OCTOBER 2016 NEWSLETTER

Glendora Seniors Computer Club

A Friendly Seniors Group Serving All Computer Skill Levels
AND to address new technology issues

General Meetings: 2nd & 4th Wednesdays of the month at 1:00 p.m.
Board Meetings 2nd Wednesday of the month at 3:00 p.m.

Volume 21, Issue 10

Halloween, Oct 31st

PROGRAMS BY: **Program Chair: Annemarie Hunt**
(All programs subject to change)

October 12th

Cameras and Photography
- by Wayne Lunde
GSCC member

October 26th

Travel and the Internet

By Annemarie Hunt

GLENDORA SENIORS COMPUTER CLUB
General Meeting Minutes
September 14, 2016

President Annemarie Hunt called the meeting to order at 1:00 PM welcoming twenty-eight (28) Club members and one guest.

ANNOUNCEMENTS:

1) 2016 APCUG International Technology Conference October 21, 22 & 23, 2016 Palace Station Hotel & Casino Las Vegas

2) Nominations are open for 2017 Officers. Connie Lang is still in need of a Treasurer. Election will be held at the December 14th Holiday Potluck Meeting.

3) Board Meeting following today's meeting.

Program: Connie Lang demonstrated various software (Boot Disk for Windows 10, formatting a flash drive, using Windows 10 Backup) and hardware devices (Flash drives, external hard drives) for backing up computers and other electronic devices i.e. Smartphones. Backing up data as

INSIDE THIS ISSUE

well as backing up entire computer with programs like Acronis - mirror image. **http://www.ugr7.com/** website for Gene Barlow and the Acronis backup software. If you are interested in purchasing this program, ask for the Glendora Seniors Computer Club discount. Cheat Sheets (3) will be emailed to members present at this meeting.

Break: Thanked John Button for cookies.

Q & A Ell Fullmer answered questions on the following topics:

1) Location of deleted pictures

2) SD cards for ultimate backup

3) Old Computers can be used for backup

4) Backing up phone pictures

Next meeting: Wednesday September 28th - Mike Schelin owner of "IT Solutions for Business" talking about internet security. Frank Duran providing cookies.

Adjournment: Meeting adjourned at 2:50 pm.

Submitted by: ***Approved By:***

Secretary Ruthann Mayrose President Annemarie Hunt

****

GLENDORA SENIORS COMPUTER CLUB
General Meeting Minutes
September 28, 2016

President Annemarie Hunt called the meeting to order at 1:00 PM welcoming 24 Club members and one guest, Annemarie's friend.

ANNOUNCEMENTS:

1) Reminded us about Gene Barlow's web site **http://www.ugr7.com/** for the Acronis backup software.
2) Programs are planned through February.
3) Checkout and read the Newsletter on line at www.gsccclub.org/Newsletter for information about the club meetings.

Program: Mike Schelin the owner of "IT Solutions for Business" spoke about internet security and some of the steps we should take to protect ourselves from hackers (bots, dark internet), changing and creating safe passwords for all our devices, making a clone (mirror image), or redundant hard drive. Filter out all domains EXCEPT .com, .org, .net. DON'T click on what you don't know. For internet shopping use PayPal or prepaid credit card..

Break: Thanked Frank Duran and Helga Djordjevic for today's cookies.

President Annemarie Hunt took a verbal survey of those present as to what their interests in future programs were—how many have and use the various electronic devices.

Q & A Ell Fullmer

FYI Uber is not available at ONT airport.

Next meeting: October 12th Cameras and photography, member, Wayne Lund.

Christel Mackinnon will bring cookies.

Calendar of future meetings:

October 12, 2016: About Cameras and Photography - Wayne Lunde, GSCC Member

October 26, 2016: Travel and the Internet - Annemarie Hunt

November 9, 2016: Windows 10, Part 2 - Jim Glass

December 14, 2016 - Christmas Party and Elections

Adjournment: Meeting adjourned at 2:30 pm.

Submitted by:

Secretary Ruthann Mayrose

Approved By:

President Annemarie Hunt

****

Submitted Articles authored by various APCUG members and furnished by Judy Taylour of the Santa Clarita Computer Club

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 relay points, either by the facility owner or by government agencies. In 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 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.

****

Back to Basics

Changing to another Email Service

By Jim Cerny, Chairman, Forums Committee, Sarasota Technology UG, Florida

June 2016 issue, Sarasota Technology Monitor

www.thestug.org

jimcerny123 (at) gmail.com

Almost all computer users use email – and you are one of them, right? Have you ever had to change your email address or change to another email provider? Recently here in Florida (and I hear in Texas and California as well) our internet provider Verizon has been taken over by Frontier. As a result of this, EVERYONE had to change from Verizon to AOL for their email. Fortunately their Verizon email address will continue to be accepted by AOL (for now). The purpose of this article is to help you understand what steps are needed to change to another email. I do recommend Gmail because it comes with several other tools provided by Google and you most likely will never have to change to another email address.

Your first task is to go to the website and establish a new email account -- that is get your new email address and password. Please write it down and do not lose it! Once you have your new email ID your major concerns are forwarding your old emails to your new email address, getting your address book (or contact list) to your new email and to notify everyone of your new address. Some emails (such as Gmail) may ask you what your other email address is and automatically bring your contact list and forward any emails from your old address to your new address. They want your email business. But if your address book is not copied over for you then you will have to do it yourself. By all means “ask Google” how to do it. For example, ask Google “How do I get my AOL address book to my Gmail contacts?” What you will most likely have to do is to create a file of your address book by “exporting” it and giving it a file name, then copying that file by “importing” it into your new email. After you do this you need to examine your entire address book, name by name, to see that all the data was copied correctly. You will probably have some editing to do

to straighten things out. For example, some phone numbers may not have been copied over or a nickname may have been placed as the last name, etc.

Next it is helpful to have all your old email “forwarded” to your new email address. This way you do not have to hurry to notify everyone on your list that you have a new email. If this is not possible, you may have to go into your old email and actually forward those important emails to your new email. From now on, only use your new email address.

Finally, send a nice email to everyone telling them your new email address. It also is essential that you read the “help” or “options” for your new email so that you are aware of how to create new email folders, sort your emails, find emails, etc. Although every email can do these basic functions, how it is done may be different on different emails. And if you are converting to Gmail, be sure to check out the many apps that are available to you with your Gmail account ID. Now you are ready to enjoy using your new email.

One word of caution -- what if you have used your email address to establish accounts with various on-line businesses or services? Movie channels, banking, club memberships, etc. may be using your OLD email address as your account ID. Unfortunately, all of these accounts must be changed to your new email ID. This may entail you having to enter all new passwords for all these accounts as well. This can be a real pain if you have many accounts, but there is really no other way around this, sorry. Be sure to write down ALL your IDs and passwords for EVERY service or app which requires an account.

Good luck and please don’t forget to Ask Google anything about your email. You will find very helpful instructions and videos to guide you. Now here’s hoping that you will never have to change your email address again!

******

DO YOU HAVE A QUESTION FOR OUR TECH GUYS, *ELL FULLMER and JIM GLASS*

Fill Out the Form Below & Bring it to the Meeting

Name: _____

Cptr Operating System: Windows 7 ___ Windows 8 ___ Windows 10 ___Mac ___ Other ____

Question:_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Elected Officers

President	Annemarie Hunt	Ajhunt1447(at)aol.com
Vice-President	Connie Lang	Connielang(at)verizon.net
Secretary	Ruthann Mayrose	ruthannmeister(at)gmail.com
Treasurer	Rita Norkin	rin369(at)live.com
Tech Advisor	Ell Fullmer	pakratt(at)gmail.com
Past President	Barbara Denny	Dennyandassoc(at)verizon.net

Have a New

Email Address?

Please Notify Membership Chair: Helga Djordjevic

hdjordjevic(at) verizon.net

Committees & Chairpersons

Program Director	Annemarie Hunt	Ajhunt1447(at)aol.com
Web Master	Ell Fullmer	pakratt(at)gmail.com
Education	Connie Lang	connielang(at)verizon.net
Newsletter Editor	Dan Leddy	ranchitoave(at)yahoo.com
Membership Chair	Helga Djordjevic	hdjordjevic(at)verizon.net
Nominations	Connie Lang	connielang(at)verizon.net
Public Relations	Barbara Denny	dennyandassociates(at)verizon.net
Asset Management	Glen Moore	mooretours(at)earthlink.net
Set-up Chair	Dale Huston	lecia.guy(at)verizon.net

Please submit Newsletter Articles by the last Friday of the Month.

Type GSCC in Subject Line.

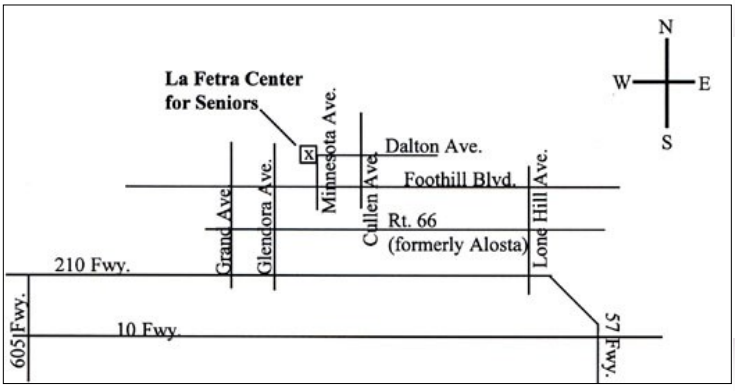
Email to Dan Leddy

ranchitoave(at)yahoo.com

Thank you to the following members for help in this month's Newsletter::

Helga Djordjevic

333 East Foothill Blvd.
Glendora, CA 91741
Telephone: (626) 914-8235



We're On The Web

Webmaster:
Ell Fullmer
www.gscclub.org
Email:
gscc(at)gscclub.org