

In This Issue

1. Consumer Awareness: Tips for Wi-Fi Security at Home – 2. Scams and Hoaxes – 3. Microsoft and Apple Security Updates – 4. Security Newsbytes

1. Consumer Awareness: Tips for Wi-Fi Security at Home

Many people rush through setting up wireless home networks to get their Internet connectivity working as quickly as possible. While this is understandable, it is also risky because unless properly secured, wireless networks are a security problem waiting to happen. Today's Wi-Fi networking products don't always help the situation either. Their security features are complicated and can be time-consuming to set up correctly. You may wish to retain the services of a qualified technician to help you be sure the job gets done right. Here are some tips for how you can improve the security of your home wireless network. Next month we'll provide tips for improving Wi-Fi security while on the road.

Replace that old access point. If your access point is older than 2 or 3 years, it probably doesn't include the latest security protocols. At a cost of \$75 or less, an up-to-date access point is cheap insurance against having your computers broken into.

Change the default passwords on your wireless access point. The default passwords are simple, often posted on the manufacturer's website, and well-known to hackers. Change them immediately, and use strong passwords.

Use WPA2 security. Older wireless access points offer WEP and WPA security which provide only weak and unreliable security. Verify that your wireless access point supports WPA2 (Wi-Fi Protected Access, version 2). If it does not have WPA2, don't use it. Get another one that does.

Change the default SSID. Wireless access points use a network name called the SSID (service set identifier). Manufacturers ship their products with the same SSID. While knowing the SSID does not by itself allow a hacker to break into your network, it is a start. More importantly, operating your access point with the default SSID suggests that security has not been handled well, and that encourages hacking.

Do not Auto-Connect to open Wi-Fi networks. Connecting to an open Wi-Fi network, such as a free, public wireless hotspot or your neighbor's wireless access point, exposes your computer to security risks. Most computers have a setting which will allow these connections to happen automatically without notifying you. Make sure auto-connect is shut off.

Enable the hardware firewall on your wireless access point. If your access point does not have a hardware firewall, don't use it. Get another one that does.

Position your access point carefully. It is normal for Wi-Fi signals to leak out through walls of your home. While a small amount of signal leakage is not a problem, the further the signal spills out into the neighborhood, the easier it is for others to pick it up. That is the first step toward someone gaining access to your wireless access point without your permission. Position your access point near the center of your home, rather than near a window or an outside wall.

Turn off your access point if you aren't using it. If it's not turned on, hackers can't break in.

If you don't feel confident about the security of your wireless access point, don't use it. Get advice and answers to your questions from a computer consultant knowledgeable about wireless security.

More information: <http://arstechnica.com/security/news/2008/04/wireless-security.ars>

2. Scams and Hoaxes

Scammers Exploit Swine Flu Fears

Unsuspecting users are receiving a Word document attachment sent by scammers posing as a Center for Disease Control update on the global spread of swine flu. If you open the document, it releases a Trojan, dubbed Agent-AVZQ, which can give control of your computer and the information stored on it to a Bad Guy.

More information: <http://homelandsecuritynewswire.com/single.php?id=8378>
<http://www.f-secure.com/weblog/archives/00001734.html>

Adobe Flash Player Scams Abound

If you visit a website that asks for Adobe Flash Player in order to play a video and you see a handy button nearby for downloading Flash, think before you push it. You may be falling for one of the most common ploys used by hackers to infect computers with malware. Other Adobe Flash Player scams employ salacious or provocative headlines in emails, on websites, social media sites, and in instant messages. These messages will often have misspellings, bad grammar or even broken English, but to make things look more convincing, they feature the official Flash Player button, hijacked from the Adobe website. The safest place to get Flash Player and updates for it is from the Adobe Update site: <http://www.adobe.com/products/flashplayer/>

More information: <http://www.lockergnome.com/windows/2009/07/17/avoiding-adobe-flash-player-scams/>

“Neopets” Under Attack by Identity Thieves

The popular website Neopets has a reputation for being kid-friendly and kid-safe. Neopets lets its members—roughly 25 million people—“adopt” cyber pets and earn points by playing games. Nearly half of players are between the ages of 8 and 12, some are as young as 6, and they communicate with each other while at play. But Neopets has been hit by Internet pirates and a scam that takes advantage of kids willing to pay big for a “magic paintbrush.” Kids are sent a seemingly innocuous email or private message on the Neopets bulletin boards telling them about a secret website that will let them make their own “magic paintbrushes.” But when the child browses to that third-party website, he or she is not downloading and installing a magic paintbrush, but malware.

More information: <http://www.foxnews.com/story/0,2933,530684,00.html>

Work-At-Home Scams Make Their Way to Twitter

Through tweets, email and websites, job hunters are being told that they can make lots of money from the comfort of home using Twitter, and falling prey to Twitter-based job scams. The Better Business Bureau warns that although the large print for such offers may promise big returns, the fine print can cost them every month.

More information: <http://www.sanantonio.bbb.org/article/work-at-home-scams-make-their-way-to-twitter-11445>

Information-Stealing Phishing Email Targets Chase Customers

The Consumer Protection Board (CPB) of New York State has issued a warning to Chase Bank customers that they could be attacked by a phishing scam involving emails that seek personal information on the pretext of upholding new security measures. Customers receive a phony email that asks them to fill in a form with details including personal identifiable information. Citing fresh security measures ostensibly launched by Chase, the fake email explains that it is important that recipients complete the form. Additionally, it displays a web-link and asks the recipients to click on the link. However, the link leads to a fake website where personal information is stolen from the consumers.

More information: <http://www.consumer.state.ny.us/pressreleases/2009/july012009.htm>

3. 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 scheduled release date is August 11th. This is a good occasion to check manually, a practice that you should follow once every two weeks, to make sure all of the updates have been installed.

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

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://support.apple.com/kb/HT1338>

iPhones & iPods: Must be updated manually:

<http://docs.info.apple.com/article.html?artnum=305744>

<http://support.apple.com/kb/HT1483>

4. Security Newsbytes

Online Backup Services Prove Unreliable

IT researcher, Michael Krigsman, set out to back up files to safe, reliable, off-site storage, using Carbonite and Mozy, two of the most respected names in the online backup market. Both products failed miserably, and each one in a perversely different way. Carbonite's simple, set-and-forget solution should make backups easy, but something bad happened along the way, and Krigsman could no longer locate or restore his files. While Carbonite tech support was quite helpful in trying to diagnose and solve the problem, his luck ran out after the issue was referred to Carbonite's product research department. Things started off well with Mozy, but turned sour when the file upload speed slowed to a crawl, making backups no longer practical. Mozy support was unhelpful and responded with canned emails unresponsive to the actual problem.

More information: <http://blogs.techrepublic.com.com/datacenter/?p=1186>

Firefox 3.5.1 Released to Patch "TraceMonkey" Vulnerability

Mozilla has announced the availability of Firefox 3.5.1 to patch a critical security vulnerability that was found in the browser's new TraceMonkey JavaScript engine.

More information: <https://developer.mozilla.org/devnews/index.php/2009/06/30/firefox-3-5-is-now-available-for-download>
<http://arstechnica.com/open-source/news/2009/07/firefox-351-released-to-patch-tracemonkey-vulnerability.ars>

Copyright 2009, SANS Institute (<http://www.sans.org>)

Editorial Board: Bill Wyman, Alan Reichert, Walt Scrivens, 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. We request that redistributions include attribution for the source of the material. Readers are invited to subscribe for free at <https://www.sans.org/newsletters/ouch>.