CAEUG Computers Are Easy User Group

Abort,
Retry,
Ignore....

Founded 1984 **ARI** is the
Official Newsletter of
Computers **A**re **E**asy **U**ser **G**roup

September 2016

Volume XXXIV Issue 9

Confirmed meeting dates

September
NO MEETING

October 15
3rd
Saturday

:: ::

Check
www.caeug.net
for confirmed
meeting dates

:: ::

MEETING
PLACE
is the
Glenside Public
Library

:: ::

Visitors
Welcome
HOPE TO SEE
YOU THERE!!

! ! ! NO MEETING IN SEPTEMBER ! ! !

due to Library scheduling conflict

Next meeting will be

on October15 (3rd Saturday)

In ROOM A

Presentation by John Spizzirri
about how he sets up a PC after a Win 7 OS is installed

Room A (10/15/16 **3rd** Saturday)

****

October is National Cyber Security Awareness Month

****

November / December
Meeting date will be
announced in the
November / December ARI

Table of Contents

Page

1 Meeting Information
2 October is National Cyber Security Awareness Month by Ira Wilsker
4 Lamp Post 184 by John Spizzirri
7 Computer Attacks by Dick Maybach

October is 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

Con't pg 3

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.

Lamp Post 184

by John Spizzirri
September 2016

Now that most of you that have Windows 10 are locked into Windows 10 because roll backs can no longer be done. The Windows 10 Anniversary Update prevents roll backs to Windows 7 or 8.1. One thing that should be done is the creation of the Windows 10 Recovery Drive. If everything goes wrong, the Windows 10 Recovery Drive will let you get back the OS. What you need is a USB flash drive. Microsoft **(MS (1))** has instructions to create the drive **((2), (3))**. According to MS, you need a "USB thumb drive with 4 GBs of space or more". PC World Magazine ran an article that claims MS is not telling the truth about the size of the flash drive needed to create the recovery drive. Based on a number of MS web sites the size ranges from 4GB to 8GB **(4)**. One of the people quoted in the article said that 16GB was required. The article recommends that 16GB should be the minimum that you have for the recovery disk creation. Let's face it. If 16GB is the minimum, double it. Microcenter in Westmont has 32GB flash drives for $8.99 **(5)**. At that price you might as well get two so you can have two Windows 10 Recovery Drives.

1) **https://www.microsoft.com/**
2) **https://goo.gl/bA8hqV**
3) **https://goo.gl/GzLEx5**
4) **https://goo.gl/i1Xegy**
5) **https://goo.gl/3lLgNP**

Time is running out for Windows 7. As of October 31, 2016, no new PC may be sold with Win 7 on it **(1)**. Also, retail sales of Win 7 will cease **(2)**. Ed Bott **(3)**, a ZDnet **(4)** writer, wrote an article last January about where to get Win 7 or Win 7 machines. It is still valid for about a month. After that you will need to seek Win 7 in the grey market **(5)** or seek off lease or refurbished machines **(6)** running Win 7. Decisions, decisions, MS forcing your hand is not my idea of good customer

Con't pg 5

relations, but that's just me.

1) https://goo.gl/l9b5qt
2) https://goo.gl/SXkK6W
3) http://www.zdnet.com/blog/bott/
4) http://www.zdnet.com/
5) https://goo.gl/YJLruQ
6) https://goo.gl/bF27lc

The latest Intel **(1)** and AMD **(2)** CPU **(3)** chips will only run Windows 10 **(4)**. The news release was worded so that the reader would think that Linux **(5)**, BSD **(6)**, and OS X **(7)** will be locked out of computing machines after the next generation of chips. This is NOT the case. I do not understand Intel and AMD caving in to MS pressure to disallow previous versions of Windows. I think this lock out is short sighted. I hope MS, Intel, and AMD live to regret this decision. I see this as a golden opportunity for Ubuntu **(8)**, Fedora **(9)**, Linux Mint **(10)**, and PClinuxOS to seize a large part of the desk top market.

1) https://goo.gl/gMsA3d
2) https://www.amd.com/en-us
3) https://goo.gl/n5seSc
4) https://goo.gl/YVFsPm
5) https://www.linuxfoundation.org/
6) http://www.bsd.org/
7) https://www.apple.com/macos/sierra/
8) http://www.ubuntu.com/
9) https://getfedora.org/
10) https://www.linuxmint.com/
11) http://www.pclinuxos.com/

Identity theft **(1)** is still a big problem. About 17.6 million people, 7 percent of U.S. adult population, were victims of identity theft in 2014, the latest year statistics are available from the Bureau of Justice Statistics **(BJS (2))**. How will you know if your identity has been compromised? The Federal Trade Commission **(FTC (3))** has a web site that details the processes of identity theft and what to do about it **(4)**. Some police departments take their responsibility seriously and provide detailed instruction **((5), (6), (7), (8))**. The departments I listed in the previous sentence were from a simple search and are by no means comprehensive. I found it interesting that identity theft was not mentioned on a number of police department's web sites. Identitytheft.gov has the information that let's you know if your identity has been stolen. The steps that should be taken as soon as possible include; file a report with law enforcement, get a copy of the police report, file a report with the FTC on line at **(FTC (3))** or call 1-877-ID-THEFT (1-877-438-4338), report the identity theft to your financial institutions (banks, brokers, credit unions), consider closing accounts, Place a "Fraud Alert" **(9)** on your credit reports at TransUnion 1-800-680-7289 **(10)**, Experian 1-888-397-3742 **(11)**, Equifax 1-800-525-6285 **(12)**. When one of the companies receives a request for a "Fraud Alert", it is expected to notify the other two companies. The "Fraud Alert" only lasts for 90 days but may be renewed. Another way to spot identity theft is by looking at your credit report from each of the credit reporting companies. A while back the companies had

Con't pg 6

to be contacted individually. That is no longer the case. The credit companies have a single site to request any or all three reports **(13)**. The reports do not contain credit scores. There are three ways to request the reports. First is an on line form, second you may call 1-877-322-8228 and third is a printable form **(14)** that can be snail mailed.

1) https://goo.gl/lyNONU
2) https://goo.gl/Nn7U2i
3) https://www.ftc.gov/
4) https://goo.gl/wlFQjl
5) https://goo.gl/AmbTME
6) https://goo.gl/DLP3qH
7) https://goo.gl/zLlW8s
8) https://goo.gl/5ykx7S
9) https://goo.gl/6ptdzU
10) https://www.transunion.com/
11) http://www.experian.com
12) http://www.equifax.com/home/en_us
13) https://goo.gl/9VPEJc
14) https://goo.gl/lknd6V

Burkini **(1)** is a form of Islamic swim wear for women that covers the whole body except the face, hands, and feet. The word is trademarked (with a q and a k) by the swimsuit designer. It is an obvious combination of the words burqa or burka **(2)** and bikini **(3)**. Recently, about 20 French beach towns on the Mediterranean banned burkinis. Enforcement of this ban has led to some controversial police actions where officers required women remove portions of their garments on the beach (not in a changing booth). The French government has overruled these local governments allowing all women to wear whatever they want at the beach. I wonder if the police officers had an assignment of watching people (women) at the beach prior to the ban. Some job **(4)**. Since the 1960's women were free to go topless at the beaches in France. Since the revelation that sunlight causes skin cancer, female toplessness has been on the decline. According to some sources, toplessness at French beaches has dropped to about two percent **(5)**. This is not the first time French police were assigned beach patrol in an effort to monitor female swim wear **(6)**. In the 1920's police had to measure the amount of skin showing to ensure that women were complying with the law that required 'modesty'. Swimming at the beach has been popular for gentry that lived close to the ocean, rivers, and lakes for hundreds of years. Average people could not afford the time or expense. With the advent of the railroads in the 1800's, ocean beach resorts opened with swimming as a method to keep cool during hot summers that became affordable by the middle class. Female bathing costumes showed virtually no skin except the face in the 1700's. The hands and feet began to show in the mid 1800's. By the last quarter of the 19th century, arms, ankles, and hair began to show. Since the beginning of the 20th century, the costumes became more form fitting and the bare thighs started to show. Victoriana magazine has a pictoral about female bathing costumes **(7)**. Comparing the burkini to the swimwear from 100 years ago, I must say that the burkini shows way too much skin to be modest. What is in the minds of these French Imams **(8)** letting French Muslim women run around with naked face, hands and feet? Obviously, the French Muslim religious leadership has dropped the ball.

Con't pg 7

1) https://en.wikipedia.org/wiki/Burkini
2) https://en.wikipedia.org/wiki/Burqa
3) https://en.wikipedia.org/wiki/Bikini
4) https://goo.gl/YCr5OC
5) https://goo.gl/ERo7l1
6) https://goo.gl/bGZAhB
7) https://goo.gl/HTyLdb
8) https://en.wikipedia.org/wiki/Imam

For those of you that have vegetable gardens, the Seed Keeper Company has may tips and (of course) products to help you keep seeds from this year's crop for next spring **(1)**.

1) https://seedkeepercompany.com/

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

Computer Attacks

By Dick Maybach
Member, Brookdale Computer Users’ Group, NJ
June 2016 issue, BUG Bytes
www.bcug.com
n2nd (at) att.net

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

(1) their attack method (how they access your PC, your data, or you),
(2) their behavior (how they get established and perhaps spread), and
(3) their payload (what they do).

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

First consider network attacks, which may not affect your computer at all. The first type, network monitoring is passive and is a digital version of a phone tap; everything you send and receive is recorded by a third party. This is easily done at a public hot spot, and requires only a laptop and widely-available software. It also can occur at ISPs and Internet

Con't pg 8

relay points, either by the facility owner or by government agencies. A second type, the man in the middle attack, is active and is much more specific. Here, a computer is set up to mimic, for example, your Internet bank. If you can be fooled into logging into it, the attacker can capture your password and other account details before forwarding your traffic to the bank site you think you are using. This is more difficult to set up than simple network monitoring and is thus less common.

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

(1) physical access,
(2) social engineering,
(3) Trojan horses, and
(4) unethical suppliers.

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

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

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

Type (2) programs are called stealth software or rootkits, type (3) programs are called viruses, and type (4) are called worms. An interesting form of virus resides in office document as a macro, for example written in Visual Basic and included in an MS Word or Excel file. These can migrate to your master template and infect every document you compose after that. When they first appeared around 2000 macro viruses were serious problems, but office suites now have effective safeguards against most; however, you

Con't pg 9

may wish to check your preferences to be sure. (Although many people use the term virus for all malware, only 17 per cent of it really behaves this way and another eight per cent acts as worms.) Combinations are also possible; for example, a virus can have stealth features. Since rootkits and viruses can affect system programs, their installation often, but not always, requires that the user grant them administrator privileges. A number of vendors offer applications to detect rootkits, but removing one sometimes requires erasing the computer's hard drive and reinstalling the operating system. Many people call type (1) programs Trojan horses, but I prefer to use that term for a malicious program's attack method rather than it's behavior after it becomes active.

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

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

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

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

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

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

Your ultimate defense against all malware is a backup made before your PC became infected. Wiping and restoring your hard disk will almost always restore your system, except in the rare cases where the malware resides in your PC's BIOS firmware, in which case you probably need expert help. Unfortunately, the Unified Extensible Firmware Interface (UEFI) adds a new vulnerability as it includes a writable boot partition on your hard disk. Since the code residing here executes before your operating system; any malware installed there becomes active before any anti-virus program. Re-installing the operating system will probably leave the infected partition unchanged. So far, this is only a theoretical threat. I mention it only to make the point that threats evolve continuously, which requires that you keep all your software, not just your anti-virus programs updated, and conscientiously practice an effective back up discipline.

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

REMINDER

NO September meeting

See you on October 15th
3rd Saturday

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 at . 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	Frank Braman
Webmaster	John Spizzirri
webmaster(at)caeug.net	