

In This Issue

1. Ten Ways to Protect Your Identity on Campus – 2. Malware – 3. Scams and Hoaxes – 4. Microsoft and Apple Security Updates – 5. Security Newsbytes

1. Ten Ways to Protect Your Identity on Campus*

1. **Lock your door.** This is the single most important way to keep your computer secure.
2. **Mark your property** in a very visible, permanent way. Just as would-be thieves are often deterred by homes bearing “Protected by ... “ signs, so is a computer thief more likely to go for an unmarked laptop.
3. **Don't assume your desktop computer is safe.** Invest in some inexpensive cables designed to tether the CPU to something immovable in the room.
4. **Use password protection.** Adjust your computer settings to prompt you for a password anytime the computer is used. And change that password from time to time.
5. **Don't reveal too much.** Social networking sites such as MySpace and Facebook may ask for your birth date, but birth dates are a boon to identity thieves. Likewise, do not reveal any other personal information on these public sites, or in response to any email requests for your Social Security number, credit card numbers, or other personal information, even if it appears to be from a familiar-sounding company.
6. **Keep thorough records.** If your laptop is stolen, can you provide a full description for the police? Write down your computer's make, model, color, and most importantly, the serial number. You might also need this information in case you want to file an insurance claim.
7. **Install a tracking device.** Use a GPS tracking device that runs invisibly on the computer to relocate the stolen property.
8. **Use a multi-layered security approach.** MyLaptopGPS,** for example, offers six layers of protection, including permanent tagging, GPS tracking, covert data recovery, remote data deletion, stolen property tracing, and property registration, for \$10 per month per computer. Other GPS tracking devices can be purchased individually for \$50 to \$400.
9. **Start shredding** (digitally shredding, that is). Use software, such as Identity Finder,***, to search and preview the personal data on your computer, including credit card numbers, Social Security number(s), birth dates, tax returns and financial aid documents.
10. **Contact your college's IT department about network security.** Many colleges provide security software or other services free to their students. Before you purchase any

computer protection system, check with the IT department of the college to ensure that system is compatible with the college's network.

* <http://www.creditcards.com/credit-card-news/10-ways-to-protect-laptop-credit-card-info-1282.php>

More information: <http://www.creditcards.com/credit-card-news/protecting-against-identity-theft-on-campus-1282.php>

** <http://mylaptopgps.com/>

*** <http://www.identityfinder.com/>

2. Malware

Net-Worm.Win32.Koobface

A worm that attacks MySpace and Facebook and transforms victim machines into zombie computers to form botnets*. Even though the worms currently only infect MySpace and Facebook users, analysts are warning users that the worms are designed to upload additional malware via the Internet. Victim machines will most likely not only be used for spreading links via these social networking sites, but also for other malicious purposes. One variant, Net-Worm.Win32.Koobface.a, spreads when users access their MySpace accounts, and creates a range of commentaries to friends' accounts.

More information: <http://www.kaspersky.com/news?id=207575670>
<http://www.geek.com/facebook-and-myspace-users-hit-by-new-koobface-worm-20080805/>

* **Botnet:** <http://en.wikipedia.org/wiki/Botnet>

XP AntiVirus 2008

The recent wave of rogue anti-malware advertised through Google's Adwords ("malvertizing") is continuing (See 3. Scams and Hoaxes below). This rogue antivirus, instead of protecting your computer from further threats, triggers pop-ups, annoying warnings, and offers false scan results in order to convince you to go to other websites that sell "specialized" products, like spyware. According to Malware Database*, a rogue XP Antivirus 2008 program is now being distributed as "MS Antivirus 2008" with a file name of MSASetup.exe

More information:

http://www.theregister.co.uk/2008/08/22/anatomy_of_a_hack/print.html

<http://news.softpedia.com/news/Rogue-XP-Antivirus-2008-Aggressively-Advertised-by-Google-92404.shtml>

***Malware Database:** <http://malwaredatabase.net/blog/index.php/2008/08/21/ms-antivirus-2008/>

Exchanger.mn a.k.a. EncPk-DA

A Trojan* downloader, embedded in a phony update for Adobe Flash Player called "adobe_flash.exe," which is distributed by fake websites. Unsuspecting users are lured to these websites by the promise of seeing the complete version of equally bogus sensational news stories allegedly from CNN and MSNBC (see 3. Scams and Hoaxes below). The Trojan connects to a malevolent server and installs additional malware.

More information: <http://www.spamfighter.com/News-10853-Fake-Spam-Allegedly-Offer-MSNBC-News.htm>

* [http://en.wikipedia.org/wiki/Trojan_horse_\(computing\)](http://en.wikipedia.org/wiki/Trojan_horse_(computing))

3. Scams and Hoaxes

Fake News Bulletin Spreads Malware

Hackers trying to plant malware on PC's have switched from touting CNN news to pushing breaking stories said to be from rival network MSNBC. The fake messages carry subject headings that include the phrase "Breaking News," along with phony news story headlines, such as "Plane crashes into prep school, hundreds of kids killed." Previously, security vendors have warned users of a massive scam that used messages masquerading as news alerts from CNN, dumping at its peak nearly 11 million messages an hour on users. The criminals who launched that attack are also behind the switch to MSNBC. People who click on the links reach a bogus update, named "adobe_flash.exe", which is actually a Trojan horse.

More information: <http://www.pcworld.com/article/149908/article.html>

Email Account Phishing Scam

Some email scams are so successful that they keep coming back. One of these is an email message that ends with a strong threat: "Warning!!! Any account owner that refuses to update his or her account within three days of this update notification will lose his or her account permanently." Faculty, staff, and students at colleges and universities have proven to be easy prey for these scammers who tailor the email so it appears to come from the campus IT department. None of these messages is legitimate, and no reputable service provider will ask account holders to verify their username and password or request any confidential information by email.

More information: <http://www.hoax-slayer.com/webmail-account-phishing-scam.shtml>
http://www.nyu.edu/its/news/archives/2008/07/phishing_scam_targeting_nyu_em.html
<http://www.helpdesk.ilstu.edu/kb/index.phtml?kbid=1364>

Internet Explorer 7 Update Malware Email

Malicious emails disguised as official Microsoft messages urge recipients to click a link supposedly to download the latest version of Internet Explorer 7. However, the messages are not from Microsoft and clicking the link will instead download and install a Trojan that can modify the Windows registry and other Windows files. The Trojan can also connect to other malicious websites and download and install more malware. The Bad Guys have attempted to make the messages seem more legitimate by including seemingly official newsletter subscription details and secondary links that lead to genuine Microsoft websites. The hackers also use a spoofed email address so that the emails appear to originate from Microsoft.

More information: <http://blog.commtouch.com/cafe/email-security-news/malware-disguised-as-ie7-update/>
<http://www.hoax-slayer.com/internet-explorer-malware-email.shtml>

[**Editor's Note (Reichert):** Updates from Microsoft are available through the Microsoft Update utility built into Windows, **not** via email notification. Don't be fooled.]

Buy Airplane Ticket Online Trojan Email

This unsolicited email advises recipients that their credit card has been charged for an airline ticket ordered via an online ticket service. The message instructs the recipient to open an attached file in order to view an invoice and print out the purchased ticket.

However, the email is not from an airline and the claim that your credit card has been used to purchase an airline ticket is untrue. The attachment contains a Trojan that infects the user's computer. The Trojan creates files on the infected computer, modifies the Windows registry and allows backdoor connections to and from a remote server.

More information: <http://www.hoax-slayer.com/airline-ticket-trojan-email.shtml>

Google AdWords Phishing Scam

This email insists that users should update their accounts by clicking on the embedded link. The sophisticated scam looks official and appears to be from Google AdWords. Email addresses such as support@google.com and adwords-noreply@google.com are used. Clicking on the link will take you to a phishing website hosted in China that closely resembles the real Google AdWords login page. The phishing campaign is being pushed by one of the six large botnets that generate 85% of the world's spam.

More information: <http://www.securecomputing.net.au/News/106862.google-adwords-customers-targeted-in-phishing-scam.aspx>

Hackers Claim to Have Kidnapped Babies in Attempt to Infect Computers

This spam campaign sets out to panic innocent recipients into opening an attachment that is supposed to contain photographs of their kidnapped infant. The emails bear the subject line "We have hijacked your baby," and demand a \$50,000 payment for the child's safe return. The attachment, "photo.zip," contains a Trojan horse, Resex-Fam, a type of malware not dangerous in itself, but which downloads other types of malicious software to the infected computer.

More information: <http://www.sophos.com/pressoffice/news/articles/2008/08/baby.html>

4. Microsoft and Apple Security Updates

Microsoft and Apple provide free security updates for their software products.

Windows: Microsoft issues patches for all Microsoft products on the second Tuesday of each month as well as out-of-cycle patches on any day of the month. The next scheduled release date is September 9th. Check manually too, once every two weeks, to make sure all of the updates have been installed.

More information: <http://www.microsoft.com/athome/security/default.msp>

OS X: Updates are issued frequently, and their contents may differ depending on which processor is in your Mac (PPC or Intel).

More information: <http://www.apple.com/support/downloads/>

iPhones: Must be updated manually:

http://support.apple.com/kb/HT1414?viewlocale=en_US

5. Security Newsbytes

Best Western Downplays Hacker Attack

Whom to believe? Hotel chain Best Western has denied falling victim to a large-scale hacking attack. A report in Scotland's "Glasgow Sunday Herald" claims that the hotel chain was invaded by a hacker who lifted eight million customer records. Data allegedly stolen included addresses, telephone numbers and credit card numbers. The attack was pulled off using a Trojan horse to infect a PC with access to the hotel's online booking system. The Glasgow Herald claims that the personal information of anyone who stayed

in any of 1,312 European Best Westerns since last year was potentially exposed in the hacking. However, Best Western counters that only one of its hotels (in Berlin) was hit and only about 10 customers were affected. Concerned customers are encouraged to call Best Western Customer Care in the US at 1-800-528-1238.

More information: http://www.theregister.co.uk/2008/08/26/best_western_hack/

Malware Infects Space Station Laptops

Computer nasties in Outer Space? NASA has confirmed that malware has indeed managed to get off the planet and onto the International Space Station. The attack code, a Windows worm, “W32.Gammima.AG” that targets online gamers, infected at least one of the laptops used on the station. NASA spokesman Kelly Humphries declined to identify the malware, saying only that anti-virus software detected a worm, but added comfortingly that “it was never a threat to any command-and-control or operations computer.” He refused to detail how the malware snuck aboard, citing “IT security issues,” but other sources speculated that it might have stowed away on a laptop or a flash card.

More information: <http://news.idg.no/cw/art.cfm?id=05DCD2CF-17A4-0F78-31AECA4CAC7F7E6B>

<http://www.informationweek.com/news/security/antivirus/showArticle.jhtml?articleID=210201099>

Copyright 2008, SANS Institute (www.sans.org).

***Editorial Board:** Bill Wyman, John York, Alan Reichert, Barbara Rietveld, Alan Paller.*

Permission is hereby granted for any person to redistribute this in whole or in part to any other persons as long as the distribution is not being made as part of any commercial service or as part of a promotion or marketing effort for any commercial service or product. Readers are invited to subscribe for free at <https://www.sans.org/newsletters/ouch>.