



The Award Winning Monthly Publication of the Mountain Computer User Group

Vol.11- Issue #11

New On The Website

Process Explorer - Does similar things as Task Manager except on steroids, great for tracking down resource, task, and performance issues.

Space Sniffer (the web address is http://www.uderzo.it/main_products/space_sniffer/index.html) - This program is similar to WinStatDir in that it scans a disk producing a display of space allocation and allows for a zoom into user specified directories.

What U C Inside!

What Would We Be Without Technology?	Page 2
The Overlooked Risks Of Staying Logged In	Page 3
Bits & PCs Swap Shop	Page 4
Tom's Tips	Page 4
Is Identity Theft In Your Future?	Page 4
Using Caution With USB Drives	Page 6
Birthday's, Anniversaries & Calendar.	Page 8

COMING NOVEMBER. 14th - THE LATEST IN MOBILE COMPUTING

I know that everyone enjoyed our presentation in October by Richard Botting and Art Frenz. It was interesting to find out what all you can do with a Microsoft Excel spreadsheet.



This month on November 14th, Jim Bell, past-president and a frequent presenter to the Mountain Computer User Group will do a special presentation on mobile computing. He will address some of the latest technologies making the headlines in the coming Christmas season. He will define, compare and evaluate the advantages and disadvantages of smartphones, e-book readers, tablet computers and netbooks. These devices share many common features but each has it's own strengths and weaknesses. Anyone considering purchasing one of these devices or just wanting to find out what everyone is talking about will enjoy the program. As always, a key part of the session will be the questions the audience brings to share.



Mountain Computer User Group
P.O. Box 474
Young Harris, GA. 30582



Officers for 2011

President

Art Frenz mcugUsers@gmail.com

Vice President

Randy Gehring

Past President

Jim Bell

Secretary/Treasurer

Diane Frenz

Publisher/Editor

Tom Allen

Webmaster

Randy Gehring

Board of Directors for 2011

Richard Botting

George Donegan

Tim Cassidy

Vacant

MCUG Monthly Meeting Schedule

The regular monthly meeting of the Mountain Computer User Group (MCUG) is held on the second Monday of every month, at 7 p.m., in the Wilson Lecture Hall (Room 201) of the Goolsby Building on the campus of Young Harris College in Young Harris, GA.

All regular monthly meetings and SIGs are open to everyone regardless of membership status.

MCUG Membership

Annual dues are \$20 and extend membership privileges to two (2) members of a household. Membership privileges include: special discounts on vendor products, access to products for evaluation and review, and association with a great bunch of people.

Affiliation

The Mountain Computer User Group is a member of APCUG, a nonprofit international organization dedicated to promoting communications between PC user groups and the computer industry.

Group Purpose

The Mountain Computer User Group is a nonprofit, tax-exempt educational organization without corporate or vendor affiliation. Its purpose is the encouragement and advancement of computer information and knowledge through "users helping users".

Where Would We Be Without Technology?

by: Art Frenz, club president

Everywhere we go we stay connected.

Remember when the only phone you could use on the road was a pay phone. It is rare to see one now days. That pay phone has been replaced by newer generations of technology. Technology is everywhere and it isn't going away. Let's face it; we live in a high tech world. So, when preparing for our vacation it seemed like Diane and I did our normal packing but then we had to make sure we had everything we needed in the order to stay connected.



First, the smartphones, make sure we have the chargers. Next don't forget the cameras, mine uses AA batteries, Diane's has a charger. Can't forget the laptop. Per the airlines we need to make sure the laptop computer bag meets "checkpoint friendly" standards. Had to buy a new back pack so it had a designated laptop only section that completely unfolds to lay flat on the x-ray belt.

We need our i-pods for the long flight and definitely the e-reader. Remember to pack the chargers and power cords for all this stuff. And, just in case, throw in a couple of flash drives. Now do we have everything? Two smart phones, one charger, 2 cameras, batteries and charger, one laptop, power cord and wireless mouse, 2 i-pods and one power cord, one kindle, can use the smart phone power cord and 2 flash drives. Oh yes, one more thing, our clothes!

Happy Traveling!

The Overlooked Risks of Staying Logged In

By Leo Notenboom on March 20, 2011

Article Source: <http://articlesbyleo.com/>

Have you ever checked your e-mail on a friend's computer, public computer, or even display model at the store, only to wonder later if that was a wise move? Is your information safe, or can someone use cookies to retrieve your log in information and access your account?

It depends on what webmail service you're using. But regardless, you may very well be at risk with any account that requires you to login.

There are three important questions that apply here:

- What does the website store in a cookie?
- How long does the website keep you logged in?
- Is the browser configured to remember passwords?



Each website determines what is and is not saved in cookies. It is possible for a site to use a cookie to save a password; however, this is poor security as anyone with access to the machine could access your account. Most commercial systems don't use this approach.

A password may be encrypted and only make sense to the service in question, but not decipherable to the user. Or, the cookie may use information to access the account that is not related to your password, but related to data contained in the service's computer. Either way, it is unlikely a stranger can access your password through cookies saved on the computer.

The greater risk comes from the way most sites allow you to stay logged in for "a while" so that you don't have to re-enter your information each time you click through different pages on the site or temporarily browse to another site. Some servers, such as banks, keep that length of time short, others keep it fairly long. The result is the same - during that time anyone can walk up to the computer and access your account.

And the solution is very simple: always remember to sign out of your account so no one else can use it.

Finally, make sure you don't allow the browser to remember your password - typically an option you check when you sign in, or an optional feature of the browser or both. If you allow either, anyone with access to the machine can use a utility program to recover your password.

If you choose to log into your account on a public computer, or even that of a friend, understand you are taking a risk and extra caution is necessary. Make sure to log off completely when you are done, and never allow the browser to save your password.

Get more free tech help and advice from Leo Notenboom by visiting <http://ask-leo.com> With over 30 years of industry experience, including an 18 year career as a software engineer with Microsoft, Leo gives real answers to real questions from ordinary computer users at Ask Leo! Subscribe to Leo's newsletter at

http://ask-leo.com/leos_answers_newsletter.html

BITS & PCs

We have no items for sale this issue.

If anyone is interested in selling or purchasing an item please email me (Tom Allen) at mcugUsers@gmail.com. It does not have to be computer or electronic related but these computer or electronics related items will have preference when there is a space issue.

Tom's Tip of the Month

For all of you who are like me and buy items, say, from Home Depot, and have your receipt but do not recognize the item from the one line description on the receipt, I have a means to determine what it is. Get on your browser and go to Homedepot.com and enter the UPS code shown on your receipt. The item and its description should come up for you to peruse. For items purchased elsewhere the same procedure should work when using the website for that particular store. I hope that this helps all of you who are plagued by this idiosyncrasy. I hope that I am not the only one that does this.

Is Identity Theft in Your Future?

By Barney Babin, a CCCC (Cajun Clickers Computer Club) member and instructor for XP, Vista & Win 7 Workshops

August 2011 issue, Cajun Clickers Computer News

www.clickers.org ccnewsletter@cox.net

Now that hackers are running rampant not only attempting to access your computer, but your accounts via commercial entities, what is a person going to have to do to assure themselves that their credit is still in good standing?

First of all, what is identity theft? According to the Federal Trade Commission (FTC), "Identity theft occurs when someone uses your personally identifying information, like your name, Social Security number, or credit card number, without your permission, to commit fraud or other crimes."

The FTC estimates that as many as 10 million Americans have their identities stolen each year. In fact, you or someone you know may have experienced some form of identity theft.

The crime takes many forms. Identity thieves may rent an apartment, obtain a credit card, or establish a telephone account in your name. You may not find out about the theft until you review your credit report or a credit card statement and notice charges you didn't make—or until you're contacted by a debt collector. If your credit card or Social Security card is stolen, simply asking the Social Security Administration or credit card companies to assign you new numbers will not solve your problem.

While on vacation in June, one of my online email accounts was hacked on a wired, not wireless, access point in my hotel room. I immediately performed some of the steps below and have had no repercussions. First, immediately change all passwords on

compromised internet accounts, email accounts, etc. - and be sure that they are "strong"

passwords, which can be verified at Microsoft, among others, at www.microsoft.com/security/pc-security/passwordchecker.aspx

Next, contact the fraud departments of each of the three major credit bureaus listed below and report your stolen identity. Ask that a "fraud alert" be placed on your file and that no new credit be granted without your approval.

Equifax Report fraud: 1-800-525-6285
Order credit report: 1-800-685-1111
Website: www.equifax.com/



Experian Report fraud: 1-888-397-3742
Order credit report: 1-888-397-3742
Website: www.experian.com/



TransUnion Report fraud: 1-800-680-7289
Order credit report: 1-800-916-8800
Website: www.tuc.com/



Next, if any accounts have been fraudulently accessed or opened, contact the security departments of the appropriate creditors or financial institutions and close these accounts.

Finally, file a report with your local police or the police where the identity theft took place. Get a copy of the report in case the bank or the credit card company requires proof of the crime later on. Also contact the fraud hotlines of the Social Security Administration at 800-269-0271 or www.ssa.gov/oig/guidelin.htm and of the Federal Trade Commission at 877-382-4357 or www.ftc.gov/idtheft or which includes a video that includes a cornucopia of useful information: www.ftc.gov/bcp/edu/microsites/idtheft/video/avoididentity-theft-video.html

You should get a free annual credit check from the three bureaus above by logging onto the website www.AnnualCreditReport.com/, which requires your social security number. Do not get the report from all three at once, but stagger the three reports out over a one

year interval as assurance that all is well throughout the year. This report will not have the credit score, but there is now a new website that will obtain this information for you free from Experian, www.quizzle.com/, — and you do not have to give your social security number. You establish an account, give the information requested, answer some questions to verify information from Experian, and when you have answered the questions correctly, both the credit report and the credit score is given to you. Of course, they will try to sell you ways to increase your score, protect your identity, etc. but you are not obligated to do this.

We may not be able to stop all hacks, but, as you can see, there are ways to lessen the impact. The responsibility falls upon us to initiate these actions.

Using Caution with USB Drives

Author: Mindi McDowellNational Cyber Alert System

Cyber Security Tip ST08-001April 2011



USB drives are popular for storing and transporting data, but some of the characteristics that make them convenient also introduce security risks.

What security risks are associated with USB drives?

Because USB drives, sometimes known as thumb drives, are small, readily available, inexpensive, and extremely portable, they are popular for storing and transporting files from one computer to another. However, these same characteristics make them appealing to attackers.

One option is for attackers to use your USB drive to infect other computers. An attacker might infect a computer with malicious code, or malware, that can detect when a USB drive is plugged into a computer. The malware then downloads malicious code onto the drive. When the USB drive is plugged into another computer, the malware infects that computer.

Some attackers have also targeted electronic devices directly, infecting items such as electronic picture frames and USB drives during production. When users buy the infected products and plug them into their computers, malware is installed on their computers.

Attackers may also use their USB drives to steal information directly from a computer. If an attacker can physically access a computer, he or she can download sensitive information directly onto a USB drive. Even computers that have been turned off may be vulnerable, because a computer's memory is still active for several minutes without power. If an attacker can plug a USB drive into the computer during that time, he or she can quickly reboot the system from the USB drive and copy the computer's memory, including passwords, encryption keys, and other sensitive data, onto the drive. Victims may not even realize that their computers were attacked.

The most obvious security risk for USB drives, though, is that they are easily lost or stolen (see *Protecting Portable Devices: Physical Security* for more information). If the data was not backed up, the loss of a USB drive can mean hours of lost work and the potential that the information cannot be replicated. And if the information on the drive is not encrypted, anyone who has the USB drive can access all of the data on it.

How can you protect your data?

There are steps you can take to protect the data on your USB drive and on any computer that you might plug the drive into:

- Take advantage of security features - Use passwords and encryption on your USB drive to protect your data, and make sure that you have the information backed up in case your drive is lost (see *Protecting Portable Devices: Data Security* for more information).
- Keep personal and business USB drives separate - Do not use personal USB drives on computers owned by your organization, and do not plug USB drives containing corporate information into your personal computer.

- Use and maintain security software, and keep all software up to date - Use a firewall, anti-virus software, and anti-spyware software to make your computer less vulnerable to attacks, and make sure to keep the virus definitions current (see [Understanding Firewalls](#), [Understanding Anti-Virus Software](#), and [Recognizing and Avoiding Spyware](#) for more information). Also, keep the software on your computer up to date by applying any necessary patches (see [Understanding Patches](#) for more information).





- Do not plug an unknown USB drive into your computer - If you find a USB drive, give it to the appropriate authorities (a location's security personnel, your organization's IT department, etc.). Do not plug it into your computer to view the contents or to try to identify the owner.
- Disable Autorun - The Autorun feature causes removable media such as CDs, DVDs, and USB drives to open automatically when they are inserted into a drive. By disabling Autorun, you can prevent malicious code on an infected USB drive from opening automatically. In [How to disable the Autorun functionality in Windows](#), Microsoft has provided a wizard to disable Autorun. In the "More Information" section, look for the Microsoft® Fix it icon under the heading "How to disable or enable all Autorun features in Windows 7 and other operating systems."

SIX CHIX

BY RINA PICCOLO



Mountain Computer User Group November 2011 Calendar

SUNDAY	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY	SATURDAY
		1	2	3	4	5
6	7	8	9 MCUG Board Meeting	10	11 VETERAN'S DAY 	12
13	14 MCUG Meeting 6:00 Q&A 7:00 Program	15	16	17 Last Day To Submit Articles !	18	19
20	21	22	23	24 Thanksgiv- ing Day ! 	25	26
27	28	29	30			

HAPPY BIRTHDAY!!!

Larry Morgan 11/06
Dolly Davis 11/10
Adrienne Cassidy 11/16



Gerald Shenkman 11/25
Larry Garrett 11/26
Mike Brown 11/30

NOVEMBER ANNIVERSARIES!!!

Mikele & Adam Carter 11/09/1969 42 yrs
Jim & Billie Bell 11/27/1971 40 yrs



John & Brenda Cassady 11/29/19?? ?? yrs
Dolly & Bob Davis 11/08/19?? ?? yrs