Interested in learning more about security?

# SANS Institute InfoSec Reading Room



## Protecting Small Business Banking

Online financial transactions are increasing exponentially; online attacks that attempt to capture credentials, intercept information, and divert funds from small businesses are as well. Small business owners are being increasingly targeted for financial based online crimes. Even worse, they are typically ill prepared and unable to take appropriate actions against the perpetrators of these crimes to recoup their losses. The current legal environment in the United States leaves these small businesses and their owners wi...

# Protecting Small Business Banking

GIAC (GSEC) Gold Certification

Author: Susan E. Bradley, (sbradcpa@pacbell.net)
Advisor: Ty Purcell (purcell.ty.sans@gmail.com)

Accepted: 06/10/2013

Abstract:

Online financial transactions are increasing exponentially; online attacks that attempt to capture credentials, intercept information, and divert funds from small businesses are as well. Small business owners are being increasingly targeted for financial based online crimes. Even worse, they are typically ill prepared and unable to take appropriate actions against the perpetrators of these crimes to recoup their losses. The current legal environment in the United States leaves these small businesses and their owners without the ability to obtain reimbursement from banking institutions resulting from these losses as well as unable to take the necessary legal actions against their attackers. It is therefore imperative to investigate ways to provide protection from these risks, and balance the needs of the business to continue to engage in online financial transactions.

# Protecting Small Business Banking

## 1. Introduction: The Problem.

Over the last several years, the use of online banking and other financial transactions have risen dramatically. A 2011 survey by the American Banking Association indicates that 57 percent of banking customers now prefer banking online as compared to just 20 percent the year before. (American Bankers Association, 2011) The definition of online banking technology includes access from traditional personal computers with web browsers as well as mobile devices that can scan and deposit checks. With these tools the customer can transfer funds, pay bills, and sync transactions with numerous accounting applications.

Online banking often includes viewing balances, reviewing transactions, or downloading bank statements. This can be accomplished online or within an accounting program and other formats. The use of this technology allows the financial institution customer to transfer funds, pay third parties, and deposit checks using remote deposit capture. These increased opportunities for remote access and mobility do not come without the associated risks that electronic activity introduces when it is performed without compensating controls.

Online banking introduces risks in the areas of authentication and nonrepudiation. The manner in which a customer performs the authentication process to their bank or credit union should, without exception, be set up in a manner to ensure that confirmation and verification of their identity can be safely conducted over the Internet. Currently many banks and credit unions use passwords and single sign on applications thus introducing a risk that a single ID grants access to the financial relationship with the bank or credit union. Nonrepudiation ensures that both parties to a transaction cannot later deny that the transaction took place. Ensuring that there are audit trails that document the transaction occurred are key to later proving that a transaction did indeed occur.

A US-Cert document originally released in 2006 noted that online banking introduced new challenges to financial security and online privacy. (US-Cert, 2008) The risks and methods

of attack that are specifically introduced by online banking include phishing attacks, malware and pharming attacks. Phishing attacks are where targeted malicious emails are used to trick an end user into entering sensitive identity information. Malware attacks are written to specifically look for bank account number patterns, credit card number patterns, account information and then send this information back to the attacker. Pharming attacks involve the installation of malicious software that sends targeted sensitive information back to the attacker.

Brian Krebs, author of KrebsonSecurity.com, tracks examples of this fraudulent activity and has been documenting the impact to small businesses on his security news site (Krebs, Cyberheists 'A helluva wakeup call', 2012) . He has noted that online fraudulent transactions involving funds stolen from business online banking accounts are not covered by FDIC insurance or by "Regulation E" of the Electronic Funds Transfer Act (or EFTA). If a business bank account is impacted by a fraudster, the bank does not indemnify the customer from losses relating to the fraud. If a fraudulent financial transfer occurs moving the funds out of the bank account to another bank or credit union, the chances are highly probable that the small business customer will have little to no recourse. If transferred to the accounts of an offshore banking institution, the opportunities for recovery are even more limited. Legal authorities such as the Federal Bureau of Investigation have few resources available to aid in recovery from another countries' member bank. The only recourse may be for the impacted business to attempt to take legal action overseas in the country where the attacker is located.

### 1.1. Attacked Machines

Typically the machines used for online banking are Windows based computers. All currently released versions of the Windows operating system are subject to these attacks. (As of May of 2013, supported operating systems are Windows XP SP2, Windows Vista, Windows 7 and Windows 8 for desktop operating machines, Windows Server 2003, Windows Server 2008, Windows Server 2008 R2 and Windows Server 2012 on the server platform.) (Wikipedia.org, 2013) The machines on these platforms are left vulnerable to attacks using various means. Attacks can come through weaknesses in the operating system itself through remote exploits. Attacks may come through exploiting various browser vulnerabilities, or through a number of third party add-ins such as Adobe Flash and Java. Additional risks to electronic banking are introduced by conducting electronic banking activities on general purpose workstations. This

may result in exposure to infection vectors on sites with banner ads that may include malicious code. Additional risks come from social engineering attacks, malware, and phishing, all attacks that an average computer user may face on a regular basis.

### 1.2. How they enter

Phishing attacks are specifically targeted emails that attempt to trick the user into providing their security credentials. These targeted emails have become very sophisticated in appearance and can fool nearly any user into believing that the email is legitimate. They can be as simple as an email intended to emulate a vendor request for credentials. They can also be as complex as Pharming attacks that use unpatched Microsoft Word and Adobe PDF vulnerabilities to enter the operating system and inject key loggers into the system. These key logging programs specifically look for financial number patterns in keyboard entries and capture web site account numbers, credit card numbers, social security numbers and other financial information.

#### 1.2.1. Attack vectors

When software is written, programmers build code to perform specific tasks. Code in the software is exploited by attackers to do something it was not intended to do (Securelist, 2012). This is known as a software vulnerability. Software is then patched or fixed with additional code to remedy the situation. Vulnerabilities can be caused by buffer overflows, cross site scripting, or other software coding problems. This can be a near constant cat and mouse game of deploying software and patching it to counter a weakness an attacker has found. In the Microsoft Security Intelligent Report, Volume 13 (Microsoft, 2012), the JS/Blacole family of exploits was the most detected exploit group in the first half of 2012. (Microsoft, 2012) This group of vulnerabilities targeted various susceptible software including Adobe Flash Player, Adobe Reader, Microsoft Data Access Components (MDAC), the Oracle Java Runtime Environment (JRE), and others. The malware distributed by the Blacole exploit pack included applications for stealing online banking credentials. (Portal, 2012) In the Blacole exploit pack, the vulnerabilities targeted were all comprised of weaknesses which had patches released by the vendor to fix the issue, but the patches were not applied by the end user. The mere lack of patching was the root cause. These types of attacks are widespread and very prevalent in the

Windows computing ecosystem.

### 1.2.2. Zero day vulnerabilities

The second manner in which attacks are made is more worrisome. There can be a period of time between when a vulnerability is discovered and when a patch for that issue is written. This "zero day vulnerability" as it is commonly called, is often used in more sophisticated attacks. Typically this is less often used in financial fraud against small businesses and aimed more towards gaining access to credentials key to the assets of the firm such as source code of a software company, intellectual property, or key security assets that bring risk to the entire company. In early 2013, the Java platform was used in several targeted zero day attacks (The Business Journals, 2013).

## 1.3. Risk to the Small Business

While computer attacks are a threat to any size business, financial attacks to a small business can be catastrophic. Studies have shown that 43 percent of small businesses impacted by a natural disaster wiping out their property, can severely damage the company to the point of eventually causing bankruptcy and failure (United States, 2007). Financial disasters where the attacker fraudulently transfers significant amounts of funds from a small business bank account can have a similar impact. A small business typically has fewer resources than a large entity to recover from a fraudulent event. Generally they do not have the ability to obtain resources from outside investors in order to stay in business. Small businesses also tend to leave excess funds in a business bank account and do not distribute them to owners until the end of the company's financial year making funds more available for fraud.

### 1.3.1. Lack of FDIC Insurance

To many the most surprising discovery after a fraudulent bank transfer is the lack of indemnification of the banking institution. In the United States of America there are several entities charged with providing the banking and credit union industry with assurances to foster the trust of the users of the bank into depositing funds with the bank. The Federal Deposit Insurance Corporation (FDIC) is the specific entity that many users of banks are familiar with.

This agency ensures that when a customer deposits funds into a bank they can be assured that the funds will be returned to the customer in the case of a default or insolvency by the banking institution. In the case of the fraudulent transactions due to insecure online banking practices, the bank is not insolvent. For business bank accounts in particular, the FDIC provides no remedy against a successful attack on a business bank account.

### 1.3.2. Lack of Legal Precedent

An impacted customer can investigate if it is possible to take legal action against the attackers or perpetrators and the receiving bank that took control of the funds. They can also consider suing the banking institution that transferred the funds. Due to many of these fraudulent transactions involving overseas banking institutions, offshore accounts and other locations, the impacted customer likely will end up in a costly legal battles. There is little precedent that supports suing the bank will provide a remedy. Many of the recent court cases regarding the loss of banking funds have put the burden of proving the cause of the fraud back on the banking customer. Only recently have there been some private settlements that appear to be placing more burden back on the banking institution for security and assurance of the transaction. In the case of Patco Construction versus People's United Bank, the Bank failed to alert the customer that high risk bank transfers had taken place. The Judge in the First Circuit Court of Appeals ruled that the Bank's security system was not commercially reasonable and thus advised the parties to come to a settlement (Zetter, 2012). But just when it appeared that there was precedent being set in the Patco case, a more recent case involving a Missouri Escrow company who sued to recover funds stolen in a 2009 cyber heist placed the burden back on the company. The company failed to follow a security procedure recommended by the bank: requiring two employees to sign off on transfers. (Krebs, Missouri Court Rules Against $440,000 Cyberheist Victim, 2013)

## 1.4. Banking institutions and their actions

Banking institutions do not provide public information about suspicious activities that occur in their computer systems. There is no mandate to release to the public information technology audits and reviews performed on the bank or credit union. Some banks have recently begun to recommend additional software that protects the system from malware and screen

scrapers such as the software from Trusteer Rapport (Wikipedia, 2012), but not all banks and credit unions are proactive. The Trusteer software program is also not without concerns as it has been identified as causing issues on workstations resulting in disruptive behavior such as the machine abruptly shuts down in a process typically called a "blue screen of death". Some banks and credit unions are adding security techniques such as multi factor authentication that involves verifying a visual icon as part of the logon process. Some ensure that the customer is only logging in from computers previously used to access the banking system. This process is enforced by requiring additional verification from an email or code sent to a text messaging system. Some require pass phrases and require that the customer change the online password or passphrase periodically. But typically none of these banking institutions provide any additional advice to those that use their systems nor do they demand that their customers use multi-factor protection. None require that additional manual verification procedures – such as phone or fax authorizations as being mandatory.

### 1.5 User lack of awareness

If a person handed money to a trusted individual and that trusted individual handed those monies to someone else without properly vetting and confirming the person they were giving the funds to was trustworthy, it would be reasonable to hold that trusted individual at fault. In the United States, business bank accounts are not protected should a fraudulent transfer occur. The burden is on the customer, not on the bank, to replace those funds. Many business banking customers do not realize that banks do not insure them when fraudulent transfers occur. There is a general lack of awareness that Federal Deposit Insurance Corporation (FDIC) which is designed to ensure that banks remain solvent and viable and that customers do not lose funds should the bank become insolvent, does not also cover these fraudulent activities. The documentation that the customer signs when opening a bank account typically does inform them of this lack of coverage, but as with many documents, it is overlooked and not understood.

#### 1.5.1. Actions by the bank to inform

In a random review of business banking web sites, nowhere was this lack of FDIC coverage for fraudulent activities stated on their web sites. Many businesses have opened up bank accounts years before online access was prevalent. The language stating the lack of

coverage is buried in a lengthy document and overlooked. When a business is applying for online access the risk of remote access is not stated, yet the benefits are touted. Convenience and mobility are stressed with little about the potential of risk. There is rarely a detailed discussion of the risks of online banking and the lack of recourse should something occur. Instead, bank customers are charged more for paper transactions and penalizing those that want to opt out of using online banking.

### 1.5.2. Actions by the media

In the security journalism community, there is an increasing chorus of voices being raised to alert users over online business banking risks. One such journalist is former Washington Post computer investigative journalist, Brian Krebs. In numerous stories on his site (Krebs, Cyberheists 'A helluva wakeup call', 2012), he points out that attacks typically showcase weaknesses on the part of the business in the form of security flaws being exploited. He also notes, however, that the banking and credit union institutions fail to see red flags of fraudulent activity.

While Mr. Krebs' fraud warnings are well known in the security community, they are less well known by the general population of small businesses. This lack of information leads the typical small business banking user to not have the much needed information in order to make proper analysis of the risk of their computer machine or mobile device to such online banking frauds. The traditional technology media only covers widespread security issues and does not cover issues that target smaller segments of businesses. Most small business bank and credit union customers are unaware of the risks of online banking and only see the advantages of information and speed of transactions that it provides. They are not provided sufficient information to allow for an appropriate risk assessment.

## 2. Banking site security

In reviewing typical bank and credit union sites, there is an emphasis on the selection of a password, but nowhere does the site stress the underlying security of the computer machine or mobile device that is being used to access the banking site. No Bank or Credit Union web site checks the system for an up to date browser, no site checks for updated plug-ins for Java and

Flash, and some sites even require the use of an older Java platform in order to perform the actions needed for banking.

### 2.1. What each banking web site requires

There is no one standard for what a bank or credit union website will use to provide an online banking experience. Some websites require that Java software be installed in order to provide the full online experience. Other websites may indicate that an add-on is required, but if the customer ignores the warnings for the needed software, the customer can click through the warning and proceed. When a website does list minimum requirements needed to access the site, it can point to a web browser that is no longer updated or supported by the manufacturer. When a site does list minimum requirements, they often showcase that the website needs a browser that was released several years ago and is no longer supported by the manufacturer of the browser software. The Bank of America web site, for example, lists minimum requirements such as Windows 98, NT, 2000, ME as well as Firefox 3 and Chrome 3.0 even though none of these platforms are actively supported by Microsoft, Mozilla or Google in 2013. (Bank of America, 2013)

#### 2.1.1. Java

When a banking website requires Java, it is wise to check what the exact version of Java that is being specified. As of May of 2013, the current released version of Java is Version 7 Update 17 (Oracle, 2013). As announced in April of 2013, Java has slowed down the release of Java 8 to put special emphasis on building a better, more secure version. (Reinhold, 2013) An online banking customer should put special emphasis on keeping Java on the most currently released version in order to be secure. Some banking sites require versions less than the most recent Java to be used on their sites. The user then has to decide between keeping a system up to date or choosing to install an older Java version in order to complete the online banking process. When selecting an online banking process, it is wise to pick a banking institution that does not even require Java on their online banking site or one that recommends the latest versions of Java. Banking web sites that recommend a minimum Java of 1.6.02 may not have appropriate secure coding practices in place. (StarOne Credit Union, 2012) Java 1.6.0.2 has not been secure since

2011 (Freitag, 2011). Java has been used in many online browser attacks and it one of the most exploited third party software products used in a browser setting (Hoffman, 2012). Java is not supported on the iOS mobile phone and iPad platform and thus is primarily a Windows exploit platform. Java exploits were used in 50% of online attacks in 2012 (Kaspersky, 2012).

### 2.1.2. Flash

Bank and Credit Union websites can also require the use of Adobe Flash in their entry portals. Typically the use of Adobe Flash is used for advertising information to the online banking user and not necessarily used in the actual application of the web site. But the user of the site may believe that Adobe Flash is required due to the error message that occurs if one does not have flash installed. The Flash platform is one that also has a myriad of security issues and has been patched many times in 2012. (CVEDetails, 2012)

### 2.1.3. Other software

Banking websites often will list minimum requirements for use of its site which include very old unsupported operating systems and older browsers. The website may even use Microsoft's proprietary ActiveX technology and recommend disabling popup blockers. (StarOne Credit Union, 2012)

Banking sites may also indicate that they need additional third party software as one enters the online banking experience. However many times the requirement is merely for the entry portal and not needed for the actual use of the site. Some applications that use connectivity to online banking information are built on platforms that do not lend themselves well to patching and other operating system maintenance. The small business accounting application QuickBooks is based on various versions of .NET (depending on the year of the QuickBooks in use). .NET, a development platform produced by Microsoft, has historically had issues with updating without error causing the user of the computer to totally uninstall .NET and then requiring a full reinstall of the .NET platform. This leads some software users to ignore security updates needed for .NET.

## 2.2. Vulnerabilities in the required software

Online banking requires the use of Internet browsers. These platforms are prone to attack. They have been subject numerous times to vulnerabilities for which there is not yet an update released to protect the system. The state of the industry of online banking is such that the three major Internet browsers, Internet Explorer, Chrome and Firefox must all be supported on the online site. Mobile banking requires that the applications support Windows, Android and iOS platforms.

### 2.2.1. Internet Explorer

Internet Explorer ships by default on all versions of Windows operating systems. As of December 2012, the supported versions of Internet Explorer include Internet Explorer 6, 7, 8, 9 and 10. Internet Explorer 6 as reported by Secunia Advisors has had 40% of its vulnerabilities result in system access to the entire machine. (Secunia, Browser vulnerability statistics , 2012) Later Internet Explorer versions do not fare much better, Internet Explorer 9 has had 53% of its vulnerabilities result in system access of the entire machine. (Secunia, Browser vulnerability statistics , 2012)

### 2.2.2. Chrome

While Chrome is not always a required browser used in online banking, it is a supported one. It is not, however, without security issues as well; albeit with lesser numbers of vulnerabilities. Chrome 23 has had one vulnerability resulting in access of the entire machine as noted by Secunia. (Secunia, Browser vulnerability statistics , 2012) Chrome's advantage as a browsing platform is that it will self-update and thus will have the latest version installed on the platform.

### 2.2.3. Firefox

Firefox's insecurities come from both the browser itself as well as the plug-ins that can be added to the browsing platform. These plug-ins may not be updated as regularly as the browser itself and can lead to the platform being insecure. Firefox does, however, have some plug-ins that add security settings such as blocking scripts, flash, and other additional security settings in the browser. (Mozilla, 2012) These can enhance the security of the Firefox browser.

### 2.2.4. Java

Java is used in many business applications and required on many online banking websites. Java provides the user with the ability to additionally manipulate data and sync information into other applications. Due to the widespread use of Java, when there is a vulnerability in the platform it can make over a billion devices vulnerable (Schwartz, 2012).

### 2.2.5. Flash

Adobe Flash 11.0 as of December 2012 had 8% of the reported vulnerabilities unpatched. Of the reported vulnerabilities, 100% of them provide a remote attack vector directly to the computer. (Secunia, Vulnerability Report: Adobe Flash Player 11.x, 2013) While typically Flash is not used on a banking web site directly, it is most often seen on the entrance to the site where banner ads for the bank are used to advertise additional services that the bank provides.

### 2.2.6. Other software

Other third party applications use application platform interfaces (APIs) to connect to the bank and import data into the application. The small business accounting platform called QuickBooks, has a vibrant third party developer ecosystem that allows developers to build solutions that hook into it. These third party applications may introduce security issues to the platform. Cross site scripting, SQL and XML injection vulnerabilities may be inadvertently added to the platform through the use of these third party vendor applications. (Intuit, 2012)

## 2.3. Additional software required by the banks

Banking institutions can also add the requirement of additional software such as ActiveX controls to their software (Eascorp). ActiveX is a proprietary Microsoft framework that is used to develop for Internet Explorer. Banking institutions typically rely on vendors to provide them with web sites, mobile applications, and other ease of use platforms. These vendors can use any number of software platforms and frameworks thus introducing a near infinite number of software platforms to review for security coding. Unfortunately for consumers of banking technology it is nearly impossible to perform a security coding review of all the applications one uses to access a bank.

## 2.4. Mobile banking

The current trend of online banking is to move more and more towards mobile banking and mobile payments. The largest vendor that supports a mobile payment network at this time is Starbucks. IPhones, combined with a tiny plastic device that plugs into the audio connector of the phone, now doubles as a mobile credit card processor. It is additionally rumored, that in the future, a credit card will not have to be removed from a purse or pocket in order to complete a purchase transaction. The store will use GPS to sense the payment device proximity and the transaction will be approved merely by talking to the Barista (Netburn, 2012).

### 2.4.1. Future fraud trends

Society is moving away from where a physical paper trail of the transactions was norm, to the current state of affairs where nearly all transactions are going digital. This process is leading to the potential of more fraudulent activity that was not anticipated when current authentication and verification techniques were put in place. A mere password is no longer sufficient to confirm and verify a financial transaction. Current trends are to inject or install malware on personal computers to obtain the credentials of the online banking account. Already there is malware on the Android platform that will enter via an app and will use the SMS feature to earn money for the attacker. (Chen, 2012)

### 2.4.2. Mobile bank deposits

Many Banks and Credit Unions are adding to their online banking platform a service that allows the user to take photographs of the check to be deposited and then deposit it to the bank. This transaction is performed without having to visit a bank or ATM terminal. These enhancements do not come without risk to the banking institution of fraudulent transactions. Banks currently manage the risk by placing a limit which can range anywhere from $5,000 to $25,000 (depending on the institution) on the amount of funds that can be deposited using these mobile banking applications. (Zhen, 2012)

### 2.4.3. Mobile malware rise

Banks and Credit Unions see mobile platforms as a way to increase customer satisfaction and retain customers. (Adams, 2013) Attackers are seeing the rise in the use of mobile platforms and are beginning to write more malware to attack this platform. Predictions are that 2013 will

see a rise in malware attacking users of mobile platforms. The Android platform in particular is seen as an increasing target. (Singh, 2012)

## 3. Potential solutions

As with any technology, the best solution to security risk is to determine a course of action that balances the requirements and the use of technology with the needs of the users. One cannot, nor should one ban users from using technology. One should strive to find the proper balance of risk of technology with protection techniques. At no time can the risks to online banking be completely removed. The exposure to risk, however, can be minimized.

### 3.1. Linux boot disk

The first recommended solution is to use an alternative operating system in a temporary bootable condition. This ensures that attackers are unable to intercept the credentials as the platform does not allow malware to be written to the platform. As recommended by Brian Krebs on his blog (Krebs, KrebsonSecurity, 2012), a Linux boot disk allows one to boot a Windows personal computer into a hardened platform. Typical attacks use the Windows operating system as the target. Using an alternative operating system places the online banking process in a less attacked platform.

The use of an alternative platform is not without issues. The download of the bootable disk must be from a reputable location. It is imperative that the content of the download is confirmed as being unchanged from when the software build was placed on the download server. On manner of determining this is to compute a value of the cryptographic integrity of the file. This computed value called SHA1 stands for Secure Hash Algorithm (Wikipedia.org, Definition of Sha-1, 2013). Upon downloading the files, the computed SHA1 value of the downloaded file should be compared with the published SHA1 from the download site. One such hash value calculator is from Slavasoft. (Slavasoft, 2013)

It should not be assumed, however, that this method is without risk. In a review of various precompiled Linux boot disks, some were not up to date with the latest versions of the browser used in the platform. In addition, using this method does not allow for interaction with various accounting software programs. A boot disk is unable to have any accounting software

installed into the volatile platform. Furthermore, many banking institutions require that a cookie file is written to the machine to record the fact that the computer is a trusted machine. Live boot disks cannot write this cookie file. The virtual machine would be seen as "untrusted" and must be authenticated each time a system is used. Many business users would find this experience unacceptable.

### 3.2. Specific tools for the Windows Platform

The Windows platform with its APIs is a platform that is used to build solutions on. It is also one the attackers build various exploit kits designed to gather passwords from the Windows platform. One such attack platform is the Blackole Exploit kit (Wikipedia.org, Definition of Blackhole Exploit Kit, 2013). These kits allow attackers to easily code and prepare attacks on the Windows platform that look for passwords and other authentication means. It typically targets Internet Explorer but has been used in attacks against Firefox and Chrome. Of all of the browsers in current use on the Windows platform, it is less likely to impact users of the Chrome browser (Larsen, 2012).

#### 3.2.1. Browser selection

On the Windows platform, one of the easiest ways to reduce attacks is to install an alternative browser. For users of Google's Chrome browser, the platform is designed to auto update even without administrative credentials on the system through the installation inside of the user's profile. That this browser takes the update decision out of the hands of the end user generally results in a more secure browsing experience.

#### 3.2.2. Restricting the use of Java and Flash

Many of the most successful online banking attacks include targeted attacks against vulnerable versions of Java and Flash. Therefore removing or restricting the use of Java and Flash on the system used for online banking can increase the security of the system. Since the introduction of Java 7 version 10, an additional security panel in Figure 1 shown on the following page, has been introduced to allow the end user to remove Java from the browser but still keep it on the workstation if there is a need for desktop based Java. It is suggestion to

remove both Java and Flash and then determine if normal business operations are unharmed by its removal.

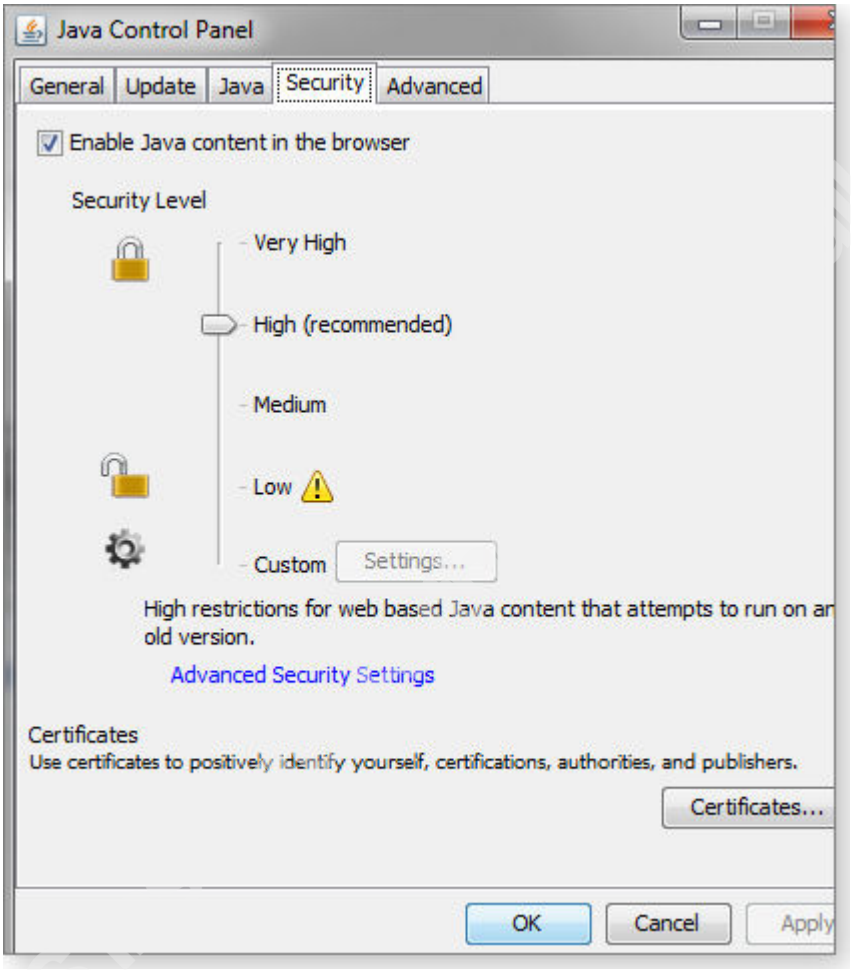


Figure 1 - Uncheck enable java content in the browser to protect the system

### 3.2.3. Non-administrator

On the Windows platform, the default setup makes the first user of the operating system an administrator. This default has historically made the platform easy to install and use, but notoriously a target for easy to write malware. With the release of Windows 7 and User Account Control (UAC), a push has been made to convince users and developers to move to the use of a non-administrative account for normal day-to-day use of the machine. In the case of Windows 7, it is strongly recommended to move to the use of a non-administrative account to use on a regular basis and restrict the use of an administrative account only when needing to install software. Specific instructions to set up a Windows 7 machine to use a non-administrative

account can be found on the Unixwiz Techtips page. (Friedl, 2013) It is highly recommended to set up two accounts on any Windows desktop. One will be the Administrator account that you use for installing software, the other will be a restricted user account for day to day use of the system as shown in Figure 2, below.

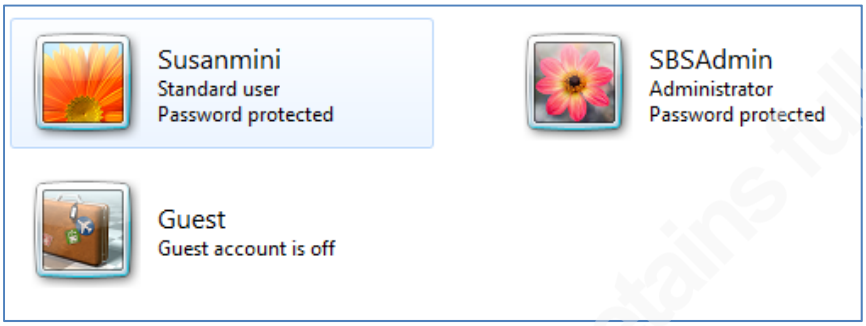


Figure 2 - Always set up multiple user accounts on the Windows platform

If using older software not specifically built for non-administrative use, an installer can use shims or adjust permissions in the registry and in the operating system to continue to use these older programs. Windows 7 natively includes many of these shims with its application compatibility techniques such as "Run as administrator" and "Run as XP" which can be selected from the Compatibility tab in Windows 7, shown in Figure 3 in the Compatibility tab properties on Microsoft Windows 7.

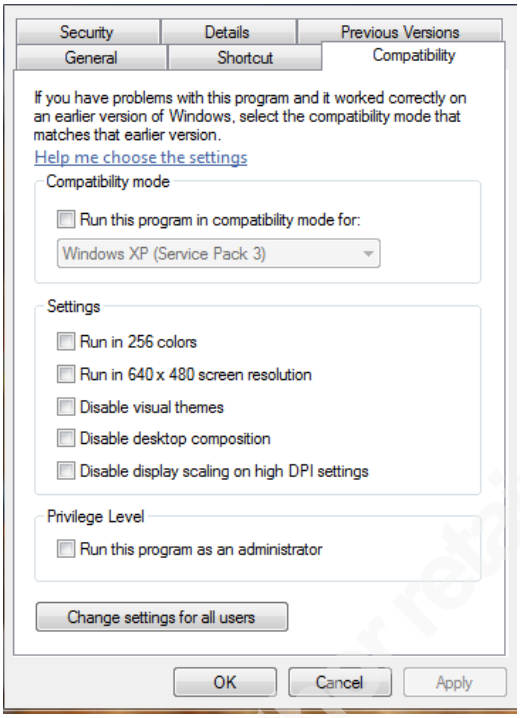


Figure 3 - Compatibility tab properties on Microsoft Windows 7

If additional adjustments are found to be necessary they can be determined using a tool from Microsoft called "LuaBugLight". This tool, downloadable from Aaron Margosis' blog (Margosis, 2013), can identify those places in the operating system where the older application needs to have adjustments made.

### 3.2.4. Installing EMET

The Windows platform has been subject to a number of attacks for which there is yet no current patch available to protect the system (zero-day). Recently a new tool has been released which has been shown to reduce these threats and protect the system from these so called zero-day attacks. This tool, called EMET or Enhanced Mitigation Evaluation Toolkit, provides a number of mitigation techniques that are designed to make it more difficult for an attacker to exploit vulnerabilities. Targeted at IT professionals, Microsoft's recently released EMET 4 is designed to reduce vulnerabilities in Internet Explorer and older applications. The current version of EMET is available from the Microsoft download site located at http://www.microsoft.com/en-us/download/details.aspx?id=38761. It was released in June of 2013. To install the tool on a Windows machine running Windows 8, Windows 7, Vista or Windows XP, .NET 2.0 will need to be installed.

EMET is unusual in that it does not require changing application code to make it work. With other security technologies, such as Data Execution Prevention (DEP), developers must recompile their apps to add support for the enhanced protection. EMET works with existing code, making it ideal for protecting legacy software. It also adds additional SSL protections to ensure that sensitive authentication websites are not spoofed with "man-in-the-middle" attacks.

The only drawback to EMET 4 is that it requires .NET 2.0. This is not a problem for Windows 7 operating systems, but when running Windows XP, .Net 2.0 will need to be installed— and then maintained via future patches.

It has been hinted that EMET will be included in future versions of Windows. Current versions of Windows 8, Windows 7 and Vista include many of EMET's security features, such as Structured Exception Handling Overwrite Protection (SEHOP) and Address Space Layout Randomization (ASLR), which is turned on by default. XP does not support SEHOP or ASLR, but EMET will add these additional security features for applications running on XP. To add EMET protection, obtain EMET from the download site and install it on a system; then launch the app.

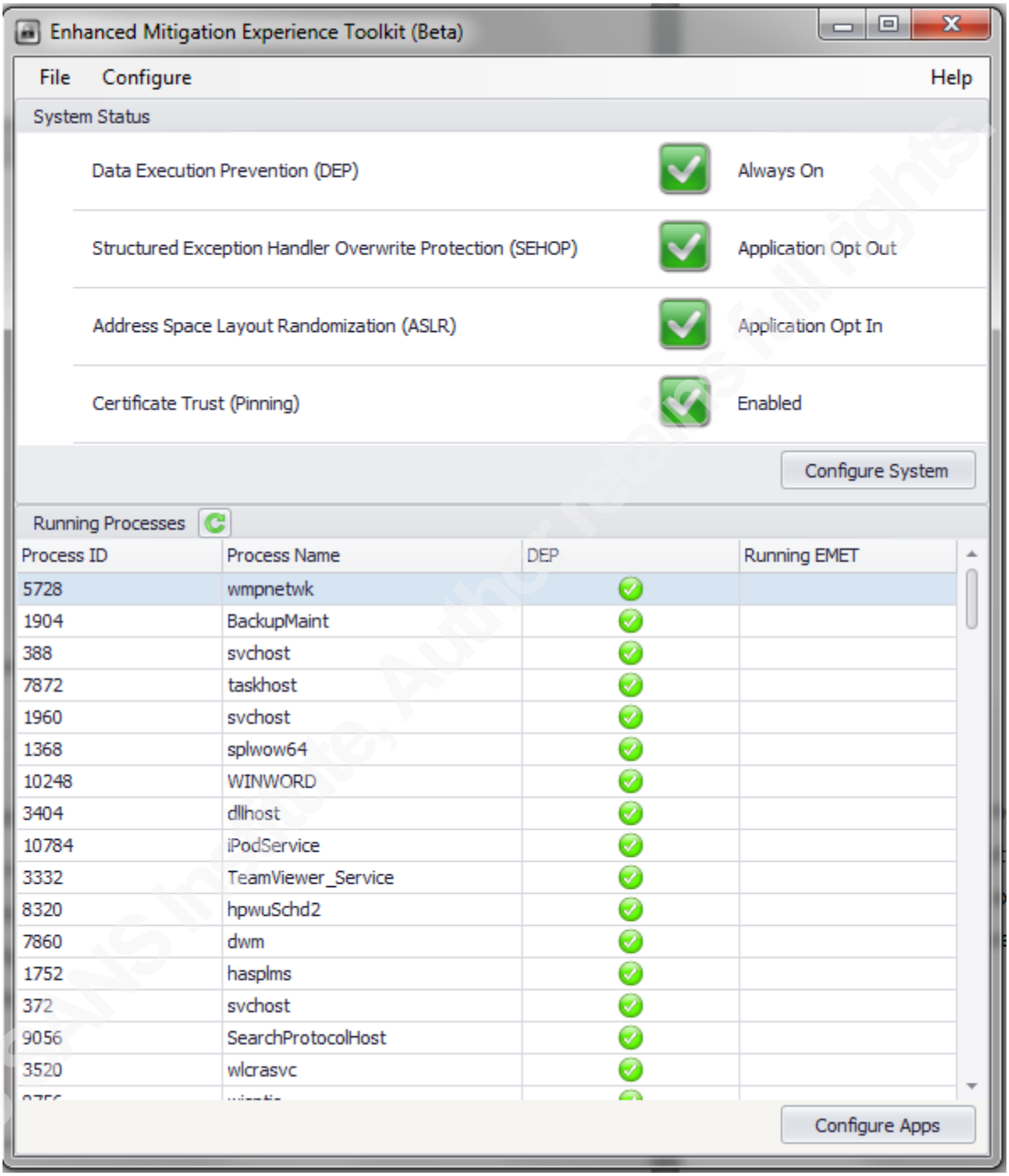


Figure 4- Reviewing EMET's default settings

The default settings, as shown in Figure 4, include protection for many processes. By default in EMET 4, Internet Explorer and Office platforms have been set to be protected. To protect any additional applications with all of EMET's security capabilities, start by clicking the Configure

Apps button at the bottom of EMET's interface. In the Application Configuration window, click Add and then browse to the application's **.exe** file (for example, c:\Program Files(x86)\Mozilla Firefox\firefox.exe). Next, check that all EMET options are selected as in Figure 5. Finally, click OK, close and re-launch Firefox and EMET. Any application that you add to the configuration will not have SEHOP enabled by default as this may cause compatibility issues. Adding SEHOP protection should be tested before implementing on multiple computers.

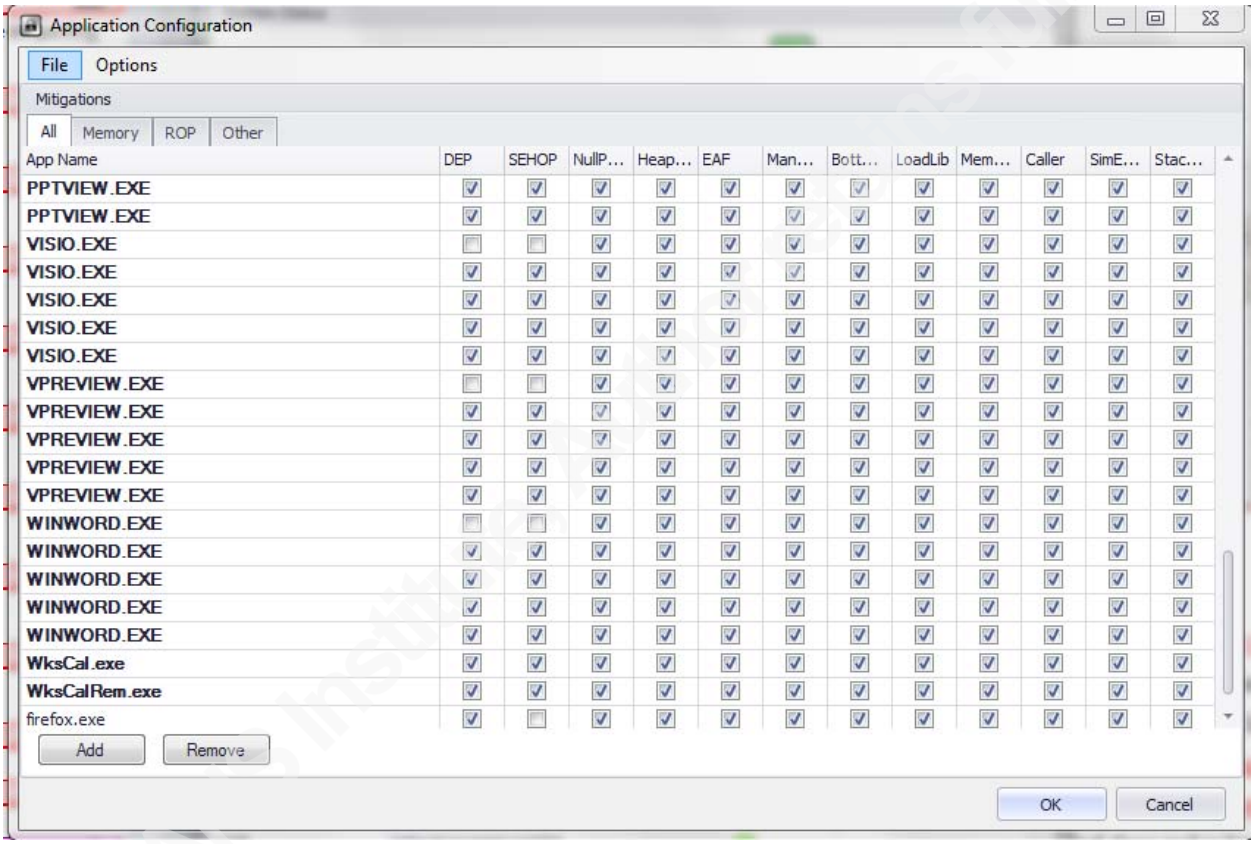


Figure 5 - Opting Internet Explorer into EMET's protection

Although Windows XP users will have less protection and fewer options with EMET, it can still help protect applications such as Internet Explorer and Adobe Acrobat from zero-day attacks. For Windows XP, don't opt for system-wide protection as the system may become instable; just start with vulnerable applications such as Internet Explorer.


Figure 6 - Reviewing EMET effect on Internet Explorer

Once EMET is installed it can be seen in action by opening up the EMET interface and reviewing those applications that are running Data Execution Protection (DEP) (as shown in Figure 6) and also those applications that have been chosen to have additional EMET protection such as Internet Explorer. EMET also includes additional protection for SSL certificates as shown in Figure 7, and Certificate pinning allows for the selection of those root certificates to have Internet Explorer check for trust. Certificate pinning was first introduced in Chrome and is now making its way to Internet Explorer in this release of EMET 4.

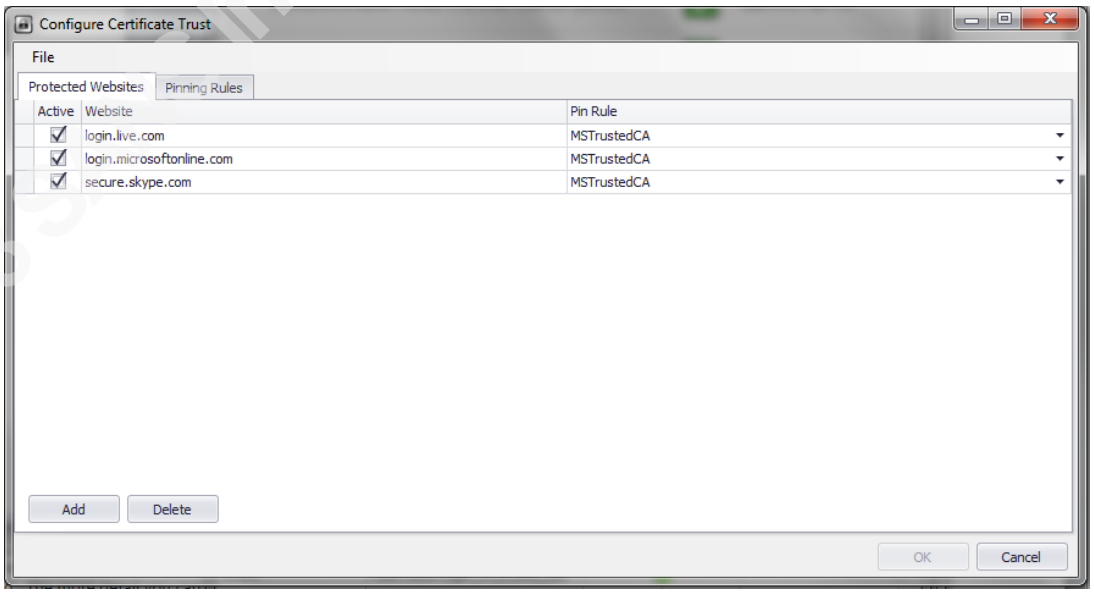


Figure 7 - Default certificate pinning

### 3.2.5. AppLocker

AppLocker is Microsoft's answer to application whitelisting. As noted on their frequently asked question page (Microsoft, 2013), "AppLocker is a feature in Windows Server 2012, Windows Server 2008 R2, Windows 8, and Windows 7 that advances the functionality of the Software Restriction Policies feature. AppLocker contains new capabilities and extensions that reduce administrative overhead and help administrators control how users can access and use files, such as executable files, scripts, Windows Installer files, and DLLs." The disadvantage to AppLocker is that it is restricted to only certain versions of the operating system. For Windows 7 it is only supported on Windows 7 Ultimate and Enterprise. For Windows 8 it is restricted to only being deployable on the Enterprise version that requires a volume license in order to purchase. For typical small businesses that buy retail and off the shelf versions of the Windows operating system which may include the Home editions, AppLocker, while being a promising security solution, is not feasible for the vast majority of small businesses. For those firms that do purchase it, it provides the ability to set up policies to only allow specific applications or files to be run. In a highly sensitive use workstation, it may be a solution to consider providing additional protection for these sensitive environments.

### 3.2.6. Use of alternative browsers

Many attacks come through browser exploits; thus it is wise to have multiple browsers on the system. If multiple browsers are installed, make sure that they are kept up to date. Chrome will update within the user mode that it is installed in, whereas Firefox will need administrative rights and may prompt for updates. Firefox has an add-on model that allows the user toolbars to assist in keeping the browsing experience more secure. One such tool is NoScript (Maone, 2013) that restricts the use of Java and scripts to only those needing Java to run. If older versions of Java are required, check to see if the Firefox browser can be used and restricted to just those web sites that need the older platforms. There are many times an upgrade to newer versions of Java is not an option. In this case investigation of other options will be required. The website Incidents.org recently pointed out alternative options (VandenBrink, 2013) including using user-agent strings to enforce and block the use of older versions of Java for casual Internet use but still allowing it to be used for certain business web sites. If the firewall that is used by the

business is sophisticated enough to handle web filtering using user agent strings, settings may need to be investigated as an option to better protect your systems.

### 3.2.7. Choice of operating systems

When an operating system is designed, it is built for the security issues and threats of the day and era in which it was written. Security cannot be easily bolted on afterwards, nor can future exploits be predicted. Microsoft's most successful operating system to date is Windows XP. This operating system was released in 2002. However, successful doesn't mean that it is the best platform for use in a secure machine. Windows XP is not easily used in a non-administrator setup. To install applications requires a log out of the user mode and then a log into the Administrator mode. Windows 7 on the other hand, introduced User Account Control allowing the computer user to provide administrative credentials while one remains in the user mode. Thus for a more secure system where it can much more easily maintained, computer machines can be run without administrative rights, Windows 7 is the much better choice of operating systems. Windows 8, the newest Microsoft based platform has additional security protections and sandboxing techniques (Henry, 2013) to ensure that it is even more secure than Windows 7.

### 3.2.8. Actions of the end user

The security of a machine is directly impacted by the actions of the user of the machine. How they use and interact with their system will determine ultimately how secure the machine is. If a workstation that has online banking access is also open to bit torrent download sites, is used to visit Facebook on a regular basis, and has a user that falls for any scam noted on the web, no matter what operating system in use, the workstation will be at risk to having the banking credentials attacked. Restrict online banking to machines where no one will be performing risky online activities. Computing devices are relatively inexpensive and additional computers that can be used for riskier activities should be purchased to remove the risk of the user actions impacting the online banking experience. In the case of online banking, dedicating a workstation to perform sensitive transactions should be a top priority.

### 3.2.9. Interaction with accounting software

Many accounting applications aid in the ease of bookkeeping by accessing online banking and downloading transactions and reconciling activities. When choosing the machine to perform banking activities, ensure that the interactions with the accounting software are fully understood and what third party software is being relied upon. If the banking applications do not need Flash or Java, remove it from the machine. One accounting vendor in particular will install an outdated version of Flash in its installer for use in training videos, but the application itself does not need Flash in order to work (Intuit, 2013). Don't assume that because the application installs either Java or Flash, that it is necessarily dependent on it to successfully operate. Test your banking computer machine to determine the minimum software it can use and still get the job done securely.

### 3.2.10. End user training

Many online banking scams can be traced back to phishing emails sent to unsuspecting users. Ensure anyone involved in the banking operation of the firm is aware of phishing attacks and how to review an email before clicking on the links it contains. Add a mail hygiene and junk mail filter service if the business Internet Service Provider (ISP) does not already include this service. Resources available to stay up to date on the latest scams, phishing attacks and other social engineering attacks include the SANS newsletter, Ouch (SANS.org, 2013) which focuses on the end user training aspect of security. This newsletter informs computer users of the latest attacks and issues that they may face when using their computer and opening up email.

### 3.2.11. Additional software

Some banks are now offering additional software to counter the use of key loggers and other online attacks. One such software is Trusteer Rapport and is offered by several banks as additional protection to computer machines. Another is DataMask provided to America Online members (AOL.com, 2013). Both software offerings advertise that they encrypt the keystrokes between the user's browser and the sensitive banking site as well as blocking screen capture events, browser add on events, cookie access and other items it deems suspicious while on the sensitive web site.

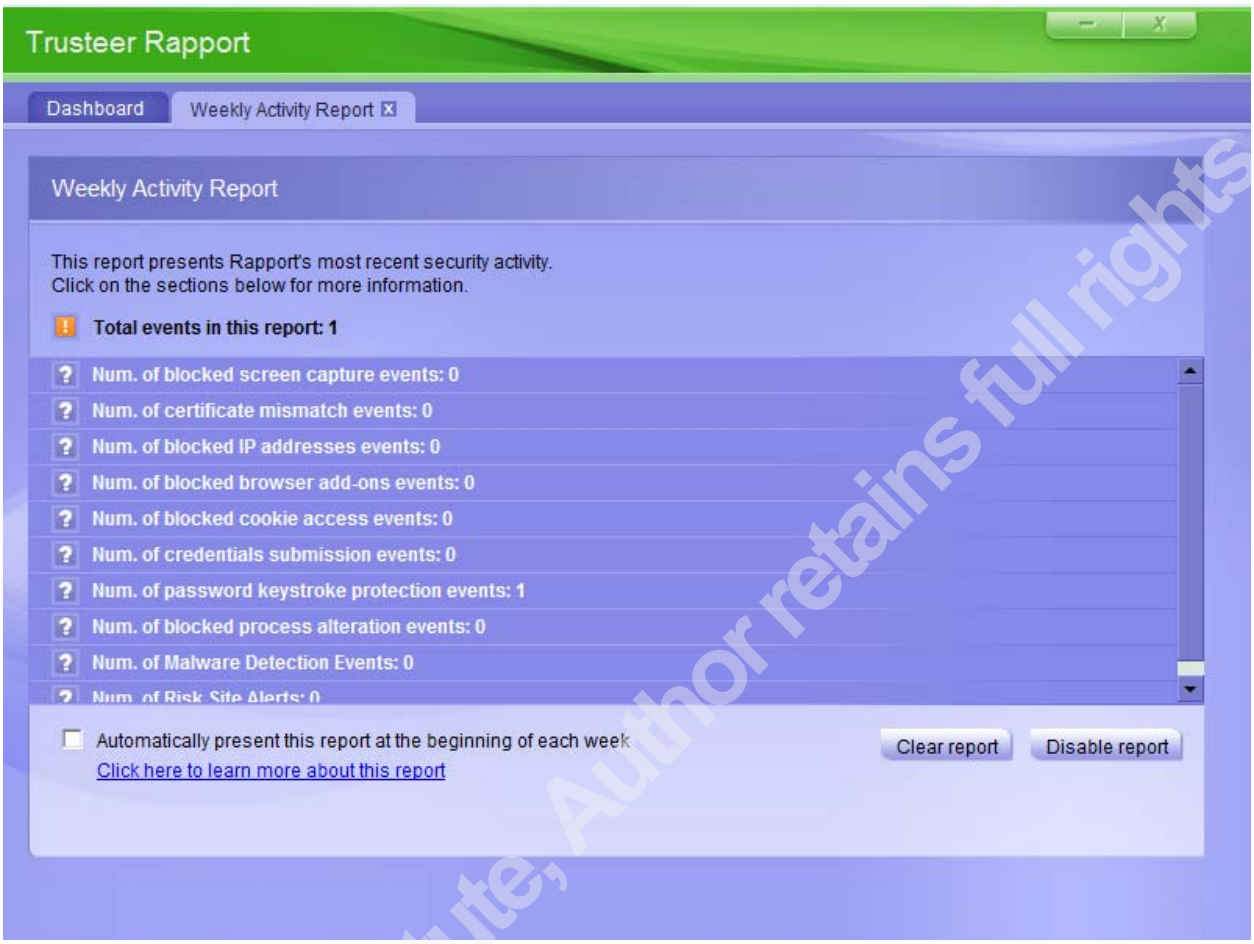


Figure 8 - Trusteer Rapport weekly activity report

Some banks also take the precaution of requiring additional verification of a device or computer that has never been to the website before. Typically the authentication is in the form of a verification code sent to a cell phone or an email address.

### 3. 3. Apple platform

The Apple platform is being used more and more in online banking. From the OSX desktop operating system to the widely used iPhone platform, the Apple platform is being used in day to day online commerce. Additional hardware has been developed to even turn the iPhone and iPad devices into various point of sale systems, credit card readers and bank deposit ATM replacement devices.

### 3.3.1. Security of the operating system platform

The Apple platform is not without flaws. On a regular basis the platform is one of the first to be attacked and taken over in various security contests that have engineers compete to take over a device. (Wikipedia.org, Definition of Pwn2own contest, 2013) The Macintosh browser, Safari, in particular has been attacked in various security contests and has been shown to be lacking in protections. However, its lack of significant market share (to date) as well as a lack of financial targets, since it supports fewer accounting software platforms, leads to its position as a more secure platform, if only by obscurity.

### 3.3.2. Browser choice

As is the case with the Windows platform, the use of an alternative browser choice can lead to a more secure browsing position. The same major supported browsers on the Windows platform are also available on the Apple platform. Google's Chrome and Mozilla's Firefox can optionally be the default browsers on the Apple platform as well.

### 3.3.3. Interaction with accounting software programs

While the Apple platform is maturing as an operating system, it is still lagging behind Windows as the choice and solution for accounting applications. Rather than the sometimes overwhelming plethora of solutions on the Windows platform, there are much fewer choices on the Macintosh desktop. Online there are an increasing number of operating system and browser agnostic solutions that are becoming more full featured and mature. The small business customer may need to investigate the available solutions before moving to the Macintosh platform.

### 3.3.4. Additional security software

Third party banking security software such as Trusteer's Rapport software has Macintosh versions that protect that platform. These types of third party software tools attempt to protect banking interactions from key loggers and other malware attacks.

### 3.3.5. Additional security settings

When moving to the Macintosh platform the worst thing one can do is to listen to the often touted benefit that Macintosh machines are not subject to malware. The reality is that the Macintosh operating system is flawed just like any man-made written computer code. It too is subject to security issues, and it's users can be defeated by social engineering tricks, scams and phishing attacks. A Macintosh system should not be run without antimalware and antispyware software installed and appropriate end user education about secure browsing and computing habits.

### 3.3.6. Choosing and changing passwords

One of the steps that most users refuse to engage in is selecting a good, strong password and then changing it on a regular basis. In addition, ensuring not to reuse the same password on multiple sites and locations will ensure that an attacker cannot gain access to multiple financial institutions by merely cracking or guessing one single password. It is best to use a pass phrase, not a password, and to be prepared to change the password on a sensitive financial account that is accessed on a regular basis. Some scientists and researchers have theorized that we can only manage a range of 5 to 9 characters at a time (Johansson, 2004) and complex passwords are difficult to manage and remember, thus causing users to choose smaller and simpler passwords as well as reusing them on multiple sites .

## 3.4. Linux platform

The Linux platform, due to its smaller market share, its fewer choices of accounting applications, and as a result, financially less attractive of a target for malicious attackers, currently has a reputation as being more secure than its Windows and even Macintosh counterpart. In fact when performing sensitive online banking transactions, it is even recommended to use a Linux live boot cd if you can, to provide a sandbox operating system with which to access a sensitive site.

### 3.4.1. Security of the operating system

Lack of attacks should not be considered proof of an operating system's superior security stance. In the world of financial attacks, if the financial reward of targeting a specific platform is

not substantial, the attackers will, to use a trite term, "follow the money". Regardless of the platform, never relax system security and introduce risky online habits on a computing platform. Such risky habits include, but are not limited to, downloading pirated content from various un-trustworthy locations on the web, and following links without verifying their source and legitimacy. Phishing attacks many times lead to Google Apps spreadsheets that urge the end user to merely enter in their credentials; as a result, the attack surface of the operating system may be irrelevant in certain types of attacks. However, one should not deny the fact that currently the Linux platform is much less a victim than either the Windows or the Macintosh platform.

### 3.4.2. Browser choice

As was earlier noted, the choice of a browser may assist greatly in increasing the security of an operating system. On the Ubuntu platform, Firefox is preferred over Chrome (Ayesha.A., 2013) due to the browser's open source foundation, speed and add-in features. Both browsers, however, have an excellent track record as being secure on the Ubuntu platform.

### 3.4.3. Interaction with accounting software programs

The accounting industry has few options for small businesses to use accounting software on the Linux platform. Few business accounting packages support Ubuntu on the desktop. Many accounting platforms will support a Linux platform for the foundation of the database used to collate and collect the transactions, but on the desktop, many of these still require a Windows based workstation to be the data entry point. As the industry begins to move more of its applications to the cloud computing based model, more applications are expected to be supported on Linux desktops and devices.

### 3.4.4. Additional security software

At the present time, many third party banking software programs provide additional phishing and security on the Windows and Macintosh platform but are not supported on the Linux platform. As the Linux platform matures into a more frequently used desktop operating system, this fact may change. In addition, as Linux is now the foundation of many android

phone platforms, as the threats turn to the mobile computing platform, the need for third party banking risk mitigating software will also increase.

### 3.5. Mobile banking

Currently there is a vast shift happening in the banking industry. The traditional brick and mortar bank branch with the human bank manager and tellers is moving to a different business model. The nearest bank branch is now a mobile phone. With a trend that started with United Services Automobile Association's (USAA) online mobile depositing application, more and more consumers are depositing funds through applications on their mobile phones. Increasingly physical bank branches are shrinking and reducing their footprints as well. (Block, 2013) Credit Unions are also joining their Bank industry counterparts by providing the ability to deposit checks with mobile phone applications.

#### 3.5.1. Security of the operating system

As this time there are two major operating systems that power the majority of the mobile operating systems. These two platforms are Android, a Linux derivative provided by Google's Chrome, and iOS provided by Apple. Both vendors deliver a robust operating system that can be used as an effective mobile banking platform, as well as a platform that can be used in phishing and malware attacks. While both platforms are typically more closed to malware attacks, they are not completely without risk. Malware can enter the closed systems via the use of social engineering through provider's app stores. (Kingsley-Hughes, 2012)

#### 3.5.2. Browser choice and other risk factors

On the mobile platforms, browser choice is less of an issue than on traditional desktop machines. The mobile platform tends to be a more closed platform and more application based rather than browser based. That is not to say that it is immune to browser based malware and phishing attacks, but the banking platforms are developed as a restricted application and thus more task driven. What is more of a risk on the mobile platform is the use of the underlying transport. Cell phones use data plans to gain access to data and thus users prefer to attach their cell phones to freely available wireless access provided in various business locations; such as, coffee shops and other places that cater to the mobile consumer of content. These free Wi-Fi

locations are a risk factor for "man-in-the-middle" attacks, spoofing of Wi-Fi connections and other devices that can sniff and collect credentials. It is recommended that no sensitive banking transactions be performed on free Wi-Fi where there is no ability to confirm that the integrity of the connection to the trusted banking site exists. Care is required in situations where man-in-the-middle attacks could occur and access should be limited when connecting to an untrusted network.

### 3.5.3 Interaction with accounting software

Certain accounting software applications such as MINT and Quicken have apps that can reside on mobile phone platforms and integrate transactions into accounting software. Hardware can be attached to various mobile platforms to provide the user with the ability to scan and collect credit card transactions. The users of these applications need to be aware of the transmission platform they are using to transmit the sensitive data to the mobile processing partner. The use of an open wireless access point in a coffee shop is the least favorable means to transmit this sensitive data to the banking institution. Even if the transmission is slower, a user of these technologies should choose a transmission method which they have confidence in that there is little to no chance of spoofed wireless access points.

### 3.5.4. Additional security software

At the present time there is little to no additional security software built to provide additional assurances on the mobile platform. This may change in the future as the platform begins to be the preferred means to interact with a bank. These security precautions may not be needed for the applications themselves as the current model of mobile application software development requires that the software must go through an acceptance by the vendor. However, even after vendor review, malware has entered into these closed systems through erroneous acceptance of store applications. There is currently no means to review and audit the security of a wireless access point from a mobile device even if the device owner maintains control. In the future, banking vendors may provide such means or perhaps site-to-site VPN connections on the mobile platform.

## 3.6. Impact of accounting software selection to security

At the present time the bulk of small business accounting software is Windows based. There are agreed upon data transfer APIs between the banking industry, Windows software and various accounting applications. One such agreed upon standard is Open Financial Exchange (Wikipedia.org, Definition of OFX, 2013) agreed to between Microsoft and Intuit for their respective platforms. This allows individual banking customers to download the transactions from their bank account directly into an accounting application and allow for automatic reconciliation. Because the windows platform is used for more small business transactions, it is more often targeted by security threats. The convenience and efficiency of this process is so great that the alternative to moving to a non-Windows based platform, where these transactional efficiencies are not available has slowed down adoption of alternative software platforms. Most businesses will continue to engage in both online banking and accounting on the Windows platform or they will move to cloud based alternatives that are platform agnostic for the client side of the application.

### 3.6.1. Requirements for online banking

Banks and Credit Unions are embracing both the use of alternative platforms to provide banking as well as fully embracing the use of mobile platforms. As they support alternative platforms more fully, it will make it more difficult for the financial attacks to be as effective. Currently the attack arsenal need only include bundles of Windows malware to be effective. As the market share of personal computers machines decreases and the market share of portable devices increases, attackers will need to diversify their portfolios of attacks in order to infiltrate the same number of targets. This most definitely will be good news for the Windows desktop platform as the attackers ultimately will move to other larger pools of targets. It will be bad news, however, for users on alternative platforms that currently see it to be a means of protection in the online financial world.

## 4. Fraud review actions

Ultimately the best defense in thwarting attackers is to have a proactive stance in fraud review as well as to choose banking institutions that is similarly proactive. Small businesses consumers of banks and credit unions ultimately have a choice which banking institution will hold their funds. In addition to reviewing the offerings of preferred services, the best rate of

return, also review those institutions that provide the business with the best manner of protection.

### 4.1. Bank Selection

The small business should choose a Bank or a Credit Union that has a track record of being proactive against fraud. A financial services provider that is investing in technology would be a wise choice. Review the Bank or Credit Union's online statements and past history of actions they have taken when under attack. Enter a local bank branch and visually review the type and operating system on the computer machines they are using in the branch location. Unfortunately for Bank and Credit Union consumers, that the vast majority of details about security breaches occurring at a financial institution are not publicly disclosed. In addition, the industry itself is not always open about the issues it is facing and only discloses the issues when such information is leaked to the press. (Acohido, 2010) Ask the banking institution if they proactively review transactions for fraudulent flags. Choose a Bank or a Credit Union that indicates that they have software that looks for trends and flags unusual transactions. Having a Bank or a Credit Union place a temporary hold on a transaction will ultimately protect the businesses' assets.

### 4.2. Interview your Banker

As mobile banking becomes the norm, the old fashioned way of business banking is coming to an end. No longer will the branch manager stop a check that is not signed, nor call the business owner when the account is about to be overdrawn. The old fashioned way that was used to maintain the business banking relationship will be replaced by technology. Banking applications can be used to set up alerts about unusual transactions or when an account is below a set limit. Evaluate the features and options provided by the online banking applications and determine which online banking "manager" provides the small business with the most tools for managing the banking experience.

### 4.3. Review and reconcile accounts

Always review and reconcile financial accounts at least monthly. The bank reconciliation is an accounting process that compares the balances on the Bank Statement to the banking records of the firm. Outstanding checks and outstanding deposits are listed and used to

reconcile back to the balance the Bank or Credit Union has on their statements. Small businesses should perform this action more often on accounts with larger balances. Review transactions occurring in the account frequently to ensure that all transactions are recognized. Perform the online review on a daily basis or more often as deemed necessary to confirm that no fraudulent transactions have occurred. Immediately contact the bank if there are any transactions not recognizable.

### 4.4. Banking relationship

Review on a regular basis the proactive nature of the Bank or Credit Union. While it can be cumbersome to move financial accounts to a new entity, it is not impossible to do so. Similar to customers reviewing a Bank or a Credit Union for their fees, and interest amounts rates paid on investments, reviewing the bank institution for their security status should be done on a regular basis.

### 4.5. Set limits

Ensure that the Bank or Credit Union allows for a maximum limit on regular transfers. Any amount in excess of these limits should require additional authentication techniques to ensure that the amounts are appropriately authorized to be transferred. Banks and Credit Unions refusing to place limits and follow basic procedures should be avoided.

### 4.6. Credit alerts

On an annual basis review the business' credit rating as well as the business owner's credit rating to ensure that no other credit cards or bank accounts have been added. In addition to online banking fraud, identity theft is increasing exponentially. An annual fraud review for both the business owner and the business ensures that both remain in good financial health.

## 5. Conclusions

Small business banking fraud is on the rise. Small business owners are often uninformed as to the magnitude of the risks they face as well as the lack of ability to recover from these losses. Awareness that business bank accounts are not FDIC insured is often the first step. This should spur users of business banking accounts to take additional actions to protect themselves from online bank fraud. Using a dedicated computer machine for such sensitive transactions and ensuring users are aware of the current phishing trends, as well as current state of affairs of attacks helps to reduce a great many risk issues. Taking additional steps such as the use of non-administrative accounts on Windows workstations is a key proactive measure as well. Removing or restricting the use of Java, Flash and other third party software used in attacks also increases the protective stance of a system. Choose a passphrase rather than a password and ensure that the passphrase is not reused on multiple sites. Change the passphrase to accounts on a regular basis.

The recommendations and options listed in this white paper are not all inclusive nor are they prohibitive. These techniques will still allow a user to perform all of the normal tasks on a system that are needed for day to day business use. As threats and risks change, it is necessary to be proactive and to continually reevaluate security choices and solutions. Vigilance is necessary in reviewing the risk factors noted by Journalists on these issues and making changes to the risk aversion choices must be done regularly.

The use of these techniques will help to ensure that small businesses remain more proactive in reviewing online banking risks and will better protect businesses and business assets from attacks by cyber criminals.

## 6. References

Acohido, B. (2010, January 6). *American Bankers Association's warning to small firms comes as a surprise*. Retrieved January 17, 2013, from The Last Watchdog : http://lastwatchdog.com/american-bankers-associations-small-business-warning/

Adams, J. (2013, January 2). *Wells Fargo, Ally Bank See the Camera as Key to Mobile Banking*. Retrieved January 7, 2013, from American Banker: http://www.americanbanker.com/issues/178_2/wells-fargo-ally-see-the-camera-as-key-to-mobile-banking-1055540-1.html

American Bankers Association. (2011, September 8). *ABA Survey: Popularity of Online Banking Explodes*. Retrieved November 5, 2012, from ABA: http://www.aba.com/Press/Pages/090811ConsumerPreferencesSurvey.aspx

AOL.com. (2013). Retrieved January 7, 2013, from AOL Datamask software provided by AOL.com: http://datamask.aol.com/?

Ayesha.A. (2013). *Chrome vs Firefox for Ubuntu*. Retrieved January 17, 2013, from Unixmen: http://www.unixmen.com/chrome-vs-firefox-for-ubuntu/

Bank of America. (2013, May 28). *Security and Support FAQs*. Retrieved May 28, 2013, from Bank of America: https://www.bankofamerica.com/onlinebanking/online-banking-security-faqs.go

Block, S. (2013). *Will Bank Branches wither away*. Retrieved January 17, 2013, from USA Today: http://www.cnbc.com/id/45341157/Will_Bank_Branches_Wither_Away

Chen, B. (2012, December 13). *Android Malware Creeps Into Cellphone Bills*. Retrieved December 30, 2012, from NYTimes Bits: http://bits.blogs.nytimes.com/2012/12/13/lookout-toll-fraud/

CVEDetails. (2012). *The ultimate security vulnerability data source*. Retrieved December 24, 2012, from CVEdetails.com: http://www.cvedetails.com/vulnerability-list/vendor_id-53/product_id-6761/Adobe-Flash-Player.html

Eascorp. (n.d.). *Installing a personal certificate*. Retrieved December 30, 2012, from Eascorp: http://www.eascorp.org/help/Ease-Link/Procedures/Installing_a_Personal_Certificate.htm

Freitag, P. (2011, February 16). *Java 1.6.0_24 Released Patches DOS Vulnerability*. Retrieved December 13, 2012, from Pete Freitag: http://www.petefreitag.com/item/786.cfm

Friedl, S. (2013). *Configuring Windows 7 for a Limited User Account*. Retrieved January 7, 2013, from Steve Friedl's Unixwiz.net Tech Tips: http://unixwiz.net/techtips/win7-limited-user.html

Henry, P. (2013). *Initial Thoughts on Windows 8 Security*. Retrieved January 17, 2013, from Lumension blog: http://blog.lumension.com/6119/initial-thoughts-on-windows-8-security/

Hoffman, S. (2012, December 24). *Java top exploited software as noted by Kaspersky*. Retrieved December 24, 2012, from Channelnomics: http://channelnomics.com/2012/12/24/java-tops-adobe-exploited/

Intuit. (2012). *Intuit Partner Platform*. Retrieved December 30, 2012, from Intuit Anywhere Security Review paper: http://developer.intuit.com/uploadedFiles/Developer/MyIDN/Technical_Resources/QBPD/IASecurityReview.pdf

Intuit. (2013). *Non-Intuit support programs installed with QuickBooks*. Retrieved May 4, 2013, from Intuit Quickbooks Support: http://support.quickbooks.intuit.com/support/articles/INF12790

Johansson, J. M. (2004). *The Great Debates: Pass Phrases vs. Passwords. Part 2 of 3*. Retrieved June 1, 2013, from Security TechCenter: http://technet.microsoft.com/library/cc512609

Kaspersky. (2012, December 21). *Oracle Java surpasses Adobe Reader as the most frequently exploited software*. Retrieved April 29, 2013, from Kaspersky Lab: http://www.kaspersky.com/about/news/virus/2012/Oracle_Java_surpasses_Adobe_Reader_as_the_most_frequently_exploited_software

Kingsley-Hughes, A. (2012, July 6). *First IOS malware hits the app store*. Retrieved January 17, 2013, from Forbes: http://www.forbes.com/sites/adriankingsleyhughes/2012/07/06/first-ios-malware-hits-app-store/

Krebs, B. (2012, November 6). *Cyberheists 'A helluva wakeup call'*. Retrieved November 8, 2012, from www.krebsonsecurity.com: http://krebsonsecurity.com/2012/11/cyberheists-a-helluva-wake-up-call-to-small-biz/

Krebs, B. (2012, July). *KrebsonSecurity*. Retrieved January 7, 2013, from Banking On a Live CD: http://krebsonsecurity.com/2012/07/banking-on-a-live-cd/

Krebs, B. (2013, March 13). *Missouri Court Rules Against $440,000 Cyberheist Victim*. Retrieved May 4, 2013, from Krebsonsecurity: http://krebsonsecurity.com/2013/03/missouri-court-rules-against-440000-cyberheist-victim/

Larsen, C. (2012, December 5). *BlueCoat Security blog*. Retrieved January 17, 2013, from Blackhole Kit doesn't like Chrome: http://www.bluecoat.com/security-blog/2012-12-05/blackhole-kit-doesnt-chrome

Maone, G. (2013). *NoScript 2.6.4.2*. Retrieved January 7, 2013, from Add Ons: https://addons.mozilla.org/en-US/firefox/addon/noscript/

Margosis, A. (2013). *LUA Buglight 2.2 with support for Windows 8*. Retrieved January 7, 2013, from MSDN Blogs: http://blogs.msdn.com/b/aaron_margosis/archive/2012/11/28/lua-buglight-2-2-with-support-for-windows-8.aspx

Microsoft. (2012). *Microsoft Security Intelligent Report*. Retrieved December 20, 2012, from Microsoft Security Intelligent Report: http://download.microsoft.com/download/C/1/F/C1F6A2B2-F45F-45F7-B788-32D2CCA48D29/Microsoft_Security_Intelligence_Report_Volume_13_English.pdf

Microsoft. (2013). *Applocker frequently asked questions*. Retrieved January 7, 2013, from Technet: http://technet.microsoft.com/en-us/library/ee619725(v=WS.10).aspx

Mozilla. (2012). *Firefox addons*. Retrieved December 30, 2012, from Add Ons: https://addons.mozilla.org/en-US/firefox/extensions/privacy-security/

Netburn, D. (2012). *Starbucks brews up mobile payment changes, adds digital tipping*. Retrieved December 30, 2012, from LATimes: http://articles.latimes.com/2012/oct/04/business/la-fi-tn-starbucks-digital-tipping-20121004

Oracle. (2013, April). *Oracle Java SE Critical Patch Update Advisory - April 2013*. Retrieved May 4, 2013, from Oracle Technology Topics: http://www.oracle.com/technetwork/topics/security/javacpuapr2013-1928497.html

Portal, M. -S. (2012). *Definition of Blacole Exploit*. Retrieved December 20, 2012, from Microsoft Security Portal: http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Blacole

Reinhold, M. (2013, April 18). *Proposed new schedule for JDK 8*. Retrieved May 4, 2013, from JDK-8 Dev mailing list archives: http://mail.openjdk.java.net/pipermail/jdk8-dev/2013-April/002336.html

SANS.org. (2013). *Ouch Newsletter*. Retrieved January 7, 2013, from SANS: http://www.securingthehuman.org/resources/newsletters/ouch/2013

Schwartz, M. (2012, September 26). *Java Vulnerability affects 1 billion plug ins*. Retrieved December 30, 2012, from Information Week: http://www.informationweek.com/security/application-security/java-vulnerability-affects-1-billion-plu/240007985

Secunia. (2012). *Browser vulnerability statistics* . Retrieved December 21, 2012, from http://secunia.com/advisories/product/11/?task=statistics

Secunia. (2013). *Vulnerability Report: Adobe Flash Player 11.x*. Retrieved April 29, 2013, from Secunia Advisories - Adobe Flash: http://secunia.com/advisories/product/38260/?task=statistics

Securelist. (2012, November). *Definition of software vulnerabilities*. Retrieved November 20, 2012, from Securelist: http://www.securelist.com/en/threats/vulnerabilities?chapter=35

Singh, S. (2012, December 25). *Android malware threat to rise in 2013 in India: Report*. Retrieved January 7, 2013, from Times of India: http://timesofindia.indiatimes.com/tech/personal-tech/computing/Android-malware-threat-to-rise-in-2013-in-India-Report/articleshow/17755132.cms

Slavasoft. (2013). *SlavaSoft HashCalc HASH, CRC, AND HMAC CALCULATOR*. Retrieved January 7, 2013, from SlavaSoft : http://www.slavasoft.com/hashcalc/index.htm

StarOne Credit Union. (2012). *ezDeposit FAQs*. Retrieved December 13, 2012, from StarOne Credit Union: http://www.starone.org/home/accountaccess/ezdeposit/ez_faq

The Business Journals. (2013, April 23). *Trend Micro Q1 2013 Security Roundup Report Highlights Concerns over Zero-Day Vulnerabilities and Increasingly Destructive Attacks*. Retrieved May 4, 2013, from The Business Journal: http://www.bizjournals.com/prnewswire/press_releases/2013/04/23/SF99294

United States, 1. C. (2007, February 8). *Gulf Coast Back to Business Act of 2007*. Retrieved December 30, 2012, from Govtrack.us: http://www.govtrack.us/congress/bills/110/s537/text

US-Cert. (2008). *US-Cert Banking Securely Online*. Retrieved November 8, 2012, from US-Cert: http://www.us-cert.gov/reading_room/Banking_Securely_Online07102006.pdf

VandenBrink, R. (2013). *When Disabling IE6 (or Java, or whatever) is not an Option*. Retrieved January 17, 2013, from Incidents.org: https://isc.sans.edu/diary/When+Disabling+IE6+%28or+Java%2C+or+whatever%29+is+not+an+Option.../14947

Wikipedia. (2012). *Trusteer Rapport software explained*. Retrieved December 2012, 3, from Wikipedia : http://en.wikipedia.org/wiki/Trusteer

Wikipedia.org. (2013). *Definition of Blackhole Exploit Kit*. Retrieved January 7, 2013, from Wikipedia: http://en.wikipedia.org/wiki/Blackhole_exploit_kit

Wikipedia.org. (2013). *Definition of OFX*. Retrieved January 17, 2013, from Wikipedia: http://en.wikipedia.org/wiki/OFX

Wikipedia.org. (2013). *Definition of Pwn2own contest*. Retrieved January 7, 2013, from Wikipedia: http://en.wikipedia.org/wiki/Pwn2own

Wikipedia.org. (2013). *Definition of Sha-1*. Retrieved January 7, 2013, from Wikipedia: http://en.wikipedia.org/wiki/SHA-1

Wikipedia.org. (2013, May 28). *History of Microsoft Windows*. Retrieved May 28, 2013, from Wikipedia.org: http://en.wikipedia.org/wiki/History_of_Microsoft_Windows

Zetter, K. (2012). *Judge orders settlement*. Retrieved December 2, 2012, from Wired.com: http://www.wired.com/threatlevel/2012/11/bank-to-pay-hacking-victim/

Zhen, S. (2012, March 13). *Take It to the Bank: Mobile Check Deposit is the Next-Gen Standard*. Retrieved December 30, 2012, from MyBankTracker:

http://www.mybanktracker.com/news/2012/03/13/bank-mobile-check-deposit-next-gen-standard/

Last Updated: January 20th, 2018

# Upcoming SANS Training

**Click Here for a full list of all Upcoming SANS Events by Location**

| | | | |
|---|---|---|---|
| SANS Las Vegas 2018 | Las Vegas, NVUS | Jan 28, 2018 - Feb 02, 2018 | Live Event |
| Cyber Threat Intelligence Summit & Training 2018 | Bethesda, MDUS | Jan 29, 2018 - Feb 05, 2018 | Live Event |
| SANS Miami 2018 | Miami, FLUS | Jan 29, 2018 - Feb 03, 2018 | Live Event |
| SANS London February 2018 | London, GB | Feb 05, 2018 - Feb 10, 2018 | Live Event |
| SANS Scottsdale 2018 | Scottsdale, AZUS | Feb 05, 2018 - Feb 10, 2018 | Live Event |
| SANS SEC455: SIEM Design Beta One 2018 | Arlington, VAUS | Feb 12, 2018 - Feb 13, 2018 | Live Event |
| SANS Southern California- Anaheim 2018 | Anaheim, CAUS | Feb 12, 2018 - Feb 17, 2018 | Live Event |
| SANS Secure India 2018 | Bangalore, IN | Feb 12, 2018 - Feb 17, 2018 | Live Event |
| SANS Brussels February 2018 | Brussels, BE | Feb 19, 2018 - Feb 24, 2018 | Live Event |
| SANS Secure Japan 2018 | Tokyo, JP | Feb 19, 2018 - Mar 03, 2018 | Live Event |
| Cloud Security Summit & Training 2018 | San Diego, CAUS | Feb 19, 2018 - Feb 26, 2018 | Live Event |
| SANS Dallas 2018 | Dallas, TXUS | Feb 19, 2018 - Feb 24, 2018 | Live Event |
| SANS New York City Winter 2018 | New York, NYUS | Feb 26, 2018 - Mar 03, 2018 | Live Event |
| CyberThreat Summit 2018 | London, GB | Feb 27, 2018 - Feb 28, 2018 | Live Event |
| SANS London March 2018 | London, GB | Mar 05, 2018 - Mar 10, 2018 | Live Event |
| SANS Secure Singapore 2018 | Singapore, SG | Mar 12, 2018 - Mar 24, 2018 | Live Event |
| SANS Secure Osaka 2018 | Osaka, JP | Mar 12, 2018 - Mar 17, 2018 | Live Event |
| SANS San Francisco Spring 2018 | San Francisco, CAUS | Mar 12, 2018 - Mar 17, 2018 | Live Event |
| SANS Paris March 2018 | Paris, FR | Mar 12, 2018 - Mar 17, 2018 | Live Event |
| SANS Northern VA Spring - Tysons 2018 | McLean, VAUS | Mar 17, 2018 - Mar 24, 2018 | Live Event |
| SANS Munich March 2018 | Munich, DE | Mar 19, 2018 - Mar 24, 2018 | Live Event |
| SANS Pen Test Austin 2018 | Austin, TXUS | Mar 19, 2018 - Mar 24, 2018 | Live Event |
| ICS Security Summit & Training 2018 | Orlando, FLUS | Mar 19, 2018 - Mar 26, 2018 | Live Event |
| SANS Secure Canberra 2018 | Canberra, AU | Mar 19, 2018 - Mar 24, 2018 | Live Event |
| SANS Boston Spring 2018 | Boston, MAUS | Mar 25, 2018 - Mar 30, 2018 | Live Event |
| SANS 2018 | Orlando, FLUS | Apr 03, 2018 - Apr 10, 2018 | Live Event |
| SANS Abu Dhabi 2018 | Abu Dhabi, AE | Apr 07, 2018 - Apr 12, 2018 | Live Event |
| Pre-RSA® Conference Training | San Francisco, CAUS | Apr 11, 2018 - Apr 16, 2018 | Live Event |
| SANS Zurich 2018 | Zurich, CH | Apr 16, 2018 - Apr 21, 2018 | Live Event |
| SANS London April 2018 | London, GB | Apr 16, 2018 - Apr 21, 2018 | Live Event |
| SANS Dubai 2018 | OnlineAE | Jan 27, 2018 - Feb 01, 2018 | Live Event |
| SANS OnDemand | Books & MP3s OnlyUS | Anytime | Self Paced |