



this issue

Top 13 End-User Tips to Stay Secure **P.1**

Upcoming Events **P.1**

Cool Tools **P.2**

Upcoming Events

Microsoft Office 2010 Sneak-Peek

A preview of the new features of
Microsoft Office 2010.

- Linked Notes
- Co-authoring
- Conversation View
- Excel Sparklines
- Backstage View

Thursday, June 17th

8:30AM-10:30AM

Computer Technologies

740 Pilgrim Parkway Ste L3

Elm Grove, WI 53122

[REGISTER TODAY!](#)

(262) 789-8210

register@ctaccess.com

Computer Technologies of WI, Inc.
740 Pilgrim Parkway L3
Elm Grove, WI 53122
262-789-8210 ph
262-789-7356 fax
www.ctaccess.com

Top 13 End-User Tips to Stay Secure



**Scott
Hirschfeld**

Technology security lies mostly in the hands of the person using the technology. This was the focus of a recent RSA technology panel comprised of Steve Wozniak, Co-founder of Apple; Bob Sullivan, technology writer for MSNBC; Craigslist Co-founder, Craig Newmark; and Hugh Thompson, head security guru for People Security. Despite all of the efforts of IT people and security specialists, these experts agreed that the most effective prevention against IT security threats is found in educating the end-user. So, how do we stay safe? Here are my...

Top 13 End-User Tips

1. Don't be tempted by SPAM. Sometimes those headlines are pretty tempting. Maybe I really do want a Rolex! Or, maybe that salacious headline is just a little bit too tempting. Following that momentary urge to check it out might just put your PC out of commission. Or worse yet, it might allow it to fall into the hands of botnet provider who will sell access to your PC to the highest bidder. A very high percentage of SPAM is geared at just this purpose.

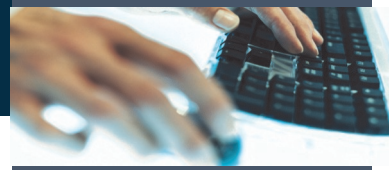
2. Don't unsubscribe. If you don't clearly remember signing up for that newsletter, don't unsubscribe. Often the unsubscribe button will

generate more SPAM from other sources, or will even hijack your machine.

3. Be savvy with attachments. Never open an attachment if you have any doubt at all that it came from a legitimate source and was sent directly to you from someone you know personally. Unless you have a friend named "UPS Update" who called you and said he was sending a file, don't open it! Attachments that are of types EXE, ZIP, COM, XML, or BAT can be especially dangerous. Do not open them without direct knowledge of their content, and confirmation that the sender intended to send them to you. These types of files can execute code on a PC that can do great damage.

4. Don't follow that Link. Much like attachments, links are dangerous. If you think the email might be legitimate, go to the link by googling it or hand-typing the URL you already know, not by clicking the link. These types of emails are known as phishing scams, and no matter how legitimate they look, they can take you to a site that will collect passwords, credit card numbers, and other personal information. Following a bad link can lead to your bank account being emptied before you even blink. Large corporations like Microsoft, Symantec, and your bank never send links.





5. Always look for the lock. Whether it is banking, or online shopping, always look for the security lock in your browser. This indicates that the site uses encryption which is a must. Also, make sure it is a reputable, recognizable company. Look for 3rd party seals of approval like eTrust or BBB. And, make sure the phishing filters are turned on in your browser.

6. Stick with reputable sites. Much of the gunk out there comes from obscure sites that don't have very good security and have been hacked. The hacker then places malicious code on the site, so that when you go there, you are infected with spyware. Avoid obscure foreign domain names as they have a higher likelihood of illegitimacy.

7. Don't load that update. If you get a notification that you need to update something, even if it looks like it comes from your PC, don't click on the update box to load it. Choose to go into the application and request and update from there. For instance, go to Microsoft Update on your machine and tell it you want to update rather than clicking on the bubble and approving it. Go to the Adobe Update Tool in your programs list and tell it to do the update. This can save you from loading some nasty stuff. Follow the same procedure if you get a notice about anti-virus updates.

8. Pop-ups are dangerous. If you get a pop-up window asking you to approve or follow a link avoid clicking it. If the popup does not have an option to delay or cancel the action, be VERY careful. This is the latest manifestation of Spyware. It pops up and pretends to be a legitimate update to your anti-virus. It gives you no way to cancel or deny it. If these characteristics match a popup that comes up on your screen while browsing a website, the best course of action is to shut you machine off with the power button. This sounds drastic, but it can avert disaster. Legitimate programs always give you a way to close, delay or cancel.

9. Bad behavior can make you a magnet. This kind of goes without saying, but sites that host inappropriate material come with a higher risk of infection. Illegal movie, music, porn sharing sites, and even some more obscure social networking sites, are known risks.

10. Never store your passwords. The stored passwords on your PC are relatively easy to access, particularly on Windows XP. If you want to store passwords use an encrypted password utility such as Roboform to manage them.

11. Make sure you are up-to-date. Keeping your Microsoft operating system (XP, Vista, or Win7) up to date goes a long way to preventing issues. Microsoft releases security updates at least once a week and these should be loaded immediately. Making sure your anti-virus and other security programs are up-to-date is another must. Businesses should have a managed approach to insuring these updates are loaded on all machines, the server, and other critical systems regularly.

12. Don't operate your computer as an administrator. One of the best ways to stay secure is to configure workstations to operate at a lower level of security than administrator. This insures that no software can install on your machine, unless an administrator authorizes it. This keeps 95% of spyware and viruses off of the PC. Almost nobody does this, due to the hassle of having to login as administrator to update or install new software, but it is good IT practice and greatly reduces your security risks.

13. Call CT. If you have concerns about a particular risk, give us a call. Preferably before you click that button!

Scott Hirschfeld is Vice-President of CTAccess/Computer Technologies of Wisconsin. Please contact Scott at scotth@ctaccess.com or 262-789-8210.

SOFTWARE Monthly Picks

Bing Maps is not just an online mapping program that uses satellite images, street views and 3-D images to give you a full picture of the location you are searching for, which is all pretty cool by itself. You can use Bing Maps to help manage & track the location of your mobile fleet. Try using map apps to add current traffic and construction information plus nearby restaurants, hotels and businesses on the route you are headed. You might just find a new favorite mapping program.

EYE ON IT Cool Tools

Copy2Contact is a great tool to help you quickly and easily save new contacts and appointments from an email to your contact list or calendar. No more re-typing or cutting and pasting. Simply highlight the text and use the Copy2Contact shortcut key to instantly create a new appointment on your calendar or add contact info to your address book. Try it for free for 14 days at www.copy2contact.com.