A DISCUSSION ON COMPUTER SECURITY

More and more we depend on our computers to edit, post-process and store our photographs, research topics on the Web, send and receive email, do our banking, pay bills, calculate our income tax, store medical information, download and listen to music, read e-books, etc. The data stored on our computers is extremely valuable to us, and it may also be valuable to a person who wants to steal our identity and/or our money. This is why learning proper computer security is so important.

Sarah Brock, our club's vice president and this month's chairperson, introduced to us her husband, Dr. Gary L. Wallace, who is also a club member. He is an Information Technology expert with multiple degrees in Information Technology, Management, and Security. He has worked in computer security with the U. S. Navy and Entergy and has served as a data analysis expert witness for the FBI and NCIS. During his presentation, Dr. Wallace gave us a tremendous amount of information and hints about computer security – more than many of us could absorb and retain in our brains. For those that are interested in more technical details, Dr. Wallace is a Professor at Tulane and Delgado where he teaches courses in Information Security and Technology.

Here are some of the things I remember him saying:
Make sure that all your computers are password protected. Your hard drives will fail eventually, so back up your data frequently. A good way to do this is to back up your data to two or more external hard drives, and keep at least one of them off premises. He recommended Acronis to make a complete image of your hard drive. That can save you a tremendous amount of time and effort should you have to install a new hard drive in your computer. He also recommended ***SyncToy 2.2*** a free program supported by Windows that allows you to sync data between multiple directories, multiple devices, or multiple computers. For Example: SyncToy will copy new information from Drive A to Drive B with or without writing over the information that is already on Drive B. Backups are only useful if they can restore your data. Test your backups by trying to restore some data.

Use a good anti-virus program such as Norton (his favorite) and update it regularly with the latest virus information. In response to the question of why Windows computers get more viruses than Mackintosh computers, he said that most of the hackers hate Bill Gates and Microsoft and create their viruses to attack Windows computers. Mac computers get viruses less often, but they can and do get Trojan horses.

Many of us have designated ourselves as the Administrator of our computers. That means that we can change all settings on our computers. Never surf the web using your administrator account. Set up another user account with which you surf the Web. The reason for this is that if you reach a Web site that has malicious content such as a virus or Trojan horse, they can do a lot more damage if they have access to your administrator account.

No information in your computer or in your emails is private. In fact, it is not against the law to read someone's email. It is against the law to commit a crime using that information. Law enforcement agencies have an FBI designed program called Carnivore that can "sniff" traffic to look for email messages in transit. Employees of your Internet service provider such as Cox Cable and AT&T can see everything that you do over the Internet. To eliminate that, Dr. Wallace suggested installing your own router between the ISP's router or gateway and your computer(s). If you have a wireless home network, make sure that it is a secured network and use MAC (Machine Address Code) addresses for each of your computers, laptops, tablets and smart phones. That way only your computers can access your wireless network.

Hackers who commit crimes with computers and do it from another country cannot be extradited and tried in this country. Our laws protect freedom of speech and freedom of expression at the cost leaving our citizens' computers unprotedted.

Concerning the email program or app that you have installed on your computer, Dr. Wallace said, "Microsoft Outlook is evil. If you get an email with a virus Outlook automatically opens it. I suggest using Thunderbird in place of Microsoft Outlook or configure Microsoft Outlook to not open emails in the reading pane automatically."

Dr. Wallace recommends using different strong passwoeds for each web site you deal with, especially if they are financial institutions. So, how do you keep track of all those different passwords? He said that when he was in the Navy, he has something like 2,000 passwords. Stegnaography to the rescue! Steganography is the science of writing hidden messages in such a way that no one apart from the sender and intended recipient even realizes there is a hidden message. Such hidden messages can be embedded in an innocent looking .jpg photo file. All you need is a free program called QuickStego http://quickcrypto.com/free-steganography-software.html to write or read the message in one of your many photos. He said that before going on their recent trip to England, he created a spread sheet with all of his and Sarah's passwords that he embedded in a photo that was on the computer they took with them. Paul Muehlemann mentioned that there are some other programs that can encrypt and store passwords on your computer or a thumbdrive such as Keepass http://keepass.info/ Dr. Wallace said that those, too, are OK as long as they encrypt the info and do not store it in a cloud. Finally don't forget to insure your computers, especially if you have several of them. Your home owner's policy may only cover about $2,000 worth of electronic equipment.

Finally, if you install a new hard drive or sell or give away your computer, format the old hard drives at least three times to wipe out your data. (Seven times if you want to make it impossible for forensic investigaters to recover any data.) It might also be a good idea to remove the hard drives and physically destroy them with a sledge hammer!

This program was very interesting and informative. Dr. Wallace answered many questions posed by club members, and I feel sure he could have continued talking for another hour or so. We thank him for taking the time to give us so many tips on the security of our computers.

Note: I asked Dr. Wallace to review my article to make sure that everything I wrote was accurate. When he returned it to me, he attached an additional list of hints and notes.

Below is a list of programs and additional notes that Dr. Gary L Wallace sent us after his program *Computer Security Discussion:*

PROGRAMS

SyncToy 2.2- Free. Supported by Windows. Allows you to sync data between multiple directories, multiple devices, or multiple computers. For Example: SyncToy will copy new information from Drive A to Drive B with or without writing over the information that is already on Drive B.

Acronis. Backup software. Used to do image backup of entire operating systems and system drives. Allows restore by file or by image. Supports ALL operating systems.

Antivirus- Norton or McAfee. Avoid AVG. Remember in purchasing an antivirus software package it should deal with viruses, backdoors, email scanning, and malware.

Quick Stego. Free. Menu-driven. Encrypts text or images within a .BMP image file.

Open Stego. Free. Command line driven but will encrypt text or images within any image file format.

Operating Systems

Never surf the web as Administrator. Set up individual user accounts that require a password to logon to the computer. These user accounts can be deleted if they become infected or compromised without damaging the operating system functions. If Administrator is infected the only solution is to rebuild the machine (format and reinstall the operating system).

Data should be in a separate directory from My Documents folder for both backup purposes and in case the individual user has to be deleted due to infection.

Event logs under Microsoft Windows tell you everything that happens on the machine- incoming and outgoing. These logs should be reviewed periodically. Right-click on My Computer: Manage: Event Viewer.

Securing your Network

Always have a separate router from your Internet provider (Cox, AT&T). Hook your personal router to the router provided by Cox, etc. This prevents your Internet Service Provider from seeing what happens on your network.

On your router, always enable MAC (Machine Address Code) filtering for wireless connectivity. This is different from providing a password to a friend who wants to use their laptop on your network. MAC filtering means that your friend must provide the MAC address of their device (Go to a Windows prompt. Type in "ipconfig /all"). Some devices call a MAC address a "physical address". Your router has a network traffic log that should be reviewed periodically.

Passwords

Change them. Always have separate passwords for each system. Change all default passwords. Do not share passwords- you and your spouse should have different passwords to log in to the bank- even if you share an account.

Three Rules of Backing Up:

1. Back up
2. Back up
3. Back up somewhere else (off site)

Do not assume your back up worked- go make sure that your files are there and functional.

Destruction of Data- format hard drives, USB drives, media, etc. THREE times to adequately erase all data (seven times to be forensically impossible to recover any data).

Do not wait for something to fail due to age to replace it- hard drives have a normal 5 year warranty. Purchase redundancy before a hardware failure before the hardware fails.

Update your data/images/etc. to the latest technology. Scan paper photos into digital files. Convert VHS tapes to digital formats.

A system is only as valuable as the data it holds. A $300 laptop that holds priceless pictures of your wedding, graduation, etc. is PRICELESS.

Data is only as valuable as your ability to restore it.

Flash drives, SD discs, memory sticks, etc. do not have moving parts so they last longer than hard drives which have moving parts.

CD/DVDs can be used for tertiary backups. Copying to them is very slow and they should not be the primary backup option.

Internet Browsers- suggest Mozilla, Firefox or Google Chrome. Never use Internet Explorer as it is heavily targeted for viruses and spam.

Phishing- when someone sends you an email soliciting personal information or provides you with a link that when clicked on gains personal information.

Virus- causes operating system errors or gathers personal information. Primarily Windows and Internet Explorer. Use Mozilla Firefox, Google Chrome, Opera, or Macintosh Safari (there is a version of Safari that works on Microsoft Windows).

Trojan- Can affect any operating system. Backdoor that gains control of your machine without your knowledge. Trojans can record your keystrokes, personal information, or use your machine to jump to other machines.

Microsoft Outlook is evil. If you get an email with a virus Outlook automatically opens it. Suggest using Thunderbird in place of Microsoft Outlook or configure Microsoft Outlook to not open emails in the reading pane automatically.

Debit Cards- always use them as credit cards. NEVER enter your PIN number at any vendor- if their system is compromised so is your personal information. When using credit cards or debit cards as credit cards, you are protected under the credit card agreement and not responsible for fraudulent charges. Debit cards offer no such protection. Most banks also offer more points or rewards if you use their debit cards as a credit card anyway because they charge a higher percentage to the vendor.