

{ bytes in brief }

LAW AND TECHNOLOGY NEWS MONTHLY

EDITORS: Sharon D. Nelson, Esq. and John W. Simek
ASSOCIATE EDITOR: Jason R. Foltin EDITOR EMERITUS: G. V. Nelson



© 2009 SENSEI ENTERPRISES, INC.

www.senseient.com

COMPUTER FORENSICS | INFORMATION TECHNOLOGY

Issue 151 - December 2009

PLEASE NOTE: The URLs referenced in Bytes frequently link to newspapers and other current news sources. These links may fail over time. [Click here to visit Sensei's home page at www.senseient.com](http://www.senseient.com)

SCHOOL SUED FOR PUNISHING TEENS OVER MYSPACE PIX

On October 30th, *The Associated Press* reported that the American Civil Liberties Union (ACLU) has filed a lawsuit on behalf of two sophomore girls after they were punished for posting sexually suggestive photos on MySpace during their summer vacation. The suit contends that Churubusco High School violated the girls' free speech rights when it banned them from extracurricular activities for a joke that didn't involve the school. Moreover, the ACLU has argued that the district humiliated the girls by requiring them to apologize to an all-male coaches' board and undergo counseling. According to ACLU legal director Ken Falk, the punishment just doesn't fit the crime. However, an attorney for the school district said that the school's principal was merely enforcing the northeast Indiana school's athletic code, which allows the principal to bar from school activities any student-athlete whose behavior in or out of school creates a disruptive influence on the discipline, good order, moral or educational environment at Churubusco High School. While some child advocates have contended that schools should assist in watching children's behavior, others aren't so sure and have stated that, in this digital era, schools must accept that students will engage in some questionable behavior in cyberspace and during off hours. While teens who have done similar things in other states have faced prosecution, the ACLU has emphasized that this case is different; the photos were a joke intended to be shared only with friends. No matter what, Martha McCarthy, a professor who teaches educational law and policy at Indiana University, thinks that the Supreme Court will have to address this issue. A copy of the complaint may be found at <http://www.courthousenews.com/2009/10/28/Lollipop.pdf>

FACEBOOK SPELLS OUT UPDATED PRIVACY POLICY

On October 29th, Facebook's head of communications, Elliot Schrage, posted a company blog entry discussing proposed updates to Facebook's privacy policy. Schrage stated that many of the proposed updates pertain to what happens to the content users have deleted from their account. Specifically, new sections have been added explaining the privacy setting you can choose to make your content viewable by everyone, the difference between deactivating and deleting a member's account, and the process of memorializing an account once the company has received a report that the account holder is deceased. The social networking site explained to users that they can "deactivate" their account, which hides the account but keeps the information for potential reactivation. Or, conversely, users can choose to delete it for good. The company further noted that even after a user removes information from his or her profile or even deletes the account, copies of that information may remain viewable elsewhere to the extent it has been shared with others, it was otherwise distributed pursuant to your privacy settings, or it was copied and comments were posted. These new proposed updates are just the latest of a long and twisted road for the social network's privacy regulations. Some individuals expressed outrage after changes to Facebook's terms of service implied that Facebook claimed an irrevocable, perpetual, non-exclusive, transferable, fully paid, worldwide license even if the member content had been deleted. In July, Facebook faced more criticism after some believed that modifications the company made to its user privacy controls would allow large quantities of profile information to be shared with third-party developers or advertisers. However, in August, the company responded by making additional changes and, in this most recent change, Facebook reiterated that it does not intend to share personal data with advertisers. Schrage's post explained that any information provided to advertisers is anonymized, meaning that it can't be traced back to a member as an individual in any way. The Facebook blog post may be found at <http://blog.facebook.com/blog.php?post=167389372130>

FACEBOOK AWARDED \$711 MILLION FROM CONVICTED SPAMMER

On October 29th, the U.S. District Court for the Northern District of California awarded Facebook \$711 million in damages from convicted spammer Sanford Wallace and recommended that the U.S. Attorney's Office prosecute Wallace for criminal contempt. Earlier this year, Wallace and two others, Adam Arzoomanian and Scott Shaw, were sued by Facebook for allegedly obtaining the login credentials for various accounts and then using those accounts to send spam to those users' friends. The spam messages sent by the cybercriminals either linked to other phishing sites or to commercial websites that paid spammers for referrals. While Facebook has stated that it does not expect to receive the vast majority of the award, the fact that Wallace faces possible jail time for violating a temporary restraining order was, in the company's opinion, an important victory in the fight against spam. This is not the first time Wallace has been found in violation of the CAN-SPAM act. In May 2008, he was found guilty of violating the act and ordered to pay \$230 million for spamming and phishing social networking giant MySpace. A Facebook blog posting on the topic may be found at <http://blog.facebook.com/blog.php?post=58219622130>

INTERNET ADDRESSES SET FOR CHANGE

On October 27th, ICANN voted to allow domain names in non-Latin-script including Arabic, Chinese and others. Some have explained that the point of this ICANN decision was to create a universal Internet code that will work in any language and globally so all the world's computers can connect with each other. No matter what the reason, the decision has paved the way for the Internet's Domain Name System (DNS) to be changed so it can recognize and translate non-Latin characters. This change does not come without challenges. ICANN has noted that the fantastically complicated technical feature allowing Internationalized Domain Names (IDN) would represent the biggest change to the coding that underlies the Internet since it was invented. However, if all goes well, the first IDNs could be in use as early as next year. It is likely that the majority of early non-Latin net addresses to be approved will be in Chinese and Arabic script, followed by Russian. Although some countries, such as China and Thailand, have already introduced workarounds that allow users to enter Web addresses in their own language, these solutions are neither internationally approved nor do they work on all computers. More information may be found at http://www.nydailynews.com/news/world/2009/10/30/2009-10-30_internet_addresses_set_for_change_after_icann_votes_in_favor_of_foreign_characters.html

WEB-BASED MALWARE INFECTIONS RISE RAPIDLY, STATS SHOW

On October 27th, *CNET News* reported that a new study from Dasient revealed that the number of websites hosting malicious software, either intentionally or unwittingly, has risen rapidly. According to the report, more than 640,000 Web sites and about 5.8 million pages are infected with malware — nearly double the number of infected pages Microsoft estimated in a report this past April. In addition, Dasient identified another 52,000 Web-based malware infections, increasing the number of unique infections logged by the company since it launched its malware analysis platform early this year to more than 72,000. The primary culprit for malware infections are JavaScript and iFrames being injected into legitimate sites, accounting for close to 55% and 37% respectively. And once a site is infected, the report noted almost half of the sites are later reinfected. Meanwhile, the Google blacklist of malware infected sites has more than doubled in the last year, registering as many as 40,000 new sites in one week. The statistics provided further illustrate a trend of attackers targeting browsers and Web applications with SQL injections, cross-site scripting and other attacks that can lead to drive-by downloads. As one commentator explained, one thing is certain, Web-based infections can come from anywhere on a site, including widgets and ads. A report discussing why and how malware attacks occur may be found at http://www.dasient.com/resources/why_how_malware_attacks.pdf

JUDGE REJECTS TD AMERITRADE DATA THEFT SETTLEMENT

On October 26th, *The Associated Press* reported that U.S. District Judge Vaughn Walker had refused to approve a class-action settlement regarding contact information stolen from online brokerage firm Ameritrade Holding Corp. In rejecting the proposed deal, Judge Walker explained that the deal appeared to do more for Ameritrade and the Plaintiffs' lawyers than it did the victims. The three main benefits Ameritrade promised in the proposed settlement were (1) to hire someone to test its security systems, (2) to retain an outside expert to check for evidence of

widespread identity theft and (3) cover the cost of one year of anti-spam service for the victims. Judge Walker explained that of these purported benefits, the first and second settlement points appear to benefit the company more than the class. However, a spokeswoman for Ameritrade and the lead Plaintiff's attorney expressed their disappointment in the ruling and reiterated their belief that the settlement did indeed provide meaningful benefits to the members of the class. Several Ameritrade officials noted that the data theft has not been linked to cases of identity theft and that the company has retained ID Analytics Inc., which has expertise in identity theft, to help investigate. Further, Ameritrade officials have said that insurance would have covered much of the cost of the proposed settlement, quelling concerns that the deal might have affected the company's earnings materially. A hearing has been scheduled for December 10th to determine what will happen next in the data breach case. More information may be found at http://www.usatoday.com/money/industries/technology/2009-10-26-ameritrade-suit_N.htm

TEXAS WOMAN SUES FACEBOOK FOR PRIVACY VIOLATIONS

On November 5th, *MyFoxDFW.com* reported that Cathryn Harris had sued Facebook and Blockbuster after she found out that Facebook added a note every time she rented a movie from Blockbuster; a note containing her full name and the title of the movie she rented. The two lawsuits – one against Blockbuster last year and one against Facebook last month – allege a partnership between the two companies that allowed Blockbuster to send Harris' movie-renting habits to Facebook without fair opportunity to opt out. The crux of Harris' contentions against Facebook is the controversial Beacon system. The system is basically a tracking flag that follows you across a network of sites and reports back to Facebook on your activity. Consumers are able to use the system to share more information about your daily activity while advertisers can use it to learn a great deal more about an individual. After the public cried foul in 2007, Facebook CEO Mark Zuckerberg apologized and subsequently changed the Beacon system policy. Notwithstanding this change, Harris contends that whether a consumer opts in or out, the Beacon system is a violation of the Video Privacy Protection Act, which prevents a company from disclosing information about a customer's rental habits without their knowledge. Meanwhile, Facebook is in the process of settling a similar California lawsuit, the outcome of which could determine whether Harris can move forward with a class-action suit. In response to the California lawsuit, the social networking giant has agreed to discontinue the Beacon advertising program and has acknowledged how critical it is to provide extensive user control over how information is shared. A copy of the complaint may be found at <http://media2.myfoxdfw.com/PDF/facebook-suit.pdf>

FACEBOOK PROVIDES ALIBI FOR ROBBERY SUSPECT

On November 12th, *Reuters.com* reported that a status update posted on the social networking site Facebook had exonerated a New Yorker who was arrested for armed robbery. Rodney Bradford was initially arrested and held for 12 days after police believed that he robbed two people in the Brooklyn housing project where he lives. However, Bradford was able to prove his innocence by showing authorities that he had updated his Facebook page from a computer in his father's Manhattan building, effectively placing him elsewhere when the crime occurred. More information may be found at <http://www.reuters.com/article/technologyNews/idUSTRE5AB5JO20091112>

MORE SECURITY BREACHES HIT MIDSIZE COMPANIES

On October 28th, McAfee released a report highlighting that more and more midsize companies are being attacked by cybercriminals at the same time that these same companies are spending less on security. The report noted that, in the past year alone, more than half of the world's 900 midsize business stated that they have seen an increase in security breaches. Plus, the cost of dealing with these security problems can be quite high. According to the report, one in five midsize companies surveyed lost \$41,000 in sales on average as a result of a breach. More than 70% believe a serious data breach could put them out of business. In spite of the increase and the potential ramifications of these attacks, the recent recession has hit these firms quite hard, with many freezing or even lowering their IT budgets. Almost 40% of the companies trimming their IT security budget plan to limit the purchase of new security products. And even though the firms realize that switching to cheaper security software may put them at a greater risk, more than a third of surveyed firms have done so. Senior vice president of global midmarket for McAfee, Darrell Rodenbaugh, explained that an organization's level of worry and awareness about increasing threats has not overcome the downward pressure on budgets and resources. In fact, he noted that his company's research demonstrated that organizations that put more effort on preventing attacks can end up

spending less than a third as much as those that allow themselves to be at risk. In the end, an ounce of prevention is really worth a pound of cure. A copy of the report may be downloaded at http://www.mcafee.com/us/research/security_paradox/index.html

JUDGE BANS TWITTER FROM COURT

On November 9th, *CBS News* reported that a federal judge in Georgia had banned spectators from sending live updates from a criminal trial. In his remarks, U.S. District Judge Clay Land explained that Rule 53 of the Federal Rules of Criminal Procedure should be interpreted to ban Twitter and other similar messaging systems. The controversy first arose after a reporter for the Columbus Ledger-Enquirer had asked permission to post Twitter updates from the corruption trial of local attorney Mark Shelnett, which was scheduled to start on Monday. Judge Land stated that the term broadcasting in Rule 53 included sending electronic messages from a courtroom that contemporaneously described the trial proceedings and were instantaneously available for public viewing. While Judge Land noted that broadcasting is typically associated with the dissemination of information via television or radio, it appeared clear that the drafters of Rule 53 intended the Rules reach to include, among other things, transmissions of trial proceedings using Twitter. It is important to note that this is just one judge's interpretation of Rule 53 and other courts, such as one in Kansas, have ruled that the use of Twitter during proceedings was perfectly fine. A copy of the complaint may be found at <http://volokh.com/2009/11/09/federal-rules-interpreted-as-barring-twitter-coverage-of-trial-from-courtroom/>

W.VA. SUPREME COURT OPTS FOR E-MAIL SECRECY

On November 12th, the West Virginia Supreme Court ruled that public officials and public employees can keep their personal e-mails secret. The decision stemmed from a suit brought by the Associated Press in an attempt to gain access to 13 e-mails between former Supreme Court Chief Justice Elliott "Spike" Maynard and Massey Energy Chief Executive Don Blankenship. Earlier, Kanawha County Circuit Court Judge Duke Bloom ruled that five of the e-mails were public, but that eight were not. Judge Bloom had reasoned that five of the e-mails were part of the public record because they discussed Maynard's unsuccessful campaign in the Democratic primary, in which he ran against two of the justices now sitting on the court. However, the Supreme Court reversed, reasoning that none of the e-mails were public records as defined under the state's Freedom of Information Act. The Act requires disclosure of information relating in any manner to either the conduct of the public business, or to the official duties, responsibilities or obligations of the particular public body. In essence, the ruling states that content is the only factor that determines whether a personal e-mail sent by any "public official or employee" is a public record under state law-- public interest in a particular case can't be used to make that determination. The *Associated Press* has expressed its belief that there can be no such thing as a 'purely personal, communication between a powerful business and political figure and the state's chief justice who also just happened to be presiding over that powerful figure's case. However, according to the court, in order for the *Associated Press'* argument to stand, the Legislature would have to change the definition of a public record to include taking the record's context into account. More information may be found at <http://www.wvgazette.com/ap/ApTopStories/20091120770>

GOVERNMENT IT CONFRONTS SECURITY THREATS DAILY

On November 12th, *InformationWeek.com* reported that a recent survey found that external attacks, malware, lost devices, and internal threats pose ongoing security challenges for many federal agencies. Of the 300 federal IT pros surveyed, 31% said that their agency experiences a cybersecurity incident of some kind daily. Of these incidents, the top issues include malware (33% of respondents), inappropriate employee activity or network use (25%), managing access for approved remote users (25%), and data encryption (23%). Those surveyed also noted an increased need for new cybersecurity technologies. Federal cybersecurity spending is expected to increase from \$7.9 billion this year to \$11.7 billion in 2014. The increase in spending will help fund projects such as a \$1.5 billion cybersecurity data center and a cybersecurity operations center. Further, the recent rise of mobile computing and smart phone use has caught the attention of federal IT pros. Concerns over the potential security headaches due to remote and mobile computing were on the rise for 60% of those surveyed, but even among those who indicated that mobile security challenges are increasing, 63% failed to use wireless encryption, despite federal requirements. Further, the report highlighted that government IT pros view external threats as being more serious than internal threats. When asked to name their most significant external threat, defense agencies identified state-sponsored cyberwar, while civilian agencies cited hackers and software vulnerabilities. Finally, a

majority of respondents opined that user education was the best way to improve cybersecurity. More information may be found at

<http://www.informationweek.com/news/government/security/showArticle.jhtml?articleID=221601320>

APPLE'S MAMMOTH UPDATE PATCHES 58 BUGS

On November 9th, Apple patched 58 vulnerabilities in its Mac operating systems, the most since May 2009. In addition, Apple appeared to retire Mac OS X 10.4, a/k/a Tiger, from security support - none of the patches affect that operating system, which debuted in April 2005. Although the number may seem large, Andrew Storms, director of security operations at nCircle Network security, stated that it really is just par for the course for Apple. 32 of the 58 patches fixed vulnerabilities deemed critical, as demonstrated by the phrase "may lead to arbitrary code execution." The patches fixed problems in 37 different components of Mac OS X, ranging from AFP Client and the open-source Apache Web server software to CoreGraphics, the Help Viewer and the Spotlight desktop search engine. Some of the most important patches included the four that patched critical vulnerabilities in the version of QuickTime originally packaged with Mac OS X 10.6, a/k/a Snow Leopard. Five other vulnerabilities were also Snow Leopard-only: A pair of bugs in the CoreMedia component's parsing of H.264 movie files, one in ImageIO's handling of TIFF files, and vulnerabilities in the kernel and launch services were patched in this update. Additionally, several open-source components of Mac OS X were also patched in Apple's update, including the Apache Web server, Fetchmail, IPSec, LibXML, OpenLDAP, OpenSSH, PHP, RADIUS and Subversion. Those users seeking to download the security update can do so from the Apple Web site or by using Mac OS X's integrated update service. Snow Leopard users, however, won't see the security update separately, since the patches were rolled into the Mac OS X 10.6.2 upgrade. More information may be found at http://www.infoworld.com/d/security-central/apples-mammoth-update-patches-58-bugs-667?source=rss_infoworld_news

A CHILD PORN-PLANTING VIRUS: THREAT OR BAD DEFENSE?

On November 10th, *CNET News* reported that there have been concerns over computer viruses being used to plant child pornography on people's computers. One such horror story is that of Michael Fiola, a former Massachusetts state employee whose state-owned work computer was found to contain child pornography images. He was fired and charged with possession of child pornography which, had he been convicted, could have landed him in prison for up to five years. However, the charges against Fiola were dropped after his attorneys demonstrated that his computer was infected by a virus that was programmed to visit as many as 40 child porn sites per minute, a feat that a human couldn't do, even if he or she tried. Fiola's case begs the question "just how serious is the risk? According to a variety of experts, it is indeed possible for malicious software to plant child pornography, but being possible doesn't mean it's likely. Generally speaking, most cybercriminals are motivated by money and there is no clear indication as to how planting child porn on an unsuspecting person's computer would help generate money for criminals. While malware authors may use someone else's computer to access the contraband without running the risk of it showing up if their PC is seized or searched, it's not an effective way to store child porn and remain undetected. Further, a good forensics expert can detect the infection. Investigators can usually figure out if an image was downloaded intentionally, based on other activity that took place on the computer at the time. Additionally, a virus and Trojan horse will likely be able to download multiple images at a time whereas a person who collects child pornography typically acquires it over a period of time. Moreover, several other factors can demonstrate whether an individual really was infected by a virus or Trojan or whether the individual was intentionally acquiring child pornography. A good investigation will look for exculpatory evidence to see if there are other explanations for the images. That investigation should start with making one or more exact copies of the suspect's hard drive and examining those copies to look for evidence of malicious software that could be responsible for the images. This is the first case in the U.S. where the publishers of Bytes in Brief, themselves computer forensics experts, have seen this defense used successfully, and with what appears to be sound evidence. The road to proving that the defendant knowingly and intentionally possessed, received, or distributed child pornography starts with establishing that the images involved are child pornography and ends with establishing that the person charged is criminally responsible for it. For now, the experts have stated that they were not aware of any cases in which botnets were used to plant child porn on other people's computers. But, as with any other security issue, the best defense is to protect your machine against intrusions by keeping your anti-virus and anti-spyware software current. More information, including a recent case that highlights the potential for concern, may be found at

<http://www.cbsnews.com/stories/2009/11/09/tech/main5589403.shtml?tag=cbsnewsLeadStoriesAreaMain:cbsnew>

AT&T LOSES FIRST LEGAL BATTLE AGAINST VERIZON ADS

On November 19th, a federal judge declined to grant AT&T a temporary restraining order that would force Verizon to stop showing advertisements that compare its 3G wireless network coverage with Verizon's coverage. In the company's suit, AT&T alleged that Verizon Wireless' advertisements suggesting that AT&T subscribers cannot access wireless Internet services throughout its network were blatantly false and caused irreparable harm to the company. While AT&T hasn't argued that the maps are incorrect in terms of showing its 3G coverage, the company's primary argument is that Verizon is misleading customers by implying that they cannot use their phones or access the mobile Web when they aren't in 3G coverage areas. According to AT&T, customers can make phone calls and access the Internet from their phones; albeit, through the company's slower EDGE or GPRS networks. However, Verizon has countered by noting that it is simply pointing out the fact that AT&T has not invested enough in upgrading its network to handle increased traffic from smartphone devices. Further, Verizon has claimed that the suit is not based on the truth or the falsity of the ads, but rather because AT&T simply doesn't want to face the truth about its network. Although AT&T has lost this legal battle, it has stated that it plans on continuing with its case. A copy of Verizon's rebuttal to the court may be found at <http://stadium.weblogsinc.com/engadget/files/VerizonTROOpp.pdf>

SURVEY: THIRD OF TEENS TEXT WHILE DRIVING

On November 17th, the Pew Research Center reported that a new survey revealed that a third of cell phone users aged 16 and 17 admitted to texting while driving despite increased publicity over the dangers of doing so. Further, the survey reported that, as passengers, 48% of the teens surveyed admitted that they have been in a car while the driver was texting, and 40% have been in a car when the driver used a cell phone in a way that put everyone in danger. More importantly, some teens fail to understand the risk and many even flaunt laws enacted to prohibit texting while driving. One teen surveyed expressed his belief that texting while driving is fine and went so far as to note that he wears sunglasses so the cops won't see his eyes looking down. This latest report reaffirms a plethora of other studies about the dangers of cell phone use while driving. One such study found that truck drivers who texted were 23 times more at risk of a "crash or near crash event" than "nondistracted driving" while another showed dramatically slower reaction times by two drivers who tried to brake while texting. Currently, several states such as California, Connecticut, Oregon and Virginia have passed laws banning texting or talking on a mobile phone while driving. The U.S. Senate is currently looking at a bill that would give federal dollars to other states that pass similar laws. A copy of the report may be found at <http://pewresearch.org/assets/pdf/teens-and-distracted-driving.pdf>

SUIT OVER SEARCH-ENGINE KEYWORDS TRIES NEW ANGLE

On November 20th, *The Associated Press* reported that Wisconsin law firm Habush Habush & Rottier had filed a suit against a rival firm over search-engine keywords, alleging that its competitor violated privacy laws. In its complaint, Habush contended that Cannon & Dunphy, a rival firm, paid for the keywords "Habush" and "Rottier," in effect hijacking the names and reputation of Habush attorneys. In fact, when a user searched for iterations of "Habush" and "Rottier" a sponsored link for the Cannon firm often shows up, just above the link for the Habush site. And while Cannon acknowledged paying for the keywords, it denied any wrongdoing, stating that it was simply following a clearly legal business strategy. What's unique about this particular suit is the angle taken by Habush. Typically, the practice of paying for keywords on Google and other search engines to boost one company's link over a rival's has prompted legal challenges alleging trademark infringement, but this Habush's suit is based on a Wisconsin right-to-privacy statute that prohibits the use of any living person's name for advertising purposes without the person's consent. Although different, at least one legal expert isn't so sure the angle is a formula for success. Ryan Calo, a fellow at the Center for Internet and Society at Stanford Law School, said the statute seemingly was meant to protect people from having their names and images misused to suggest they endorse or represent something, which isn't the case here. More information may be found at http://www.google.com/hostednews/ap/article/ALeqM5hnlqI2aj9Ux408IS_iA621J9LNigD9C2TC080

FBI SAYS HACKERS TARGETING LAW FIRMS, PR COMPANIES

On November 17th, *The Associated Press* reported that the FBI has issued an advisory that warns law firms and public relations companies of a noticeable increase in efforts to hack into their computer networks to steal sensitive data—a trend that cyber experts say began as far back as two years ago but which has grown dramatically. The attacks are what cyber security experts describe as "spear phishing," attacks that come through personalized spam e-mails that can slip through common defenses and appear harmless because they have subject lines appropriate to a person's business and appear to come from a trusted source. While opening a "spear phishing" e-mail itself does not pose a danger, these messages often contain Web links or attachments – from a photo to an executable program – that when clicked on or opened will infiltrate the network or install malicious programs. Once the hacker is in the network, he or she often plants a computer program that searches for, collects and copies files and sends them to a computer server, usually in another country. The program also may create a back door that will allow hackers to get back in later. And attackers have good reason to go after law firms. According to Bradford Bleier, unit chief with the FBI's cyber division, law firms have a tremendous concentration of really critical, private information. If an attacker is able to infiltrate those computer systems, he or she would have access to a plethora of economic, personal and personal security related information. Often, the hackers target firms that are in the process of negotiating a major international deal, looking for documents that lay out the company's playbook for the deal, or its negotiating positions and tactics. The FBI has noted that this recent increase in attacks should, at the very least, have companies re-evaluating what they put on their networks because hackers are getting more sophisticated. More information may be found at

http://www.google.com/hostednews/ap/article/ALeqM5hsG8BcireHiOQHAdCIW9_LF2KzcgD9C1AB400


Bytes in Brief® is a FREE monthly digest of Internet law and technology news delivered to you by e-mail. For members of the legal and business community interested in Internet law and technology developments, *Bytes in Brief* provides a synopsis of related news and links to sources with more expanded coverage. In the time it takes to drink a cup of coffee, *Bytes in Brief* is designed to make sure you are tracking major developments in this fast moving area.

If staying current in this field is important to you and you find yourself buried under unread magazines, newspapers and journals, *Bytes in Brief* can help you stay in touch without a major outlay of time or expense.

To subscribe, enter your e-mail address into the sign-up box below. It will take you offsite to the *Constant Contact* website, where our opt-in only list is maintained and updated. After you confirm your e-mail address, you will receive an e-mail asking for confirmation that you do wish to become a *Bytes In Brief* subscriber. Once you reply to that e-mail, you will be added to the subscription list.

Subscribe to *Bytes in Brief!*

Email:

Privacy by  **SafeSubscribe**™
For Email Marketing you can trust

Copyright © 2009 Sensei Enterprises, Inc. All rights reserved.