THE GIGABYTE GAZETTE

The Monthly Newsletter

of the

Sun City Summerlin Computer Club

June, 2017

Table of Contents

President's Message

by Howard Verne

Dear Computer Club and friends

A reminder that May was our last monthly meeting until September. **June, July and August will be dark**. This provides a great time for everyone to enjoy the summer with your families. However, keep an eye on the Gigabyte newsletter because some classes and SIGs will continue thru the summer.

You have, no doubt, been hearing of all the problems the world has been having with computer malware. Our HW SIG stands ready to help you with any problems. You can help protect yourself by not clicking on links from sources you are not familiar with. The ONLY protection against ransomware is computer backups. Again, the HW SIG technicians will be happy to show you how to back up your computer to your own external back up unit.

Your computer club board is already planning for our November appreciation dinner for all our wonderful volunteers. For those members who have asked for a social event, this is it. The cost for you is only to volunteer 15 hours of time to help make our club a success. Call any board member and we will find the right spot for your volunteer service.

Have a good summer, see you September 7th.

Howard Verne, President
(702) 527-4056 ***pres.scscc@gmail.com***

Issue Contributors

Tom Burt	**Kathy Kirby**
David Kretchmar	**Pat Lemay**
Howard Verne	

Submissions Welcome

We are always looking for new information to share with our club members. If you have computer or technical information you would like to share with members of the club, send your articles to Tom Burt at tomburt89134@cox.net. Thank you to everyone for your contributions.

SCSCC Board of Directors Actions

The Computer Club Board of Directors took the following actions on

May 10, 2017

Chuck Wolff made a motion that the minutes of the April 12, 2017 Board Meeting be approved as submitted. The motion was seconded by Irene Burt and unanimously approved by the Board.

Jeff Wilkinson made a motion that the Guest Rules for the Computer Club are adequate and require no changes. The motion was seconded by Tom Burt and unanimously approved by the Board.

Kathy Kirby made a motion that there be no Board Meetings for the months of June and July 2017 and that the President will call for a special meeting if necessary. The motion was seconded by Chuck Wolff and unanimously approved by the Board.

Chuck Wolff made a motion that the meeting adjourn at 10:00. The motion was seconded by Kathy Kirby and unanimously approved by the Board.

General Membership Meeting

There will be NO General Meetings in June, July or August 2017. Our next General meeting will be held at 7 PM on Thursday, September 7th, 2017 in Desert Vista Room 5.

Regular club educational activities (SIGs, Q&As, Seminars, Classes and the Repair Lab) will continue throughout the summer.

For Club information go to **www.scscc.club**, contact Howard Verne, President at 702-527-4056 or email him at **pres.scscc@gmail.com**.

Welcome New Members

The following new members joined the Computer Club between April 26th and May 26th.

Paul Beilman
Jerry Cabanilla, Sr.
Charlie Cule
Katica Cule
Paula Defino
Steve Defino
Carole Graham
Michael Lee
Robert Newton
Karen Olsen
Elma Quinn
Donna Roskens
Randy Slinn

June 2017 Calendars

To view this month's classroom and lab calendars, click the following hyperlink:

http://www.scscc.club/Calendars/scscc_calendar_2017-06Jun.pdf

Special Interest Groups

Special Interest Groups (SIGs) provide a forum for general discussion on a specific computer related subject. Admission to all SIGs is on a first-come, first-seated basis and is subject to the maximum allowed by fire code regulations. All of the following meetings are held in the Classroom. <W> or <M> or <H> indicate whether a SIG would be of interest to a Windows, Macintosh or Hand-held Device (i-thing or Android) user.

Genealogy <W> ***Dark Jun - Aug***
2nd Thursday, 10:00 a.m. Sep., 2016 to May 2017
Karen Ristic (702-749-6489)

Genealogy is one of America's most popular and rewarding hobbies. With billions of records now available online, researching your family tree has never been easier–if you know where to look and which key words you'll need to use to create an accurate family tree from start to finish. Check out Karen's new series of workshops in the lab on the ***second Tuesday of the month***.

GMail <W/M>
1st Thursday, 10:00 a.m.
Pat Lemay (702-254-1499)
This SIG covers Gmail as well as other Google applications. All members are welcome. This is your place to learn about all things Google.

Hardware / Software Repair Lab <W >
Every Tuesday, 1:00 p.m. to 4:00 p.m.
Chuck Wolff (702-233-6634) and
Chuck Hagen (702-418-2614)
The Repair Lab provides **CLUB MEMBERS ONLY** with no cost assistance for those having upgrades and / or hardware and software problems with their computers. Bring in only your PC tower and your problems. Our TECH team will give you our best effort. ***Be sure to mark your cables so you can re-connect when you get home***.

Internet Investing <W/M>
3rd Thursday, 9:00 a.m. in even months
Next meeting: June 15.
Tom Burt (702-341-7095)
The Internet Investing SIG provides a forum for members interested in using Internet resources for researching and managing investments to meet, discuss, and learn more about the topic. The SIG's target audience is members with intermediate computer skills and investment experience, but all members are welcome.

iPad <iPod, iPhone, iPad>
4th Wednesday, 9 a.m.
Zane Clark (702-562-3684)
This SIG will be your forum for learning about and discussing the Apple iPhone, iPod and iPad tablet devices. It's for Apple hand-held device owners of all experience levels.

Macintosh Users' Group ***Dark Jun - Aug***
2nd and 4th Tuesday, 6:30 p.m.
Kathy Yeko (818-414-6110)
This SIG is for Macintosh users of all experience levels. We will have Q&A, so bring your questions and/or problems.

Photoshop Elements<W>
4th Mondays, 1:00 p.m.
Mary Miles
This SIG covers many of the basic and advanced elements found in Adobe Photoshop Elements, especially layers. If you wish to make the most of your photographs, this SIG will be very helpful. This SIG's target audience is intermediate digital imaging users, but all members are welcome.

Beginner's Digital Photography <W>
Dark – May - Sep
3rd Mondays, 1:00 p.m.
Stu Gershon (702-255-3309)
Picasa is still a viable, reliable photo editor for beginners, but this year we will also take a look at Google Photos and other FREE editing programs. You're invited to bring your equipment (Laptops or Cameras) so that you can have that "hands on" experience!

This SIG's target audience is beginner to intermediate digital photography users, but all members are welcome.

Windows 10<W>
First and Third Saturdays at 10:30 am
Bill Wilkinson (702-233-4977)
Each session will be devoted to assisting new Windows 10 owners in becoming familiar and comfortable with Microsoft's newest operating system for desktop and laptop computers. Assistance will be given individually or in small groups as circumstances warrant. Bill's notes are available by clicking HERE.

Kaffee Klatches

Kaffee Klatches provide a forum for general discussion on all computer-related subjects. Admission to all Kaffee Klatches is on a first-come, first-seated basis and is subject to the maximum allowed by fire code regulations. All of the following meetings are held in the Classroom. **<W> or <M> or <H> indicate whether a SIG would be of interest to a Windows, Macintosh or Hand-held Device (i-thing or Android) user.**

Windows 10 Kaffee Klatch <W>

First and Third Saturdays, 9:00 a.m.
Bill Wilkinson (702-233-4977)

If you are a novice or near-beginner computer user, or if you just want some refresher information together with a refreshing cup of coffee, then jump-start or recharge your computing knowledge by attending these Win 10 KK sessions. At each session, attendees will explore from one to four topics of particular interest to beginners and near-beginners. The topics are always announced a couple of days in advance via e-mail to SCSCC members who have subscribed to the club's message board. Each topic is presented in a step-by-step manner and is supported by "how to" notes that can be easily and conveniently downloaded from the SCSCCBKK.org web page. Following each "up front" presentation of one or more topics (approximately 60 minutes in duration), an informal open-ended Question and Answer period takes place for those who wish to participate, listen, reflect, or inquire.

Kaffee Klatch <W/M/H>

Every Tuesday, 8:30 a.m.
Sandy Mintz (702-838-2525)

This KK is for all users, from beginning to advanced. The KK discussions are not restricted to any one subject, computer platform or computer-knowledge level but should be computer or technology related. We will try to answer your questions, help you keep your systems updated and provide some useful "tips and tricks." If you have a tip or information you would like to share, we encourage you to bring it in and share since the SCSCC is built on "neighbor helping neighbor." The fellowship is great, the coffee is good, and the education received from the KK attendees is priceless. Stop by on Tuesday morning and have a cup of coffee with us.

June 2017 Classes

Because there are a limited number of computer stations available for hands-on participation, pre-registration is necessary for all classes. See individual class descriptions for details on how to register.

Windows 10
Conquering the Basics and Beyond

Making the Easy Transition From Earlier Editions of Windows

A Nine-Hour Hands-On Course
Limited to 12 Participants

Next Class Dates: June 5, 6 & 8 - 9 AM to noon

Lead Instructor: Bill Wilkinson

Prerequisites: Club Membership for 2017 ($10); Comfortable with using a mouse; some basic knowledge of an earlier edition of MS Windows (XP, Vista, 7 or 8/8.1).

Place Your Name on the Pre-Registration List for an upcoming three-Session Class

If you are interested in placing your name on a high-priority reservation list for the next available class, simply send an email message to: **WILKINLV5@COX.NET** and include the following information:

- Include "**Windows 10 Class**" in the Subject Title
- Your first and last name
- Your 8-digit Sun City Summerlin Association number
- Your telephone number
- Your email address

Your message will be promptly acknowledged by return email. No telephone inquiries please.

Please note: All hands-on classes are limited to 12 participants. This class fills very quickly.

BOOT CAMP CLASS
for Windows Win7, Win8.1 and Win10 Users

No classes in June
Each Session Meets from 9 am - noon.
Lead instructor: Bill Wilkinson

Place Your Name on the Registration List
for the Next Three-Session Class
(Dates to be Determined as Interest Dictates)

Course Description:

Boot Camp is an introductory course designed for residents who are novice users of the Microsoft Windows operating system. **It also serves as an excellent review for intermediate users who want to fill some gaps in their computer knowledge.**

This hands-on class has a **limited enrollment of 12** with each participant working at an individual computer station in the Computer Lab. A team of lead instructor and four coaches will provide step-by-step instruction that will include demonstrations, guided practice and individual coaching assistance.

These strategies will be covered:

- Secrets for using the mouse and the keyboard effectively
- Basic vocabulary needed for an understanding of Windows (Vista, Win 7, and Win 8.1)
- Managing and organizing your personal data files (documents, pictures, videos, and music)
- Protecting your computer from viruses and other malware
- Safely downloading and installing applications from the Internet
- Efficient and safe use of an Internet browser and search engine.

Course Fee: $10 for current club members; $20 for non-members

Materials include: a step-by-step user's manual and a flash drive

Registration Details:

If you are interested in placing your name on a reservation list for the next available class, simply send an email message to: **WILKINLV5@COX.NET** and include the following information:

- Include "**Boot Camp Class**" in the Subject Title
- Your first and last name
- Your 8-digit Sun City Summerlin Association number
- Your telephone number
- Your email address

The Genealogy Computer Lab Workshop

Presenter: Karen Ristic
Location: SCSCC Lab

Dark Jun - Aug

In this workshop, using the lab student computers, we will explore some of the many genealogy web sites, such as *FamilySearch.org, One-step Webpages, Ellis Island,* and more.

June 2017 Seminars, Q&As and Workshops

For Computer Club seminars, there is no requirement for advanced registration unless explicitly stated. Seating is first-come, first-seated.

Android Cell Phone Q&A

Wednesday, June 7th at 1 PM
Presenter: Susan Heifetz
Location: SCSCC Classroom

Susan will answer your questions about how to use an Android smart phone.

Making a Video Slideshow

Wednesday, June 14th
Presenter: Mary Miles
Location: SCSCC Classroom

Mary will demonstrate how to take a set of your favorite photos and generate a video slide show with transitions and effects.

Google Chrome Web Store

Thursday, June 15th at 1 pm
Presenter: Pat Lemay
Location: SCSCC Classroom

The Chrome Web Store is Google's online store for web applications for Google Chrome or Google Apps. The software allows users to install and run web applications for the Google Chrome browser. The store hosts free and paid applications. The Store has been described as being like Google Play, but for "apps on the web". You can download and install games, extensions and themes.

This class will be taught on the desktop Windows version of Chrome.

Backup Tools & Strategies

Thursday, June 22nd at 9:30 AM
Presenter: Tom Burt
Location: SCSCC Classroom

With ever-increasing threats of ransomware and other nasty viruses, backing up your system and your data files is one of the most important things you, as a computer user, *must* do on a regular basis. This 2-hour seminar will review key concepts and activities related to performing backups on your PC.

We'll review Tom's composite backup strategy that uses **Acronis True Image** for regular complete hard drive backups plus a blend of **Windows File History** and **cloud or network services** to back up frequently changing files. We'll demonstrate several of these powerful backup systems. Along the way we'll clarify imaging, cloning, incremental backups, file backups and other features. We'll also reserve plenty of time for your own questions and answers.

The seminar notes will be available about **June 18th** at: http://www.scscc.club/smnr

Tom's Tech-Notes

RansomWare
Defense and Recovery

Tom Burt, SCSCC Vice-President

This month I want to add my voice to that of many others in the club to urge our club members and other Sun City residents to take very seriously the threat of a ransomware virus attack on your PC, Macintosh, Android device and yes, even your IOS device. While PCs are the dominant target, all of those listed are potential targets.

What is Ransomware?

Ransomware is malicious software that infects your PC and then surreptitiously encrypts (scrambles) some, or all, of your data files. The virus can encrypt not only files on your PC's hard drive, but on any network shared folders that your PC connects to. The virus also attempts to replicate itself to other PCs on the network.

Once a ransomware virus has done its dirty work, it pops up a screen alert to tell the PC user that the files have been encrypted. It offers to provide a decryption tool / key in exchange for a ransom payment, usually in the Bitcoin digital currency. The user is given a few days to pay up, after which the offer is no longer available.

Other variations of ransomware block your PC from booting until the ransom is paid.

Here's a link to an article that describes ransomware in more depth.

https://www.trendmicro.com/vinfo/us/security/definition/ransomware

How Do You Get Infected?

A ransomware virus is software. To infect your computer, it first must be installed and then executed. Usually the installer sets up the virus so that, when the computer is booted, the virus piggybacks on some other system component. Or its startup directions may be buried in the system's lists of automatic startups.

Commonly, the ransomware installer / payload comes to your email inbox as an attachment to an email. The attachment is usually a PDF or Word document or a .zip file. The email will look official and say something like: "Attached is our second invoice for $385.20 for your recent order. We would appreciate it if you would remit payment as soon as possible." The purpose of the message is to get you to open the attached document. When you do so, a macro or auto-run script in the attachment executes. It secretly downloads and installs the actual malware and launches it.

It's also possible to get infected by clicking hyperlinks that go to malicious websites. These websites often "spoof" legitimate ones, looking like Citibank, Wells Fargo, Wal*Mart and so forth. The malicious websites attempt to take advantage of known security bugs in your web browser to automatically install malicious software.

Another common way to get infected is to download and install "free" software. Even downloads from reputable sites may inadvertently carry malicious payloads that piggyback on the install of the main free component. A variation on this is a malicious website will display a popup message like: "Cox.net (or Microsoft) has determined that your PC has a serious virus infection. It is urgent that you resolve this at once before your identity is stolen. Call this number for immediate assistance – xxx-yyy-zzzz". The user calls the number and the "technician" at the other end asks the user to allow the tech to remotely connect to the user's PC and do a scan to determine the severity of the infection. After the scan, the tech informs the user that it will cost $500 to remove all the infections found. If the user refuses, the tech will probably say "Too bad – your PC is now locked. Pay up or else!"

How to Defend Yourself

Defense against ransomware viruses (and all malware) requires a coordinated set of behaviors and actions.

1. Most important is to regularly back up your irreplaceable data files to a medium that, once the backup is done, can be disconnected from your computer. A USB flash drive or external hard drive are ideal for this. If you have an offline backup of your data files and, ideally, an image or clone of your entire internal hard drive(s), you can't be held up for ransom. Space here doesn't allow me to go into depth about backup, but I'll be doing a seminar on backup tools and strategies on Thursday, June 22nd.

2. Don't rely on automatic backup systems. MS OneDrive or other cloud-based systems as well as automatic backups to external drives, such as File History or Acronis Continuous File Backup. They may be backing up encrypted copies of your data or, if they're connected to an infected system, the external drives' contents may also get encrypted.

3. Use a quality "real-time" anti-virus / anti-malware tool and keep its virus definitions up to date. Windows' built-in Windows Defender has been upgraded over the past two years and now has a good reputation. MalwareBytes Pro, AVG, Avast and Kaspersky are also considered good. It's worth spending the modest annual fees to get the better versions of these products. Make sure your antivirus tool makes regular full scans of your system to catch malware that the real-time protection may have missed. Also, **do a scan before making a clone or image backup**. If you don't, you may be backing up an infected system.

4. The best way to deal with a malware infection is to ***not get one in the first place***! This means learning and practicing safe procedures for reading email and web surfing. Here are some things you can do:

    a. Don't directly open email attachments, even when they seem to have come from people or institutions you know. If in doubt, just delete it! Before opening an attachment, save it to the desktop or the Documents folder. Then right click on the file and scan it for viruses.

b. Turn off the Preview Pane in your email reading program. The preview pane is automatically opening the email. Instead, use the two-line text preview that most email readers provide.
c. Scan through the list of new emails in your inbox before opening any of them. Delete any that are obvious junk. Of the remainder, drag any that you aren't certain are safe into the Junk / SPAM folder. You can safely view them there. Emails opened from the Junk folder are displayed in plain text and have hyperlinks and images disabled. The true targets of hyperlinks are also displayed. Delete any emails that look suspicious.
d. Before clicking any hyperlink, hover your mouse over it to display a tooltip that shows the actual target web address. If the target site doesn't match the text of the hyperlink, don't click it!
e. If you just CAN'T RESIST downloading free software, always try to go to the actual software developer's website. Often, third party download sites repackage the original freeware with add-ons that you don't want and that may be malicious. Also, when running the setup, always choose the "custom" install option. This allows you to separately OK each installation in the package.
f. Finally, NO ONE out on the Internet – especially Cox or Microsoft – is monitoring your PC to see if it has a malware infection. If you get any such message in a pop-up, it is a scam. Do not click any hyperlinks or call any phone numbers. Similarly, if you get a telephone call claiming they are Microsoft support and advising you that your computer is infected, it is a scam! **DO NOT LET ANY STRANGER CONNECT TO AND SCAN YOUR PC**. Do NOT pay a stranger money to remotely repair your PC. I recommend that if you think your PC is infected, that you bring it to our weekly Tuesday afternoon Repair Lab session and have it checked out.

Recovering from an Infection

If, despite your best efforts (or if you ignored all the above) your computer is attacked and you become a victim of ransomware, your response will depend on how current and complete your computer and data backups are. Everyone's situation is different. As noted above, our Tuesday Repair Lab team can help you in various ways. Here are a few considerations.

1. If you have a current and complete backup of your system, it's probably best to wipe your hard drive and do a full restore from the backups. You may still have work to do to recreate very recent changes to your data files. ***Caution*** – ransomware viruses don't always attack immediately; they may lurk, hidden for days, weeks or months before striking. It's important to do a virus scan before making a backup clone or image.

2. If you have backups only of your data files, you will probably have to wipe the system hard drive and then do a clean install of your operating system, followed by reinstalling all your applications and, finally, your data. This is a large job and may take hours to days. Make sure you have good records of everything that was installed and all the required product activation keys.

3. The Repair Lab team now has a variety of tools that can break through ransomware encryption. However, the cybercrooks are relentless in modifying their malware to use new algorithms and encryption keys. Nonetheless, it's worth a try before you give up.

4. As a last resort, you may consider paying the ransom. To do this, you will have to set up an account at one of the Bitcoin exchanges, such as Coinbase.com. You will have to purchase

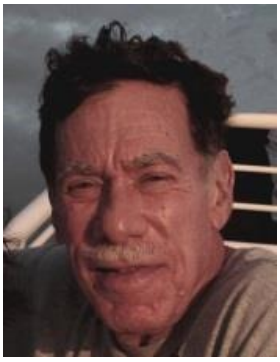
enough Bitcoin to cover the ransom demand and then make the transfer to the cybercrook's account. ***Caution*** – you're dealing with criminals! There's no guarantee they'll deliver. And if they do, there's no guarantee that, even if they do decrypt your data, that they'll also completely remove the ransomware. So, they may get you again, and again! Once your encrypted data files are recovered, make a safe, offline backup copy of them. Then you should at minimum run a deep virus scan. Better would be to wipe your hard drive as in item 2 above.

Conclusions

While I have mainly discussed ransomware in this article, *all* malicious software is dangerous. The same social engineering infection techniques are used by identity thieves. If they can get malicious software installed and running on your PC and can scan your files, they can find your account numbers, PINs, passwords and personal information and use that to hijack your financial accounts. Recovering from identity theft can be miserable.

I can't stress enough, the Internet is a wonderful resource for finding and sharing information, for making connections and for doing business, but it also a dangerous jungle. Predators are everywhere. If you are going to go there, you must be constantly wary and take steps to protect yourself.

Take to heart the preventive steps described earlier and hopefully you won't have to deal with the recovery steps.



Kretchmar's Korner

By David Kretchmar, Computer Hardware Technician

Don't Buy Identity Theft Insurance

Lifelock is the heavily advertised consumer data protection service that is offered by Symantec, a cyber security company better known for their Norton Security Suite. Symantec acquired LifeLock early in 2017.

Lifelock premiered in 2005; you might remember the commercials at that time featuring Lifelock CEO Todd Davis revealing his Social Security number to the public. Lifelock failed to disclose that Davis' identity was stolen at least 13 times during the advertising campaign. Lifelock brushed off critics, claiming that Lifelock prevented Davis' identification from being stolen many other times, thereby proving the value of Lifelock.

Lifelock attempts to frighten consumers by saying:

"Considering everything you do online, data breaches and companies that sell your information, it's easier than ever for criminals to steal your identity. They can open accounts, buy properties, and even file tax returns in your name. There's a new victim every two seconds, so don't wait to get protection!"

But of Course LifeLock has the answer:

Note that LifeLock does not offer a family plan; Lifelock coverage for a married couple is well over $50 a month. Lifelock does offer a small discount when a couple enrolls.

What Do You Get for Your Money?

Sadly, very little, except a false sense of security. If you are the victim of identity theft, most institutions will absorb the cost and charge you nothing. The few consumers who do suffer monetary damages rarely lose significant amounts of money.

Go to LifeLock's website and you will notice that ***"Not all transactions at all accounts monitored"*** is asterisked everywhere. Basically this gives them an out in case anything actually ever happens to one of your accounts.

A close reading of all of LifeLock's service and reimbursement "guarantees" discloses so many exceptions and conditions that any guarantees are essentially worthless. There have been numerous consumer complaints against LifeLock over the lifetime of that company.

LifeLock's Legal Problems

The Federal Trade Commission in 2015 asserted that LifeLock violated a 2010 settlement by continuing to make deceptive claims about its identity theft protection services, and by failing to take steps required to protect its users' data. In late 2016 LifeLock paid consumer damages of over $100,000.000.00. This was almost half of LifeLock's annual advertising budget, and they spend a lot on advertising. LifeLock has so far successfully sealed the court records relating to the settlement, but I think it is fair to assume that the final settlement addressed the FTC's 2010 and 2015 complaints.

The 2010 settlement stemmed from previous FTC allegations that LifeLock used false claims to promote its identity theft protection services. The settlement barred the company and its principals from making any further deceptive claims. It required LifeLock effectively safeguard personal data it collected from customers, and required LifeLock to pay $12 million in consumer refunds.

How Can I Protect Myself?

LifeLock's primary service is nothing you can't do yourself. If you think someone has stolen your identity, for instance you receive an American Express monthly statement showing purchases, but you do not have an American Express card or account. You would first contact that card's customer service.

Next you can contact each of the three major credit bureaus, TransUnion, Experian or Equifax, and place a credit freeze, also known as a security freeze, on your record. The freeze is good until you lift it, and should prevent any new accounts from being opened. A credit freeze prohibits, with certain specific exceptions, the consumer reporting agency from releasing the consumer's credit report or any information from it without the express authorization of the consumer. You can temporally lift the freeze if you want to open new accounts.

There is no charge for a credit freeze if you are a victim of identity theft.

To get a free credit freeze you should first file a police report or (much more easily) create an Identity Theft Report at:

www.identitytheft.gov/Assistant#what-to-do-right-away

This FTC site is easy to navigate and has some excellent information on what to do after an identity theft.

Conclusions and Recommendations

Don't buy identity theft insurance from LifeLock or any of the other outfits selling this protection. LifeLock cannot do nearly as much as you can do yourself to prevent, and recover from, identity theft.

The best way to protect yourself against loss is to keep an eye on your own bank, credit card and brokerage accounts and statements. Download your annual free credit reports yourself, and safeguard your passwords. If you are paranoid about identity theft, go ahead and put credit freezes on at the three major credit bureaus.

June Lab Monitor Schedule

Open Lab sessions are held twice per week: 9 am to noon on Wednesdays and Saturdays.

JUNE 2017	Monitor Schedule
Marcy Ishum	SATURDAY
Donna Bailey	June 3, 2017
Carol Przybycien	WEDNESDAY
Linda McMullin	June 7, 2017
Fred Cohen	SATURDAY
Ann Warhaftig	June 10, 2017
Jan Edwards	WEDNESDAY
Jim Edwards	June 14, 2017
Mary Hedin	SATURDAY
John Zuzich	June 17, 2017
Blanche York	WEDNESDAY
Jeff Southwell	June 21,2017
Mary Hedin	SATURDAY
Susie Scott	June 24,2017
Joyce Davidson	WEDNESDAY
Marilyn Gramms	June 28, 2017