krebsonsecurity.com/wp-content/uploads/2013/08/Versafe-SOC-Mobile-attacks-summary-1.pdf

There seems to be a great deal of interest in the cybercrime underground  market for developing or procuring tools to trojanize Android devices. According to a recent report from security firm Trend Micro, the number of malicious and high-risk Android apps steadily increased in the first six months of 2013. According to Trend, the number of malicious and high-risk apps took three years to reach 350,000, a number that has already doubled in just the first half of 2013.

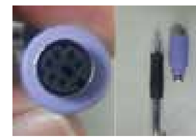
Fortunately, a modicum of common sense and impulse control can keep most Android users out of trouble. Take a moment to read and comprehend an app's permissions before you install it. Also, consider downloading and installing apps only from Google's Play store, which scans all apps for malware. This isn't perfect, but they do scan all apps posted.  Also there are numerous free and paid anti-malware applications available for Android.  All Android devices should be protected.

http://krebsonsecurity.com/2013/08/a-closer-look-perkele-android-malware-kit/

# HALL ASSOCIATES



## Risk-Based Decision Making Commentary
## 20 Oct 2013 Newsletter



### New Security Threat: Cash Register Skimmers

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

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

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

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

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

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

http://www.cnbc.com/id/101115205?goback=.gde_4387290_member_5796781791742287875#!





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

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

**1. Stay away from English-language passwords**

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

**2. Create fake security answers**

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

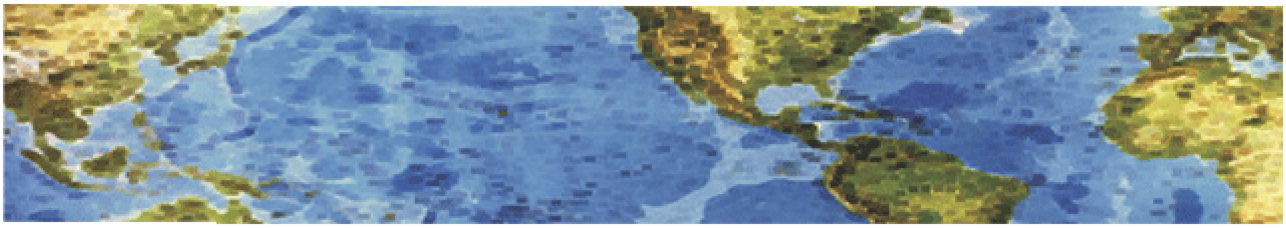
**3. Have a favorite poem or song?**

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

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

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

# HALL ASSOCIATES



# Risk-Based Decision Making Commentary
# 22 April 2013 Newsletter

## HIPPA Requirements for Business Associates

If your company handles one or more "personal health records" it would be **VERY** prudent for you to fully comprehend the severity of the legal impact. The following is a very brief example of some of the concerns.  The penalties for mishandling even one record can be very costly.

The new HIPAA  expanded "business associate" definition to include health information organizations, e-prescribing gateways **or others** that provide data transmission services for protected health information (PHI) to a covered entity and that require routine access to the health information. Companies that offer a personal health record to one or more individuals on behalf of a covered entity **are also now** considered business associates.

In the past month, eight out of 15 breaches added to the Department of Health and Human Services' "wall of shame" tally have involved business associates. And business associates have been implicated in about 21 percent of the 571 breaches affecting 500 or more individuals that HHS has tracked since September 2009.  Business associates have been involved in many of the largest incidents, including, for example:

- A September 2011 breach affecting 4.9 million individuals involving SAIC, a business associate of TRICARE, the military health program;
- A December 2010 incident affecting 1.7 million patients involving New York City Health and Hospitals Corp. and it's business associate, GRM Information Management;
- A March 2012 breach that compromised data of 780,000 individuals and involved the Utah Department of Health and its business associate, the Utah Department of Technology.

With the enforcement date of Sept. 23 for HIPAA Omnibus less than five months away, it's possible that even more business associate-related breaches will appear on the tally. That's because under HIPAA Omnibus, not only are business associates and **their subcontractors** for the first time **directly liable** for HIPAA compliance, but also the definition of business associates has been expanded to include more kinds of vendors, including many cloud service providers.
http://www.healthcareinfosecurity.com/breaches-business-associates-role-a-5709

**Have you evaluated what data you have and whether or not it is "protected"?  There are now numerous types of "protected" data with onerous legal liabilities if compromised.**


To subscribe or unsubscribe from this newsletter,  send an e-mail to halld105048@yahoo.com.

# HALL ASSOCIATES


## <u>**Android Malware**</u>

The amount of malware (malicious software) aimed at infecting Android devices (mostly mobile phones and tablets) more than doubled in 2012. The number of pieces of malware targeted against an Android platform rose from less than 25,000 in 2011 to <u>**over 65,000 in 2012**</u>. A report published by a mobile security company, estimates that nearly **33 million** devices were infected in 2012 – an increase of over 200% from 2011.

The most popular way of infecting Android devices is through application repackaging – taking popular applications from the Google Play Store, adding malicious code and than uploading the corrupted application to an “unofficial” application market site. Such infections occur when Android users download cut-rate applications from “unofficial” sites to avoid paying the full price at the Google Store. Such malware can provide cybercriminals access to any data stored on your mobile device, including account information and passwords. (***You do encrypt your data on all your mobile devices, don’t you?***).

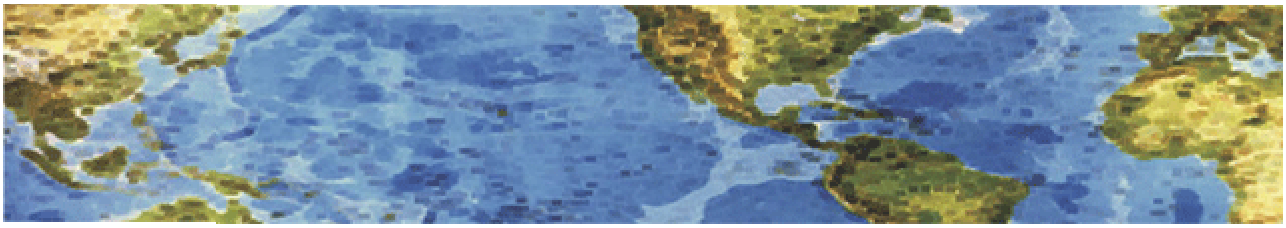
Cybercriminals can also steal Android user’s personal (and business) data through malicious websites. Subtle changes in URLs redirect users to criminal clones of the sites you think you are accessing. Once there, you are prompted to provide personal or account information. Based on some research, people are less likely to be suspicious or security-minded on mobile devices than they are on their PCs.

Smishing (a combination of SMS and phishing) involves sending an unsolicited text message (SMS) to a target and getting them to click on a link in the message. This in turn downloads and installs the malware application. Some of this malware accesses premium text message services in the background, sends messages and causes your phone bill to skyrocket.

You can avoid becoming malware victims by being <u>**very careful**</u> about clicking on links and installing applications. Access the internet on your Android device with the same level of concern for security that you do on your Windows PC. Don’t click on any links or open attachments in e-mail messages without scanning for viruses and malware and if you do not recognize who sent them. Make sure you are really on the web page you seek before filling out any personal information or passwords. Small screens make it harder to see the full URL, but taking a moment to check could be <u>**extremely**</u> useful. Download applications only from Google Play store. Google does try to keep malicious code from apps there. Finally, install one of the available Android anti-virus applications, keep it updated and use it.

http://www.technewsdaily.com/17817-android-malware-doubles.html

Hall Associates



# Risk-Based Decision Making Commentary
# 23 April 2014 Newsletter

## Why Do Data Breaches Happen?

Wham—news of a data breach breaks. Updates flood the internet, accusations fly between parties, and everyone speculates. Why? How? What happens now? Amid the chaos and the hype, it can be difficult to get clear, accurate information about what's really going on when a data breach occurs. While data breaches are certainly a complex issue, equipping yourself with basic knowledge of them can help you to navigate the news, to handle the aftermath, and to secure your data as best as you can.

Let's get the story straight on why data breaches happen by looking at four common myths.

**Data Breach Myth 1: Data breaches happen when someone at a company or organization steals data.**

While the scandal of an insider hack seems oh-so-Hollywood, this is rarely the case. In 2012, according to an annual study by Verizon, 94% of data breaches were perpetrated by outsiders. These outside hackers may not even be in the same country as the organization they hack. Because most data breaches are not insider jobs, even organizations that you trust are at risk of having a breach. It's not as simple as picking out bad apple employees or avoiding sketchy companies. In fact, it's not only companies that need to worry about their data security.

**Data Breach Myth 2: Data breaches only happen at stores where you make purchases.**

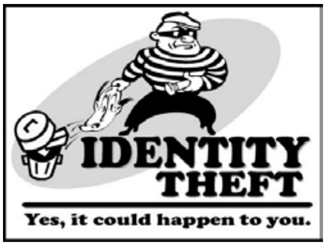
When you hear the phrase "data breach," what comes to mind? If it's Target, you're not alone. The magnitude of the Target Data Breach during the 2013 holiday season was unprecedented, with up to 70 million cards affected. The aftermath and press coverage continues even months after the incident. It's easy to see why large retail stores seem like the new face of data breaches. Yet, it's important to remember that all sectors are at risk of experiencing a data breach because of the value of data. Just look at Indiana University, University of Maryland, Yahoo, the state of South Carolina, and the California DMV, who all recently experienced data breaches. In fact, retail accounts for only 15% of all data records lost or stolen, according to SafeNet.

Hackers are not just after credit card numbers that they can fraudulently charge. Other sensitive information—name, email, address, or social security number, for example—can be sold or abused for a profit. It's important to use caution when you give out any of your data online or in person, and not only when you swipe your card.

**Data Breach Myth 3: Data breaches happen every once in a while when there is a hole in security.**

Data breaches happen all the time. A report by the Online Trust Association estimated that over 740 million personal records were exposed in 2013 alone, over the course of 614 breaches.

# Hall Associates






We don't always hear about data breaches because companies in some states are currently not required to disclose this information. In the aftermath of the Target data breach, Congress is attempting to pass legislation requiring timely data breach notification.  Though data breaches hinge on exploiting a "hole" in security, this oversimplifies the problem. It's impossible for the average consumer to know the ins and outs of a company's security practices, and even if this information was made available, we could not predict what barriers hackers could break down to access valuable data. The real security hole is the poor standard of data security across the board.

**Data Breach Myth 4: Data breaches happen because companies are careless**.
The increasing frequency and magnitude of data breaches is a clear sign that organizations need to prioritize the security of personal data. Breached companies may be guilty of carelessness with private information, but we have to remember that the data breach game has an element of chance: many organizations that have not been breached are still gambling with user data by not ramping up their security standards.  So while it's easy - and mostly justified - to point fingers at companies that experience breaches, it's important to remember these occurrences are  symptoms of a larger problem. Collaboration between all sectors, including governments, banks, credit cards companies, retailers, and consumers, will be needed in order to raise the security bar.
http://www.abine.com/blog/2014/data-breach-myths-debunked/

**An Oldie But A Goodie**
I got an e-mail from a correspondent that just received a phone call from someone claiming to be a "Windows representative".  She (the accent was possibly from India) tried to tell my correspondent that her computer was sending out a virus infecting other computers – and she needed to get signed on remotely to her computer to fix the problem.  The correspondent would not allow that.  She said she would call her local computer person but that made the caller mad.  She then asked for the caller's phone number so the caller hung up.  Interestingly enough there was a phone number on her caller ID – 215 area code.  Assumption is that the phone number was spoofed.

No scam is too old/outdated enough for people world-wide to not continue to try it.  The new scams simply build on older ones – these things never go away.  So we need to be aware of all possible scams, or at least be aware of proper responses to any request for access or personal information.


# Hall Associates

## Phishers Divert Home Loan Earnest Money

Real estate and title agencies are being warned about a new fraud scheme in which email bandits target consumers who are in the process of purchasing a home. In this scheme, the attackers intercept emails from title agencies providing wire transfer information for borrowers to transmit earnest money for an upcoming transaction. The scammers then substitute the title company's bank account information with their own, and the unsuspecting would-be homeowner wires their down payment directly to the fraudsters.

This scam was laid out in an alert sent by First American Title to its title agents:

"First American has been notified of a scheme in which potential purchasers/borrowers have received emails allegedly from a title agency providing wire information for use by the purchaser/borrower to transmit earnest money for an upcoming transaction."

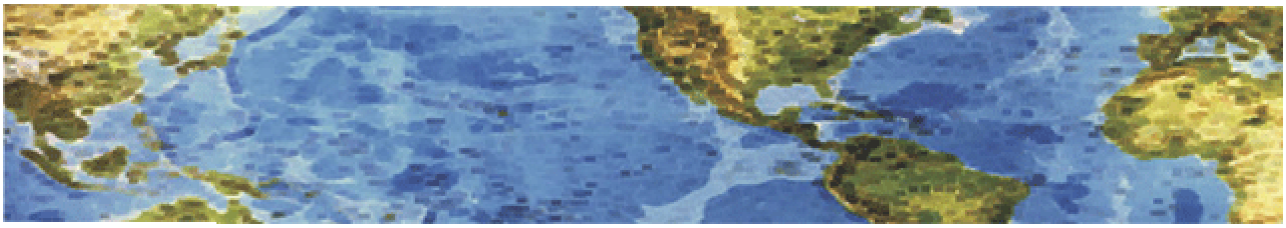
"The messages were actually emails that were intercepted by hackers who then altered the account information in the emails to cause the purchasers'/borrowers' funds to be sent to the hacker's own account. The emails appear to be genuine and contain the title agency's email information and/or logos, etc. When the purchasers /borrowers transferred their funds pursuant to the altered instructions, their money was stolen with little chance of return. This scam appears to be somewhat similar to the email hacking scheme that came to light earlier this year that targeted real estate agents."

"It is apparent in both scams that the hackers monitor the email traffic of the agency or the customer and are aware of the timing of upcoming transactions. While in the reported instances, a customer was induced to misdirect their own funds, an altered email could conceivably be used to cause misdirection of funds by any party in the transaction, including the title agent themselves."

This scam is almost certainly not unique to First American Title; scams that work against one corner of an industry generally work against the industry as a whole. Attacks like this one illustrate the value of two-factor authentication for email. The larger providers have moved to enabling multi-factor authentication to help users avoid account compromises. Gmail.com, Hotmail/ Live.com, and Yahoo.com all now offer multi-step authentication that people can and should use to further secure their accounts. Dropbox, Facebook and Twitter also offer additional account security options beyond merely encouraging users to pick strong passwords.

http://krebsonsecurity.com/2014/04/phishers-divert-home-loan-earnest-money/

# HALL ASSOCIATES



## Risk-Based Decision Making Commentary
## 24 July 2013 Newsletter


### Scams about the Royal Baby Lead to Identity Theft

The first celebrity scams about the royal-baby have begun to appear. The first real picture of the royal baby appeared on July 23, and so did the first royal-baby scam. Kaspersky Lab reported on its SecureList blog that an email spam campaign had begun, luring in victims with promises of a hospital webcam. But instead of showing you nurses and infants, the link takes you to a site loaded with the Blackhole browser exploit kit, a particular nasty drive-by download that tries one attack after another against your browser in the expectation that something will get through.

Whenever there's a big news story, scammers and cyberthieves are quick to take advantage of Internet users' curiosity in order to plant malware on their computers, mobile devices and phones and steal sensitive personal information. So be very careful if you're searching for news about the royals or for terms such as "royal baby photos" or "Princess Kate.“ Online criminals carry out search engine poisoning to turn news-seekers into victims, using marketing techniques to boost phony links to supposedly exclusive items up to the top of Web search results. **But instead of being taken to real news or photos, victims often end up on corrupted or deliberately phony sites that can infect their computers, devices and phones.**

Note that cybercriminals have been preying on celebrity news junkies in the form of phishing emails that promise "exclusive" information about a breaking story ever since the internet began. For example, the royal family has revealed the new prince's birth weight, but that's about all anybody knows so far. The public is clamoring to know the little guy's name, eye color and any other tiny detail. Scammers feed off this hunger and try to get the better of nosy news hounds by emailing to victims messages that claim to have links to secret details about the royal baby. But the recipient will first have to take a survey, log in to Facebook (beware of fake login pages) or provide his name, address and credit-card number.

To avoid falling for attacks such as these, use good anti-virus software and pay attention where online links actually lead. As I've noted before, don't click on any links in email messages you're not expecting and few you are expecting. Stick to major and trusted news sites. If anyone is going to have the latest scoop, it's probably not going to be confined to an obscure and fishy-looking website.

http://www.technewsdaily.com/18579-royal-baby-scams.html?cmpid=529630

# HALL ASSOCIATES



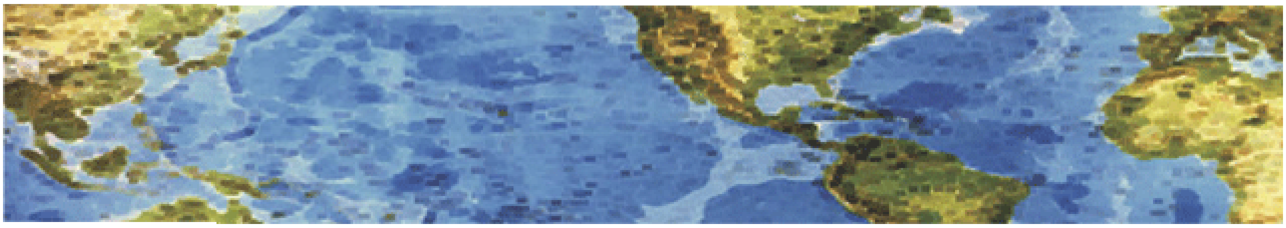
## Avoiding Online Scams

There are a number of recommendations on how to avoid becoming a victim of an on-line scam. But note that online scams keep changing and becoming more sophisticated. These recommendations are good but will be added to continually.

**1. Know who you are dealing with** regardless of the type of transaction – find a seller's physical address (not just a P.O. Box) and phone number. Do an internet search for the company name and website and look for negative reviews.
**2. Understand that wiring money is like sending cash**. It's nearly impossible to reverse such a transaction or trace the money, especially out of the country.
**3. Don't wire money to strangers, to sellers who insist on wire transfers for payment, or anyone who claims to be a relative or friend in an emergency** who wants to keep the request a secret or for you to respond immediately.
**4. Read your monthly statements or check online daily**. If you see charges you didn't authorize, contact your bank, card issuer or other creditor immediately.
**5. Give only to established charities after a disaster**. Don't give to those that have sprung up overnight. For donating tips, check out www.ftc.gov/charityfraud.
**6. Don't agree to deposit a check and wire money back.** Uncovering a fake check can take weeks and you are responsible for any check you deposit.
**7. Don't reply to messages asking for personal or financial information**. No government agency or legitimate business will ask for personal or financial information over e-mail, period.
**8. Don't play a foreign lottery.** Messages saying you have already won are scams. You will most likely be asked to pay "taxes", "fees" or "customs duties" to collect your prize.

Report any online scams – file a complaint with the Federal Trade Commission **(http://www.ftc.gog/complaint)** and your state Attorney General **(http://www.naag.org/current-attorneys-general.php).** For lottery material from a foreign country, give that to your local postmaster. You can also report cyber incidents to the Departtment of Homeland Security:
**http://www.dhs.gov/how-do-i/report-cyber-incidents**

# HALL ASSOCIATES



## Risk-Based Decision Making Commentary
## 24 October 2014 Newsletter

### Microsoft PowerPoint Vulnerable to Zero-Day Attack

It seems that there is no end to the Windows zero-day vulnerabilities, as recently Microsoft patched three zero-day vulnerabilities in Windows which were actively exploited in the wild by hackers, and now a new Zero-day vulnerability has been disclosed affecting all supported releases of Windows operating system, excluding Windows Server 2003. Microsoft has issued a temporary security fix for the flaw and also confirmed **that the zero-day flaw is being actively exploited by the hackers through limited, targeted attacks using malicious Microsoft PowerPoint documents sent as email attachments.**

According to the Microsoft Security Advisory published on Tuesday, the zero-day vulnerability resides within the operating system's code that handles OLE (object linking and embedding) objects. OLE technology is most commonly used by Microsoft Office for embedding data from, for example, an Excel spreadsheet in a Word document. **The vulnerability (designated as CVE-2014-6352) is triggered when a user opens a PowerPoint file containing a malicious Object Linking and Embedding (OLE) object.** ***(Don`t click on links contained in e-mails!)*** For now on, only PowerPoint files are used by hackers to carry out attacks, but all Office file types could be used to carry out same attack.

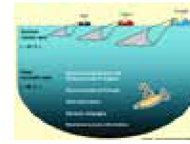
"The vulnerability could allow remote code execution if a user opens a specially crafted Microsoft Office file that contains an OLE object. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user," the advisory explained. By gaining same rights as a logged-in user, an attacker could infect victim's computer by installing other malicious programs on it. Microsoft has released a Fix - "OLE packager Shim Workaround" - which will stop the known PowerPoint attacks. But it is not capable of stopping other attacks that might be built to exploit this vulnerability. Also, the Fix is not available for 64-bit editions of PowerPoint on x64-based editions of Windows 8 and Windows 8.1. Meanwhile, Microsoft also urged Windows users to pay attention to the User Account Control (UAC) prompt, a pop-up alert that require authorization before the OS is allowed to perform various tasks, which would warn a user once the exploit starts to trigger – asking permission to execute. **But users many times see it as an inconvenience and many habitually click through without a second thought**.

Earlier this month, Microsoft released eight security bulletins, as part of its monthly patch update, fixing three zero-day flaws at the same time. One of which (CVE-2014-4114) was discovered by iSight partners in all supported versions of Microsoft Windows and Windows Server 2008 and 2012 that was being exploited in the "Sandworm" cyberattack to penetrate major corporations' networks.

http://thehackernews.com/2014/10/microsoft-powerpoint-vulnerable-to-zero.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TheHackersNews+%28The+Hackers+News+-+Security+Blog%29&_m=3n.009a.740.wb0ao05fi9.fhf

**https://technet.microsoft.com/en-us/library/security/ms14-oct.aspx**


# HALL ASSOCIATES



## Darknets: Murky recesses of the hidden web

The Brazilian police investigation that cracked a high-tech child porn ring earlier this month has shone a spotlight on the darker recesses of the web, an area which still poses massive technology challenges to law enforcement. The ring was buried deep inside a “darknet” – private networks built from connections between trusted peers using unconventional protocols.

Darknets are just one part of what is known as the deep web – a vast network which is not indexed by search engines such as Google and Bing. While most of the deep web is not mired in criminality - resources such as academic databases and libraries are said to make up much of its content - darknets typically run on the fortress-like Tor network. Tor, which stands for ‘The Onion Router,’ started out as a military project, but now functions largely as a highly clandestine civilian network. Every connection that you make with Tor is not only encrypted, but it’s routed via three ‘hops’ around the world.

Users connect to the network by downloading a free Tor web browser, which can then be used to access myriad 'hidden' sites. There are specific repositories that are lists of what is available. The Tor Metrics web site says that the network has just over 2.25 million users. People communicating via Tor include the likes of whistleblowers and journalists as well as activists and dissidents, particularly in countries with repressive regimes. With Tor offering extremely high levels of anonymity, however, criminals have been quick to exploit it. Today, for a cybercriminal, it’s quite easy. Crooks can and are using Tor-based black markets for drugs, weapons, underage sex and hacking/malware services.

Law enforcement and intelligence agencies across the globe are working hard to peel away the anonymity of Tor users. Confronted with the challenge of breaking the network’s encryption or attacking flaws in its infrastructure, attackers are concentrating their efforts on the latter option, according to a security expert. Still, though, much of Tor remains clouded in secrecy. Even the number of sites running on the network is a mystery, although there are estimates that it may be a relatively modest number, probably in the hundreds.

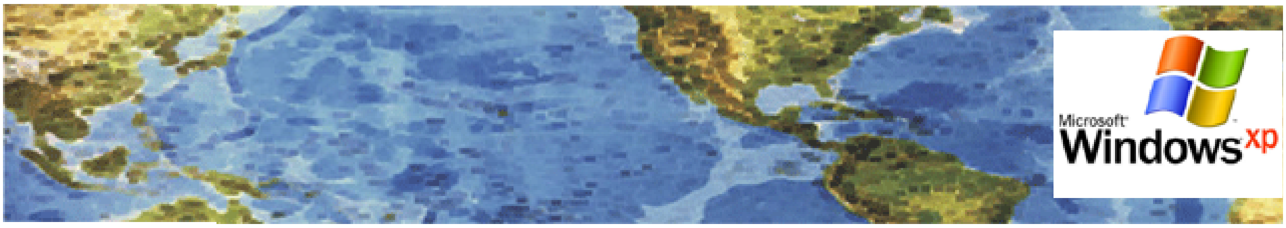
**New ‘Google’ for the Dark Web Makes Buying Dope and Guns Easy**

The dark web just got a little less dark with the launch of a new search engine that lets you easily find illicit drugs and other contraband online. Grams, which launched earlier this year and is patterned after Google, is accessible only through the Tor anonymizing browser but fills a niche for anyone seeking quick access to sites selling drugs, guns, stolen credit card numbers, counterfeit cash and fake IDs — sites that previously only could be found by users who knew the exact URL for the site.

The engine also includes a number of Google-like features including an “I Feel Lucky” search button (one test of it produced listings for high-quality crystal meth) and other features that allow users to filter out results for sites they don’t want to see and sort items for price and the most recent listings. There are even plans for advertising a la Google adwords, according to the developer of Grams, who has been posting announcements about his progress on Reddit.

http://www.foxnews.com/tech/2014/10/24/darknets-murky-recesses-hidden-web
http://www.wired.com/2014/04/grams-search-engine-dark-web/ /

# HALL ASSOCIATES




## Risk-Based Decision Making Commentary
## 25 August 2013 Newsletter

### The End Is In Sight – For Windows XP Support that is.

Microsoft will cease support for Windows XP on April 8, 2014, and disasters of biblical proportions could follow! Unprotected by continued security patches, Windows XP could become a festering wasteland where banking Trojans rob people blind, shifty criminals hijack little old ladies' computers on a whim, and innocent PCs get drafted into botnets to work at exploitative data mines all day long.

OK, the above scenario might be a little extreme, but Windows XP users (of whom there are still a huge number) have known since April 2013 that XP's days were numbered, and many of them have yet to switch over to Windows 7 or 8. Come April 2014, this will make Windows XP into a haven for malicious hackers, as users will have little recourse against new forms of malware.

The threat of malware is pressing. As long as Windows XP has a sizable user base, it will remain a tempting target for purveyors of harmful software. After April 2014, Windows XP will not receive any more security updates. Savvy users can still avoid and treat malware, but others will find their systems infected and have little to no recourse. There are supposed to be people developing XP exploits and saving them up and waiting till after the sundown date. In any case, there are people who figure out how to exploit various operating systems and sell them to someone else to actually develop the malware. This is a serious and growing marketplace. A few new malware types might not be a major problem, but a gradual buildup almost certainly will. Every time a new problem in XP is found, those things will build on one another, month after month, and the risk will increase almost exponentially over the next few years.

Note that most Windows 7 and 8 bugs are based on the core Windows software, **which has not changed since Windows 95**. This means that when Microsoft releases patch notes for 7 and 8, it will give exploiters a number of easy new ways to compromise XP. Three or four new bugs each month may seem harmless, but the problems will be additive; within a few months, an XP system could be vulnerable to 15 or 20 crippling flaws. And the only recourse you have, if you are not a security developer able to correct your system yourself, is to change to Windows 7 or 8.

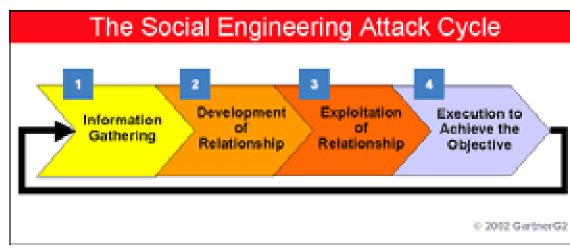
http://www.tomsguide.com/us/windows-xp-malware-deluge,review-1872.html?cmpid=532509

## New Version of Email Scam (At least to me)

Print http://us-mg6.mail.yahoo.com/neo/launch?.rand=a1cple21c037h#mail

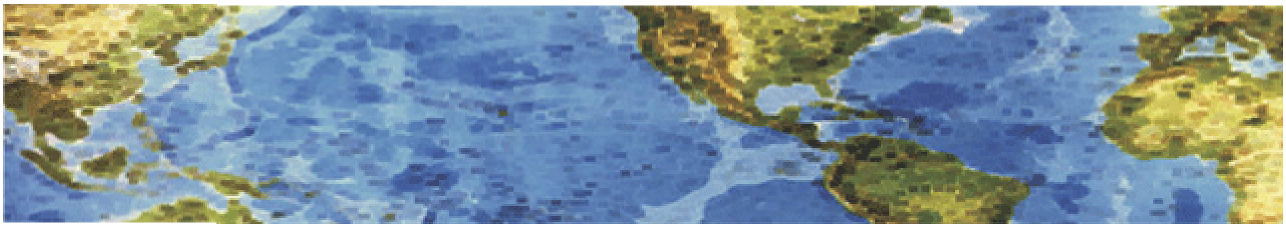

**Subject:** LOTTERY BENEFICIARY #3.
**From:** Gillian and Adrian Bayford (elba_esta@inah.gob.mx)
**To:** elba_esta@inah.gob.mx;
**Date:** Thursday, August 22, 2013 4:50 AM

We are Gillian and Adrian Bayford. My wife and I won the biggest Euro Millions lottery prize of 148 Million GBP and we just commenced our Charity Donation and we will be giving out a cash donation of 1,500,000.00 GBP to 5 lucky individuals and 10 charity organizations from any part of the world. To verify the genuineness of this email, check this web page;
http://news.sky.com/story/972395/148-6m-euromillions-jackpot-winners-named
Your email address was submitted to my wife and I by the Google Management Team and you are therefore approved 1,500,000.00 GBP.
For claims, fill and submit the below details.
============
Full Name:
Address:
Country:
Age:
Occupation:
Sex:
Mobile/Tel:
Scan copy of identification:
============
Congratulations & Happy Celebrations in Advance.
Gillian and Adrian Bayford's
Email:gillianandadrian@qq.com




**Social engineering, in this case the e-mail,** is the act of manipulating people into performing actions or divulging confidential information, rather than by breaking in or using technical cracking techniques. While similar to a confidence trick or simple fraud, the term typically applies to trickery or deception for the purpose of information gathering, fraud, or computer system access. Fraudsters are perfecting their abilities to target and manipulate people. Well-crafted social engineering schemes take advantage of common user behavior. While this e-mail may look dumb and you think "No one is their right mind would fall for this" it is really a great example of social engineering. Only those ignorant enough, greedy enough or desperate enough will respond, thereby minimizing the scammers task of getting people to work on. Don't click on unknown links or **provide personally identifiable information** to someone you don't positively know. I would not recommend going to the referenced web site just to see what this is. In some cases that's all you need to do to download malware. The best way to avoid being scammed is by knowing what to look for and to NOT give out any personal information to anyone unless you absolutely know who you are giving your information to.

# HALL ASSOCIATES



## Risk-Based Decision Making Commentary
## 25 Oct 2013 Newsletter

### Hackers Stole $100,000 from Users of a California ISP

In 2013 there has been a dramatic increase in the number of hack attacks attempted against banks, credit unions and utility companies using various techniques including DDoS attack, SQL injection, DNS Hijacking and Zero-Day Flaws. SQL Injection is one of the most common security vulnerabilities on the web and is successful when the web application is not sufficiently secured.

Recently a hacking Group named 'TeamBerserk' claimed on Twitter that they have stolen $100,000 by leveraging user names and passwords taken from a California ISP Sebastian (Sebastiancorp.com) to access victims' bank accounts. A video proof was uploaded on the Internet, shows how hackers used a SQL injection attack against the California ISP Sebastian to access their customers' database that included e-mail addresses, user names and clear text passwords and **then used the same data to steal money from those customers.**

Using SQL Injection on an unsecure web application, hackers can determine the structure and location of key databases and can download the database or compromise the database server. In this case, hackers took just 15 minutes to hack into the website **using an automated** SQL Injection tool -- stole customers' database and then immediately accessed the victims' Gmail accounts, linked PayPal accounts and bank accounts. The main problem here is that many people just use the same password over and over. Is your Facebook password the same as your Twitter password and the same as your back account password?

This hack shows **why it's extremely dangerous** to use the same password on more than one Web site. In the POC video, the hacker randomly chooses one username and uses his relative password against Paypal, Gmail and even Citibank account logins and that actually worked **because the victim was using the same passwords for all websites.**

If you are using a single, or only a few, passwords for all of your important accounts, you need to change that. If you have any type of accounts that are accessed online, bank account, credit cards, financial, etc., conduct a thorough security audit on them. Check every time you access the account to see when the last time "you" logged in to see if anyone else has accessed it. Be sure to keep using different and strong passwords for each website.
http://thehackernews.com/2013/10/hacker-stole-100000-from-users-of.html


## Obamacare launch spawns 700+ cyber-squatters capitalizing on Healthcare.gov, state exchanges

More than 700 websites have been created with names playing off of Obamacare or Healthcare.gov, making it likely that some Americans will mistakenly hand over private information to unknown third-parties. For instance, there is a website — www.obama-care.us — that brands itself as part of the "Obamacare enrollment team," directs people to an "Obamacare enrollment form" and asks users for their name, address, Social Security number and other contact information. According to a counter at the bottom of the page, more than 3,000 people have visited obama-care.us.

This website does not actually enable people to enroll in Obamacare. It was registered with GoDaddy.com on Sept. 2 — less than a month before the official launch of the health care exchange websites — according to who.is, a website that provides information on internet domains and their owners. The practice of setting up websites with names that are similar to high-profile pages is known as cyber-squatting. It can be used by private businesses looking to siphon traffic away from their competitors, by marketers selling ads to private companies — by visiting a website, you're revealing your interest in a given product — or by identity thieves.

A legitimate website established in 1994 goes by the name "healthcare.com" — exactly the same as the website for the federal health care exchange, except that the official site ends with a dot-gov suffix. That raises the question of why federal officials chose a URL of such similarity to an existing health-related web site. The retired cybersecurity expert guessed, based on his experience in the industry, that healthcare.com could receive as much as 30 percent of traffic intended for the main federal exchange page. He said that cyber-squatters generally siphon 10 to 40 percent of the a site's traffic, adding that the official Obamacare sites will likely be on the upper end of that range, given the large number of squatters.

To prevent cyber-squatting, professional website owners typically purchase domain names that are similar to the main page. "I was shocked to find out that they have not picked up any of these other top-level domains," the cybersecurity expert said. He also provided the Washington Examiner with a list of 221 websites that he identified, using proprietary software, as cyber-squatters taking advantage of the healthcare.gov rollout — websites such as healthcarer.com — and another 499 that he identified as squatting on state exchange websites. Online security expert John McAfee predicted such a problem weeks ago. "There is no central place where I can go and say, 'OK, here are all the legitimate brokers and examiners, for all of the states,' and pick and choose one," McAfee told Fox News' Neil Cavuto. "[I]nstead, any hacker can put a website up, and make it look extremely competitive, and because of the nature of the system — this is health care, after all — they can ask you the most intimate questions and you're freely going to answer them.

Check out http://washingtonexaminer.com/obamacare-launch-spawns-700-cyber-squatters-capitalizing-on-healthcare.gov-state-exchanges/article/2537691 for the entire article.