

**In This Issue**

1. *New Year's Computer Security Resolutions* – 2. *Malware* – 3. *Scams and Hoaxes*  
– 4. *Microsoft and Apple Security Updates* — 5. *Security Newsbytes*

**1. New Year's Computer Security Resolutions****THIS YEAR I WILL:**

1. Install good-quality anti-virus software, anti-spyware, and a software firewall;
  - **More information:** <http://www.microsoft.com/protect/viruses/xp/av.mspix>  
<http://www.clamxav.com/>
2. Patch and update my security software, operating system, and software applications regularly and promptly;
  - **More information:** <http://www.microsoft.com/protect/computer/updates/mu.mspix>  
<http://docs.info.apple.com/article.html?artnum=106704>
3. Learn how to recognize suspicious web addresses;
  - **More information:** [http://cups.cs.cmu.edu/antiphishing\\_phil/quiz/index.html](http://cups.cs.cmu.edu/antiphishing_phil/quiz/index.html)
4. Beware of lesser-known security issues, such as cellphone “bluesnarfing;”
  - **More information:** <http://www.youtube.com/watch?v=dlTjEnrePxc&feature=related>
5. Be careful when using any wireless network—at home or on the road.
  - **More information:** <http://www.youtube.com/watch?v=pgBHjZUKW54&feature=related>  
<http://www.youtube.com/watch?v=ScEaD-SikrM&feature=related>

**THIS YEAR I WILL NOT**

1. Open email attachments unless I know who sent the message and what is in the attachment;
  - **More information:** <http://www.microsoft.com/protect/computer/viruses/email.mspix>  
<http://docs.info.apple.com/article.html?artnum=108009>
2. Click on links embedded in emails unless I know who sent the message, what the link is for, AND where it will take me;
  - **More information:** <http://www.nocpa.org/phishing/phishing-phishingcrime.html>
3. Fall for official-looking emails that ask for personal or financial information;
  - **More information:** <http://www.microsoft.com/protect/yourself/phishing/identify.mspix>
4. Fall for free offers of copyrighted materials which may be tainted with malware, and BTW, may be illegal to use;
  - **More information:** <http://www.docbug.com/blog/archives/000455.html>  
<http://www.copyright.gov/help/faq/faq-digital.html#p2p>
5. Participate in online social networking—or allow my children to—without knowing the risks.
  - **More information:** <http://www.netsmart.org/>

**2. Malware**

**Delf.ctlk.** A Trojan that locks up your PC and demands \$35 to return control to you. Infected computers display a full-screen message that reads "ERROR: Browser Security and Antiadware [sic] Software component license expired [sic]. Surfing PORN, ADULT and some other kind of sites you like without this software is dangerows [sic] and threatens with infection of your computer by harmful viruses, adware, spyware, etc." The extortionists demand that the user dial a 900 number in order to pay the ransom.

**More information:**

[http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9054867&source=rss\\_news10](http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9054867&source=rss_news10)

**Prg Bank.** A Trojan, crafted by a German-speaking hacker crew, which is looting commercial bank accounts by launching focused phishing attacks. The malware is able to mimic the steps the human account owner would take to move money. A variant of the “Prg Banking” malware, the new Trojan has stolen the equivalent of hundreds of thousands of dollars from bank accounts in the U.S., U.K., Spain, and Italy.

**More information:**

<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9053018>

**Trojan.Qhost.WU.** A Trojan that replaces Google text advertisements with ads from another source, depriving Google of revenue and causing problems for end users. Web pages that normally contain advertisements from Google either do not display the advertisement or display an advertisement from a source other than Google.

**More information:** <http://www.spywareremove.com/removeTrojanQhostWU.html>

### 3. Scams and Hoaxes

**IRS Tax Refund Phishing Scam**

Bogus emails that claim the recipient is eligible for a tax refund from the Internal Revenue Service (IRS). The message instructs recipients to click on a link to apply for their refund. The email is not from the IRS, and clicking the link opens a bogus website designed to steal personal information such as credit card details and social security numbers. The scam email itself also uses seemingly official graphics and formatting to fool potential victims into believing its claims.

**More information:** <http://www.networkworld.com/community/node/23371>

**Facebook Deleting Inactive Users Hoax**

A bogus warning is rapidly circulating via Facebook Wall and FunWall posts, as well as email and instant messages. According to the message, Facebook is becoming overpopulated and inactive users will soon be deleted to create more space. The message instructs recipients to send the information to others to prove that they are active members or risk having their account "deleted without hesitation." The contents of the message are completely untrue.

**More information:** <http://www.hoax-slayer.com/facebook-overpopulated-hoax.shtml>

**Photobucket MySpace Comment Virus Warning**

A bogus message warns that a "virus" is circulating via MySpace that can compromise the user's Photobucket account. The message claims that clicking a link in a bogus MySpace comment allows the virus to take control of the user's Photobucket account and delete all images and videos or post nude photos to everyone on his or her friends' list. This ploy is designed to trick MySpace members into revealing their MySpace login details. Clicking links in the bogus Myspace comments opens a fake webpage designed to mirror the MySpace home page, complete with a login form.

**More information:** <http://www.hoax-slayer.com/photo-bucket-virus-warning.shtml>

### 4. Microsoft and Apple Security Updates

Microsoft provides free security updates for Windows, as does Apple for Mac OSX and the iPhone.

**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

January 8th. 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://docs.info.apple.com/article.html?artnum=305744>

## 5. Security Newsbytes

### **One-Fifth of Windows Applications Go Unpatched**

One in five applications installed on Windows PCs are missing security patches according to Secunia, a respected Danish security firm. More than 20% of the applications scanned by its Personal Software Inspector (PSI) utility were open to attack because available fixes for security flaws had not been applied.

**More information:**

[http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=spam\\_malware\\_and\\_vulnerabilities&articleId=9054502&taxonomyId=85](http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=spam_malware_and_vulnerabilities&articleId=9054502&taxonomyId=85)

### **“Crapware” Just As Susceptible To Security Vulnerabilities**

Pre-installed software on new laptops and desktops, dubbed "crapware" by many, can just as easily be the entry point for malware as any other software. Case in point: the HP Software Update tool. For the third time this year, a remotely exploitable, zero-day vulnerability\* has been found in software pre-installed on new Hewlett Packard notebook computers. The flaw, which could allow a hacker to “brick” the system and make it unbootable, affects every HP laptop that shipped with HP Software Update, the computer's built-in patch management utility. HP has issued a patch and instructed users to run HP Software Update on any machine that has the application, even if the update service is never used.

**More information:**

<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9054038>

<http://www.eweek.com/article2/0,1895,2237376,00.asp>

<http://seclists.org/bugtraq/2007/Dec/0273.html>

\*A previously unknown software defect that allows a hacker to gain access to or control over a computer over a network without the knowledge or consent of its owner.

**Editor’s Note (Wyman):** The HP Software Update flaw is the third manufacturer’s software snafu that HP owners faced in 2007. Although HP has released a patch for the latest flaw, you get that patch by running the non-secure HP Software Update tool. That’s the kind of murky Catch-22 that will leave some HP owners wondering: What’s the best thing to do? For the owners of any of the 82 or so models of HP notebooks affected, doing nothing is not a wise decision. Even if you have never used HP Software Update or don’t think you ever will, unpatched vulnerable software ticks away on a computer like a time bomb. Someone else unaware of the risk may use your system and run the defective software; some vulnerable software can pose a threat even if you don’t run it. So, follow HP’s advice. Run the HP Software Update tool on your notebook right away, and if you should reload the software on your notebook, run it again because the HP software CD that came with your system will put back the original flawed tool.

## Malware-Laced Banner Ads Invade Social Networking Sites

If you haven't patched that media player or web browser in a while, now would be a good time. MySpace, Excite, and Blick have been caught serving banner ads that attempt to install malware on machines running unpatched software. People who visit MySpace chat forums using out-of-date web browsers and media player plug-ins, such as Macromedia Flash and QuickTime, are being treated to drive-by downloads of adware, such as Virtumonde\*, WinFixer\*\* and ClickSpring\*\*\* hidden in banner ads on the social networking sites.

**More information:** [http://www.channelregister.co.uk/2008/01/04/malware\\_laced\\_banners/](http://www.channelregister.co.uk/2008/01/04/malware_laced_banners/)

\* <http://research.sunbelt-software.com/threatdisplay.aspx?name=Virtumonde&threatid=15196>

\*\* <http://research.sunbelt-software.com/threatdisplay.aspx?name=WinFixer&threatid=41898>

\*\*\* <http://research.sunbelt-software.com/threatdisplay.aspx?name=clickspring.purityscan&threatid=10115>

## Mac QuickBooks 2006 Deletes Data without Warning

A few weeks ago QuickBooks 2006 for Mac users discovered that a buggy automatic update from Intuit wiped out all files on their desktop. The company warned customers against using QB 2006 for Mac, but later recommended that they shift files from the desktop to other folders. Later a spokesperson for Intuit announced a patch would be available December 31<sup>st</sup> that would fix the flaw by disabling permanently the software's upgrade mechanism. Two days later Intuit issued another warning "that the prior bug re-manifests itself when QuickBooks Pro 2006 for Mac is initiated at public Internet hotspots." Intuit urges users not to run QB 2006 for Mac while within range of a wireless access point until a solution is available.

**More information:**

[http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=spam\\_malware\\_and\\_vulnerabilities&articleId=9054998&taxonomyId=85](http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=spam_malware_and_vulnerabilities&articleId=9054998&taxonomyId=85)

## US Data Breaches Quadruple in 2007

The loss or theft of personal data such as credit card and Social Security numbers soared to unprecedented levels in 2007. While companies, government agencies, schools and other institutions are spending more to protect ever-increasing volumes of data with more sophisticated firewalls and encryption, the investment often is too little, too late. The San Diego-based Identity Theft Resource Center lists more than 79 million records reported compromised in the United States through December 18th--a nearly fourfold increase from the estimated 20 million records reported in all of 2006. Another group, Attrition.org, estimates more than 162 million records were compromised through December 21st worldwide. Attrition reported 49 million worldwide last year.

**More information:**

<http://ap.google.com/article/ALeqM5ip0gRFSz0t677cXwg2z4WRKJ0TgwD8TRVTI00>

[http://www.idtheftcenter.org/artman2/publish/lib\\_survey/Press\\_Release\\_-\\_2007\\_Breach\\_List.shtml](http://www.idtheftcenter.org/artman2/publish/lib_survey/Press_Release_-_2007_Breach_List.shtml)

<http://attrition.org/dataloss/>

\*\*\*\*\*

*Copyright 2007, SANS Institute (www.sans.org).*

*Editorial Board: Bill Wyman, 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>.*