Bits and Bytes

Arkansas' Premier Computer Club

January 2011
Dick Wenzel, 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

Here's a web site you might want to visit and add to your favorites folder —www.ic3.gov. That's the address for the Internet Crime Complaint Center. If you're not familiar with this site here's what they have to say about their organization.

"The Internet Crime Complaint Center (IC3) is a partnership between the Federal Bureau of Investigation (FBI), the National White Collar Crime Center (NW3C), and the Bureau of Justice Assistance (BJA).

IC3's mission is to serve as a vehicle to receive, develop, and refer criminal complaints regarding the rapidly expanding arena of cyber crime. The IC3 gives the victims of cyber crime a convenient and easy-to-use reporting mechanism that alerts authorities of suspected criminal or civil violations."

On the home page there are links to the FBI, NW3C, and BJA. There are two other helpful links on the home page. The first link takes you to an area of the site that provides "Internet Crime Prevention Tips". The second link takes you to an area that describes the current and ongoing Internet trends and schemes. While the cyber criminals are becoming more and more sophisticated, a little common sense can be your best defense against becoming a victim. When you're on the Internet, be careful what you click on. Even on reputable web sites malicious links can be located on the page outside of the article you're reading. The one thing you never want to do is click on a popup ad—use Alt+F4 to remove the ad from the screen. If that doesn't work, close the browser or, as a last resort, shut down the computer. Any time you experience suspicious computer activity while on the Internet, you should seriously consider doing a complete antivirus and malware scan before you shut down the computer.

There's no reason to be paranoid about online shopping, you just need to be extra careful and follow a few simple rules. The most important rule — never enter personal information on a web page that is not secure. It's absolutely essential that you check for the two indicators that are displayed on a secure web page. Do you need to be concerned about entering your credit card information on a secure web page? It's safer than letting your server in a restaurant disappear with your card for five minutes. If you want to become a regular Internet shopper consider obtaining a credit card (not a debit card) from your local bank that you use only for Internet purchases.

Here are some additional issues unique to online shopping. Three common ways attackers can take advantage of online shoppers.

Targeting vulnerable computers — If you don't take the necessary steps to protect your computer from viruses and malicious software (malware) an attacker may be able to gain access to your computer and all of the information stored on the hard drive. It's equally important for the vendors to protect their computers to prevent attackers from accessing customer databases. While you don't have any control over the vendors operation, watch the news for reports about successful data breaches.

Creating fraudulent web sites and email messages — Attackers can create malicious web sites that appear to be legitimate or email messages (phishing or spoofing) that appear to have been sent from legitimate individuals, companies or organizations. Charities are especially vulnerable after natural disasters. Attackers create these malicious web sites or email messages in an attempt to obtain personal and financial information.

Intercepting insecure transactions — If you or the vendor don't use encryption, an attacker may be able to intercept your personal information as it's being transmitted.

To help protect yourself while shopping online, do the following.

Make sure your firewall is operational, your antivirus program is up to date, and that you have several good malware detection and removal programs. The data base for your antivirus program should be updated every time you start your computer. Periodically check for a newer version of your antivirus program. After making sure your antivirus program and malware detection and removal programs are up to date, scan your hard drive for viruses and malicious software.

Keep your operating system and all the programs you have installed on your computer up to date to eliminate known problems and vulnerabilities an attacker could exploit. On the second Tuesday of every month Microsoft provides updates to your operating system, Microsoft programs, and the hardware installed on or attached (like printers) to your computer.

This is a more difficult task. Make sure the settings for your operating system, firewall, antivirus program, malware detection and removal programs, browser, and email program are configured to provide maximum protection without adversely affecting functionality. You'll probably need to seek the advice of a knowledgeable person to accomplish this.

As mentioned earlier, make sure you're on a secure web page before you provide personal information.

Do business with reputable companies. If you're not familiar with a company, Google the company name and use the information to evaluate their legitimacy. Also, take the time to read their privacy statement and review their site certificate, especially the "issued to" information. Finally, all good companies will provide a toll free telephone number and a physical location.

When making purchases on the Internet always use a credit card, not a debit card. Reputable companies will not run your credit card until they ship your purchase. More important, credit cards provide you more protection if a problem arises.

Finally, make copy of the Purchase Order Number, the confirmation email, and shipping information. Use this information to check your credit card statement. If you use a dedicated credit card from your local bank it's easy to cancel the card if necessary.

We're still soliciting suggestions for Bits and Bytes topics, classes, workshops, and meeting presentations. Try using the red suggestion box located on the table at the back of the room—it's very user friendly.

Having a problem with your computer? Having a problem doing something on the computer? If you're a Club member 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. If you're not a Club member you're welcome to join the Club and take advantage of this service.

ended up contacting the Microsoft Volume Licensing Service Center after having this same problem with six staff accounts. They sent me the following reply which walked me through solving my issue:

We reviewed your agreement, and we were able to determine that you've activated your Software Assurance benefits for TechNet SA Managed Newsgroup, but not necessarily your actual subscriptions. I got in contact with the TechNet Team (800-344-2121, M-F 5:30 AM-5:30 PM PST) who confirmed that you aren't using any of your TechNet subscriptions associated to your agreement. To assign and activate the subscriptions from the Volume Licensing Service Center (VLSC) website, please follow these steps below:
1. Sign onto the VLSC website at https://www.microsoft.com/licensing/servicecenter with your Windows Live ID.2. Click on "Subscriptions" at the top menu bar. 3. On the following page click on "Click here to visit the Relationship Summary and select a License ID to view or manage your Technet subscriptions."4. The link will redirect you to your “Relationship Summary” page. Click on the desired license ID.5. On the following page click the “click here” link next to “Technet Administration”. Please note that this will bring up a pop up window and you may have to disable any pop up blockers. 6. On the following page highlight the desired license row so that it turns yellow and from the drop down menu select "view Details" and click on "OK"7. On the following page you may manage your Technet subscription.
The TechNet Team also explained that they can assist you over the phone to activate the subscriptions, as well as answer any questions you may have in regards to your downloads and keys associated to the subscription.

After you receive the "Congratulations! You have successfully registered this license and/or media. message you should receive an email within 3-4 business days.