December 2015 Newsletter

Glendora Seniors Computer Club

A Friendly Seniors Group Serving All Computer Skill Levels

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

Volume 20, Issue 12

Merry Christmas and a Happy New Year

You are cordially invited to attend the

Annual GSCC Christmas Party/Potluck/Silent Auction

on December 9, 2015, at 1 pm at the La Fetra Building.

There will be door prizes, delicious food, games, bargains,

and - we will elect our new 2016 Board of Directors.

Bring your treasures for the auction and a dish of your choice.

See you there !

PROGRAMS BY: Program Chair: Annemarie Hunt

December 9

Christmas Party

INSIDE THIS ISSUE

Glendora Senior Computer Club
General Meeting Minutes
November 04, 2015

President Barbara Denny called the Meeting to order at 1 PM welcomed 22 members.

ANNOUNCEMENTS:

Next meeting: December 9th Christmas Party Potluck, Silent Auction, Door Prizes and Election of 2016 Board. Michael and Berta are invited guests.

Vice-president Wayne Gue - nominations for the **2016 Board:**

President – Annemarie Hunt, Vice-President – Connie Lang, Secretary – Ruthann Mayrose, Treasurer – Rita Norkin, Tech Advisor – Ell Fullmer. Programs and Publicity – Barbara Denny.

Program Chair - Annemarie Hunt showed the Glendora YouTube video of the La Fetra Open House and reminded us to "SAVE YOUR GOODIES" for the silent auction!

Program:

Michael Harrington a local computer tech from Bright Idea Technologies - IT Services & Computer Repair presented the program **I Tunes, and It's Many Uses -*I Tunes and what does it do* -**

It is used to play, download, and organize digital audio and video (as well as other types of media available on the iTunes Store) on personal computers running the OS X and Microsoft Windows operating systems. The iTunes Store is also available on the iPhone, iPad, and iPod Touch

Break: Thank you Annemarie for today's donuts.

Q & A – Ell Fullmer, Annemarie Hunt and Barbara Denny covered questions on the following topics:

1) **Driverbooster.com a free program to find outdated drivers on your PC and download the latest version.**

2) Transfer data via cable from laptop to PC.

3) Additional storage for Apple products?

Next meeting: December 9th Christmas Party Potluck, Silent Auction and Election of 2016 Board.

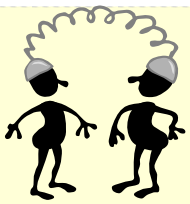
Adjournment: Meeting adjourned at 3:00 pm.

Submitted by:

Secretary Ruthann Mayrose

Approved By:

President Barbara Denny



The Computer Guys *Ell Fullmer*, will be meeting on

THE SECOND Thursday of the month: December 10, 2015

9:00 a.m. to 12 noon — Second Floor — La Fetra Center

10 Tips for Online Shopping Safety

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

Amazingly, in today's topsy-turvy world, because of vulnerabilities in the processing of credit and debit cards used at retail stores and the hackers who are focusing on those vulnerabilities, right now shopping online can actually be safer than swiping your card at a local store. For safety sake, however, there are a few online shopping rules that you should follow.

1. The first of these is to always have a good antivirus program installed on your computer and to update your antivirus program and other software like the operating system whenever an update is available. When in doubt, don't click on links. This is especially true of email where phishing schemes are prevalent, but you should also be careful when you are surfing the Web or visiting social media websites.

2. Shop at trusted, established websites. Don't use any sites that you've never heard of. If you want to try a new website, check to see if any friends or acquaintances have used it successfully.

3. Pay only through secure sites. Typically the address in your browser will change from "http:" to "https:" during a secure connection.

4. Never email your credit card number, social security number, or personal information to anyone. No reputable seller will request it by email since email is not secure.

5. Do your banking and shopping from home where you are on your own secure network. Wi-Fi hotspots at local coffee shops and other establishments usually do not offer enough protection unless the user takes some added precautions, which can be cumbersome for the average user.

6. Create strong passwords consisting of numbers, letters, and symbols. Do not use words or names. Make the password for each banking and shopping site unique. Keep your passwords private.

7. Credit cards are generally the safest option for shopping online. When using a credit card, you have limited liability and the ability to have the credit card company intervene if something goes awry. Debit cards can also be a good choice as long as you have investigated their liability limits, which may be higher than those of credit cards.

8. Keep a paper trail. Let's face it, none of us have perfect memories. Print and save records of your online transactions, including the name of the seller, product description, price, and date of purchase. Most reputable merchants allow you to print a receipt after the transaction is complete. You can use these printed receipts to compare to your bank and credit card statements.

9. Monitor your bank accounts and credit card purchases regularly. Report any discrepancies or unusual charges to your financial institution immediately.

10. Your social security number is the key to your identity. Be miserly about sharing it with anyone, especially online. No reputable merchant will ever ask for your social security number to make a purchase. Credit card theft is pretty easy to get through. Usually you notify your financial institution and they issue you a new card. Identity theft is much more difficult to handle because a thief can open lines of credit in your name, buy a car, and obtain new credit cards. In order to steal your identity, the thieve needs personal information like social security number, address, phone number and financial information. So be careful when giving out any such information.

Many financial experts say that having your bills sent to you electronically and paying them electronically is safer than sending and receiving them by mail. They also recommend shredding paper documents with personal information. So whether you use a credit card at a physical store, you shop and pay bills online, or you pay bills by mail, the key word is "caution." Our mothers taught us to watch our wallets and keep the doors closed. Now we have a lot more convenience, and also a lot more to watch out for.

This article has been obtained with permission to reprint by non-profit or other user groups, with credit given to the author, the publication and the user group.

STOP. THINK. CONNECT. INTERNATIONAL MOBILE DEVICE SECURITY TIPS (ENGLISH)

Keep a Clean Machine.

Just like our desktop and laptop computers, the software on our mobile devices (e.g., smart phones and tablets) must be kept up-to-date and free from malicious software.

- Protect all devices that connect to the Internet. Smart phones, tablets, gaming systems, and other web-enabled devices all need protection from viruses, malware, and other online threats. The best defense against online threats is to keep your mobile security software, web browsers, and operating systems up-to-date.
- Monitor your device's data usage and investigate discrepancies. An unexplained spike in your device's data usage could indicate the presence of spyware. Running security software to identify and remove unwanted software could protect your bill—and your personal data.
- Know the source of your app. Fraudulent apps often masquerade as popular products. Be sure to verify you are downloading the legitimate app and only download from trusted app marketplaces.
- Keep apps up to date. Apps are periodically updated to add new features and better security. Ensure your apps are regularly updated and delete apps you no longer use.
- Do not "jailbreak" or "root" your mobile device. Running non-standard apps may prevent the installation of important security updates from the manufacturer and may void your device warranty.

Restrict Device Access.

Mobile devices contain a significant amount of personal information, such as contacts and saved login information. Lost or stolen devices can be used to gather information about you and others.

- Secure physical access to your device. Be aware of your surroundings when using your device in public. "Shoulder surfing"—looking over a victim's shoulder to capture passwords, personal identification numbers, or other data—has become a greater threat in recent years.
- Lock your mobile device. Use a strong passcode or passphrase, facial recognition, or fingerprint authentication to restrict access to the personal information on your device.
- Remotely manage your device. Many mobile devices have features that allow users to remotely find, lock and erase content should their device is lost or stolen.
- Think before you app. Understand and be comfortable with what information (e.g., location, your contacts, social networking profiles) the app would access and share before you download the app.
- Protect your data. Back up your data onto a personal computer, an external hard drive, a flash drive, a network, or the cloud. Keep track of any stored passwords on the device and be sure to change these if your device is lost or stolen.

Clear data on your old devices. Erase all your personal data and saved passwords before selling, exchanging, or disposing of your old mobile device.

Connect with Care.

Exercise caution and use common sense when connecting to public (open) Wi-Fi networks.

- Be mindful of what is at risk. Open networks are vulnerable to monitoring, allowing user information (e.g., browsing history, passwords) to be collected. Use a virtual private network (VPN) or connect to trusted, secure networks as they provide unreadable (encrypted) transmissions.
- Get savvy about Wi-Fi hotspots. When using public Wi-Fi, limit the type of business you conduct, and adjust the security settings on your device to limit who can access your phone.

Be mindful of remote connectivity. Disconnect Wi-Fi, Bluetooth, near field communication (NFC), or other remote connectivity services when not using them.

Be Web Wise.

We can all take steps to keep ourselves safer and more secure online.

- Stay current. Keep pace with new ways to stay safer online. Check trusted websites for the latest information and share with friends, family, and colleagues to encourage them to be web wise.
- When in doubt throw it out. Links or attachments in email, posts, and texts are often the ways cybercriminals try to steal your information or infect your devices.
- Protect your money. When banking and shopping online, check for web addresses with “https://” which means the site takes extra measures to protect your information. Sites beginning with “http://” are not secure.

Own your online presence. Set security and privacy settings so that you are comfortable with the information you share. In addition, block those that you want to avoid contact with.

Be a Good Online Citizen.

Being safer online makes the online world more secure for everyone. Practicing good online habits benefits the global digital community.

- Share about others only as you would be comfortable having them share about you.

Never give out anyone else’s personal information (e.g., email, social media handle, mobile number, photos, videos) to a third party without that person’s permission.

4 WAYS TO REDUCE YOUR DIGITAL EXHAUST

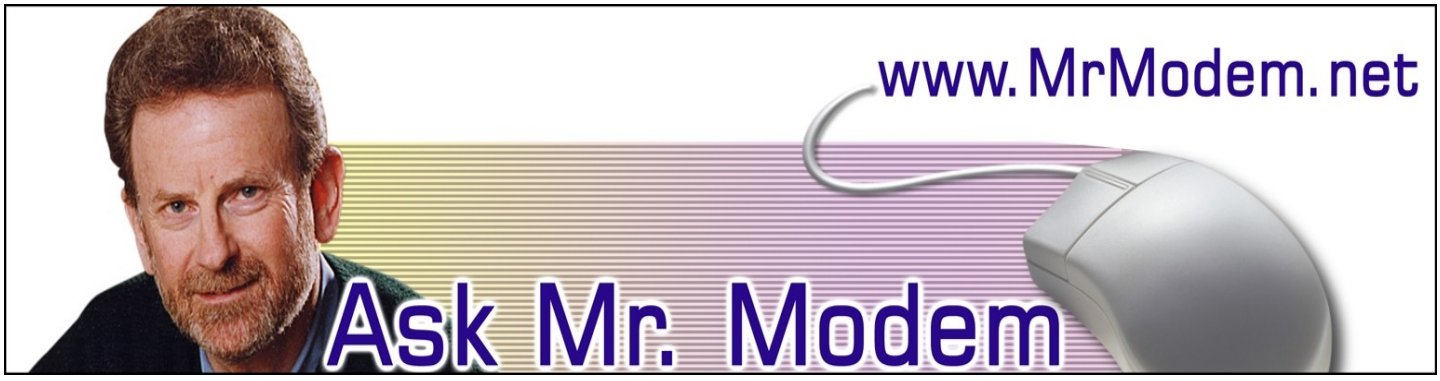
Many argue that data mining provides a customized experience online yet your data is shared, purchased and sold between hundreds of companies and you may never use their services. With so many online services collecting and sharing information about you – from dating apps to online retailers – your personal profile is more comprehensive than you may realize. This is a major concern for many privacy advocates. Here are tips to help you manage your privacy and reduce your digital exhaust.

Change your settings: Look over your privacy settings on your browser, social media profiles and other online accounts and make sure you’re providing as little information as possible by turning off your location and cookies and opting out of other online trackers.

Use ad blockers or privacy add-ons: Tools like Privacy Badger from the Electronic Frontier Foundation can help you turn off creepy trackers running in the background on some sites, as well as those ever-present social media icons on websites you visit.

Log out every time: For an extra layer of privacy, log out of your social media accounts when browsing the web to avoid trackers from sending information to social media channels.

Consider using pro privacy alternatives: As a result of the data mining, concerned users turn to alternative tools, such as browsers, VPN services and social media services that help to hide their online footprints.



On Sunday, February 1, 2015 3:47 AM, Mr. Modem <mrmodem@mrmodem.net> wrote:

Ask Mr. Modem! – February 2015
www.MrModem.com

Investigate Slow Connection

Q. I'm using high-speed Internet over a phone line. It works okay, but on occasion it goes so slow that most sites never finish downloading. Is this a provider problem?

A. I would start your investigation with your Internet service provider, and initially determine what connection speed range you should have. Your provider's Web site will have that information or you can call their Customer Service department. With that information in hand, run several speed tests using a site such as speedtest.net, bandwidthplace.com or cnet.com/internet-speed-test.

Connection speeds can vary greatly throughout the day and night, so conduct tests at varying times over several days. If your average upload and download speeds fall below what you should be receiving, contact your provider's Tech Support. In that way you will have evidence to support your assertion that the connection speeds you are receiving are not what were represented and your provider can investigate from there.

Q. I received a message from Yahoo! Mail telling me that I'm running out of storage space and that I need to provide my password so they can increase my capacity. You've warned us about anybody that asks for our passwords, so I'm suspicious. Is this for real or what?

A. Your suspicion is justified. I'm glad you remembered what I so frequently yammer about: Never provide your password or voluntarily confirm any other personal or account information when requested to do so by email. No legitimate organization or service will ever ask you for that information. Just delete the message you received and don't give it another thought.

Q. In my old version of Firefox I was able to bookmark a site to a folder. But now if I click the star, it doesn't allow me to select a folder. I have to move it into a folder after the fact by opening all bookmarks. Is there an easier way?

A. In the current Firefox, you can instantly create a bookmark by selecting the star icon at the top right of the browser. When the star turns blue, your bookmark is created, so tap or click the star again. (Medical Tip: When you turn blue, call 9-1-1.) You will see options to edit the bookmark. You can also drop it into an existing folder using the drop-down menu, or create a new folder.

Q. When I installed the latest version of Microsoft Office on my Windows 8 computer, all my favorite key-stroke combinations, such as ALT + F + V for Print Preview are gone. Now I have to use the mouse or touch-pad, click in the corners, scroll here and there -- it drives me crazy. Any suggestions, Mr. M?

A. The good news is that most of your favorite keyboard commands are still present, but have been changed. Why? Because it would obviously make too much sense to leave them as they were. Your beloved Print Preview is now ALT + CTRL + I.

Accessing a list of all keyboard commands is as simple as clicking the question mark in the upper right of the page. Word Help will open. Type “keyboard shortcut” and you will find a complete listing. I tested a bunch of them out under both Windows 7 and Windows 8 and didn't run into any problems, so I think you will be very pleased with the results.

Mr. Modem’s DME (Don’t Miss ‘Em) Sites of the Month

Ba Ba Dum
Ba Ba Dum is a language game that lets you practice your vocabulary in one of eleven different languages, including my native Svenska. When you arrive at the site, click Play to begin and select the language you want to practice by clicking the country's flag graphic. For a real challenge, you can practice in a randomized assortment of languages. In the top-right corner you will see your score. There are two numbers: Your cumulative score and the score for the language you are currently playing. This site presents a fun way to practice vocabulary in different languages.
http://babadum.com

Crossword Puzzles
If you’re a crossword-puzzle enthusiast, this is an online treasure trove of puzzles. With a repository containing more than 32,000 crosswords, you are guaranteed endless hours of entertainment or escapism.
www.crosswordpuzzlegames.com/

Pica Pic
Created by Hipopotam, this site features a digitalized collection of handheld games. These games triggered a wave of nostalgia for me. I can still remember playing my Little Mermaid game on the school bus and almost being beaten to death. Good times, indeed. Use the menu at the bottom to select a game and use the arrows at the left and right of the screen to scroll back and forth. A down arrow shows which game is currently selected. If you mouse over the game, a Play button appears. If you want to play that game, click it to begin. This will enlarge the game and display its controls. The games feature the same sounds as if you were playing the original handheld version.
www.pica-pic.com

December 2015

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: _____

Computer Operating System: Windows 7 ___ Windows 8 ___ Windows 10 ___ Mac ___ Other _____

Question:_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Elected Officers

President	Barbara Denny	dennyandassoc(at)verizon.net
Vice-President	Wayne Gue	wa212gue(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	Connie Lang	connielang(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
Asset Management	Glen Moore	mooretours(at)earthlink.net
Public Relations	Barbara Denny	dennyandassoc(at)verizon.net
Membership Chair	Helga Djordjevic	hdjordjevic(at)verizon.net
Nominations	Wayne Gue	wa212gue(at)verizon.net
Programs Chair	Annemarie Hunt	Ajhunt1447(at)aol.com
Webmaster	Ell Fullmer	pakratt(at)gmail.com
Education		
Newsletter Editor	Dan Leddy	ranchitoave(at)yshoo.com
Set-Up Chair	Bill Hart	Bobbibill(at)peoplepc.com

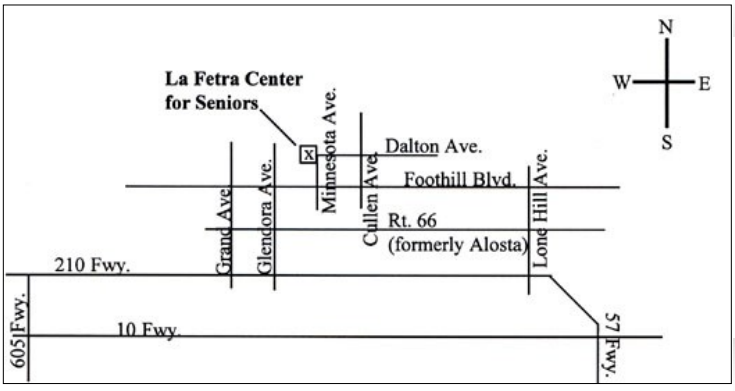
Please submit Newsletter Articles by the last Friday of the Month.

Type GSCC in Subject Line.

Email to Dan Leddy

ranchitoave(at)yahoo.com

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