CENTRAL FLORIDA Computer Society

USERS HELPING USERS

Your technology helper for almost 40 years.

THE BUSSLINE

(BUSSLINE is the term for the complex multi-functional circuitry on a computer motherboard, a PC's heart.)

Vol. 115 No. 8 Newsletter of the Central Florida Computer Society, Inc. [Non-Profit, 501(c)3] Nov. 2015

CFCS Computer Giveaway

FREE COMPUTERS

WITH SOFTWARE TO MEET NEEDS

The Central Florida Computer Society is establishing a computer donation program!

New computers will be donated to organizations or individuals where a charitable need is established. Sufficient software to meet the established need will be included.

Computers will be delivered and set up free of charge.

A limited number of computers will be available.

All decisions as to number of computers, necessary software and charitable need shall be the responsibility of the CFCS Board of Directors.

All decisions are final!

For info email president@cfcs.org

Our next CFCS meeting

is on Sunday, November 8:

The Main Meeting is at 2:00, Nov. 8: Geeks on Tour will present a program from their reservoir of computer knowledge. Geeks on Tour is well known for their weekly educational broadcast about smartphones and tablets, which takes place at **2pm Eastern time** on any Sunday, or check them out at geeksontour.org

Here is what our president, Jack Pearson, had to say in a recent email about the Geeks:

“Meet Jim and Chris Guld, the *Geeks on Tour*. They are Geeks who will teach about really using your smart mobile technology. They call themselves "Geeks" but they have the ability to explain even complex technology in very plain, easy to understand language. You will learn how they use Smart Phones and Tablets and the many things they can do to enhance your life. The meeting is not system specific. Demonstrations use both Android and Apple devices. They are going to discuss how to get the most usage from your smart mobile devices, including both phones and tablets, and they will differentiate between the capabilities of iOS operating system-based devices (Apple) and Android. Their presentation will include the user interfaces, supported apps, internet usage, camera capability and mobile payment systems,

The Inside Stories:

among other things. They will also discuss technological advances for these products which are on the horizon. At the conclusion, the speakers will be available to answer your questions.

If you would like to actually see the *Geeks on Tour* (Chris and Jim Guld) . Come to CFCS Nov 8th, 2015 Meeting at Seminole Library , 215 Oxford Rd, Cassellberry, FLA

1. Seminole Library opens at 1 pm

2. We will not have the "Windows Sig" on Nov 8th

3. You are welcome to arrive at Meeting anytime after 1 pm, the "Geeks on Tour" will be setting up.

4. At about 1:15-1:30 pm -We will start our business before the "Geeks on Tour" broadcast (I will be asking members to sign up at this meeting to be on slate of officers for 2016.) We need a lot of candidates for 2016 Elections, so please plan to Be an Officer in 2016

Elections of new 2016 Officers will be held at the Sunday Jan 10 General Meeting

5. Main Meeting will start at about 2 pm. The "Geeks on Tour" will do their live Nationwide WiFi broadcast from our Meeting.

6. PLEASE PLAN TO ATTEND THE GENERAL METING ON SUNDAY NOV 8th AT SEMINOLE LIBRARY LIVE.

Thank you for your co-operation on the above matter
See you There

JACK PEARSON - PRESIDENT CFCS

NEXT MONTHS' MEETINGS

Dec. 14: **Glen Coffield of Smart Guys Computers** will make his annual Holiday visit to our elves society and present us with his always potent viewpoint on all things happening in our favorite place, the world of tech. Since it is Christmas Time, he may even surprise us with a few gifts, but only if each member who has a pot belly and white hair dresses up like Satna Claus! LOL

Jan. 10: **Staples Tech Adviser & Mgr.** Everyone was so impressed with the talk given several months ago from the two Staples Wizards, that we have asked them back again, pending their corporate approval. Stay tuned.

Earlier on the same day of each presentation, the WINDOWS Special Interest Group (SIG) meeting is held. The **WinSIG** now meets at 1:15 pm, and is hosted by Hewie Poplock, former president of both CFCS and FACUG, and author of Hewie's Views and Reviews. Hewie, who has led the Central Florida Computer Society WinSIG for over 15 years, will start a little more than an hour before the CFCS General Meeting.

If you use or plan to use Windows, these discussions, demonstrations, and Q&A sessions will be of immense value to you. Geared to intermediate level Windows users, tips, tricks, and information on all versions of Windows are discussed. An e-newsletter is sent periodically with meeting information and links discussed at the meeting. You need not attend both meetings, but many members do. Non members are always welcome. Sign up for the free e-newsletter at cfcs.org .

Important Note: The WinSIG is now conducted via the Internet, with the usual useful info from Hewie. So either attend the meeting with your fellow club members, or join Hewie online:

Meeting Name: WinSIG08Nov
Invited By: Hewie Poplock

To join the meeting:
https://cfcs.adobeconnect.com/winsig08Nov/

This month's Windows SIG Meeting scheduled topics will be available later in the week on Hewie.net/winsig

If you have never attended an Adobe Connect meeting before:
Test your connection: https://cfcs.adobeconnect.com/common/help/en/support/meeting_test.htm

Get a quick overview: http://www.adobe.com/go/connectpro_overview

Adobe, the Adobe logo and Adobe Connect are either trademarks or registered trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Hewie's Blog and many useful articles (including the meeting notes) can be found at http://hewie.net/

While you are checking out blogs, don't forget Mike Ungerman's excellent one at:

http://musings-from-mike.blogspot.com/

The CFCS website is at http://www.cfcs.org . Be sure to check it out for up-to-date information.

Bring your questions about Windows or any computer questions to be fielded by a room full of computer enthusiasts. The questions will be answered during the Windows SIG or during the "Askit Baskit" portion of the main meeting. We even have a few lurking Mac owners, and when we turn off the lights to better view the presentations, you may notice the glow of numerous iPods in the crowd. CFCS was the first to put the 'YOU' in USER-friendly!

OUR OTHER SPECIAL INTEREST GROUPS (SIG)

The TECH DISCUSSION SIG meets on the fourth Tuesday of each month from 7 to 9 pm at Dennys on 436 and Oxford Rd. SIG leader is Vice President Stan Wallner.

This SIG is a non-structured, open conversational group for CFCS members, that has no specific topic or speaker, but is simply a round table discussion. It is not an advanced group, but a place for people to come and discuss various tech subjects, such as new products and technologies, hardware, software, web-related, etc.

Bring in articles from magazines, newsletters, unusual problems/situations that have arisen, questions, etc. Also, new or ailing devices or notebook pc's are welcome, either for "show and tell" or discussion or demo of situations.
A screen and projector are available, but not always there. If you want it to demo something, please E-mail: tech-sig@cfcs.org a day or 2 ahead.

Another feature of this SIG is the Tech-SIG Yahoo Group mail. We now have 64 people communicating through this, with tips and tricks, "Ask-It Basket" type questions, etc. Also, a second, on-line VIRTUAL meeting of the TechSIG is being experimented with on the second Tuesday of each month. Co-hosted by Mike Ungerman and Stan Wallner, it may attract a long distance audience. Stay tuned to the e-Blast for times and details - it is not yet permanently scheduled, but will be announced in the e-BLAST and on theTech-SIG Yahoo Group mail. If you are not on that list and want to be, please E-mail: tech-sig@cfcs.org

The iSIG meets on the third Monday of each month at 7:00 PM at Florida United Safety Council, 1505 East Colonial Drive, Orlando FL 32803. This building is located across from the Publix on Colonial Drive in the Colonialtown section of downtown Orlando. They have secured WiFi, and vending machines are available. The iSIG meetings cover the products that use the iOS, which includes the iPhone, iPad, and iPod Touch. This is a combined effort of the Central Florida Computer Society http:// www.cfcs.org and the Florida Macintosh Users Group http:// www.flmug.com. Other groups are invited to participate. Attendees are consumers, developers, consultants, and publishers, who find common interests and discuss how to handle topics from both the consumer & the developer perspectives. The SIG leader is Sean Kane, Certified Apple Technical Coordinator, long-time Mac and iOS user, and a technologist and consultant to The Walt Disney Company.

Android SIG
The new Android SIG is held at the Dennys on 436 in Casselberry, on the second Tuesday of each month, at 7 pm. Each attendee is asked to prepare a five minute spiel about an Android discovery they have made. Suggestions include favorite apps, how-to-use residents apps, tricks and tips, etc.

FUTURE SUNDAY MEETING SPEAKERS

Your hard working Board of Directors has not obtained a speaker for February, so please return the email Jack Pearson sent out to Tech-SIG asking for speaker suggestions.

The board needs to appoint a program chairperson, but so far no one has volunteered to take the position. Perhaps YOU could volunteer for the job. The duties would be to contact potential speakers proposed by any members, and remind said speaker several times before the meeting, so they can prepare and be there at the right time and date.

Even if you are not able to serve as Chairperson, every member is encouraged and empowered to suggest a speaker, and to ask anyone you happen to meet, to become one. If they seem interested, get their business card or contact info and email such to your CFCS president, who is the de facto acting Program Chairperson until we get an official one.

CFCS $25 Dollar Giveaway

There will be a $25 Giveaway drawing at the next General Meeting. All paid-up members will be eligible to take part. Pay your dues this Sunday, if you haven't already done so. Dues are $25 a year.

EACH MEMBER MAY WIN THIS GIVE AWAY ONCE DURING YEAR

Jack Pearson

ERECTION NOTICE

CFCS Elections will be held in January. See cfcs.org for slate. Notice that we have used the new politically correct spelling, since that is the way it is pronounced in the Middle East (where they don’t actually have elections).

Slate of Officers for Jan 10th Election

President – Arvin Meyer

Vice President – Stan Wallner

Treasurer - Betty Ann Ogus

Secretary - we need you to volunteer

Director – Forrest Cheek

Be a smart guy.
You could pay your yearly dues to CFCS simply by making computer related purchases at Smart Guys or Refresh Computers. Buy a laptop, or less, get free dues with the money you save

MEMBERSHIP RENEWAL

Membership renewal invoices will be e-mailed from ***treasurer@cfcs.org*** approximately thirty (30) days prior to your membership expiration. Invoices will be snail mailed to members for whom there is no e-mail address in the membership database and to those members whose e-mail was returned to ***treasurer@cfcs.org*** for any reason. Please help us by adding this address to your contacts list and setting your spam filter to let our message get to your inbox. We do not share your e-mail address with others (We hate that too!), but it is necessary for full participation in the Society, including receiving your newsletter.

Members will be requested to renew their membership by paying dues on time. Dues may be paid by cash or check at the meeting, by PayPal at ***http://www.cfcs.org/membership/membership.php*** or by mailing a check to:

CFCS
Address: PO Box 520084,
Longwood, FL 32752

If you do not receive a renewal invoice, lose it or have questions about your dues and or membership status, please inquire at the sign-in table or send an e-mail to: ***treasurer@cfcs.org***.

Membership Cards: A new membership postcard with the membership card included for the next year will be distributed at the meeting following your renewal. The Cards will be mailed to those members who request same by e-mail to ***treasurer@cfcs.org***.

The Rankin File

What is Medical Identity Theft?
Bob Rankin, bob@rankin.org

Medical Identity Theft on the Rise

Your credit and bank account balance are not the only valuables that identity thieves are after. As health care costs have soared, so have incidents of “medical identity theft” in which crooks steal the credentials that enable one to obtain health care and sell them to other crooks. Here's what you need to know...

Medical identity theft is on the rise. And sadly, it is much more difficult to guard against this type of ID theft, and much harder to clean up the havoc it can create for a victim.

The Medical Identity Theft Alliance estimates that over 2.3 million Americans have been victims of medical ID

(Continued on page 6)

THE CENTRAL FLORIDA COMPUTER SOCIETY is a charitable, scientific and educational, nonprofit organization, founded in 1976 and incorporated in 1982 to encourage interest in the operation and development of computers through meetings with free exchange of information and educational endeavors.

Newsletter: The CFCS Newsletter © 2008 is the official newsletter of the Central Florida Computer Society, Inc. It is published every month by CFCS for the purpose of keeping members and others informed of computer-related news and activities of the Society. Circulation: 25,000.

THE CFCS Mailing Address:
CFCS
PO Box 520084, Longwood, FL 32752

Membership: CFCS membership includes participation in the Society's activities and subscription to this Newsletter.

Annual Dues Schedule:

Individual ……………………….$	**25**
Extra family member ..……..…..	**15**
Student (Full time)………………	**15**
Corporate membership……..…..	**100***

*Includes free business card ad

Members are responsible for sending a change-of-address notification (including e-mail) to:
membership@cfcs.org.

Gifts to CFCS are welcome, and because of the Society's nonprofit tax status, are tax deductible.

Meetings: CFCS meets each month on the 3rd Sunday at 2:00 p.m. at the **location described on page 24..** Guests and the general public are invited to attend. Special Interest Groups (SIGs) within the Society meet regularly. See Special Interest Groups listings on pages 6 & 7.

CFCS Web site: **www.cfcs.org**

Editorial: Articles for publication in the CFCS Newsletter should be *emailed* to the Editor at: ***editor@cfcs.org***. Please use Microsoft Word format, Times New Roman font, 12 point, if possible. The deadline for submitting articles is the first of each month.

Articles by authors other than directors of CFCS and the Newsletter staff do not necessarily reflect the policies or sanction of the Society. Unless otherwise indicated, articles in the CFCS Newsletter may be reprinted in newsletters of other nonprofit organizations, without permission, provided credit is given.

This issue was created using Microsoft Office 2003 and MS Publisher 2013 Edition. ◙

Interested in making a difference?
Then volunteer with CFCS! The programs and benefits that members receive would not exist without members also volunteering. There are vacancies for a Program Chair/ Coordinator, Education Chair and Advertising Chair. Please contact Jack Pearson, if you have any questions, comments, or suggestions. president@cfcs.org

Board of Directors

President	Jack Pearson	407-880-7339	***president@cfcs.org***
Vice Pres.	Stan Wallner	407-862-2669	***vicepresident@cfcs.org***
Secretary	Bess MacConnell	407-252-5624	***secretary@cfcs.org***
Treasurer	Betty Ann Ogus		***treasurer@cfcs.org***
Director 1	Tom Ault	407– 247-9165	***dir1@cfcs.org***
Director 2	Ted Goodwin	407-894-1180	***dir2@cfcs.org***
Director 3	Forrest Cheek	407/629-4139	***dir3@cfcs.org***
Newsletter Editor	Robert Black	407-421-4213	***editor@cfcs.org***
President Emeritus	Arvin Meyer	407-327-3810	***presidentemeritus@cfcs.org***
SIG Chair	Ken Larrabee	407-365-2660	***sigs@cfcs.org***

Chairpersons and Coordinators

Special Interest Groups	Ken Larrabee	407-365-2660	***sigs@cfcs.org***
APCUG	Hewie Poplock		***apcug@cfcs.org***
Education	(Open)	(e-mail only)	***education@cfcs.org***
FACUG	Arvin Meyer		***facug@cfcs.org***
Hardware Manager	Arvin Meyer	407-327-3810	***hardware@cfcs.org***
Helpline Volunteers	Griff Moore	(e-mail only)	***helpline@cfcs.org***
Membership	Don VanDemark		***membership@cfcs.org***
Photographer	Robert Black	407-421-4213)	***photographer@cfcs.org***
Program Coordinator	Hewie Poplock	(e-mail only)	***programs@cfcs.org***
Reviews (S/W & Books)	Mike Ungerman	(e-mail only)	***reviews@cfcs.org***
Webmaster	Cheryl Wilson	(e-mail only)	***webmaster@cfcs.org***

Newsletter Committee

Editor: Robert Black

Associate Editor:

Proofreader: CFCS BoD

CFCS Newsletter Advertising

Computer ready rates, for one time insertion, Electronic Edition:
Full Page $200.00 Quarter Page $75.00
Half Page 125.00 Business Card 25.00
Advertising deadline: the first day of month of issue. Electronic copy is
required.
All ad copy and correspondence should be sent by email to:
advertising@cfcs.org
*Annual Rates, Paid in Advance, for 12 insertions
Full Page $1200 Quarter Page $450
Half Page 750 Business Card 150

CFCS is associated with both
International & Florida User Group Associations:

www.apcug.net

theft, and 2014 saw 500,000 more cases than the previous year. That bad news is sure to get much worse. The MITA's latest survey was conducted in November, 2014, before the disastrous leak of 80 million patients' personal health information from Anthem. And just yesterday, I read that an "error" on Amazon's Web Services platform exposed 1.5 million people's private medical records.

Criminals can use victims' birth dates, Social Security Numbers, and the ID numbers found on insurance cards to obtain medical services and prescriptions at hospitals, clinics, and doctors' offices. While medical providers today routinely scan your driver's license, you may notice that they aren't very diligent about verifying its authenticity.

Medical Identity Theft

A fake license that wouldn't fool a liquor store clerk can be used to rack up thousands of dollars in health care costs very easily. Insurance cards, generally, don't bear photos or signatures. Using stolen medical credentials, a crook may visit multiple hospitals, pharmacies, and doctors to obtain services and drugs – often narcotics.

The records of these transactions are added to victims' health care records, and should be visible on your Explanation of Benefits letters, but bogus healthcare transactions often go undetected for months or even years.

The MITA's survey found that the average victim did not learn of medical ID theft until three months after it happened, and 30 percent victims could not determine when their health care credentials were improperly used. Health care privacy laws force victims to be intensely involved in investigations of medical fraud.

Can't Get No Satisfaction

If you've ever challenged a hospital bill, you know how hard it can be to prove that you did not authorize or receive the treatment claimed. Only 10 percent of victims in MITA's survey indicated they were "completely satisfied" with the resolutions of their cases. About 65 percent of respondents said they ended up paying an average of over $13,000 to resolve disputed claims.

MITA estimates that medical ID theft crimes are a $5.6 billion industry. Larry Ponemon, head of The Ponemon Institute that conducts MITA's annual surveys, believes that "a medical record is considered more valuable than everything else" to cybercrooks. Credit cards expire and are replaced frequently, rendering them useless to fraudsters after a short time. But Social Security numbers and personal health information don't change; a crook can use them practically forever.

There is no way to "freeze" health care credentials as one can freeze a credit card account. There are no centralized reporting agencies analogous to Experian, TransUnion, and Equifax that collect health care activity and can monitor it for suspicious patterns. Health care providers are trained to be helpful to patients, not skeptical of their identities.

In short, there are very few protections against medical ID theft and little help resolving its consequences. My 10 Tips to Avoid Identity Theft will help you safeguard your personal and financial records.

Aside from that, the most important thing you can do to guard against medical ID theft is reactive: read all of those "explanation of benefits" letters that come from your health care providers and insurance company as soon as they arrive. If you see anything suspicious, do not delay in challenging it.

Are you concerned about other forms of identity theft? Your best defense is knowledge and a proactive stance. See my articles *Free Credit Reports Online* and *10 TIPS: Identity Theft Protection* to learn what steps you can take, both online and offline, to protect yourself.

ANDROID SECURITY BUGS

By Ira Wilsker

Security bug could threaten 950 million Android devices
Ira Wilsker, *Assoc. Professor, Lamar Institute of Technology; technology columnist for The Examiner newspaper* www.theexaminer.com*; deputy sheriff who specializes in cybercrime, and has lectured internationally in computer crime and security.*

In recent weeks, at least two potentially frightening new vulnerabilities have been discovered that could threaten an estimated 95 percent of the one billion devices running the Android operating system. The good news is that as of this writing, there have been no documented attacks on Android devices that take advantage of these two security vulnerabilities. The bad news is that now that information on these security vulnerabilities has been widely published, as well as presented at the recent Black Hat hacker and security convention in Las Vegas, it may only be a matter of time until some bad guys start to take advantage of these security vulnerabilities.

Google, the progenitor of Android, was promptly made aware of the vulnerabilities as soon as they were uncovered, and has produced patches and fixes for many of the Android devices that have these vulnerabilities. The problems is that with the exception of a few models of Nexus smart phones supported directly by Google, it is up to the phone manufacturers or the cell phone carriers to release the upgrades and patches to close these vulnerabilities. At present, none of the major third party security software publishers provide any protection, leaving many of us vulnerable.

One of these newly discovered Android vulnerabilities was given the moniker "Stagefright" by its finder, Joshua Drake, vice president of platform research and exploitation at Zimperium. Drake first reported on the Stagefright vulnerability in April, disclosing his findings to Google, which quickly developed and provided security patches to its Android partners. Most of these Google partners who have not yet provided the patches to their respective customers may not do so for months, if at all; many phone manufacturers and carriers have explicitly stopped supporting and patching older Android phones, which are still in use by the millions. In several media interviews, as well as his Black Hat presentation, Drake explained that, "All devices should be assumed to be vulnerable." As stated in a July 27 Forbes magazine interview, Drake said that he believes that as many as 950 million of the one billion Android phones currently in use may be vulnerable to the Stagefright vulnerability. Drake went on to say that only older Android phones running versions of Android below version 2.2 will not be potentially affected by this bug.

It is important for Android users to understand that Stagefright is not a virus or other form of malware that could infect a phone, but is instead a bug, or unexpected and unforeseen security vulnerability in the Android software itself. This vulnerability is in the heart of the Android software that processes, plays and records multimedia files.

According to Drake, the security vulnerability may allow a hacker to illicitly access the targeted device by simply sending an MMS message (text message) or multimedia file. What is especially nefarious about the Stagefright vulnerability is that it can be taken advantage of by a hacker without any action by the user; the victim does not have to open or click on anything in order for the hacker to access a device. It is also theoretically possible for a hacker to capitalize on this vulnerability when an unsuspecting victim opens a purloined video file on a website. Once a hacker has taken advantage of this security gap in Android, he can access the victim's camera, microphone, and any data or images in the device's external storage. On some devices the hacker can also gain root access to the inner workings of the device.

In order to easily determine if a particular Android device is vulnerable to the Stagefright vulnerability, Zimperium has released a free "Stagefright Detector App" available from the Google Play Store. A similar detector utility was just released by the security software company Lookout, which it simply calls "Stagefright Detector." While these utilities will detect the vulnerability, it will still require a patch or other fix from the phone maker or the cell phone carrier supporting and updating the device.

When I first read of this Stagefright vulnerability and the availability of the detector, I downloaded and installed the detector. My year old Huawei Ascend Mate 2 phone, which had previously been upgraded by Huawei to Android Lollipop 5.1 (from 4.4), had the Stagefright vulnerability; coincidently, just yesterday (the day before typing this column), I received a patch from Huawei that, among other benefits, closed the Stagefright vulnerability on my phone. I reran the Stagefright detector from Zimperium to confirm the fix, and the vulnerability on my phone has definitely been patched by the recent update.

Another Android security vulnerability was disclosed at the recent Black Hat security convention. Well-known security company Check Mate disclosed this newly recognized bug, which it named "Certifi-Gate," which may potentially allow a hacker to take control of a victim's phone by utilizing the "Remote Support Tools (RSTs)" software that was installed on the phones by the manufacturers, often at the behest of the cell phone carriers selling those particular phones. Check Mate promptly notified the device makers and cell phone companies of the vulnerability.

According to Check Mate, there are millions of phones and tablets made by Samsung, ZTE, HTC, LG and other manufacturers that have incorporated this vulnerable "remote support" function software on their phones; according to Google, Nexus phones do not have this particular vulnerability. Using a security method known as digital certificates, hackers can spoof or counterfeit these supposedly secure digital certificates, allowing them the same access to the internals and functions of the phone that had previously only been allowed to legitimate support personnel. Once the hacker has tricked the phone or tablet into accepting a spurious digital security certificates, he or she now has direct access to personal information stored on the phone and can turn on the microphone to remotely record conversations, track the location of the device and its user, and otherwise threaten the security and privacy of the victim.

While the device manufacturers and cell phone carriers were promptly notified of the vulnerability, it may be months, if ever, before they push the patches to this newly discovered vulnerability. Users can download a free utility that will show the user if a device is vulnerable to this remote support vulnerability. Written by Check Mate, the utility "Certifi-Gate Scanner" can be downloaded directly from the Google Play Store.

According to Check Mate, in order for hackers to take advantage of this vulnerability, the user must first download and install an application that contains the code that gives the hacker the access. The Google Play Store continuously monitors the apps that it makes available, checking them to make sure that they do not contain any malware. Check Mate advises that users to install applications from a trusted source, such as Google Play."

With the continual battles among users who seem to love arguing iOS and iPhones versus Android devices, iPhone users should not gloat over these Android vulnerabilities. At the Black Hat convention in 2013, which is where many hackers and crackers rub shoulders with security experts, the vulnerabilities of iOS devices, specifically iPhones, was discussed. In one of the presentations, despite the false but widely held belief that iPhones are immune to attack and are very secure by nature, researchers from the Georgia Institute of Technology were able to inject persistent, undetectable malware into iPhones, iPads and other iOS devices using the latest generation of the iOS operating system. Using a modified USB charger, nicknamed "Mactans" after a type of black widow spider, the researchers were able to compromise any current generation Apple device in under a minute.

Check your smart phone for these vulnerabilities, and do not download apps from any source other than reputable sources such as the Google Play Store or the Amazon App Store. Do not open any text messages from people that you do not recognize, although text messages can be spoofed just as e-mails are frequently spoofed. If you find that your device maker or phone carrier is providing a patch, update, or upgrade, strongly consider taking advantage of the offer and update your device immediately.

The Rankin File

10 Ways to Protect Yourself from Identity Theft

By Bob Rankin, Ask Bob Rankin

http://askbobrankin.com/10_tips_identity_theft_protection.html

A new study shows that identity fraud is increasing, affecting over 13 million U.S. consumers in the past year. Big spikes were noted in 'new account fraud' and 'account takeover fraud' -- two of the most damaging types of ID theft. In addition, a series of massive data breaches at major corporations leaves consumers vulnerable to phishing and other forms of fraud. Poor password practices are a factor as well. Read on for my tips on avoiding fraud and identity theft...

Identity theft is one of the most traumatic non-violent crimes to which one can fall victim. When a crook uses your good name to commit fraud or robbery, the impact on your reputation, employability, and credit is severe and can last for years. It's even possible to find yourself arrested for crimes you did not commit. So it's important to protect yourself against identity thieves.

The telltale signs that your identity has been stolen can be subtle and go unnoticed for months, even years. Inexplicable charges on your credit card bill may be chalked up to clerical errors. Letters from creditors you've never heard of and certainly never did business with may be ignored. But eventually, an enormous credit card bill, legal papers or police show up at your door. You are denied a mortgage or a job. Then the real nightmare of proving "I didn't do it" begins.

Prevent Identity Theft

It can be maddeningly difficult to clear your name, costing hundreds of hours and thousands of dollars. That's why it's important to take steps NOW to make it as difficult as possible for a scammer to victimize you. Take action on these ten tips as soon as possible, and you'll tips the scales in your favor:

Check your credit report on a regular basis, to see if there is any incorrect information, or accounts you don't recognize. My article Free Credit Reports Online explains how U.S. citizens can get three free credit reports per year, and avoid the credit report scammers.

Shred your sensitive personal documents before throwing them away. A battery-powered cross-cut shredder can render your banking and credit card information unreadable and costs less than $30. "Dumpster diving" is a favorite, low-tech way by which ID thieves collect bank statements, credit card numbers, Social Security Numbers, and other bits of your identity from your trash.

Be wary of telephone solicitors asking for personal or financial information to "verify your identity." Common scams involve someone who claims to be from your bank or credit card company, claiming that there is a problem with your account. If you did not initiate the call, hang up and call the toll-free number on your statement, then ask for the security department. This happened to me recently, in the wake of the Chase Bank breaches. A person claiming to be from Chase called my unlisted number and asked for me by name. I Googled the number on the caller ID, and found that many others reported similar calls.

Keep important documents, such as tax returns, birth certificates, social security cards, passports, life insurance policies and financial statements secure in your home. A fireproof safe is a good idea, but remember to bolt it to the floor or hide it well. Consider using TrueCrypt or Bitlocker to encrypt your personal and financial data, in case your computer is lost or stolen.

ATM Safety: Make sure no one is looking over your shoulder when you enter your debit card's PIN at an ATM or point-of-sale terminal. I recommend the "two finger method" where you point two fingers at the ATM keypad, but only press with one. This makes it nearly impossible for someone nearby to discern your PIN while you're entering it. You should also be wary of "skimming" devices at ATMs and gas pumps, which can be used to steal your card information. See *All About Skimmers* to learn how to identify these devices. http://krebsonsecurity.com/all-about-skimmers/

Memorize PINs, account numbers, and passwords; do not write them down. And for heaven's sake, do not put such data on scraps of paper kept in your wallet, purse, or laptop case! See my related articles Is Your Password Strong Enough? and Password Managers for Multiple Devices. http://askbobrankin.com/is_your_password_strong_enough.html http://askbobrankin.com/sync_your_passwords_on_windows_mac_and_smartphones.html

Get blank checks delivered to your bank branch, not to your home mailbox from which they may be stolen. On a similar note, eliminate junk mail which may contain "convenience checks" and credit card offers that can also be intercepted from your mailbox. Visit OptOut Prescreen for help eliminating these dangerous nuisances. https://www.optoutprescreen.com/?rf=t

Credit Cards: Check to see if your online banking service has a feature to notify you by phone, text, or email when you when a credit card transaction exceeding some threshold occurs. Also, when you order a new credit or debit card, mark the calendar and follow up promptly if it does not arrive within 10 business days. Ask the card issuer if a change of address request was filed, and if you didn't do it, hit the panic button.

Don't give your Social Security Number to any business just because they need a "unique identifier" for you. Instead, ask if you can provide alternate proofs of identity, such as your driver's license or birth certificate.

Consider placing Fraud Alerts with the major credit bureaus, so new accounts cannot be opened without your knowledge. Call Equifax (800-525-6285), and they will pass along the request to both Experian and Trans Union. Fraud alerts expire after 90 days, so you can repeat the process quarterly, or lock down your credit file with a Credit Freeze. A freeze is permanent and free (in most U.S. states) but it may interfere with loans applications, employment screening, signing up for utility or phone service, new insurance policies, and other transactions. (See this Consumer's Union guide to credit freezes.) You'll need to contact each credit bureau (Equifax, Experian, and Trans Union) to request the credit freeze.
http://consumersunion.org/research/security-freeze/
https://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp
http://www.experian.com/consumer/security_freeze.html
http://www.transunion.com/corporate/personal/fraudIdentityTheft/fraudPrevention/securityFreeze.page

There are plenty of common sense things you can do to protect against identity theft, but sometimes it's beyond the control of even the most vigilant. The Javelin Research 2014 Identity Fraud Report reports that there is a new identity fraud victim every 2 seconds, and found that data breaches perpetrated on large companies such as Target, Home Depot and JP Morgan Chase are a "treasure trove" of data that could be used to commit identity theft and fraud. Here's a very interesting infographic showing the major data breaches of 2014, and what types of consumer data were affected.

What about LifeLock?

You may be considering LifeLock or a similar identity theft protection service. Although this can be helpful, no company can guarantee that identity theft will never happen. These services monitor your bank account, and look for suspicious online activity done in your name. They'll alert you if they spot any red flags and promise to help you repair the damage. But because of lawsuits filed by the credit bureaus, Lifelock can no longer place fraud alerts on your behalf. Also, all identity protection services are barred from offering Identity theft insurance coverage to residents of New York state.

It can be a nuisance to manage fraud alerts manually. But given the recent focus by scammers on new account fraud and account takeover fraud, a service such as LifeLock, Identity Guard or Trusted ID may still be useful. The downside is that most cost about $10/month, and none of them can claim to prevent all forms of identity theft.
www.lifelock.com
www.identityguard.com
www.trustedid.com

Mac OS X Tip

BCUG Bytes

By Lee Maxwell, co-leader MacWaves,
the Mac/iDevice User Group of the BCUG
August 2015 issue, BCUG Bytes
Leemaxwell [at] gladmaxcom
www.bcug.org

Adware is becoming one of the most significant threats to users of computers, both Windows PCs and Macintoshes. Besides causing annoying changes in the performance of a web browser, it can also be used to convince you to allow a nefarious stranger access to your computer.

Case in point: A member of MacWaves, the Macintosh User Group part of BCUG, emailed me about a recent experience. I'm quoting her email:

“This afternoon, when going to a website, I received a message that my computer was infected by a virus — I could not do a force quit from Safari, nor could I get rid of that
message —it wasn't a mail message — it came up right in the middle of my screen —on the message with the warning about the computer being infected by a virus, there was a number to call, which, out of desperation, I called [that number], and was told I reached Apple Support.

“I was told that they were getting a number of calls from people who were receiving the same message — and this gentleman would see what he could do to help — by looking at my desktop!! I've done this a number of times with Apple, and did allow it. (I am kicking myself about doing this—but never had a problem whenever Apple did this in the past.) Not sure what he did — numbers kept appearing, and after 5 or more minutes, he said that he would share the diagnosis with the 'Apple anti-hacking team' and remove the virus — that would take 40 - 50 minutes. He said it was due to a Zeus Malware???

Never heard of it!

"When I heard that, I told him that I would prefer to take my computer to the Apple store and have them do whatever — he told me that they would not be able to fix it as it was a network problem —and it was a virus affecting lots of computers in my area.

"I said I had his number and would get back to him after I consulted my Mac User Group or Apple. He said I would have to get back to him within 30 minutes or they would not be able to help; then I knew something was wrong.

"I called Apple — they told me it was a scam — and the gal I spoke to went over everything (checking my desktop, etc. as well as library, apps, documents, etc.) and everything seemed to be fine. I told her I was locked out of Safari and could not even do a Force Quit. Everything seems to be corrected and she also had me install MalwareBytes for Macintosh on my computer.

"Not sure why I was so gullible at first — should have known better than to listen to this guy — especially with his accent, the poor connection which I kind of knew must have been out of the US— but he said he was in California —with the Apple anti-hacking team!!!

"I learned my lesson — hope they were not able to get any info from my computer — Apple said they thought everything was O.K.

"Since then, I changed a couple of my more important passwords just in case — and will probably change a few more."

The email is pretty self-explanatory, so I will only give some advice to Macintosh users:

If you see a pop-up window like this, do not do what it tells you to do. Instead, try to quit the web browser you're using. If it won't quit, click on the Apple Menu icon on the left side of the menu bar, choose the Force Quit command. In the window that appears, choose the name of the web browser and click Force Quit (Command-Option-Escape), then click OK.

If you have a different web browser on your Mac, use it to download MalwareBytes for Mac, the renamed AdwareMedic, install it via opening the downloaded .dmg file and drag-and-drop the MalwareBytes for Mac icon onto the Applications folder icon, then launch it from the Applications folder and use it to scan for and remove adware.

If for any reason you can't do that, contact Apple Tech Support.

October was National Cyber Security Awareness Month

Ira Wilsker, *Assoc. Professor, Lamar Institute of Technology; technology columnist for The Examiner newspaper www.theexaminer.com; deputy sheriff who specializes in cybercrime, and has lectured internationally in computer crime and security*.

For the past 14 years, I have been promoting the annual National Cyber Security Awareness Month, encouraging individuals, schools, colleges, governmental agencies, corporations, clubs, and other groups to get involved. Every year since its founding in 2001, this annual event has been recognized by bipartisan presidential proclamations declaring October as National Cyber Security Awareness Month. While many organizations around the country hold a myriad of events during the month of October promoting cyber security, locally the premier event is hosted by the city of Port Arthur and its most capable information technology manager, Fay Young.

In recent weeks, hundreds of thousands of taxpayer records have been digitally stolen from the IRS; a multitude of financial institutions have had their customers' account data purloined by hackers for nefarious purposes; and millions of individuals have been victimized by a variety of online attacks from hackers who steal their personal information, hold their data for ransom, and trick individuals into disclosing usernames and passwords. Sensitive military data has been stolen by hackers and other data thieves, and unfriendly foreign government hackers have stolen hundreds of billions of dollars' worth of American intellectual property and used it to unfairly undercut American industry or to dissect and copy our most advanced military weaponry.

I am amazed that despite years of imploring individuals to use different and complex passwords for each of their online accounts, many people still use the same easy-to-guess passwords to access all of their accounts. Hack or crack any one of those, and all of the victim's accounts now belong to the hacker. Bank accounts are drained, multiple illicit purchases are made from online sellers and delivered to parties unknown (all of which are then billed to the victim); inappropriate e-mails are sent to people of authority and power, traceable back directly to the victim; and scams can be perpetuated on the friends, relatives, and acquaintances of the victim by sending spam that is apparently coming from a trusted sender.

Now that so-called "smart devices," mostly Android, Windows, and iOS powered phones and tablets, are taking over roles previously performed on desktop and laptop computers, they have become the targets of choice of dishonest people out for the fast buck, at the expense of the otherwise innocent users. A popular online pundit, Kim Komando, recently posted the "7 Worst Apps That Violate Your Privacy." Some of these questionable apps are popular games played by kids all over the world, but these are more than just games, as they compile and send extensive personal information, contact lists, microphone and camera captures, and other content from the phone to third parties for questionable purposes. Immensely popular social media apps are being inappropriately utilized by pedophiles engaging in "victim acquisition." While for many of us our smart phones are addictive, we must also be aware of the risks that these wonderful devices impose upon us.

It is not too late for people to promote the concepts of cyber security awareness right now, and is also certainly a worthwhile project for next October. An abundance of material including brochures, videos, lesson plans for all age and academic levels, and other content is readily available for free from Stay Safe Online (staysafeonline.org). For teachers, college professors and administrators from K-12 to graduate school, Stay Safe Online offers prepared information that is ready to present to appropriate audiences. The website lists age-appropriate concepts for which the organization provides complete and free instructional content and media. It's easy to participate and use.

Businesses have become prime targets for cyber crooks who have stolen enormous amounts of money directly from the businesses as well as their customers. Hundreds, if not thousands, of small and midsized businesses have fallen prey to scams that illicitly transferred funds from their bank accounts to distant thieves, mostly in Russia, Eastern Europe, China, Nigeria, Iran, Pakistan, and other locations where the likelihood of recovery or even of prosecution is nil. In recent history, we are all aware of the massive credit card thefts from many other well-known retailers. Millions of those credit card numbers, complete with enough additional information to conduct unlawful online transactions, as well as to produce excellent quality counterfeit credit cards, were widely available for sale online, mostly on Russian websites. Within days of the massive Target breach, thousands of counterfeit credit cards bearing data stolen from Target were confiscated by Customs and other law enforcement agencies along the Mexican border, many of those cards already used to purchase thousands of dollars of goods from American merchants, and then carted back across the border. Richard Clarke, a renowned cybersecurity expert who advised several presidents, has written that all of the Fortune 500 corporations have been the victims of hackers, and billions of dollars' worth of intellectual property have been stolen, mostly by the Chinese. Obviously, businesses and their employees need to be made

aware of the cyber risks that they face on a daily basis, and be adequately trained in safe cyber practices.

Businesses can utilize the free materials and teaching guides available to them under the "RE: Cyber" program from the alliance. Executives and managers up to the top executive level as well as the board of directors may find the educational information available at staysafeonline.org/re-cyber appropriate for their degree of fiduciary responsibilities, as the information covers Cyber Threat Trends; Getting Started (with a corporate cyber security program); Board Oversight; Cyber Risk Assessment and Management; Cybersecurity Maturity Model; Cyber Regulation; Legislation and Policy; and Creating A Culture of Awareness. For employees, the material available online at staysafeonline.org/business-safe-online will cover many of the most important topics that the rank and file (as well as managers and executives) may need to be safer while online.

The general public will also find valuable information available at staysafeonline.org/stay-safe-online. Topics covered include, Malware & Botnets, Spam & Phishing, Hacked Accounts, and Securing Your Home Network. I cannot emphasize enough the utter necessity for everyone to become familiar with these most basic home cyber security and safety concepts not just to protect our computers and our personal finances, but to also protect our most valuable assets – our children.

I am offering an open invitation for everyone to attend a free, public celebration of "National Cyber Security Awareness Month," which will be held on Thursday, Oct. 1, at the Port Arthur City Hall, 444 Fourth Street, 5th Floor, starting at 9 am.

Kudos go to Fay Young, the Port Arthur Information Technology Manager, who has so ably promoted these annual National Cyber Security Awareness Month events for the past several years. We need many more like her doing much of the same in our schools, colleges, businesses, computer clubs, and other organizations. Individuals also need to be better aware of proper cyber security in order to protect their personal computers and other smart devices.

While I personally applaud and commend those who are involved with promoting and implementing these most useful and valuable events, I personally believe that cyber security is too important to "only" be a monthly event. Protecting our cyber world needs to be a continuous practice.

Those interested in attending the Port Arthur event should preregister online at registration.cityofportarthurtx.net.

Password Generation Hint

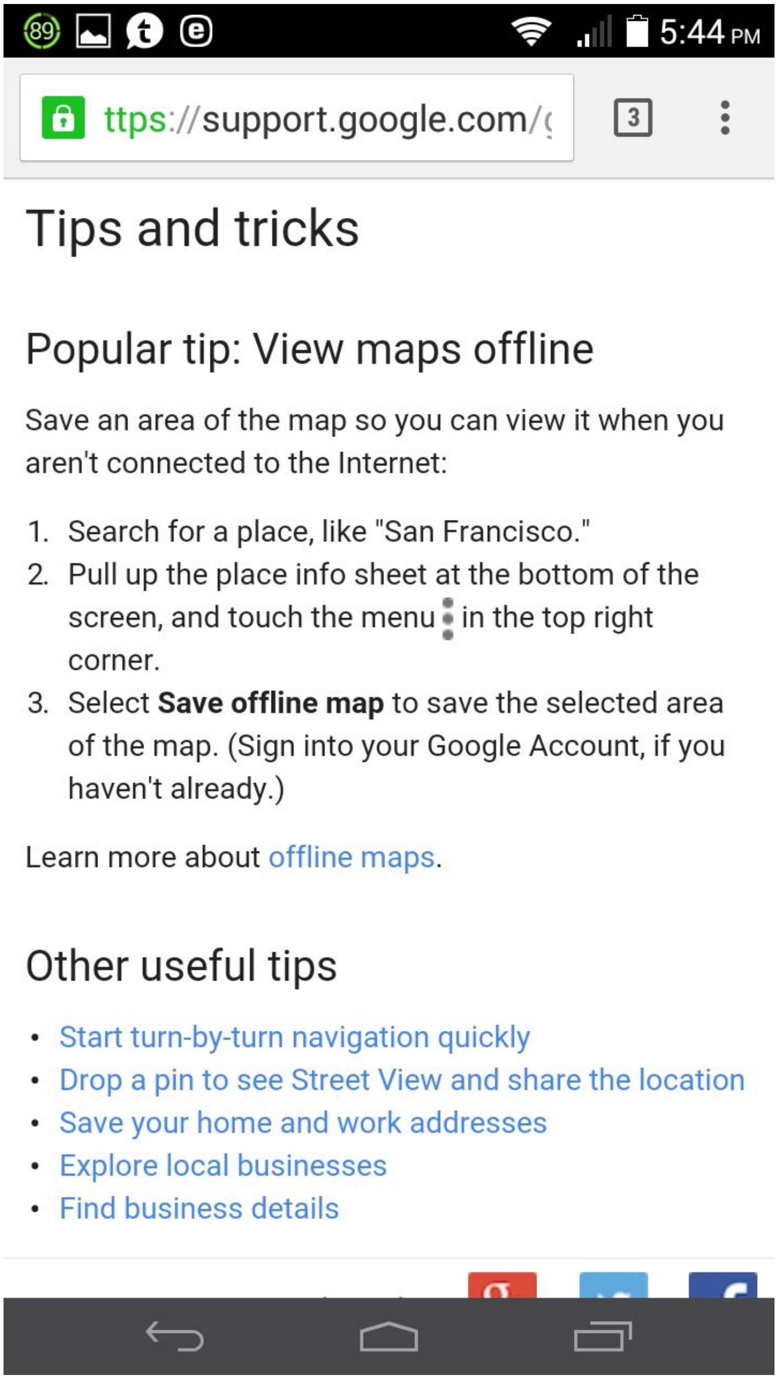
By Jerry Goldstein, Member,
The PC Users Group of Connecticut
August 2015 issue, The Program
http://www.tpcug-ct.org/
Adrabinowitz (at) att.net

Thanks to the lack of safety of those holding our passwords, we are often notified of user information and password theft occurring by those we provide our information to. Banks, stores, and other major corporations announce data thefts and loss regularly. As a result we need to be constantly on vigil and update our passwords regularly.

Remembering passwords is difficult enough without having to change them at least twice a year. Password manager programs are great but even they can fail and then you can lose all your passwords.

A new password theme has been worked out that helps you to remember your ever changing password scheme. The method uses a consistent password coupled with the name of the site you are at. Create a base password like: Qstn&16^, and combine it with the website you are visiting to create a unique password for that site. So if you go to the TPCUG Yahoo Forum site you would use, for example, Qstn&16^tpcg. This combines the usage of leaving out vowels in a word to remember the password better while making the password harder to break, using numbers and characters, one capital letter, and using at least an eight part letter/character basic password for better protection. You use the same basic Qstn&16^ with all your sites and just add in the website's name without vowels. You now have a single password to remember that can be used everywhere.

Since the likelihood of one of the sites you use that password is going to be hacked this year you want to take one extra step to avoid having to revise all your passwords every time a hack occurs. Value your sites according to Low, Medium, and High security needs. For low value sites, like the shoe store or grocery store you add LV to your password. That would be: Qstn&16^LV as your base password for low value sites. Medium value sites add MV and high value sites, like banks and credit cards,



Tips and tricks

Popular tip: View maps offline

Save an area of the map so you can view it when you aren't connected to the Internet:

1. Search for a place, like "San Francisco."
2. Pull up the place info sheet at the bottom of the screen, and touch the menu ⋮ in the top right corner.
3. Select **Save offline map** to save the selected area of the map. (Sign into your Google Account, if you haven't already.)

Learn more about offline maps.

Other useful tips

- Start turn-by-turn navigation quickly
- Drop a pin to see Street View and share the location
- Save your home and work addresses
- Explore local businesses
- Find business details

add HV.

For high value sites it is recommended you also use secondary authentication, such as having to answer a question after your user name and password are approved. Remember not to use your correct information on your authentication answers. Your correct information is too easily available on the internet to use as an authentication. Dates of birth, schools you attended, and family and pet first and maiden names are readily found on many people's Facebook profiles and postings. Use something different that you can easily remember instead.

Protecting yourself is never going to be as easy as locking your doors and windows any more. Banks lose your data regularly as laptops filled with information are left behind by bank employees when they stop off for their morning coffee. Thousands of hackers work feverishly to break your passwords and steal your identity. The methods offered here are just methods to help you protect yourself. Doing due diligence in the battle against identify theft is an ever ongoing battle. Stay alert and you may get lucky and not hacked, for a while.

Malvertising

By Dave Palmer, Member,
Tampa PC Users Group, Florida
March 2015 issue, Bits of Blue
www.tpcug.org
dkp205 (at) hotmail.com

Just as ‘malware’ is short for malicious software, ‘malvertising’ is short for malicious advertising. Like many services on the Internet, online advertising has become highly automated. And like nearly everywhere else on the Internet, cyber criminals have found ways to corrupt that automation to turn a profit.

Have you noticed that after you do some online research for a specific purchase that you soon see online ads for similar products on different websites? That’s a result of websites leaving ‘cookies’ on your computer. Cookies don’t identify you personally but they can identify you as having an interest in a category of products. In addition, the IP address of your computer provides a general geographic location. When you visit other websites, they read your IP address and any cookies left recently. They also provide this information to an ad network which quickly adds interest-based or location-based ads to the websites you visit. Now advertisers and ad networks know your approximate location and the categories of products you’re interested in.

How online advertising works

Ad networks consist of publishers, advertisers and the middlemen who connect the two. Publishers are the owners of the websites you visit. They sell advertising space on their websites. Then there’s the advertiser, the individual or business that has a product or service they want to advertise. They buy advertising space on websites. The sites you visit usually do not play a direct role in choosing the ads you see. Instead, a middleman, a third-party advertising company, manages the ad selection and placement for both the publisher and advertiser. This makes the process more efficient for everyone. The process is highly automated – humans are only rarely involved – usually only at the beginning for initial approval.

This business model, advertising supported by ad networks, supports a large portion of the Internet, providing the 'free' information and web-sites we have come to rely on. Online advertising can come in many forms. Ads can be a single static image without animation, ads can be animated in one of several different ways, or ads can be video-based. There are popup ads, pop-under ads, banner ads and a dizzying array of shapes sizes, styles, formats and technologies involved.

As this advertising business model has developed, ad networks have spread across the Internet. Over time the sheer volume of ads has given rise to a massive and tangled conglomeration of ad networks, ad exchanges and other related businesses that buy, sell, trade and swap ads and ad space constantly as the tides of supply and demand shift constantly. Of course, opportunistic cyber criminals weren't far behind. They soon found many ways to abuse the system for profit.

Delivering the payload

Bad guys may scam the system by posing as legitimate advertisers. They may hack into legitimate but dormant accounts. Either way they gain access to the ad networks. They then create legitimate-looking ads to disguise malware to either deliver malware directly from booby-trapped ads, or to redirect viewers to a poisoned website that delivers the malware payload. In most cases neither the publisher (the website displaying the ad) nor the ad network providing the ad knows the ad is booby-trapped.

One major obstacle to detection of malicious ads is that they are not persistent. Once the user leaves a website or closes the browser, all traces of the ad disappear. In addition attackers take great pains to make their ads hard to detect. They may enable their malicious payloads only after their ads have been approved. They may set the malicious ads to only attack every 10th user. They may set up many different domains and redirect victims many times before the victims reach the poisoned website. These and other practices make detection quite difficult.

Once installed on the victim's computer, malware may look for login information for e-mail, social media, and bank accounts, as well as for identity information. In some cases the malware can lock the user's computer and demand a ransom.

Click fraud

Another way the bad guys' corrupt legitimate advertising is to commit 'click fraud.' Click fraud occurs in pay per click (PPC) online advertising when machines or programs imitate a legitimate user and click on an ad to generate a charge per click without having any interest in the ad itself.

Hackers may use the malware installed by ads to commandeer the victim's computer and add it to the hacker's botnet – a network of hijacked computers used for criminal activities. Botnets (bots) are often used for click fraud. Click fraud sometimes begins when unscrupulous publishers or ad networks hire hackers to boost their numbers or to generate income. Computers in the botnet are instructed to visit various websites and click on specific ads.

Here are a few eye-opening stats from an adweek.com article (http://goo.gl/9zrH7X). Up to 50% of publisher activity is from botnets - automated click fraud. Bots account for 11% of display ad views and 23% of video ads. Of the $43.8 billion in ad revenue, fraudulent activity accounts for $6.3 billion. More than half of traffic from 3rd parties claiming to lift publisher's traffic numbers comes from bots. Click fraud is a major problem in that it raises costs for legitimate publishers, advertisers and ad networks. Click fraud can also be used indirectly to attack legitimate competitors and force them to pay higher advertising costs.

What can be done?

Unfortunately there's little agreement on who is responsible for addressing these threats. Both publishers and advertisers need to take action to limit malvertising on their networks. In addition a number of companies now exist to validate that ads are being seen by humans. They include WhiteOps, ComScore, Integral Ad Science, The Media Trust and Double Verify, among others. But since consumers are under a serious and direct threat, we must do what we can to protect ourselves.

How to protect yourself
In some cases the bad guys are hoping they can redirect your browser from your intended website to a poisoned website so they can download malware into your computer. For that scenario to work your browser has to:

allow the redirect and
contain a vulnerability that allows malware to be installed and
operate in administrative mode to allow the installation.

I've included some instructions below on how to set up the Big 3 browsers to prevent redirects*. In case you still operate daily in administrative mode, Merle wrote an excellent explanation of how to create a standard user account in the October 2014 edition of the TPCUG newsletter.

In some cases the ad is booby-trapped with some executable script, often Flash, JavaScript, etc. Your protection is to use script-blocking software - NoScript for Firefox and ScriptSafe or Script Blocker for Chrome. Things are a bit more complicated with Internet Explorer. Don't use Internet Explorer unless absolutely necessary. If you're an IE diehard check out the instructions here: http://goo.gl/YTcQpK.

Although script blockers are not terribly convenient, removing malware is way beyond inconvenient. In the end, the threats from malvertising are really no different from other malware threats across the Internet. So the protection advice is no different either. To reduce the threat from vulnerabilities, first minimize your 'attack surface,' that is, remove programs you're not using. The next step towards minimizing your vulnerability is to keep everything updated – your operating system, browsers, programs, add-ons, plug-ins, etc. Backup your data and system regularly. Use a password manager and strong passwords.

Preventing redirects*
Chrome

To prevent Chrome from being redirected to another site without your knowledge, click the "Customize and Control Google Chrome" button. The button has three horizontal lines on it.
Click "Settings."
Click the "Show Advanced Settings" link to display more setting options.
In the Privacy section, click "Enable Phishing and Malware Protection."
Close the browser window.

Google now displays a warning if the browser is trying to redirect you.

Mozilla Firefox
In Firefox, click the "Open Menu" button, which has three horizontal lines.
Click the "Options" button in the panel that opens.
Click the "Advanced" button and then the "General" tab.
In the Accessibility section, check the "Warn Me When Websites Try to
Redirect or Reload the Page" box. Click "OK."

Internet Explorer
Internet Explorer doesn't have a way to expressly stop redirects. Instead, you have to limit the whole Internet.
Click the "Tools" button, which looks like a gear
Click "Internet Options"
Click the "Security" tab.
In the Security Levels for This Zone pane, set the slider to "High." This prevents IE from running ActiveX controls, which is how many browser

Have a Blast!

SIGN UP FOR WEEKLY EMAIL!

All meetings and speakers are subject to change, and late alterations are always possible. To keep completely on top of events, log on to CFCS.org and subscribe to our weekly e-mail update, the E-Blast!

redirects are carried out. However, this might prevent some safe sites from loading correctly.

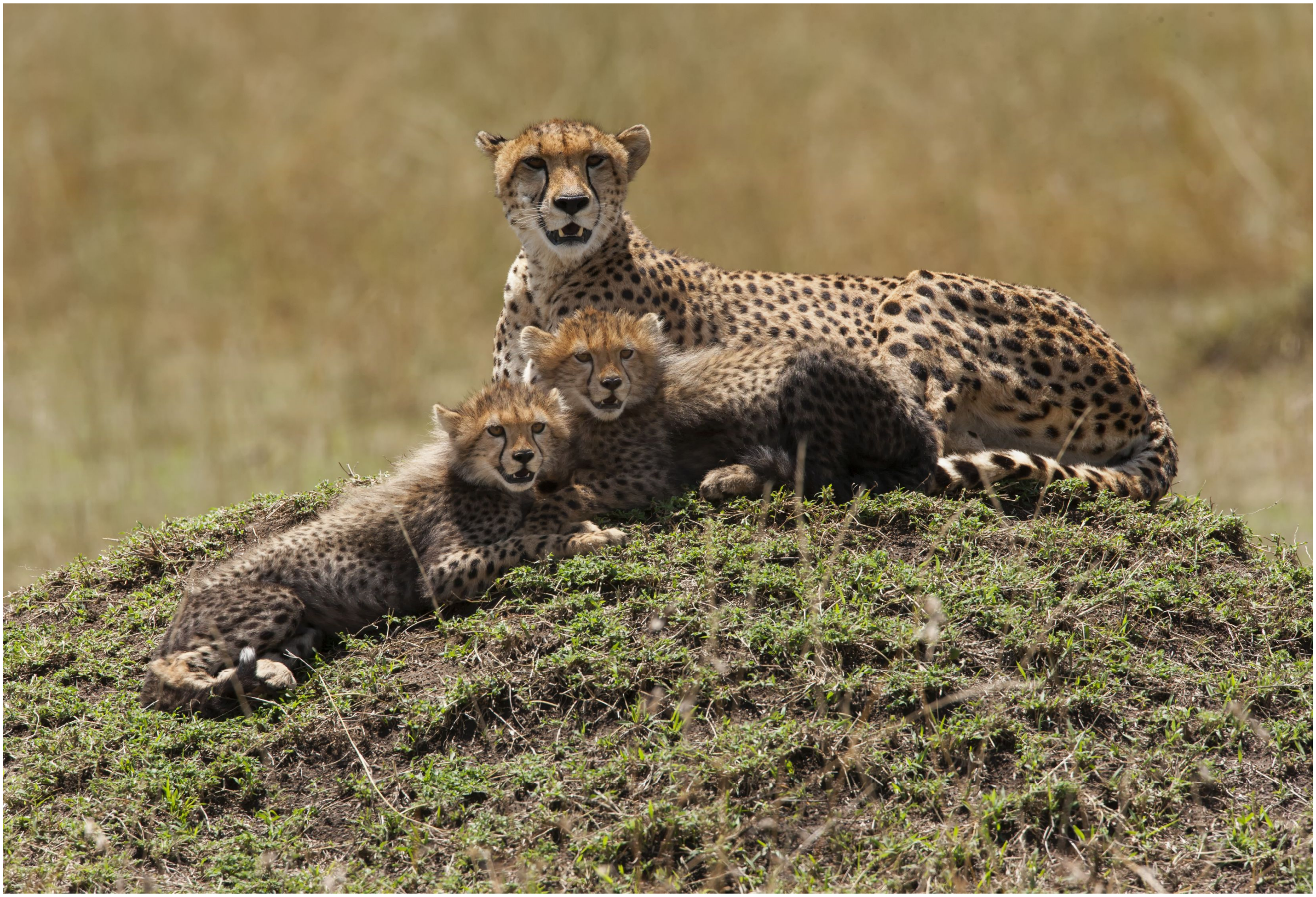
Click "OK."

These steps work for Google Chrome 40, Internet Explorer 11 and Mozilla Firefox 35. Other versions might use different steps.

*The above instructions were taken from: https://www.ehow.com/how_8744477_do-links-redirectingdifferent-sites.html

Dick Dehler Wins First Place in National Photo Contest

CFCS member Dick Dehler, who was injured during a photo safari to Africa, was finally rewarded for his efforts (and time spent in a Nairobi hospital), by winning first place in the APCUG 2015 photo contest. Dick won in the Animal category. To view the other winners, go to http://apcug2.org/2015-newsletter-photo-and-website-contests-begin-july-10-2015/



Dick's Dehler's entry in the APCUG 2015 Photo Contest is entitled "Feline Mother with Cubs".

How to Set Windows 10 Privacy & Security Options

Sandy Berger, CompuKISS
www.compukiss.com
sandy (at) compukiss.com

Windows 10 has many Security and Privacy options that you can quickly and easily change. In fact, you have more control over these options in Windows 10 than you do in most other operating systems. Want to get started? Just follow these simple instructions.

Once Windows 10 is up and running, you can still set many of the Security and Privacy options. Just click on Start and go to the Settings, then click on the Privacy control panel icon.

You will see a long list of options and you can turn each of these off if you like.

In the Privacy area you can even quickly turn off the camera, microphone, and location information. And you can stop sending some information to Microsoft. Click on “Manage my Microsoft advertising and other personalization info” and you will get more information on how that works and also get the ability to turn off targeted ads.

Actually Windows 10 gives you more control of the privacy options than most other operating systems. As far as privacy goes, Windows 10 is no better or worse than many of the other operating systems that you use on your other connected devices. Yet, if you use Windows 10, you should check out the Privacy and Security options

Keep Your PC Clean

By Merle Nicholson, Secretary,
Tampa PC Users Group
April 2015 issue, *Bits of Blue*
Merle (at) merlenicholson.com

You're going to say, “Here's Merle again, preaching on the same ol,” but keeping your computer fully functional goes further than just buying antivirus and doing backups. Here's my take on what we have to look out for.

Emails: We're getting emails – it seems constantly – with requests to straighten out your credit rating, fi x an error on the mortgage, a report on someone logging into a credit card account that you don't even own. Or worse, one that you do own. Scams – all of them. Any legitimate concern – they'll NEVER send you an email. It's a scam to get you to reveal something that will harm you. They need to be deleted immediately. You'll soon be able to recognize each one because they're persistent, and you'll delete without opening. Better still, mark the email as spam, and the next time you get one from them hopefully your email client will recognize it and put it in your spam folder for later deletion.

The objective is to never open the spam email in the first place. Sometimes you have to. But first, let's make a small change to your email client. If there is a pane (a section of the email window) that automatically shows the content of the email; turn that off. If it's on – guess what: You have already opened that spam. That's not good. You want to be able to select it and hit delete without reading it. If the reading pane is showing, it's too late.

No legitimate business will ask you to click on something in an email unless you're expecting it. For instance, I buy something from Amazon, and they send me a link to get a tracking number. There's something there that I recognize: The previous transaction. But if I get something from Amazon that doesn't contain a known previous transaction, just urging me to click on a link, forget it. I may open the browser independently of the email and log into my account to check, but probably not.

Incidentally, there's a system of second level login security on some websites. One of my sons told me about it when he knew I was using PayPal, and he directed me where to set it up. I associated my mobile phone number to my PayPal account and checked one option. Now when I log in, I'm stopped asking for a six digit number to type in to continue. There's a “Send SMS” button to click and when I do, they immediately send a message to my mobile phone with the number to type in. You have five minutes before the number expires. I really like this. I can glance at a six digit number and remember it long enough to type it in, so I don't see that I've lost a thing. I'd like to see more of this – my banking site first comes to mind.

Finally on this subject, guess how many unopened emails you should have. If you guessed none, you're managing your mail effectively. If you have hundreds, you're not managing at all. How can you find the important emails if you have hundreds of unopened ones?

To get on the right track, sort all your current email by sender, start at the top and block delete the entire senders mail if it's not of interest. But just before that, right-click on the first one in the group and mark it as Spam. If your email doesn't have a Spam filter, it's time to change email clients.

Downloads: One very disconcerting trend on websites is the appearance of multiple “Download” buttons on a page where you expect a single download of a product. I do have several products, some paid and some free that require new versions. I'm directed to the site and I see a confusing number of Download buttons. What is happening is that the owners of the site have sold a section of their page to a service that provides content. That content is then sold to advertisers, and I'd guess there is very little oversight of the content. In any case those things with Download buttons can't be to your benefit. Be alert, cancel this quickly if you can; if there's a file being downloaded, there's a notification on the lower left of your browser; it can be canceled if you're quick. If you don't catch it, there's a menu item to “Show in Folder”, go to that file and delete. Hold Shift, hit Delete or Shift, right-click Delete. Be careful! The next thing you have to look out for are downloads of things you don't want that are attached to things you do need. When you want to update Flash, or PDF readers, and get the update, very frequently you'll see a popup that has a toolbar or something else already checked for installation. UnCheck those first. Do it slowly and make sure you understand everything that is happening.

Phone Calls from Microsoft Support: You have to believe me. Microsoft does not know what PC you have, cannot tell you have a problem, and certainly will never call you! There is no mechanism existing that can do that to benefit you. None. That the speaker is saying something in a language vaguely resembling English has to be the first clue.

Offers to “Fix” your PC: Merle's Rule Number 1 is worth repeating. No software can “Fix” your computer. It doesn't exist. If you're having problems it's because you have software installed causing it. That's Too Much Software, don't add more! First uninstall all software you don't need. You don't need anything that has the word “Toolbar” in it. You don't need “Repair My PC” software. You don't need “PC Cleanup” software and you certainly do not need someone to log into your computer remotely to repair it, even if they say they are “Microsoft Support.” Even benign PC repair software stands on its ability to clean up the registry. Guess what? No one needs that. Ever. You also don't need but one antivirus software installed and running. Then look at all your browser add-ons. Anything with the word “toolbar,” disable it.

Actually there is plenty of software that will fix specific problems. But first you must identify the problem in detail first. Frankly, if you have the knowledge to do that you probably wouldn't have the problem in the first place.

Last, make sure you are completely up-to-date on all Windows Updates. Don't just assume that it's being done automatically. Check on that first. One of the tricks malware pulls is to block or turn off automatic updates. Microsoft creates and sends you a “Malicious Software Removal Tool” on the second Tuesday of each month.
Currently it detects and removes the top 264 malware. It runs automatically. The tool is a part of the Windows Update process.

There are lots of things you can do to be safe, and operate your computer with a minimum of fuss, but if you're having problems with your computer that you can't handle, get some help. This is one reason you are a member of a computer club. Every club has several people who are very adept at cleaning up your system when it’s misbehaving.

Is Windows 10 Spying on Us?

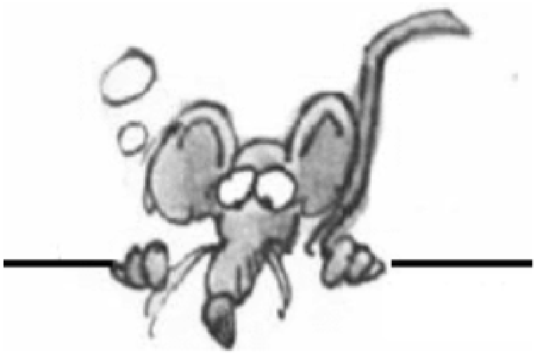
Sandy Berger, CompuKISS
www.compukiss.com
sandy (at) compukiss.com

Is Windows 10 spying on me? I have been asked this question over and over. My answer may surprise you!

There has been considerable publicity about Windows 10 being used as a spying tool for Microsoft. Blogs and even some fairly reputable websites have jumped on this bandwagon. Most of this publicity is aimed at making headlines to increase readership. As you well know, today’s news is dominated by racy headlines, even if they are sometimes trumped up. Some of this bad Microsoft publicity is focused on increasing public paranoia to sell products.

One of my followers recently sent me a copy of an audio interview of Dr. Katherine Albrecht in which she trashed Windows 10 in an article entitled “Windows 10 is full blown electronic tyranny.” Dr. Albrecht is a very intelligent, articulate, and well-educated lady. In this interview she says that Windows 10 keeps the microphone turned on all the time to bug homes and offices across the country. She says that Microsoft is making a copy of every file you create with Windows 10. However she also uses this interview to promote her Startmail product which is supposed to keep you safer.

Let’s see if I can negate a few of her claims. First, Windows 10 uses your microphone to let you verbally communicate with Cortana, their new virtual assistant. Cortana is not listening all the time unless you change the settings and request that she does so. With the default settings, Cortana will only listen when you press the microphone button just like you would press the home button on an iPhone or iPad to ask Siri a question. Also, it is very easy to turn Cortana off or alternately to turn off your microphone completely.



NIBBLERS

By Jeannine Sloan

Dr. Albrecht also says that Microsoft is sending the entire contents of all Windows 10 hard drives to their servers. Simply put, Microsoft is not copying all your files or documents. In the last month Windows 10 has been installed on 75 million devices. If Microsoft were to keep a copy of every one of those hard drives, we would be talking about thousands of Petabytes of data. To give you an idea of how much data that is, it is estimated that the entire written works of mankind from the beginning of recorded history in all languages would take up about 50 Petabytes. Simply copying that amount of data would take years plus an astronomical amount of storage space and electricity.

Another complaint is that Windows 10 can be set up to share Wi-Fi passwords. Again this is not turned on by default. You must choose to use it, and when you do, you must authorize it and the passwords are encrypted.

I can sum up the reality of this situation in one simple statement. With Windows 10, Microsoft is doing no more snooping, spying, or collecting data than other large companies like Apple, Google, and Amazon. I have read the Microsoft Services Agreement, the Windows license agreement, and the Microsoft Privacy Statement carefully. I have also looked at several privacy documents from Google and Apple. They all have similar clauses.

The bottom line is that if you use any cloud storage like Microsoft’s One Drive or Apple’s iCloud, if you use an online email system like Gmail, Outlook, etc., or if you use services to sync your documents between computers and/or mobile devices, there is a copy of your data out there in the Cloud. Your cell phone provider, your ISP, your cable provider, your smart TV, and even your car knows a lot about you, as well. Facebook, Twitter, Instagram and other social media sites probably know more about you than you might ever expect. Most companies are using your data to learn more about you, whether to give you better service or to send you targeted ads. If they are subpoenaed, they will give your information to the lawful agencies, but then if you have drawn that kind of attention to yourself, those agents may be busting down your door and seizing your computers as well.

Right now Microsoft, Google, Apple, and Amazon are not spying on you or willfully giving the contents of your hard drive to anyone. Of course, an entire company could go bad, but currently you are at more of a risk from the bad guys and hackers than you are from the major companies. There are a lot of really good security people constantly monitoring the dealings of all the major companies.

So don’t worry about Windows 10. It is no worse than Windows 7 or Mac OS X. If you want to be more secure, don’t subscribe to any cloud services, don’t use online email, and don’t expect your data to sync between devices. If you want to be really secure don’t access the Internet on your computer or tablet, don’t use a cell phone, and don’t buy a smart TV or any of the new Internet-connected devices, including a car.

Of course, if you do that you will be going back in time about 30 years. I know I wouldn't want to give up the knowledge, connectivity, productivity or entertainment that we have gotten from these devices.

If you want to keep using Windows 10, but want a little more security, here is how you can adjust the settings.

By Jeannine Sloan, Member, Twin Cities PC Group www.tcpc.com

Selected Nibblers

Stolen Consumer Data Is a Smaller Problem Than It Seems
Data breaches are an example of a threat that looks worse than it turns out to be. The sheer size of hackings shocks and startles when the attacks are first reported, but it's rare that journalists check on the actual consequences. "The bad guys are getting good," said David Robertson, the publisher of The Nilson Report, a data provider for the card industry, "and the good guys are getting even better."
http://nyti.ms/1WMeoIC

Foiling Malicious Links and Files
Every day, malicious websites and attachments try to trick you into downloading their
dangerous payload. Fortunately, there are websites and tools to help you determine if it's safe and what might be a trap designed to steal personal information and money.
http://bit.ly/1IfPoG0

One of the sites recommended is: VirusTotal is a free service that analyzes suspicious files and URLs and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware. Bookmark it.
https://www.virustotal.com

Device Security
Whatever brand of tablet or cell phone you use it's always good to install and regularly use an anti-malware app. TechRepublic recommends Malwarebytes. Always run a scan after installing an app (no matter from where the app was installed).
From TechRepublic

Next-Generation Firewall
A next-gen firewall can look inside the envelope to check it also doesn't contain dangerous content. Likewise, it can have smarter rules so you can say "block all known dodgy addresses" rather than having to explicitly state "don't allow mail from Joe the scammer at number 23 Spam Lane." The great thing about these smart rules is that you can transfer the responsibility for keeping an updated list of dodgy addresses to your firewall vendor rather than maintaining them manually yourself.
http://tinyurl.com/o4749p5

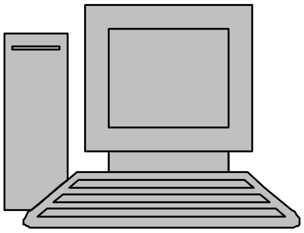
Considerations for Safer Downloading
Here are a few guidelines for reducing the risk of computer infection when you download and install software.

First: CREATE a restore point as a safety net.
Download ONLY from trustworthy sites (CNET, ZDNET, Microsoft) and be cautious even then.
AVOID any site that uses a download manager.
BE CAREFUL of sites that display multiple ―download‖ buttons.
If downloading a video AVOID an .exe extension and/or a video player.
AVOID using default install, use ―Custom‖ so you can uncheck any included crapware
NOTHING is free. The EULA will tell you if there is bundled crapware. Read the EULA.
This list was shared with me by a professional computer technician.

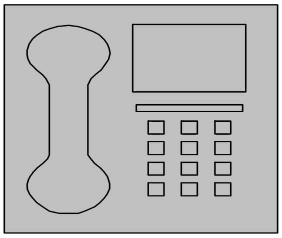
Malware Bots
Common crime ware functions built into bots include:
Logging your keystrokes to steal online usernames and passwords
Searching through your files for interesting data to steal.
Tricking you into clicking on ads to generate pay-per-click revenue
Posting "recommendations" for your friends on your social networks.
Acting as a proxy, or relay, and charging rent to other crooks so they can use your internet connection to cover their tracks.
Mapping out your network from the inside to assist with future attacks.
Attacking other people's websites, making you look like the crook.
Sending out spam, often in vast quantities
Updating the running malware to add new features and stay ahead of your defenses.
Downloading more malware at the whim of the crook who is in control.

Read more at: http://bit.ly/1OkhkJn

Avoid Malware
Anytime I fear that I may have clicked on something suspicious or I sense that my computer is running slower than normal, I always run Housecall just to make sure that my computer hasn't been infected with a virus or malware. This is step 2 of the article at this site:
http://tinyurl.com/psv9npy



HelpLine



HelpLine is a **free** service to members of CFCS only. The following volunteers have offered to field questions by **phone or via e-mail** with software and hardware problems listed below. Please be considerate of the volunteer you are calling.

As a **free** service, you should not be asked to pay for help or be solicited for products or services. If anything to the contrary occurs, please contact the HelpLine coordinator immediately. Their names will be removed from the list.

Additional volunteers are needed in some existing categories and for new categories. If you are interested, please contact the **HelpLine** coordinator at e-mail: ***helpline@cfcs.org***

Please Note - This is a service for CFCS MEMBERS ONLY **HelpLine Listings**

Digital Photography & Video

Ken Larrabee	407 365-2660	anytime
KLarrabee@cfl.rr.com		

DOS

Stan Wallner	407-862-2669	5 pm-7 pm
smwallner@yahoo.com		
Kris Hestad	321-459-2755	
kris.hestad@surfdogs.com		

Hardware

Ken Larrabee	407-365-2660	anytime
Stan Wallner	407-862-2669	5 pm-7 pm
smwallner@yahoo.com		

MS ACCESS

Arvin Meyer, MVP	407-327-3810	7 pm - 9 pm
Access-sig@cfcs.org		

MS Office Products:

MS Word, Excel, Power Point, Outlook and Access

Doug Gabbard	(e-mail only)
Dougga@gmail.com	

Security

Arvin Meyer	407-327-3810
Access-sig@cfcs.org	

Networking - Home or Office

Doug Gabbard	e-mail only
Dougga@gmail.com	

SQL-Server

Arvin Meyer	407-327-3810
Access-sig@cfcs.org	

Windows

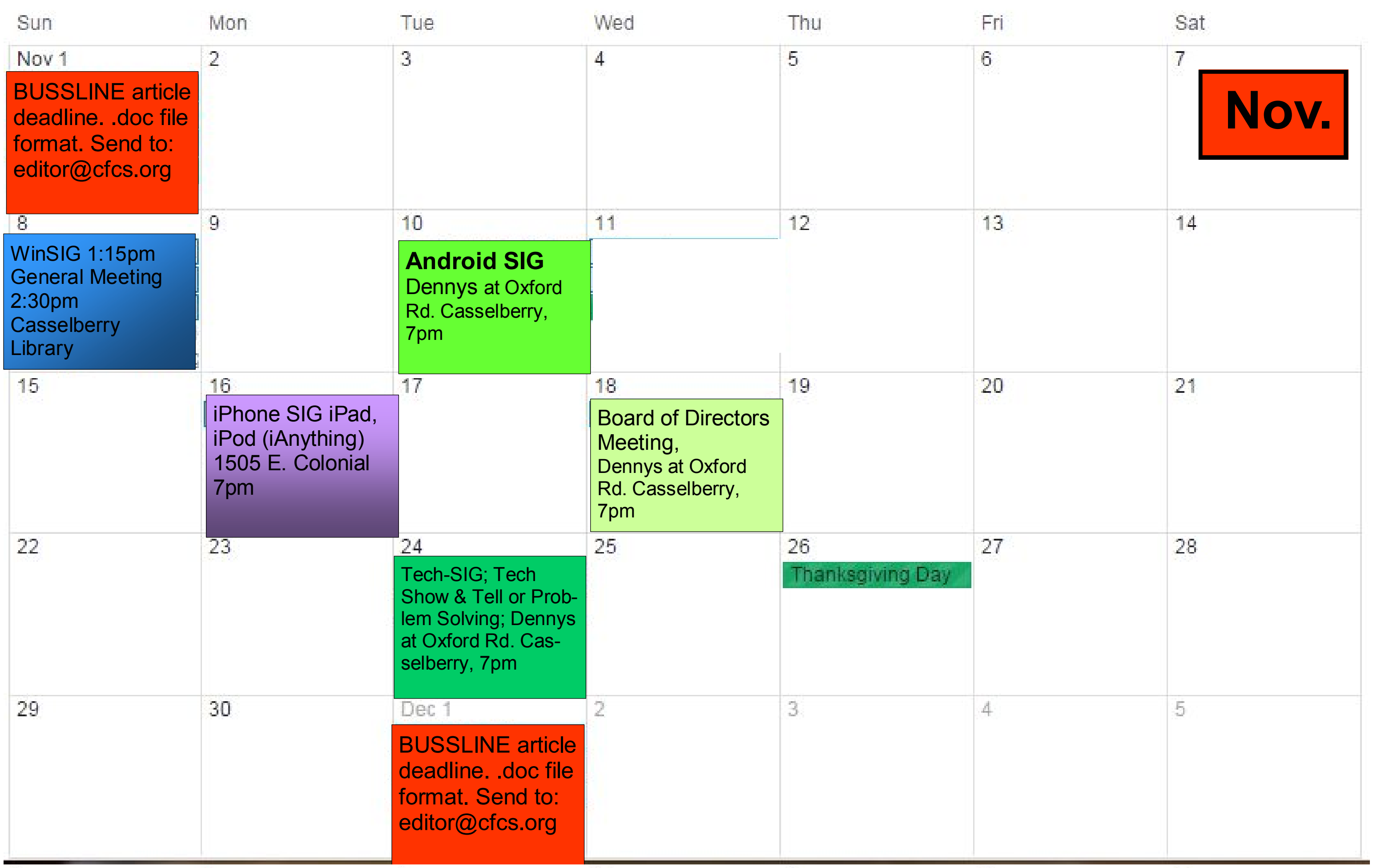
Hewie Poplock	407-362-7824 5 pm-7 pm
hewie@hewie.net	
Kris Hestad	321-459-2755
kris.hestad@surfdogs.com	

WinZip

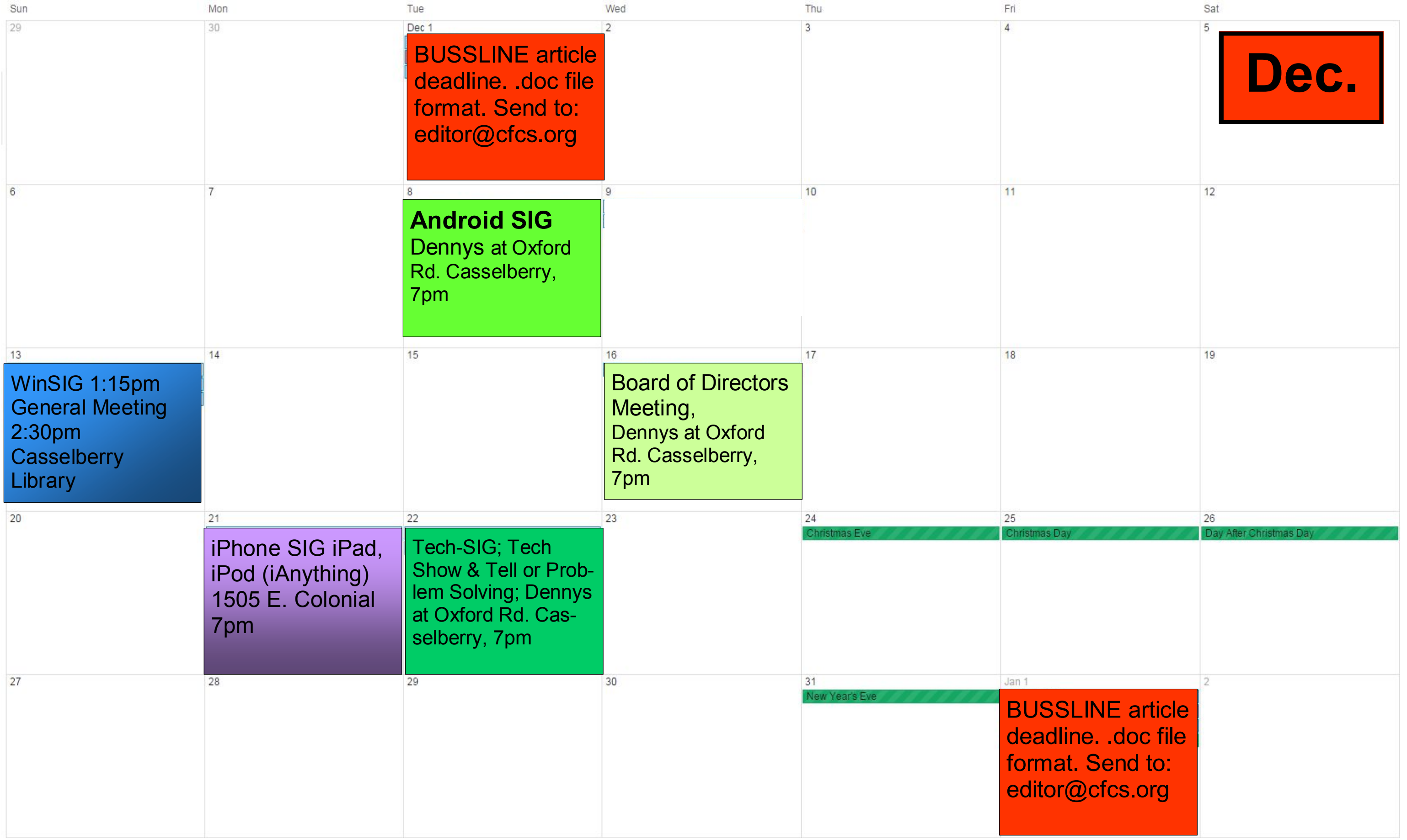
Arvin Meyer	407-327-3810
Access-sig@cfcs.org	

Wireless Routers

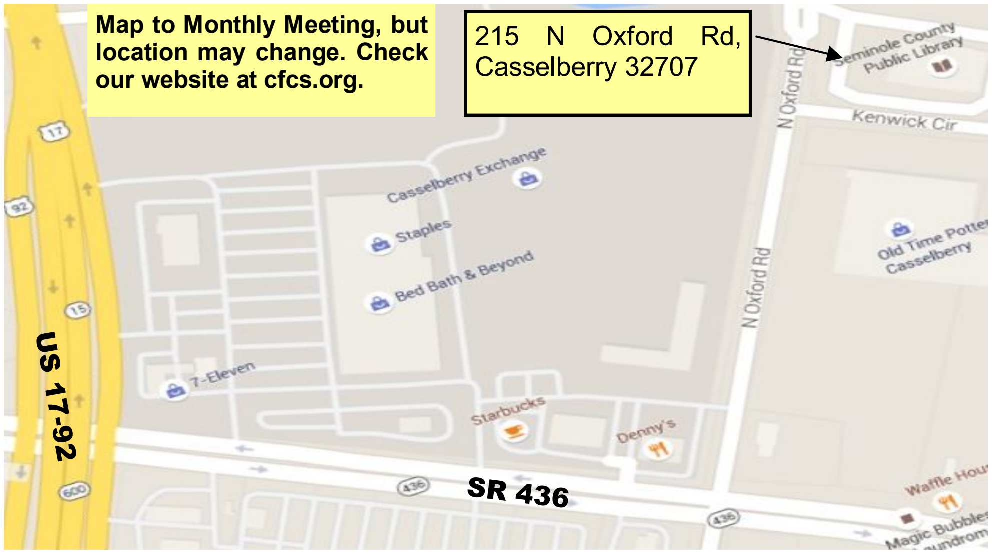
Kris Hestad	321-459-2755
kris.hestad@surfdogs.com	



Sun	Mon	Tue	Wed	Thu	Fri	Sat
Nov 1 BUSSLINE article deadline. .doc file format. Send to: editor@cfcs.org	2	3	4	5	6	7 Nov.
8 WinSIG 1:15pm General Meeting 2:30pm Casselberry Library	9	10 Android SIG Dennys at Oxford Rd. Casselberry, 7pm	11	12	13	14
15	16 iPhone SIG iPad, iPod (iAnything) 1505 E. Colonial 7pm	17	18 Board of Directors Meeting, Dennys at Oxford Rd. Casselberry, 7pm	19	20	21
22	23	24 Tech-SIG; Tech Show & Tell or Problem Solving; Dennys at Oxford Rd. Casselberry, 7pm	25	26 Thanksgiving Day	27	28
29	30	Dec 1 BUSSLINE article deadline. .doc file format. Send to: editor@cfcs.org	2	3	4	5



Sun	Mon	Tue	Wed	Thu	Fri	Sat
29	30	Dec 1 BUSSLINE article deadline. .doc file format. Send to: editor@cfcs.org	2	3	4	5 Dec.
6	7	8 Android SIG Dennys at Oxford Rd. Casselberry, 7pm	9	10	11	12
13 WinSIG 1:15pm General Meeting 2:30pm Casselberry Library	14	15	16 Board of Directors Meeting, Dennys at Oxford Rd. Casselberry, 7pm	17	18	19
20	21 iPhone SIG iPad, iPod (iAnything) 1505 E. Colonial 7pm	22 Tech-SIG; Tech Show & Tell or Problem Solving; Dennys at Oxford Rd. Casselberry, 7pm	23	24 Christmas Eve	25 Christmas Day	26 Day After Christmas Day
27	28	29	30	31 New Years Eve	Jan 1 BUSSLINE article deadline. .doc file format. Send to: editor@cfcs.org	2



Map to Monthly Meeting, but location may change. Check our website at cfcs.org.

215 N Oxford Rd, Casselberry 32707

More security vulnerabilities disclosed for phones, carriers

Ira Wilsker, *Assoc. Professor, Lamar Institute of Technology; technology columnist for The Examiner newspaper www.theexaminer.com; deputy sheriff who specializes in cybercrime, and has lectured internationally in computer crime and security.*

If you are like me, I carry my cell phone everywhere, carrying on voice conversations, sending and receiving text messages, utilizing countless apps, and surfing the Web. Until recently, I gave very little heed to the security of these external communications as our smart devices are supposed to be somewhat secure. GSM carriers like AT&T and T-Mobile utilize encryption to make communications secure; CDMA carriers like Sprint and Verizon also claim to have secure networks. Yes, I do have a major security app on my Android phone that scans new apps and text messages for malware, as well as protects from hazardous websites. Google created Android to be secure, with apps running in a somewhat closed memory space, called by some a "sandbox," which is supposed to prevent purloined apps from talking over the phone. IPhone fanatics, along with many Apple fans in general, believe that their devices are immune to attack, as Apple would not dare to allow any threats to harm their beloved devices.

Now welcome to the world of stark reality. In a recent column, I wrote about two newly revealed vulnerabilities, known as "Stagefright" and "Certifigate," that may threaten the security, safety and privacy of nearly a billion smart phones and tablets. Since then, others have come forward demonstrating previously unannounced security vulnerabilities that threaten the security of our smart phones, often including both iPhones and Android devices in their threat assessments.

One of these newly disclosed threats explicitly targets the most technology innocent and uninformed among us. Appropriately called "grandma malware," this clever piece of malware sneaks onto Granny's phone using a compound method of infection designed to defeat many of the simplest security precautions. While recently updated Web browsers and desktop security software, as well as updated phone operating systems, have likely patched the vulnerabilities, Granny's often older and unpatched computer and phone may be vulnerable. The first step in the infection sequence occurs when the victim downloads an innocent looking app, often a game or simple photo utility, onto their computer using any one of the older versions of most of the common Internet browsers, which are still in wide use. This small utility, explicitly designed to appeal to a "grandma," does not itself contain any malware, and will pass the scrutiny of many of the less sophisticated desktop security products. This utility sits quietly and apparently innocently on the victim's computer, often performing its intended tasks. The app surreptitiously monitors Web surfing until Granny logs on to an app store, such as the Google Play Store. The malicious utility captures the logon and connection information from the app store; with this information, the malware is invisibly downloaded wirelessly to the smart device, installing itself on Granny's phone. Once installed, this malicious app immediately gathers personal data from the phone and sends it to parties unknown. Even if this malware is detected and removed in a subsequent security scan by a third party security utility, it is too late; all of the personal information was stolen within seconds of the app being installed on granny's phone. Granny's private information has just been stolen, and she might very well become an identity theft victim; as is common in criminal enterprises, the most vulnerable among us are more likely to be victim-