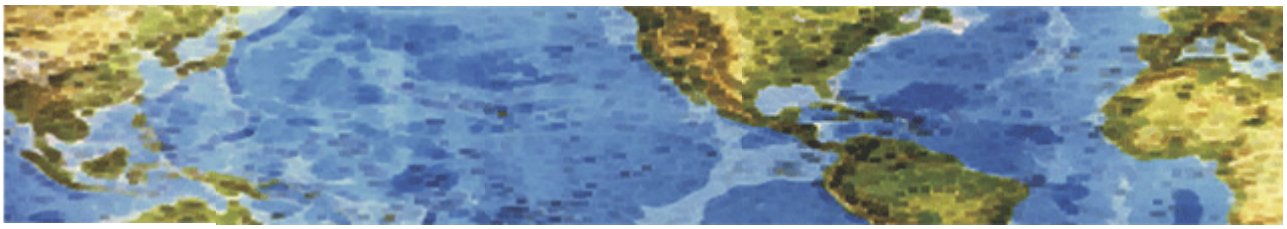
HALL ASSOCIATES



Risk-Based Decision Making Commentary
August 2012 Newsletter #2

Hackers Do Target Small Businesses

Small businesses are more at risk from identity theft than large companies. Large businesses can afford to hire IT professionals that focus solely on security while small businesses don't even know what vulnerabilities exist. While many small businesses think that their small size means that they are not on a Hacker's radar screen, the existence of holes in their systems is exactly what is attracting the criminals. Hackers use automated tools to search the internet and look for vulnerable sites and computers.

The main defense against this is making sure that your computer systems are safe and secure. Make sure that the software is updated and all patches are installed properly, have policies in place so that employees don't visit dubious web sites, click on e-mail links or inadvertently share information with the wrong person. Have strong passwords on all systems and make sure all your data is encrypted. Encryption is the simplest and most powerful security measure.

If you are infiltrated or breached, and personal customer data falls into the wrong hands, how you respond makes a world of difference. You should notify law enforcement about the breach immediately and notify customers/other businesses that are impacted to give them the chance to reduce potential misuse of their information.

This early notification demonstrates that you are taking the incident seriously and potentially could reduce your responsibility for future uses of the data. When notifying customers, it is necessary to look at the type of compromise, the information stolen, the chances of the information being misused and the potential damage.

HALL ASSOCIATES

Bogus Vendor Bills Bucket

Billing schemes come in all different shapes and sizes but small businesses are a primary target. Unlike larger businesses, small businesses rarely have segregation of duties and limited internal controls, making them more vulnerable to scammers. Small businesses rarely mandate payment compliance rules that employees have to abide by.

The current average cost of fraud for small businesses is $155,000 (2010). And once you have been the target of one scam artist, your information is shared with others on a list of easy prey. To protect yourself you first must know what to look for.

One popular scam is the phony grant scheme. A small business will get a call from a so-called grant writing service that promises government grants. However, first you must pay a processing fee of $3000 to $5000 and the grant company will get you into the waiting list. The “grant company” then disappears.

Another scam is the compliance scan. This scam targets SBs that are incorporated. They get an official looking letter stating that they are not in compliance with annual filing minutes and require a processing fee. Many simply assume that this is official and pay the fee.

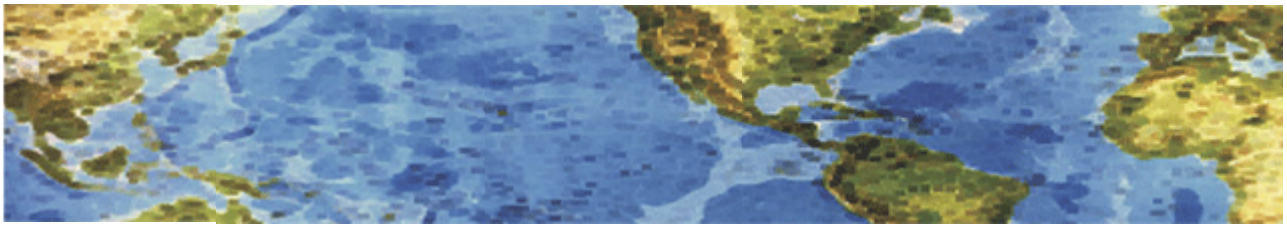
In another scam, someone will offer you free samples of printing toner and send you the product even if you say no. Before long, you will be hit with a grossly overstated bill and the company won’t accept returns.

In another scam, a business will get a call supposedly from their phone company telling you that they want to check the line and to press 90#. Once that happens, the scam artist can place long distance phone calls and bill them to your business.

In another scam, someone will collect enough information about a business to make a phony bill look legitimate. The fake bills will be small enough not to raise a red flag and may even include past due of final notice notes to pressure the SB to pay quickly. When it comes to paying bills, be sure to read the fine print and never accept free products over the phone.

Be sure to educate all employees about the different scams so that they know what to look for. You need to know who you pay money to and need to follow the rules.

HALL ASSOCIATES



Risk-Based Decision Making Commentary
July 2012 Newsletter

Why Should Small Businesses Use Risk Management?

Risk is a part of being in business. Risks can be managed and bad outcomes can be controlled in large part. The greatest challenge for small businesses is to find the proper balance between peace of mind and profitability. Trying to eliminate (or ignore) risk from your business is unrealistic and can be prohibitively expensive or cause you to be so risk averse that your business never grows. And the risk environment you face as a small business is constantly changing.

What is the main challenge? For most businesses it is to determine what risks pertain to them and to use a repeatable, effective and minimal cost process to identify, assess, control and monitor risk without interrupting their business activities. This series of newsletters will discuss what can affect you and how you should respond to protect your business, your employees and yourself. If you have any questions or comments, let me know at halld105048@yahoo.com.

One major example of a rapidly changing risk environment is that of Information Technology and Cyberspace use. Your business increasingly works with and through the Internet and IT systems, making the risks inherent in IT systems and cyberspace far more visible and significant than ever. There are more and different threats "in the wild" every few months, making use of the Internet and cyberspace increasingly more problematic. It's not a case of **IF**, but **WHEN** you will be troubled by one or more of these threats. IT and cyberspace risks, when they occur, can cause business losses - lost revenue, lost customers, lost reputation, lost personnel effectiveness, lost productivity. And if you don't know what risks you face in your business, you will not be prepared for them.

So what is an IT or cyberspace risk? Basically they are any threat to your information, data, critical systems and business processes. Why should you be concerned about them? Because anyone in a business, especially management, has a responsibility to identify areas of risk and respond in a timely fashion by improving processes, augmenting controls and requiring testing to ensure that the business is properly identifying and responding to risks. Failure to identify, assess, control and monitor risk sets the business up for serious problems and significant financial losses now and in the not-so-distant future.

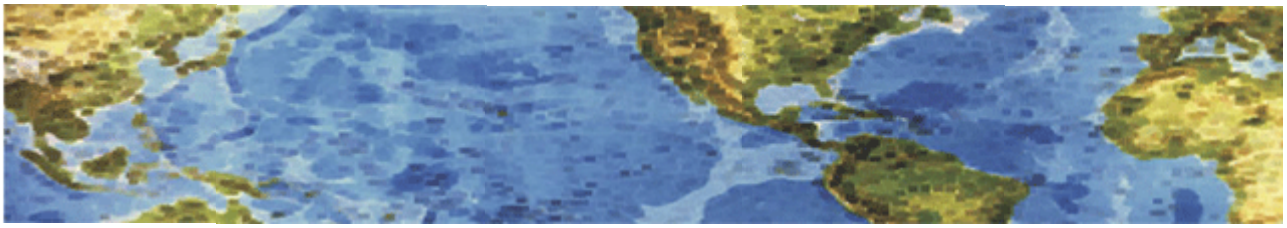
HALL ASSOCIATES

Latest Cyberspace Recommendations

We had a question at my last presentation about "Is PayPal safe to use?". PayPal is as secure as any other online credit account, but no such account is entirely safe, especially from the user side. Following are some recommendations I have found that should enable you to minimize (not eliminate) potential risks when using such sites. Note, however, that these are only recommendations and you should determine exactly what you need to do depending on your specific circumstances.

1. Don't link your PayPal account to your bank account or debit card account. If your PayPal account is compromised, it's money taken directly out of your bank account and by federal law (Regulation E) you only have two days to refute a fraudulent charge with your bank. . But if you link your PayPal account to your credit card and it's compromised, then you have 60 days to refute those charges with your credit card company. However, I did find a note that stated "A spokeswoman for Access Communications, acting as PayPal's representative, has said that PayPal's protection from unauthorized transactions gives the user 60 days to dispute the charges, no matter what the funding source".
2. Don't click on links in the body of emails from PayPal. Those emails might not really be from PayPal. Rather, they may be phishing e-mails from scammers designed to get you to enter your credentials. Instead, manually type in the PayPal address into your browser, log in to your account and see if there are any communications for you from PayPal. Remember, **NO** organization, be it PayPal, a credit card system, a bank, a commercial firm or the Federal Government, will **EVER** ask for your account information or personal information via e-mail.
3. Keep your PC, Cell Phone, I-Pad, etc. security up-to-date. Make sure you have installed the latest critical security patches to your operating system, as well as the latest browser patches and have updated antivirus/internet security software. If whatever you use to connect to a site is compromised with spyware or malicious software when you're using a financial site like PayPal, then others have access to your computer, phone, I-Pad, etc. and can access your user names and passwords. And that is not PayPal's fault.
4. Never log in to PayPal from a public PC or someone else's computer, phone or I-Pad. Each of these is only as secure as the person who logged in before you. Someone could easily have installed spyware or malicious software that will log all your keystrokes.
5. Maintain good records for all Internet commerce. It's a good idea to download and print final pages so that you have backups for purchases made and products bought and sold.
6. Treat your PayPal account like you treat your online banking account. You need to ensure that you have authorized any transactions, large or small. Typically, someone will start draining your account using a series of small withdrawals, hoping you won't notice. So you need to refute those charges as soon as possible and let PayPal know that your account may have been compromised.

HALL ASSOCIATES



Risk-Based Decision Making Commentary
November 2012 Newsletter #2

Mobile Device Malware Risk Increases

Mobile malware (malicious software downloaded to your smart phone) is exploding at a time when financial institutions and small businesses are increasing their mobile banking offerings and consumers are making broader use of smart phones and tablets. A recent study from software and security firm Trend Micro finds that mobile malware attacks hit record numbers in the third quarter, with Android devices as the primary targets. The increase in the threat is dramatic, but traditional countermeasures being used require many more updates than is practical on handsets, or consume too much battery power - or both. Also many (most?) mobile device users are often too hasty to provide sensitive personal and financial information when prompted by an app or browser request. But the most critical area to address is technology. Security specialists say many banks and credit unions have not invested enough in malware detection and protection technologies, regardless of the channel. Might be very useful to check your financial institution's mobile security efforts as well as increase your own

Security experts and law-enforcement authorities say anything stored on a mobile device or input via mobile applications could potentially be at risk.

Malicious or potentially malicious mobile applications jumped from 25,000 to 175,000 over one quarter. Those mobile apps primarily targeted devices running Google's Android operating system, and most contained adware or spyware. Adware is often pushed to mobile users as a free software offer in exchange for consumer information. Although some adware is legitimate, hackers are using adware that morphs into spyware to collect user information for nefarious purposes. Hackers already highjack out-of-band authentication measures put in place to verify transactions initiated via online banking, as well as steal credentials and other sensitive information input via mobile-banking apps and mobile browsing.

The Federal Bureau of Investigation's Internet Crime Complaint Center issued an alert in October about newly identified spyware risks targeting Android devices. The FBI identified two new Android Trojans known as Loozfon and FinFisher. Loozfon is designed to steal mobile numbers and contact details saved in address books, while FinFisher is spyware that enables hackers to remotely control and monitor a compromised device. The aim of both Trojans: To steal or collect personal and sensitive information stored on Android devices.

Most users (***YOU!***) have not started to think about a mobile device as a computer. They don't feel that the mobile phone or tablet is something that can be compromised. Android's significant mobile market share, coupled with its openness and ***users' reluctance to proactively secure*** Android devices, has made it an easy target for cybercrime.

HALL ASSOCIATES

Are Your E-Mails Really Private – NO!

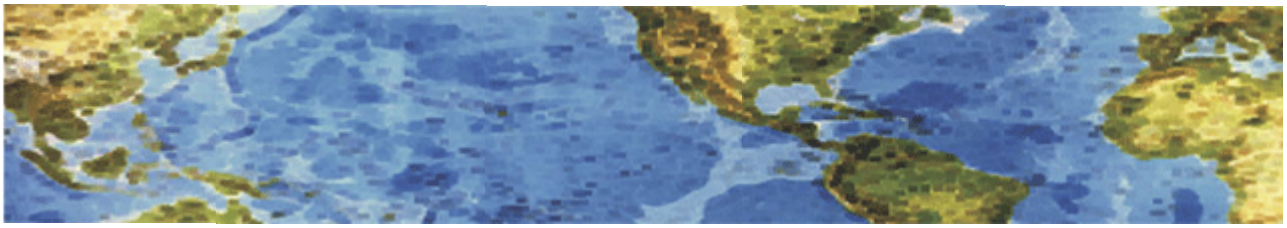
The Internet and e-mails do seem to have an anonymizing (being anonymous or private) effects on people's thoughts. From where you sit, most people are little more than a signature and a couple of hundred black words on a white field. It's a fact, or fiction, that gives many Internet users solace. Although E-mail is supposedly private and believed to be confidential, there are many ways that E-mails can be found, seen, and read -- even if you have deleted them. The real world equivalent of an email is a postcard. When you send a postcard you know that a lot of people can read it if they want to, but they're probably be too busy to bother.

And as some people have recently learned in very real and damaging ways, online anonymity is not a guarantee. Ask former CIA Director Gen. David Petraeus and his biographer Paula Broadwell, who used the tried-and-failed technique of leaving communiqués in the draft folders of email accounts. Ask the members of the hacktivist movement Anonymous, whose leaders have been outed, arrested and convicted due to their supposedly untraceable online activities. **If anything, the Internet has made the world a less anonymous place. There are more details about more people available from more places than there have ever been. And we all throw it up there willingly.**

Although an e-mail provider does not go into your account and read e-mails you send or receive, the e-mails are archived. Your activities are also logged (to some extent). If the company's records are subpoenaed, the company must turn over all records concerning your account, including e-mails received and sent. The authorities may also look at times you signed on and off from an Internet Provider or E-mail Provider. Is it possible to communicate with others online with absolute certainty that messages won't ever be found, read and traced back to you? The short answer is NO. But you can be anonymous, sort of. It all depends on who is looking for what and how much trouble you want to go through.

Don't let all this put you off sending those email postcards. They're safe enough. Email is a less secure than your telephone or normal mail, but still safe enough for most purposes. **Just don't put anything in an email (or in an e-mail attachment) that you wouldn't want to see on the evening news.**

HALL ASSOCIATES



Risk-Based Decision Making Commentary
October 2012 Newsletter #1

Personal Data Theft

The confidential information of nearly 300,000 students, faculty and employees at Northwest Florida State college have been accessed by hackers in a massive security breach that happened sometime between May and September. The data accessed was in several different databases, but the hackers were able to combine all into one download. The data included names, SSNs, birthdates, bank account information for direct deposits, and other personal information.

Over 50 employees (to date) have reported issues with identity theft. Their information has been used to obtain personal loans or get credit cards. The college, local, state and federal authorities are involved in trying to locate the hackers and stop the information from being passed around the internet.

This breach shows how your information could be targeted by hackers. Does your personal and bank account information reside on somebody's server from years ago or yesterday? Have you ever provided direct deposit information to anyone at any time in your life? Do you know if their databases are protected? Have you ever requested all such information be purged or at least taken off internet accessible computers once your association with the company, college or organization was over? Do you know if the company, college or organization is encrypting and periodically assessing their systems to ensure there has not been a breach? Looks like this one was found only after some employees complained of identity theft.

Several organizations (like the credit rating companies and others) will provide a continuous web search for account numbers, SSNs and other personal information so if your information does hit the web, you can find out quickly.

HALL ASSOCIATES

Apple Device ID Targeted

Apple ID Holders have been targeted in the latest phishing scam. An Apple ID is essentially and all-access pass to an individual's Apple devices, applications and the iCloud. It allows customers to seamlessly sync their devices in order to back up and access data at home, in the office or on the road. It makes managing your online life easier – unless a scammer gets their hands on it – then seamless integrations becomes a nightmare.

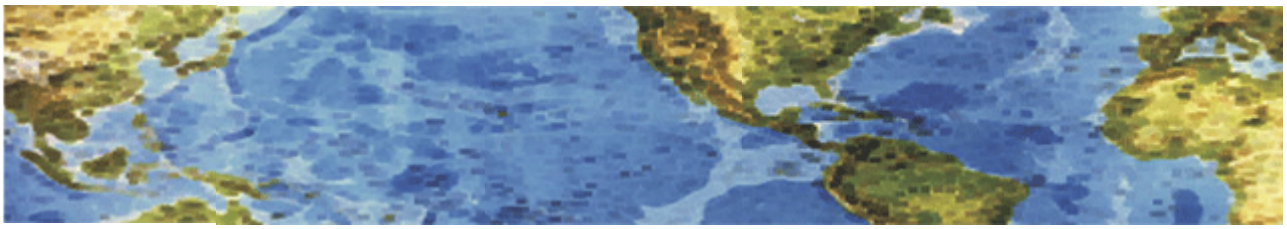
This latest phishing scam targets Apple ID holders and attempts to dupe them into giving up their account information by informing them "that their Apple ID has been suspended". The e-mail usually reads:

Dear Customer, Your Apple ID has been temporarily suspended! Somebody just tried to sign in into your Apple account from another IP address. Please confirm your identity today or your account will be suspended due to concerns we have for the safety and integrity of the Apple community.

Despite the poor appearance and awkward English, the link victims are asked to follow sends them to a web page that looks almost exactly like the Apple corporate site (here would be a good place to really check the URL in the e-mail). There, users can "sign in" using their Apple ID and password. That provides these scammers enough information to access and steal personal information, data and anything else you have in your Apple devices.

All internet users are being targeted by phishing scams. Cybercriminals are on a constant (usually automated) hunt for your vulnerabilities so they can access your information. When online, everyone should be wary of sharing login information with **ANY** website, even if it appears to be a trusted one. Scammers often create dummy pages that look very familiar in the browser, but not in the address bar. So do not trust, but verify everything.

HALL ASSOCIATES



Risk-Based Decision Making Commentary
September 2012 Newsletter #1

New Media – Old Risks, Risks of Using Social Media

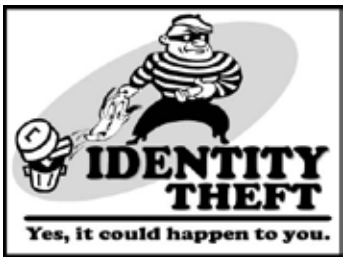
Social media is now a mainstream form of communication. You might not yet be using social media for your business, but some if not all of your employees are probably actively engaged on their own accounts. And your customers and prospects may well be posting about your products/services/ customer relations out there in the Cyberworld. With social media, everything gets around the entire world with the click of a mouse. That should be reason enough to address social media as part of your business risk management framework and establish social media policies.

A few social media risks a business should consider when developing a social media policy:

1. Negative comments posted by an employee (not during work hours) triggering claims of harassment by other employees.
2. Excessive use of social media during work hours, reducing productivity or affecting customer relations.
3. A disgruntled client/customer (or a cyber extortionist) posting negative comments across social media sites.
4. An employee posting confidential information (or Privacy act or HIPPA information) to a social media site either deliberately or inadvertently.
5. Giving in to the temptation to game the system by posting self-generated reviews and testimonials either anonymously or under false names in social media (prohibited by law in the US and most other countries).
6. Not using content created by others properly in promoting your business.
7. Not using “entirely” truthful descriptions when describing your products and services.
8. Blurring the line between business and personal social media communications.
9. Providing information that may be mistaken or is somehow misleading.

Using social media for business promotional purposes can be very beneficial, but can also lead to legal liabilities if a systematic approach is not applied. Social media is now very important and can be very useful to a business, but a healthy respect for the associated risks needs to be cultivated. The risks can lead to catastrophic problems if they are not managed proactively. Most of the social media risks can be handled by policies, but all policies (especially those pertaining to cyber) need to be supplemented with training of all employees. Most people cause problems accidentally because they don’t know any better.

HALL ASSOCIATES

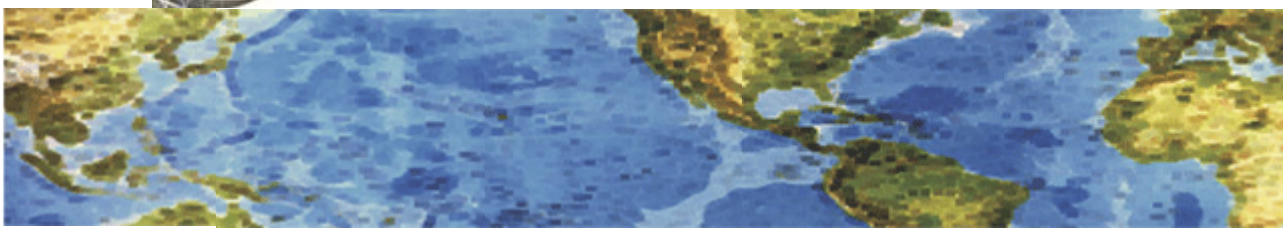


College Student Identity Theft

Millions of Americans have their identities stolen each year as cybercriminals scour the internet for easy victims. College students are not immune. They make up about 25% of all identity theft victims according to the Better Business Bureau. College students need a strong understanding of how to protect their personal information and defend against identity theft. Following are ten recommendations to help college students defend against identity theft (it's impossible to totally protect against identity theft and everyone's situation is different):

1. Always check your bank statements and bills carefully – develop good habits and scrutinize each statement and bill for unexplained or unexpected withdrawals or charges.
2. Sign up for electronic statements – most college students don't shred paper documents with personal information on them, they just toss them out in the trash.
3. Monitor your credit rating – Cybercriminals really don't care about the $100 in your bank account, they are after SSN and credit histories that will allow them to open new accounts, take out loans or get new IDs.
4. Don't use unsecured Wi-Fi networks, computers or websites – Students regularly use unsecured wireless networks and public computers scattered around campus. When doing this, they should remember that anything being typed can be read by someone else. Don't log into a bank site or any site that requires a user name and password.
5. Use only secure connections when submitting important information – Always look for the https:// and the lock image on the website before submitting sensitive information and login credentials.
6. Don't let your personal computer or tablet or smartphone become a communal machine - Lock up your devices when not using them so that other people can't use them and NEVER let anyone use your device when you are logged in.
7. Use passwords and encryption – Always protect your devices with passwords (strong passwords!) and encrypt the data to prevent anyone else getting your data even if the device is lost or stolen.
8. NEVER share passwords – not even with roommates or your new (or old) BFF living down the hall.
9. Don't put too much information on social media sites – Don't fill out all the available fields on a social networking site and don't input personal information that could be used to establish an identity, set a password or used for a security question.
10. Bottom line – Don't trust anyone completely. Students are very trusting, but don't share passwords and PINS with friends and don't let someone look over your shoulder if you are entering passwords or PINs on a computer, phone or ATM. Secure your sensitive papers rather than leave them on your desk.

HALL ASSOCIATES



Risk-Based Decision Making Commentary
September 2012 Newsletter #3

Copier Data Security: A Guide for Businesses by the FTC

Does your company keep sensitive data — Social Security numbers, credit reports, account numbers, health records, or business secrets? If so, then you've probably instituted safeguards to protect that information, whether it's stored in computers or on paper. That's not only good business, but may be required by law. According to the Federal Trade Commission your information security plans also should cover the digital copiers your company uses. If the data on your copiers gets into the wrong hands, it could lead to fraud and identity theft.

The hard drive in a digital copier stores data about the documents it copies, prints, scans, faxes or emails. If you don't take steps to protect that data, it can be stolen from the hard drive, either by remote access or by extracting the data once the drive has been removed. Digital copiers store different types of information in different ways. For example, photocopied images are more difficult to access directly from the hard drive than documents that are faxed, scanned or printed on the copier.

If you acquire a copier, make sure it's included in your organization's information security policies. Copiers should be managed and maintained by your organization's IT staff. When you buy or lease a copier evaluate your options for securing the data on the device. Most manufacturers offer data security features with their copiers, either as standard equipment or as optional add-on kits.

Depending on the information your business stores, transmits, or receives, you also may have more specific compliance obligations. For example, if you receive consumer information, like credit reports or employee background screens, you may be required to follow the Disposal Rule, which requires a company to properly dispose of any such information stored on its digital copier, just as it would properly dispose of paper information or information stored on computers. Similarly, financial institutions may be required to follow the Gramm-Leach-Bliley Safeguards Rule, which requires a security plan to protect the confidentiality and integrity of personal consumer information, including information stored on digital copiers.

http://business.ftc.gov/documents/bus43-copier-data-securityis a link to the full article.

HALL ASSOCIATES

FTC Halts Computer Spying

Secretly Installed Software on Rented Computers Collected Information, Took Pictures of Consumers in Their Homes, Tracked Consumers' Locations

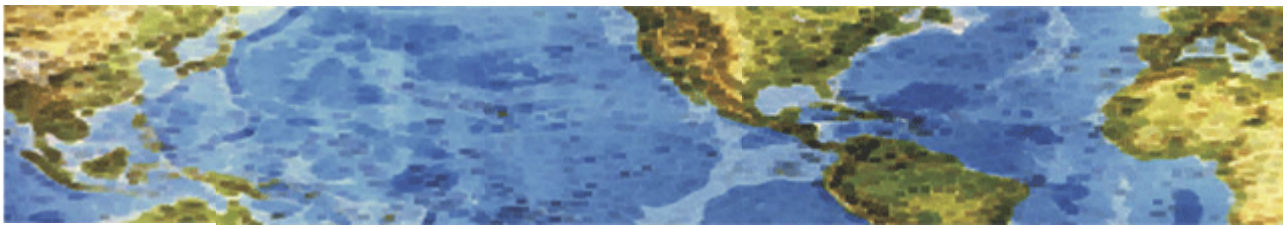
Seven rent-to-own companies and a software design firm have agreed to settle Federal Trade Commission charges that they spied on consumers using computers rented from them, capturing screenshots of confidential and personal information, logging their computer keystrokes, and in some cases taking webcam pictures of people in their homes, all without notice to, or consent from, the consumers. The software design firm collected the data that enabled rent-to-own stores to track the location of rented computers without consumers' knowledge. The settlements bar the companies from any further illegal spying, from activating location-tracking software without the consent of computer renters and notice to computer users, and from deceptively collecting and disclosing information about consumers.

"An agreement to rent a computer doesn't give a company license to access consumers' private emails, bank account information, and medical records, or, even worse, webcam photos of people in the privacy of their own homes," said Jon Leibowitz, Chairman of the FTC. "The FTC orders today will put an end to their cyber spying." The FTC named DesignerWare, LLC, a company that licensed software to rent-to-own stores to help them track and recover rented computers. The FTC also reached settlements with seven companies that operate rent-to-own stores and licensed software from DesignerWare, including franchisees of Aaron's, ColorTyme, and Premier Rental Purchase.

According to the FTC, DesignerWare's software contained a "kill switch" the rent-to-own stores could use to disable a computer if it was stolen, or if the renter failed to make timely payments. DesignerWare also had an add-on program known as "Detective Mode" that purportedly helped rent-to-own stores locate rented computers and collect late payments. DesignerWare's software also collected data that allowed the rent-to-own operators to secretly track the location of rented computers, and thus the computers' users. When Detective Mode was activated, the software could log key strokes, capture screen shots and take photographs using a computer's webcam, the FTC alleged. It also presented a fake software program registration screen that tricked consumers into providing their personal contact information. Data gathered by DesignerWare and provided to rent-to-own stores using Detective Mode revealed private and confidential details about computer users, such as user names and passwords for email accounts, social media websites, and financial institutions; Social Security numbers; medical records; private emails to doctors; bank and credit card statements; and webcam pictures of children, partially undressed individuals, and intimate activities at home, according to the FTC.

The seven rent-to-own companies were charged with breaking the law by secretly collecting consumers' confidential and personal information and using it to try to collect money from them. Use of the bogus "registration" information was deceptive, the FTC alleged.
http://www.ftc.gov/opa/2012/09/designware.shtm is the link to the full story.

HALL ASSOCIATES



Risk-Based Decision Making Commentary
September 2012 Newsletter

Hackers Do Target Small Businesses

Small businesses are more at risk from identity theft than large companies. Large businesses can afford to hire IT professionals that focus solely on security while small businesses don't even know what vulnerabilities exist. While many small businesses think that their small size means that they are not on a Hacker's radar screen, the existence of holes in their systems is exactly what is attracting the criminals. Hackers use automated tools to search the internet and look for vulnerable sites and computers.

The main defense against this is making sure that your computer systems are safe and secure. Make sure that the software is updated and all patches are installed properly, have policies in place so that employees don't visit dubious web sites, click on e-mail links or inadvertently share information with the wrong person. Have strong passwords on all systems and make sure all your data is encrypted. Encryption is the simplest and most powerful security measure.

If you are infiltrated or breached, and personal customer data falls into the wrong hands, how you respond makes a world of difference. You should notify law enforcement about the breach immediately and notify customers/other businesses that are impacted to give them the chance to reduce potential misuse of their information.

This early notification demonstrates that you are taking the incident seriously and potentially could reduce your responsibility for future uses of the data. When notifying customers, it is necessary to look at the type of compromise, the information stolen, the chances of the information being misused and the potential damage.

HALL ASSOCIATES

Bogus Vendor Bills Bucket

Billing schemes come in all different shapes and sizes but small businesses are a primary target. Unlike larger businesses, small businesses rarely have segregation of duties and limited internal controls, making them more vulnerable to scammers. Small businesses rarely mandate payment compliance rules that employees have to abide by.

The current average cost of fraud for small businesses is $155,000 (2010). And once you have been the target of one scam artist, your information is shared with others on a list of easy prey. To protect yourself you first must know what to look for.

One popular scam is the phony grant scheme. A small business will get a call from a so-called grant writing service that promises government grants. However, first you must pay a processing fee of $3000 to $5000 and the grant company will get you into the waiting list. The “grant company” then disappears.

Another scam is the compliance scan. This scam targets SBs that are incorporated. They get an official looking letter stating that they are not in compliance with annual filing minutes and require a processing fee. Many simply assume that this is official and pay the fee.

In another scam, someone will offer you free samples of printing toner and send you the product even if you say no. Before long, you will be hit with a grossly overstated bill and the company won’t accept returns.

In another scam, a business will get a call supposedly from their phone company telling you that they want to check the line and to press 90#. Once that happens, the scam artist can place long distance phone calls and bill them to your business.

In another scam, someone will collect enough information about a business to make a phony bill look legitimate. The fake bills will be small enough not to raise a red flag and may even include past due of final notice notes to pressure the SB to pay quickly. When it comes to paying bills, be sure to read the fine print and never accept free products over the phone.

Be sure to educate all employees about the different scams so that they know what to look for. You need to know who you pay money to and need to follow the rules.