

The Rochester Computer Society, Inc.
a computer club open to everyone

MONITOR

Vol. 33, No. 10

October 2016

Next Meeting - Tuesday, October 11

Presentation, via Skype

Protecting Yourself, Your Computer and, Your Identity
by [Norbert \(Bob\) Gostischa](#), Avast Software Evangelist

* * * Upcoming Presentations - Tuesday, November 8 * * *

Gifts & Gadgets and Black Friday Predictions by Arpad Kovacs

Tuesday, December 13, via Skype

Free, and Alternatives to Free, Software by John Kennedy

East-Central Ohio Technology Users Club

In This Issue

Computer Attacks

Musings of an Apple Tyro

Setting up a New Computer

How Do I Encrypt a File?

Firefox and Security Addons for Linux

Communications – Voice and Digital -

All in one Package

How to get the Windows 10 Anniversary Update

Interesting Internet Finds

Dick Maybach

Lorrin R. Garson

Ask Leo!

Tony Dellelo

Phil Sorrentino

Sandy Berger

Steve Costello

Founded 1982

www.rcsi.org



Member of
An International
Association of Technology
& Computer User Groups

Computer Attacks

By Dick Maybach

Member, Brookdale Computer Users' Group, NJ

An important factor in defending your computer is to understand how it might be attacked. This topic fascinates many computer owners and has been the subject of many articles, books, advertisements, and discussions. One result of this is a jumble of terminology with words having meanings almost as slippery as the programs they are trying to describe. In this article I'll attempt to untie the terminology knot with brief definitions of the most common terms. You can learn (much) more with an Internet search for any of these terms, provided you read with skepticism. We'll start by using **attack** to describe any malicious act directed at a computer, the data it contains, or its user. We can classify attacks in three different ways:

1. their **attack method** (how they access your PC, your data, or you),



"Your Computer User Group of the Air", Saturdays from 12:00 pm to 2:00 pm with Nick Francesco, Dave Enright, and Steve Rae. Broadcasting on JAZZ 90.1 FM from Rochester, NY. Call 966-JAZZ (585-966-5299) or 1-800-790-0415

Get 35% off from O'Reilly, No Starch, Paraglyph, PC Publishing, Pragmatic Bookshelf, Rocky Nook, Site Point, or YoungJin books you purchase directly from O'Reilly. Just use code "DSUG" when ordering online or by phone 800-998-938. Free ground shipping on orders of \$29.95 or more.

Some Past Presentations:

Keeping Mobile Devices Secure
Mobile Payments
Flash Drives-Not Just for Storage
Features, Mac OS X & Windows
Tablets, the Programs and Uses
Preview of Windows 10
Personal Finance Software
Amazing Browser Tips
How Domain Name Sys Works
Linux is Like Cars
Close up Photography
Virtual Computer OS Demo

2. their **behavior** (how they get established and perhaps spread), and
3. their **payload** (what they do).

To a great extent, these characteristics are independent, and we can look at each in turn. Much of the confusion about malware arises because authors don't make it clear whether what they are describing is an attack method, a behavior, or a payload.

First consider network attacks, which may not affect your computer at all. The first type, **network monitoring** is passive and is a digital version of a phone tap; everything you send and receive is recorded by a third party. This is easily done at a public hot spot, and requires only a laptop and widely-available software. It also can occur at ISPs and Internet relay points, either by the facility owner or by government agencies. A second type, the **man in the middle** attack, is active and is much more specific. Here, a computer is set up to mimic, for example, your Internet bank. If you can be fooled into logging into it, the attacker can capture your password and other account details before forwarding your traffic to the bank site you think you are using. This is more difficult to set up than simple network monitoring and is thus less common.

Let's now look at computer attack methods, which include

- physical access,
- social engineering,
- Trojan horses, and
- unethical suppliers.

Someone with **physical access** to your PC can install malicious hardware or software. Although this is sometimes called the **evil maid** attack (presumably because it's done by a hotel's housekeeping staff), it more commonly occurs

when someone uses your PC with your permission and inadvertently infects it

during, for example, a careless Internet browse. You now have a compromised PC for such tasks as your Internet banking. **Social engineering** or **phishing** occurs when someone tries to convince you to disclose sensitive data or perform some action that compromises your computer. You might receive a phone call or an e-mail message claiming to be from your credit card company requesting your account information, or one from tech support offering to remove a virus they somehow have detected remotely. Many attacks occur as **Trojan horses**, where malevolent software hides inside something that appears useful, interesting, or at least harmless. Examples include e-mail (often appearing to be from somebody you know) with an attachment that installs software, Web pages that run programs on your PC, and macros embedded in office files. Finally, there are **unethical suppliers** that include software you neither need nor want with their products. Although the most common culprits are Websites, it can take the form of **shovelware**, useless and sometimes intrusive programs installed on PCs, and malicious software on supposedly blank media.

Once **malware** (which malicious software is often called) infects your PC, it can behave in four different ways:

TSC

Computer
and Electronics
Repair

Custom Computers - Electronic Surplus and Recycling
 Home Service - Small and Mid Size Business IT Mgmt.

765 Elmgrove Rd, Ste 2
Rochester, NY 14624

Phone (585) 429-6880
Fax (585) 429-7671

www.tscelectronics.com

Special Interest Group

Linux Sig

The workshop is the **third Saturday of each month**, at Interlock Rochester, 1115 East Main St. www.interlockroc.org



Enter through door #7 on the end of building, near *Comics Etc* and Goodman St. Find 'Interlock' on the intercom directory to get buzzed in and go upstairs to suite #200. We have experts on hand to fix problems and answer questions about Linux and FOSS (**f**ree and **o**pen **s**ource **s**oftware). **Bring your system** in so we can help you get the most out of it. Hope to see you there.

The RCSI 'Monitor' newsletter can be found in most public libraries in Monroe County, and many college libraries. *Free* copies can also be found in the following computer stores; Microworx, TSC Electronics, Just Solutions, and Pod Computers.

- reside there as a normal program file,
- attempt to hide by changing its form or the operating system configuration,
- spread through your computer by attaching a portion of itself to other files, or
- send copies of itself to other computers, usually via the Internet.

Type (2) programs are called **stealth software** or **rootkits**, type (3) programs are called **viruses**, and type (4) are called **worms**. An interesting form of virus resides in office document as a **macro**, for example written in Visual Basic and included in an MS Word or Excel file. These can migrate to your master template and infect every document you compose after that. When they first appeared around 2000 macro viruses were serious problems, but office suites now have effective safeguards against most; however, you may wish to check your preferences to be sure. (Although many people use the term virus for all malware, only 17 per cent of it really behaves this way and another eight per cent acts as worms.) Combinations are also possible; for example, a virus can have stealth features. Since rootkits and viruses can affect system programs, their installation often, but not always, requires that the user grant them administrator privileges. A number of vendors offer applications to detect rootkits, but removing one sometimes requires erasing the computer's hard drive and reinstalling the operating system. Many people call type (1) programs Trojan horses, but I prefer to use that term for a malicious program's attack method rather than it's behavior after it becomes active.

Note that network attacks, social engineering, and macro viruses are operating-system agnostic. OS X and Linux users are just as vulnerable to them as are Windows users.

The object of most malware is to deliver a payload that is to perform some action to harm the computer owner or benefit the malware supplier. The payload is independent of the attack method and also of the malware's behavior. Examples are:

- (1) ransomware,
- (2) adware,
- (3) spyware,
- (4) key loggers,
- (5) botnets, and
- (6) hijackers.

Ransomware restricts your access to your PC and displays a message on how you can purchase instructions or software to remove the limitation. In some cases it encrypts files and demands the fee in return for the password to regain access to them. Sometimes there is just a threat, such as pay a fee within 10 days or your hard disk will be formatted. **Adware** continually displays advertising messages on your screen, although this can be legitimate (if annoying) when it's associated with trial software and seeks to sell you the paid version. **Spyware** transmits sensitive information, such as account information and passwords to an Internet location without your permission. Some people lump adware and spyware together and call both spyware, but I prefer to keep them separate, since spyware is more costly. A **key logger** records your keystrokes and forwards them to an Internet location with the intent of capturing log-in information; it can be implemented by either hardware or software. Malware can make your PC a component of a **botnet** (also called a zombie army), a computer network sometimes used to distribute spam or to attack other Internet sites by trying to overwhelm them. Other payloads, having a variety of names that often include the term **hijack**, change the configuration of your browser by changing your home page or your search engine or by adding menu bars.

By far the best time to defend your computer is in the attack phase, where healthy suspicion is your friend. Be careful reading e-mail, surfing the Internet, and using your laptop in public places. Note that some form of social engineering is a component of most attacks. After the attack, an anti-virus program may be able to recognize the malware's behavior and prevent it from delivering its payload. Here, you depend on the malware spreading relatively slowly, so that anti-virus vendors have had time to develop a defense before you encounter it, and fortunately this is most often the case. Once the payload has been delivered, the damage has been done, and you will have to stop using the computer until it can be cleaned, change your passwords, and work with your bank, credit card vendors, and others to repair the damage.

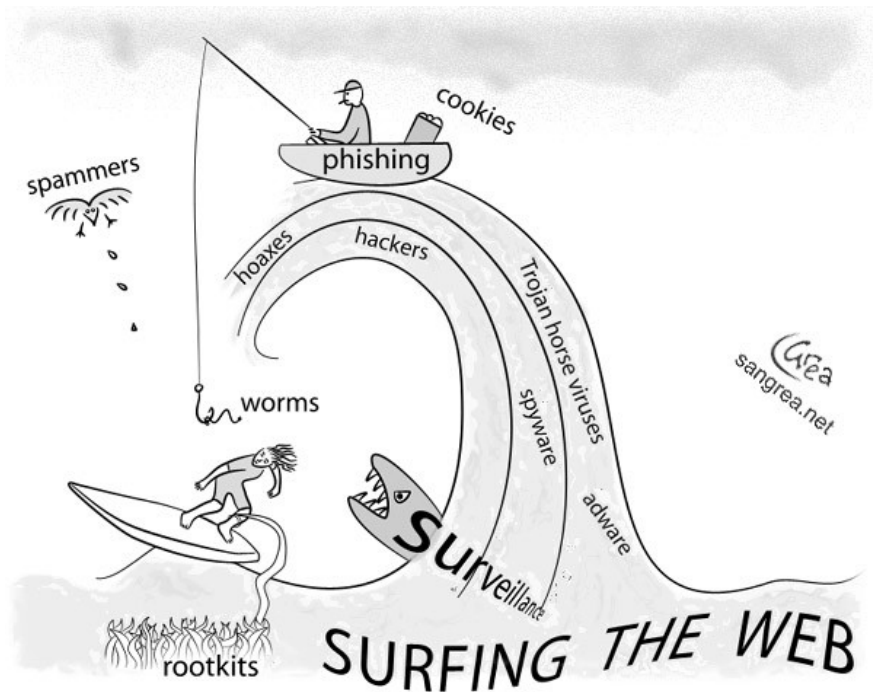
We usually think of malware defense only for PCs, but it also infects all computer-driven devices, such as smart phones and network routers. It's important that you include these in your safe computing plan.

Your ultimate defense against all malware is a backup made before your PC became infected. Wiping and restoring your hard disk will almost always restore your system, except in the rare cases where the malware resides in your PC's BIOS firmware, in which case you probably need expert help. Unfortunately, the Unified Extensible Firmware Interface (UEFI) adds a new vulnerability as it includes a

partition on your hard disk. Since the code residing here executes before your operating system; any malware installed there becomes active before any anti-virus program. Re-installing the operating system will probably leave the infected partition unchanged. So far, this is only a theoretical threat. I mention it only to make the point that threats evolve continuously, which requires that you keep all your software, not just your anti-virus programs updated, and conscientiously practice an effective back up discipline.

To summarize, we can classify computer threats according to their attach method, their behavior, and their payload. Attack methods include physical access to a computer, social engineering, Trojan horse software, and unethical suppliers. Once established, malware can behave as normal software, a rootkit, a virus, a worm, or a combination of these. Typical payloads are ransomware, spyware, key-logger, botnet, and hijacking. Network attacks are special in that they occur outside your computer.

From the June 2016 issue, BUG Bytes, www.bcug.com, n2nd@att.net.



Musings of an Apple Tyro

Setting Up a New Computer

By Lorrin R. Garson
Potomac Area Technology and Computer Society

Buying a new computer isn't like buying a new car—turn on the engine and go. No! No! This applies to any type of computer, Apple, Windows or Linux. That new computer out of the box is quite vulnerable. Here are some suggestions to protect your new machine and you.

1. Be sure your new system is connected to the Internet.
2. You need to install the latest operating system updates. Depending on how long your new machine sat on the store's shelf this can take just a few or many minutes.
3. Install a second Web browser. Computers come with a browser (Safari for Apple, Internet Explorer or Microsoft Edge for Windows), but you need at least two browsers. Why? If a single browser gets badly corrupted or deleted, how are you going to recover the browser without a browser? Firefox, Chrome and Opera are good choices and there are numerous others.
4. Time to install anti-virus software... or not. For Windows systems, it's essential. Windows Defender comes with new Windows machines, but sometimes PC makers turn it off and install trialware for a premium security product like Norton or McAfee. Turn on Defender or the trialware and, if you think appropriate, buy the premium package soon. For Apple computers, most home users don't install anti-malware software, but this is a somewhat controversial issue. There is numerous free anti-malware software for Windows, Apple and Linux systems.
5. Clean out the bloatware. This applies to 2 machines from big-

name PC makers but not Apple or Linux computers. PC Decrapifier (“...it’s like TP for your PC”) has good reviews and is available from <https://www.pcdecrapifier.com/>. CCleaner is another respected tool (see <http://www.piriform.com>). Be sure to create a restore point before running these program, just in case.

6. If appropriate, transfer your files from the old computer to the new machine. If you have switched operating systems this will be more challenging, although ordinary files (Microsoft Office, pictures, etc.) are generally straightforward to move.
7. Implement backup. Hopefully before purchasing your new machine you decided on a backup plan and acquired the necessary software and an external storage device or two. Remember, disk drives have a significantly higher failure rate the first year than in the next 2-3 years.
8. Acquire and install your “must have” software. Hopefully here also you have planned ahead for what you need. Don’t forget a password manager.

At this point you should be good to go, but you’ll spend the next several weeks fine tuning your new computer environment.

Gargantuan Disk Drives

Perhaps with your new computer you need a lot of storage. Consider buying Seagate’s 8 TB hard drive for \$385. See <http://bit.ly/1Q2AjrO>. If that isn’t enough you can plunk down an estimated \$13,000 for a 13 TB SSD drive from Fixstars. See <http://bit.ly/1nnnwXS>. Very few people are going to need anything like this capacity, but this shows how storage capacity is growing.

Troubleshooting Wi-Fi

Occasionally we all experience Wi-Fi problems. Frequently just turning off the power to routers and switches, waiting a bit, then turning devices back on solves the problem. But when this doesn’t do the trick, OS X on Macs has a nifty diagnostic tool most users

down the “option” key and left-Finder menu. This will display telling values will often indicate if

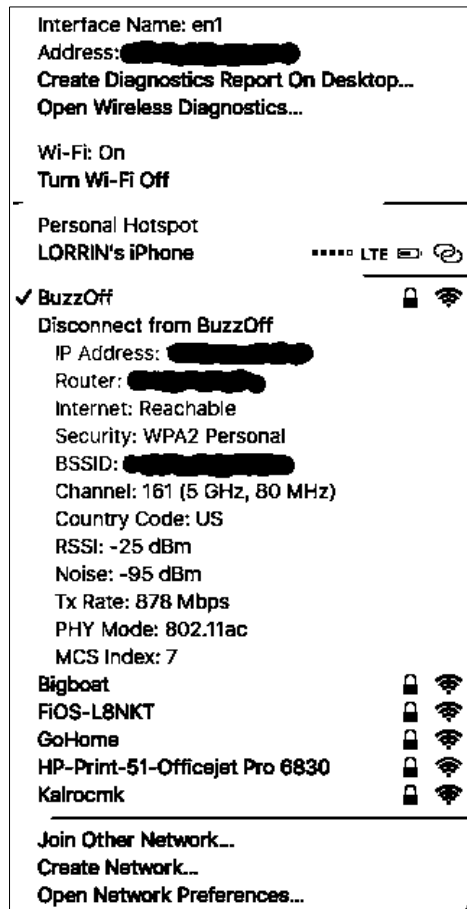
- Tx Rate (878 Mbps in which data is being your computer.
- RSSI (-25 dBm). This which shows the the better.

Left-clicking on “Create “Open Wireless Diagnostics...” will information. It is suggested you experiencing a problem to normal operation.

Also see <http://bit.ly/1SiQcOF> and

Mactracker

On occasion it can be Apple product. Mactracker, free This Application can provide ever made as well as information example, in the next figure is the under the “General” tab.



don’t know about. To access this tool, hold click on the wireless icon () on the the panel shown next. Two particularly you are having a problem, specifically: this case) which is the actual speed at transmitted between your access point and

is the “Received Signal Strength Indication” strength of your signal. The closer to zero


Diagnostics Report On Desktop...” and generate much detailed analytical experiment with this tool when not understand what values are associated with

<http://bit.ly/1SiQxRr>

challenging to find information for a specific from the Apple’s App Store, to the rescue. detailed information on every Mac computer on Apple mice, keyboards iPads, etc. For information of an iMac 21.5-inch, late 2013

Swift Available for Linux Apple made its Swift programming language open-source some time ago, but now has made it available for Linux (Ubuntu 15.10 and 14.4). This won't have a direct impact on 99.9+% of home users. This move is aimed toward the Linux server market. Many servers use Linux as their OS. Apple benefits by getting developers to improve Swift with their suggestions and by enticing developers to adopt Swift aims to get developers to create software for OS X and iOS. Who knows, Swift may be available for Windows and Android some day. See <http://bit.ly/20qmXsE>.

From the May 2016 issue, PATACS Posts, www.patacs.org, newslettercolumnist@patacs.org.



iMac (21.5-inch, Late 2013)

General

Software

Memory and Graphics

Connections

History

Notes

OVERVIEW

Introduced

September 2013

Discontinued

October 2015

Model Identifier

iMac14,1 or iMac14,3

Model Number

A1418

EMC

2638

Order Number

ME086LL/A (2.7 GHz), ME087LL/A (2.9 GHz)

Initial Price

\$1,299 (2.7 GHz) \$1,499 (2.9 GHz)

Current Price

Show Current Price

Support Status

Supported

Colors

Silver and Black

Weight and Dimensions

12.5 lbs., 17.7" H x 20.8" W x 6.9" D

PROCESSOR

Processor

Intel Core i5 (4570R, 4570S) or Core i7 (4770S) ("Haswell")

Processor Speed

2.7 or 2.9 GHz (Core i5) or 3.1 GHz (Core i7)

Architecture

64-bit

Number of Cores

4

Cache

4 MB (2.7 GHz) 6 MB (2.9 GHz) 8 MB (3.1 GHz) L3

System Bus

Intel Direct Media Interface (DMI) at 5 GT/s

STORAGE AND MEDIA

Storage

1 TB (5400-rpm SATA), 1 TB Fusion Drive, or 256 or 512 GB flash storage

Media

Optional Apple USB SuperDrive



1925 South Ave.

Corner of South Ave. and East Henrietta Rd.

244-2240

Laptops starting At



\$129⁹⁹

Desktops starting at



\$149⁹⁹

Rochester Computer Society

Members receive 10% off

(must have membership card to redeem)

What we do

Windows, Mac, and Linux

PC Repair

Mac Repair

Virus Removal

Custom System Builds

Data Destruction

Electronics Recycling

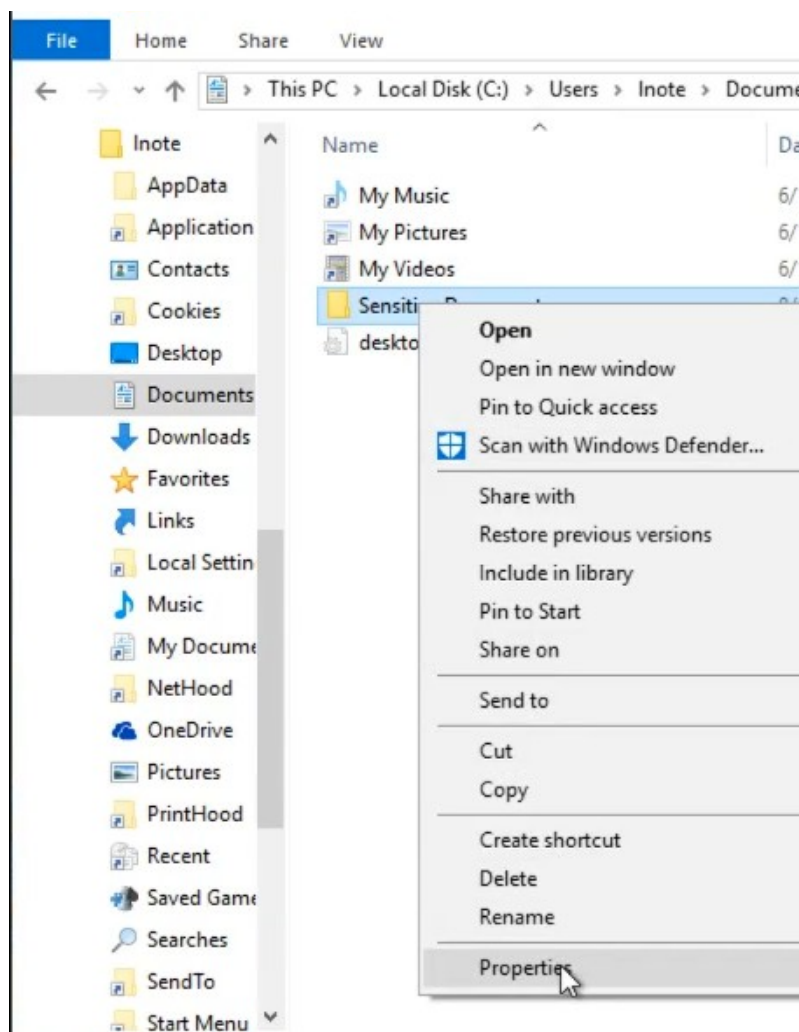
www.podcomputers.com



4

The Rochester Computer Society, Inc

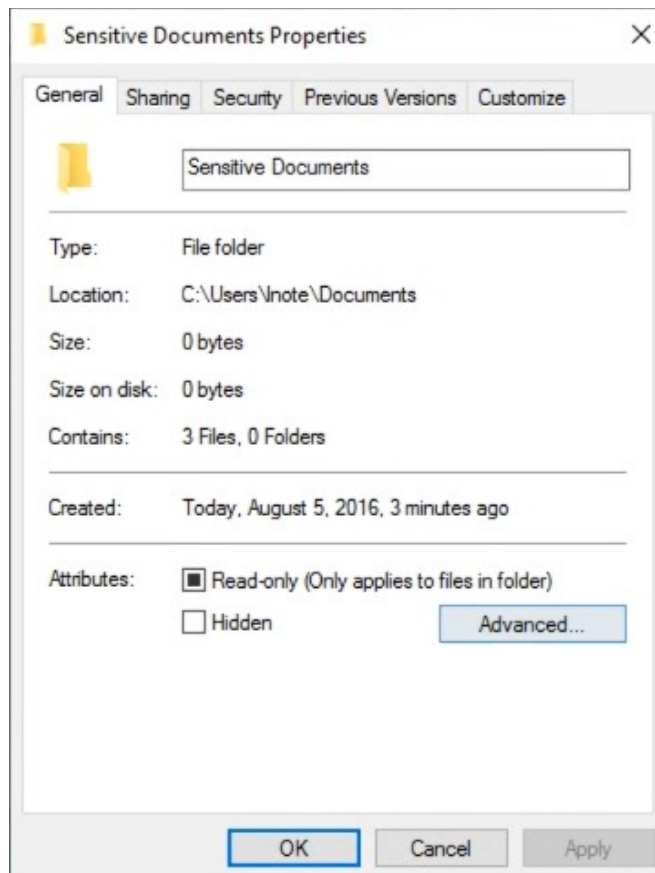
How Do I Encrypt a Folder? It's not uncommon to want to encrypt a folder and all it contains. There are several techniques to encrypt a folder, each with pros and cons. Sometimes encrypting a single file isn't enough. Sometimes you want to encrypt all the files in a folder, and often the sub-folders as well. As you might imagine, there are several different solutions, depending on your particular needs. I'll review some of the alternatives, as well as their pros and cons.



Using Windows to encrypt files and folders

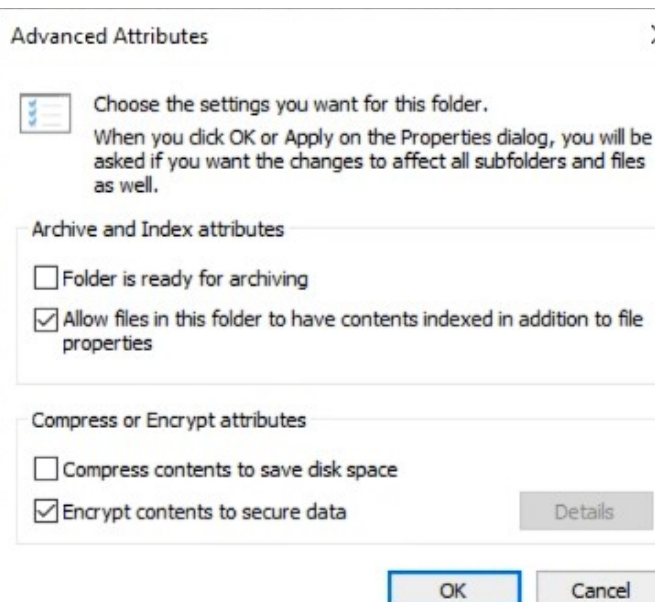
If you're running Windows Professional Edition or better, and your disk is formatted using NTFS (most Windows hard disks are these days), then Windows can encrypt your files and/or folders for you using EFS, or the Encrypting File System. The technique is very simple. Right-click on the file or folder you want to encrypt – my example here is a folder called “Sensitive Documents” – and click on Properties. In the resulting dialog, on the General tab, click on Advanced.

In the resulting “Advanced Attributes” dialog, make sure that “Encrypt contents to secure data” is checked. Click OK. You may be asked whether you want the single item encrypted, or more. In the case of folders, the second option is to encrypt the folder and everything within it. In the case of encrypting a file, the second option is to also encrypt the folder containing the file. The choice is yours, depending on what you're attempting to do. (In general, I find encrypting a folder and everything within it the most straightforward choice.)



The good news: It's simple, easy, and almost completely transparent to encrypt a folder. Your folder, and all the files it contains, are encrypted. As long as you're not logged in, anyone who steals or otherwise gains access to your computer, or even just your hard drive, cannot gain access.

The bad news: Anyone (including malware) who has access to your computer while you're logged in



can access your files, bypassing the encryption. In fact, anyone who can log in by virtue of knowing or cracking your log-in password can, as well; your log-in password is, perhaps, the weakest link. The files are encrypted on your hard drive, and there's no way to share the encrypted files with others.

VeraCrypt

VeraCrypt is a successor to the once very popular TrueCrypt. It has a couple of different approaches to high-quality encryption, one of which we can use to encrypt a folder – or at least something very similar.

You can use VeraCrypt to create an encrypted container secured with a passphrase. This is a single encrypted file kept on your computer's hard drive. You then

“mount” that file using VeraCrypt, supplying the passphrase to decrypt it. Once mounted, the unencrypted contents of that file appear as a separate drive – often called a virtual drive – on your system. Reading data from and writing data to that virtual drive transparently decrypts and encrypts the data stored in the container file. Once the drive is unmounted, the data is once again inaccessible without re-mounting the container and knowing the passphrase.

The specific details are beyond the scope of this article, but as an example, you might create a container C:\Users\loginname\Documents\MySensitiveDocuments, and give it a nice, secure passphrase. When you mount MySensitiveDocuments using VeraCrypt and that passphrase, you can then assign it a drive letter – I’ll use “S:” for this example. Now any program can read and write files and folders to drive “S:”; when doing so, the data is stored inside of the file MySensitiveDocuments in encrypted form. Once you unmount the container, drive S: disappears, and the data is no longer visible in unencrypted form.

Using VeraCrypt to manage an encrypted container in this way is very similar to having an encrypted folder.

The good news: VeraCrypt provides high-quality encryption, and is available on multiple platforms. Containers created by VeraCrypt are not tied to your login, but are secured by a passphrase. The containers can be copied from machine to machine and opened anywhere. Once mounted, encryption and decryption is transparent to any program reading and writing data on the virtual drive.

The bad news: Containers are monolithic, meaning that regardless of how many files they contain, they are still a single container file. The container size is specified when you create it, and cannot be resized. The only way to move encrypted data from one place to another is to copy the entire container.

BoxCryptor

BoxCryptor uses a model similar to VeraCrypt, but is designed to work optimally with online or “cloud” services. Rather than storing everything in a single container, BoxCryptor maintains individually encrypted files.

When you install and configure BoxCryptor, you point it at an empty folder on your machine which will contain your encrypted data, and specify a passphrase to use for encryption. You then mount that folder using BoxCryptor and your chosen passphrase. Much like VeraCrypt, a virtual drive appears. Files and folders transparently written to and read from that virtual drive are encrypted and stored within the folder you originally specified. Once you unmount the folder, only the encrypted copies remain accessible.

The major difference between BoxCryptor and VeraCrypt is that BoxCryptor maintains the encrypted files and folders as individual files and folders rather than using a single, monolithic container. The article BoxCryptor – Secure Your Data in the Cloud goes into the differences in more detail.

The good news: BoxCryptor provides high-quality encryption and is available on multiple platforms. It’s highly suited to storing encrypted data on online storage services. Like VeraCrypt, your data is protected by a passphrase, and is not tied to your login. Once mounted, encryption and decryption is transparent to any program reading and writing data on the virtual drive. There are no size issues, other than the disk space you have available.

The bad news: You cannot easily copy individual files encrypted using BoxCryptor to other machines, though of course the entire encrypted folder is designed to be replicated to other machines and cloud storage providers.

It’s difficult to make a recommendation

Normally, I’d make a recommendation as to what technology might be best suited. Unfortunately, this really is a case where different tools solve the generic problem – how to encrypt a folder – in different ways that involve different trade-offs. You may need to evaluate those trade-offs differently. What I can tell you is what I’ve settled on – and that’s BoxCryptor.

I don’t use operating-system encryption at the file or folder level. (I use whole disk encryption to secure my entire hard drive – more on that coming soon.) I use cloud storage heavily – both my own and that of popular services. BoxCryptor ensures that anything I consider even somewhat sensitive is stored securely encrypted, as it’s automatically replicated not only to online storage, but across my various computers as well.

The Mozilla Firefox web browser (or simply known as Firefox) is a free and open source web browser which is enhanced by the availability of numerous add-ons for it, including some that are designed to protect your privacy and security when you browse the web. Firefox is available for GNU/Linux, Apple Mac OS X, Microsoft Windows and other operating systems. ***Since the security addons recommended here are browser based, they may also be used for Windows and OS X, as well.*** Websites are the most common source of malware infection, so accessing them securely is vital. We recommend that you use Mozilla Firefox and install the add-ons covered in this guide. If you would prefer to use a browser other than Mozilla Firefox, the alternatives below are also available for GNU/Linux, Apple Mac OS X and Microsoft Windows:

Tor Browser

Google Chrome

Google Chromium (Chromium is the open source version of Chrome).

Firefox has many easy-to-use add-ons that improve your privacy and security when you browse the Web. You can choose which add-ons to install, and decide how to configure them, depending on your circumstances. If you are using a computer that is managed by someone else (at an Internet cafe, for example, or in your place of work), you might have to make these adjustments repeatedly. This guide covers the installation and basic configuration of the following add-ons; HTTPS Everywhere, Privacy Badger, NoScript, and Click&Clean.

The overwhelming majority of malware and spyware infections originate from webpages. It is important that you keep your browser up to date and always consider whether it is safe to visit unknown websites, particularly those that are sent to you by email. Before you decide to open a questionable webpage, you might try scanning the web address using the following page scanners; www.virustotal.com, www.onlinelinkscan.com, or www.phishtank.com. You can also check the reputation of a website by using scanners, such as; <http://safeweb.norton.com>, www.urlvoid.com. Last month, 'Web of Trust' was reviewed and may be added to Firefox.

Many Linux distributions come with Firefox installed by default, and most have a package management system or software center that makes it easy to install and update Firefox (along with any additional software that it requires to operate). Many Linux distributions include a trademark-free version of Firefox called Iceweasel, which is just the same tool with a different name. It is extremely important that you keep your Web browser up-to-date.

You can configure Firefox to use a search engine of your choice. To do so, follow the steps below:

Step 1: Select Edit > Preferences in your Firefox menu bar.

Step 2: Click Search in the side bar of the Preferences screen.

You can now choose your default search engine and decide which other search engines should be accessible through the Firefox search box. **We recommend DuckDuckGo as a default search engine** because it does not track or profile its users, or share its users' personal information with third parties. Other privacy-focused search engines that you can choose to add as search engine options to choose in the Firefox toolbar's search bar include; StartPage, Ixquick, and Disconnect.

HTTPS Everywhere, is an add-on that helps Firefox connect securely to websites that support encryption. When you access a page using a Web address that begins with "http://" (such as <http://www.amazon.com>), your connection is unencrypted. The information you send to and receive from that website can be seen by anyone with the ability to monitor your Internet traffic. This includes your (ISP-Internet Service Provider), and many surveillance platforms. When you access a page using a Web address that begins with "https://" (such as <https://www.amazon.com>), your connection will be encrypted, and third parties will find it much more difficult to intercept the data you send and receive. Unfortunately, even websites that do support https often fail to redirect visitors to the correct Web address. This is the problem that HTTPS Everywhere was designed to solve.

HTTPS Everywhere maintains a list of websites that support https and automatically requests an encrypted connection for those websites—even if you click on a link (or enter an address into your browser) that begins with http. To install HTTPS Everywhere, follow the steps below:

Step 1: Select Tools > Add-ons in your Firefox browser menu bar.

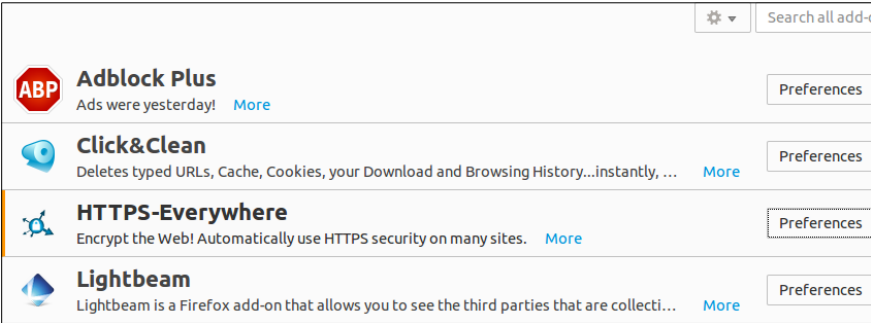
Step 2: In the "Get Add-ons" section, type *HTTPS Everywhere* in the search bar and press enter. You should now have a list of all available add-ons in front of you, including HTTPS Everywhere.

Step 3: Click [Install], next to HTTPS Everywhere, to download and install the add-on.

Step 4: Restart your Firefox browser to install

HTTPS Everywhere.

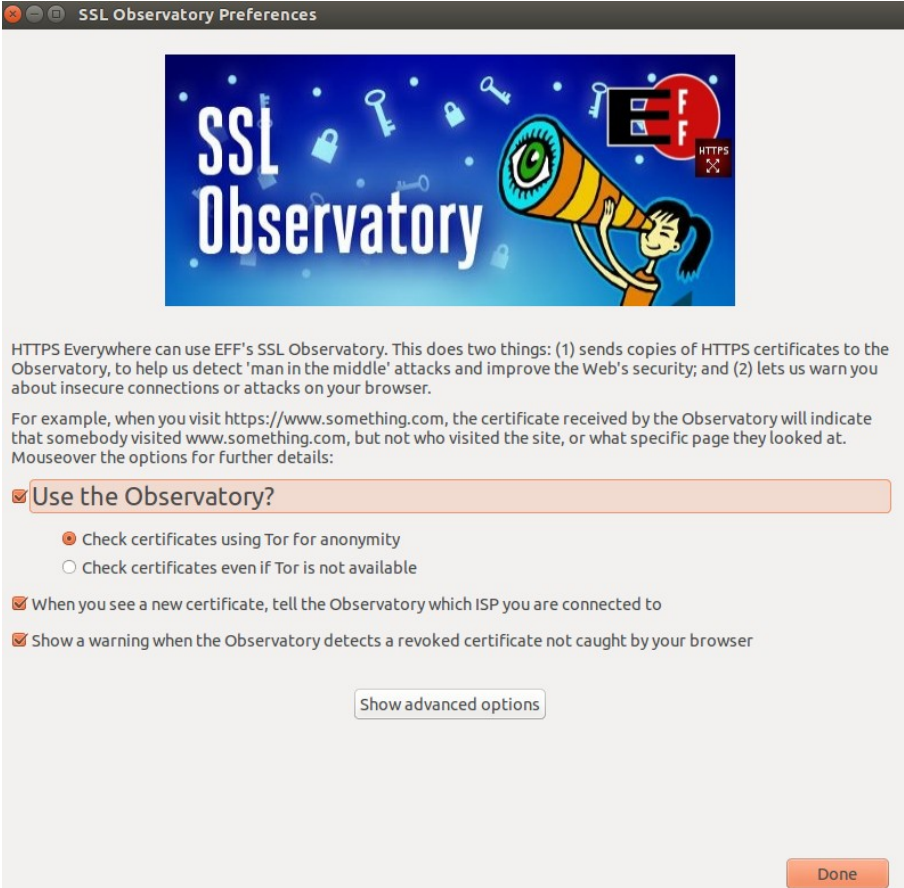
Step 5: Verify that HTTPS Everywhere was installed successfully by selecting Tools > Add-ons > Extensions in the Firefox menu bar. HTTPS Everywhere should be displayed, along with your other add-ons.



HTTPS Everywhere is now installed. When you connect to a website that is included in the list maintained by the add-on, and that supports https, your connection will be encrypted automatically.

Note: When HTTPS Everywhere is working, you should still see "https://" in your browser's address bar. If you do not, then your connection is unencrypted.

If you click on “Preferences” next to HTTPS-Everywhere, the following window should appear:



Here you can choose whether you want to use the EFF's SSL Observatory, which warns you about insecure connections or attacks to your browser. We strongly recommend that you use this SSL Observatory for better browser security.

Privacy Badger is a browser add-on that prevents third-party companies from tracking your online activities. It is available for Firefox, the Tor Browser, Chrome, and Chromium.

To install Privacy Badger, follow the steps below:

Step 1: Select Tools > Add-ons in your Firefox

Step 2: In the “Get Add-ons” section, type enter. You should now have a list of all including Privacy Badger.

Step 3: Click [Install], next to Privacy Badger, When the add-on is installed, Firefox



browser menu bar.

Privacy Badger in the search bar and press available add-ons in front of you,

to download and install the add-on. will display Privacy Badger's "Thank you" page.

Step 4: Verify that Privacy Badger was

installed successfully by selecting **Tools > Add-ons > Extensions** in the Firefox menu bar. **Privacy Badger** should be displayed, along with your other add-ons.

The **Privacy Badger** add-on is now installed and can help prevent third party tracking of your online activities. You can click **[Preferences]** to change **Privacy Badger's** settings (though the default values are fine).

Click&Clean is a browser extension that helps you clear your browsing history with just one click. Without privacy enhancing features, a browser can collect different types of information that it stores on the hard disk of your computer. Such data can include your location, browsing history, search history, cookies, cache, active logins and site preferences. This local storage can be deleted by manually cleaning your browser history with a tool like **Click&Clean**.



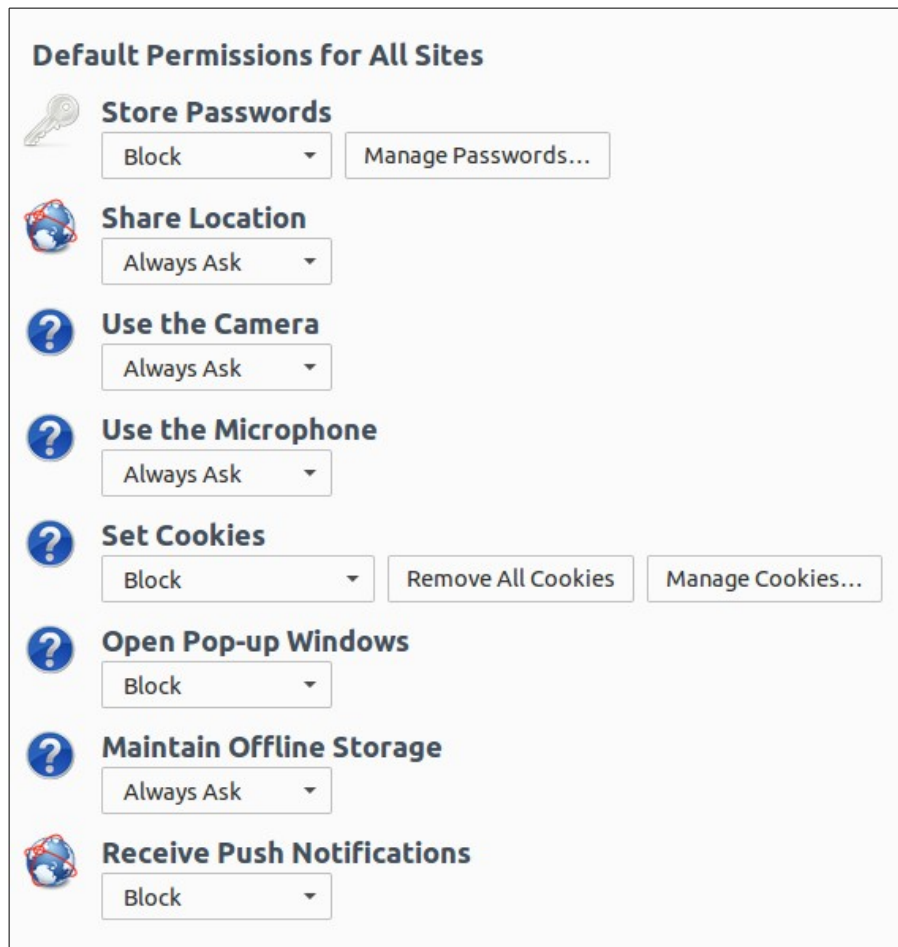
You can install **Click&Clean** through the following steps:
Step 1: Select **Tools > Add-ons** in your Firefox browser menu bar.
Step 2: In the “Get Add-ons” section, type *Click&Clean* in the search bar and press enter. You should now have a list of all available add-ons in front of you, including **Click&Clean**.

Step 3: Click **[Install]**, next to **Click&Clean**, to download the add-on

Step 4: Restart your Firefox browser to finish installing **Click&Clean**.

Step 5: Verify that **Click&Clean** was installed successfully by selecting **Tools > Add-ons > Extensions** in the Firefox menu bar. **Click&Clean** should be displayed, along with your other add-ons.

Alternatively, just look at your browser – the **Click&Clean** icon should be there now. If you click on the arrow next to it, you will notice that it offers a variety of features like incognito browsing, privacy testing, cookies, permissions and preferences. The privacy test feature gives you the ability to see what services are running on your browser that you might have forgotten about. The cookies feature shows you what cookies are currently stored on your computer. By



using the permissions feature you can change your browser's default settings to enhance your privacy. These settings/permissions include blocking or asking for permission every time the browser wants to store your passwords, share your location and use your camera and microphone. Examples of how you can set your browser's permissions are shown above. In the preference section you can also choose if you want to automate the cleaning of your browser data. You can also clear your browsing history every time you close your browser, so that you do not need to think about your browsing history again.
Note: As an alternative, you can use an external application like **BleachBit** for this purpose.

No Script

When you visit a website, your browser automatically downloads content from that site. In addition to text and images, this content often includes scripts, which are essentially small programs that run inside your browser. **NoScript** is a Firefox add-on that prevents your browser



from running such programs without your permission.

The vast majority of these scripts are harmless and serve only to make webpages more interactive. Some of them are malicious, however, and some of them are third-party trackers capable of building a profile of your online activities. Unfortunately, **No Script** cannot automatically identify which scripts are safe and which are harmful. So, when you first tell it to **Block Scripts Globally**, it will prevent many websites from displaying properly. Once you start whitelisting scripts from different locations,

however, things will begin returning to normal, and you will still be protected from potentially dangerous Web content. To install NoScript, follow the steps below:

Step 1: Select Tools > Add-ons in your Firefox browser menu bar.

Step 2: In the “Get Add-ons” section, type *NoScript* in the search bar and press enter. You should now have a list of all available add-ons in front of you, including NoScript.

Step 3: Click [Install], next to NoScript, to download and install the add-on.

Step 4: Restart Firefox to install NoScript.

Step 5: Verify that NoScript was installed successfully by selecting Tools > Add-ons > Extensions in the Firefox menu bar. NoScript should be displayed, along with your other add-ons.

Your browser now supports NoScript and blocks malicious code from running on your computer. Although NoScript might seem a little frustrating at first (as the websites you have always visited may not display properly), you will immediately profit from the automated object-blocking feature. This will restrict pesky advertisements, pop-up messages and malicious code built (or hacked) into web pages.

NoScript will run silently in the background until it detects the presence of JavaScript, Adobe Flash or other script-like content. At that point NoScript will block this content and the status bar will appear on the bottom of the Firefox window. The NoScript status bar displays information about which objects (for example, advertisements and pop-up messages) and scripts are currently prevented from executing themselves on your system. But since NoScript does not differentiate between malicious and real code, certain key features and functions (for instance, a tool bar) may be missing.

Some web pages present content, including script-like content, from more than one website. For example, a website like www.twitter.com has two sources of scripts (twitter.com and twimg.com). To unblock scripts in these circumstances, start by selecting the Temporarily Allow [website name] option (in this instance, Temporarily allow twitter.com). However, if this does not allow you to view the page, you may determine, through a process of trial and error, the minimum number of websites required to view your chosen content. For instance, on Twitter, you need to select the Temporarily allow twitter.com and Temporarily allow twimg.com options, in order for Twitter to work. For websites that you trust and frequently visit, select the Allow [website name] option. Selecting this option permits NoScript to permanently list that website as trusted.

Note: A vulnerability in NoScript was recently identified. We continue to recommend NoScript because this vulnerability does not present a threat unless you also install a separate (intentionally malicious) add-on. We strongly recommend researching add-ons before you install them and removing any add-ons that you do not need or about which you are uncertain.

This guide was paraphrased and reprinted under the creative commons license granted by the 'securityinabox.org' website.

Communications - Voice and Digital - All in one package

By Phil Sorrentino, Contributing Writer, philsorr@yahoo.com
The Computer Club, Florida

Sound familiar? Well, it should; it describes a Smartphone. A smartphone provides voice (analog... sort of) and digital (computer to computer) communications, all in a package you can stick in your pocket and carry around. Communications, as you would find in Wikipedia, may be defined as “the purposeful activity of information exchange between two or more participants in order to convey or receive the intended meaning through a shared system of signs and semiotic rules.” (Yes, I had to look up semiotic, too.) Basically, it is the means of getting information (knowledge of something) to or from some other person or place. Communications is very different from Transportation. Nothing physical ever gets moved from place to place, only “information” or the knowledge of something, is moved.

In voice communications, sound is the information that is conveyed. In digital communications, digital data is the information conveyed. For both types of communications, you need a transmitter at one end of a communications path, and a receiver at the other end. In voice, usually a person’s mouth is the transmitter, and at the other end there is usually another person’s ear (pretty straight forward for us here in the 21st century). In digital communications, the transmitter and the receiver are digital computing machines, a.k.a. computers. We are all familiar with mouths and ears, because they have been around for a long time. But, digital computers are relatively new, and have only been around for 60 or so years, and they have only been small enough to be carried around by a person, and powerful enough to do the job, in the last 5 or 10 years (the iPhone was introduced in 2007).

So, the smartphone in your pocket is really quite a powerful communications device. We use its voice

communications capability to contact other people as we would use any other telephone. (Remember crank phones, pay phones, and flip phones?) And we use its data communications capability to contact any other computer in the world on the internet (a server computer; that is). The voice capability does not seem too astounding since we've had telephones since the early 1900s. It is the data communications capability that really makes this device so useful, and powerful. (As it turns out, the voice communications, although we think of it as analog, is really just another form of digital communications. In a modern phone, the voice is immediately converted to a digital stream of data and it is that data that is communicated to the receiving device where it is converted back to analog voice right before it goes to the receiver's ear.)

Of course, there is also an elaborate communications infrastructure in place that lets the smartphone do its magic. The most important part of this infrastructure is the "cellular phone network", or the collection of cell phone towers that have sprung up all over the country over the last 30 or 40 years. These networks allow phones to be mobile; that is, they do not have to be located at fixed locations, like the older "landline" phones. They also allow phones to be tracked so you can carry on communications while you are driving down a high speed interstate highway. The cell phone network is eventually connected to the internet giving the users of that network access to the internet. (Just as an aside, there are four major cell networks in the US, Verizon, AT&T, Sprint, and T-Mobile.) Another more recent part of the infrastructure is the wide-spread adoption of the Wi-Fi local area network. This part of the infrastructure provides access to the internet by any mobile device within the Wi-Fi's useable radius of maybe a few hundreds of feet. Wi-Fi is implemented using a Wi-Fi router, connected to a modem, which in turn connects to an Internet Service Provider, like Verizon, Comcast, or Brighthouse. These networks have become ubiquitous and are available in homes, shopping centers, libraries, airports, and many restaurants.

So, the users of mobile devices have access to the internet by either a cell phone network, or Wi-Fi local area networks. The cost for using the cell phone network is usually covered by a plan which includes phone call minutes, texts, and data. The cost for using the Wi-Fi network is nothing beyond the monthly cost of having the service provided. Once a plan is in place with a network provider and a Wi-Fi is setup, a mobile device has access to the internet, via either of these methods, using the Apps on the device. And, it is the collection of Apps on the device that really harnesses the power of the smartphone, allowing it to take advantage of the elaborate infrastructure. Data communications on the internet usually employs a Client-Server approach. Apps on the mobile device are considered "clients" and they communicate with "server computers" on the internet. These servers are setup to do certain things; for instance, a bank server might provide information about your bank accounts. Once the bank App on the device is selected, the App may only need the appropriate "User Name", and "Password" to provide results. Because the App is for a specific bank, the App knows what server to contact (the internet URL), how to go about contacting that specific server (TCP/IP), how to interpret the data received from that server, and how to reveal the bank account balances on the display to the App user.

There are many Apps on a Smartphone that provide communications with either other phones or computers. A "phone" App allows the user to make and receive phone calls. Messaging Apps usually provide the ability to send emails to email addresses, or send texts to phone numbers. Some messaging Apps allow the inclusion of pictures, video, and audio attachments. Another App lets the user send a picture and determine how long the picture will be able to be viewed before it is removed from the server and the receiving device. So, Apps help the Smartphone provide Voice and Data Communications; most of these Apps have arrived in just the last few years. Can you imagine what the future has in store?

Taken from <http://sccccomputerclub.org> / Philsorr.wordpress.com.

* * * SOFTWARE & COMPUTER TIPS * * *

How to Get the Windows 10 Anniversary Update

By Sandy Berger, Compu-KISS

On August 2, Microsoft released a pretty big overhaul of Windows 10 which they call the Windows 10 Anniversary Edition. It's a big update, but you don't have to fret. Windows 10 will still look and act pretty much the same as it did before the upgrade, this new version will bring minor tweaks to the operating system and several features upgrades. Here's what you need to know.

The Anniversary Update, like all Windows 10 upgrades and updates is free. Microsoft is delivering this update to more than 350 million devices around the world, so it is being rolled out slowly, which means it won't immediately be available to all users.

As I write this, a week after the launch, Microsoft seems to be a bit slow. Many are

still be waiting for the upgrade to appear on their computer. If you have gotten the upgrade, you will probably know it because you will have answered installation prompts. If you aren't sure, you can Press Windows key + R then type: winver, then hit Enter on your keyboard. Look at the OS version number. If it reads "1607," you have the Anniversary Update installed. If you want to be able to tell by your screen, just press the Windows key on your keyboard or click on the Windows icon at the bottom left of the screen. The old version Start Screen that pops up will have your name at the top of the window and will say "All Apps" at the bottom. The new version will have three bold lines at the top of the window and at the bottom you see an alphabetized list of apps and programs instead of the "All Apps" selection

Want to hurry your installation. Go to the Settings, then choose Update & Security, the Update. You can then click on Check for Updates. If that doesn't show any new updates, just click on Learn More and you will be presented with a page where you can download and install the Anniversary Update.

Hope you enjoy it! Taken from www.compukiss.com, sandy@compukiss.com.

Interesting Internet Finds - June, 2016

Steve Costello, Boca Raton Computer Society
editor@brcs.org, <http://ctublog.sefcug.com>

In the course of going through the more than 300 RSS feeds, I often run across things that I think might be of interest to other user group members. The following are some items I found interesting during the month of June 2016.

Android Tip: A Faster Way to Launch the Android Camera App

<http://heresthethingblog.com/2016/06/01/android-tip-faster-launch-camera/>

Quick camera access for Android Marshmallow devices.

How to Set Up and Use Open365, an Open Source Alternative to Office 365

<http://www.howtogeek.com/256450/how-to-set-up-and-use-open365-an-open-source-alternative-to-office-365/>

If you are using LibreOffice, and would like to try out the Open365 (beta at this time) alternative to Office 365, this post from *HowToGeek* is a must read.

5 Common VPN Myths and Why You Shouldn't Believe Them

<http://www.makeuseof.com/tag/5-common-vpn-myths-shouldnt-believe/>

If you don't use a VPN (Virtual Private Network), and you should, check out this *MakeUseOf* post. Your reason is probably one of these myths.

Ten Tips for Donating a Computer

<http://www.techsoup.org/support/articles-and-how-tos/ten-tips-for-donating-a-computer/>

Upgrading to a new computer? Have an unused working computer just laying around? Well check out this post for how to donate your old computer so someone in need will be able to have one.

5 Things You Need To Know About Password Managers

<http://www.pcworld.com/article/3085395/security/5-things-you-should-know-about-password-managers.html>

I know there are a lot of you that don't think you need a password manager. If you are one of them, read this post to learn some reasons why you should.

Seven Tips on Keeping Your Phone Safe While Traveling

<http://www.cnet.com/news/seven-tips-on-keeping-your-phone-safe-while-traveling/>

This is the time of year for vacation travel, so check out this post to refresh yourself on how to keep your phone safe while you are out there.

Most Fridays, more interesting finds will be posted on the *Computers, Technology, and User Groups Blog*:

<http://ctublog.sefcug.com/tag/interesting-internet-finds/>

The posts are under Creative Commons licensing.

Update your iPhone right now — especially if you're an activist

reported by Jason on August 26, 2016

excerpts taken from <https://safeandsavvy.f-secure.com> website

A little iPhone history was made this month — an iOS device was infected by just clicking on a link. This sort of attack had previously only worked on devices where the owner had purposely installed a “jailbreak” hack. Here’s how this historic attack happened, according to The Verge:

Earlier this month, an Emirati human rights activist named Ahmed Mansoor got a suspicious text. It promised new details of torture in the country’s state prisons, along with a link to follow if he was interested. If Mansoor had followed the link, it would have jailbroken his phone on the spot and implanted it with malware, capable of logging encrypted messages, activating the microphone and secretly tracking its movements.

The attack is detailed in a new report from Citizen Lab and Lookout Security.

To our cyber security advisor Erka Koivunen, this is a glaring example of a threat that is not “advanced” — as in APT, advanced persistent threat. Here, the most exploitable iPhone vulnerability ever known has now been exposed and patched — for what? You just don’t see zero-day vulnerabilities like this — especially on what had been one of the more secure platforms available — that often.

So, if you haven’t already, update now. And if you’re involved in politics in *any way* whatsoever, realize that someone will try to hack you — sooner or later. So beware of those links in strange texts and email attachments in general.

September's presentation of 'Mobile Device Security', was presented by Jerry Seward. His suggestions are true for home use or when traveling, locally (wi-fi hotspots) or out of town. Following, are his nine suggestions to help maintain a secure environment, while using any mobile device, such as a smart phone or tablet.

1. **Make sure your software is up to date**
2. **Employ strong passwords** (Jerry uses LastPass, <https://lastpass.com/>)
3. **Don't mess with the security settings** (unless you are quite technical and will be responsible for any tweaks or changes)
4. **Avoid unencrypted public wireless networks**
5. **Paying to access a wi-fi network, doesn't mean it's secure**
6. **URLs beginning with 'https:' are safer (but not foolproof)**
7. **Use a VPN (Virtual Private Network, like Hotspot Shield)**
8. **Turn off cookies and autofill**
9. **Watch your apps** (keep up to date and delete if no longer using)

Additional software suggested by Jerry, Hotspot Shield and Lookout. **Hotspot is an extension** available for the Chrome and Firefox browsers. Unblock any blocked website or content and stay secure and private with Hotspot Shield VPN. Easy-to-use interface and one-click activation. Unlimited bandwidth and completely free.

Lookout Security and Antivirus (<https://www.lookout.com/>), is available through Google Play or App Store. Use Lookout to protect your smart phone and tablet from mobile threats that can steal your data, listen in on your conversations, or take control over your phone. It can backup and restore your data. Sometimes, you also need to find your phone, if it's lost. Lookout does that too.

For those of you that would like a copy of the newsletter in booklet form, here is a link to my 'cloud storage'.

<http://tinyurl.com/tonydel-rcsi-newsletters/>.

RCSI Officers

Pres: Steve Staub 429-9877

srstaub1@rochester.rr.com

VP: Mark S. Lawson . . . 544-5377

mslawson51@peoplepc.com

Treas: Dennis P. McMahon

denmac733@gmail.com

. 235-1260

Secretary: www.rcsi.org

Board Members at Large

Sally Springett 442-3776

sspringe@rochester.rr.com

term ends 9/20

Jan Rothfuss 347-6020

jan_rothfuss@hotmail.com, 9/19

Tony Dellelo 734-6149

tonydel@techie.com, 9/18

Bob Avery 385-4491

webmaster@rcsi.org, 9/17

Standing Committees

Webmaster: Bob Avery

Programs: Tony Dellelo

Membership: Steve Staub

Monitor editors: . . Sally Springett
Tony Dellelo

Linux SIG: . . . Carl Schmidtman

unixgeek@faultline.com

Planning Meeting

Held on 1st Tuesday of each month
at 7 pm, at either Sally
Springett's or St. John's Meadows.

Newsletter Printing

The Sept newsletter was printed
at St John's/Chestnut Court by
Chuck Wells, Don Nichols and
Steve Staub, with the help of Don
Wilder (computer and printer
operator). We will try and print on
the 1st or 2nd Thursday morning,
following the monthly meeting.

APCUG 2016 INTERNATIONAL TECHNOLOGY CONFERENCE

October 21, 22 & 23, 2016, Palace Station Hotel & Casino, Las Vegas

BE EDUCATED, ENTHUSED AND ENTERTAINED!

Join us for our 2016 Tech Conference and learn about the ever-changing world of technology. Whether you are using a Windows-based or Linux computer, a Chromebook, Android or Apple device, this is the conference for you. For additional info, <http://apcug2.org/apcug-2016-conference/>

Articles by RCSI members

may be reprinted by other

user groups, without special

permission, provided they are

unaltered and the publication

sends a copy to RCSI (2 Bambi

Lane, Rochester, NY 14624) or

emails a copy to the author.

Articles by authors from other

organizations retain their original

copyright. Articles provided by

the Association of Personal

Computer Users Groups (APCUG)

may be reprinted if credits remain
intact.

Computer Recycling

Some Residential Drop off

Locations: **Call first**, to find out

what is accepted, especially for

'tube type' tvs or monitors.

Deeley IT

---(Pittsford), 585-381-3100

Tech Source

---(Rochester), (585) 789-1785

Stereo Shop

----(Webster), 585-787-7467

Certified Document

Destruction & Recycling,

accepts electronic waste, but

charges 40 cents/pound for crt

type monitors. Located in

Rochester at 1133 Emerson St,

482-9400, www.cdd-r.com

TSC Computer & Electronics

Repair, accepts most electronic

waste, including printers. Does

not accept crt type monitors or

tvs. They are located at 765

Elmgrove Road, Gates. 429-6880,

www.tscelectronics.com