June 2014

Microsoft REGISTERED Refurbisher

Charlotte County Computer Group

30th YEAR Anniversary

1984 - 2014

The Next General Meeting of CCCGC in June will be

Cancelled

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. VI

The President's Platform by Ron Wallis, President CCCGC

Inside this issue:

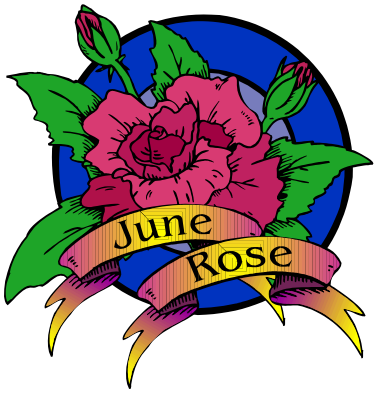
There will NOT be a June Meeting

Our next General Meeting will be July 1st.

The Officers and Board of Directors have revised the Charlotte County Computer Group Corp. By-Laws. The revisions were voted and approved at a Board meeting on May 6th 2014.

The By-Laws will be read to the membership and voted on at the July 1st General meeting.

The revised By-Laws will be available to all members, and can be read on our office computer.



Charlotte County Computer Group

2280 Aaron Street
Port Charlotte, FL 33952

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

Charlotte Bytes

Computer Drawing

Art Lyons was wishing he could win the computer to replace the one that just crashed. Out popped the ticket and he was declared the winner. He and his son packed up the computer and off they went. For all those that purchased a ticket, better luck next month.

50/50 Winner

George Buono was all smiles when his ticket was pulled.

He will find something to buy with is new found money.

Door Prize Winners

Left To Right

Karen Prosuch

Bettye Tkacik

Estrella Kaciur

Ron Wallis

Rip Yarnell

WELCOME

New Members

Jackie Polle	**Martha C. King LaFoy**	**Eugene Mikita**
Leola Butterfield	**Scott Drake**	**Eleanor Abplanalp**
Vera Harlin	**Frank Knittel**	**Buz Terry**
Betty Green	**Lynn M Sabin**	**Norma Mansfield**
Ted Swiatek	**Judy Swiatek**	**Julius Palermo**
Tony Battista	**Michael D Gezzar**	**Ruth Ann McGavic**
Frances Kinslow	**Robert Callan**	**Valerie A Rose**
Carolyn A Burke	**Joe Strohmier**	**Dave Wallin**
Robert Hilton		

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

Ron Wallis was the speaker and the subject was EASEUS ToDo Backup and maintenance . You should clean your machine before attempting a backup. There is no reason to back up problems. You can use the website as well to back up your computer.

Go to www.ninite.com to install the programs needed to clean your computer, or check to see if you have the most current version. You definitely need a virus protector and Windows 8 comes with Microsoft Essentials which is free and works in real time. You also need Malware Bytes, C Cleaner and we like Super Anti-spyware. If you run these programs regularly, you can then do a backup that won't have issues in the backup. When using these programs, always check to see if there is an update before you run the program.

Now we are ready to talk about EASE US.

Go to our website cccgc.info and on the right hand side on the top there is a link to EaseUs, download it. After you download the software, install the program on your computer. In order to make an image of the entire computer choose Disk/Partition and backup to the external hard drive. Keep at least two back up images, better yet three would be safer. When you back up the third time, you could delete the first and then repeat this process.

If your hard drive crashes, you can buy a new one put it in the computer and then run this program in reverse or called Restore. You then have your computer restored to the date you did the back up.

L ydia

Charlotte Bytes

Charlotte County Computer Group

Information: (941) 295-7672

(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

Magnetic Stripe Credit Card

VIPRE Security News

Tech Talk May 2014

Is the End Nigh for the Magnetic Stripe Credit Card?

After a spate of highly publicized security breaches at major retailers, notably Target, many

U.S. banks and retailers are looking at their options, including getting rid of the magnetic stripe credit cards.

Last year, about 40 million Target credit and debit card accounts were breached -- compromising customers' credit and debit card numbers, expiration dates, PIN numbers and codes on the cards' magnetic stripes. In addition, about 70 million Target customers had their names, phone numbers, e-mail addresses and mailing addresses compromised.

Target plans to replace its current magnetic stripe cards with ones that have embedded data chips by the first quarter of 2015. MasterCard and Visa have said they want merchants and banks to be ready to start accepting Europay MasterCard Visa (EMV) cards by October 2015.

Debit and credit cards based on the EMV technology use an embedded microchip, instead of a magnetic stripe, to store data and are considered almost impossible to clone for fraudulent purposes.

Another technology that may be adopted is tokenization. This a method for protecting card data by substituting a card's Primary Account Number (PAN) with a unique, randomly generated sequence of numbers, alphanumeric characters, or a combination of a truncated PAN and a random alphanumeric sequence.

With tokenization, credit and debit card data is encrypted at the point where it is captured and sent to the merchant's payment processor where the data is decrypted and the transaction is authorized. The processor then issues a token representing the entire transaction back to the retailer while the actual card number itself is securely stored in a virtual vault.

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

June 2014 CCCGC Events Calendar

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
1	2 **Libre Office** 2 to 4 PM John Palmer	3 **NO General Meeting**	4	5 **Open Forum** 2 to 4 PM Dick Evans	6	7
8	9	10	11 **Writing Family History** 2 to 4 PM Larry Hurley	12 **Open Forum** 2 to 4 PM Dick Evans	13	14
15	16 **AndroidTablets** 2 to 4 PM Yvette Pilch	17 **Maintenance** 2 to 4 PM Ron Wallis	18	19 **Open Forum** 2 to 4 PM Dick Evans	20	21
22	23	24 **Windows 8.1** 2 to 4 PM Ron Wallis	25 **Journey to Meet Ancestor** 2 to 4 PM Larry Hurley	26 **Open Forum** 2 to 4 PM Dick Evans	27	28
29	30 **Backup** 2 to 4 PM Yvette Pilch					

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

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: Mava Graves

We're on the Web
www.cccgc.net

How Connected Standby Works (or Why Your Windows 8 PC's Battery Drains So Fast)

Thinkpad-tablet-2-connected-standby

"Connected Standby" is a new feature in Windows 8. At first, only ARM devices with Windows RT supported Connected Standby. Some Intel Atom PCs with full Windows 8 now support it, too — and it will only become more common.

This is Microsoft's attempt to give Windows 8 and 8.1 the "always-on" state people get from iPads, Android tablets, and smartphones. A PC with Connected Standby can't use other power-management states like Sleep and Hibernate.

What is Connected Standby?

RELATED ARTICLE

HTG Explains: Should You Shut Down, Sleep, or Hibernate Your Laptop?

Computers can sleep, hibernate, or shut down. Sleep allows you to quickly resume using your laptop at the cost of... [Read Article] http://www.howtogeek.com/128507/htg-explains-should-you-shut-down-sleep-or-hibernate-your-laptop/

If you have a typical PC or Mac with an Intel or AMD chip, your computer has several different power states. Your computer is either on, off, or in a power-saving state. Laptops normally go into sleep mode if they're not used for a while or if the lid is closed. In sleep mode, your PC maintains power to its memory so it can start up very quickly. PCs can also hibernate, and may automatically hibernate if you leave them in sleep for a while. In hibernation mode, your PC saves the contents of its memory to its hard drive and shuts down. When you boot it, it loads the system state back from the hard drive and

restores everything you had open. Both sleep and hibernate allow your computer to save its state and get back to it more quickly, but the computer is basically off and can't do anything while sleeping or hibernating.

In contrast, the smartphones and tablets most people use work differently. When you put an iPad, Android tablet, or a smartphone down and leave it for several hours, its screen turns off. The device goes into a very low-power mode. However, it's not in a PC-style "sleep" or "hibernate" mode. Your tablet or phone will check for new emails, receive notifications, and perform other tasks. It does this by frequently waking up. The tablet or phone feels like it's always on — you never have to wait for your phone to boot up from hibernate.

PCs are slower. Even a PC that's asleep will take a second to start back up. After the PC starts up, it has to check for new content. If you're chatting on an instant messaging program, you'll disconnect and not receive any messages when your computer is asleep.

ARM vs. Intel: What It Means for Windows, Chromebook, and Android Software Compatibility

Intel x86 or x64 processors have traditionally been found in laptops and desktops, while ARM processors have been found in... [Read Article] http://www.howtogeek.com/180225/arm-vs.-intel-what-it-means-for-windows-chromebook-and-android-software-compatibility/

Continued on page 13

makeuseof

3 Dangers Of Logging On To Public Wi-Fi

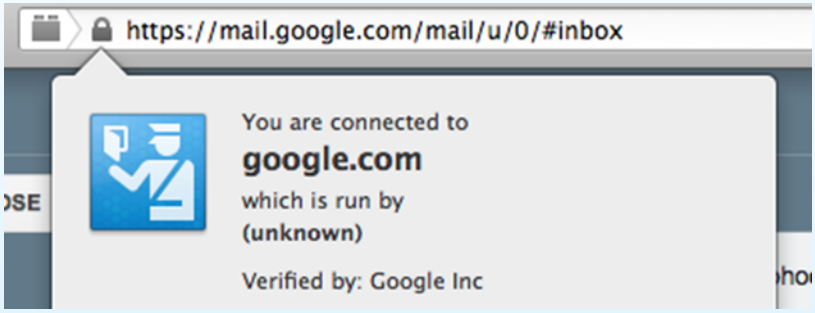
By Justin Pott

You've heard that you shouldn't open PayPal, your bank account and possibly even your email while using public WiFi. But what are the actual risks?

Well, your home WiFi is (hopefully) encrypted; the WiFi at the coffee shop isn't. This means you're at risk of people monitoring your online activity, or worse – unless you know how to protect yourself. Here are a few dangers, and how to avoid them.

Unencrypted Browsing Is Public

WiFi uses radio waves, and radio waves are anything but direct. They broadcast, and this means that anyone within range can see everything you're doing online, if they have the right software.



This means that, without protection, anyone who wants to can see:

- **Every site you visit**
- **Every bit of text you send out**
- **Your login information for various sites**

The danger here is clear, so naturally you're going to want protection. At home, you can encrypt your WiFi network http://www.makeuseof.com/tag/wpa2-wep-and-friends-whats-the-best-way-to-encrypt-your-wi – this prevents snooping by making all of your traffic unreadable with a key. Public WiFi, however, usually isn't encrypted – you can tell this is the case when you don't need to type a password in order to connect.

Does this mean you're defenseless? No.

Your first line of defense is OpenSSL, a kind of encryption offered by many websites: Google, Facebook and most banks, to name a few. This technology encrypts the traffic between you and another site, meaning no one will be able to snoop on that activity. You'll know OpenSSL is on when you see "HTTPS" in your browser's address bar, like this:

You can make such secure connections the default using plugins like HTTPS Everywhere.

OpenSSL isn't bulletproof – it was recently proven to be vulnerable by Heartbleed. Most sites have patched that up at this point, but the bug proved that everything is potentially vulnerable, even with OpenSSL turned on.

Vulnerabilities, and the fact that many websites aren't encrypted at all, mean those deeply concerned about privacy should look into using a VPN (Virtual Private Network). These services route all of your computer's traffic through another server, and usually encrypt that traffic – meaning snooping is impossible. Look into our list of the best VPN services if you're interested, and consider signing up for a service with encryption. It's the best way to completely shield yourself from would-be snoops.

Your Fellow Users May Be Infected

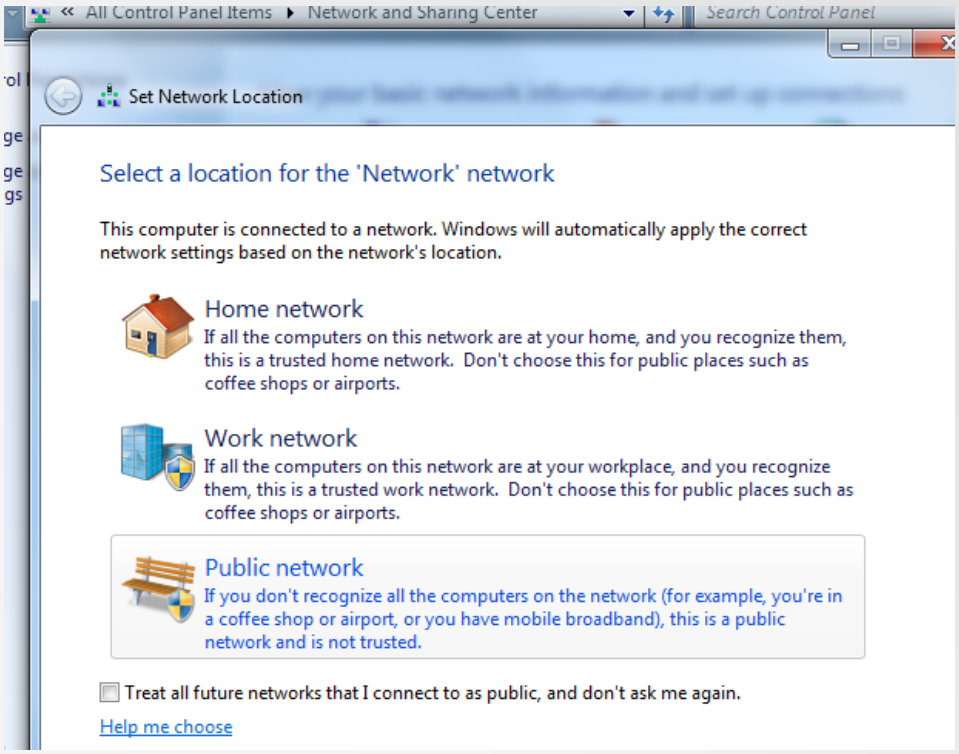
Of course, snooping isn't the only potential danger on a public WiFi network: there's also the risk of malware. Your fellow coffeeshop patron might be running Windows XP SP1 without any malware protection, putting your computer at risk of infection. This is why it's essential to make sure you've got a firewall running when you connect to a public WiFi network. In Windows, the simplest way is to set all public WiFi networks as "Public", when you're prompted:

Continued on page 8

CCCGC

Charlotte Bytes

3 Dangers Of Logging On To Public Wi-Fi



This will turn off your computer's local file sharing, and block most network traffic. Connecting through a VPN would have a similar effect.

Malware protection is also a good idea if you regularly connect to public networks. Check out best of Windows software page for recommendations, if you're not already protected. You'll also find a variety of third-party firewalls, which can also protect you while you're using third party networks.

The WiFi Network May Be A Trap

Sometimes free WiFi seems too good to be true; sometimes, it is. If you're connected to a WiFi network, and have no idea whose network it is, beware: the hotspot might exist entirely to steal your personal data.

Setting up a WiFi network is neither hard nor expensive, and scammers have started doing so in the hopes they can steal passwords and other personal information. If you connect to a network called something like "Free WiFi", with no password required and no welcome screen, it might be a trap.

Connect to one of these networks and you'll think you're connecting to the Internet as-per-usual, but in reality you're falling for an elaborate phishing scam. You won't be able to tell, but you could be entering your email username and password into a fake version of the site you think you're visiting, giving your password to a scammer in the process. OpenSSL can't protect you in such cases – everything will appear to be working as usual.

The exact nature of these attacks can vary, but this outline of a DNS-based attack is worth a read for the technically inclined.

How can you protect yourself from such networks? The best way is to connect to WiFi networks only if you know who's running them. Ask business owners what the name of their network is, to ensure you're connecting to something legitimate.

But even this isn't necessarily enough – it's possible for a coffee shop's network to be hijacked or replaced. If security is essential, consider an encrypted VPN.

Think Ahead

There are other dangers to using public WiFi – scammers are imaginative, and unsecured Internet connections offer a lot of room to use that creativity. But a few key points to keep in mind, if you want to stay safe:

- If your traffic isn't being encrypted, it's being broadcast – and anyone who wants to can listen in.
- Ensure you've turned on your firewall, and have up-to-date malware protection, or you could run into problems.
- If security is a must, consider using public WiFi only through an encrypted VPN service.

I'm sure you can think of other security tips, so please: help your fellow readers in the comments below.

CCCGC

Charlotte Bytes

What is HTTPS and Why Should I Care?

HTTPS, the lock icon in the address bar, an encrypted website connection — it's known as many things. Knowing what it means is important, as it has serious implications banking online, shopping, and avoiding phishing.

When you connect to most websites, your web browser uses the standard HTTP protocol. HTTPS is the secure, encrypted counterpart to HTTP — it literally stands for "HTTP Secure," which is "Hypertext Transfer Protocol Secure."

The Problem With HTTP

When you connect to a website with HTTP, your browser looks up the IP address that corresponds to the website, connects to that IP address, and assumes it's connected to the correct web server. Data is sent over the connection in clear text, so an eavesdropper on a Wi-Fi network, your Internet service provider, or state intelligent agencies like the NSA can see the web pages you're visiting and the data you're transferring back and forth. An eavesdropper could see any passwords, credit cards, or other data if it were sent over HTTP.

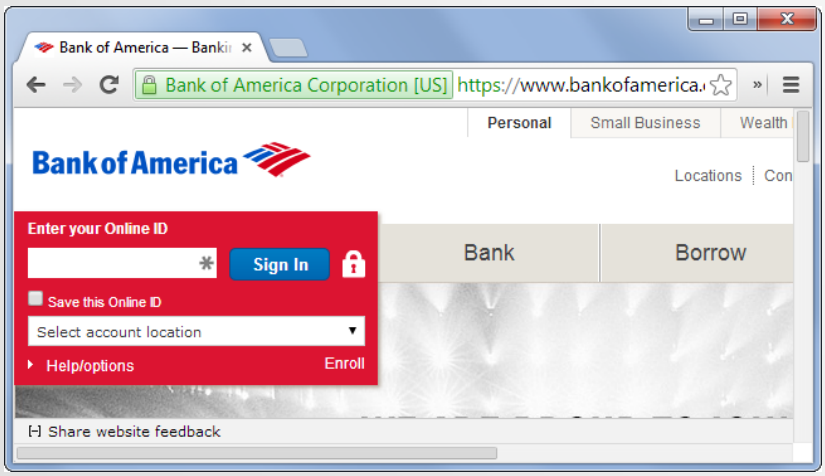
RELATED ARTICLE

HTG Explains: What is Encryption and How Does It Work?

Encryption has a long history dating back to when the ancient Greeks and Romans sent secret messages by substituting letters only decipherable with a secret key. Join us for a quick history lesson and learn more about how encryption works. [Read Article] http://www.howtogeek.com/howto/33949/htg-explains-what-is-encryption-and-how-does-it-work/

There are big problems with this. For one thing, there's no way to authenticate that you're connected to the correct website. Maybe you think you accessed your bank's website, but you're on a compromised network and you were redirected to an impostor website. You want passwords and credit card numbers to be encrypted and secured so no one can eavesdrop on them and steal your personal data. There's also the risk of people eavesdropping on the websites you visit and searches you make.

In short, HTTP has problems because HTTP connections are never encrypted. HTTPS adds encryption in an attempt to fix these problems.



How HTTPS Solves This Problem

RELATED ARTICLE

HTG Explains: How Browsers Verify Website Identities and Protect Against Imposters

Have you ever noticed that your browser sometimes displays a website's organization name on an encrypted website? This is a... [Read Article]

http://www.howtogeek.com/119723/htg-explains-how-browsers-verify-website-identities-and-protect-against-imposters/

Continued on next page

Charlotte Bytes

See us on the Web
www.cccgc.net

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

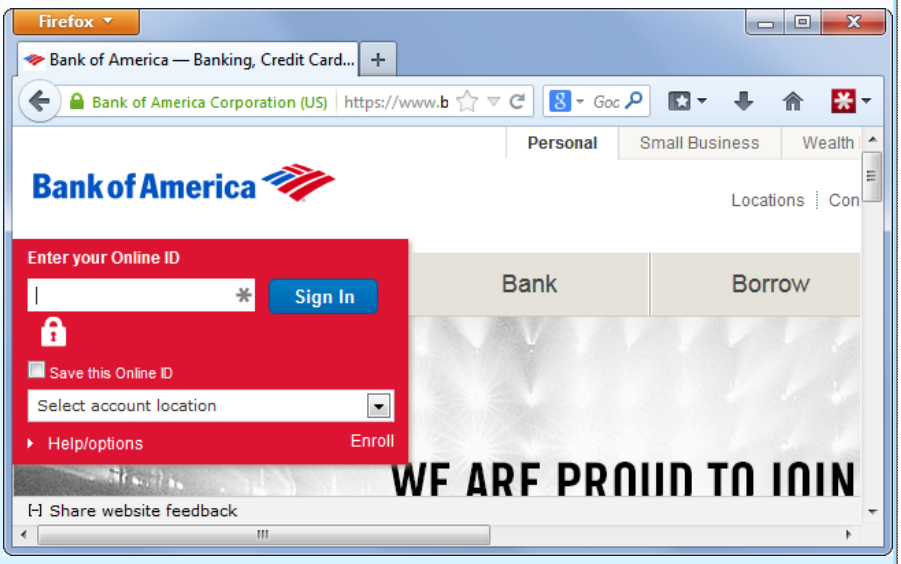
CCCGC

What is HTTPS and Why Should I Care?

HTTPS isn't perfect, but it's certainly much more secure than HTTP. When you connect to an HTTPS secured server — secure sites like your bank's will automatically redirect you to HTTPS when you attempt to log in — your web browser checks the web-site's security certificate and verifies it was issued by a legitimate certificate authority. This helps you ensure that, if you see "https://bank.com" in your web browser's address bar, you're actually connected to your bank's real website — the certificate issuing authority vouches for them. Unfortunately, certificate authorities sometimes issue bad certificates and the system breaks down. Although it isn't perfect, the presence of HTTPS is still helpful.

When it comes time to log in or send other personal data like a credit card number and payment details, this data should be sent over an encrypted connection with HTTPS. This prevents other people from eavesdropping on your sensitive data.

HTTPS also provides additional privacy. For example, Google's search engine now defaults to HTTPS connections. This means that people can't see what you're searching for on Google.com — previously, anyone on the same Wi-Fi network would be able to see your searches. If a connection to Wikipedia is en-crypted with HTTPS, people wouldn't be able to see which article you're viewing on Wikipe-dia. They could only see that you're connected to Wikipedia.



Identifying HTTPS Websites

You can tell you're connected to a website with an HTTPS connection if the address in your web browser's address bar starts with https://. You'll also see a lock icon, which you can click for more information about the web-site's security. This looks a bit different in each browser, but all browsers have the https:// and lock icon in common.

When You Should Care

HTTPS is important whenever you're logging into something or giving payment details. If you're about to enter a password or other personal information, check your address bar and ensure that you're on an HTTPS site. If you're not, it's not really safe to enter such sensitive data. Most websites should be doing this properly now, but a badly coded site may still send your sensitive data in unsecured plain-text if it's set up to connect over HTTP.

RELATED ARTICLE

Why Using a Public Wi-Fi Network Can Be Dangerous, Even When Accessing Encrypted Websites

"Don't do your online banking or anything sensitive on a public Wi-Fi network." The advice is out there, but why... [Read Article]
http://www.howtogeek.com/178696/why-using-a-public-wi-fi-network-can-be-dangerous-even-when-accessing-encrypted-websites/

HTTPS is also valuable because it provides some verification of website identities. If you're using an unfamiliar network and you connect to your bank's website, ensure that you see the HTTPS and the correct website address. This helps you ensure that you're actually connected to the bank's website, although it's not a foolproof solution. If you don't see an HTTPS indicator on the login page, you may be connected to an impostor website on a compromised network.

Conclusion on page 15

CCCGC

Charlotte Bytes

What the Heartbleed Bug Is and Why You Need to Change Your Passwords Now !

SSL (Secure Sockets Layer) is a standard security technology for establishing an encrypted link between a server and a client—typically a web server (website) …

HTTPS or HTTP over SSL is a way to encrypt data sent and received over the Web so that monetary and other sensitive transactions are secure…

The last time we alerted you to a major security breach was when Adobe's password database was compromised, putting millions of users (especially those with weak and frequently reused passwords) at risk. Today we're warning you about a much bigger security problem, the Heartbleed Bug, that has potentially compromised a staggering 2/3rds of the secure websites on the internet. You need to change your passwords, and you need to start doing it now.

Important note: How-To Geek is not affected by this bug.

What Is Heartbleed and Why Is It So Dangerous?

In your typical security breach, a single company's user records/passwords are exposed. That's awful when it happens, but it's an isolated affair. Company X has a security breach, they issue a warning to their users, and the people like us remind everyone it's time to start practicing good security hygiene and update their passwords. Those, unfortunately, typical breaches are bad enough as it is. The Heartbleed Bug is something much, much, worse.

The Heartbleed Bug undermines the very encryption scheme that protects us while we email, bank, and otherwise interact with websites we believe to be secure. Here is a plain-English description of the vulnerability from Codenomicon, the security group that discovered and alerted the public to the bug:

The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. This weakness allows stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet. SSL/TLS provides communication security and privacy over the Internet for applications such as web, email, instant messaging (IM) and some virtual private networks (VPNs).

The Heartbleed bug allows anyone on the Internet to read the memory of the systems protected by

service providers and to encrypt the traffic, the names and passwords of the users and the actual content. This allows attackers to eavesdrop on communications, steal data directly from the services and users and to impersonate services and users.

That sounds pretty bad, yes? It sounds even worse when you realize roughly two-thirds of all websites using SSL are using this vulnerable version of OpenSSL. We're not talking small time sites like hot rod forums or collectible card game swap sites, we're talking banks, credit card companies, major e-retailers and e-mail providers. Worse yet, this vulnerability has been in the wild for around two years. That's two years someone with the appropriate knowledge and skills could have been tapping into the login credentials and private communications of a service you use (and, according to the testing conducted by Codenomicon, doing it without a trace).

Although no group has come forward to flaunt all the credentials and information they siphoned up with the exploit, at this point in the game you have to assume that the login credentials for the web sites you frequent have been compromised.

Continued on next page

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

What the Heartbleed Bug Is and Why You Need to Change Your Passwords Now!

What to Do Post Heartbleed Bug

Any majority security breach (and this certainly qualifies on a grand scale) requires you to assess your password management practices. Given the wide reach of the Heartbleed Bug this is a perfect opportunity to review an already smooth-running password management system or, if you've been dragging your feet, to set one up.

Before you dive into immediately changing your passwords, be aware that the vulnerability is only patched if the company has upgraded to the new version of OpenSSL. The story broke on Monday, and if you rushed out to immediately change your passwords on every site, most of them would still have been running the vulnerable version of OpenSSL.

If you're practicing lax password management and hygiene, it's only a matter of time until one of the increasingly numerous...
[Read Article] http://www.howtogeek.com/176038/how-to-run-a-last-pass-security-audit-and-why-it-cant-wait/

Now, mid-week, most sites have begun the process of updating and by the weekend it's reasonable to assume the majority of high-profile web sites will have switched over.

You can use the Heartbleed Bug checker here to see if the vulnerability is open still or, even if the site isn't responding to requests from the aforementioned checker, you can use LastPass's SSL date checker to see if the server in question has updated their SSL certificate recently (if they updated it after 4/7/2014 it's a good indicator that they've patched the vulnerability.) Note: if you run howtogeek.com through the bug checker it will return an error because we don't use SSL encryption in the first place, and we have also verified that our servers are not running any affected software.

That said, it looks like this weekend is shaping up to be a good weekend to get serious about updating your passwords. First, you need a password management system. Check out our guide to getting started with LastPass to set up one of the most secure and flexible password management options around. You don't have to use LastPass, but you do need some sort of system in place that will allow you to track and manage a unique and strong password for every website you visit.

Second, You need to start changing your passwords. The crisis-management outline in our guide, How to Recover After Your Email Password Is Compromised, is a great way to ensure you don't miss any passwords; it also highlights the basics of good password hygiene, quoted here:

Passwords should always be longer than the minimum the service allows for. If the service in question allows for 6-20 character passwords go for the longest password you can remember.

Do not use dictionary words as part of your password. Your password should never be so simple that a cursory scan with a dictionary file would reveal it. Never include your name, part of the login or email, or other easily identifiable items like your company name or street name. Also avoid using common keyboard combinations like "qwerty" or "asdf" as part of your password.

Use passphrases instead of passwords. If you're not using a password manager to remember really random passwords (yes, we realize we're really harping on the idea of using a password manager) then you can remember stronger passwords by turning them into passphrases. For your Amazon account, for example, you could create the easily remember passphrase "I love to read books" and then crunch that into a password like "!luv2ReadBkz". It's easy to remember and it's fairly strong.

Third, whenever possible you want to enable two-factor authentication. You can read more about two-factor authentication here, but in short it allows you to add an additional layer of identification to your login.

Conclusion on page 15

CCCGC

Charlotte Bytes

How Connected Standby Works (or Why Your Windows 8 PC's Battery Drains So Fast)

Connected Standby is a low-power state that allows Windows 8 and 8.1 to function more like a tablet or smartphone than a typical PC. It's supported on Windows RT devices like the Surface RT and Surface 2, but Intel is also working on adding support for Connected Standby to its own CPUs so Intel-powered tablets can catch up to ARM devices. Your PC will work more like your phone.

How Does Connected Standby Actually Work?

RELATED ARTICLE

What You Need to Know About Buying Touch-Enabled Windows 8.1 PCs

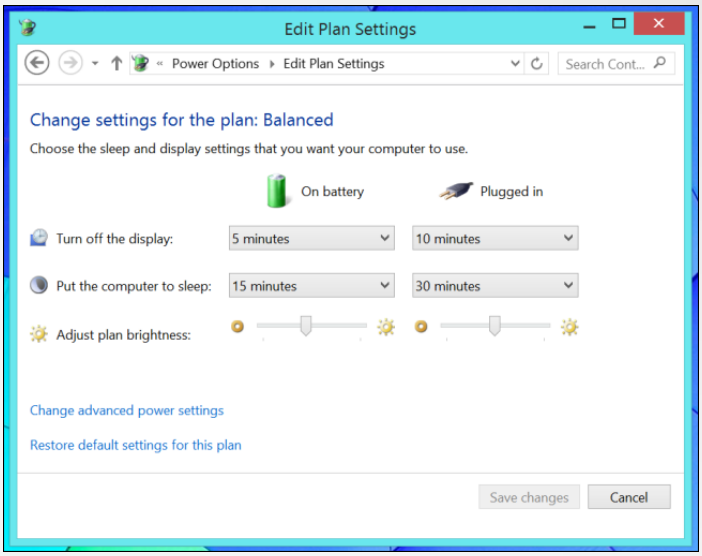
It has now been over a year since Windows 8 was released. A lot has happened — we're now on... [Read Article] http://www.howtogeek.com/175859/what-you-need-to-know-about-buying-touch-enabled-windows-8.1-pcs/

You can't just get Connected Standby on any computer. It requires special support for Connected Standby in the CPU and the rest of the computer system. You buy a Windows device and it either supports Connected Standby or it doesn't.

Connected Standby replaces the standard Sleep and Hibernate power states found on most PCs. This means that you can't actually use Sleep or Hibernate instead of Connected Standby. You can still control how long the display stays on — when the display powers off, Connected Standby begins instead of Sleep.

You can also shut down your PC normally.

When in Connected Standby mode, your PC will listen for notifications and wake up regularly to fetch new emails, update live tiles, and perform other similar tasks. When you get a chat message, your PC can wake up and notify you. Its screen will stay off the whole time while it does this, just as your smartphone can keep doing work while its screen is off. Note that these fetching features only work with Windows 8' s "Store apps", so the full-screen Mail app will fetch new email but your desktop email client won't.



All Windows RT devices use Connected Standby. They have ARM chips, so they support this sort of always-on, low-power state. At the moment, this only includes the Surface RT, Surface 2, and Nokia Lumia 2520 — all devices produced by Microsoft themselves. Windows RT is not popular.

Intel is bringing Connected Standby to more and more chips. Intel's "Clover Trail" series of Atom chips support connected standby. Buy a tablet like the Thinkpad Tablet 2 and it will use Connected Standby rather than standard Sleep and Hibernate features. Connected Standby is a feature ideal for mobile devices with low power consumption, but Intel has become obsessed with catching up to ARM in this space. We wouldn't be surprised to see Connected Standby make its way into higher-power Intel CPUs eventually. This feature will only become more common, even among laptops.

For now, higher-power CPUs like Intel's own Haswell line of Core processors don't support Connected Standby. This does mean that you can't have that sort of always-on, tablet-style experience on Haswell-powered tablets like Microsoft's Surface Pro 2. The device can sleep or hibernate, but not stay on all the time with Connected Standby.

Conclusion 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

How Connected Standby Works (or Why Your Windows 8 PC's Battery Drains So Fast)

How Can I Disable Connected Standby?

Connected Standby can't be disabled, which may be inconvenient if you just want to save power. For example, you can set aside a typical laptop down for several weeks and it should go to sleep and then hibernate, saving most of its battery power.

On the other hand, if you're putting a PC with Connected Standby down for several weeks, it will continue running, regularly waking up to download new content. After several weeks, the device will definitely have an empty battery.

Intel's website states that "A system in Connected Standby stays updated, is reachable through real-time communication apps, and can remain in state a week or more on a single battery charge."

This is great if you want this always-on experience. On the other hand, this means that your laptop's battery will drain when you're not using it and be empty after a week — or less, if you're using it. You may pick up a device a few days later to find a surprising amount of battery power drained.

While you can't disable Connected Standby, you can get around this limitation by powering the tablet or laptop off if you're not going to use it for a while. The device won't wake up if it's powered off completely. This means going through a normal Shut Down process, not just tapping its power button.

You could also enable Airplane Mode before putting your PC to sleep. Your device won't be able to fetch new content or communicate with the Internet at all. It should stay asleep instead of waking up regularly to check on your emails and tweets.

Overall, Connected Standby is a good feature that allows Windows 8.1 tablets and PCs — even those with Intel chips — to function more like the mobile devices they are. Microsoft should still provide a way to let people disable this feature without enabling Airplane Mode every time they put their device to sleep. Many people will get Atom-powered tablets and laptops they'll want to use like PCs without unnecessary battery drain when idle.

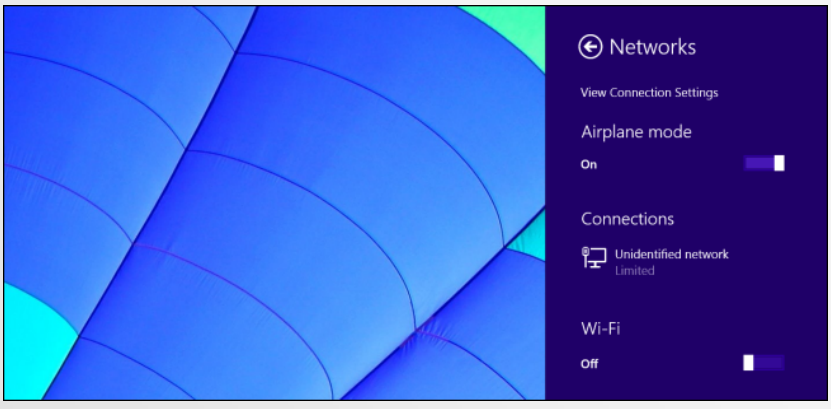


Image Credit: TAKA@P.P.R.S on Flickr, Phil Roeder on Flickr`

Official Publication of the Charlotte County Computer Group Corp.

PROMOTING COMPUTER LITERACY AND EDUCATION IN CHARLOTTE COUNTY

What the Heartbleed Bug Is and Why You Need to Change Your Passwords Now !

RELATED ARTICLE

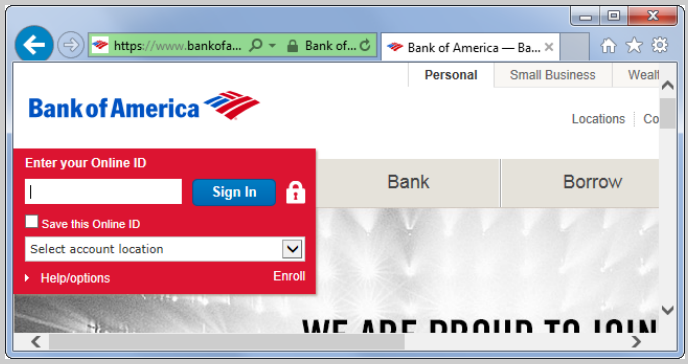
What Is Two-Factor Authentication and Should I Be Using It?

More and more banks, credit card companies, and even social media networks and gaming sites are starting to use two-factor... [Read Article] http://www.howtogeek.com/117047/htg-explains-what-is-two-factor-authentication-and-should-i-be-using-it/

With Gmail, for example, two-factor authentication requires you to have not just your login and password but access to the cell-phone registered to your Gmail account so you can accept a text message code to input when you log in from a new computer. With two-factor authentication enabled it makes it very difficult for someone who has gained access to your login and password (like they could with the Heartbleed Bug) to actually access your account.

Security vulnerabilities, especially ones with such far reaching implications, are never fun but they do offer an opportunity for us to tighten our password practices and ensure that unique and strong passwords keep the damage, when it occurs, contained.

What is HTTPS and Why Should I Care?



Avoiding Phishing Tricks

RELATED ARTICLE

Online Security: Breaking Down the Anatomy of a Phishing Email

In today's world where everyone's information is online, phishing is one of the most popular and devastating online attacks, because... [Read Article] http://www.howtogeek.com/58642/online-security-breaking-down-the-anatomy-of-a-phishing-email/

Some clever phishers have realized that people look for the HTTPS indicator and lock icon and may go out of their way to disguise their websites. You shouldn't click links in phishing emails — but, if you do, you may find yourself on a cleverly disguised page. Nothing stops a scammer from getting a certificate for their scam server, so there's nothing to stop scammers from using HTTPS as well — in theory, they're only prevented from impersonating sites they don't own. You may see an address like https://bankofamerica.com.3526347346435.com. In this case, you're using an HTTPS connection, but you're really connected to a subdomain of a site named 3526347346435.com — not Bank of America.

Other scammers may imitate the lock icon, changing their website's favicon that appears in the address bar to a lock to try to trick you.

Bear in mind that the presence of HTTPS itself isn't a guarantee a site is legitimate. It confirms you're using an encrypted connection and provides some peace of mind that you're connected to the right site, but even that isn't completely guaranteed.