August 2014

Microsoft REGISTERED Refurbisher

Charlotte County Computer Group

30th YEAR Anniversary

1984 - 2014

The Next General Meeting of CCCGC will be **August 5, 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. VIII

The President's Platform by Ron Wallis, President CCCGC

Inside this issue:

It's hard to believe that August is here already. Where did the summer go?
It seems like Memorial Day was just a few weeks ago. The kids will be back in school and the requests for computers will be rolling in.

Soon it will be Labor Day, the official end of the summer season, at least for the people up north. The snowbirds will start coming home soon. We are always glad to welcome them back.

This summer we did have a sad note, the passing of our much loved director Mava Graves, who is greatly missed.

Linda Corrick has been appointed to serve out Mava's term as director. We welcome her and look forward to working with her.

So far this year we have refurbished over 180 computers, and the busiest season is still ahead. We have also repaired many, many members computers through our members help program. We're glad to see thing going so well.

With your help we can keep it up.

Thanks,

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

Richard Mullennex had the ticket that takes the machine to its new home. His computer had died some time ago so this is a welcome addition. Thanks to all that purchased tickets. Good luck next time.

50/50 Winner

Harold Howard has won again!! Congratulations. For all those others that purchased tickets, good luck next month.

Door Prize Winners

Left To Right

ROSEMARY CRAEMER

RICHARD MULLENNEX

THOMAS ERHARDT

CHUCK WRIGHT

RON WALLIS

WELCOME

New Members

James Holden	Richard Angstadt	Hugh Havlik
Martha Hoover	Kristi Cunningham	Maryanne Freeman
Robert Tabb	Carol Dunekirchen	Joyce Burke
Barbara Cooper	Pierre J Fisher	Arturo Angeles
Debbie Amico	Eddie Gonzales	Wayne Pilikian
Joan Pilikian	Terry Seymour	John Stahl
Wanda Carter	Roy Strelchur	Floyd Bowser
Marcia Clark		

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

Yvette Pilch, Vice President read the proposed bylaws to the membership prior to the vote to accept them. After they were read, a vote was taken and the membership approved them with a 2/3's majority. The bylaws are now official.

Dick Evans entertained us with his wit and knowledge of office systems. Dick covered Microsoft Office, Libre Office and Open Office. Libre and Open Office word documents and spreadsheets can be converted to or from MS Office. The trend is to use the cloud software i.e. One Drive and Google Drive. Each cloud office program has its learning curve and takes time to understand how to get the most out of it. Our club has classes with John Palmer on Libre and Dick Evans covers any issues including Microsoft office.

Lydia

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

Security News **Summer is a Great Time to Review and Improve the Ways You Protect Your Privacy**

The lazy, hazy days of summer are rolling along as predictably as ever, with one beautiful day blending smoothly into the next. Everybody is doing their best to enjoy themselves somehow, someway.

But, besides pursuing enjoyment, you might want to view summer as an ideal time to review and improve the ways you protect your privacy. You have, or seem to have more time on your hands. The days are long and the nights are pleasant. So, why not retreat to your favorite spot for an hour or two and jot down some thoughts about beefing up your privacy.

Despite all the news about identity theft and credit card breaches, most Americans surprisingly don't do much to protect their privacy on the Internet.

Sixty-two percent of respondents in a recent national Consumer Reports survey of 3,110 online consumers said they had done nothing to protect their privacy on the Internet. Perhaps, most of us are seized by fatalism or paralysis, or just foolishly hope vendors will take care of their privacy?

Your Info: At risk Everywhere

A recent Consumer Reports article notes that the vulnerability of a computer system is known as its "attack surface" -- all of the points at which an attacker can gain entry and make off with valuable data. These days, as the threat of malicious software and sophisticated cybercriminals reaches every corner of modern life, each consumer has vulnerabilities, too. They extend from the laptop in your home to the doctor's office where you get your yearly checkup. The first step in protecting yourself is to know where you are exposed.

In the Cloud

Widely used cloud services such as Dropbox and Evernote are great for storing files and organizing tasks, but they have a spotty security record, according to the Consumer Reports article.

On Your Computer

The article states that "the arsenal of scams and attacks aimed at your computer is truly breathtaking." This arsenal includes malware and ransomware, as well as increasingly sophisticated phishing.

On Your Smart Phone

Android phones are the main target of hackers, simply because there are so many Android phones. However, plenty of malware exists in third-party marketplaces outside of the Google Play store.

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

August 2014 CCCGC Events Calendar

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
					1	2
3	4 **Libre Office** 2 to 4 PM John Palmer	5 **General Meeting** 7:15 PM Classes 5:00 PM 6:00 PM	6 **EaseUs Backup** 2 to 4 PM Ron Wallis	7 **NO Classes**	8	9
10	11 **Libre Office** 2 to 4 PM John Palmer	12	13	14 **NO Classes**	15	16
17	18 **AndroidTablets** 2 to 4 PM Yvette Pilch	19	20 **Windows 8.1** 2 to 4 PM Ron Wallis	21 **NO Classes**	22	23
24	25 **Windows 8.1** 2 to 4 PM Yvette Pilch	26 **Maintenance** 2 to 4 PM Ron Wallis	27	28 **NO Classes** **Board Meeting** 6:30 PM	29	30
31		**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: Linda Corrick

We're on the Web
www.cccgc.net

VIPRE

Ransomware Attacks Android Devices

Trojan malware called Simplelocker raised its ugly head last month, attacking SD cards in tablets and handsets, scrambling certain types of files on them before demanding cash to decrypt the data.

The message was in Russian, and payment was requested in Ukrainian currency -- evidence that the malware was quite limited in its reach. But, who knows, next month the message may be in English, and the criminals may be seeking payment in US dollars, Euros or British pounds.

Clearly, Android users should be very cautious about installing software from sources other than the Android application store, and should pressure their phone supplier to promptly provide security updates to defend against known vulnerabilities.

Porn alert

The affected device owners were presented with a message saying that their phones and tablets were locked because they had viewed and distributed child pornography, zoophilia and other perversions. The message went on to instruct the victims to pay 260 hryvnias ($22, £13) via the Ukrainian MoneXy cash transfer system. "After payment your device will be unlocked within 24 hours. In case of no PAYMENT YOU WILL LOSE ALL DATA ON your device!" it added. Although this is the first reported instance of Android ransomware encrypting files, there have been other types. In May of this year, there was a variant of Simplelocker that prevented Android apps from launching, effectively making infected devices useless, unless a $300 payment was made. While malware for the Android platform has not reached epidemic proportions as seen with Windows-based PCs, we recommend protecting your Android-based smartphones and/or tablets with VIPRE Mobile Security.

3.1 Million Smart Phones Were Stolen In 2013, Nearly Double the Thefts in 2012 About 3.1 million Americans were the victims of smart phone theft in 2013, according to Consumer Reports' Annual State of the Net survey. That's nearly double the 1.6 million thefts that the company projected in 2012. At least 1.4 million smart phones were lost and not recovered last year, up slightly from the 1.2 million in 2012, noted the report. On a positive note – the proportion of smart phone users who set a screen lock with a 4-digit pin increased by about 50 percent in 2013. Still, the vast majority of smart phone owners neglected to take more aggressive measures, such as using screen locks stronger than 4 digits or installing software that could locate their phone or remotely erase its contents. How smart phone users secure their phones:

- Set a screen lock with a 4-digit pin (36 percent)
- Backed up data to a computer or online (29 percent)
- Installed software that can locate the phone (22 percent)
- Installed an antivirus app (14 percent)

Conclusion on Page 7

Conclusion from page 6

- Used a PIN longer than 4 digits, a password, or unlock pattern (11 percent)
- Installed software that can erase the contents of the smart phone (8 percent)
- Used security features other than screen lock (e.g. encryption) (7 percent)
- Took none of these security measures (34 percent)

"Given how much personal information smart phones can contain – from photos, contacts, email accounts to social-networks, shopping, and banking apps – losing one of these devices or having one stolen can definitely be cause for panic," said Glenn Derene, Electronics Editor, Consumer Reports.

"Our survey revealed that the number of lost and stolen smart phones is on the rise, and too many smart-phone users are needlessly imperiling their personal data by not taking basic security measures."

New OpenSSL Bug Could be Worse Than Heartbleed

More weaknesses have been detected in the OpenSSL web encryption standard, just months after the Heartbleed bug was found to be affecting the same technology. Tatsuya Hayashi, the researcher who found the latest bug, told England's Guardian newspaper that the latest flaw "may be more dangerous than Heartbleed" as it could be used to directly spy on people's communications.

Heartbleed was deemed to be one of the most critical internet vulnerabilities ever when it was uncovered in April. OpenSSL is supposed to protect people's data with digital keys but has been exposed as flawed numerous times in recent months.

The latest vulnerability was introduced in 1998 and has been missed by both paid and volunteer developers working on the open-source project for 16 years.

Using the vulnerability found by Hayashi, attackers sitting on the same network as a target, such as on the same public Wi-Fi network, could force weak encryption keys on connections between victims' PCs and web servers.

Using those keys, attackers could intercept data. They could even change the data being sent between the user and the website to trick the victim into handing over more sensitive information, such as usernames and passwords. This is known as a "man-in-the-middle" attack.

The vulnerability affects all PC and mobile software using OpenSSL prior to the latest version, believed to include the Chrome browser on Android phones, and servers running OpenSSL 1.0.1 and the beta version for 1.0.2.

Many popular browsers appear to be safe from attack, noted Google security engineer Adam Langley, in another blog post. "Non-OpenSSL clients (Internet Explorer, Firefox, Chrome on Desktop and iOS, Safari, etc) aren't affected. Nonetheless, all OpenSSL users should be updating," he said.

CCCGC

Charlotte Bytes

6 Tips For Creating An Unbreakable Password That You Can Remember

By Ryan Dube

You can lock every door and window of your house, but if you use a skeleton key the odds are pretty good someone is probably going to end up robbing you blind. The same is true of your passwords. If your passwords are not unique and unbreakable, you might as well open the front door and invite the robbers in for lunch.

A few years ago, Damien described a few ways to come up with strong passwords, http://www.makeuseof.com/tag/how-to-create-strong-password-that-you-can-remember-easily/ like making sure you use special characters and that the password is at least 8 characters long. Still, creating a complex password is only half the job, the other half is actually remembering it.

And, is any password truly unbreakable? Not really, but in a recent interview with Bruce Schneider, Bruce referenced one of his blog posts about choosing a secure password. His advice was to take sentence and turn it into a password. His exact words were, "Choose your own sentence – something personal."

This sounds like a simple concept, but even coming up with a sentence that you'll remember can be as difficult as coming up with a password itself. About a year ago, Yaara offered some tips that could help you remember your passwords. http://www.makeuseof.com/tag/7-ways-to-make-up-passwords-that-are-both-secure-memorable/ The following are a few more tips that might help you develop passwords that are especially complex, nearly unbreakable, but also memorable.

1. **Nursery Rhymes**

One preferred method of coming up with complex passwords that pass every IT security policy out there – even those that require 15 character passwords – is the nursery rhyme technique.

The way this works is you choose one of your favorite nursery rhymes, capitalize the first letter of each sentence, replace certain letters with numbers, and follow that up with an exclamation point or some other symbol at the end. For example, take the nursery rhyme Little Boy Blue, which goes like this:

"Little boy blue, come blow your horn. The sheep's in the meadow. The cow's in the corn."

Now you transform that replacing any "s" with "5" and any "L" with a 1 or a 7. Here's the new password.

"7bbcbyhT5itmTcinc!"

That's an 18 character password that includes numbers, letters, uppercase, lowercase and at least one special character.

2. Favorite Line of a Song or Movie

A technique similar to that above uses famous movie quotes to come up with the password rather than nursery rhymes. There are actually very popular nursery rhymes people may use, that hackers could guess. Using a favorite movie line – especially one that is particularly obscure – will make this approach much more secure. You may also consider replacing characters with numbers that are not so easy to guess.

For example, lots of people would think to replace an "s" with a "5" , but if you choose a different number, it'll be harder to guess. Replace every "s" with a 6 or 7 instead – easy to remember because they start with the letter "s". You might also replace every t with a 3 using the same logic.

Using this new approach, you may start with the famous movie like from Al Pacino in the movie Scent of a Woman:

"If I were the same man that I was thirty years ago I'd take a flamethrower to this place!"

This quote then becomes:

"IIw36m3Iw3yaI3af33p!"

This concept is basic cryptography 101, but it'll at least provide a compromise between coming up with a password that is very difficult to hack, but also one that a normal human brain can remember.

Continued on Page 9

6 Tips For Creating An Unbreakable Password That You Can Remember

3. Use Industry Lingo

One alternative of this is using very specialized industry lingo to come up with the phrase. Nursery rhymes or even movie quotes could be guessed with a computer algorithm running through as many possibilities as a computer can manage. However, industry-specific lingo is much harder to guess.

For example, if you're a nurse, your phrase might be:

"The aortic coarctation led to an agonal response, BLS and finally intracerebral infarction."

(I've no idea if that makes any sense, but you get the point).

Replacing "a" with 0 results in the following password:

"T0clt00rb0fii!"

This is only 14 characters rather than 18, but much harder to guess.

4. Personal Dates

An alternative technique to using sentences is using mostly numbers. Of course, random numbers aren't exactly simple to remember either. However, one technique that I learned from my father (he used it for choosing lottery ticket numbers) was to go with important family dates.

Now, the first thing many people think is to use birthdays. Unfortunately, these days it's far too easy for the savvy hacker to discover online. You need something a little more advanced than that. A good approach is to use dates of events only you would remember as important to you, but no one else would really know about. The day that you first took a roller coaster ride. The day that you kissed for the first time. The day your parents gave you your first bike.

Take the three dates that you are sure to remember, and line them all up in a row. Replace the slashes with a lower-case L, a space between dates with a "_", and end with a special character like "!" or "#". Such a password would look something like this:

"10l08l86_03l14l94_09l06l98#"

This password is 27 characters, so it can only be used in systems that can handle very long passwords. If allowed however, it'll allows you to have one of the most secure passwords possible.

5. Use a Keyboard Pattern

Here's a fun password approach that uses the same technique as the smartphone login pattern. In this case, what you're going to use is your keyboard. Draw some kind of recognizable pattern on your keyboard, and then use the letters and numbers as the password. For example, let's say you create a pattern on your keyboard as shown below.

If you start this pattern at the number 3, it should be pretty easy for you to draw out the pattern each time. If it helps, you might even draw recognizable images or letters on top of the keyboard. In the case above, the password ends up as follows:

"3waxcvgy7890-="

Using this approach, you can alter the complexity of the pattern to lengthen the password. A hacker could potentially run an algorithm through that would attempt every password possible on a keyboard by connecting every key to one another, so making the pattern as complicated as possible – such as going back and forth or making complex, diagonal lines – should make that kind of hacking much more difficult.

Conclusion on Page 15

Charlotte Bytes

See us on the Web
www.cccgc.net

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

CCCGC

What You Need to Know About Creating System Image Backups

System images are complete backups of everything on your PC's hard drive or a single partition. They allow you to take a snapshot of your entire drive, system files and all.

Windows, Linux, and Mac OS X all have integrated ways to create system image backups. There are sometimes good reasons to do this, but they shouldn't be your regular backup strategy.

What is a System Image?

RELATED ARTICLE

http://www.howtogeek.com/189452/8-backup-tools-explained-for-windows-7-and-8/

8 Backup Tools Explained for Windows 7 and 8

A system image is a file — or set of files — that contains everything on a PC's hard drive, or just from one single partition. A system imaging program looks at the hard drive, copying everything bit by bit. You then have a complete system image you can copy back onto a drive to restore the system state.

The system image contains a complete snapshot of everything on the computer's hard drive at any given time. So, if you have 500 GB of space used on a 1 TB drive, the system image will be about 500 GB. Some system image programs use compression to shrink the system image's size by as much as possible, but don't count on saving much space in this way.

Different system image programs use different types of system images. For maximum compatibility, you should use the same tool you used to create the system image to restore it. Windows itself creates system images that contain multiple files with the .xml and .vhd file extensions. System images are just one of the many back up tools included in Windows.

What Files Should You Backup On Your Windows PC?

Everybody always tells you to make sure that you are backing up your PC, but what does that really mean? And what files do you actually need to backup? Today we'll walk you through the basics of backing up your PC, what you should back up, and why.

[Read Article]

System images aren't the ideal way to create normal backups of your computer and its files. System images are very large, and they contain files you really don't need. On Windows, they'll probably include tens of gigabytes of Windows system files. If your hard drive crashes, you can always just reinstall Windows — you don't need backup copies of all these files. The same goes for program files. If your hard drive crashes, you don't need an image of your installed Microsoft Office and Photoshop program files — you can just reinstall these programs on a new Windows system. I am sure HTG must know the time and trouble it takes to **reinstall windows and all its updates**, and then reinstall all the programs if you have the disks or are able to find them.

System image backups will capture files you can easily redownload and reinstall as well as files you don't care about. You can't control what is and isn't backed up — you end up with an image containing everything on your hard drive. (In Easeus and Acronis Backup software, you can control what is backed up.)

Because so much data has to be backed up, a system image will take a much longer time to create than a smaller, more focused backup. It will also be harder to import on another computer. If your entire computer dies, you won't be able to just restore a system image that was created on another computer — your Windows installation won't run properly on different hardware. You'd need to reinstall Windows anyway.

Continued on Next Page

CCCGC

Charlotte Bytes

Conclusion from page 10

What You Need to Know About Creating System Image Backups

This doesn't just apply to Windows. Macs include an integrated way to create system images, and Apple advises you only restore system files on the same Mac the backup was created on.

For typical backups, you should just back up the files that are actually important to you. If your system ever goes down, you can then reinstall Windows and your programs and restore your personal files from the backup. Use File History to do this on Windows 8 or Windows Backup to do this on Windows 7.

When You Should Create a System Image

System images can still be useful. For example, let's say you want to upgrade your computer's hard drive — maybe you're upgrading from a slower mechanical hard drive to a speedy solid-state drive. You can create a system image of your computer's hard drive, swap the drive out for an SSD, and then restore that image to the SSD. This will migrate your entire operating system to the SSD. Of course, if both drives can fit in your computer at once, you may be better off using a system imaging program to copy the contents of your hard drive directly to the SSD rather than creating a system image backup and then restoring from that, which will take twice as long.

These types of images can also be used by system administrators, who could roll out a standard system image on different PCs across their network. A server or other mission-critical computer could be configured and a system image created to restore the software to that specific state.

If you're a typical home user looking to back up your files, you probably don't need to create a system image.

How to Create and Restore System Images

To create a system image on Windows 8.1, open the Control Panel, navigate to System and Security > File History, and click the System Image Backup link at the bottom-left corner of the window. On Windows 7, open the Control Panel, navigate to System and Security > Backup and Restore, and click the Create a system image option.

You can then restore these backup images using the Advanced Startup Options on Windows 8 or the System Recovery option on Windows 7. These can be accessed from a Windows installation disc or recovery drive.

On a Mac, you can use Time Machine create and restore system image backups. Time Machine backs up system files as well as your own files, and you can restore a Mac from a Time Machine backup from Recovery Mode. On a Linux PC, you can use the low-level dd utility to make an exact copy of a drive and restore it later.

Acronis True Image and Norton Ghost are popular third-party disk imaging tools you can use for this, too.

(I prefer EaseUs To Do Backup as it is easy to use works great and is free!!)

While developing Windows 8.1, Microsoft removed the "System Image Backup" option from the user interface and forced people to access it from a PowerShell window. After widespread complaints, Microsoft restored this option to the graphical interface.

Microsoft's motive was pretty clear here — average PC users shouldn't be distracted by system image backups and should just use a simple backup solution like File History. Microsoft eventually restored the graphical option to make people happy, which is fine — but they were right that most Windows users shouldn't use it.

Image Credit: Phillip Stewart on Flickr

CCCGC

Microsoft REGISTERED Refurbisher

Charlotte Bytes

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

Why We Hate Recommending Software Downloads To Our Readers

Windows software downloads are a mess. Many programs try to drag adware and other malicious junk onto your computer. Even safe programs we test sometimes turn to the dark side and start bundling junk later.

More experienced geeks may not fall for this stuff as often, but we have all kinds of readers here. We prefer to avoid putting our readers into situations where they could be infected because they downloaded something we recommended.

Software Downloads Change

Here's the worst thing we have to deal with. We regularly test software and find it's clean and work well, so we recommend it to our readers. We did our due diligence — everything is fine.

But applications are often sold to new owners, or the current owner becomes desperate for income. These formerly trustworthy applications add adware, browser toolbars, spyware, and other junk to their installers. New readers download these tools because we recommended them, and we then start getting emails asking why we're recommending software that infects our readers' computers.

It's impossible to police and regularly check all the software we link to, and we don't want a huge archive of articles linking to sketchy software that can hurt our readers. If an application isn't completely trustworthy and there's a different way to do something, we'll probably recommend that way.

This shouldn't apply to more trustworthy software, but it sometimes does. We regularly recommend software like Firefox, Chrome, LibreOffice, CCleaner, VLC, and other popular applications. However, we've also recommended popular applications like Foxit Reader and µTorrent and seen them turn to the dark side. Lesser-known utilities are even more suspect.

Lowell Heddings @howtogeek

Foxit Reader is bundling Conduit search hijacking awfulware too. Time to purge all links from HTG. Adware, Toolbars, and Other Junk in Installers

Installers filled with junkware are perfectly normal in the Windows software scene. This is true even for established, legitimate software. Oracle's Java runtime attempts to install the Ask Toolbar. µTorrent is a popular BitTorrent client, but have you tried downloading it recently? You have to click through various offers that attempt to install the Conduit Search adware and a scammy PC cleaner on your computer. This junk is marked as "Recommended by BitTorrent", so less experienced users may think it's actually recommended software, not that they're being paid to recommend junk they would never use themselves.

RELATED ARTICLE

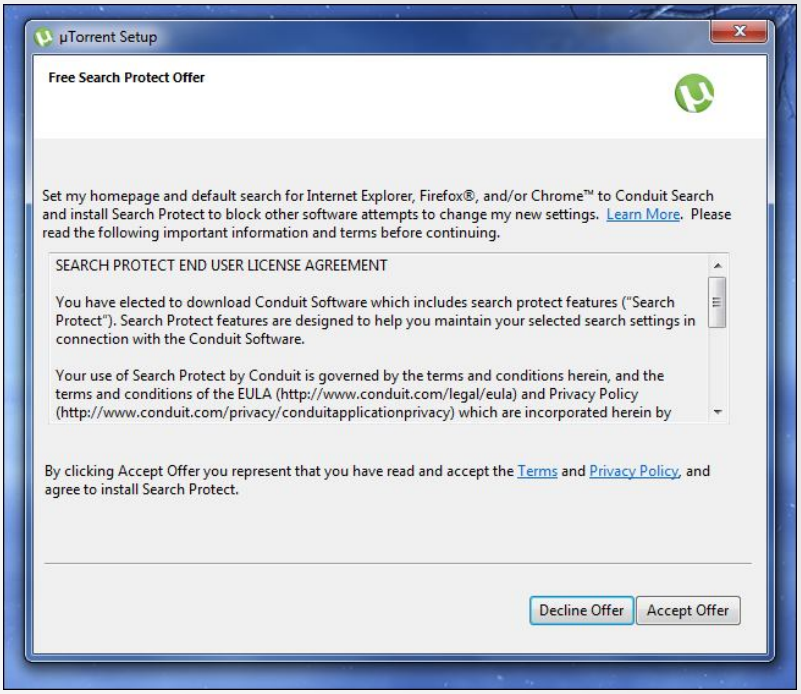
The Shameful Saga of Uninstalling the Terrible Ask Toolbar http://www.howtogeek.com/138516/the-shameful-saga-of-uninstalling-the-terrible-ask-toolbar/

If you managed to get infected with the absolutely terrible Ask Toolbar on your computer, don't be ashamed – it... [Read Article] Next Page.

CCCGC

Charlotte Bytes

Why We Hate Recommending Software Downloads To Our Readers



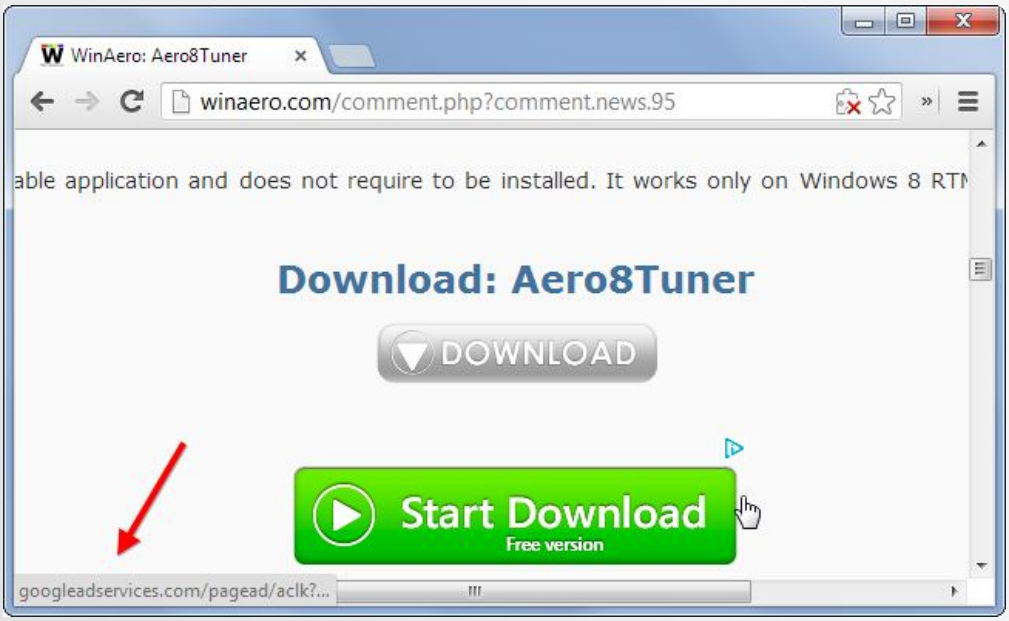
We've tried to avoid this in the past by including warnings in the article. We'd write something like "Be careful when installing this software, because it will try to install junk on your computer. Be sure to decline the offers." But not all readers will pick up on that warning. Some readers may see the warning and accidentally agree as they click through the installation wizard — it's meant to trick you, after all. The Ask Toolbar even attempts to hide before installing itself, so you can't immediately uninstall it if you accidentally agree. You'll have to wait until later — Ask is hoping you'll forget to do that.

Yes, we Windows geeks have built up an immunity to this type of junk. Many of us don't even notice — we just carefully click through installers and consider it normal. But many people still fall for this trap.

Fake Download Links

RELATED ARTICLE

How to Avoid Installing Junk Programs When Downloading Free Software http://www.howtogeek.com/168691/how-to-avoid-installing-junk-programs-when-downloading-free-software/



The web is littered with traps for novice users when downloading software, from fake "Download" buttons that are actually advertisements... [Read Article]

Fake download links are particularly obnoxious. You go to a program's download page and see five different "DOWNLOAD" buttons. Which is the real download button, and which are actually advertisements that will lead you away from the real software to something that will damage your computer?

Sure, there are tricks you can use here. You can mouse over a link and see where it goes. If you download software for long enough, you'll pick up a sort of sixth sense and realize which are fake download links and which aren't. But these links trick people.

Continued on Page 14

Charlotte Bytes

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

See us on the Web
www.cccgc.net

CCCGC

Why We Hate Recommending Software Downloads To Our Readers

We're not thrilled about the other software downloads these sites push, either. For example, let's go back to µTorrent again. When you download µTorrent, µTorrent "recommends" you download the VLC media player. This sounds like a great recommendation — VLC is a very good media player.

This link won't take you to VLC's official download page; it takes you to a third-party download site. Who knows what this other site is wrapping VLC in — you'll probably get infected with some type of junk if you install it. If they're paying for these advertisements, they're making money from these downloads somehow.

To add insult to injury, µTorrent actually warns you to "Beware of online scams!" when you install it. This warning says you should only download µTorrent from its official site because you could get infected by malware if you download µTorrent from an unofficial site. Yet they're "recommending" you download VLC from a shady third-party site.

Official Publication of the Charlotte County Computer Group Corp.

PROMOTING COMPUTER LITERACY AND EDUCATION IN CHARLOTTE COUNTY

Conclusion from Page 9

6 Tips For Creating An Unbreakable Password That You Can Remember

6. Establish a Rudimentary Hardware Key

The final technique that's worth trying for an ultra-secure password is the hardware key approach. In most corporations, employees are provided with a hardware "token" or key, which has a digital number on it that changes at a regular interval. That number is used as one part of the login process.

In much the same way, you can print out and carry a card where you've written down part of your password pair. The other part of the pair would be the part of the password that you need to remember.

For example, your password might be "2BeOrNot2BeThatIsThe?" So, you would write down "ThatIsThe?" on a piece of paper, and this will remind you what your entire password is.

The value here is that even if someone finds the written portion of your password, they still won't have the part of it that exists in your head. At the same time, it gives you a powerful tool to extract that part of the password out of your head when you're having a bad memory day.

Ultimately – the password that you go with should be the one that works best for your situation. You can use any of the techniques above, or come up with one of your own, but the idea is to develop a password that is so unusual, with such a variety of character types, that hacking that password becomes a nearly impossible chore.

Image Credits: baby crib via ziviani at Shutterstock, s_bukley / Shutterstock.com, Nurse making call via Monkey Business at Shutterstock, Riding a bike via Brian Jackson at Shutterstock