September 2014

Microsoft REGISTERED Refurbisher

Charlotte County Computer Group

30th YEAR Anniversary

1984 - 2014

The Next General Meeting of CCCGC will be **September 2, 2014**

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. XXVI

No. IX

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

September is almost here. School is back in session, the vacationers are returning, and soon the snowbirds will be coming back in full force. Our busy season is upon us.

Our success depends on our volunteers. We need a tech in the repair dept. to help refurbish computers and repair members machines through our members help program. If you are able to do computer repair and you would like to volunteer please see Ron at the general meeting or at the office. We also need people to help with the recycling and to help in the office. Even half a day would be greatly appreciated. If you are interested see Lydia or Grover.

With Christmas not too far off many of you will be getting new computers which will be running Windows 8 or 8.1 Windows 8 and 8.1 do not set up as easily as previous versions of Windows. If you get a new machine and are having problems setting it up we will be glad to help. Setup can sometimes take couple of hours with all the important updates , so appointments will be necessary to do this.

Welcome back to all who have been away during the summer. We look forward to seeing you.

P.S. If any of you have something you would like to have a class in or a topic you would like to have presented at the general meeting, please contact the office or one of the officers. This is your club and we welcome your input.

Ron

Charlotte Bytes

Computer Drawing

Debbie Amico was so surprised that she won the computer with ticket CZ003. Debbie said she never wins anything but she did this time. Congratulations Debbie.

Thank you everyone for participating and good luck next time.

50/50 Winner

Caroline Farber won the 50/50 of $31. Nothing like extra bucks in your pocket.

Congratulations. To everyone else good luck next time.

Door Prize Winners

Left To Right

Glenn Taylor

John Hegard

Marlene Erhardt

Rose Mary Craemer

Richard Bader

WELCOME

New Members

Donna Skallerud	**Linda Kopp**	**Sarah Martinez**
Marie Joseph	**Thomas Parente**	**John Stremming**
Lawrence Bener	**Susan Kovacs**	**Charles Kovacs**

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.

Scott Baty presented us with how to keep safe online.

He gave us a great deal of excellent information.

Cookies are a small text file placed by your computer used to track you as well as provide other information on where you have browsed. You have to accept some of them in order to get to sites that you want.

Software firewall has been in existence since service pack 2 on XP. A Router is a hardware firewall where you can set the mac address, filtering and password to prevent malicious software from coming in.

GOtag will add a geographical location if turned on, it will keep track of where you took pictures on Ipad or android for instance.

HTTP is the foundation of the data sent over the internet. More important is HTTPS. The S is very important, it means the site is encrypted. You never want to connect without the HTTPS when inputting sensitive data.

Trojans, Worms and Spyware: Worms have the ability to replicate itself. Trojans can come in with a good program. Spyware will appear in your regular browsing habits, for instance a person looking for bar-b-que grill brought in spyware. When he browsed again it only directed him to bar-b-que grills.

Keyloggers keep track of your keystrokes on your computer. Keep a good antivirus and anti spyware on your computer and keep them up to date. You can only have one anti virus program, but can have more than one antispyware program. Norton has a good antivirus program since 2009 when they revised their program.

Scott does not like Glarys software any longer. It has too many nag screens and confusing download buttons. Scott brought us to the Glarys web site and when he hovered over the download button the site changed and was hard to tell if it was good or bad. When Scott put in the HTTPS and clicked on that site he couldn't get it and it needed to be refreshed.

In Bleeping Computers there is information on ads for PC Cleaner. If you run it, it will come up with thousands of problems which in fact are normal registry entries. PC Cleaner is very bad.

Additional tool bars search providers will steer you to their web sites and not where you want to go. You can disable the tool bars in your search providers, delete your browsing history, and go to control panel, programs and features to uninstall the tool bars.

Program High-Lights

Go to Snopes to check if something is real or fake, i.e. scary viruses or malware like the one going around the internet that said it would burn your hard drive.

Beware of callers saying they are from Microsoft and your computer has problems. Microsoft does not call anyone, and they do not know if your computer has problems.

Go to the FBI.gov site. They have a great deal of information on cyber crimes, email scams and a variety of warnings.

Do not leave your computers on overnight. You're just asking for trouble. BotNets control over thousands of machines using your resources for illegitimate operations.

Y vette

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

www.cccgc.net

Researchers Find That Wearable Devices Can Read Passwords

Doing online banking in public has always been tinged with a little danger. The stranger sitting beside you in the cafe or other public place might be reading the bank PIN and password you just typed into your mobile device.

From that unlikely scenario, fast forward to this more plausible one: the cool-looking, well-groomed person donning Google Glass a few tables away in the cafe may be using the device to record your keystrokes. The thief can be nearly ten feet away and doesn't even need to be able to read the screen -- meaning glare is not an antidote.

Google Glass is a hands-free, head-mounted computer developed by the Internet search giant that allows users to capture high-definition video via voice command. **It's perfect snooping tool for thieves.**

A team of researchers at the University of Massachusetts' Cyber Forensics Laboratory has shown that thieves and hackers can use video from wearable devices such as Google Glass to spy on unsuspecting people. Besides the Google device, the team conducted extensive experiments using other video-recording devices such as a Logitech webcam, an iPhone 5 camera and a Samsung smartwatch.

The researchers created software that maps the shadows from fingertips typing on a tablet or smartphone. Their algorithm then converts those touch points into the actual keys people were touching, enabling the researchers to crack the passcode. They tested the algorithm on passwords entered on an Apple iPad, Google's Nexus 7 tablet, and an iPhone 5.

Microsoft® REGISTERED Refurbisher

For more information go to www.cccgc.info

View/download Bytes

Please be sure to register online for classes

Charlotte County Computer Group

30th YEAR Anniversary 1984 - 2014

Classes & Events Calendar

September 2014 CCCGC Events Calendar

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
	1 Labor Day Office Closed	**2** General Meeting 7:15 PM Classes 5:00 PM 6:00 PM	**3** Maintenance 2 to 4 PM Ron Wallis	**4** Open Forum 2 to 4 PM Dick Evans	**5**	**6**
7	**8** EaseUs Backup 2 to 4 PM Yvette Pilch	**9** Windows 8.1 2 to 4 PM Ron Wallis	**10** MS Office 2 to 4 PM Larry Hurley	**11** Open Forum 2 to 4 PM Dick Evans	**12**	**13**
14	**15** Libre Office 2 to 4 PM John Palmer	**16**	**17** EaseUs Backup 2 to 4 PM Ron Wallis	**18** Open Forum 2 to 4 PM Dick Evans	**19**	**20**
21	**22** AndroidTablets 2 to 4 PM Yvette Pilch	**23** Windows 8.1 2 to 4 PM Ron Wallis	**24** MS Office 2 to 4 pm Larry Hurley	**25** Open Forum 2 to 4 PM Dick Evans Board Meeting 6:30 PM	**26**	**27**
28	**29** Libre Office 2 to 4 PM John Palmer	**30** Maintenance 2 to 4 PM Ron Wallis				

NOTICE

All Non Meeting Night Classes will be held in **Our New CCCGC Office.**

Notes:

OFFICE HOURS: 10:00 AM-2:00 PM
MONDAY -FRIDAY
Please sign up for classes ONLINE:
http://www.cccgc.info

CCCGC

Charlotte County Computer Group

30th YEAR Anniversary

1984 - 2014

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.

Officers and Board of Directors for 2014

President: Ron Wallis

Vice President: A Yvette Pilch

Secretary: Ron Muschong

Treasurer: Larry Hurley

Director: John Hegard

Director: Grover Mudd

Director: Lydia Rist

Director: Frank Messina

Director: Linda Corrick

We're on the Web
www.cccgc.net

the How-To Geek

Computer Help from your Friendly How-To Geek

ATM Skimmers: 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 in such a way, the skimmer will create a copy of your card and capture your PIN.

If you use ATMs, you should be aware of these attacks. It's often possible to spot ATM skimmers, or at least to protect your PIN so ATM skimmers won't be able to capture it.

How ATM Skimmers Work

An ATM skimmer has two components. The first is a small device that's generally inserted over the ATM card slot. When you insert your ATM card, the device creates a copy of the data on the magnetic strip of your card. The card passes through the device and enters the machine, so everything will appear to be functioning normally –but your card data has just been copied.

The second part of the device is a camera. A small camera is placed somewhere it can see the keypad — perhaps at the top of the ATM's screen, just above the number pad, or to the side of the pad. The camera is pointed at the keypad and it captures you entering your PIN. The ATM appears to be functioning normally, but the attackers just copied your card's magnetic strip and your PIN.

The attackers can use this data to program a bogus ATM card with the magnetic strip data and use it in ATM machines, entering your PIN and withdrawing money from your bank accounts.

ATM skimmers are becoming more and more sophisticated. Instead of a device fitted over a card slot, a skimmer may be a small, unnoticeable device inserted into the card slot itself.

Instead of a camera pointed at the keypad, the attackers may be using an overlay — a fake keyboard fitted over the real keypad. When you press a button on the fake keypad, it logs the button you pressed and presses the real button underneath. These are harder to detect. Unlike a camera, they're also guaranteed to capture your PIN.

Charlotte Bytes

CCCGC

Five Security Myths Debunked

Myth #1: No One Would Want To Hack Me,

I Don't Have Anything Worth Taking or contacts that would make us a specific target of a criminal. However, what many people are unaware of is most of cyber threats are internet-wide fishing expeditions by automated bots looking for vulnerable computers and networks.

Contrary to what you might think, the criminal behind the bot simply wants to use your device or its storage as a remote unit for contraband material (such as child pornography) or as a zombie/slave in denial-of-service (DOS) attacks on Web sites.

Myth #2: Services Such as Tor and VPNs Make Me Completely Anonymous

Tor is free software that helps you defend against traffic analysis, a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security. It offers tremendous anonymity from companies that harvest your data, your ISP, and even the government to a degree. (Also used by hackers for illegitimate purposes.)

A VPN encrypts all of your traffic so you can be sure your communications are secure.

However, these and other services are not foolproof. A skilled and determined hacker can decrypt just about anything!

Myth #3: MAC Filtering and Disabling SSID Will Protect my Wi-Fi Network

Both of these strategies will provide some protection but will not stop a hacker or piece of malware from breaking in.

MAC (Media Access Control) filtering basically permits or denies network access to specific devices through the use of blacklists and whitelists. It is mostly futile against serious hackers or botnet.

Equally futile is hiding your wireless network's SSID (Service Set Identifier). It may keep your nosy neighbor from seeing the name of your network, but as soon as you use your wireless network, you send your SSID name over the air anyway.

Myth #4: Incognito Mode Protects My Privacy

Incognito mode does protect your privacy -- but only from other people using your computer. However, it does not protect you from everybody and everything on the Internet. Even though you're warned each time you open an Incognito window, many people still think that browsing in Incognito mode means they can't be tracked, their ISP can't see what they're browsing, or they're somehow anonymous to the party on the other end of their connection. Unfortunately, none of the above is true.

Myth #5: I Don't Need Anti-Malware Because I Don't Do Anything Risky

This is perhaps the biggest and most persistent computer security myth. Even if you think you don't do anything risky, you are always at risk from threats and attacks. It's wise to install anti-malware security, such as VIPRE Antivirus. VIPRE combines powerful antivirus and anti-spyware technologies with automated patching of vulnerable software, a firewall to stop malicious web traffic, an anti-spam filter, and a bad website blocker.

ATM Skimmers: How to Protect Your ATM Card

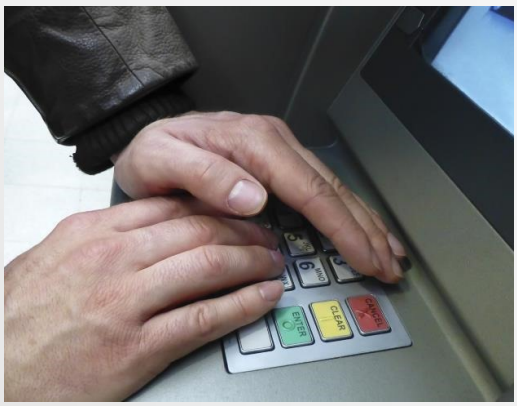
ATM skimmers generally store the data they capture on the device itself. The criminals have to come back and retrieve the skimmer to get the data it's captured. However, more ATM skimmers are now transmitting this data wirelessly over Bluetooth or even cellular data connections.

How to Spot ATM Skimmers

Here are some tricks for spotting ATM skimmers. You can't spot every ATM skimmer, but it won't hurt to take a quick look around before withdrawing money.

Jiggle the Card Reader: If the card reader moves around when you try to jiggle it with your hand, something probably isn't right. A real card reader should be attached to the ATM so well that it won't move around — a skimmer overlaid over the card reader may move around.

Look at the ATM Machine: Take a quick look at the ATM machine. Does anything look a bit out-of-place? Perhaps the bottom panel is a different color from the rest of the machine because it's a fake piece of plastic placed over the real bottom panel and the keypad. Perhaps there's an odd-looking object that contains a camera.



Examine the Keypad: Does the keypad look a bit too thick, or different from how it usually looks if you've used the machine before? It may be an overlay over the real keypad.

Check for Cameras: Consider where an attacker might hide a camera — somewhere above the screen or keypad, or even in the brochure holder on the machine.

If you find something seriously wrong — a card reader that moves, a hidden camera, or a keypad overlay — be sure to alert the bank or business in charge of the ATM. If something just doesn't seem right with the machine, go find another ATM machine.

Basic Security Precautions

You can find common, cheap ATM skimmers with tricks like attempting to jiggle the card reader. But here's what you should always do to protect yourself when using any ATM machine:

Shield Your PIN With Your Hand: When you type your PIN into an ATM machine, shield the PIN pad with your hand. Yes, this won't protect you against the most sophisticated skimmers that use keypad overlays, but you're much more likely to run into an ATM skimmer that uses a camera — they're much cheaper for criminals to purchase. This is the number one tip you can use to protect yourself.

Monitor Your Bank Account Transactions: You should regularly check your bank accounts and credit card accounts online. Check for suspicious transactions and notify your bank as quickly as possible. You want to catch these problems as soon as possible — don't wait until your bank mails you a printed statement a month after money has been withdrawn from your account by a criminal.

Tools like Mint.com — or an alert system your bank might offer — can also help here, notifying you when unusual transactions take place.

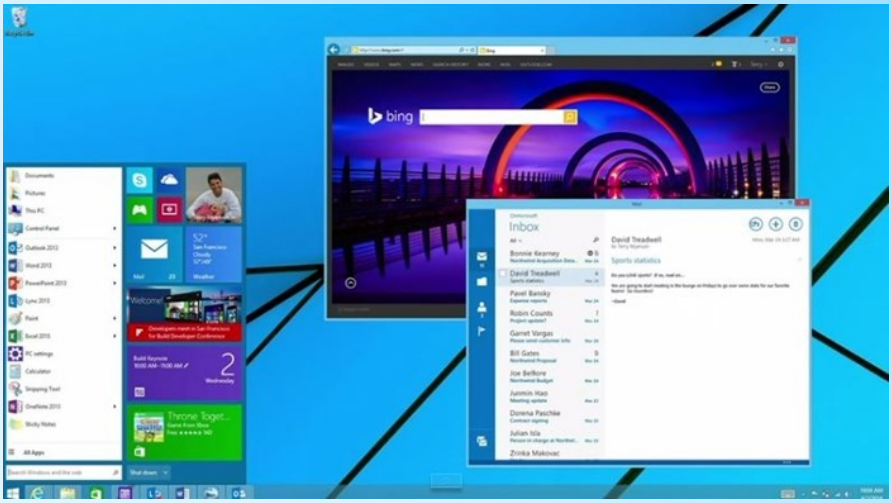
To learn more about this terrifying topic — or just to see photos of all the skimming hardware involved — check out Brian Krebs' All About Skimmers series over at Krebs on Security.

Image Credit: Aaron Poffenberger on Flickr, nick v on Flickr

Into Windows

Admin Updated on Jul 21st, 2014

4 Simple Reasons Why Windows 9 Will Be A Big Hit Like Windows 7



Millions of PC users are eagerly waiting for the next version of Windows. Now that Windows 8 and an update to the same have failed to impress most PC users, it's obvious that Microsoft will try to ship the next major version of Windows operating system as early as possible and will try its best to make it good and better than Windows 8.1.

More than once Microsoft has confirmed that the development of next version of Windows is in progress and will include a Start menu!

If early reports and indications are anything to go by, the upcoming version of Windows, likely be named as Windows 9, will be a big hit and will be more or less like Windows 7. Following are the four reasons why Windows 9 will be look and feel like Windows 7. What this also means that, those of you looking for a radically different operating system might be disappointed with the next big release.

Reason 1 Start menu is returning

To start with, Windows 9 will ship with a Start menu for traditional desktop and laptop users. The all new Start menu will include live tiles (just like in Windows 8/8.1) and will look more or less like the Start menu in Windows 7. While it's not still clear whether Microsoft will release another update to Windows 8.1 to offer Start menu or will include the Start menu only with the next major release of Windows, the all new Start menu will probably see the light of the day with the next version of Windows, Windows 9.

Reason 2 Modern apps can be run just like traditional programs

At its Worldwide Partner Conference, Microsoft has confirmed that modern apps or the apps installed from the Store can be resized and run just like traditional desktop programs in the next version of Windows.

Reason 3 Microsoft is listening to your feedback and actively using it

At the recently concluded WPC, Microsoft has clearly told the world that it's listening to the feedback received from millions of Windows users and actively using the same to build the next version of Windows.

As we all know, most Windows users want to see Windows 7 in the next version of Windows, and Microsoft will make Windows 9 more or less like Windows 7 based on the feedback received by PC users to avoid delivering another Windows 8.

Reason 4 Start screen is not coming for desktop users

There is so much negativity around the Start screen that most PC users are hesitating to upgrade to Windows 8/8.1 just because of this Start screen and modern interface. While I personally like the Start screen in Windows 8 and love the improved Start screen in Windows 8.1 Update 1, not all users are aware of the fact that it's highly customizable and offers more features than the Start menu in Windows 7.

In Windows 9, the Start screen will likely appear only if the Windows is installed on a computer that supports touch. In other words, Start screen will continue to appear for tablet users and you can expect an option to turn on or off the Start screen on desktops and laptops without touch screen.

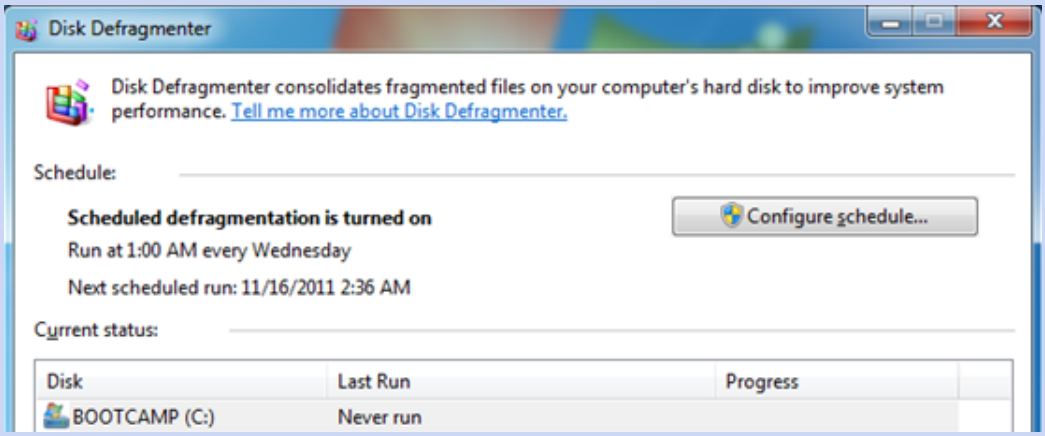
Charlotte Bytes

See us on the Web
www.cccgc.net

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

CCCGC

Do You Really Need to Defrag Your PC?



Ask any PC tech person how to make your computer faster, and almost every one of them will tell you to defrag your PC. But do you really need to manually trigger a defrag these days?

The quick answer: You don't need to manually defragment a modern operating system. The longer answer: let's go through a couple scenarios and explain so you can understand why you probably don't need to defrag.

If You're Using Windows with an SSD Drive

If you're using an SSD (Solid State Drive) in your computer, you should not be defragmenting the drive to avoid excessive wear and tear—in fact, Windows 7 or 8 is smart enough to disable defrag for SSD drives. Here's what Microsoft's engineering team has to say on the subject:

Windows 7 will disable disk defragmentation on SSD system drives. Because SSDs perform extremely well on random read operations, defragmenting files isn't helpful enough to warrant the added disk writing defragmentation produces…

….the automatic scheduling of defragmentation will exclude partitions on devices that declare themselves as SSDs.

If you're running Windows Vista, you should make sure to disable the automatic defrag and question your operating system choices, and if you're using Windows XP with an SSD, one has to wonder why you'd have such an expensive solid state drive running with an ancient and unsupported operating system when you could switch to Linux instead.

If you're running Windows Vista, you should make sure to disable the automatic defrag and question your operating system choices, and if you're using Windows XP with an SSD, one has to wonder why you'd have such an expensive solid state drive running with an ancient and unsupported operating system when you could switch to Linux instead.

RELATED ARTICLE

HTG Explains: Should You Use an SSD Optimization Utility?

Traditional mechanical disk drives need to be defragmented for optimum performance, although Windows now does a good job of doing...
[Read Article] http://www.howtogeek.com/170752/htg-explains-should-you-use-an-ssd-optimization-utility/

If You're Running Windows 7 or 8.x

If you're using either Windows 7, 8, or even Vista, your system is already configured to run defrag on a regular basis—generally 1 AM every Wednesday. You can check for yourself by opening up Disk Defragmenter and seeing the schedule there, as well as the last run and fragmentation levels.

For instance, in the screenshot below, you'll see that the last time it ran just a few days ago, and there was zero percent fragmentation. Clearly the schedule is working just fine.

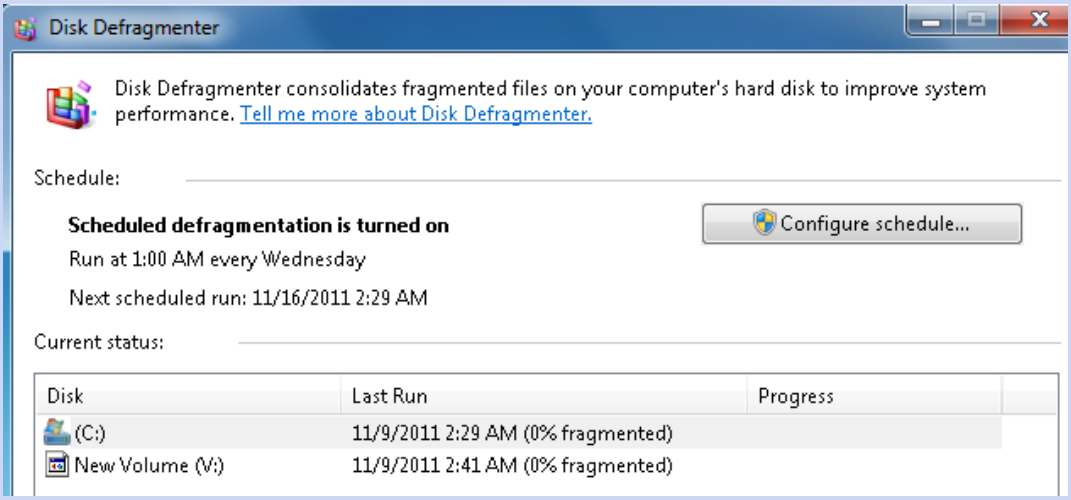
Continued on next page

CCCGC

Charlotte Bytes

Do You Really Need to Defrag Your PC?

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

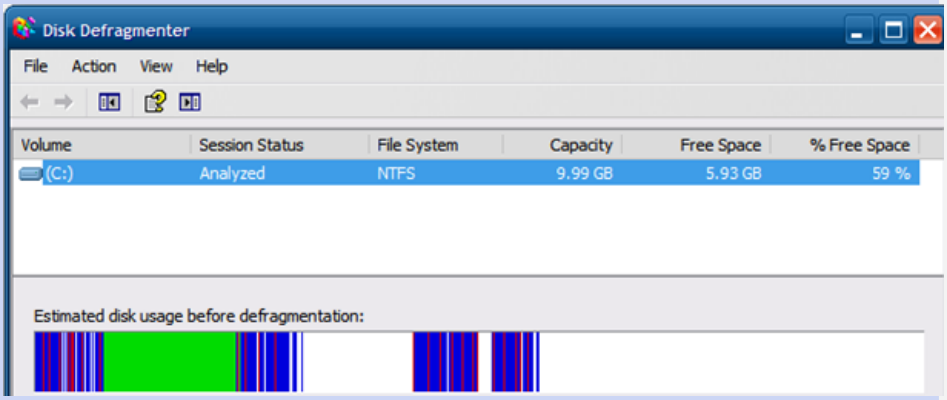


The one exception to this rule is if you turn your PC off every time after using it—essentially, if you never let the PC sit idle at all, the defrag task will never get a chance to run. This is probably not the case, but if you check and your drive hasn't been defragged in a while, you might have to start doing it manually.

Windows XP

Sadly there's no automatic defragmenter in Windows XP, which isn't surprising since it's 10 years old. This also means that you are going to need to either manually defragment the drive on a regular basis. How regular? Well, that depends on how much data you're creating, downloading, writing, and deleting. If you're a heavy user, you need to run it once a week. Light user, maybe once a month.

Luckily there's a much better option—you can quickly and easily setup an automatic defrag in Windows XP using task scheduler. It's pretty simple, and you can configure it to run whenever you want.



Do Third-Party Defrag Utilities Really Matter?

RELATED ARTICLE

6 Things You Shouldn't Do With Solid-State Drives

Solid-state drives are different from the mechanical, magnetic hard drives in wide use. Many of the things you've done with...

[Read Article] http://www.howtogeek.com/165472/6-things-you-shouldnt-do-with-solid-state-drives/

It's impossible to write an article about defrag and not at least mention third-party defrag utilities—but unfortunately we don't have solid benchmarks to prove that they improve performance better than the default defrag built into Windows. Our general, non-scientific testing has shown that commercial defrag utilities definitely accomplish the task a little better, adding features like boot-time defrag and boot speed optimization that the built-in defrag doesn't have. They can generally defrag system files a little better, and they usually include tools for defragging the registry as well.

But here's what they won't tell you: Over the years, as hard drives have gotten much faster at both sequential and random reads and writes, the usefulness of defrag has dropped a bit. Your hard drive 10 years ago only had to be partially fragmented to cause system slowdown, but these days, it'll require a very fragmented drive to make that happen. Another factor are the giant hard drives in modern computers, which have enough free space that Windows doesn't have to fragment your files in order to write them to the drive.

Conclusion on page 15

CCCGC

Charlotte Bytes

Comcast is turning your home router into a public Wi-Fi hotspot

By Jose Pagliery @Jose_Pagliery June 16, 2014: 11:08 AM ET

It's been one year since Comcast started its monster project to blanket the entire nation with continuous Wi-Fi coverage. Imagine waves of wireless Internet emitting from every home.

It's potentially creepy and annoying. But the upside is Internet everywhere.

If you're a Comcast cable customer, your home's private Wi-Fi router is being turned into a public hotspot.

It's been one year since Comcast (CMCSA) started its monster project to blanket residential and commercial areas with continuous Wi-Fi coverage. Imagine waves of wireless Internet emitting from every home, business and public waiting area.

Comcast has been swapping out customers' old routers with new ones capable of doubling as public hotspots. So far, the company has turned 3 million home devices into public ones. By year's end it plans to activate that feature on the other 5 million already installed.

Anyone with an Xfinity account can register their devices (laptop, tablet, phone) and the public network will always keep them registered -- at a friend's home, coffee shop or bus stop. No more asking for your cousin's Wi-Fi network password.

But what about privacy? It seems like Comcast did this the right way.

See your online secrets revealed

Outsiders never get access to your private, password-protected home network. Each box has two separate antennae, Comcast explained. That means criminals can't jump from the public channel into your network and spy on you.

And don't expect every passing stranger to get access. The Wi-Fi signal is no stronger than it is now, so anyone camped in your front yard will have a difficult time tapping into the public network. This system was meant for guests at home, not on the street.

As for strangers tapping your router for illegal activity: Comcast said you'll be guilt-free if the FBI comes knocking. Anyone hooking up to the "Xfinity Wi-Fi" public network must sign in with their own traceable, Comcast customer credentials.

Still, no system is foolproof, and this could be unnecessary exposure to potential harm. Craig Young, a computer security researcher at Tripwire, has tested the top 50 routers on the market right now. He found that two-thirds of them have serious weaknesses. If a hacker finds one in this Comcast box, all bets are off.

"If you're opening up another access point, it increases the likelihood that someone can tamper with your router," he said.

Official Publication of the Charlotte County Computer Group Corp.

PROMOTING COMPUTER LITERACY AND EDUCATION IN CHARLOTTE COUNTY

Conclusion from page 12

Comcast is turning your home router into a public Wi-Fi hotspot

Related: Stalker is a creepy look at you, online

What about connection speed? Having several people tapping a single machine tends to clog

With two separate networks, each antenna has its own data speed cap. Comcast said the private channel provides whatever speed customers already pay to get (most have 25 Megabits per second). The public hotspot channel is given 15 Mbps and allows up to five people to connect at a time.

That means having your data-hungry friends over shouldn't slow down your Netflix (NFLX, Tech30) stream.

Comcast spokesman Charlie Douglas promised "there's more than enough capacity" in the cables connecting to people's homes to make this work.

"You shouldn't experience any conflict between the two networks," he said. "It's something our engineers thought about carefully. The last thing we want to allow is to create a bad user experience."

Comcast's project that started in northern New Jersey has now spread to Boston, Chicago, Houston, Indianapolis, Minneapolis, Philadelphia, San Francisco, Seattle and elsewhere.

"Before this, there was no value in having Internet when you're not at home," Douglas said. "Every time you left the house you walked away from your subscription. But with all these hotspot locations, you can connect to the Internet remotely. Everyone's device is mobile. It makes a lot of sense."

But what if you hate the idea of your private boxes turned into public hotspots? You can turn it off by calling Comcast or logging into your account online. The company says fewer than 1% of customers have done that so far.

See next page to disable your Comcast boxes.

CCCGC

Microsoft REGISTERED Refurbisher

Charlotte Bytes

BGR Topics

Internet

How to Disable Comcast Xfinity Wi-Fi Hotspot

By Chris Smith on Jun 11, 2014 at 1:12 PM

Comcast has a brand new feature for its Internet subscribers called Xfinity Wi-Fi, but it's going about it the wrong way, likely making even more enemies in the process. SeattlePi reports that Comcast is turning some of the Wi-Fi routers placed in the homes of subscribers into a "massive public Wi-Fi hotspot network," but it's doing so without giving customers the opportunity to opt out before the service is rolled out.

In theory, Xfinity Wi-Fi sounds like a neat idea, as it can provide free Internet access to other Xfinity subscribers as long as they're within reach of such an Xfinity Wi-Fi hotspot. Moreover, the extra load on the router does not affect the bandwidth of the customer who houses it, as the device creates two independent networks, one private, and one public, using additional bandwidth for the public one.

As such, any users on the public Xfinity Wi-Fi network will not slow down customers' connections, according to the company.

Comcast apparently informed its subscribers about the move in the mail a few weeks ago, and then email notifications go out after the service is turned on for each user. The company on Tuesday turned 50,000 Comcast Internet customers into public Wi-Fi providers in Houston, with 100,000 more hotspots to be activated by the end of June.

Users only have the opportunity to disable the service after it's activated. A Comcast FAQ section further details Xfinity Wi-Fi, while the following guide, as listed by SeattlePi, should help Comcast customers disable the new Xfinity Wi-Fi hotspot feature:

Log into your Comcast account page at customer.comcast.com.

Click on Users & Preferences.

Look for a heading on the page for "Service Address." Below your address, click the link that reads "Manage Xfinity WiFi."

Click the button for "Disable Xfinity Wifi Home Hotspot."

Click Save

Charlotte Bytes

CCCGC

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

See us on the Web
www.cccgc.net

Do You Really Need to Defrag Your PC? Conclusion from page 11

RELATED ARTICLE

HTG Reviews the Blazing Fast LaCie External SSD (Thunderbolt / USB 3.0)

If you need really fast external storage for your laptop, you might be interested to know that you can buy an... [Read Article] http://www.howtogeek.com/180094/htg-reviews-the-blazing-fast-lacie-external-ssd-thunderbolt-usb3/

If you're looking to eek every last drop of performance out of your spinning hard drive, a third-party defrag utility is probably what you need… or you could put that cash towards a new SSD, which would massively increase performance.

Wrapping Up

Didn't feel like reading the whole article? Skipped down to here for some unknown reason? Here's the quick version:

(Fastest) Windows with an SSD Drive: Don't Defrag.

Windows 7, 8, or Vista: It's automatic, don't bother. (check to make sure the schedule is running)

Windows XP: You should upgrade. Also, you should setup defrag on a schedule.

Bottom line: Upgrade to an SSD and your PC will be fast enough to leave defrag where it belongs: a distant memory.

Conclusion from page 7

The Solution to All Your ID Problems: an Implanted Chip?

If you could have a chip implanted or carry around an ID card that meant you never again had to prove your ID, remember logins and passwords and so on, would you do it? That's the question PCAdvisor.co.uk put to more than 4,000 people. The results might surprise you.

Thirty-nine percent of the 4,095 respondents said they would be willing to carry an ID card or be chipped.

Fifty percent said they would not be willing to have a chip implanted or carry around an ID card in return for the 'freedoms' involved.

"I do not have to be doing something illegal to want aspects of my private life to remain private," wrote one person. "We already have controversy over GCHQ (Government Communications Headquarters) monitoring various aspects of technology using the excuse of combatting terrorism, so do we really want chips that allow even more governmental intrusion into our lives?"

"We all have some form of ID, but we do not have a legal requirement to carry it at all times," noted another respondent. "If it gets to the point that it becomes a legal requirement to carry ID at all times then, sorry, but the terrorist has won."

Other respondents suggested that carrying an ID card or chip would ensure that people are correctly identified if they require medical attention. Some people thought that having just one form of identity could also be convenient.