

Abort,
Retry,
Ignore....

Founded 1984 **ARI** is the
Official Newsletter of
Computers Are Easy User Group

August 2015

Volume XXXIII Issue 8

Confirmed meeting dates

August 22
4th Saturday
Room B

Sept 26
4th Saturday
Room A

Oct 24
4th Saturday
Room A
:::

Check
www.caeug.net
for confirmed
meeting dates
MEETING
PLACE
is the
Glenside Public
Library
:::

Visitors
Welcome
HOPE TO SEE
YOU THERE!!



The August 22 presentation will be a discussion about present and past issues of the ARI by our members.

The discussion will be moderated by
Kathy Groce, John Spizzirri and Michael Goldberg

Meeting will be held in Room A
8/22/15 4th Saturday



Lamp Post 172

August 2015

by John Spizzirri

Just as a clarification, long URLs have been shortened by using the Google URL shortener **(1)**. To use it you must have a GMail account.

1) <https://goo.gl/>

Want to lose weight, quit smoking, or reduce some other activity? Play Tetris (for at least 3 minutes). That's the message in a scientific study published in Science Direct **(1)**. You can read the highlights of the article at the linked URL or you can read the whole article for about \$40. I saw the reference to the article in the International Business Times **(2)**. You can test this finding by playing Tetris **((3), (4), (5))** on line.

Con't pg 2

Table of Contents

Page

- 1 Lamp Post 172 by John Spizzirri
- 6 Five Things the Tech Industry Won't Tell You by Greg Skalka
- 9 Cybercrime and Phishing by Kathy Frey
- 10 August 2015 DVD of the Month List

- 1) <http://goo.gl/jcWCjG>
- 2) <http://goo.gl/3LdKpw>
- 3) <http://www.freetetris.org/index.html>
- 4) <http://www.tetrisfriends.com/>
- 5) <http://www.tetris24.com/>

If you are planning to give away any money to charity, you may want to check Charity Navigator (1), a charity rating resource. They list many local and national charities with various rating measures.

- 1) <http://www.charitynavigator.org/>

John McAfee ((1), (2)), founder of McAfee Associates (an anti-virus program company), writing for International Business Times about the Internet of Things (IoT (3)) stated that the risks of IoT are not all known. The IoT is the integration of sensors into various items or things that can be connected to the Internet. For instance, a refrigerator could be connected to the Internet. The sensors in the refrigerator could detect that a stock of a commodity (milk, bacon, Twinkies, etc.) was running low. Once detected, it could e-mail the refrigerator owner about the low stock or it could order more directly from a supplier. The risks of IoT that are known are scary. A demonstration at this year's Defcon (4) showed how certain cars could have their brakes 'turned off' by a cracker on a cell phone. The problem that McAfee sees is that the 'things' manufacturers know all about how to make things but nothing about connecting to the Internet. In the previous example, can the refrigerator maker protect the owner from crackers? Without proper safeguards a cracker could turn off the refrigerator or order huge amounts of food. On a more serious note, the article mentioned a man that "took control of a United Airlines flight simply by hacking into the entertainment system." In another article (5), McAfee said, "Can we survive the overwhelming self-delusion of companies who believe that their data is secure, or companies who have been hacked and tell us that the holes in their system have been closed?" I think he is right.

- 1) https://en.wikipedia.org/wiki/John_McAfee
- 2) <http://goo.gl/EO6jun>
- 3) <https://goo.gl/MYINqT>
- 4) <https://www.defcon.org/>
- 5) <http://goo.gl/o9LL37>

In a different article, a cracker claims that he can use GM's OnStar (1) app to remotely open and start your OnStar equipped car ((2), (3)). If you own an OnStar car you may be interested in this article. Chrysler (4) had a major recall (5) due to cracking of it Jeep brand, Internet connected cars.

- 1) <https://www.onstar.com/us/en/home.html>
- 2) <http://goo.gl/elG01Y>
- 3) <http://goo.gl/1s95KJ>
- 4) <http://www.chrysler.com/en/>
- 5) <http://goo.gl/jC1KH6>

The New York Times put out an article with a quiz **(1)** to help you know if your personal data may have been exposed. It includes dates when data may have been exposed. There are some helpful hints on how to avoid exposure in the future.

1) <http://goo.gl/1TAQw0>

On a similar note, BGR [a website] put out an article on how to avoid seven of the most common on-line scams **(1)**. Each scam is explained. What you must do to avoid the scam is also detailed.

1) <http://goo.gl/hP4rWI>

If you use BitDefender as your anti-virus product, you will definitely be interested in this article **(1)**. BitDefender admitted a data breach. A cracker claims he stole unencrypted passwords. BitDefender is a Romanian company. The company said that the number of stolen user names and passwords was less than one percent of their data base. If you use BitDefender, you may want to change your password TODAY. The new password should be at least eight characters long, include upper and lower case letters, have at least one numeral, and at least one symbol. You can check your password for 'crack-ability' at Gibson Research Corporation (GRC **(2)**). I DO NOT recommend the word password as a password, but here is a way to make a password much harder to crack. Using the word 'password', which is eight characters long, capitalize the p, change the s's into 5's and add a period at the end. Using the GRC haystack checker the time to crack 'password' is 18 minutes but the time to crack 'Pa55word.' is over 200,000 centuries. Those numbers are just estimates and do not take into account that password guessing programs guess the 10,000 most popular passwords **(3)** first and then tries variations of those 10,000 next before guessing using a dictionary.

1) <http://goo.gl/G9A7Sb>

2) <https://www.grc.com/haystack.htm>

3) <http://goo.gl/KL1nr9>

You may have noticed that 'Patch Tuesday' **(1)** is now a thing of the past with the advent of Windows 10. Since the end of July my Windows 7 machines have had at least three updates that did not coincide with a Tuesday. My machines had to reboot with each update. Fortunately, there was no inconvenience to me - these times. Some of the pundits are calling this a good thing **((2), (3))**. I think that updates should not require a reboot - just like Linux updates. Windows 7 is not the only OS to get updates. Windows 10 only two weeks after its release has had five patches **(4)**. Gee, I had been led to believe by Microsoft (MS **(5)**) that the early testers, the Windows Insider Program **(6)**, were to have worked out all the bugs. I guess the true 'beta release' **(7)** was to the public. Windows 10 updates began causing problems even before the general release because of a Nvidia **(8)** driver issue that caused problems for people who use multiple monitors **(9)**. The Current Branch for Business (CBB **(10)**) patches are for 'mission critical' business customers who will not get patches until all the rest of us, the beta testers, have had the patches forced on us for a few months. The bugs, if any, will be worked out in the consumer community before big business gets the patches **((11), (12))**. To be fair the CBB users will not get Windows 10 for free. The testing of the patches is free to them.

- 1) <http://goo.gl/PO2dla>
- 2) <http://goo.gl/EDGxyB>
- 3) <http://goo.gl/F2dnux>
- 4) <http://goo.gl/ehcWZP>
- 5) <https://www.microsoft.com/>
- 6) <https://insider.windows.com/>
- 7) <https://goo.gl/S1oyFq>
- 8) <http://www.nvidia.com/page/home.html>
- 9) <http://goo.gl/TgvWQq>
- 10) <http://goo.gl/ArnCNZ>
- 11) <http://goo.gl/vGxFBV>
- 12) <http://goo.gl/QX52xN>

Some of the unexpected behavior of Windows 10 do not require patches (they must be undocumented features). Windows 10 shares your Wi-Fi password with all your Skype contacts, Outlook contacts, and Facebook friends ((1), (2)) if they are in range of your Wi-Fi. Here is the step by step to disable (3) this 'feature'. Windows 10 spies on you, your content, and your on line activity (4). ZDNet does not think this a problem (5). I think that ZDNet believes that everybody reads the small print. A quote from the BGR article is a quote from the MS privacy statement with Windows 10. I'll include it here because it is disturbing.

"Finally, we will access, disclose and preserve personal data, including your content (such as the content of your emails, other private communications or files in private folders), when we have a good faith belief that doing so is necessary to: 1. comply with applicable law or respond to valid legal process, including from law enforcement or other government agencies; 2. protect our customers, for example to prevent spam or attempts to defraud users of the services, or to help prevent the loss of life or serious injury of anyone; 3. operate and maintain the security of our services, including to prevent or stop an attack on our computer systems or networks; or 4. protect the rights or property of Microsoft, including enforcing the terms governing the use of the services – however, if we receive information indicating that someone is using our services to traffic in stolen intellectual or physical property of Microsoft, we will not inspect a customer's private content ourselves, but we may refer the matter to law enforcement."

Here is a way to minimize the spying ((6), (7)). Even though you have turned off the spying (as much as possible) Arstechnica says that Windows 10 still spys on you (8). Now we will get to the lesser annoyances. Windows 10 uses your bandwidth (9) to install patches on other people's machines when you are on a public network in a fashion similar to bittorrent (10). Windows 10 automatically changes your default web browser to Edge (11) upon installation (12). Also, Windows 10 wipes your child safety settings (13) when upgrade from 7 or 8. If you have created child safety settings in the past, you know how tedious this is. After the install, you have to do it again. Lastly, as of this writing, patches for Windows 10 are creating problems (14) including an endless crash loop.

- 1) <http://goo.gl/ohX4YD>
- 2) <http://goo.gl/NvQCtp>
- 3) <http://goo.gl/Lw7rr0>

- 4) <http://goo.gl/ZmQvq3>
- 5) <http://goo.gl/upwX8O>
- 6) <http://goo.gl/wDLaQV>
- 7) <http://goo.gl/UqSfM4>
- 8) <http://goo.gl/BRGppW>
- 9) <http://goo.gl/EtlE1N>
- 10) <https://goo.gl/tEGTgz>
- 11) <https://goo.gl/k0Y13m>
- 12) <http://goo.gl/WRCuU3>
- 13) <http://goo.gl/dBZ8UB>
- 14) <http://goo.gl/e17nF2>

Installation of Windows 10 has its own set of troubles. To start it off is an article about how you hope the install will go **(1)**. MS employee, Yusuf Mehdi, upgrades from Win 7 to Win 10 without a hitch. Next we have CNet's article on how to upgrade or install Win 10 on any PC **(2)**. I will emphasize the one paragraph. There are no guarantees, so BACK UP your stuff before starting. Once started or complete, there is no going back to what you had. This is a one way upgrade. Next there is a way to install without Windows Update **(3)**. This article gives you the steps to create media (DVD or flash drive) to install a 'fresh' copy of Windows 10. The download site for the ISO file is here **(4)**. If the Cheatsheet article is not clear try the Verge **(5)**. Here is an error that some people got while trying to upgrade **(6)**. Here is a list of issues some people have had while installing Windows 10 **(7)**. Here is a check list to check before upgrading to Windows 10 **(8)**. John Brandon has the attitude that I have taken - wait until most of the issues have been fixed **(9)**. If you feel that you must jump now, you can go to the nearest Microsoft Store **(10)** and they will install it for you for free, if you qualify.

- 1) <http://goo.gl/RjYhNj>
- 2) <http://goo.gl/3bnCe1>
- 3) <http://goo.gl/7llqM7>
- 4) <http://goo.gl/f6oLon>
- 5) <http://goo.gl/SXAmZH>
- 6) <http://goo.gl/BRCw4D>
- 7) <http://goo.gl/KD6DwW>
- 8) <http://goo.gl/yfsVko>
- 9) <http://goo.gl/Bqlyb1>
- 10) <http://goo.gl/mSP3Ah>

Here are some of the reported bugs so far **((1), (2), (3), (4), (5))**.

- 1) <http://goo.gl/MWXd0t>
- 2) <http://goo.gl/4mnnMa>
- 3) <http://goo.gl/3R2OO6>
- 4) <http://goo.gl/5x0zSa>
- 5) <http://goo.gl/i6gr24>

A trojan that is going around was discovered by Cisco bloggers **(1)**. It is much like bit locker **(2)**. It

works like this. You receive an e-mail allegedly from Microsoft. That is the tip off. Microsoft will NEVER send you an e-mail (unless you are corresponding directly with them). There is a link in the e-mail to upgrade to Windows 10. Once you click the link, your hard drive will be encrypted and you will be extorted for some amount of Bitcoin (3) amounting to \$300 or more. If you get an e-mail from MS, delete it.

- 1) <http://goo.gl/EifLJV>
- 2) <https://en.wikipedia.org/wiki/BitLocker>
- 3) <https://en.wikipedia.org/wiki/Bitcoin>

Between you, me and the LampPost, that's all for now.

President's Corner **Five Things the Tech Industry Won't Tell You**

By Greg Skalka, President
Under the Computer Hood User Group, CA
February 2015 issue, Drive Light
www.uchug.org president (at) uchug.org

In a nod to the Wall Street Journal Sunday's imaginative, interesting and informative "10 Things . . . (xxx) Won't Tell You" columns, I offer my half-sized version. The tech industry's annual new product celebration, CES (Consumer Electronic Show), occurred in January. I've never attended, but I enjoy reading about the latest tech items presented each year.

Each year brings a new batch of innovative products that get the favorable buzz. Sometimes items at the show succeed in the marketplace, while others never make it to prime time.

1. 'The latest is not necessarily the greatest.'

The main purpose of a lot of new products is often not to help the customer but to make money for the tech companies. Occasionally this results in products that despite a big marketing effort are not well received by consumers. It may be due to a company going in the wrong direction, hastily putting out a shoddy product or attempting to pass off a few changes (some perhaps not really wanted by consumers) as a new product.

Windows 8 is an example of a desire to sell something that the customer really does not want. Microsoft seems to get it right in terms of operating systems only about every other attempt. They were very successful with Windows 98, but then disappointed with the release of Windows Me (Millennium Edition). They captured almost all the market with the popular Windows XP OS, but then followed it up with poorly-received Vista.

After correcting their mistakes in well-received Windows 7, their successor, Windows 8, went in a direction most computer users did not want to go. Since Microsoft has decided that they must skip the number nine, all we can do is hope Windows 10 is an improvement when it is released this year, as our time with Windows 7 is limited (mainstream support ended on Jan. 13; extended support, which includes free security updates, will end in five years).

Unfortunately, Microsoft continues to irritate me with their new versions of Office. It is a very powerful application but most users only scratch the surface of its capabilities. I use it daily for

work, but never to its fullest potential. Yet they continue to add additional obscure features and greatly change the familiar user interface to let them somehow justify selling a new version every other year or so. Now they want to sell it by subscription, so users can become just a revenue stream.

And let's not get me started on Microsoft Bob.

2. 'Your old stuff probably still works just fine for what you need.'

Some consumers are enamored with the latest thing and must upgrade whenever possible. It seems to me that these are the customers Apple is often targeting with their new smart phones and tablets. Tech companies would like their customers to think like some car buyers used to (and some maybe still do), and trade up to their latest product every year or two. In most cases, the product the consumer already has meets most if not all of their present real needs. Just as with automobiles, "trading in" for a new smart phone, laptop, camera or office suite too often can cost a lot with little increase in benefits.

A number of PC users hung on to Windows XP a lot longer than Microsoft would have liked. Though the poor reputations of Vista and Windows 8 contributed, a lot of XP users resisted switching because XP met their needs. Businesses were particularly reluctant to switch. I am presently using three XP computers at my work, a small telecom equipment design firm. I also still have a couple of XP computers at home (I wrote this column on one), though I'm definitely phasing them out because of security concerns.

A lot of technology costs a lot when initially introduced, but drops in price once it is more widely adopted and production volumes increase. Staying off the cutting edge can save money but still provide a good user experience.

3. 'This new stuff may seem great, but it is still a long way from reality.'

Highly innovative new products can capture the imagination, but most successful new products are the result of iterative development. These iterations can require years to finally come up with an implementation that is cost-effective for consumers.

I was excited about Google Glass when I first heard about it a few years ago. I'd hoped by now it would have had greater availability and a lower price, but instead Google has just announced that it is halting production of this model. I am encouraged that Microsoft is working on the HoloLens device, but I expect I'll be waiting a while longer to personally experience this type of device. With luck Google will continue development of Glass as well; I'd hate to see it become the Segway of computing device.

It also seems to be taking a long time to get autonomous cars into the hands of consumers. The Google Self-Driving Car project has been in existence for a number of years, having logged nearly 700,000 autonomous miles. A new prototype without human controls will begin testing this year. A number of major auto manufacturers are also at work on autonomous cars. Google believes that it will be able to offer a self-driving car to the public between 2017 and 2019. The legal issues may take as long to work out as the technical ones, however. Meanwhile, we may get there piecemeal as car-makers offer features like self-parking (for parallel parking) and auto braking now

4. 'New technology may provide benefits, but there are usually unintended consequences.'

Almost every new technology introduced has resulted in job losses somewhere in the

economy. The automobile put a huge dent in buggy sales. Streaming video wiped out most of the jobs involved in video disc rental. Computers and robotics greatly reduced factory employment. Digital cameras decimated the photographic film industry and computers and tablets have reduced the need for photo prints.

These technologies have of course created new jobs of different types, but this forces great change on the industries and employees. Email and social media have greatly reduced the number of letters delivered by the Postal Service, so it has had to recast itself as a deliverer of Amazon packages. Unskilled labor is being pushed out as almost all workers, from the burger flipper to the airline pilot, must deal with video displays and electronic controls on the job.

The Internet has revolutionized communications, education, shopping, entertainment and our relationships. Smart phones and social media have greatly changed our culture and our society. We get our news, find our jobs and pick our mates using the Internet. Crime has followed the technology path to our money; it is not in the banks, but in our personal information. Identity theft, phishing, cyber terrorism, sexting and laws against texting while driving are all unintended consequences of our new technology.

Our technology may have had a hand in changing our planet's climate and it may ultimately provide us with a remedy, but some initial tech solutions have provided mixed results. Nuclear power has the promise of carbon-free energy, but radioactive leaks have resulted in disasters. Wind power seems to be a clean renewable source of energy but the large rotating blades may also cause excessive bird kills. The new Ivanpah Solar Electric Generating System in the Mohave Desert may be scorching thousands of birds each year with its concentrated reflected light.

How will new tech advances change our economy and our society in the future? We can guess that widespread use of autonomous cars might make our highways safer, increase productivity by reclaiming lost commute time and wipe out the taxi industry. What other unanticipated effects will it have on us? Police body cameras and other public video surveillance may reduce misconduct, but how will they affect privacy? Will virtual reality technology wipe out the travel industry? Will increased use of online communications and telepresence devices leave us virtually connected but physically isolated in our homes? Will biotech advances turn us into a long-lived, genetically engineered species? Will our computers and autonomous vehicles achieve artificial intelligence? We can never fully predict the future.

5. 'Playing the Luddite is pointless, as technology is transforming our society as we speak.'

The Luddites were 19th century English workers who rebelled against technology by smashing the new machines that were taking their jobs. They were not successful in stopping progress and it is likely modern opposition to technology would be ineffective on the whole. Cell phone networks are being spread through almost every developing country and satellite-based Internet and Wi-Fi installations are increasing, so soon no one will be able to escape technology's reach. Our culture and our relationships are being changed by our technology. We may not be able to put the genie back in the bottle, even if we wanted to.

Cybercrime and Phishing

By Kathy Frey, Member, Computer Club of Green Valley, AZ

Summer 2015 edition Green Bytes

www.ccgvas.org [frey58 \(at\) cox.net](mailto:frey58@cox.net)

At one time or another we all will be a victim of some form of Cybercrime and Phishing. The use of any preventive product is of little help if you don't practice safe computing. Help protect yourself:

1. Watch out for "phishy" emails. The most common form of phishing is emails pretending to be from a legitimate retailer, bank, organization, or government agency. Delete them. Do not open them.
2. Don't click on links within emails that ask for your personal information.
3. Beware of "pharming." This was also known as redirect. In this version of online ID theft, a virus or malicious program is secretly planted in your computer and hijacks your Web browser. When you type in the address of a legitimate Web site, you're taken to a fake site without realizing it. Malicious programs can be either spyware, adware or malware. Run your spyware scanning programs. Malwarebytes is a recommended program.
4. Never enter your personal information in a pop-up screen.
5. Only open email attachments if you're expecting them and know what they contain.
6. Phishing also happens by phone. You may get a call from someone pretending to be from a company or government agency, making various kinds of false claims and asking for your personal information. Quite often it is about some problem with your computer. There is no way they can possibly know if you even own a computer. If you have caller ID, screen your calls, and do not answer calls from phone numbers you do not recognize.
7. If someone contacts you and says you've been a victim of fraud, verify the person's identity before you provide any personal information. Get a phone number and call them back. Or call who they are supposed to represent and ask if that business is making those kinds of calls.
8. Report phishing, whether you're a victim or not. Tell the company or agency that the phisher was impersonating.
9. Don't be embarrassed, take action immediately if you've been hooked by a phisher. If you provided account numbers, PINS, or passwords to a phisher, notify the companies with whom you have the accounts right away. For information about how to put a "fraud alert" on your files at the credit reporting bureaus, contact the Federal Trade Commission's ID Theft Clearinghouse, www.consumer.gov/idtheft.

Most Recent Scam Alerts from the Federal Trade Commission:

Stand up to fake debt collectors - April 10, 2015

Unlocking the code - April 3, 2015

The FTC didn't send that sweepstakes letter - April 2, 2015

Scammers play name game and get caught - March 27, 2015

An invoice today gets the doctor to pay - March 26, 2015

Reluctant to be rude? - March 25, 2015

Don't pay for a vacation to nowhere - March 19, 2015

It's the IRS calling...or is it? - March 12, 2015

Cleaning up without getting cleaned out - March 6, 2015

10. When shopping online be careful and look for boxes that are pre-checked for you to receive offers from them or their partners. Be sure to uncheck the boxes and opt-out if you don't want to receive any communications. Even legitimate retailers count on you not unchecking the boxes to opt-out.

August 2015 DVD of the Month

AdwCleaner - Updated spyware cleaner

ARI - Monthly newsletter

AudioBook - Free audio book

DVDDOMlists - Contents of CDs and DVDs of the Month

Farbar Recovery Scan Tool - Diagnose and fix boot issues

FarBarScanner - Diagnose network connectivity

GrantPerms - Grants permissions to files and folders

JRT - Updated Junkware Removal Tool

ListParts - Lists all partitions

Malwarebytes - Updated anti-malware software

MemberContributions - Things members send me

MiniToolBox - Diagnose network connectivity

NirLauncher - Updated utility launch program

OldTimeRadio - Old radio audio files

PeaZip - Updated zip file encoder/decoder

RKill - Updated Terminates known malware processes

RogueKiller - Updated Terminates and remove malicious processes

SearchMyFiles - Updated file and folder search tool

SophosVirusRemover - Virus remover from Sophos

TailExpert - Log analyzer for windows

Vidiot - Video editor program

Meeting Location and Special Accommodations

The Glenside Public Library address is at 25 E Fullerton Avenue, Glendale Heights, Illinois. Please park away from the building. Thank you. The meeting(s) are not library sponsored and all inquiries should be directed to Mike Goldberg

. Individuals with disabilities who plan to attend this program and who require certain accommodations in order to observe and / or participate in the program are requested to contact CAEUG president, Mike Goldberg at , at least five (5) days prior to the program, so that reasonable accommodation can be made.

Mailing address:

CAEUG
P.O. Box 2727
Glen Ellyn, IL 60138

Members Helpline

Any member with a specific expertise can volunteer to be on the Members Helpline.

Hardware problems, XP, Win 7, Linux
and Virus Removal
- John Spizzirri

CAEUG OFFICERS

President Mike Goldberg
president(at)caeug.net

V.P. (Programs) Roger Kinzie

Secretary Al Skwara

Treasurer John St. Clair

Newsletter Ed Kathy Groce

Board Member Billy Douglas

Webmaster John Spizzirri
webmaster(at)caeug.net