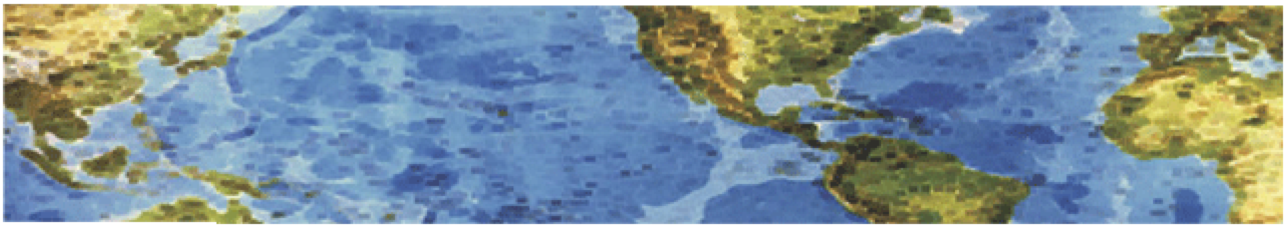
HALL ASSOCIATES



Risk-Based Decision Making Commentary
April 2 2013 Newsletter

FTC Releases Top 10 Complaint Categories for 2012

Identity Theft Tops List for 13th Consecutive Year in Report of National Consumer Complaints

Identity theft is once more the top complaint received by the Federal Trade Commission, which has released its 2012 annual report of complaints. 2012 marks the first year in which the FTC received more than 2 million complaints overall, and 369,132, or 18 percent, were related to identity theft. Of those, more than 43 percent related to tax- or wage-related fraud. To file a complaint, visit the FTC's online Complaint Assistant or call 1-877-FTC-HELP (1-877-382-4357). The FTC's website provides free information on a variety of consumer topics.

Attackers Exploited Vulnerabilities in ATM Networks Connecting to Bank VPNs and GSM/GPRS Networks, Malware Infected ATMs and POS Systems.

A new malware targeting point-of-sale (POS) systems and ATMs has stolen payment card information from several US banks, researchers say. The author behind the malware appears to have links to a Russian cyber-crime gang. Called "Dump Memory Grabber", the malware scans the memory of point-of-sale systems and ATMs looking for credit card data. The researchers believe the malware has already been used to steal data from credit and debit cards issued by major US banks, including Chase, Capital One, Citibank, and Union Bank of California. Unlike the more well-known banking malware, which infects individual user computers and intercepts online banking credentials and credit card details, attacks on POS systems and ATMs are far more insidious. In this case, cyber-criminals are infecting ATMs and physical POS systems, such as stand-alone kiosks and modern cash register systems, to harvest information from debit and credit cards. Criminals can use the information to create cloned physical cards.

Most of these POS/ATM attacks relied on the "help of insiders," such as the employees in charge of maintaining POS systems and authorized to update the software, the security firm said. A few POS systems running Windows XP or Windows Embedded with Remote Desktop or VNC software were infected remotely, and in some cases, attackers exploited vulnerabilities in ATM networks connecting to the bank's VPN or GSM/GPRS networks.

Dump Memory Grabber is not the first malware family to target POS and ATMs. There are many different malware families targeting POS systems recently. A few months ago, Dexter was observed infecting POS systems at well-known retail outlets, hotels, and food establishments and capturing card data during the sales process. Dexter is believed to have stolen nearly 80,000 credit card records at several Subway restaurants last year. Infection vectors include **physically inserting a malicious USB drive**, or via the Web if the target system was directly connected to the Internet.

http://www.securityweek.com/exclusive-new-malware-targeting-pos-systems-atms-hits-major-us-banks

HALL ASSOCIATES

Protect Your Identity During Tax Season

Identity theft has become a growing problem in the U.S., and tax season is prime season for Americans to have their information and finances compromised. During the first nine months of 2012, the IRS identified 641,690 incidents of tax-related identity theft, a significant increase from the 47,730 reported claims in 2008. There are two basic ways that tax fraud occurs: scammers use your personal information to redirect your tax return to them, or they use your Social Security number to get jobs or loans. Scammers get their hands on personal data through a variety of ways, including breaking and entering a home or car and stealing mail or a W2 form. The biggest way you can become a victim of fraud is by not protecting your physical information. You need to be wary of providing your personal information to any third parties, particularly your Social Security number.

Tips on what you can do to prevent tax fraud this filing season.

1. File early. The sooner you file your return, the less opportunity someone else has to file a return in your name.
2. Research all third-party providers. A little due diligence goes a long way when it comes to using online tools. Before using any online filing application, review the privacy policies, how long your documents and information are stored and how it's destroyed. Be picky about who you have doing your taxes because identity fraud rings might front as a tax preparing company. Before hiring someone to do your taxes, verify their status with the Better Business Bureau and the Internal Revenue Service's Office of Professional Responsibility.
3. Don't respond to unsolicited emails. The IRS will never initiate a contact with you through email.
4. Encrypt information in emails. Whenever possible, physically hand your information to your tax preparer instead of through email. If you have to email it, always encrypt your files and only send this information to someone you trust.
5. Don't sign blank forms. Never sign a blank or incomplete tax return or one that your tax preparer has failed to sign. Since someone can use the blank form that's signed to commit fraud, have the tax return completed first and then sign it only after you've reviewed it with your tax preparer.
6. Protect your mail and your information
7. Double check your tax forms. When you receive your forms, make sure the income is really your income and not someone else's, says Reynolds. People who have a difficult time getting lawful employment will use your information to get lawful employment. They'll defer their tax liability until the end of the year and pass that onto the victim.

What do you do if your Identity has been stolen? Contact the IRS at 1-800-908-4490, complete an IRS Identity Theft Affidavit (Form 14039) and call the credit bureaus and your credit card companies. The IRS will issue a temporary number.

http://www.foxbusiness.com/personal-finance/2013/03/26/how-to-protect-your-identify-during-tax-season/#ixzz2OggV2j2n