

Information at your Fingertips!

If you are our client, then you know we maintain all of your I.T. assets in our private database and we also make that available to you through our secure web portal. Need to know how many licenses of MS Office you have? How about warranty coverage on a PC or Server? Or what work we performed last month? It's all there for you to view online through the secure portal at www.starpointit.com – click on the support link then click the customer portal.

“As a business owner or executive, I know you don't have time to waste on technical and operational issues. That's where we shine! Call us and put an end to your IT problems finally and forever!”

David Davis, StarPoint IT Solutions – 1-800-869-0135 x101

Latest News

We're Moved

2251 San Diego Avenue, Suite A-150
San Diego, CA 92110

We're Hiring

StarPoint is looking for outstanding I.T. consultants in San Diego!
If your referral gets hired you get \$2500!
See job details at www.starpointit.com/jobs

We would like to welcome to the StarPoint family the following firms:

Grace Hollis LLP
Liedle, Lounsbery, Larson & Lidl
Wilson Getty
SJ Creations, Inc.
Hayes Handpiece Franchises



this issue

Twitter Settles **P.1**

CBS News Report **P.2**

\$100M Scareware **P.3**

Latest StarPoint News **P.4**

Twitter settles FTC case over data security lapses that gave hackers access to user accounts

WASHINGTON (AP) — Twitter has agreed to settle charges by federal regulators that it put the privacy of its users at risk by failing to protect them from data security lapses last year that let hackers access their accounts.

The Federal Trade Commission said Thursday the settlement bars Twitter from misleading consumers about its security and privacy practices and requires the start-up to establish a comprehensive information security program.

No monetary damages were assessed.

The FTC complaint said the breaches allowed hackers to gain administrative control over the online service, which lets users send brief messages called tweets to each other. According to the FTC, hackers were able to view email addresses and other private user information, gain access to user messages, reset user passwords and send phony tweets from user accounts.

At least one phony tweet was sent from the account of Fox News and another phony tweet was sent from the account of then-President-elect Barack Obama offering more than 150,000 followers a chance to win \$500 in free gasoline, the FTC said.

The agency charges the incidents deceived users because Twitter's privacy policy pledged to “employ administrative, physical, and electronic measures designed to protect your information from unauthorized access.”

“When a company promises consumers that their personal information is secure, it must live up to that promise,” David Vladeck, head of the FTC's Bureau of Consumer Protection, said in a statement. One breach occurred in January 2009 after a

hacker used an automated password-guessing tool to gain control of Twitter. The second breach occurred in April 2009 after a hacker broke into a Twitter employee's personal email account, which stored two passwords that were very similar to the employee's administrative password for Twitter.

The FTC said Twitter was vulnerable to these attacks because it used weak, lower case common dictionary words as administrative passwords and failed to take reasonable steps to prevent unauthorized access to its system. Such steps include prohibiting employees from storing administrative passwords in plain text in their email accounts, periodically changing administrative passwords and restricting access to administrative controls.

In a blog post, Twitter General Counsel Alexander Macgillivray said that even before the company reached the agreement with the FTC, it had already implemented many of the security practices highlighted by the agency. He added that the company quickly closed the security holes, notified affected users and disclosed what had happened in blog posts following both incidents.

Macgillivray also noted that Twitter employed fewer than 50 people when the breaches occurred.

“At the time of the incidents, we were ... in the midst of perhaps unprecedented user growth for an Internet company; and, didn't employ the security methods that we use today,” the company said on Thursday.

Twitter said 45 accounts were accessed in the first incident and 10 accounts in the second incident.

Source: JOELLE TESSLER AP Technology Writer

Good News For Early Adopters...

It's good news for business travelers and vacationers alike. The Transportation Security Administration says the iPad won't have to be removed from carry-on baggage at security checkpoints. It's just half-an-inch thick and has no parts that can block images when the machines go through the screening machine.

Electronics that are smaller than the standard laptop, such as the Kindle, Sony Reader, and small notebook computers, can also stay in the bag. But it's not an actual rule. Screeners still have the discretion to ask that the devices be removed in order to further inspect them or the cases they are in.

The TSA recommends checkpoint-friendly bags that have a separate laptop flap that can be unfolded flat on the machine belt.

Shocking New CBS News Report



Reveals Why Your Office Copy Machine Is Actually A Security Time Bomb

This just in: According to a recent CBS news report, copy and multi-function machines in offices contain a huge, unknown security risk that all businesses must address immediately or face the legal, financial, and PR repercussions of a security breach.

A Surprising Fact About Your Office Copier

Nearly every printer, copier and multi-function machine manufactured after 2002 contains a hard drive that stores the images of every document you've ever copied, faxed, or scanned. These document images stay on that machine's hard drive forever and can quickly and easily be reproduced with a little know-how. Surprisingly, this little fact has not received any press – until now.

A CBS Undercover Investigation

In April of this year, a reporter went undercover to a New Jersey copier warehouse that had over 6,000 used copy machines in stock for resale. This investigation reveals a shocking fact – it's incredibly easy for a person to retrieve and reproduce every single document ever scanned, copied, or faxed through the machines available for resale.

As part of the investigation, the CBS reporter pulled 4 random machines that were available for sale and purchased them for approximately \$300 each. These machines were immediately loaded onto a truck and delivered within 2 hours to this reporter's office. Using a free application available online, he was able to access the hard drive of each machine and reproduce the documents within 30 minutes. What he uncovered was unbelievable.

Disturbing Facts Revealed By The Investigation

They discovered that one of the machines was formerly owned by the City of Buffalo, New York, Sex Crimes Division. In no time at all they were able to access over 249,000 documents that passed through that machine, including lists of sex offenders and crime data. Another machine from the Buffalo PD Narcotics Division contained a list of drug raid targets. The third machine was from a construction company. It contained blueprints of buildings, over \$40,000 in check copies, as well as pages of paystubs, names, and the social security numbers of employees.

But the fourth machine was the most disturbing. It was previously owned by a New York health insurance firm and contained over 300 pages of detailed medical records including drug prescriptions, blood tests, and even a cancer diagnosis – all which blatantly violate the new HIPAA laws.

Know What Your Responsibility Is

Before you trade in, resell or dispose of any office copier, scanner or multifunction machine you MUST make sure the hard drive is wiped clean of all information as you would any computer in your office. Failure to do so could result in damaging security breaches and identity theft for your company, staff, and customers. This goes DOUBLE if you use your office machines to scan, fax, or copy social security numbers, credit cards, or medical records of any kind.

As always, we are here to assist you with all things digital. If you are getting ready to dispose of or trade in a copier, scanner, fax, or multi-function machine, give us a call. We can make sure your data is forever erased and inaccessible to criminals looking for an easy hit.

Alleged \$100M scareware sellers facing charges Two years after an FTC complaint, Innovative Marketing is now facing criminal charges

Three men are facing federal fraud charges for allegedly raking in more than US\$100 million while running an illegal "scareware" business that tricked victims into installing bogus software.

Two of the men, Bjorn Sundin and Shaileshkumar Jain, operated an antivirus company called Innovative Marketing, which sold products such as WinFixer, Antivirus 2008, Malware Alarm and VirusRemover 2008. The third man charged, James Reno, ran Byte Hosting Internet Services, the company that operated Innovative Marketing's call centers.

The company's products generated so many consumer complaints that the FTC brought a civil action against Innovative Marketing and Byte Hosting in 2008, effectively putting them out of business.

On Wednesday, a grand jury in Chicago handed down the criminal charges, meaning the three men now face jail time if convicted.

Reno is expected to turn himself in for arraignment, the U.S. Department of Justice said in a press release Thursday. Authorities believe that Jain and Sundin are living in Ukraine and Sweden, respectively.

In a September 2009 e-mail to the IDG News Service, Reno said he was a young and naïve businessman who was taken advantage of by Innovative Marketing. "I made some mistakes, of course," he said, "however they kept us in the dark on a lot of their operation."

According to prosecutors, Innovative Marketing set up fictitious advertising agencies that would buy online inventory from media companies, pretending to represent legitimate companies. They then pushed out ads with hidden computer code that generated scary-looking pop-up messages, designed to look like operating system errors or antivirus scans.

By Robert McMillan, IDG News Service

Have you heard of the Khan Academy?

I recently came across the Khan Academy website through a program that I saw on PBS. Salman Kahn, who created the site, has a mission to educate the world for free. His breadth of knowledge is genius and his ability to explain complex problems in simple terms is short of amazing. An excellent resource for any student or for anyone who wants to learn on a variety of subject matters from finance to physics – all free! Go to <http://www.khanacademy.org/>.

Welcome - Alex Soler

Please join us in extending a warm welcome to Alex Soler, who is the latest addition to our team. Alex comes to us from Brentwood, TN where he worked for Aspect Software. Fluent in Spanish, he led the primary support for their Latin American region. Prior to Aspect Alex worked for Dell where he provided a variety of support services to their consumer, government, small and large business sectors. Alex will support the team by providing desktop support both remotely and onsite for our clients. Please join all of us in welcoming Alex to the StarPoint team.



Majority of Fortune 500 Companies possibly infected with Botnets

Think Fortune 500 companies are on the ball? Think again. According to a startling RSA study released this week, as many as 88 percent of Fortune 500 companies might be affected by botnet activity.

As frightening as that sounds, RSA stands behind those numbers. Sean Brady, manager of the Identity Protection and Verification Group at RSA, says his firm analyzed data stolen by the Zeus botnet from compromised PCs in August. The evidence they found led them to IP addresses and email accounts belonging to the U.S.'s top corporations.

"Domains individually representing 88 percent of the Fortune 500 were shown to have been accessed to some extent by computers infected by the Zeus Trojan," the study said.

It also appears that the smaller company, the higher the threat. The study noted a higher ratio of botnet activity to employee accounts in companies with fewer than 75,000 employees. Protect your organization against malicious malware and spyware damage with StarPoint's StarMON layered security approach.

Email STARMON@STARPOINTIT.COM now and receive an important message with a special offer.