December 2014

Microsoft REGISTERED Refurbisher

Charlotte County Computer Group

30th YEAR Anniversary

1984 - 2014

The Next General Meeting of CCCGC will be **December 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. XII

The President's Platform by Ron Wallis, President CCCGC

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

Christmas is almost here and most of the snowbirds have returned. We welcome you back and wish everyone a Happy and safe Holiday Season.

The election and swearing in of officers will be at the December meeting, so there will not be a presentation.

Everything else will be the same, John Palmer's beginners class at 5:00 pm, Scott's forum at 6:00 and door prizes, 50/50 and the computer raffle.

We will be serving coffee, beverages and cookies. We thought it would be festive for the members to socialize a bit before the Holidays.

Please come and join the fun.

Merry Christmas Happy Hanukkah and a Healthy New Year

Notice:

We have a desperate need for monitors and USB keyboards

Ron

Charlotte Bytes

Computer Drawing

To change her luck, Linda Corrick agreed to be the nominating committee chairman.

She got lucky and won this month's computer. Her ticket was pulled out then the shock, then the smile appeared. Linda won this great computer.

Thanks to all who tried to be the winner. Keep trying. It will happen

50/50 Winner

ED TKACIK

Do you recognize the name or the picture? If you look in the October Bytes you will find he last month. Talk about luck. He cleaned us out again!

Good luck on future drawings.

Door Prize Winners

Left To Right

ROSE KOPENEC

ALLYN BASCOM

PALMA TAR SPIELDENNER

FRANK MESSINA

JOANNE NICHOLSON

WELCOME

New Members

Kenneth Brese
Peter Harrinton
Tom Johnson
Maryann Evans
JoAnne Oldham
Martha Mackey
Brenda Walker
Guy Davignon
John Kaldeway
Shirley Brese
Jean Sheppard
Louis Galterio
Arthur Wilson
Frank Mackey
Mary Joy Donovan
James Marlow
Robert Harris

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.

Linda Corrick, Nominating Chairman, announced the slate of candidates. There were no floor nominations.

LARRY HURLEY presented the group with an overview of genealogy. It starts with notes, like full names, birth dates, anniversary dates and maybe a list of children. Many documents containing information that have been handed down may be at home stashed in a drawer might not be listed or on record anywhere else. The internet is a valuable source in finding many long forgotten names, relatives, old addresses, military records, old jobs, divorces, weddings, church documents and awards earned and many other types of records.

Take all these papers, put them in a stack and start organizing them on the computer, make headings and put the items related to the heading in the file. Before long, you have lots of files and then more files within files.

You need to protect the data that you have worked on. You can keep a file on the computer but make a back up so you will not lose the information.

Soon you will find there is a huge amount of information which will lead to more information. This can be a very rewarding venture for you and your family members. If you want to find out more about genealogy, contact

Larry Hurley for the place to start.

Program High-Lights

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

2015 Nominees

The following candidates for Officers and Directors for the 2015 business year will be voted on and installed at the December General Meeting.

President: Ron Wallis

Vice President: Dick Evans

Secretary: Ron Muschong

Treasurer: Larry Hurley

Director : John Hegard

Director: Frank Messina

Three other Directors continue to fill their term of office.

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

December 2014 CCCGC Events Calendar

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

Security News Room

VIPRE

JPMorgan Chase is Victim of the Largest Cyberattack in Banking History

JPMorgan Chase, one of the nation's largest financial institutions, admitted last month that

hackers had gained access to the personal information -- names, email addresses phone numbers and addresses -- of 76 million households.

The company said the attackers did not penetrate enough to get account information, and that there was no evidence of any money being stolen or moved from one account to another.

The bank discovered the breach during the summer but did not alert customers for months. Under federal and state law, JPMorgan did not have to alert customers about the breach because only contact data was hacked -- not financial information such as account numbers and social security numbers.

The big concern for bank customers is whether they trust that JPMorgan is telling them the truth. Secondary concerns are that email addresses will enable the hackers to engage in "phishing" expeditions to trick customers into providing them with additional personal information.

If you're a Chase customer, here are some things you should consider doing:

Watch out for scammers. Don't trust any phone calls, emails or letters claiming to be from the bank. If the 'bank' contacts you, verify the authenticity of each communication by calling the number on your bank card or on a previous statement.

Change your login and request a new debit/credit card ASAP. Better safe that sorry. You can't trust that the bank is being completely honest about the level and depth of its breach -- or, indeed, that it knows just how successful the hackers have been at penetrating its security measures.

Check your bank statement regularly. Carefully review your bank and credit card statements for any unexpected charges -- especially tiny ones. Fraudsters will often test a stolen debit or credit card by charging a few cents on the card, thereby avoiding attention.

A report in The New York Times said the hackers were able to gain "the highest level of administrative privilege" on more than 90 of the bank's servers. Such access allows the criminals to transfer funds, close accounts, and basically do whatever they want with the data.

CCCGC

Charlotte Bytes

Tablets Aren't Killing Laptops, But Smartphones Are Killing Tablets

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

Tablet sales growth is declining, and Apple is selling fewer iPads every quarter. PC sales are improving. Ever-larger smartphones make great consumption devices. Microsoft has even realized Windows should be a desktop operating system, because PCs aren't going anywhere.

Tablets used to seem like the future. Everyone would abandon laptops and desktops – or, at least, everyone would have a smartphone, a tablet, and a PC. But tablets are now looking more like a niche product.

Tablet Sales vs. PC Sales – Hard Data

RELATED ARTICLE

Are PCs Dying? Of Course Not, Here's Why

Reports of the PC's demise have been greatly exaggerated. We've all heard that everyone's just buying tablets and throwing out... [Read Article] http://www.howtogeek.com/183381/are-pcs-dying-of-course-not-heres-why/

When we explained why PCs aren't dying, we noted that tablet sales were growing slower than ever, while the PC's decline was slowing down. Now, we can look at the latest data:

Tablet sales are growing more slowly, according to Gartner's October 2014 figures. In 2013, tablet sales were up 55 percent from 2012. In 2014, they were up just 11 percent from 2013. (Source)

iPad sales are declining, according to Apple's Q3 2014 numbers. iPad sales declined 19 percent from the previous quarter and nine percent from the previous year. (Source)

PC sales are recovering, according to Gartner's July 2014 figures. PC sales were up 0.1 percent in Q2 2014 from Q2 2013. It's a small increase, but the trends are clear — PCs are trending up, and tablets are trending down. The PC's downward slide seems over. (Source)

Smartphones Are Pushing Out Tablets

Smartphone screen sizes are increasing every year. Android phones have been growing larger and larger for years, and Microsoft's Windows Phones have followed suit. Even Apple could no longer resist the trend — the iPhone suddenly grew larger with the iPhone 6 and 6 Plus. (And, if there was any doubt, all the data shows smartphone sales are increasing.)

No, smartphones aren't going to kill laptops or desktops any time soon. But they do appear to be taking a chunk out of tablets. Compare an iPhone 6 Plus, or even an iPhone 6, to an iPad. Compared to an iPhone 6 Plus, an iPad Mini looks absurdly small — why would you bother using the iPad Mini if you owned both? The iPad's software doesn't really take advantage of the larger screen like it should. You can't run multiple apps at once, a feature that might justify picking up a tablet. Yes, there are niche apps that can take advantage of the larger display for some professional uses, but tablets become less compelling as your smartphone becomes larger.

The same is true in Android land. Google has killed the Nexus 7 tablet now that they have a Nexus 6 smartphone. Why would you want a 7-inch tablet if you have a 6-inch phone? Android tablets also can't display multiple applications side-by-side, so the big advantage to having a larger tablet is just having a larger screen to consume media on.

Continued on next page

CCCGC

Charlotte Bytes

Tablets Aren't Killing Laptops, But Smartphones Are Killing Tablets

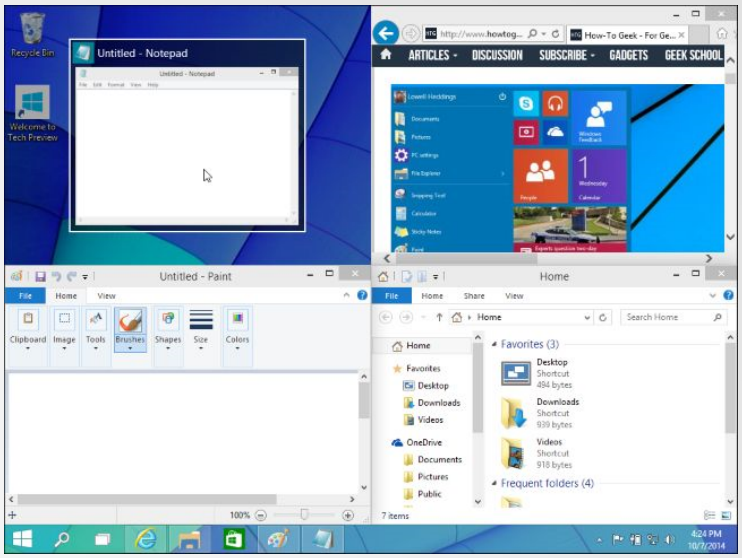
Continued from page 7

Microsoft Realized People Still Use PCs

RELATED ARTICLE

Why I Still Use Windows 7 After a Year of Trying to Like Windows 8

Have you upgraded to Windows 8 yet? We've published a lot of Windows 8 articles here at How-To Geek, and... [Read Article] http://www.howtogeek.com/145984/why-i-still-use-windows-7-after-a-year-of-trying-to-like-windows-8/



If Windows 8 was a "touch-first" operating system, as Microsoft said it was, the Windows 10 Technical Preview is a "mouse-and-keyboard-first" operating system. Microsoft has woken up and realized people will still be using PCs and that Windows should be a good operating system for desktop usage.

The magnitude of this shift can't be overstated. During Windows 8 development, Paul Thurrot and others reported that, inside Microsoft, the plan was to work towards removing the desktop from future versions of Windows. In Windows 8, the desktop was "just an app" — remember that? And maybe that app would be gone entirely by Windows 9 or 10. That's no longer happening. After years of user complaints, Microsoft has realized that touch-based tablets alone aren't the future.

Tablets Can't Replace PCs, but Smartphones Can Replace Tablets

So really, what's the point of a tablet? Smartphones are becoming larger, and they're always with you and have a data connection. Tablets can't run more than one app at a time, anyway — Windows tablets can, but very few apps are available for them. Once your smartphone's screen is large enough, it can provide that simplified, one-app-at-a-time, touch-based consumption experience anywhere. Why bother with a tablet?

Laptops (and desktops) are also still necessary, providing a powerful mouse-and-keyboard interface with multiple windows and multitasking. For productivity use — or just multitasking — an iPad or Android tablet is much clunkier to use than a standard Windows, Mac, Linux, or even Chrome OS PC.

So where does that leave tablets? Larger phones are encroaching from the low-end, and laptops are becoming lighter and more battery-efficient at the high-end. You can even get laptops that can perform some tablet duties — Microsoft is betting big on this convergence. Why buy a tablet? When would you use it instead of your big smartphone, or your laptop? Sometimes, sure — enough to buy one and drag it around with you all the time? Not necessarily.

Tablets need to evolve, so they can actually use that bigger screen to do more than a smartphone can do. A tablet with multitasking, perhaps even with a larger screen, now that's a bit more compelling. The Surface Pro 3 is such a machine. Google's will offer a keyboard dock for their new Nexus 9 so it can be more of a productivity machine. And Apple is rumored to be working on an "iPad Pro" with a larger screen and multitasking, too.

Now, tablets aren't dead. Far from it. But they aren't looking as healthy as they used to. There was a time when all the pundits thought tablets would replace laptops for most people, but that definitely isn't happening. Many people thought everyone would have "three screens" — smartphone, tablet, and laptop or desktop — and that doesn't seem inevitable, either.

Tablets are getting squeezed in the middle, and they'll need to actually become more powerful productivity machines with multitasking to compete against laptops at the high-end. The idea that everyone will replace their laptop with a 10-inch screen that can only run a single app at a time — now there's an idea that seems dead. Tablets will need to become much more like PCs to actually replace laptops — but then you'll just have a different type of PC, anyway.

Image Credit: SirMo76 on Flickr, William Hook on Flickr, Scott Akerman on Flickr

Charlotte Bytes

See us on the Web
www.cccgc.net

makeuseof

CCCGC

Your USB Devices Aren't Safe Anymore, Thanks To BadUSB

Matthew Hughes

On 7th October, 2014

If you bought a computer before 1997, you probably noticed that the back was a pock-marked mess of connectors and ports. And if you bought a new printer and scanner, odds were good it would only work with a certain type of port.

And if the pins on the connector broke, your device was worthless. It was a nightmare. And then USB arrived.

Universal Serial Bus (USB) was created by a consortium of seven major technology companies, all hoping to solve one important question; 'How do I connect this device to my computer?'. Almost 20 years later, USB has reached a level of absolute ubiquity.

This ubiquity has been both a blessing and a curse. Whilst USB has made using peripherals and removable storage trivially easy and convenient, there has recently been a discovery of a vulnerability with USB that makes every computer in the world vulnerable. It's called BadUSB, and you need to know about it.

Meet BadUSB

The earth-shattering revelations that USB isn't as secure as first thought was first disclosed by security researchers Karsten Nohl and Jakob Lell in July, 2014. The malware they created – dubbed BadUSB – exploits a critical vulnerability in the design of USB devices which allowed them to hijack a user's Internet traffic, install additional malware and even surreptitiously gain control of a user's keyboard and mouse.

The BadUSB malware isn't stored on the user-accessible storage partition, but rather on the firmware of a USB device – including Keyboards, phones and flash drives. This means that it's virtually undetectable to conventional anti-virus packages, and can survive the drive being formatted.

Fortunately, would-be attackers have been unable to take advantage of BadUSB, due to Nohl and Lell not publishing the code in order to give the industry an opportunity to ready a fix. Until recently, that is.

In a talk given at DerbyCon – a computer security conference held in Louisville, Kentucky – Adam Caudill and Brandon Wilson demonstrated their successful reverse-engineering of BadBSD, and published their exploit code on code-sharing platform GitHub.

The motivation behind releasing BadUSB was simply to spur-on a notoriously slow-moving industry to add some security to how USB works. But, this means that from this point onwards, USB is no longer safe.

But when one looks at the history behind USB, one realizes that USB has never been especially secure.

USB As An Attack Vector

The term 'attack vector' refers to the path taken by an attacker in order to compromise a computer. These range from malware, to browser exploits (such as the one recently found in the stock browser on Android), to vulnerabilities in software already installed on the computer (much like Shellshock).

Conclusion on page 10

CCCGC

Conclusion from page 9

makeuseof

Your USB Devices Aren't Safe Anymore, Thanks To BadUSB

The use of a USB flash drive as a potential attack vector isn't especially new or uncommon. For years, hackers have dropped USB drives in public areas, just waiting for someone to plug them in and unlock the nasties stored within. Just ask Dutch chemical firm DSM.

In 2012, they reported finding flash drives that had been intentionally dropped in their parking lot. Upon examination, they were found by DMS's internal IT staff to contain malware which was set to auto-run and harvest login credentials, potentially giving an attacker access to privileged and confidential information.

If one looks even earlier, we can see malware that specifically took advantage of the Sandisk U3 flash drives. Discontinued in 2009, this line of consumer USB drives contained a partition which 'tricked' the computer into thinking it was a CD-ROM. This streamlined the process of installing and managing portable applications, but also meant that it would auto-run whatever was stored in this partition. A package of malware (called the USB Switchblade) was developed, that allowed an attacker with physical access to a post-Windows 2000 computer running with root to obtain password hashes, LSA secrets and IP information.

Of course, any USB-based attack can be easily thwarted by avoiding plugging in devices that you don't personally own, which brings me on to how you can protect yourself against future BadUSB-based attacks.

How To Stay Safe

I've got some bad news. It's going to be incredibly challenging to fight any attacks that are based upon the BadUSB exploit. As it is right now, there are no firmware-level security systems for USB. A long-term fix to the issue would require a significant update to the USB standard, the most recent of which was USB Type-C. This would still leave thousands with older hardware lacking the update vulnerable.

So, what can you do? Well, it's still very early days, but there's one fix that's guaranteed to protect you from BadUSB. Simply put, you've got to have your wits about you. If you see a USB drive lying about, ignore it. Don't share USB drives. Don't let people put untrusted USB devices in your computer.

Don't Have Nightmares

Although BadUSB is incredibly frightening, it's important to put the risk in perspective. USB has never had a huge amount of popularity as an attack vector. Furthermore, at the time of writing, there are no documented examples of BadUSB-based attacks 'in the wild'.

CCCGC

Microsoft REGISTERED Refurbisher

Charlotte Bytes

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

Oracle Can't Secure the Java Plug-in, So Why Is It Still Enabled By Default?

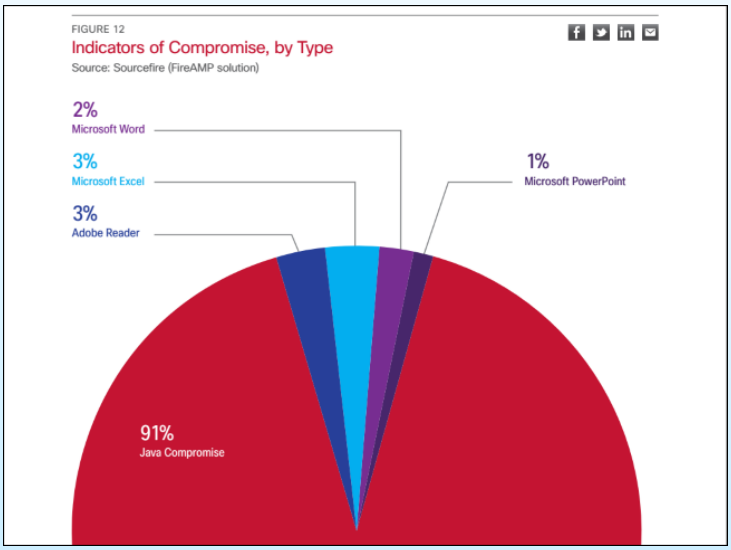
Java was responsible for 91 percent of all computer compromises in 2013. Most people not only have the Java browser plug-in enabled — they're using an out-of-date, vulnerable version. Hey, Oracle — it's time to disable that plug-in by default.

Oracle knows the situation is a disaster. They've given up on the Java plug-in's security sandbox, originally designed to protect you from malicious Java applets. Java applets on the web get complete access to your system with the default settings.

The Java Browser Plug-in is a Complete Disaster

Defenders of Java tend to complain whenever sites like ours write that Java is extremely insecure. "That's just the browser plug-in," they say — acknowledging how broken it is. But that insecure browser plug-in is enabled by default in every single installation of Java out there. The statistics speak for themselves. Even here at How-To Geek, 95 percent of our non-mobile visitors have the Java plug-in enabled. And we're a website that keeps telling our readers to uninstall Java or at least disable the plug-in.

Internet-wide, studies keep showing that the majority of computers with Java installed have an out-of-date Java browser plug-in available for malicious websites to ravage. In 2013, a study by Websense Security Labs showed that 80 percent of computers had out-of-date, vulnerable versions of Java. Even the most charitable studies are scary — they tend to claim more than 50 percent of Java plug-ins are out-of-date.



In 2014, Cisco's annual security report said 91 percent of all attacks in 2013 were against Java. Oracle even tries to take advantage of this problem by bundling the terrible Ask Toolbar and other junkware with Java updates — stay classy, Oracle.

The Java plug-in runs a Java program — or "Java applet" — embedded on a web page, similar to how Adobe Flash works. Because Java is a complex language used for everything from desktop applications to server software, the plug-in was originally designed to run these Java programs in a secure sandbox. This would prevent them from doing nasty things to your system, even if they tried.

That's the theory, anyway. In practice, there's a seemingly never-ending stream of vulnerabilities that allow Java applets to escape the sandbox and run roughshod over your system.

Oracle realizes the sandbox is now basically broken, so the sandbox is now basically dead. They've given up on it. By default, Java will no longer run "unsigned" applets. Running unsigned applets shouldn't be a problem if the security sandbox was trustworthy — that's why it's generally not a problem to run any Adobe Flash content you find on the web. Even if there are vulnerabilities in Flash, they're fixed and Adobe doesn't give up on Flash's sandboxing.

CCCGC

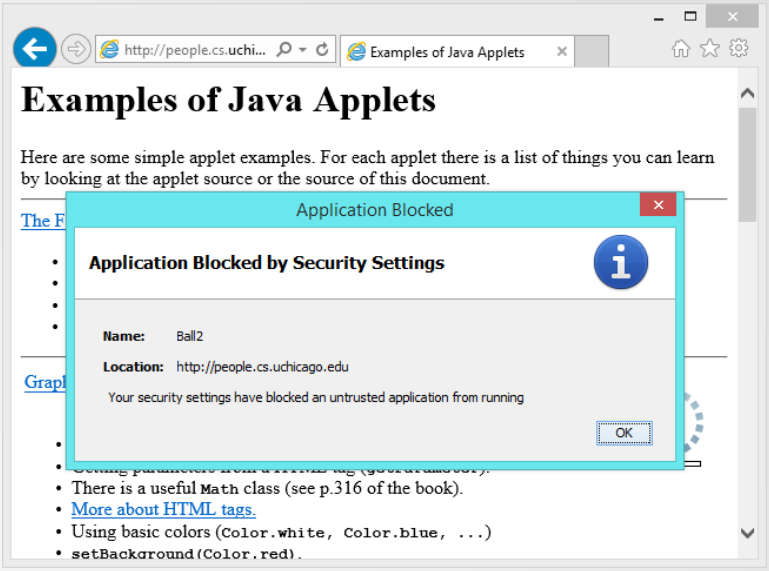
Charlotte Bytes

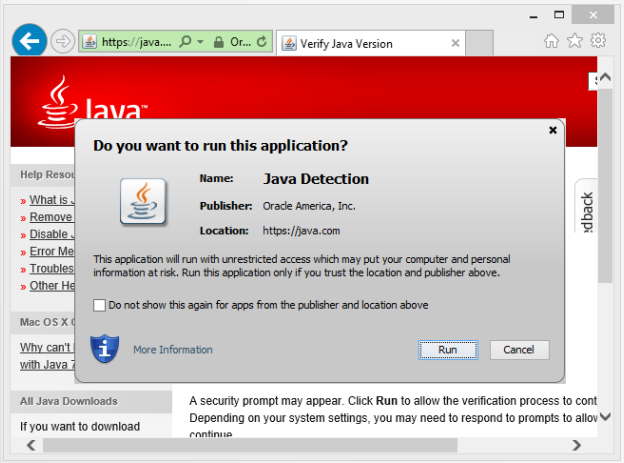
Oracle Can't Secure the Java Plug-in, So Why Is It Still Enabled By Default? Continued

By default, Java will only load signed applets. That sounds fine, like a good security improvement. However, there's a serious consequence here. When a Java applet is signed, it's considered "trusted" and it doesn't use the sandbox. As Java's warning message puts it:

"This application will run with unrestricted access which may put your computer and personal information at risk."

Even Oracle's own Java version check applet — a simple





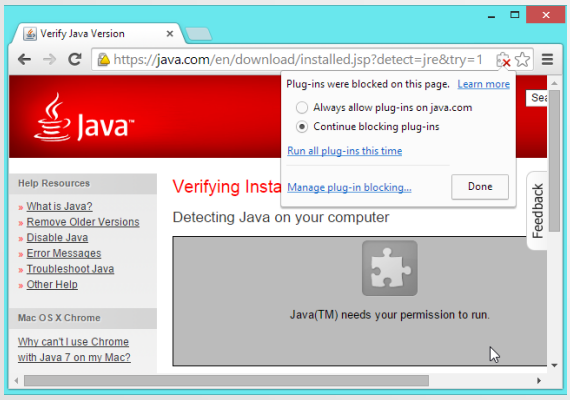
little applet that runs Java to check your installed version and tells you if you need to update — requires this full system access. That's completely insane.

In other words, Java really has given up on the sandbox. By default, you can either not run a Java applet or run it with full access to your system. There's no way to use the sandbox unless you tweak Java's security settings. The sandbox is so untrustworthy that every bit of Java code you encounter online needs full access to your system. You might as well just download a Java program and run it rather than relying on the browser plug-in, which doesn't offer the additional security it was originally designed to provide.

As one Java developer explained: "Oracle is intentionally killing off the Java security sandbox under the pretense of improving security."

Web Browsers Are Disabling It On Their Own

Thankfully, web browsers are stepping in to fix Oracle's inaction. Even if you have the Java browser plug-in installed and enabled, Chrome and Firefox won't load Java content by default. They use "click-to-play" for Java content.



Internet Explorer still automatically loads Java content. Internet Explorer has improved somewhat – it finally began blocking out-of-date, vulnerable ActiveX controls along with the "Windows 8.1 August Update" (aka Windows 8.1 Update 2) in August, 2014. Chrome and Firefox have been doing this for much longer. Internet Explorer is behind other browsers here — again.

How to Disable the Java Plug-in

Everyone who needs Java installed should at least disable the plug-in from the java Control Panel. With recent versions of Java, you can tap the Windows key once to open the Start menu or Start screen, type "Java," and then click the "Configure Java" shortcut. On the Security tab, uncheck the "Enable Java content in the browser" option.

Conclusion on page 16

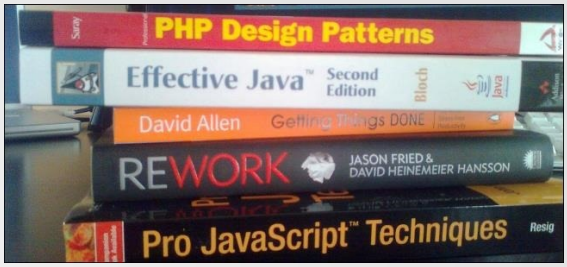
Charlotte Bytes

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

See us on the Web
www.cccgc.net

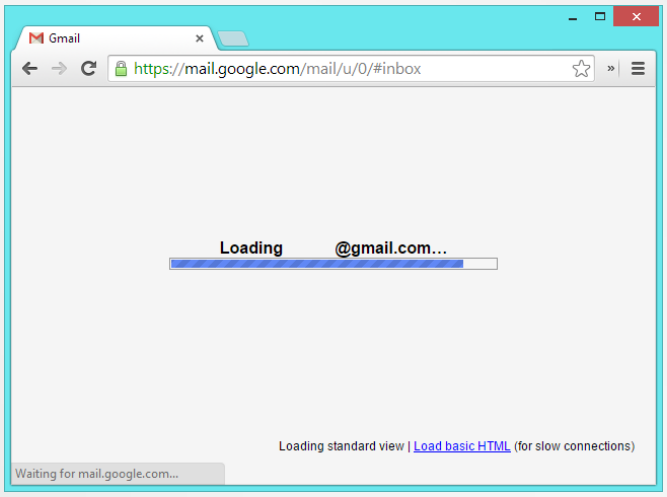
CCCGC

Java and Javascript Programming Books



JavaScript Basics

JavaScript is a programming language used by web pages. HTML is the layout language that defines how web pages are laid and and JavaScript is the language that lets web pages be more dynamic. JavaScript is what enables web applications like Gmail to function, and JavaScript is used by practically every website at this point.



JavaScript was originally designed to be a lightweight scripting language to run in web browsers. It isn't a separate browser plug-in that comes from one company — every browser includes its own different JavaScript engine. Browsers natively run JavaScript code without relying on a third-party plug-in. There's been much competition among browser vendors to make JavaScript faster and better.

Why Is It Called JavaScript, Then?

JavaScript really has nothing to do with Java; it isn't just a simplified subset of Java. JavaScript was developed under the name "Mocha" and was named "LiveScript" when it appeared in a beta release of the Netscape Navigator web browser back in 1995.

In 1995, Netscape announced the language would be named "JavaScript" in a joint announcement with Sun. This happened around the time Netscape added support for Sun's Java applets. We can look back at the announcement today:

> *"The JavaScript language complements Java, Sun's industry-leading object-oriented, cross-platform programming language…*
>
> *JavaScript is an easy-to-use object scripting language designed for creating live online applications that link together objects and resources on both clients and servers. While Java is used by programmers to create new objects and applets, JavaScript is designed for use by HTML page authors and enterprise application developers to dynamically script the behavior of objects running on either the client or the server."*

The announcement goes on and on like this, talking about both Java and JavaScript. This is usually seen as an attempt by Sun and Netscape to associate the new language — JavaScript — with the Java language that was popular at the time. The name made people a bit confused and caused them to associate the new language with Java, giving JavaScript some instant respect. If it's called JavaScript and was announced by Sun in an announcement that talked about Java a lot, surely it was related to Java — right? Nope.

In 1998, Brendan Eich, who invented JavaScript, claimed in an interview that JavaScript was intended "look like Java, but be a scripting language" for lightweight usage. It might look a bit like Java, but it's very different.

In 1998, Brendan Eich, who invented JavaScript, claimed in an interview that JavaScript was intended "look like Java, but be a scripting language" for lightweight usage. It might look a bit like Java, but it's very different.

Conclusion on page 14

Charlotte Bytes

CCCGC

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

See us on the Web
www.cccgc.net

Java and Javascript Programming Books

Conclusion from page 13

JavaScript is Practically Mandatory for the Modern Web

RELATED ARTICLE

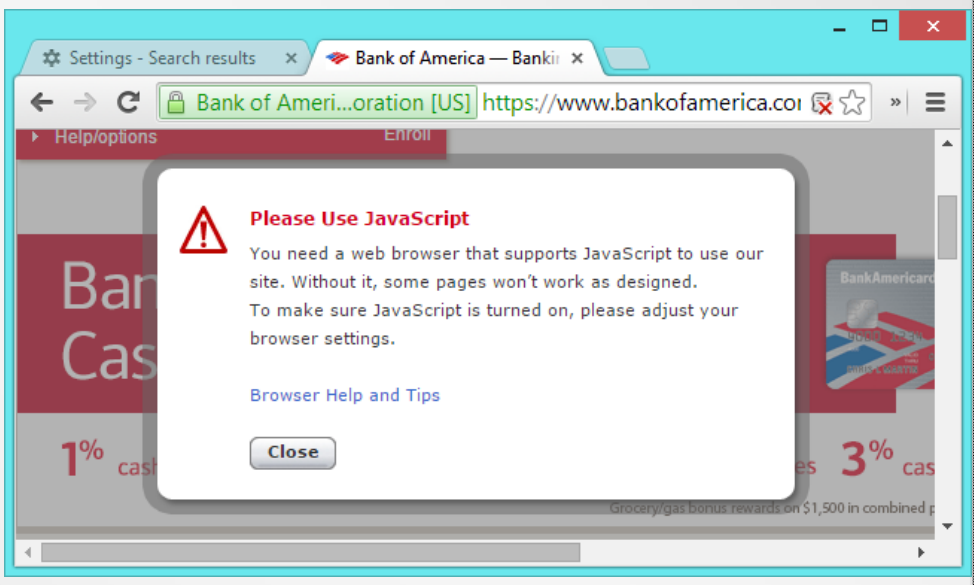
HTG Explains: Should You Disable JavaScript?

Few people disable JavaScript, but many who do are very vocal about it. JavaScript makes the type of web pages... [Read Article]

http://www.howtogeek.com/138865/htg-explains-should-you-disable-javascript/

We've moved away from Java content in the browser over the years. While Java is still widely used, it's become a dirty name when associated with web browsers. Java has also become an increasingly disliked piece of consumer software known for bundling junkware with security updates.

Where the Java name was originally intended to add credibility to JavaScript, the Java association is now tarnishing its name. It's easy for JavaScript to come to mind when you see apocalyptic headlines about Java plug-in vulnerabilities. That was the whole point of the name — to make them seem related.



Some people go out of their way to disable JavaScript in their web browsers with add-ons like NoScript. But **JavaScript** isn't insecure like **Java** is in the browser. Yes, there's an occasional security vulnerability in a web browser that can be exploited via JavaScript, but the hole is patched up and we move on. This isn't unique to JavaScript — there could be a security vulnerability in a web browser that could be exploited via HTML, CSS, or other technologies, too. There's no way to completely protect yourself against possible future browser vulnerabilities. Just keep your browser and its plug-ins updated.

JavaScript powers the modern web, whether you're using a browser on your computer or smartphone. Disabling it would make many websites unusable.

On the other hand, the Java browser plug-in is used on very, very few websites. If you disable the Java browser plug-in, the web will continue working normally. You'll probably never notice you don't have it.

Image Credit: nyuhuhuu on Flickr, Marcin Wichary on Flickr

Why I pay in cash and why you may want to too

By Martin Brinkmann on September 19, 2014 in Security

Whenever I'm out to buy something, as opposed to buying online, I pay for all the goods I buy in cash. Instead of handing over a card or inserting it into a card reader of sorts, I hand over the money directly to the cashier.

I try to do this even in situations where this is uncommon, in hotels for instance if they ask for your credit card. It is usually possible to deposit some money instead of handing over your card and that's what I do normally.

In this article I'm going to lay out the reasons for being against card and digital payment systems.

There is a large drive towards a cashless society where everyone pays by card or digitally with the help of smartphones, watches, or other means of identification.

While that may seem comfortable at first, it introduces a series of problems at the same time.

Lets take a look at some of the issues and find out how cash and non-cash payments differ here.

1. It is harder to keep track of payments if you pay digitally.
2. There is a chance that you buy more than you can afford.
3. Fees and commissions.
4. You give up control.

With card and digital payments, your information get stored and one can link payments to purchases.

Card and payment information are stored as well, and may be stolen by thieves.

It is harder to keep track of payments if you pay digitally or by card and there is a chance that you buy more than you can afford.

While some people may be able to keep track of all their card and digital payments throughout the month, for instance by keeping a detailed record of all their payments, most likely don't.

This falls in line with the second argument against digital payment systems: buying more than you can afford.

With cash, all you can spend is what you have. That's easy enough to keep an eye on throughout the day or month. With cards and digital payments, many don't really know how much they have left to spend which may lead to debt in the long run.

According to studies, people spend between 12% and 18% more when they are using credit cards.

Fees and commissions

Even though you may not pay fees or commissions while using credit cards, merchants to usually. While you could say that this is the problem of the merchant then, guess who is paying the bill in the end?

With cash payments, there are not any fees or commissions involved. Well, unless your bank charges you for withdrawing money from ATMs for example or directly.

Control

If you have followed the crisis of the Euro you may have seen videos or pictures of people standing in line in front of banks trying to withdraw money to make purchases and regain control over it.

While you give up control when you use banks, you give up even more when cash money is not used anymore.

Conclusion on next page

Official Publication of the Charlotte County Computer Group Corp.

PROMOTING COMPUTER LITERACY AND EDUCATION IN CHARLOTTE COUNTY

Using Cash

conclusion from page 14

Privacy

Cash payments cannot be tracked while card payments can. Every card payment is stored digitally so that anyone with access can not only find out what you bought and how much you paid for it, but also where you bought it and when.

Security

Your payment information may not be stored permanently by companies but they are at the very least until the payment has been processed correctly.

Recent and not so recent attacks on point of sale systems in the United States have shown how dangerous this can become. Home Depot confirmed a breach affecting stores in the US and Canada recently where attackers managed to gain access to 56 million customer payment cards and a hack of Target earlier this year leaked more than 40 million card information.

Closing Words

Card payments are convenient which in my opinion is the only thing that is positive about them. It may sometimes be also more secure especially when it comes to making large payments and depending on where you live and buy.

There may be situations where you need to pay by card. Depending on the country you are living in, credit card payments may be the norm while cash payments are not.

Here in Germany, the majority of customers pay cash when they shop locally while part pays using debit cards. Credit Card payments on the other hand are not even supported by many shops.

In the US, things are different. In 2012, plastic card purchases comprised 66 percent of all in-person sales according to a report published in 2012 by market research firm Javelin Strategy & Research with projections that the figure will increase further in the coming years.

What about you? Do you pay cash or by using cards?

Oracle Can't Secure the Java Plug-in, So Why Is It Still Enabled By Default?

Conclusion from page 12

Even after you disable the plug-in, Minecraft and any other desktop application that depends on Java will run just fine. This will only block Java applets embedded on web pages. Yes, Java applets still exist in the wild. You'll probably find them most frequently on internal sites where some company has an ancient application written as a Java applet. But Java applets are a dead technology and they're vanishing from the consumer web. They were supposed to compete with Flash, but they lost. Even if you need Java, you probably don't need the plug-in.

The occasional company or user that does need the Java browser plug-in should have to go into Java's Control Panel and choose to enable it. The plug-in should be considered a legacy compatibility option.