Bits and Bytes

Arkansas' Premier Computer Club

April 2008
Don Hood, President

Bella Vista Computer Club - John Ruehle Center
Highlands Crossing Center, 1801 Forest Hills Blvd, Suite 120 Bella Vista, AR 72715-3016
Web site: www.bvcompclub.org
E-mail: jrc@bvcc.arcoxmail.com

In February 2008, *PC Magazine* published an article titled "72 Tips for Safer Computing". Here are a few of their tips.

Install antivirus (AV) – Keep it up to date, run a regular scan, and let it check your incoming messages. Without this, your PC is virtually guaranteed to be infected.

Update antispyware – This may be bundled with your AV; keep it up to date and scan occasionally. It's a good idea to install a couple of antispyware apps, such as Windows Defender (it comes with Vista) and Spy Sweeper.

Use a bidirectional firewall – Prevent unwanted inbound and outbound traffic on your PC. Two-way firewalls come standard with Mac OS and Windows Vista. Users of older Windows versions should get a third-party firewall such as CheckPoint's.

Don't mix multiple firewalls or antivirus software – It might seem like twice the protection to have two firewalls, but it's likely to double your headaches. Same with dual AV. (Antispyware is another story.)

Allow auto updates – Let Windows and Mac OS update when they want to, since Microsoft and Apple are constantly patching any security holes they find.

Don't accept EXEs – Downloading executable files (ending in .exe, .com, .bat, and .scr) is hard to avoid, but be wary of those e-mailed to you. That goes for .doc and .xls files as well; they can carry macro-based viruses.

Route traffic – If you have broadband service but don't have a router, get one. Wired or wireless, they're cheap.

Change the default – Most routers by default come with a username like "admin" and no password. If you don't change the defaults, anyone on the network could take over as admin.

Stop the broadcast – Your wireless network's name, the SSID (service set identifier), is broadcast to make it easier for devices to get access. Turn off the broadcast. It's not a foolproof precaution, but it keeps nontechie neighbors off your LAN.

WPA is good – Wi-Fi Protection Access (WPA) is the best encryption there is for securing a Wi-Fi connection. If you have a router and device that supports Wi-Fi Protection Setup (WPS), which automates the creation of encryption keys, even better.

Activate the hardware firewall – Your router should support NAT (network address translation) so Internet users scanning for open ports to exploit can't see your computer. It should also support SPI (stateful packet inspection) to distinguish legitimate network traffic from bad. Don't turn these features off.

Root and rootkits – Your system may be clean, but keep your eyes out for info about new rootkits; they are among the hardest malware to eliminate. If you're infected, try Systernals' free RootkitRevealer at www.microsoft.com/technet/systernals/utilities/Rootkit-Revealer.mspx.

Know what's running – windows runs a lot of background programs that are invisible to you. Task Manager (Ctrl-Alt-Delete to view) reveals them, but you can learn more with Process Explorer (free, www.microsoft.com/tecnet/systernals). It spells out XP and Vista processes in plain English.

Call for help – Microsoft will provide free technical support if your question concerns viruses or spyware. Call 866-PCSafety (866-727-2338).

Use strong words – A "strong" password mixes numbers and letters, and not in alphabetical or numerical sequence ("abcd1234" is not strong). Mix the case and throw in punctuation marks. Use an entire phrase if space allows; longer is better. PassPub.com randomly generates strong passwords you can use.

Don't AutoComplete passwords – Browsers will not only store your passwords but also fill them in for you. This is a bad idea on a shared or office-based PC. In Foxfire, use the master password instead. In IE, go to Internet Options, click the Content tab, and go to AutoComplete settings to disable.

Beware of greeting frauds – Online holiday greeting cards are great for phishers. Disreputable sites can collect info from the people who send cards, and then again from the recipient who clicks to watch one. Stick to the Hallmark store. Or just send cash.
Beware of pop-up security fakes – Ever been surfing along and get a pop-up window telling you to scan or disinfect, and offering a handy product to do so? Seem too good to be true? That's because it is – it' adware.
Check rogue software – Software you install may be stealing your information – especially software that claims to help you by finding spyware! If you suspect a program, check it against the list of known bad-guy applications at www.spywarewarrior.com.
Look for the lock – If you're going to send personal information via a Web site you want to make sure the site encrypts that traffic. Look for the https (notice the "s") in the URL, and a lock icon in the address bar or status bar. Don't send any info – such as a credit card number – unless the site is encrypted. However, even the bad guys can run an encrypted site. Just 'cause it's secure doesn't mean you can trust it.
Eat your cookies – In the past, cookies caused plenty of worries. Now, however, they're usually harmless – without them, you'd be entering a lot more passwords on sites you visit all the time. However, regular checks by your antispyware software will clean out the ones you don't want tracking your surfing.
Get a secondary e-mail address – The proliferation of free Web-based e-mail from Google, Yahoo!, Microsoft, and others means there's no excuse for giving out your regular e-mail to anyone but friends.
Don't reply – Never, ever, ever send a reply to a spam. Even if it's for a product you want. Doing so confirms you read it, and your address goes on the spammers' list for eternity.
Know your rights – No one reads end-user license agreements (EULAs), the legalese that pops up when you install a program, but you know you should. Check them out with EULAlizer (free, www.javacoolsoftware.com). It analyzes EULAs to point out potential problems.

You can read the entire article at www.pcmag.com/article2/0,1759,2254028,00.asp

==========

Grisoft has just released version 8.0 of their Internet security products. As of April 1st there was nothing on the Web site to indicate they will be offering a free version. The only free version available for home use is version 7.5. Avast (www.avast.com) and AntiVir (www.free-av.com) still offer a free antivirus program.

Adobe has just launched a Web-bases photo storage and editing program called Photoshop Express. The Web site is www.photoshop.com/express/landing.html. If you want to read what c/net has to say go to www.news.com/8301-10784_3-9903446-7.html.

There are a lot of presentations posted on the Club's Web site at the link titled Meeting Presentations. We thought it might be helpful to update some of the presentations that are a little out of date. So far we've completed two; Buying Electronic Stuff and Computer Security.

The first eight hour Basic Computing class using Windows Vista is scheduled for May 13.

Having a problem with your computer? Having a problem doing something on the computer? Stop by one of the Open House Help Clinics we have at the John Ruehle Center and see if we can solve your problem. These clinics are from 10 a.m. to 1 p.m. on the first Saturday and the third Wednesday of the month. The clinics are open to the public so you can invite a friend or neighbor. There has been a significant increase in the number of people taking advantage of this service. If everyone arrives during the first hour there will probable be a wait.