

Bits and Bytes

Arkansas' Premier Computer Club

August 2010
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.arcoxml.com

The following articles are from the August 6, 2010 Cloudeight *InfoAve Premium* newsletter.

Just a click away

Windows all versions

What's the first thing you learned when you first started to use a computer? If you think about it, the first thing you learned to do was to click things. You have to click an icon to open your email or browser. You have to click a link to go to a web page. All of us, when we first start to learn computers are click happy. It's fun. How many other things can you do it life and get instant results? On a computer, you click something and something usually happens.

The trouble is that clicking becomes a knee-jerk reaction. There's just something fascinating about a hyperlink. You just want to click it. How many of you clicked the previous sentence? It looks like a link, but it's not. And we hope by now you trust us enough to know we're not going to put any dangerous links in our newsletters. But admit it, even if you didn't click on that sentence, you were tempted to, right?

Criminals and pranksters and spammers - all of the malevolent ones who lurk on the Internet, prey on those who just cannot resist a link. And even those of us who know better than to click links when we shouldn't, sometimes find ourselves wondering where the link leads to.

Despite what some experts say, if someone gets their identity stolen it's by clicking a link that leads to a phishing site.

The quickest way to get your computer infected with bots, viruses, spyware, adware and malware is to click links without thinking. Even if you have the best antivirus and the two best antispyware programs installed and updated on your computer - you shouldn't be clicking links in untrusted emails or Web sites of which you're not sure.

There are new viruses and Trojans being spread around the Internet that are highly evolved. They appear to be legitimate programs, and install as legitimate programs, but once installed they proceed to shut down your security programs (antivirus, antispyware, etc.) and proceed to unload their nefarious bundle unto your computer. And once that happens, you're computer is helpless. The virus can spread so fast, by the time you realize what's happening, it's too late. A very good friend of mine had that happen to him. He clicked a link in an email that he shouldn't have - it appeared to have come from a friend. By the time he called me, it was too late. He had to format his computer and reinstall Windows - and three weeks later he is still reinstalling all his programs because he didn't listen to me when I told him to keep a good, mirror-image backup. He does listen to me now though.

My friend is not a beginner. By anyone's standards he's very smart and very careful. But because one time he didn't think before he clicked, it cost him a lot of time and a lot of aggravation. It could have cost him a lot more.

Whether you're talking about computers or the Internet - everything is just a click away. Not thinking before you click a link could cost you a lot. Software programs cannot think - but you can. Antivirus and antispyware can only protect you from malicious files and programs - but they cannot protect you from yourself.

Yes, when you're on the Internet everything is just a click away - and so is having your computer ruined, your identity stolen or your bank account drained.

Think before you click a link.

The YouSendIt spam

All Windows users

Recently a very aggressive virus is being spread by bots across the Internet. It pretends to be from a respectable site called "YouSendIt", which provides a service that allows users to send very large files without attaching them to email. The real giveaway is that the email, which purports to be from YouSendIt, actually carries an attachment, which is a virus or a Trojan. If you click the attachment, and you're not protected by a good, updated, antivirus program, you'll infect your computer.

On Thursday, our mail servers received over 200 of these emails, we deleted them all of course. These infected spam emails are being distributed by the hundreds of millions, so if you haven't seen one yet, you will see one soon.

The body of the email contains a short message which says, something like, "Barry Smith has sent you a file with YouSendIt.". The names are random so it may be Molly Jenkins, or Andrew Willis etc. The mail claims to come from YouSendIt, but the email address is the same address as the person who supposedly sent it - just the way YouSendIt does it.

YouSendIt is a reputable site, but this spam wasn't sent by YouSendIt. YouSendIt.com is just the victim - and if you open the attachment, you'll be the victim too.

If you get an email that claims that someone has sent you a file using YouSendIt, delete it. Don't open the attachment. The attachment is a form of zip file and it contains a malicious payload - if you open it and your antivirus doesn't detect it, your computer will be infected.

This is a good time to remind you again - NEVER open an attachment unless you're sure you know what it is and who sent it to you. Email addresses can be faked and it may well look like a friend has sent you an attachment. If you weren't expecting it, don't open it. Verify it first with your friend. It's too bad that things have to be this way, but that's the way they are. It may well be that your friend never sent you an attachment even though the mail appears to have come from him or her. It's better to wait and verify, than to take a chance with an attachment that contains a malicious payload.

If the email comes from an email address you don't recognize, it's a no-brainer: DO NOT OPEN IT!

Here's something else to remember when you're bouncing around the Web looking for information. Do not click graphics or other media that are outside the text of the article you're reading. The majority of what you see outside the article you are reading is third party advertising. In many cases the web site you're on does not control what's being presented. Therefore, if you do click something you have no way of knowing if it's safe or malicious. Links within the text of the article you're reading are probably 99.99% safe. The best advice; look, read, think, don't rush, and use common sense.

=====

The editor of the Bits and Bytes is suffering from a mild case of writers block. If you have a topic you would like to see covered in the newsletter, add it to the Suggested Topics for Bits and Bytes Articles sheet located on the table at the back of the room.

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. Starting September 1 these Open House Help Clinics will be for Club members only.