February 2015

Microsoft REGISTERED Refurbisher

The Next General Meeting of CCCGC will be **February 3, 2015**

Charlotte Bytes

See us on the Web
www.cccgc.net

Official Publication of the Charlotte County Computer Group Corp.

PROMOTING COMPUTER LITERACY AND EDUCATION IN CHARLOTTE COUNTY

VOL. XXVII

No. II

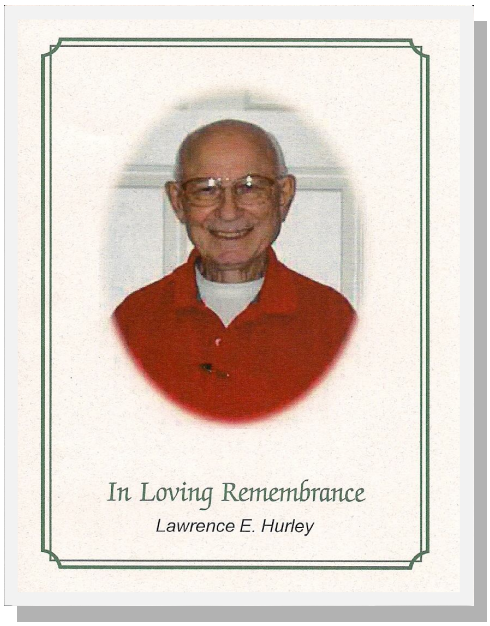
Inside this issue:

Charlotte County Computer Group

2280 Aaron Street
Port Charlotte, FL 33952

Phone: 941-585-0356
941-625-4175 x244
E-**mail:**
office@cccgc.net

The President's Platform by Ron Wallis, President CCCGC



We lost a good friend and a long and loyal club member. Larry Hurley was installed as Treasurer in December, sadly he passed away in January. Larry was formerly President for two years between 2003 to 2005. He was also formerly a Director and in charge of our scholarship program to local area high schools in which he still excellently performed the duty as Treasurer. Larry also had been a presenter at many of our general meetings, and two Wednesdays a month he taught software programs. Larry was presented a few years ago with Lifetime Membership. There isn't enough space to account for all of his contributions to this Club throughout the years. He will be sorely missed.

We are pleased to welcome Ron Tatro as our Treasurer and we welcome him to our executive board. Ron has been a member for some years, and he also helps out in the repair department. Thanks Ron for accepting the position.

We are still in need of flat screen monitors and USB keyboards. We also need volunteers to help with recycling and to help in the office at the desk.

The presentation for February's meeting had to be cancelled so we are working on another one. If anyone has an interest on a particular subject please let us know.

Ron

Charlotte Bytes

Computer Drawing

George Kopenec was the winner this month. He also was a drawing winner. Last month Rose Kopenec was the winner. Talk about luck. Off the computer went. You must play to win. Hope it is you next month.

50/50 Winner

Glenn Taylor was the winner this month. He jumped up out of his seat and came right up to claim his money and tried to get back to his seat before we could get the picture taken.

You need to play to win. Your picture could be here next month.

Door Prize Winners

Left To Right

Grover Mudd

Joanne Nicholson

Yvette Pilch

Caroline Faber

George Kopenec

WELCOME

New Members

Christine Brown	**Dmitry Dembin**	**Tanya French**
Fred Kopf	**Dave Carter**	**Ricardo Reyes**
Alice Shirley	**Jack Sutherland**	**Dennis Wilkins**
Victor Emmelkamp	**Joan Chick**	**Steve Bertacchini**
Barbara Dubicki	**Howard McGee**	**Edward Webb**
Fay Good	**Linda Props**	**George Ferris**
Doris Dunn	**Kimberly Ramos**	

The Executive Board and Members of CCCGC welcome each of you to the group. We're Here To Help. Membership Has Its Privileges.

If you have any questions, concerns or need computer help, please contact us at the office. We will endeavor to help you any way we can.

Program High-Lights

85 Members attended this meeting.

Ron started the meeting announcing that the office will be closed on Friday to allow all members to attend the memorial service planned for Larry Hurley.

Scott Baty took the floor and talked about Internet Safety and Security. You must take it seriously. Don't put anything out on the internet that you wouldn't put on a billboard at your house. It is out there and will always be there. With social media taking over, it becomes harder to avoid problems. Many statistics were given showing how the poplulation is on line one way or the other with facebook, twitter, chat rooms, instant messages, instagram and on and on and on.

Never share your password with anyone! We were given statistics on different browers and how to use them safely. It really is a personal choice. Tough passwords are also extremely important.

There is a link on the cccgc.info website to check out January's program. Take the time to check them all out.

Scott told the audience that Jelly Bean Computer is in the process of being dissolved. Scott is going to concentrate on his health, his family, and personal stuff. He thanks the computer group for all the help we have given him and he will be able to cover some future meetings when he has time.

L ydia

Microsoft® REGISTERED Refurbisher

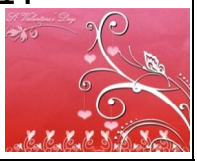
For more information go to www.cccgc.info

View/download Bytes

Please be sure to register online for classes

Classes & Events Calendar

February 2015 CCCGC Events Calendar

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
1	2 **Libre Office** 2 to 4 PM John Palmer	3 **General Meeting** 7:15 PM Classes 5:00 PM 6:00 PM	4	5 **Open Forum** 2 to 4 PM Dick Evans	6	7
8	9 **Libre Office** 2 to 4 PM John Palmer	10	11 **Maintenance** 2 to 4 PM Ron Wallis	12 **No Class**	13	14 
15	16 **Reflect Backup** 2 to 4 PM Ron Wallis	17	18 **Reflect Backup** 2 to 4 PM Ron Wallis	19 **No Class**	20	21
22	23	24 **Windows 8.1** 2 to 4 PM Ron Wallis	25 **Maintenance** 2 to 4 PM Ron Wallis	26 **Open Forum** 2 to 4 PM Dick Evans **Board Meeting** 6:30 PM	27	28
		NOTICE All Non Meeting Night Classes will be held in **Our CCCGC Office.**			**Notes:** OFFICE HOURS: 10:00 AM-2:00 PM MONDAY -FRIDAY **Please sign up for classes ONLINE:** http://www.cccgc.info	

Charlotte Bytes

Charlotte County Computer Group

Information: (941) 585-0356

(941) 625-4175 x244

Official publication of the Charlotte County

Computer Group Corporation

2280 Aaron Street

Port Charlotte, FL 33952

www.cccgc.info

Over the past few years I have logged many miles on service calls, helping people with their computers. In all the conversations I've enjoyed, no one has ever told me "I wish I had spent more time at work". As most of you know, I have decided to dissolve Jellybean Computers. This was not an easy decision yet in many ways it was what I'd call a Slam-Dunk.

I am very thankful to all the clients with whom I've shared time and especially The Charlotte County Computer Corp. The support of this Computer Club and all of its' members, has been incredible. I have every intention of continuing to help out as I am able, and you will have me. Who knows perhaps I can find time to teach that class we talked about.

This Club is a treasure of computer knowledge, skill, and help. Let us know as we continue the 30 plus years of promoting Computer literacy and education in Charlotte County, what it is you would like to see in the presentations and the free classes offered by your Computer Club.

I chose this club from a couple in the area because of it's commitment to our youth and to those who are making a difference in our community. Recycling is a way in which we can all make a difference, (and the club will recycle most any computer component). It is also the source of our inventory for creating these Computer Systems for the areas youth.

My sincere thanks to each of you and to the Computer Club for the blessing you've been to myself, my family and Jellybean Computers.

Scott Baty

The Charlotte County Computer Group Corp.

Is a non-profit 501(c)3 organization as classified by the Internal Revenue Service.

Donations, gifts, bequests, legacies, devices and transfers are deductible under federal laws.

We're on the Web
www.cccgc.net

Vipre Security News Room

Credit Card Hacks Will Cost You Money -- One Way or Another

Losses from credit and debit card fraud in the United States totaled about $11 billion in 2013, up from about $8 billion in 2012, according to a recent report from Javelin Strategy & Research.

The Pleasanton, California-based consulting firm noted that such fraud usually does not affect consumers directly. The majority of the cost of credit card fraud falls on banks that issue the cards and on merchants. In most cases, federal law limits consumers to paying a maximum $50 charge against hundreds or thousands of dollars of merchandise.

However, (either through fees or higher prices for goods and services) the burden of covering fraud costs everyone.

Consumers typically feel the banks' 'pain' through higher fees, interest rates and penalties.

Javelin said that more than 8 percent of all consumers were affected by some kind of card fraud in 2013. The firm estimated that the average tab per consumer was $106, which covers legal fees, time taken off work to deal with their problems, and the cost of notarizing and mailing documents among other things.

Chips Will Likely Reduce Credit Card Fraud

To cut their losses, credit card companies are requiring retailers to buy machines that will read cards containing embedded computer chips known as EMV (Europay, MasterCard and Visa) cards, and to include encryption and tokenization in their security systems.

The chip in the card issues a unique code for each transaction. Retailers that do not install the technology for consumers to pay with those cards will be liable for any fraud.

Similar changes in Europe cut down on credit card theft, but the technology applies only when the customer is present and not for online or phone transactions that rely on the credit card number alone. That liability remains with retailers.

Macs, iPads and iPhones: Not as Inpregnable to Malware Attacks as You Might Think

Users of Apple Computers' Macs, iPads and iPhones are increasingly being targeted with malware by the cyber bad boys -- news that might encourage all you PC users to stay with good ol' Microsoft and its host of flawed angels.

While recent reports detail increased criminal focus on users in China and the U.S., Apple users everywhere need to take proactive measures to safeguard their devices and information.

Apple users in China have a new threat to contend with that attacks iPhones and iPads through Apple's Mac OS X operating system, according to Palo Alto Networks. The company describes the threat as "WireLurker" because it waits for a device running Apple's iOS mobile operating system to connect via USB to a Mac laptop or desktop.

The software -- hidden in apps downloaded from China's third-party Mac OS X app stores -- adds malicious code to legitimate iOS apps. The malware attack has been limited to China, so far.

Meanwhile in the U.S., Apple users in 2013 accounted for the largest portion of attacks on MacOS X, with 98,077 users being attacked, which totaled 39 percent of all Mac OS X attacks, according to Kaspersky Lab's year-in-review blog post.

The targeting of U.S. users is easy to explain: there are more users of Apple products in America than in any other country, and Apple products are growing in market share.

More than 3 million attempts to infect Mac OS X-based computers were blocked this year, compared to 1,363,549 blocked attempts on Android-based devices.

The U.S. also topped the list of countries where Mac online resources were seeded with malware. The U.S. accounted for 27 percent of infected online resources.

the How-To Geek
Computer Help from your Friendly How-To Geek

The 10 Most Ridiculous Movie Myths That Turned Out to Be True

Hollywood doesn't understand technology and "hacking." That's what we thought, anyway. But many of the ridiculous things we've seen in movies turned out to be completely true.

We laughed off many of these myths when we saw them in movies. "Don't believe what you see on TV," we told people. Boy, were we wrong.

The NSA Spying on Everybody

One of the oldest themes is a government that knows all and sees all. If the hero needs some information to stop a plot, they can tap into a seemingly infinite amount of real-time information to find the villain, determine who they're communicating with, and then track them in real-time. Alternately, the all-seeing government surveillance state is often portrayed as a villain.

Image Credit: Unknown on imgur

We all scoffed at this, but much of it appears to be true. The NSA (and other countries' intelligence agencies) are monitoring Internet traffic and phone calls, building up huge databases they can query. That scene where the hero taps into a massive database that gives them all the information they need — well, it's more true than we could have ever imagined.

Heck, even The Simpsons mentioned this in 2007's The Simpsons Movie!

Your Location Can Be Tracked

Cell phones can be tracked by triangulating their relative signal strengths between three nearby cell towers, we know that. But the US government has gone to even greater lengths. They've placed fake cellular towers on small airplanes and flown over urban areas, intercepting communications between a suspect's cell phone and the real cell tower to determine someone's exact location without even needing to a cellular carrier for help. (Source)

Yes, that scene where a hero boards an airplane and flies over an urban area, staring at a map as they track a suspect's exact location somehow— that's true, too.

Webcam Hijacking

Webcams can be scary. They offer a way for an unseen attacker to view us from afar. They may be used by a twisted mind to exploit someone, demanding that someone strip for the webcam or their secrets or private photographs will be sent to family members or the public. Or, a webcam may simply function as a convenient way for someone to snoop on an otherwise-secure area.

Webcam hijacking is certainly real, too. There's a whole community of twisted minds using RAT (Remote Access Tool) software to spy on people, hoping to catch a glimpse of them undressing, and attempting to manipulate them into stripping for the camera. (Source) The UK's GHCQ intelligence agency captured millions of Yahoo! webcam images, including many pornographic ones.

The 10 Most Ridiculous Movie Myths That Turned Out to Be True

Continued from page 7

the How-To Geek
Computer Help from your Friendly How-To Geek

Hacking Traffic Lights and Cameras

Cut to the dramatic chase scene. Our heroes are chasing after a skilled hacker. Or, our heroes need to use their hacking skills to catch up with the villain. Either way, someone is manipulating the traffic cameras, turning them green when they need to drive through and red when their pursuers need to drive through. Or, our heroes hack into the traffic camera grid to spy on someone's movements throughout a city. Or, even worse, a city is taken over by a supervillian who turns all the traffic lights green to cause chaos while cackling maniacally.

That makes for a dramatic scene, but it's silly — or is it? It turns out that hacking traffic lights and their cameras is often trivial. Researchers have found that many traffic lights are connected to open Wi-Fi networks and using default passwords. (Source)

2003's The Italian Job features a character "hacking" traffic lights, turning all lights at an intersection green to create a traffic jam.

Darknet Drug Rings, Arms Trafficking, and Hitmen

RELATED ARTICLE

HTG Explains: **What is Bitcoin and How Does it Work?**

Geeks have had their own "money" for some time, but typically it is within the context of online gaming. While... [Read Article]

http://www.howtogeek.com/141374/htg-explains-what-is-bitcoin-and-how-does-it-work/

There's a secret part of the Internet where the criminals lurk, below the shiny exterior that us upstanding citizens walk over everyday. You can get anything here, for a price. Any type of illegal drug you want, stolen credit card numbers, fake identification documents, illegal weapons, and professional hitmen for hire.

Much of this is true thanks to the "darknet" — Tor hidden services, for example. It's become more public knowledge thanks to the bust of Silk Road, but other sites have sprung up. Of course, there's no guarantee all this stuff is actually legitimate. When Silk Road's "Dread Pirate Roberts" attempted to hire hitmen and pay them in BitCoin, he seems to have hired both someone who took the money and vanished as well as police who used it to build a case against him. There's no evidence the hundreds of thousands of dollars in BitCoin he spent actually got anyone killed, so maybe this criminal mastermind isn't as clever as he thought he was.

Hacking Security Cameras and Security Systems

Our heroes — or villains — need to break into a secure location. To scope it out, they hack the security cameras and examine the place's security, noting the amount of guards, their patrols, and other security features they'll need to bypass.

It's convenient, but also not too hard. Many IP security cameras have horrifically weak security and can be trivially hacked. You can even find websites that provide a list of publicly exposed security cameras you scan snoop on yourself. (Source)

Like many other products, security systems themselves often have horrifically weak security, so they can be shut down or jammed if someone put the effort in.

Continued on page 13

CCCGC

Charlotte Bytes

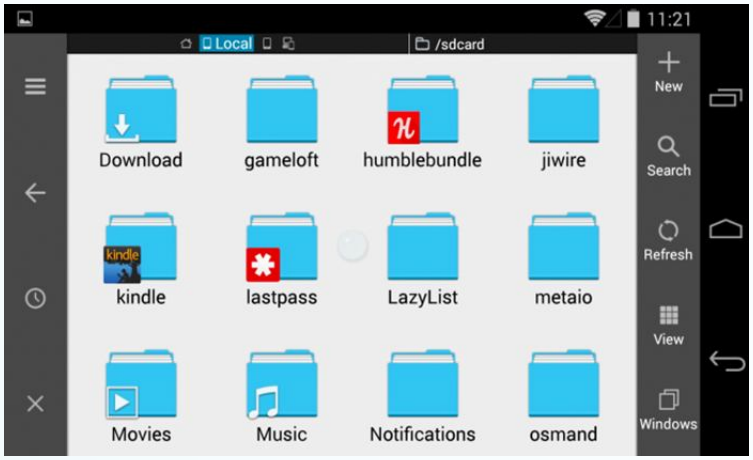
How to Manage Files and Use the File System on Android

Android's user-visible file system is one of its advantages over iOS. This allows you to more easily work with files, opening them in any app of your choice. But Android doesn't include a file manager app by default.

Some manufacturers do preinstall their own file manager apps on their Android devices, so you may have one anyway. Not every Android user needs to mess with this stuff, but it's there if you want it.

Installing a File Manager App

Some manufacturers do preinstall their own file manager apps, like the My Files app on Samsung devices. However, there's a good chance you'll need to install your own file manager app.



ES File Explorer is quite nice for this. It's the most popular file management app, it's packed full of powerful features like the ability to access network shares, and it's free. If you've tried it in the past, you may have been disapointed not seeing a Gingerbread-style interface, but it now offers a more Holo-style file manager interface. It's far from the only good option, and you can use almost any app you like — even the one your manufacturer included with your device.

File Management Basics

RELATED ARTICLE

5 Ways to Free Up Space on Your Android Device

Phones and tablets only have so much internal memory. If you're running out of space for apps or data, there...

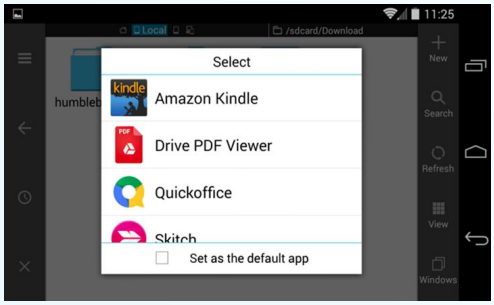
[Read Article] http://www.howtogeek.com/112356/5-ways-to-free-up-space-on-android/

You probably don't want to spend time moving files around and arranging your device's file system, but you can. Bear in mind that many of the folders you see when you open your file manager are created and used by apps for their cache files, so you shouldn't remove them. However, you can free up space by removing unnecessary files stored here.

There are quite a few folders created already that you might want to use, including the following:

DCIM: Photos you take are saved to this folder, just as they are on other digital cameras. Apps like Gallery and Photos display photos found here, but this is where the underlying image files are actually stored.

Download: Files you download are saved here, although you're free to move them elsewhere. You can also view these files in the Downloads app.



Movies, Music, Pictures, Ringtones, Video: These are folders designed for storage of your personal media files. When you connect your device to a computer, they give you an obvious place to put any music, video, or other files you want to copy to your Android device.

You're free to browse the file system from any file manager. File manager apps allow you to select and manage files — renaming, moving, or deleting them. A single tap on a file will bring up a list of installed apps that claim they support that file type. You can work with files directly, opening them in apps like you would on your computer.

Copying Files To or From a PC

RELATED ARTICLE

Android USB Connections Explained: MTP, PTP, and USB Mass Storage. Older Android devices support USB mass storage for transferring files back and forth with a computer. Modern Android devices use... [Read Article]

Continued on page 10

Charlotte Bytes

See us on the Web
www.cccgc.net

the How-To Geek
Computer Help from your Friendly How-To Geek

CCCGC

How to Manage Files and Use the File System on Android

Conclusion from page 9

Copying Files To or From a PC

RELATED ARTICLE

http://www.howtogeek.com/192732/android-usb-connections-explained-mtp-ptp-and-usb-mass-storage/

The process of copying files to or from a PC is easy. Just connect your Android device to a laptop or desktop computer using the appropriate USB cable — the one included with your device for charging will work. With the Android device in its default MTP mode (PTP is also available, and USB mass storage may be available on older devices), it will appear in your Windows or Linux file manager window as a standard device. You can view and manage the files on your Android device's internal storage, moving them back and forth as you please.

Macs don't include MTP support, so you'll want to install the Android File Transfer app on your Mac and use it to transfer files back and forth when you connect your device. The app will automatically open whenever you connect an Android device to your Mac.

If you have an SD card, you can remove the SD card from your Android device and insert it into an SD card slot into your computer, managing it that way. The SD card will appear as a typical connected storage device in your file manager, just as USB flash drives do.

For wireless file transfers, we like AirDroid. It allows you to connect to your Android device over Wi-Fi with just a web browser, moving files back and forth without the necessity of a cable. It will likely be a bit slower, but it can be a life-saver if you're out and about and didn't bring the appropriate USB cable.

Understanding the File System Layout

Android's file system layout isn't identical to your PC's. Here's how it divides its storage:

Device Storage / Emulated SD Card: This is the pool of storage you'll be working with and accessing. Your'e free to access and modify any files here. Think of it a bit like your user directory on Windows or home directory on Linux or Mac. As on desktop operating systems, many apps dump some data files here — not sensitive data like passwords and login credentials, but downloaded files and other cache items. Due to a quirk in the way Android was originally designed, this is still presented as an "/sdcard" directory even on devices that don't have an SD card slot at all. The on-device storage is presented to apps as if it were an SD card where they can dump their data for compatibility reasons.

Actual SD Card: Many Android devices also have SD card slots. You can plug the SD card into your computer or another device, load files onto it, and then plug it into your device. Or, you can save photos and other files onto the SD card on your device, plug it into your computer, and move files off of it. Even files with actual SD cards will have internal storage that functions as an emulated SD card, so the layout may be a bit more confusing if you have a device with SD card. You'll find both types of storage in different folders under the /storage directory.

Device Root / System File System: Your Android device also has a special system filesystem where its operating system files, installed applications, and sensitive application data are stored. You and the apps you use can't modify this file system for security reasons. This also ensures apps can't read another app's sensitive data — picture a malicious application attempting to read the saved credentials from an online-banking app. This limitation can be bypassed with root access, allowing you to write to and modify system files as you please. You probably don't need to do that, of course.

Google's "stock" Android doesn't ship with a file management app because it isn't considered strictly necessary. Files you download are available for use directly in the Downloads app. Photos you take appear in the Photos or Gallery apps. Even media files you copy to your device — music, videos, and pictures — are automatically indexed by a process called "Mediaserver." This process scans your internal storage or SD card for media files and notes their location, building up a library of media files that media players and other applications can use. However, while a user-visible file system isn't necessarily for everyone, it's still there for people who want it.

CCCGC

Charlotte Bytes

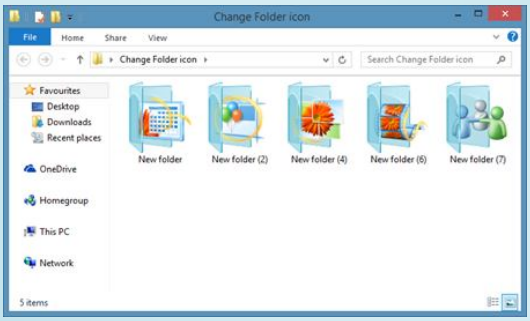
Into Windows

How To Change Folder Icon In Windows 7/8

Admin Updated on Sep 15th, 2014

The folder icon in Windows operating system has been more or less the same since the release of Windows Vista. In fact, Windows 7 and Windows 8/8.1 use the same set of icons introduced first with Vista, and the soon to be released Windows 9 will most likely carry the same set of icons if present rumors are anything to go by.

PC users who love customizing Windows might want to change the default icon of a folder in Windows operating system. Having a unique folder icon helps you quickly identify the folder you are looking for, especially if you have tens of folders with the default color and icon. Take, for example, if you want to quickly identify the folder that you open very often, you can replace the default folder icon with a custom one.



The beauty of Windows operating system is that it's highly customizable with or without the help of third-party applications. Ever since the days of Windows XP, Windows operating system has an option to change the default folder icon without the help of third-party tools but very few users have used this handy feature.

Here is how you can change folder icon, for free, without the help of third-party applications.

Customizing default folder icon

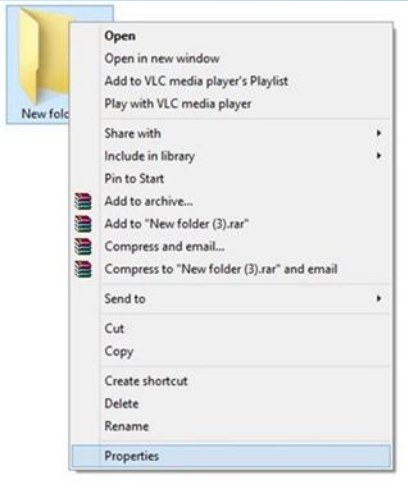
Note 1: This method is applicable to all recent versions of Windows, including Vista, Windows 7, and Windows 8.

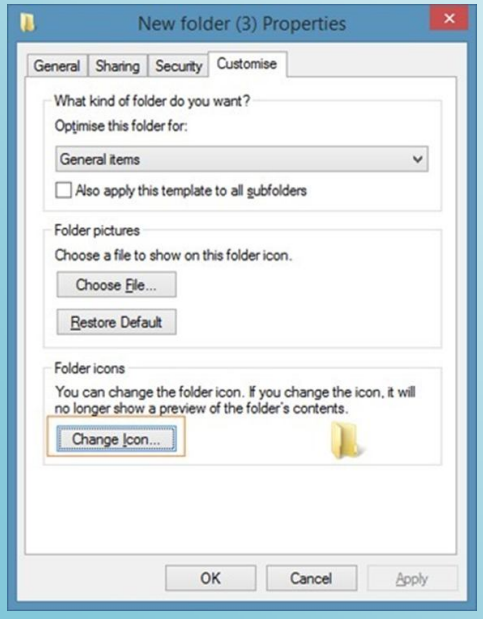
Note 2: Changing the icon of a folder will not change the icons of other folders. For instance, changing the icon of New Folder 1 will not change the default icon of New Folder 2.

Step 1: Navigate to the folder that you want to customize by changing its default icon.

Step 2: Right-click on the folder and then click Properties to open the Properties dialog.

Step 3: Switch to the Customize tab. Under Folder Icons section, click on the button labelled "Change Icon" to select an icon for your folder. And if you have a custom icon and want to use the same, simply click on the Browse button and navigate to the location where the custom icon is located. Select the icon and click Open button.





Conclusion on page 17

CCCGC
Microsoft REGISTERED Refurbisher
Charlotte Bytes
ghacks.net

Run Trend Micro's Anti-Threat Toolkit as a second opinion scanner

By Martin Brinkmann on September 15, 2014 in Software

I like to run second opinion scanners from time to time on computer systems to make sure that no malware or other unwanted software has slipped by the primary defenses running on those PCs.

While that is the case, I don't have have a preference for a tool that I run in this case but use different programs.

There are programs that I value a lot, like Malwarebytes Anti-Malware or Hitman Pro, but it never hurts to run other programs as well on the system.

Trend Micro Anti-Threat Toolkit is a free portable program for recent versions of the Windows operating system.

Once it has been downloaded to the local system it can be started right away. The program opens a command prompt on start and runs a couple of commands there before the graphical user interface is started.

The program, like many on-demand scanners, is rather basic when it comes to the options it offers. While you find a settings button, it displays only two options that you can modify.

The first allows you to select folders that you want scanned, the scanned to disable sending information to Trend Micro's Protection Network, a cloud based service offering up to date protections against threats which the program may not support yet without it.

A scan is started once you hit the scan button. Scans can take quite some time to complete. A test scan using defaults on a fast Windows 7 Pro system with a Solid State Drive as its primary hard drive took more than 30 minutes to complete.

Results are displayed in the interface afterwards with options to display additional details, scan again or to fix issues that were found.

Some threats may require a reboot of the system. This is outlined after you select the fix now button in the program interface. This restarts the computer and displays the Windows Boot Manager afterwards with an option to run the Trend Micro Clean Boot program.

Anti-Threat Toolkit can detect various kinds of malware, from viruses and trojans to rootkits, rogue programs and spyware. A fix may include the restoration of system policies and Registry settings that were changed by malware.

To download the program, click on any of the solutions posted on the page posted in the summary section below. There you find direct download links for 32-bit and 64-bit versions of the program that you can run on computer's with or without Internet connection.

http://esupport.trendmicro.com/solution/en-us/1059509.aspx

Related Articles

Kaspersky's AVZ Antiviral Toolkit is a portable second-opinion scanner http://www.ghacks.net/2014/03/23/kasperskys-avz-antiviral-toolkit-portable-second-opinion-scanner/

Anti-Malware Toolkit Downloads Security And Cleanup Tools http://www.ghacks.net/2008/08/14/anti-malware-toolkit-downloads-security-and-cleanup-tools/

Trend Micro RootkitBuster http://www.ghacks.net/2009/10/01/trend-micro-rootkitbuster/

CCCGC
Microsoft REGISTERED Refurbisher
Charlotte Bytes
the How-To Geek
Computer Help from your Friendly How-To Geek

The 10 Most Ridiculous Movie Myths That Turned Out to Be True

Continued from page 8

Hacking ATMs for Cash

RELATED ARTICLE

ATM Skimmers Explained: How to Protect Your ATM Card

An "ATM skimmer" is a malicious device criminals attach to an ATM. When you use an ATM that's been compromised... [Read Article] http://www.howtogeek.com/193958/atm-skimmers-explained-how-to-protect-your-atm-card/

ATMs are a great hacking target. If someone needs some cash, they can simply hack an ATM to get it. While the ATM may not start shooting bills all over the street as it might in the movies, we've also seen a variety of ATM hacks springing up. The most pedestrian of them involve attaching a magnetic strip reader and camera to the machine itself to "skim" people's ATM card credentials, but there are attacks that work directly by hacking the ATM's software. (Source)

This one shows up as far back as 1991's Terminator 2, where John Connor jacks a device into an ATM and gets it to dispense some free cash.

Security Backdoors in Encryption Protocols

RELATED ARTICLE

Here's Why Windows 8.1's Encryption Doesn't Seem to Scare the FBI

The FBI doesn't seem worried about Windows 8.1's default "device encryption" feature. Microsoft's encryption works a bit differently — Microsoft holds the keys and could hand them over to the FBI.

The FBI isn't happy about the latest versions of iOS and Android using encryption by default. FBI director James Comey... [Read Article] http://www.howtogeek.com/199171/heres-why-windows-8.1s-encryption-doesnt-seem-to-scare-the-fbi/

"It's no good, sir — he isn't talking. We'll never break the encryption on his hard drive." It's a line that might be spoken before a clever government hacker speaks up and says it's no problem. After all, the government has a backdoor into the encryption and can crack it. That's just a dramatic version of a possible scene — in reality, this usually manifests itself as the government being able to crack any encryption it wants, just because.

We've now seen backdoors inserted into encryption systems in the real world. The NSA manipulated the NIST into inserting a backdoor into the Dual_EC_DRBG encryption standard, which was recommended by the US government. (Source) The NSA then paid $10 million to RSA Security in a secret deal, and this compromised encryption standard was then used by default in their BSAFE library. (Source) And that's just a backdoor we know about.

Windows 8.1's default "device encryption" goes out of its way to hand a recovery key over to Microsoft, so the government could get it from them. Backdoors may also look like this one in Windows, which offers some convenient features for Windows users, access for the US government, and plausible deniability for Microsoft.

Hotel Key Cards Can Be Easily Hacked

Does someone want to get into a hotel room? No problem! Hotel room locks are easily hijacked thanks to their card readers. Just pop open the lock, do something with the wires, and you're in.

Continued on page 14

Charlotte Bytes

the How-To Geek
Computer Help from your Friendly How-To Geek

See us on the Web
www.cccgc.net

CCCGC

The 10 Most Ridiculous Movie Myths That Turned Out to Be True

Conclusion from page 13

Hotel Key Cards Can Be Easily Hacked

Whoever invented this myth probably didn't spend much time thinking of it, but it's possible. With some cheap hardware and a few seconds, an attacker could open up the assembly on the outside of the lock, plug hardware into an open port, read the decryption key from memory, and open the lock. Millions of hotel room locks around the world are vulnerable to this. (Source)

Onity, the company that manufactured the locks, will give hotels a cap to put over the port and screws that make the assembly harder to unscrew. But hotels don't want to fix this, and Onity doesn't want to give out replacement locks for free, so many locks will never be fixed.

Passwords Can Be Easily Hacked

How Attackers Actually "Hack Accounts" Online and How to Protect Yourself
People talk about their online accounts being "hacked," but how exactly does this hacking happen? The reality is that accounts...
READ ARTICLE

http://www.howtogeek.com/169847/how-attackers-actually-hack-accounts-online-and-how-to-protect-yourself/

Passwords are never too much of an obstacle in the movies. Either a clever person sits down and attempts to guess someone's password, or they plug something in and quickly crack their password.
Many passwords are horrible, so trying combinations like "password," "letmein," a child's name, a pet's name, a spouse's birthday, and other obvious bits of data will often let you luck into someone's password. And, if you re-use the same password in multiple places, attackers probably already have login information for your accounts.
If you do gain access to a password database so you can perform a brute-force attack against it, it's often quick to guess the password thanks to lists that include obvious, common passwords. Rainbow tables also speed this up, offering precomputed hashes that let you quickly identify common passwords without spending a lot of computing power.

These are far from the only myths that turned out to be true. If there's one common thread here, it's that security (and privacy) is often an afterthought in the real world, and the technology we use is never as secure as we'd like it to be. As we charge towards ever-more connected devices thanks to we'll need to take security much more seriously.

"The Internet of Things," http://www.howtogeek.com/183431/htg-explains-what-is-the-internet-of-things/

Image Credit: Kenneth Lu on Flickr, Aleksander Markin on Flickr, Sean McGrath on Flickr, Tax Credits on Flickr, NSA

Charlotte Bytes

CCCGC

Windows Secrets
Everything Microsoft forgot to mention.

See us on the Web
www.cccgc.net

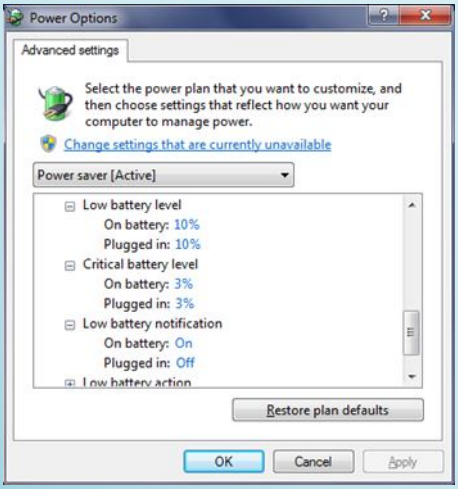
Get More Runtime From A Single Laptop Battery Charge

By Joe Keeley on 15th December, 2014 | Windows

Laptops are fantastic for their portability, but the inevitable downside for a lot of systems is that their battery charge doesn't last long. Don't fear, because this guide will offer tips on how to get more from a single charge.

Not only do some laptops offer poor time performance from a single charge, but you'll also find that your battery gets less efficient over time. It isn't always cheap to buy a replacement either, which makes it even more important to get the most from your battery in day-to-day use.

This guide will focus on Windows tips for extending your battery from a single charge, using tools built into the operating system. For information on how hardware affects battery life check our in-depth, hardware battery saving guide.



Adjust Your Battery Warnings

There's nothing worse than realizing that your battery is low before you've had a chance to do anything about it. One way of becoming more aware of how your battery is doing is to adjust the battery warnings that Windows gives.

To do so, search for edit power plan on your system and select the result. From here select Change advanced power settings and a new window will open. At the top of this window you can select which power plan to edit, but it'll default to the one you're using.

Scroll the list until you reach Battery and then expand the options. You'll now be able to adjust at what battery percentage levels Windows will notify you through Low battery level. You should adjust this to what works best for you, but something like 25% will probably be suitable. Be sure to ensure that the Low battery notification is set to On.

You can also adjust the Critical battery level, which is when your computer will hibernate in order to save your current state if you hadn't already done so from the previous warning. Again, vary this depending on your use, but 10% is a safe choice.

Don't Sleep, But Hibernate

When finished with their current session, many laptop users will simply close the lid, which typically puts the device to sleep. Although there's nothing wrong with this, your battery is draining even while in sleep mode.

Perform a system search for change what closing the lid does and select the result. This will take you to a window that will allow you to do exactly that, along with what pushing the power button does.

The default state for closing the lid is usually sleep, but this probably isn't the best choice. Sleep still retains some power in order to keep everything quickly accessible when you load the laptop back up, so you could come back and find you've lost a good chunk of battery.

Continued on next page

Get More Runtime From A Single Laptop Battery Charge

Windows Secrets
Everything Microsoft forgot to mention.

A better alternative is to change this to Hibernate from the dropdown. Hibernation remembers your state, but it completely powers down the system. This will mean that there's no chance of your laptop being awoken from anything on the system. You might have shut the lid on your system and found that it boots itself up later to perform an update or scheduled task – hibernate doesn't allow this.

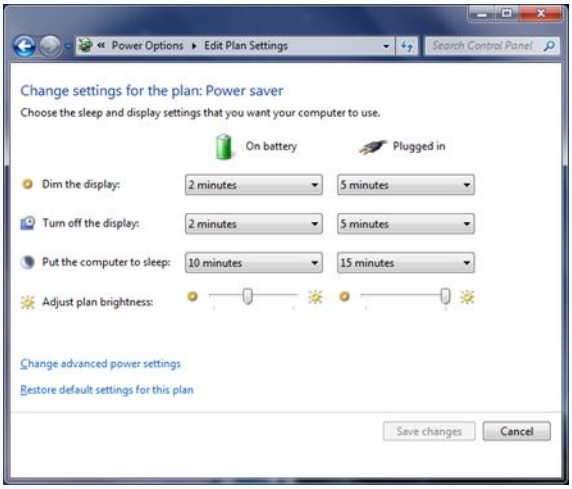
However, bear in mind that hibernation does mean the computer needs to boot up again, which in itself uses power. Nevertheless, if you're not going to be using your computer for hours then this is still a better option than sleeping.

Moreover, if your system runs on a solid state drive, you should probably disable hibernation because it could damage your drive.

Turn Down The Brightness

A report on Windows 7 from Microsoft engineers showed that the screen of your laptop is where over 40% of the power goes. As such, you need to be very frugal with your display output, if you want to conserve the juice.

The best way to conserve power on the monitor is to turn down the brightness. Although looking at a bright laptop screen is far preferable to a dim one for certain work, the former choice will be relentlessly sucking the power.



Perform a system search for power settings, select the option and it'll bring up a new window. There will be a slider at the bottom that allows you to alter the screen's brightness, which is useful for a quick fix, but let's go one step further.

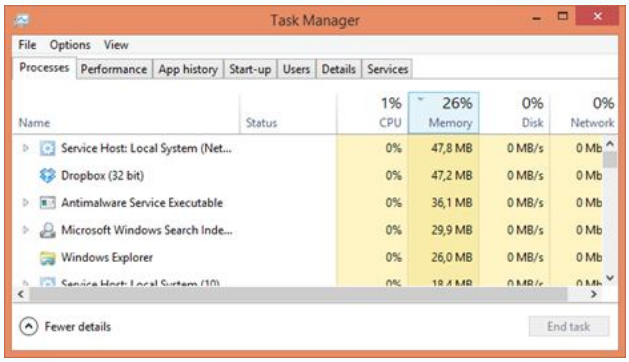
From this window, click Choose when to turn off the display from the left-hand navigation. From here you can choose when to Dim the display and Turn off the display. If you want to be truly efficient, set the dim to the lowest possible setting (1 minute). Set the turn off time to something that suits you, but 2 minutes will do.

To quickly adjust brightness on the go, you might be able to use keyboard controls. Alternatively, press Windows key + X (Windows 7) or Windows key + I (Windows 8 & 10) to bring up a menu or sidebar that contains the brightness slider.

Ditch Extraneous Programs

Are you sure that you've only got the programs you need running? While one or two extraneous applications loaded in the background might not cause much issue, a number all mounted up is a sure fire way to sink your battery into the red pretty quickly.

Press Ctrl + Shift + Esc to open up the Task Manager. Switch to the Processes tab and you'll see a list of everything that is running on your system. The higher the Memory, chances are the higher the drain on your battery. Select a process you want to stop and click End Process.



Bear in mind that some of these programs may be automatically set to run on system start up. It might make sense to remove them from that list altogether if you don't actually need them. For advice on what programs you can probably ditch, along with how to disable them from start up, check out our Make Windows Start Faster guide.

Although ending the process will save your battery, you shouldn't actually start uninstalling anything until you're plugged back into the mains. It's always useful to tidy up what you have installed, but that's going to suck power you want to keep.

Microsoft REGISTERED Refurbisher

See us on the Web
www.cccgc.net

CCCGC

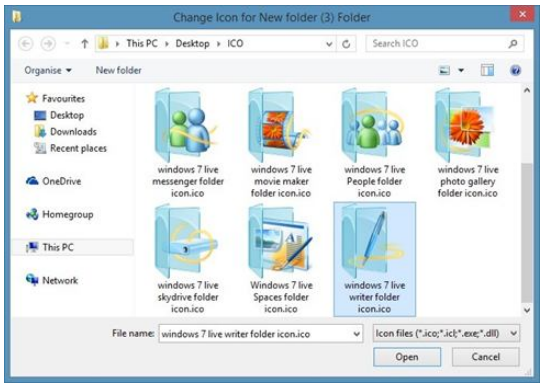
Official Publication of the Charlotte County Computer Group Corp.

PROMOTING COMPUTER LITERACY AND EDUCATION IN CHARLOTTE COUNTY

Into Windows

How To Change Folder Icon In Windows 7/8

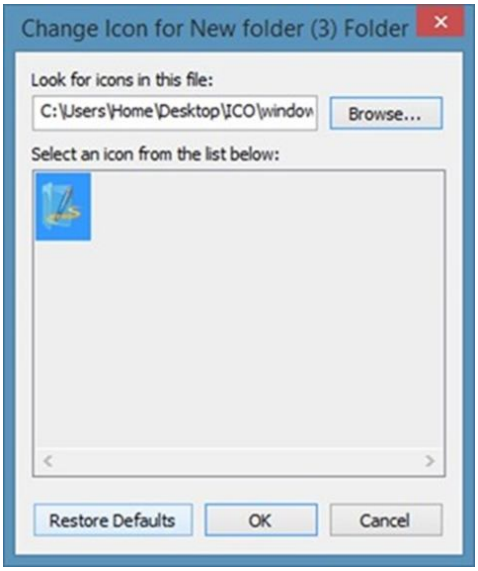
Conclusion from page 11



Note that icon file must be in .ico format. You cannot select or use a picture file folder icon without converting it to .ico format. There are many free tools and online services out there to convert your pictures into icons (.ico).

Tip: You can download hundreds of free folder icons by visiting DeviantArt website and searching for folder icons.

Step 4: Finally, click OK button and then click Apply button to change the icon of the folder.



Get More Runtime From A Single Laptop Battery Charge

Conclusion from page 16

Unplug Any Devices

Everything external that you have plugged into your laptop will use a lot of battery – even your mouse. It's more efficient to stick to the trackpad if you can. The same goes for anything else you've got connected up, like speakers or USB toys. It should go without saying that you should definitely not be charging anything else (like your phone) through your laptop.

Take the same approach for your Wi-Fi adapters. If you're not connected to any Wi-Fi networks, it's worth disabling the adapters. Perform a system search for view network connections and select the result. Then right click your wireless connection and Disable. Although it may not actually be connected, it'll still be using battery.