January 2015

Microsoft REGISTERED Refurbisher

The Next General Meeting of CCCGC will be **January 6, 2015**

Charlotte Bytes

Editor
A Yvette Pilch

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. I

The President's Platform by Ron Wallis, President CCCGC

Inside this issue:

Dec Computer Drawing	2
50/50 Winner	2
Door Prize Winners	2
Instal. of Officers & Directors	3
New Members	3
Classes & Events Calendar	4
Firefox/Chrome Browsing Mode	5
Officers & Board of Directors	5
Application Specific Passwords	6
App Specific Passwords Cont.	7
App Specific Passwords Concl	8
Poodle Attacks	9
Poodle Attacks Continued	10
Poodle Attacks Conclusion	11
Understanding Network Hdwre	12
Hardware Continued	13
Hardware Conclusion	14
Businesses Fail Continued	15
Businesses Fail Continued	16
Business Fail Conclusion	17

Charlotte County Computer Group

2280 Aaron Street
Port Charlotte, FL 33952

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

Another year has gone by and it has been a good one for the club. In the past year we have seen a considerable increase in membership and have added to our volunteer staff. We have refurbished over four hundred computers. We have taken care of hundreds of computer problems for our members with our members help program. We have increased the number of classes we teach for our members. It really has been a good year.

At the last meeting we had election of officers and we will have the same executive board as last year with one exception. Yvette, our Vice President, who has been a mainstay of this club for some time, is taking a well-deserved vacation from executive office. We are happy to report that she will be continuing with her many other duties, one of which you are reading. This newsletter is here because of her great editing. We thank her for her loyalty and dedication to the club.

Yvette will be replaced by Dick Evans who I'm sure you all know from the many classes he teaches and the presentations he gives.

We welcome Dick as our new Vice President. I'm sure he will be an asset to the executive board.

We hope you all had a great Christmas and wish you a Happy Healthy New Year.

Ron

Charlotte Bytes
Editor

Computer Drawing

Rose Kopenec was quite surprised when her ticket was pulled out. We packed up the computer and off it went to a new home.

50/50 Winner

Shannon Jones jumped up to claim all the money and you can see in the picture, he was enthusiastic about getting the green stuff.

Door Prize Winners

Left To Right

LARRY PLOWMAN

LIEDA BOYKO

JOHN MADDEN

FRANK MESSINA

KENNETH BRANDEL

WELCOME

New Members

Cindy Martin	**Keith Shortuse**	**Jan Shortuse**
John Grebas	**Linda Grebas**	**Gerald Maxwell**
Nancy Wenger	**Hal Wenger**	**Lisa Fleeman**
Ada Lawson	**Gale West**	**Robert Jacobs**
Monica Wawrzyniak	**Robert Wawrzyniak**	**Susan Joan Sterling**
Betty Sterling	**Dianne Dautell**	**Joe Raskay**
Reggie Bengtson	**Jim Oliver**	**Jean Wydra**
Pattyjean Wydra	**Gerald Allen**	**Ronald Lunsford**
Richard Lehman	**Rosemary Sexton**	**Beverly Murray**
Renate Roberts	**Robert Clauson**	

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

Installation of Officers and Directors for the business year 2015 was conducted by Harold Nixon

President	Ron Wallis
Vice President	Dick Evans
Secretary	Ron Muschong
Treasurer	Larry Hurley
Director	John Hegard
Director	Grover Mudd
Director	Lydia Rist
Director	Frank Messina
Director	Linda Corrick

After the installation all members enjoyed a social evening with coffee and cookies.

.

Lydia Rist Linda Corrick Grover Mudd Ron Muschong Larry Hurley Frank Messina John Hegard Dick Evans Ron Wallis

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

January 2015 CCCGC Events Calendar

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
				1 New Years Day	2	3
4	5 **Libre Office** 2 to 4 PM John Palmer	6 **General Meeting** 7:15 PM Classes 5:00 PM 6:00 PM	7 **Maintenance** 2 to 4 PM Ron Wallis	8 **Open Forum** 2 to 4 PM Dick Evans	9	10
11	12 **AndroidTablets** 2 to 4 PM Yvette Pilch	13	14 **Reflect Backup** 2 to 4 PM Ron Wallis	15 **Open Forum** 2 to 4 PM Dick Evans	16	17
18	19 **Libre Office** 2 to 4 PM John Palmer	20 **Windows 8.1** 2 to 4 PM Ron Wallis	21	22 **Open Forum** 2 to 4 PM Dick Evans	23	24
25	26 **Windows 8.1** 2 to 4 PM Yvette Pilch	27	28 **Maintenance** 2 to 4 PM Ron Wallis	29 **Open Forum** 2 to 4 PM Dick Evans **Board Meeting** 6:30 PM	30	31
		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

PROMOTING COMPUTER LITERACY AND EDUCATION IN CHARLOTTE COUNTY

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 2015

President: Ron Wallis

Vice President: Dick Evans

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

A core difference between Firefox's and Chrome's private browsing mode

By Martin Brinkmann on October 13, 2014

Most modern browsers ship with a private browsing mode that can be started independently from the main browsing session. It prevents the recording of history information in the browser so that information about the private browsing session cannot be retrieved once the window has been closed.

While it is certainly possible to achieve the same goal manually without that mode, for instance by clearing the history, cookies and cache files selectively to erase traces, it is comfortable to use and not as time-consuming.

All private browsing modes work in a similar way. They spawn in a new browser window which is independent from the main session. Users can open tabs in the window and access as many sites as they want.

There is however a difference between how Firefox's private browsing and Chrome's incognito mode function.

If you are using Chrome's incognito mode, you may have noticed that you cannot restore a closed tab in that mode. Not every user requires that functionality but if you happen to use the mode a lot, you may have encountered situations where you closed a tab only to come to a point later on where you needed to re-open it in the browser.

That's not possible however and if you cannot remember the address or the site you opened it from, you are out of luck and cannot open it again.

And Firefox? Firefox handles private browsing windows as their own instances. This means that you can re-open closed tabs when you are using Firefox's private browsing mode. To do so either use Ctrl-Shift-t or right-click on the tab bar and select the undo close tab option from the context menu.

Side note: Opera handles this the same way as Google Chrome, likely because it is also based on Chromium, while Microsoft's Internet Explorer the same way as Firefox.

You may wonder why the implementation differs when it comes to the undoing of tabs in private browsing. There does not appear to be an official answer for that but the most likely explanation is that Firefox and Internet Explorer handle the information on the **window level** while Chromium-based browsers on a **tab level** instead.

Are you using a private browsing mode? Which implementation makes more sense to you?

Warning: Your "Application-Specific Passwords" Aren't Application-Specific

Application-specific passwords are more dangerous than they sound. Despite their name, they're anything but application-specific. Each application-specific password is more like a skeleton key that provides unrestricted access to your account.

"Application-specific passwords" are so-named to encourage good security practices — you're not supposed to reuse them. However, the name may also provide a false sense of security to many people.

Why Application-Specific Passwords Are Necessary

RELATED ARTICLE

HTG Explains: 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/

Two-factor authentication — or two-step verification, or whatever a service calls it — requires two things to log into your account. You have to first enter your password, and then you have to enter a one-time-use code generated by a smartphone app, sent via SMS, or emailed to you.

This is how it normally works when you log into a service's website or a compatible application. You enter your password, and then you're prompted for the one-time code. You enter the code, and your device receives an OAuth token that considers the application or browser authenticated, or something like that — it doesn't actually store the password.

However, some applications aren't compatible with this two-step scheme. For example, let's say you want to use a desktop email client to access Gmail, Outlook.com, or iCloud email. These email clients work by asking you for a password and then they store that password and use it every time they access the server. There's no way to enter a two-step verification code into these older applications.

To fix this, Google, Microsoft, Apple, and various other account providers that offer two-step verification also offer the ability to generate an "application-specific password." You then enter this password into the application — for example, your desktop email client of choice — and that application can happily connect to your account. Problem solved — applications that wouldn't be compatible with two-step authentication now work with it.

Wait a Minute, What Just Happened?

RELATED ARTICLE

Don't Get Locked Out When Using Two-Factor Authentication: 5 Recovery Methods to Set Up

Two-factor authentication secures your accounts with an additional authentication method, often a time-limited code generated by a mobile app. But... [Read Article] http://www.howtogeek.com/130844/secure-yourself-by-using-two-step-verification-on-these-16-web-services/

Most people will probably continue on their way, secure in the knowledge they're using two-factor authentication and are safe. However, that "application-specific password" is actually a new password that provides access to your entire account, bypassing two-factor authentication entirely. This is how these application-specific passwords allow older applications that depend on remembering passwords to function.

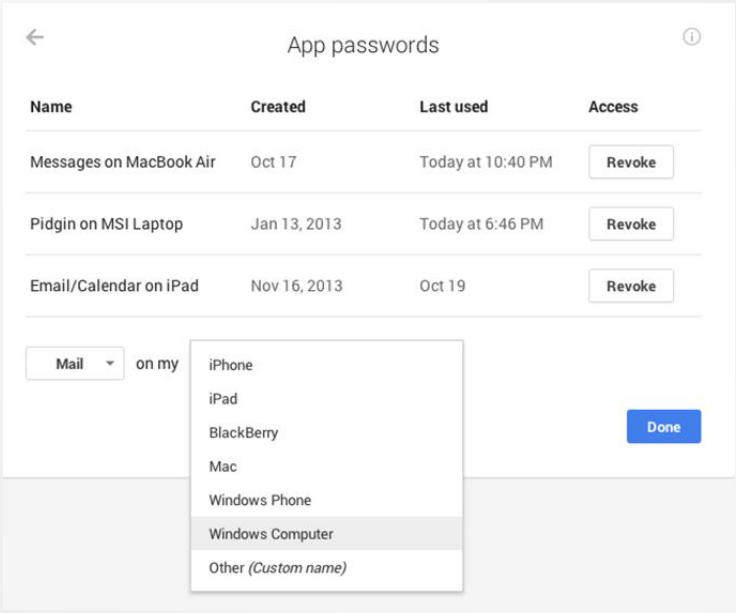
Backup codes also allow you to bypass two-factor authentication, but they can only be used once each. Unlike backup codes, application-specific passwords can be used forever — or until you manually revoke them.

Continued on next page

CCCGC

Charlotte Bytes

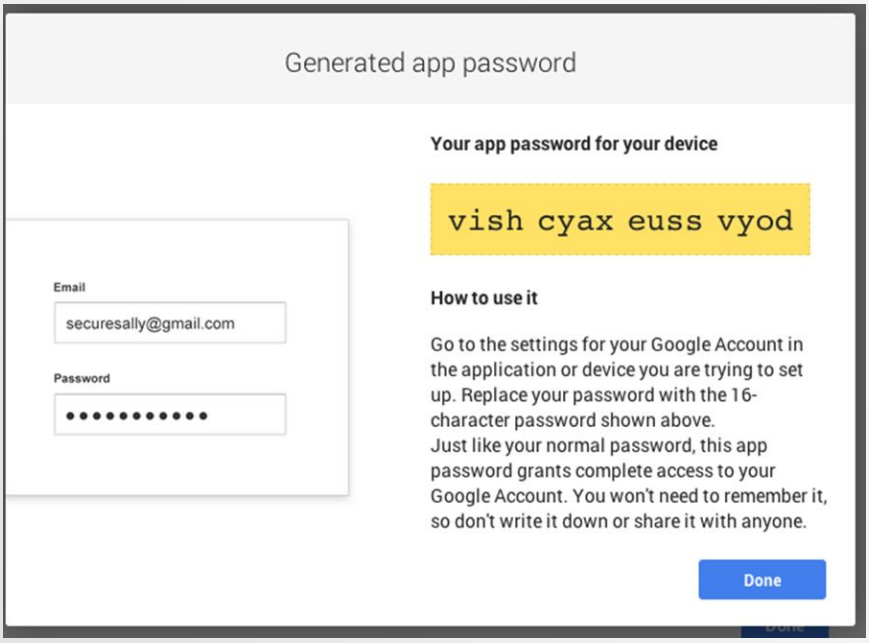
Warning: Your "Application-Specific Passwords" Aren't Application-Specific



Why They're Called Application-Specific Passwords

These are often called application-specific passwords because you're supposed to generate a new one for each application you use. That's why Google and other services don't allow you to actually view these application-specific passwords once you've generated them. They're displayed on the website once, you enter them in the application, and then you ideally never see them again. The next time you need to use such an application, you just generate a new app password.

This does provide some security advantages. When you're done with an application, you can use the button here to "Revoke" an application-specific password and that password will no longer grant access to your account. Any applications using the old password won't work. The app password in the screenshot below was revoked, so that's why it's safe to show it off.



Application-specific passwords are certainly a big improvement over not using two-factor authentication at all. Giving away application-specific passwords is better than giving every application your primary password. It's easier to revoke an app-specific password than to change your main password entirely.

The Risks

If you have five application-specific passwords generated, there are five passwords that can be used to access your accounts The risks are clear:

1. If the password is compromised, it could be used to access your account. For example, let's say you have two-factor authentication set up on your Google account, and your computer is infected by malware. The two-factor authentication would normally protect your account, but the malware could harvest application-specific passwords stored in applications like Thunderbird and Pidgin. Those passwords could then be used to directly access your account.

Conclusion on page 8

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

Conclusion from page 7

Warning: Your "Application-Specific Passwords" Aren't Application-Specific

The Risks Continued

2. Someone with access to your computer could generate an application-specific password and then hold onto it, using it to get into your account without the two-factor authentication in the future. If someone was looking over your shoulder while you generated an application-specific password and captured your password, they'd have access to your account.

3. If you provide an application-specific password to a service or application and that application is malicious, you haven't just given a single application access to your account — the application's owner could pass the password along and other people could use it for malicious purposes.

Some services may attempt to restrict web logins with application-specific passwords, but that's more of a band aid. Ultimately, application-specific passwords provide unrestricted access to your account by design, and there's not much that can be done to prevent it.

We're not trying to scare you too much, here. But the reality of application-specific passwords is that they aren't application-specific. They're a security risk, so you should revoke application-specific passwords you no longer use. Be careful with them, and treat them like the master passwords to your account that they are.

CCCGC

Charlotte Bytes

Protecting yourself from POODLE attacks

(Padding Oracle On Downgraded Legacy Encryption)

By Susan Bradley

No, this isn't about Fluffy gone rogue. To keep our online browsing safe, we rely heavily security protocols — the "S" in HTTPS.

But a new exploit — POODLE — shows that commonly used security protocols aren't as secure as we thought; websites and browsers will both need an upgrade.

Pulling a new trick on a very old dog

By now, it might seem that an exploit is serious only if it has a catchy name attached to it. (I won't go down the list of clever names; doing so might get Windows Secrets blocked by overly cautious ISPs.) The latest threat is **Padding Oracle On Downgraded Legacy Encryption** — POODLE, for short. That's not a name that immediately brings viciousness to mind. As a poodle owner over the years, my greatest worry was being licked to death. But the recently revealed weakness in the Secure Sockets Layer (SSL) protocol that allows the POODLE exploit has the digital-security world worrying about a new round of nasty malware bites.

Perhaps most problematic, there's no quick patch or easy fix; the flaw is hard-coded within SSL 3.0. As Scott Helme explains on his blog, the "attack, specifically against the SSLv3 protocol, allows an attacker to obtain the plaintext of certain parts of an SSL connection, such as the cookie."

A note on terminology here: SSL and TLS (Transport Layer Security) are often referred to simply as SSL. However, TLS officially replaced the SSL 3.0 protocol over a decade ago. But like most things on the Web, the SSL 3.0 protocol lives on and is still in widespread use. (See the Wikipedia "Transport Layer Security" page for more details.) In short, the SSL protocols are all vulnerable; the TLS protocols, as far as we know, aren't.

The POODLE exploit compromises the SSL protocol by forcing the server/browser connection to downgrade its TLS connection to SSL 3.0. That change allows leaks of cookie information, which could then lead to the disclosure of sensitive, personal information.

Fortunately, POODLE is not an easy exploit. It might take an attacker several hundred HTTPS requests before successfully forcing the Web server and a client browser to downgrade to a vulnerable SSL connection. On the other hand, the Web's patchwork nature gives POODLE exploits an extremely large kennel to work in.

Protecting browsers from POODLE attacks

Most of us have two or more browsers installed on our systems. Unlike a Windows fix, there's no one patch that will protect our browsers from POODLE. Instead, we must make adjustments within each browser; with Firefox, we must also download and use a Mozilla add-on until a new version of Firefox arrives in a month or so.

Be aware: After making these adjustments, you might find that business websites don't work properly. So I recommend making the following adjustments to one browser and leaving another browser for those sites that are still waiting for the changes needed to protect themselves from POODLE. (Again, the fix for this exploit has to happen on both ends of Internet connections — the client and the server.)

Continued on page 10

Charlotte Bytes

See us on the Web
www.cccgc.net

Windows Secrets
Everything Microsoft forgot to mention.

CCCGC

Protecting yourself from POODLE attacks (Padding Oracle On Downgraded Legacy Encryption)

The following changes force your browser to not use SSL 3.0. Here's what to adjust in the top three browsers.

Chrome: In Google's browser, edit the shortcut that launches the browser, adding a flag to the end of the Shortcut path. Start by selecting the icon normally used to launch Chrome. Right-click the icon and select Properties. Under the Shortcut tab, find the box labeled "Target" and insert --ssl-version-min=tls1 immediately after chrome.exe" (see Figure 1). It should look something like this (note the space between .exe" and --ssl-):"C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" --ssl-version-min=tls1

(Note: If your original Chrome path doesn't start and end with quotes, don't add one after chrome.exe.)

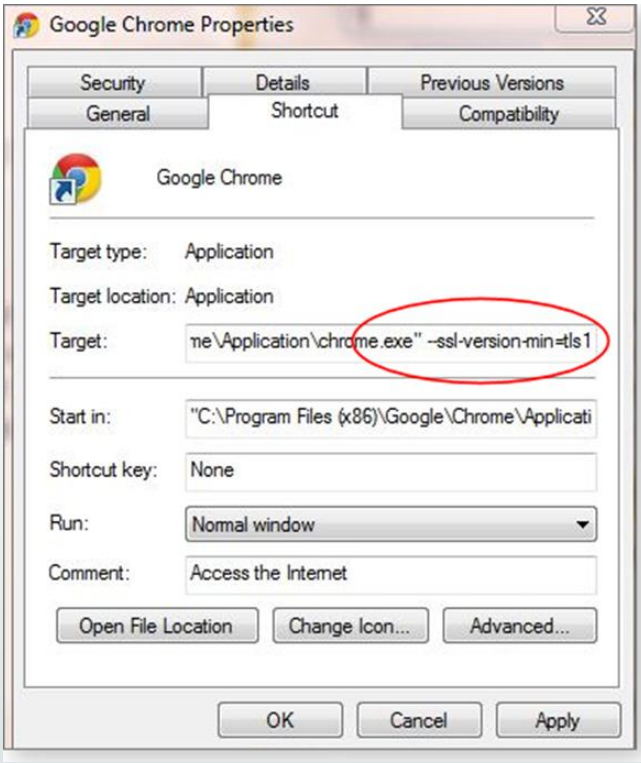


Figure 1. Disable SSL 3.0 support in Chrome by adding a flag at the end of the Properties/Target path.

From now on, launch Chrome only with this edited shortcut. Launching the browser from any unedited launch icons won't provide protection from POODLE. Consider clicking on the General tab in the Chrome Properties dialog box and giving the edited shortcut a unique name — such as "Chrome - no SSLv3" or something similar. Then you'll always know you're using the right shortcut.

Firefox: As noted in the Oct. 14 Mozilla blog post, Firefox 34, due to be released on Nov. 25, will disable SSL 3.0 support. In the meantime, Mozilla recommends installing the add-on (download site), "SSL Version Control 0.2" (see Figure 2), which will let you control SSL support within the browser. (Some websites have recommended adjusting Firefox settings in the configuration file, but Mozilla recommends using the add-on instead.)

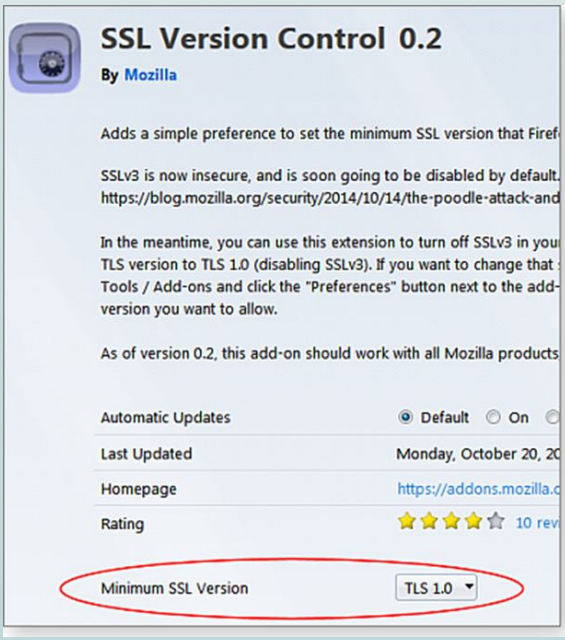


Figure 2. To disable SSL 3.0 support in Firefox, Mozilla offers a browser add-on.

Internet Explorer: In IE, click the gear (settings) icon, open Internet options, and then select the Advanced tab. Scroll down the Settings list to the Security category, and then look for Use SSL 3.0. Uncheck the box (see Figure 3), click OK, and then relaunch IE.

Network admins can make this change to all PCs on the local network via Windows' Group policy. Go to the Internet Explorer settings and modify the Turn off encryption support object (Windows Components\Internet Explorer\Internet Control Panel\Advanced Page).

Continued on next page

CCCGC

Charlotte Bytes

Conclusion from page 11

Protecting yourself from POODLE attacks

(Padding Oracle On Downgraded Legacy Encryption)

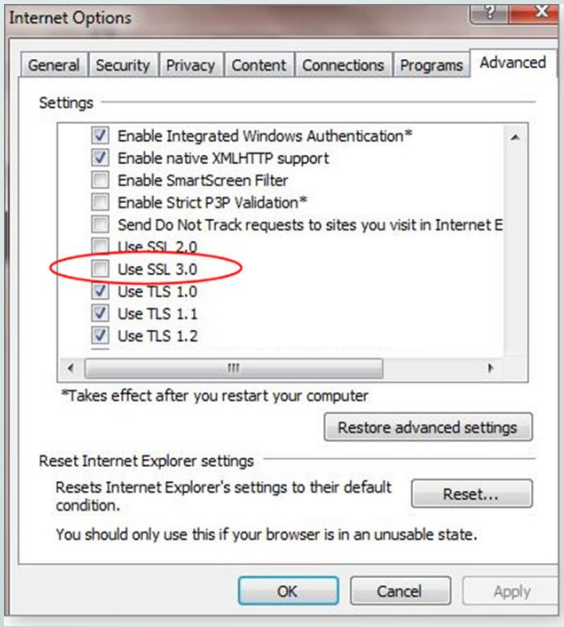


Figure 3. In IE, uncheck "Use SSL 3.0" in the advanced settings dialog box.

Microsoft released an initial security advisory on this topic; expect to see additional guidance in the near future.

How to test your browser's TLS/SSL protection

Several websites test whether your currently open browser supports SSL 3.0. For a simple test, Poodletest.com displays a poodle dog if your browser still supports SSL 3.0, and a Springfield terrier if it doesn't. On the other hand, Qualys SSL Labs (site) provides a more detailed analysis of the SSL protocols your browser supports.

As noted above, some business sites such as online banking might still need SSL 3.0. Again, I recommend leaving SSL 3.0 support on one browser; it'll be faster and safer than repeatedly adjusting browser settings. If you're running a Web server or small-business server, you should disable SSL 3.0 support to better protect connected workstations and Internet-based phones.

An InfoSec Community Forums Incidents.org page lists how to block SSL 3.0 on various Web-based platforms.

For example, in Windows Server, create (or modify) a Registry DWORD value as follows:

In your Registry editor, go to:
HKey_Local_Machine\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols

Under the Protocols, create a key called "SSL 3.0." Then, under that key, create another key called "Server."

Create a DWORD called "Enabled" and give it a value of 0.

Reboot the server; you and any connected clients will now be protected from POODLE exploits.

Compromised cert highlights a system in doubt

POODLE is a clear indication that the TLS/SSL system we rely on needs work. In fact, the entire system of security protocols and certificates could well be a house of cards. For example, HP recently announced that one of its certificates has been used to sign malware. As noted in a Krebs on Security post, HP will revoke on Oct. 21 the certificate it has used for some of the software that shipped with older products. Unfortunately, HP isn't completely sure what impact that change will have on the ability to restore some HP computers. Look for my future updates on that topic.

Another round in the dogfight over Internet security. As has been widely noted, POODLE effectively kills the SSL 3.0 protocol. Following the aforementioned steps, let's make sure POODLE's bark is worse than its bite (sorry, I couldn't help myself). However, there's a silver lining to this latest security mess — it should now force everyone on the Internet to finally abandon a dated, insecure protocol.

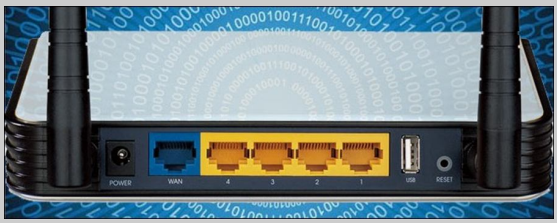
CCCGC

Microsoft REGISTERED Refurbisher

Charlotte Bytes

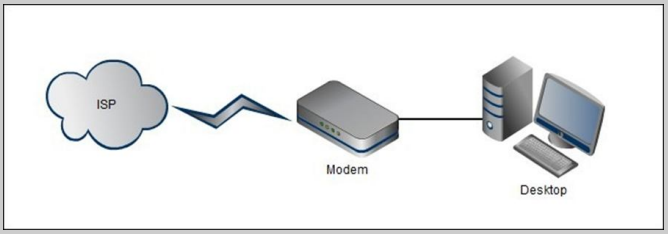
the How-To Geek
Computer Help from your Friendly How-To Geek

Understanding Routers, Switches, and Network Hardware



Today we're taking a look at the home networking hardware: what the individual pieces do, when you need them, and how best to deploy them. Read on to get a clearer picture of what you need to optimize your home network.

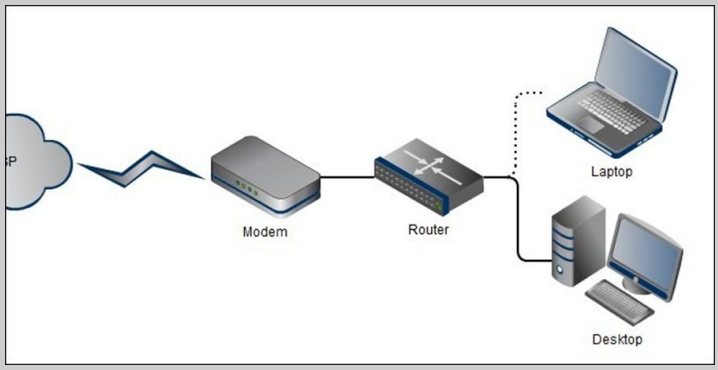
When do you need a switch? A hub? What exactly does a router do? Do you need a router if you have a single computer? Network technology can be quite an arcane area of study but armed with the right terms and a general overview of how devices function on your home network you can deploy your network with confidence.



Understanding Home Networking Through Network Diagrams

Rather than start off with a glossary of networking terms—and in the process slam you with a technical terms with no easy point of reference—let's dive right into looking at network diagrams. Here is the simplest network configuration available: a computer linked directly to a modem which is in turn linked through a phone line/cable/fiber optic uplink to the individual's internet service provider.

It doesn't get less complicated than this arrangement but there is a price to pay for the ultra-simplicity of the setup. This user cannot access the internet with a Wi-Fi device (thus no access for smart phones, tablets, or other wireless devices) and they lose out on the benefits of having a router between their computer and the greater internet. Let's introduce a router and highlight the benefits of using one. In the diagram below we've introduced two elements to the network: a wireless router and a laptop connecting to the network via that wireless connection.



When should you use a router? Given the low cost of home routers and the benefits gained from installing one on your network **you should always use a router (which almost always includes a firewall feature).**

Home routers are actually a a combination of three networking components: a router, a firewall, and a switch. In a commercial setting the three pieces of hardware are kept separate but consumer routers are almost always a combination of both the routing and switching components with a firewall added in for good measure. First let's look at what the router function does.

At the most basic level a router links two networks together, the network within your home (however big or small) and the network outside your home (in this case, the Internet). The broadband modem provided to you by your ISP is only suited to linking a single computer to the internet and usually does not include any sort of routing or switch functionality. A router performs the following functions:

IP sharing: Your ISP assigns you one IP address. If you have a desktop, a laptop, a media box on your TV, and an iPad, that one IP address clearly isn't going to cut it. A router manages those multiple connections and ensures that the right packets of information go to the right places. Without this function there would be no way for a person on the desktop and a person on the laptop to both browse the web as there would be no distinguishing between which computer was requesting what.

Continued on page 13

CCCGC
Microsoft REGISTERED Refurbisher

Charlotte Bytes

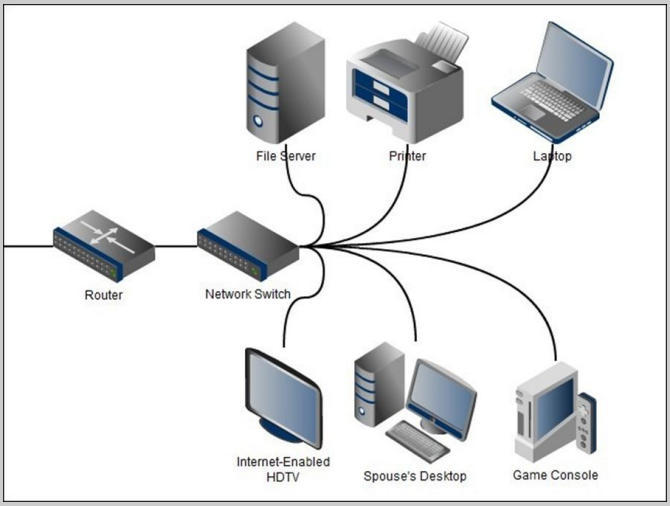
the How-To Geek
Computer Help from your Friendly How-To Geek

Understanding Routers, Switches, and Network Hardware

Network Address Translation (NAT): Related to the IP sharing function, NAT modifies the headers in packets of information coming into and out of your network so that they get routed to the proper device. Think of NAT like a very helpful receptionist inside your router that knows exactly where every incoming/outgoing package should go and stamps the department on them accordingly.

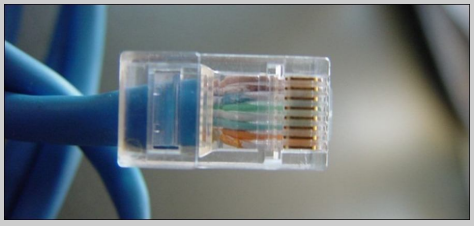
Dynamic Host Configuration: Without DHCP you would have to manually configure and add all the hosts to your network. This means every time a new computer entered the network you would have to manually assign it an address on the network. DHCP does that for you automatically so that when you plug your XBOX into your router, your friend gets on your wireless network, or you add a new computer, an address is assigned with no human interaction required.

Firewall: Routers act as basic firewalls in a variety of ways including automatically rejecting incoming data that is not part of an ongoing exchange between a computer within your network and the outside world. If you request a music stream from Pandora, for example, your router says, "We're expecting you, come on in" and that stream of data is directed to the device that made the request. On the other hand, if a sudden burst of port probing comes in from an unknown address your router acts as a bouncer and rejects the requests, effectively cloaking your computers. Even for a user with a single computer a simple $50 router is worth it for the firewall functionality alone.



In addition to the inside-to-outside network functionality outlined above, home routers also act as a network switch. A network switch is a piece of hardware that facilitates communication between computers on an internal network. Without the switching function the devices could talk through the router to the greater internet but not to each other—something as simple as copying an MP3 from your laptop to your desktop over the network would be impossible.

Most routers have four Ethernet ports which allow you to plug in four devices and have them communicate via the switch function. If you need more than four Ethernet connections you'll need to upgrade to a router with a larger port bank (a rather expensive proposition that will usually only boost you up to eight ports) or you can pick up a dedicated switch. Note: You only need to upgrade if you're running out of physical ports for hard line connections. If you only have one computer and one networked printer plugged into your four-port router (and everything else on your network is Wi-Fi based) there is no need to upgrade to gain physical ports. That said, let's take a look at a network with a dedicated switch.



Decoding Network Speed Designations

Now that you've got a clear picture of how exactly your network should be physically configured let's talk about network speeds. There are two primary designations we are interested in: Ethernet and Wi-Fi. Let's take a look at Ethernet first.

Ethernet connection speeds are designated in 10BASE. The original Ethernet protocol, now 30 years old, operated as a max speed of 10 Mbit/s. Fast Ethernet, introduced in 1995, upped the speed to 100 Mbit/s. Gigabit Ethernet was introduced shortly after that in 1998 but didn't gain much traction in the consumer market until recently. As its name suggests, Gigabit Ethernet is capable of 1000 Mbit/s. You will commonly see these designations noted on networking gear and its packaging as 10/100 or 10/100/1000 indicating which Ethernet version the device is compatible with.

Continued on page 14

Official Publication of the Charlotte County Computer Group Corp.
PROMOTING COMPUTER LITERACY AND EDUCATION IN CHARLOTTE COUNTY

Understanding Routers, Switches, and Network Hardware

Conclusion from page 13

In order to take full advantage of the maximum speeds all the devices in the transfer chain need to be at or above the speed rating you want. For example, let's say you have a media server in your basement with a Gigabit Ethernet card installed and a media console in your living room with a Gigabit Ethernet card but you are connecting the two together with a 10/100 switch. Both devices will be limited by the 100 Mbit/s ceiling on the switch. In this situation upgrading the switch would boost your network performance considerably.

Outside of transferring large files and streaming HD video content across your home network there is little need to go out and upgrade all your equipment to Gigabit. If your primary computer network usage involves browsing the web and light file transfers 10/100 is more than satisfactory.

Understanding Wi-Fi Speeds

Wi-Fi speeds are designated by letter, not by number. Unlike the easy to translate number-as-network-speed designation we find with Ethernet the Wi-Fi designations actually refer to the draft versions of the IEEE 802.11 networking standard that dictates the parameters of the Wi-Fi protocol.

802.11b was the first version widely adopted by consumers. 802.11b devices operate at a maximum transmission of 11 Mbit/s but the speed is highly dependent on signal strength and quality—realistically users should expect 1-5 Mbit/s. Devices using 802.11b suffer from interference from baby monitors, bluetooth devices, cordless phones, and other 2.4GHz band devices.

802.11g was the next major consumer upgrade and boosted the max transmission to 54 Mbit/s (realistically about 22 Mbit/s accounting for error correction and signal strength). 802.11g suffers from the same kind of 2.4GHz band interference that 802.11b does.

802.11n is a significant upgrade to the Wi-Fi standards—devices use multiple-input multiple-output antennas (MIMO) to operate on both the 2.4GHz and relatively empty 5GHz bands. 802.11n has a theoretical maximum of 300 Mbit/s but accounting for error correction and less than ideal conditions you can expect speeds in 100-150 Mbit/s range.

802.11ac is a huge upgrade that brings wider channels (80 or 160 MHz versus 40 MHz), more spatial streams (up to eight) and things like beamforming, which sorta send the waves directly to your device instead of bouncing all around, making things much faster. How much faster? There are some models that can do one gigabit per second. It's extremely fast.

Like Ethernet, Wi-Fi speeds are limited by the weakest link in the direct network. If you have an 802.11n capable Wi-Fi router but your netbook only has an 802.11g capable Wi-Fi module you will max out at the 802.11g speeds. In addition to the speed limitations there is a very pressing reason for abandoning the oldest popular Wi-Fi protocol 802.11b. You must use the same level of encryption on every device in your network and the encryption schemes available to 802.11b devices are weak and have been compromised (WEP encryption, for example, can be compromised in a matter of minutes by a moderately skilled child). Upgrading your Wi-Fi router and wireless equipment allows you to upgrade your wireless encryption as well as enjoy faster speeds. If you haven't done anything to secure your router now would be a good time to read our guide to locking down your Wi-Fi network against intrusion.

Also like Ethernet, upgrading to the maximum speed—in this case 802.11n—is best suited for people moving large files and streaming HD video. Upgrading to 802.11n will have a negligible impact on your web browsing speed but will have an enormous impact on your ability to wirelessly stream HD content around your home.

At this point you've got a handle on how your home network needs to be laid out and you have an understanding of what the network speed designations mean and how they impact you and your network. It's time to upgrade your switch, roll out some new Wi-Fi bandwidth, and enjoy a better optimized home network.

Charlotte Bytes

Windows Secrets
Everything Microsoft forgot to mention.

See us on the Web
www.cccgc.net

CCCGC

How Businesses Fail To Protect Customer Info

By Doug Spindler

Most Internet users should know by now that personal digital security is in large part our own choice and responsibility.

But in truth, our electronic security is also in the hands of the companies we do business with — and they're not all taking that fact seriously.

Everyone who gives personal information to an online entity or makes a credit-card purchase in person or provides that card information over the phone is counting on a significant level of trustworthiness. We assume that a business puts the protection of our private data above its goal of maximizing profits.

But with the seemingly weekly revelations of hackers stealing our names, email addresses, credit-card numbers, passwords, and so forth from corporate databases, it's small wonder many Internet users are scratching their heads and asking, "What the heck is going on?"

This article is about online security. However, it's not another primer on what steps you should take to secure your data. Instead, it looks at the attitudes and actions companies take to secure your private information. It's also about what you can do to make companies more proactive at keeping your data secure.

Prodding business to do the right security thing

Smart companies listen to their customers. Although it often takes many customer complaints to change a company's ways, sometimes all it takes is one. Here's a case in point. Most of us know by now that we should be using long and complex passwords. But my OfficeMax account would accept only numbers and uppercase and lowercase letters.

I thought that was dumb. Why can't I use special characters? So I wrote a letter to the CEO of OfficeMax, asking why the company wasn't doing everything it could to safeguard customers' private information. I pointed out the weakness in the company's password rules and requested that OfficeMax allow more password complexity. Just to drive home the point, I also reminded the CEO of past OfficeMax data breaches.

Surprisingly, a few days later the OfficeMax chief technology officer (CTO) called and informed me that my letter had prompted OfficeMax to implement a new password policy that allows customers to use special characters in their passwords. I thanked the CTO, but I also silently wondered why, if the change could be so quickly — and apparently so easily — implemented, OfficeMax hadn't implemented it a long time ago? Why did a customer have to point out the weaknesses in the company's password policy?

Contrast OfficeMax's actions with that of Home Depot. In November 2013, Target's credit-card point-of-purchase terminals were breached and customer credit-card numbers stolen. Security analysts later published details about how the attack was carried out, and they noted the countermeasures a company could implement so as not to be the next victim.

What did Home Depot do? Apparently nothing. This past April, it was hit by a massive breach that used techniques similar to those of the Target breach — i.e., the hackers attacked point-of-purchase terminals. One has to ask: After the details of the Target attack were published, why didn't Home Depot immediately perform a security audit and put the recommended security enhancements in place? Target's breach was a lesson learned; Home Depot's breach, to my mind, was completely inexcusable. If your neighbor was robbed, wouldn't you take some time to review your security measures?

And, more important, why didn't the credit-processing companies require all retailers to implement countermeasures?

Obviously, there's a lot of money made from stolen credit cards. Every successful breach only encourages others to try the same tactics on other targets. Large retailers give hackers the biggest bang for their malicious bucks. And though individual customers might be reimbursed for their losses, every breach represents a significant cost to all of us. (See, for example, the May 14 Krebs on Security post, "The Target breach, by the numbers."

Continued on page16

Charlotte Bytes

CCCGC

Windows Secrets
Everything Microsoft forgot to mention.

See us on the Web
www.cccgc.net

How Businesses Fail To Protect Customer Info

Continued from page 15

Giving customer privacy short shrift

Unfortunately, security policies still vary widely among businesses, both small and large. For instance, after I recently purchased a cellphone from Sprint, I discovered I couldn't use a secure, complex password for my Sprint account. That made me worry that it's just a matter of time before Sprint's customer accounts are hacked.

Even more worrisome is the security of our medical records. A hospital hired one of my colleagues to run a security audit. One of the requested checks was the hospital's Wi-Fi network. Could he connect to the Wi-Fi system from the hospital's parking lot?

Yes, he could connect to the hospital's network from the parking lot — but he could also connect from a coffee house almost two blocks away. More frightening: By using a protocol analyzer, he could connect to the hospital's network without a password and view unencrypted patient data.

My colleague pointed out this glaring security breach to the hospital's IT department in his final report and was duly thanked. Although no longer working for the hospital, my colleague periodically performed the same test over the next year — just to see whether the hospital had secured its wireless network. It hadn't.

A disclaimer here: I told my colleague that his "unofficial" testing was probably illegal. While under contract, he had permission to connect to and analyze the hospital's network. But once he'd submitted his report and the contract was complete, he had no right to perform the additional tests. I recommended that he stop his extra curricular activities and instead file a report on the U.S. Department of Health and Human Services (HHS) website.

According to the site, people who feel their health-information privacy has been violated, based on Health Insurance Portability and Accountability Act (HIPAA) laws, can file complaints with HHS. The HIPAA laws offer legal protections to anyone who makes a legitimate complaint.

Here's another unfolding story. A well-respected, IT-security professor was preparing for a class lecture. One of his Google searches came back with a link to a server at a major university medical center.

Clicking the link revealed thousands of patient personal-health information (PHI) records.

Doing what he considered the responsible thing, he informed the medical center's IT department that they were leaking PHI. Although he never received a reply to his emails, within several hours the patients' data was no longer accessible. Feeling he'd simply done a good deed, he thought nothing more of it.

But about a month later, the professor discovered that the medical center was accusing him of unethical behavior. Not only did the medical center take this story to the press, it contacted the professor's college and demanded that he be fired. The medical center claimed he'd used hacking tools to show students how someone might access protected data via the center's website. It also stated that he'd published instructions for the hack on the college's site. I know that he did nothing of the sort.

I think the university/medical center put out this false information to hide its own failure to protect patient information. The university never contacted the FBI or other law-enforcement agencies to report this alleged crime. In fact, once the professor retained an attorney, the university appeared to back away from the charges. It will longer answer the attorney's letters. Let's hope that's the end of this episode.

This example highlights the two-part nature of corporate breaches and a company's response once data theft comes to light. The victim of an attack must first secure the breach; it must then quickly and clearly tell customers what has happened and what will happen next. The medical center's IT department obviously responded quickly, but the university failed the public-relations side miserably. The organization could have simply said: "Oops! Thanks for letting us know." Instead, it took the unwarranted step of attacking the messenger.

Continued on next page

CCCGC

Charlotte Bytes

How Businesses Fail To Protect Customer Info

Conclusion from page 16

Given the potential costs of a breach, it's surprising that businesses are slow to learn from previous security failures. Again, Home Depot could have prevented its massive breach if it had immediately implemented recommended counter measures. And if businesses are slow to implement credit-card protection, card-processing companies such as Visa and Master Card should require retailers to rapidly upgrade their point-of-sale systems.

That change won't be cheap, but it will come. It must. Cyber thieves are constantly looking for new and easy targets. As with any "business," these hackers want the largest return from the least investment.

Though the expense of a breach is initially borne by the compromised business, ultimately consumers pay the price. As noted in a Security Affairs post, a Ponemon security report states that the cost of a breach to a U.S. company in 2014 is about $201 per lost record — up from $188 in 2013.

Personally, I don't think new laws are the answer to cyber crimes. Rather, we need to hold accountable those whom we trust with our confidential information. For some companies, data theft might be considered just "part of the cost of doing business." But it's our data and our cost. That careless practice also guarantees we'll have to cope with ongoing data breaches.

Tips for protecting our credit cards

There are many sources for information on how to help keep your credit card secure. For example, see the U.S. Federal Trade Commission site, "Protecting against credit card fraud." **http://www.consumer.ftc.gov/articles/0216-protecting-against-credit-card-fraud.** It lists best practices and notes how to report a lost or stolen card. Another page discusses how to secure your personal information.

Of course, Windows Secrets has covered personal-security issues in our Top Stories and On Security columns. See, for example, Susan Bradley's July 3 Top Story, "Revisiting the WS Security Baseline: Part 1." An online search using "protecting your credit cards" will turn up many more tips from numerous sources.

Also, as my OfficeMax experience demonstrates, if a company you do business with appears to have inadequate security — such as allowing only simple passwords — feel free to complain to the company loudly and often. You'll improve the security not only of your own confidential information, but also that of hundreds or thousands of other customers.

A final note on an old but ongoing scam

By now, nearly everyone who goes online should have at least heard of the infamous Nigerian-letter email scams. So you might be surprised to hear that these scams are still quite successful. There are reports that the perpetrators have netted about a billion dollars per year — for many years. In fact, a music video featuring a Nigerian singing "I go chop your dollar" became an international hit. (The song can be found on YouTube; I have to admit it's catchy.) The song is about Nigerian email scammers.

Success, of course, always breeds competition. Now folks in Ghana are competing for scam victims. In a practice called Sakawa, Ghanaians mix email scams with religion. Sakawa Boys pay a local priest or witch doctor to help them make lots of money. Some of these scams involve online dating services.

Often money goes to Africa via local grocery stores that offer international money transfers. Clerks I've talked to state that someone sends money to an unknown recipient several times a week. When I ask clerks whether they suspect the money transfers are scams, they say, "Yeah, we know; but company policy prevents us from saying anything." Some clerks say it breaks their hearts because they know the victim won't have enough money left to buy food.

In many (if not most) cases, the victims are elderly — folks with too little income and too much trust. If you have elderly friends or relatives, talk to them about scams — and do what you can to keep them from getting ripped off. For more information on new scams, check out Scanorama **http://www.scamorama.com/** (whose motto is "Why should scammers have all the fun?) and fraudaid.com. **http://www.fraudaid.com/threats.htm**