Practicing Safe Computing by Hal Bookbinder
Index

Article	Published	Page
#28: "Password Managers, Again"	January 2018	30
#27: "Take care when you use Google"	December 2017	29
#26: "What is the 'Dark Web'?"	November 2017	28
#25: "Top 10 Tips for Detecting Phishing"	October 2017	26
#24: "The Internet is forever"	September 2017	25
#23: "Phishing email from your Bank"	August 2017	24
#22: "Modems and Routers"	July 2017	23
#21: "Verizon 2017 Data Breach Report"	June 2017	22
#20: "Protection from WannaCry Ransomware"	June 2017	21
#19: "Malware Protection"	May 2017	20
#18: "Viruses, Worms, Trojan Horses, Spyware"	April 2017	19
#17: "Searchable Government Databases"	March 2017	18
#16: "Wireless Access"	February 2017	17
#15: "Yahoo again, Biggest Hack Ever!!!"	January 2017	16
#14: "Verifying What You See"	December 2016	15
#13: "Yahoo Email Services"	November 2016	14
#12: "Password Managers"	October 2016	13
#11: "Sharing Your Family Tree & Identity Theft"	September 2016	12
#10: "Passwords"	August 2016	11
#09: "Social Engineering"	June 2016	10
#08: "Avoiding becoming victim of Ransomware"	May 2016	9
#07: "Backing up your System"	April 2016	8
#06: "Is it true that Apples are safer than PCs?"	March 2016	7
#05: "What are 'cookies' and should they concern you?"	February 2016	6
#04: "Is Your Virus Protection Actually Working?"	January 2016	5
#03: "A Free Scan of Your Computer"	December 2015	4
#02: "Credit reporting agencies"	November 2015	3
#01: "Don't help them steal your identity"	October 2015	2

Go to Index

Practicing Safe Computing #1: “Don’t help them steal your identity” by Hal Bookbinder
Originally published in the October 2015 issue of *Venturing into our Past* (JGSCV)

You receive an email letting you know that your information may have been part of a recent breach of health records. The email looks official with the familiar logo of a hospital that has treated you. It expresses sincere apologies and is signed by the CEO of the hospital. It asks you to click on a link to find out more about what the hospital will do to protect you from identity theft.

When you click on the link you see a screen with the hospital’s logo that lets you know that they will pay for credit monitoring service for the next 2 years at no cost to you. You can decline and take your chances or accept the free offer. It seems like a no-brainer and you are relieved that the hospital is taking the breach and your financial protection seriously.

You click on the “I accept” button and a form is displayed to initiate the coverage. You are asked for your full name, mailing address, phone, email, date of birth, etc. You are a bit concerned however when you see that you are also asked for your social security number and a major credit card. When you click on the question mark by these fields, an explanation is displayed that makes sense.

You enter the data and confirm its accuracy. The screen provides you with a reference number for your free policy and a phone number to call if you have any questions. Surprise, you have been “phished” and your data is on its way to a third world country where it will be sold to con artists who may use it to steal your identity, purchase big ticket items on your credit or obtain Federal tax refunds in your name.

Never provide personal information when contacted unexpectedly, no matter how legitimate and logical the request seems; do not even provide basic information like your address and phone number. Rather, close the email and if you are concerned contact the hospital (or bank or insurance company) directly. You will likely find out that they never sent the email.

Institutions may well send you email about an issue. However, when an unsolicited email asks for personal information, this is a warning that you are at risk. These scams rely on the headlines of the day. Today’s headlines tell of huge data breaches. So, when you get an email about this, it seems legitimate. These criminals know what they are doing. Always remain on your guard.

If you have been phished, take immediate action. Close credit or debit cards or bank accounts whose information you provided and contact the three main credit-reporting agencies to place a fraud alert on your accounts. These are minimum actions, do your research to see what other steps you should take. Yes, it is a hassle, but nothing like the hassle if your identity is compromised.

Go to Index

Practicing Safe Computing #2: "Credit reporting agencies" by Hal Bookbinder
Originally published in the November 2015 issue of *Venturing into our Past* (JGSCV)

My October "Safe Computing" article suggested you contact the credit reporting agencies if you have been "phished" and feel that your identity may have been compromised. This article covers how to do this and what you might request.

There are three major credit-reporting agencies in the U.S. - TransUnion, Experian and Equifax. By law, you are entitled to one free credit report from each every year. To get your free credit report, go to www.annualcreditreport.com. You will be quizzed to ensure your identity. For example, you might be asked the amount of your monthly mortgage or car payment and be given a number of ranges.

You can obtain any or all of your three credit reports. While there are some differences, for the most part they are redundant. Therefore, what I do is put a reminder on my calendar at four-month intervals to get one of the three credit reports, keeping me aware throughout the year. Check the report carefully for accuracy. It will provide you with instructions for contesting erroneous information.

There are commercial sites, with the words "free" in them that look a lot like the official free site above. Using some will start a monthly charge while others are truly free and rely on up selling you additional services. If you do sign up for a credit monitoring service, be sure you know what you are getting for your money. In addition, check your credit card statements carefully for any resultant charges.

If you are concerned that your identity may have been compromised, consider establishing a "security freeze" with each of the three credit reporting agencies. With a credit freeze, the agency will not approve credit, loans and services being approved in your name without your consent. However, this may delay, interfere with or even prohibit the timely approval of legitimate requests for new credit.

The nominal fee for a security freeze is typically waived if you are over 65 or have submitted a complaint with a law enforcement agency stating that you believe you are a victim of identity theft. You can later temporarily, or even permanently, suspend the security freeze. Again, a nominal fee is typically waived if you have an active complaint.

A less intrusive alternative is a "fraud alert". This requests that the potential credit grantor verify your identification before proceeding with the transaction. A fraud alert is free and lasts 90 days. If you request a fraud alert of any of the three companies, they are required to notify the other two. (However, I would verify that the others have recorded the alert). A fraud alert can be renewed for 90 days. It can be extended to one or seven years if you have submitted a complaint to a law enforcement agency.

Contact Information for the Credit Reporting Companies:
TransUnion, http://www.transunion.com, 1-800-680-7289,
Experian, http://www.experian.com, 1- 888-397-3742,
Equifax, http://www.equifax.com, 1-888-766-0008
To obtain your free annual credit report:
https://www.annualcreditreport.com
For more information:
http://www.consumer.ftc.gov/articles/0155-free-credit-reports
http://www.federalreserve.gov/creditreports
https://www.ftc.gov/faq/consumer-protection/get-my-free-credit-report

Go to Index

Practicing Safe Computing #3: "A Free Scan of Your Computer" by Hal Bookbinder
Originally published in the December 2015 issue of *Venturing into our Past* (JGSCV)

You are surfing the web when a screen pops up telling you that you have 23,179 instances of malware (or viruses or worms) or porn on your computer. It offers to scan your computer and remove these at a low cost or even for free. Never take these people up on their offer to protect you through a one-time cleaning of your computer. They are great at scaring you. Do not take the bait.

The pop-up has no idea how many instance of bad stuff you have on your computer (though it is a pretty good bet that even with anti-virus software, you have some), If you give the soliciting message the authority to scan or to fix the problem you are giving them control of your computer. In addition, you have no idea what they will actually do with that authority. One thing for sure, it will benefit them and not you.

In a similar scam, the pop up informs you that you are infected with some specific virus (often one that you have recently read about in the news). This message is likely being spammed to hundreds of thousands of others expecting that some percentage will pay to be "cleaned." If you pay, at best there will be a faux cleanup letting you know that everything is now Ok.

At worst, the spammer, once given control of your computer will install new viruses, steal your information, or even freeze your computer with ransomware (a topic for another article). The company name displayed often mimics well-known and trusted brands. However, these trusted companies do not operate in this way. If you give these con artists control, nothing good will come of it.

If the message scares you, this is not all bad. You should be concerned to keep your computer free of malware. Close the message without responding. Do not click on the box in the popup asking to be taken off the contact list. This just confirms to the spammer that you are real and you will result in even more spam.

Allay your concerns by running your antivirus software to check the current state of your computer. If your virus protection is out of date, get a current subscription. Consider going to a trusted site (like www.microsoft.com or www.mcafee.com) and see what tools they offer to check the health of your computer. However, under no circumstances give control to strangers who, unsolicited, reach out to you.

Similarly, do not fall for emails that you receive offering free or low-cost scans and cleanup of your computer. Again, you really do not know with whom you are dealing. Do not accept the offer no matter how tempting, scary, or trustworthy it seems. In addition, as before, never click on the request to receive no further emails. This will instead result in you being placed on even more spammers' lists.

Go to Index

Practicing Safe Computing #4: “Is Your Virus Protection Actually Working?” by Hal Bookbinder
Originally published in the January 2016 issue of *Venturing into our Past* (JGSCV)

We all know the importance of maintaining virus protection on our computers, but many do not realize that their virus protection is not protecting them at all. Virus protection consists of two equally critical components. One is an engine that runs regularly to scan your files and messages for signs of malware and to then block or clean the malware that is found.

The second component is a list of current malware patterns. Without this, your anti-virus engine may continue to run and to protect your computer against the malware that was known in the past, but may not recognize the latest patterns and so let them slip by. You must maintain your subscription or the updating of patterns will cease, even as the engine continues to function.

Folks are sometimes fooled in that they see that the anti-virus product that came free with their computer continues to run long after its initial period has ended. They ignore the messages encouraging them to make a subscription payment figuring that they will handle this later, and the product seems to be working.

Some think that going for a time without virus protection is no big deal. They can always purchase an even better product later. However, as the days drag into weeks and then months the computer continues at risk and the malware multiplies. Additionally, some of this malware can burrow so deeply into the system that removal without a complete and expensive rebuild becomes impossible.

While your friends may prefer one product to another, all of well-known commercial products work well. The critical thing is to ensure that you have some product installed and that its list of patterns is being kept up to date. If not sure, go to the website of the product, you have and it will certainly offer to run a scan to tell you if you are up to date and running properly or at risk.

Sometimes software installation instructions instruct you to temporarily turn off your virus protection. Unfortunately, people sometimes neglect to turn it back on and so are running at substantial risk. Your virus protection should be set to scan all incoming messages, periodically check your entire system, and regularly download the latest malware patterns. If unsure, use the default settings.

Two virus-protection programs are not better than one. Each will perceive the other to be doing something that warrants monitoring. This conflict may actually slow your computer as each continues to confirm that the other is not, in fact, malware. So, if you decide to switch to another anti-virus program, uninstall the old one and then immediately install the replacement.

One anti-virus product, PC-Matic, touts that it is American made and uses “white-listing” to better protect you from visiting dangerous websites. While I like both concepts, I do not endorse this or any product. I just encourage you to spend the $15-$30 per year and stay current. This is far better than losing valuable data and paying $300-$400 to reinstall your system.

Go to Index

Practicing Safe Computing #5: "What are 'cookies' and should they concern you?" by Hal Bookbinder
Originally published in the February 2016 issue of *Venturing into our Past* (JGSCV)

While baked cookies can add on the pounds, computer cookies are so light that you can have hundreds or thousands of them on your computer and they will not slow it down. Cookies are small files of data that are used to facilitate your use of the Internet. They are not inherently bad. You can set your security settings to disallow them, but you will not like the results, as you will find that you cannot access many sites that require cookies to be enabled. You can set your system to purge cookies each time you close your browser or simply let them accumulate.

Cookies provide "persistence" which allows you to stay logged into a website. When you log in to a site, a handshake value is placed in a cookie file on your computer that is specific to that website. Each time you then send a transaction to that website (an update or query), the transaction grabs this handshake and includes it, thus confirming who you are and that you are indeed still logged in.

Cookies can contain preferences to personalize your experience for a specific website. Therefore, if you identify topics of interest and these are displayed when you go to the site, this is because your preferences are stored in a cookie and sent to the website when you access it. If you identify at a brokerage site which page is to be initially displayed, this information is similarly stored in a cookie. Cookies are unique to a single website and generally only useable when linked to that website.

A potentially dangerous use of cookies is to use them to store your login information, including your password, for a particular site on the Internet. You have certainly been asked if you "want to be remembered from this computer" and so speed your login. If you accept this offer, your ID and possibly your password are stored in a cookie that is then queried when you later access the site.

Even though the information is encrypted (i.e. scrambled so that it cannot be easily read), it could be used by someone who gains access to your computer to log into sites with your credentials. Malware could even use or export them. As I would prefer to leave no opportunity for another to log into my brokerage account, bank or credit union and take actions in my name I routinely decline to accept offers by websites to remember me.

Deleting cookies will not harm your computer. However, this will remove the website "personalizations" you have constructed over time. You can instruct your computer to delete all cookies each time you close your Internet browser, except those related to selected "favorite" sites. This is precisely the way I have set up my Internet Explorer, Chrome and Firefox browsers.

For specific instructions for your setting cookie rules for your browser, search for "Managing cookies in Firefox 40.0.3" using the actual name and version of your browser. To find the version of Firefox you are using, click on three bars symbol in the upper right hand corner of the page, then click on (?) and then "About Firefox". For Chrome, click on the three bars symbol, then "Help and About" and then "About Google Chrome". For Internet Explorer, click on the Tools icon (looks like a gear), and then "About Internet Explorer".

Go to Index

Practicing Safe Computing #6: “Is it true that Apples are safer than PCs?” by Hal Bookbinder
Originally published in the March 2016 issue of *Venturing into our Past* (JGSCV)

Yes, it is true. Apples IOS operating system has proven to be less impacted by viruses than PCs running any version of Windows. The reason is two-fold. First, with about 7.2% of the market for desktop and laptop computers vs. 91.4% for Windows based PCs, virus creators find it more attractive to write malware for PCs (the remaining 1.4% of personal computers use a variant of the Linux operating system).

The second reason relates to the way Apple updates its operating system vs. the way Microsoft updates Windows. Microsoft does its best to provide for backward compatibility. In other words, they want to see that programs that ran on earlier versions of the operating system continue to run. This translates into lots of old code being included in current Windows operating systems.

With about 50 million lines of code, much of it carried forward, there are many opportunities for mischief as hackers discover flaws in the software that they then exploit through malware. When this occurs, Microsoft releases a security patch to close the flaw and the anti-virus companies release an update to counter it. However, they are always playing catch up and there is an inevitable lag.

When Apple releases a major operating system upgrade, it is built fresh. If older software will not run, so be it. Apple is more focused on the overall user experience with its current operating system and associated software rather than compatibility with older versions. So, as an Apple user you may find that you have to buy a new version of software when upgrading to the newest operating system.

By writing new code, Apple can concentrate on protections and the user experience and does not have to content with protecting old operating system code. While Apple does a good job in controlling viruses endangering the Apple system, it does not do as much regarding viruses and worms simply using the Apple as a landing place on their way to a Windows PC.

Apple users remain at risk for phishing in which unscrupulous folks strive to obtain personal data. Therefore, Apple users still need to be on their guard. Half a dozen companies provide Apple-specific anti-virus software. While the risk is lower, Apply users owe it to themselves (and the PC users with whom they interact) to acquire and run anti-virus software on their machines.

As PC Magazine wrote on February 13, 2015, “Mac users simply cannot be complacent and leave their machines unprotected. Even if they never encounter malware, they would certainly benefit from social media protections and keeping their machines from being used to attack other computers. And with numerous free options, there's simply no excuse; get antivirus protection for your mac today.” - *11 Antivirus Apps for Mac*.

Go to Index

Practicing Safe Computing #7: “Backing up your System” by Hal Bookbinder
Originally published in the April 2016 issue of *Venturing into our Past* (JGSCV)

We all know that we should be regularly backing up our data. However, the fact is that many of us do not back up our data frequently enough, if at all. Some think it is complicated or expensive and many have become complacent after years of using computers without problems. Do not wait for a data loss to shake this complacency.

We all need to frequently back up our data and store these backups in a different location from the computer on which it normally resides. Many purchase an external hard drive and set it up so that automatic backups are taken daily. This is good as far as it goes. However, what happens in a disaster where there is a fire, flood, or earthquake and both the computer and its local backup are destroyed?

This can be avoided by using one of the available commercial services through which your data is automatically backed up to the cloud. These services are relatively inexpensive. Alternatively, you could set up a cloud backup yourself by placing a cloud storage device at another location and backing up to it using software that performs regular backups, daily or more frequently.

Recognize that backing up everything on your computer is not necessary. The Operating Systems and computer software can be re-installed. Downloaded music and movies can be re-downloaded. However, your own pictures, family information, research, financials and more should be backed up off site.

Consider setting up a logical drive or directory on your computer dedicated to the data that is to be backed up. You can routinely copy the contents of this drive or directory onto a USB “thumb” drive and keep it on your key chain as I do. So, I have my data wherever I happen to be, whether or not I have Internet access.

This is not a substitute for regular, scheduled backups, but an additional step you may consider. If you have a particularly important file that you have just created and cannot afford to lose, you could copy it to the thumb drive or attach it to an email and send it from your home to office or vice-versa.

Most of us have experienced that horrible feeling when our computer loses power after we have put a great deal of time into creating or updating a file and just before we were going to save it. To avoid this, set your system to regularly save your files as you update them. Consider setting this to occur every five or ten minutes. Additionally, consider taking a backup of any critical file before you start modifying them.

Another approach is to keep your data in the cloud. These cloud services routinely back up your data for you. However, as I never like leaving anything to chance I would want to have two physical backups under my own control as well, in two different physical locations. If I sound paranoid, I am a little. Once you experience a painful data loss, you may become a bit paranoid as well.

Go to Index

Practicing Safe Computing #8: "Avoiding becoming victim of Ransomware" by Hal Bookbinder
Originally published in the May 2016 issue of *Venturing into our Past* (JGSCV)

Ransomware is a form of malware that encrypts files on your computer and then demands payment in exchange for the passkey to access them.

In February, Hollywood Presbyterian Medical Center became the victim of a ransomware attack. Cybercriminals took control of the hospital's computers and encrypted data so that the hospital could not access or record patient notes. The cybercriminals demanded a payment to provide the hospital with the necessary passkey to unlock its files. The hospital paid $17,000 in bit coins, an untraceable way to pay the cybercriminals who likely accomplished this attack from a country with weak extradition treaties. The cybercriminals provided the passkey and Hollywood Presbyterian was back in business. They insist that no patient was at risk during the episode. However, they redirected emergency patients to other hospitals while dealing with the attack.

Cybercriminals target individuals as well as institutions. Playing the numbers, they likely make more money at $200 to $400 per attack against individuals who tend to focus less on protecting their systems than institutions. Most people will readily fork over a few hundred dollars to regain control of their system and data. When the cybercriminals take control, they display a warning screen letting you know you have been hacked and instructing you to purchase bitcoins or a cash card and then go to a site on the untraceable "dark web" to make your payment. The passkey to unlock your data is then provided. The cybercriminals want to maintain their reputation for honesty after the payment is made.

"Locky" is the nickname of one strain of ransomware. It encrypts and then renames all your important files so that they have the extension .locky. It generally arrives as an email attachment. When you open the attachment, it appears scrambled and you are instructed to "enable macros" to unscramble the message. In actuality, this will run code to implant the ransomware on your computer. "Jigsaw" is another new ransomware program that actually starts destroying files if you delay in obtaining the bitcoins to pay off the cybercriminals. It displays a countdown clock on your screen to let you know that you have one hour to make the payment and if late, you will not get back all of your data files.

To protect yourself:

- Be cautious about unsolicited attachments. If in doubt, do not open it.
- Avoid going to sites on the Internet that you do not know to be safe.
- Do not enable macros in document attachments received via email.
- Consider installing the Microsoft Office viewers. They let you see what documents look like without opening them in Word or Excel and do not permit macros.
- Maintain current virus protection and automatically download security patches for your various programs (like Office, Flash and Chrome).

Finally, backup regularly and keep a recent copy off-site. You will then have the unhappy choice of paying the cybercriminals for the passkey or paying your computer support person to reinstall your system and files. Such is life in the cyber age!

Go to Index

Practicing Safe Computing #9: “Social Engineering” by Hal Bookbinder
Originally published in the June 2016 issue of *Venturing into our Past* (JGSCV)

Ever notice that when a big headline hits the news you get emails on the topic? This is a typical way social engineers get through your defenses. Prince suddenly died this past April. The news, the blogs, television and radio contained almost non-stop coverage of the tragic event, speculating on the cause of his death and extolling his memory. You likely received at least a few emails on the event.

Since the story was all over the place, we tend to be less suspicious of an email on it. Therefore, if you are into pop music, or just a news junkie, you may have opened the email without thinking whether it might contain a virus. You might have even clicked on the button in the email to play a commemorative Prince tune. Social engineers recognize that folks let their guard down in such circumstances.

However, you feel that this will never happen to you because you would just delete such a message. After all, you are not into such pop music culture and know not to open emails from sources you do not know. Ok. Now substitute a recent bus bombing in Israel or the latest outrageous thing that Donald Trump said or (and I love this one) an email about the latest scam in the news.

Social engineers use topical news to send out viruses to infect your computer and possibly steal your personal information. So, maintain your guard when you receive emails on the latest headline. If you do not recognize the source, be wary about opening the email. In addition, never, never, click on any link or button contained in the email. You will be inviting viruses to come aboard your computer.

When you get a call from Citibank informing you that they have a thieving teller who has been inappropriately accessing customers’ accounts and that they need your help to trap her, be wary. They may even offer you an award if you help provide evidence. Of course, they will need some information from you. The person is friendly and seems sincere and very believable, which is typical of a good social engineer. You want to help, and the $500 reward does not hurt.

You think that you would never be fooled by such a call. You know it is likely a scam. However, when it occurs, you may not be thinking as clearly. In addition, the caller seems so nice, friendly and believable. Enough people fall for such approaches to provide the social engineer with a regular stream of stolen identities and cash. Never be tricked into giving out personal information when you are contacted by phone, email, instant messenger or at your door.

Additionally, older people tend to be more trusting. Possibly, it is because we grew up in a different age. Whatever the reason, do not let yourself be fooled into sharing your personal information, opening emails or linking to websites when contacted by social engineers who rely on our good nature, greed, curiosity, trust and desire to be helpful.

Go to Index

Practicing Safe Computing #10: “Passwords” by Hal Bookbinder
Originally published in the August 2016 issue of *Venturing into our Past* (JGSCV)

We all know that we should be careful about selecting, protecting and changing passwords. However, how can you do this when you are told to maintain different passwords for your various websites, that they must be long and complicated, that you should not write them down and you should change them frequently? Impossible! Right? While this may be an annoying challenge, it is not nearly as bad as suffering an attack in which your accounts are emptied or critical personal information is stolen.

Passwords should not include any information that could be found about you. You mention that “blue” is your favorite color on Facebook. Your bio says you were born in the “Bronx”. You occasionally mention your dog “Scooby” in emails. These bits of information provide a great start in guessing your password. Do not use family names, pet names, towns or streets where you now or have ever lived, phone numbers or favorite colors, foods, songs, movies or drinks. Simply putting a “1” at the end will not help. Hackers will use automation to try all these things and will add digits and special characters.

Do not use simple sequences like “ABCD”, “4321”, “1111”, “1a2b3c4d”, or “1234ABCD”. Do not use “QWERTY”, “14789” or any other simple string of characters from your keyboard or phone keypad. If it is simple to remember, it is simple for the hacker to crack. The hacker’s automated tool will attempt all of these predictable sequences.

The best passwords are random collections of upper and lower case letters, numbers and special characters. However, these are generally impossible to remember. Therefore, your best bet is to choose a couple of unrelated words and combine them, with a digit or two and a special character or two. So, say you choose “Home” and “Spring” and make the password “Home4Spring5!” or the slightly more complicated, “HoMe4SpRiNg5!”.

Realistically, if you have a half dozen or more of these you will have a hard time remembering them. However, if you write them down, this list could fall into the wrong hands. I record them in a password-protected file on my encrypted computer. I just have to remember one complex password, the one to open this file.

This is a low-tech version of a password wallet - an online tool that keeps all of your passwords and provides them as needed directly when needed. Better wallets will even generate new complex passwords as required. Then, you could have a hundred complex passwords, all different. You will need to remember just one password, the one to authorize and access your password wallet.

While you can pay for an encrypted USB stick or a software based password wallet, there are excellent free services as well. One is “dashlane.com”. However, you still have the challenge of remembering that one complex password to get into your password wallet. Ok, write it down, just in case you forget, and store it in a safe place, like your safe deposit box - and not on the back of a business card in your wallet!

Go to Index

Practicing Safe Computing #11: “Sharing Your Family Tree & Identity Theft” by Hal Bookbinder
Originally published in the September 2016 issue of *Venturing into our Past* (JGSCV)

Some choose not to share their family trees out of concern about identity theft. Your tree does contain personal data of interest to identity thieves such as birth date and place, address, phone number, email and mother’s maiden name. However, it does not contain the information they most want including social security number, credit card, bank account and investment account numbers and passwords.

At the recent IAJGS conference, Randy Schoenberg stated that there are “zero instances of identity theft resulting from shared family trees.” He further stated that family members perpetrate the majority of identity theft. While it would surprise me if there were truly no instances of identity theft related to the sharing of family trees, a quick Internet search did not turn up much.

According to Bruce Kennedy in CBS Moneywatch, “Numbers vary, but a study quoted by credit information firm Transunion revealed that nearly one-third of identity theft victims later determined that a family member or relative was responsible for the crime.”

Posting your family tree can vastly increase it as you link up with others and identify possible relatives about whom you knew little or nothing. There is simply no better way to expand your tree than through the cooperative effort of others, some whom you may not yet know.

You may find some or all your tree already posted by others and this may contain incorrect or private information. You may also see information on living relatives. Some sites suppress such information, others permit it. There is no legal obligation to hide such information. While this may disturb you, you have little legal right to force its removal.

Before you upload your tree, read the “terms of use” for the site. You may find that by uploading your data, you are “contributing” it and the company has ongoing rights to its use, even if you no longer want it exposed. Check on what privacy is offered and what rights you have. You may not like what you find. However, you may conclude that the tradeoff is something with which you can live. Identify thieves have other ways to get the personal information they need. They do not need access to your family trees.

To lessen the likelihood of identity theft, use and regularly change complex passwords, password-protect the logon to you home computer, log off when you walk away, do not provide other users “administrator” rights, shred your paid utility bills and carefully review all credit card and bank statements. Take note if you do not receive an expected statement, periodically review your credit report and consider tightening the rules pertaining to getting credit under your name with the credit agencies. All of these steps were discussed in prior articles in this series.

There are legitimate reasons for not sharing your family trees. However, there are more important steps to take to protect yourself from identity theft.

Go to Index

Practicing Safe Computing #12: "Password Managers" by Hal Bookbinder
Originally published in the October 2016 issue of *Venturing into our Past* (JGSCV)

Password managers store your login information for the sites that you visit. They then automatically log you in to the site once you bring up the login page. Better password managers will generate unique complex passwords for you, fill in forms and synchronize across your devices. Some even provide legacy features to pass on your access to another, so that if you become incapacitated or die, someone will be able to access your accounts.

I tried the free version of one of the very best password managers, Dashlane 4. It did a great job in automatically capturing IDs and passwords as I logged into websites and then replayed them when I went to those sites again. However, it was constantly pushing me to purchase the commercial version that was required for important functions like being able to view, update, delete or synchronize passwords across various devices. Eventually, I uninstalled it and focused on the free password managers.

An excellent free password manager is LastPass 4.0. It is intuitive, providing "cards" for each website you wish to access and displaying them in logical folders. You enter a description, ID and password into each card. I set up separate folders for financial sites, frequent flyer sites, genealogy sites, email sites, retail sites and social sites. I then simply clicked on the card for the site that I wished to open and LastPass logged me in.

LastPass presumes sites have a single ID and single password to log in. You may have to enter some fields for sites that do not fit this profile. For example, the American Airlines' Frequent Flyer site requires an ID, a last name and a password. LastPass entered the ID in both of the first two fields requiring me to overtype my last name - a minor annoyance.

Some sites do not permit you to go directly to a login page but rather have an icon on the home page that displays the login function. In these cases, clicking on the LastPass card icon brings up the home page. You must then click on the login icon and then have LastPass fill in the required information. Some of the commercial tools are more sophisticated and include unique profiles for hundreds of sites.

LastPass also generates complex passwords on request that you can use to better protect yourself. This is especially for important sites. Download it from http://www.lastpass.com. Please do your own investigation to select the right tool for you.

Commercial password managers cost $20 to $40 per year. For excellent comparisons of these tools, see "The Best Password Managers of 2016" (http://www.pcmag.com/article2/0,2817,2407168,00.asp) and "The Best Free Password Managers of 2016" (http://www.pcmag.com/article2/0,2817,2475964,00.asp).

A password manager is a convenient, secure way to maintain different passwords for the various sites that you visit. Of course, you must create and remember a password for your password manager. Consider recording it in a secure location, like your safe deposit box - just in case.

Go to Index

Practicing Safe Computing #13: "Yahoo Email Services" by Hal Bookbinder
Originally published in the November 2016 issue of *Venturing into our Past* (JGSCV)

You are all likely aware of the mass theft of user data from Yahoo in which information for over 600 million customers was stolen in 2014, becoming known only in the last few months. (If you have a Yahoo account and have not changed your password since 2014, do so immediately. If you use the same password on other accounts, change them as well.)

Yahoo is reeling and playing defense in trying to retain its business. The LA Times reported in its October 11, 2016 edition that Yahoo has quietly shut down the ability of users to turn on mail-forwarding services. According to the article, Yahoo claims that this is temporary while they "improve" the service. This standard function permits you to receive email in one mailbox and immediately forward a copy to another. It permits you to consolidate all email into one mailbox.

I have email accounts in Gmail, Yahoo, MSN, UOP (University of Phoenix), UCLA Bruin and Roadrunner (Times Warner Cable) and consolidate them all into my primary UCLA Medical Center account. Therefore, if you send an email to me at hal@jgscv.org or hal.bookbinder@ucla.edu, you will likely get a response from hbookbinder@mednet.ucla.edu. This is the account that I monitor.

Along with consolidating email, forwarding is also used to facilitate moving from one email service to another and Yahoo clearly does not want to help you do this. Once you set up a new email service, by setting up forwarding, email from those who use your old email automatically shows up in your new mailbox. By using an "out of office" notification in your old mailbox, you can let them know that this mailbox will shortly close. Alternatively, you can just notify those you want to be aware of the change.

You then can opt to close your old email or not. If you close it, those who use it will get a message that it is not a valid address. If you leave it active but simply stop using it, emailers, including spammers, will have no awareness that it is now dead. Some family or friends may wonder why you are ignoring them.

If you had forwarding turned on in your Yahoo email before they took this action, the Times reports that it should still work. Yahoo simply turned off the ability to invoke this feature. This is presumably a defensive move to make it more difficult to move away from Yahoo. Likely, the blowback they will get will result in Yahoo restoring the function. With their mass-hacking, bleeding money (reported loss of $5.19 per share as of 7/18) and anti-customer actions such as these, one might question whether to remain with Yahoo it all.

Of course, there are issues with other email services as well. Many are concerned about the scanning of emails reportedly done by Gmail and what other free services are doing with your information. Email has become a lifeline. Pay attention to your email service and have an escape plan.

Go to Index

Practicing Safe Computing #14: “Verifying What You See” by Hal Bookbinder
Originally published in the December 2016 issue of *Venturing into our Past* (JGSCV)

We all receive emails from friends passing on the latest information that they got from the Internet. It sounds plausible, you trust your friend and so you pass it on to more friends, or worse yet, act on the information without checking it first.

In February 2016, folks were receiving advice to reset their iPhone date manually to January 1, 1970. Various reasons were given which sounded compelling. Yet, doing so would result in permanently disabling your iPhone. Apple acknowledged this bug and fixed it in iOS 9.3.1 in April. I am not brave enough to check it out myself on my iPhone. DO NOT TRY IT!

Another item that periodically circulates is a notification that you may be infected and to check your computer for a particular file or value to confirm this. It then advises that you should immediately take an action, like deleting a particular file or running a script from a particular website. The file or value indicated is a normal component and removing that file may cripple your PC. Be assured that the script, should you choose to run it, will be infecting or otherwise damaging your PC.

Be careful about acting on, or passing on, information you get on the Internet, whether through searching websites, emails out of the blue, or emails from trusted friends. Much of what is passed around is completely false or plausible sounding half-truth. Taking action without checking it out may cause you real damage. Sending it to friends may just spread a falsehood, or worse, a virus.

If you get an unsolicited advisory regarding your financial institution log directly into their website (DO NOT CLICK THE LINK IN THE EMAIL) to check it out. If you get an advisory related to Microsoft, Dell, Apple, Intuit or whatever, similarly check it out before taking action. Links in emails may bring you to a page that looks legitimate, but is not. If you attempt to log in, you may be giving your log in information to folks who may use it fraudulently. Subsequent challenge questions may be used to obtain even more information.

Two websites that have a good reputation for investigating and debunking Internet nonsense are www.snopes.com and www.truthorfiction.com. The descriptions below come from Wikipedia.

> “Snopes.com, also known as the Urban Legends Reference Pages, is a website covering urban legends, Internet rumors, e-mail forwards, and other stories of unknown or questionable origin.] It is a well-known resource for validating and debunking such stories in American popular culture, receiving 300,000 visits a day.”
>
> “TruthOrFiction.com (or TruthOrFiction.org) is a "myth busting" website about urban legends, Internet rumors, e-mail forwards, and other stories of unknown or questionable origin. The topics are researched by TruthOrFiction's staff, and rated "Truth" (if true), or "Fiction" (if untrue). When the accuracy is not known with certainty, the stories are rated "Unproven," "Disputed," "Reported to be Truth" or "Reported to be Fiction." Partially true stories are rated "Truth & Fiction."

Go to Index

Practicing Safe Computing #15: "Yahoo again, Biggest Hack Ever!!!" by Hal Bookbinder
Originally published in the January 2017 issue of *Venturing into our Past* (JGSCV)

In mid-December, Yahoo announced that they had discovered another hack in which 1,000,000,000 (one billion) accounts were compromised. The hack occurred in 2013 and so the hackers have had three years to exploit the information. This is twice the size of the hack that they announced just a few months ago (see article in November 2016 newsletter).

In addition to IDs and passwords, the hackers retrieved challenge questions answers (like, "What is your mother's maiden name?"). People tend to use the same password and/or challenge questions on their accounts. With the information from Yahoo, hackers can use programs that generate various combinations until they are able to access your other accounts. Challenge question answers may also be discoverable or guessable – especially if they are true.

While Yahoo claims that the breach did not include financial information, identifying your bank and other financial institutions is relatively easy using services available on the Internet. Alternatively, the hackers can simply try to access your accounts at a series of financial institutions until they find the one that works.

Previous articles have provided recommendations to secure your account access. However, they did not address the issue of challenge questions being compromised. Here are steps you should take:

1) Have different, complex, passwords for each of your accounts, especially ones that are sensitive, like financial and medical sites. (August, 2016)
2) Use a password manager to generate your complex passwords. I use LastPass. Complex passwords that you build yourself may still be able to be guessed. (October, 2016)
3) Store all of your login information in a password manager secured with its own complex password which you will need to remember. (October, 2016)
4) Keep a copy of the password to your password manager in a safe place, possibly your safe deposit box and definitely not on a slip of paper in your wallet! (October, 2016)
5) Set up your challenge questions with false and varied answers. Consistent, accurate challenge answers are discoverable. But, how can you now remember them? (new)
6) Record the challenge questions and answers in the notes area associated with each login in your password manager. (LastPass provides a visual "card" for each account). (new)
7) Change your passwords periodically - every 90 days is a good rule. (October, 2016)
8) Never click on an email link to what you think is your account. It may take you to a simulated page that simply captures your login information. Type the address yourself. (October, 2015)
9) Be careful when sharing personal information and never share login information. (June, 2016)
10) Immediately change your password if you suspect your password may have been compromised. (August, 2016)

The Yahoo breaches were not discovered for three years. So, do not wait for an announcement that your account may have been compromised. Take action now!

Think it is too much trouble to take these steps? Compare it to the trouble if your financial, medical or even social accounts are hacked. At a minimum, secure your most critical accounts.

Go to Index

Practicing Safe Computing #16: “Wireless Access” by Hal Bookbinder
Originally published in the February 2017 issue of *Venturing into our Past* (JGSCV)

You have a wireless router so that you can connect from anywhere in your home. Be aware of the exposures that come with wireless. Some of us retain the standard settings (ID and password) on the router. Anyone can easily find out the standard settings for your Linksys, Asus or other brand of router. This ID and password permits them to log into your router and update its settings.

Once someone logs in, they can then use this information to hijack your router, eat up your bandwidth or even intercept your traffic. Your wireless access does not stop at the walls of your house but can be accessed by your neighbors and by folks on the street. So, take the obvious first step and change the ID and password on your router. In addition, make it one that is not easy to guess. I routinely find folks with the password of “password”. Misplaced the paperwork on your wireless router? Just check the router manufacturers’ website for instructions.

You need to also set a wireless password so that only the devices you want to be able to connect to your router are able to do so. If you do not, your neighbor or the fellow on the street may be sharing your bandwidth, slowing your access. So, be sure to set a wireless password as well as updating the router login ID and password. Once you set the wireless password, you will need to add it to your laptop, tablet and smart phone so they will be able to access your wireless network.

A second line of defense is to encrypt your network traffic. This way, even if someone is able to intercept your transmissions, they will have a difficult time unraveling it. When you connect to a secure website, it generally has “https://” at the beginning instead of “http://” Your bank will quickly take you to their “https://” entry point where your subsequent traffic will be encrypted. For example, if you type in “www.bankofamerica.com”, you will be taken to “https://www.bankofamerica.com/”.

Many email systems, including Gmail, encrypt your messages. When you next go to “www.gmail.com” notice that what is displayed is “https://mail.google.com/mail/#inbox”. If you use another email service, look to see if it takes you to an encrypted website. If it does not, consider switching to one that does.

It is especially important that your transmissions be encrypted when you connect in an exposed, shared environment like Starbucks or the airport. Someone with the appropriate device may be intercepting the transmission and “listening in”. If you cannot get an encrypted connection, be very careful what you share. You never know who is listening.

While we typically obtain a wireless router so we can access the Internet from anywhere in the house, be sure to read the guide that comes with it and you will see that there are other functions that you may want to consider - including setting up a firewall and locking down access to adult or dangerous sites. More about routers and firewalls in a future article.

Go to Index

Practicing Safe Computing #17: "Searchable Government Databases" by Hal Bookbinder
Originally published in the March 2017 issue of *Venturing into our Past* (JGSCV)

The articles in this series have focused on avoiding computing problems. This article shifts to some government resources that may help find people. We will get back to avoiding problems next month.

Government agencies maintain numerous interesting searchable databases. For example, the Office of Inspector General at the U.S. Department of Health & Human Services maintains a searchable database regarding individuals and entities currently excluded from participation in Medicare, Medicaid and all other Federal health care programs. As of February 2017, it contained 2,974 entities and 63,306 individuals. One can search by the first letter(s) of the entity name or surname (Entering the wildcard "%" retrieves everything).

Searching the Entity database for "Los Angeles" returned three hits. Here is the first entry:

> Entity: LOS ANGELES DOCTORS HOSPITAL CORPORATION, General: OTHER BUSINESS, Specialty: HC CONGLOM – PARENT, Address: 2231 S WESTERN AVE, LOS ANGELES, CA 90018-0000, Excl. Type: 1128(a)(1)- PROGRAM-RELATED CONVICTION, Excl. Date: 06/14/2012

Searching the Individual database for "COHEN" returned 37 hits. The first one is:

> First Name: ABBOTT, Middle Name: B, Last Name: COHEN, DOB: 12/25/1968, General: PODIATRY PRACTICE, Specialty: PODIATRY, Address: 105 PRENTISS, ALPENA, MI 49707-0000, Excl. Type: 1128(a)(4)- FELONY CONTROLLED SUBSTANCE CONVICTION, Excl. Date: 08/19/2004

You can use this database to check out individuals and entities about whom you might have a concern. You also might be able to find information on lost or potential relatives. Try it with the surnames you are researching. Access it at https://oig.hhs.gov and select the "Exclusions" tab. The first option is its Online Searchable Database. It also contains a helpful FAQ.

Various federal and state entities maintain publicly accessible staff directories. For the U.S. Department of Health & Human Services go to http://directory.psc.gov/employee.htm. It provides the specific organization for which the person works, his/her job title, location, phone and email.

If interested in seeing if an organization has a publicly accessible directory, enter "Staff Directory - DHS CA" (citing the specific agency you want). In this case, you will find a staff directory for the California Department of Health Services. Try it with federal, states or local agencies. Be creative. If your search does not work, try alternative wording like "phone directory" or "employee directory."

The first several listed responses to such searches will often be commercial search facilities which themselves scour many publicly available databases for information on individuals…for a fee. They pay to be listed at the top. If you skip over them and look for URLs ending in "CA.GOV", "NY.GOV" or just "GOV" you have gotten beyond the commercial sites. If you are interested in California governmental sites, include "CA.GOV" in your Google search.

Of course, not all government databases are free. For example, I was searching for a nurse and knew that each state maintains a registry of licensed nurses. In another search, I was trying to find someone based on mortgage information. A friend has a professional practice that subscribes to various licensure and property databases. Accessing these databases quickly located the individuals.

The scope and availability of governmental databases are more than you might imagine. Happy hunting!

Go to Index

Practicing Safe Computing #Article #18 - Viruses, Worms, Trojan Horses, Spyware by Hal Bookbinder
Originally published in the April 2017 issue of *Venturing into our Past* (JGSCV)

Malware (**mal**icious soft**ware**) comes in diverse forms. “Viruses”, “worms”, “Trojan horses”, “spyware”, “adware”, “zombies”, “ransomware” and “scareware” are different forms of malware. Some of these refer to the way the malware transports itself to your computer and others to what it does once you are infected.

There are two ways of transporting malware to your computer. You unknowingly invite “viruses” onto your computer and share them with others while “worms” find you on their own. They can be equally disruptive, from being petty annoyances to being highly destructive. The designation “virus” or “worm” describes how they travel and not their function or destructiveness.

Viruses may arrive on emails you open or websites you visit. Typically, a further action results in their installation, like clicking on a button or link on the website or in the email. Sometimes, the mere fact of visiting a dangerous website or opening an infected email is sufficient. Worms are routinely on the lookout for new hosts and once they find them, transport themselves to the unlucky target.

The rest of the terminology refers to the actions taken by the malware. Trojan Horses appear to be something benign or desirable. However, when you run them, they are also installing viruses on your computer. You receive a birthday card that instructs to click on it for a tune and sure enough when you do so it plays “Happy Birthday”. At the same time, it is installing a virus.

Spyware is a form of virus or worm that captures information on your computer and sends it to an outside recipient. This might include copying and sending your address book, your financial or medical information or IDs and passwords you may have stored in your computer. Some spyware records your keystrokes as you type, emailing them to the recipient. Adware invokes popup advertisements. Visiting websites might trigger these popup ads. A timer may also trigger them. Generally, adware is more annoying than dangerous.

Zombies, once installed in your computer, make your computer a “slave” to an outside “master”. They periodically check the remote site for instructions and take action when instructed to do so. Zombies may turn your computer into a relay for spam, forwarding a downloaded email to your contact list (seemingly coming from you) or to a list provided by the master. Alternatively, zombies can attack specified websites, with thousands of zombie computers overwhelming the target with simultaneous traffic. Since zombies are continually checking with their masters for instructions, they can slow your computer.

Ransomware encrypts your data and instructs you to pay a fee to regain control. The more aggressive forms of ransomware will threaten to, and then proceed to, destroy your data. Scareware, as the name implies will use social engineering techniques to instill fear, generally to cause you to buy unneeded software or services. Sometime it will attempt to scare you into taking potentially disruptive actions or running dangerous software.

Go to Index

Practicing Safe Computing #19: “Malware protection” by Hal Bookbinder
Originally published in the May 2017 issue of *Venturing into our Past* (JGSCV)

The April Practicing Safe Computing article described the various types of malware and mentioned that the designation “worm” and “virus” relate to the way the malware arrives in your computer. Viruses come in emails, or reside in websites or files you might access. To avoid them, you could avoid dangerous websites, avoid opening strange emails, avoid clicking of buttons that trigger programs to run and avoid accessing files on USB drives. Of course, if you religiously followed these rules, you would accomplish little on your computer.

Worms require no action to find you to implant their malware on your computer. They are constantly scanning for devices to which they can connect and once they discover a potential host, transport themselves to that host. They could be resident in a website you open or come to you from another infected device. The Stuxnet worm crippled Iran’s nuclear reactors for more than a year. It is likely that an Iranian scientist placed an infected USB flash drive into his PC. Stuxnet infected the PC and used it as a launching pad to transport itself to the computers controlling the centrifuges concentrating uranium.

Each device on the Internet broadcasts its address and availability so that others may see it. The downside is that this exposes a computer to worms. To lessen the risk, install a firewall between your computer and the Internet. The firewall broadcasts its address and availability (or none at all) and shields the address of your computer. Worms cannot see your computer through the firewall unless you provide a pathway by connecting to an infected website or inserting an infected USB drive. Be sure to turn on the built-in firewall on your computer or wireless router.

In addition to firewalls and being careful as to websites, emails and USB drives, you must have current anti-virus software on your computer. If you are not certain whether your anti-virus protection is up to date and configured properly, go to the vendor’s website and check. They have utilities to verify whether your software is functioning properly. If unsure, choose the default configuration.

An article by Neil Rubenking in the March 3, 2017 issue of PC Magazine evaluated 46 utilities to protect your Windows PC from malware. It lists the following ten as the best antivirus protection programs of 2017: McAfee AntiVirus Plus, Webroot SecureAnywhere Antivirus, Bitdefencer Antivirus Plus 12017, Symantec Norton AntiVirus Basic, Kaspersky Anti-Virus (2017), Avast Pro Antivirus 2017, Emsisoft Anti-Malware 11.0, ESET NOD32 Antivirus 10, F-Secure Anti-Virus (2017) and Trend Micro Antivirus Security (2017).

The article contains a side-by-side comparison of functions and links to more in-depth reviews. Access it at: http://www.pcmag.com/article2/0,2817,2372364,00.asp. All these products function well. Pick one that you prefer and be sure to configure it to check all of the files, emails and websites you access. While most have higher “regular” prices, watch for sales and spend $20 to $40.

Go to Index

Practicing Safe Computing #20 – "Protection from WannaCry Ransomware" by Hal Bookbinder
Originally published in the June 2017 issue of *Venturing into our Past* (JGSCV)

The WannaCry ransomware has been all over the news as it has infected hundreds of thousands of computers worldwide, impacting major institutions as well as individuals. While all of the information below is available online, I have not found it written in nontechnical terms in a single place. Hope you find this helpful.

What is the issue?

- The WannaCry (or WannaCrypt) ransomware exploits a vulnerability in all versions of the Windows Operating System (OS).
- Microsoft issued the following to explain this exploit, http://tinyurl.com/me8rx8g.
- The above bulletin contains a link to Microsoft Security Bulletin MS17-010, which includes the security patch to fix this vulnerability.

Do I need to worry?

- If your computer is running a supported version of the Windows OS (7, 8.1 or 10) AND is set to automatically accept security patches from Microsoft, you should be protected.
- If you are running Windows 10, automatic updates are turned on and cannot be turned off by the home user, so you should be protected.
- If you are running a supported version but it is not set to automatically accept security patches, you are at risk.
- If you are running a non-supported version Windows OS (8.0, XP or earlier), you are at risk.

What if I do not know which version of Windows I am running?

- A quick facility to check what Windows OS you are running is http://tinyurl.com/zmk89k4 (this is not a Microsoft site). It will display your OS at the top of the page and give you instructions if you want more details.
- Alternatively, you can find instructions at http://tinyurl.com/hd645o6. Though not quite as convenient and only covering supported versions, this is a Microsoft site.
- What if I am running Windows 7 or 8.1 and do not know if automatic updating is turned on?
- For instructions, see the following Microsoft publication, http://tinyurl.com/z6t342p. Go down to the portion entitled "Turn on and use Automatic Updates".
- If you find that you do not have automatic updating turned on, you are strongly advised to turn it on.

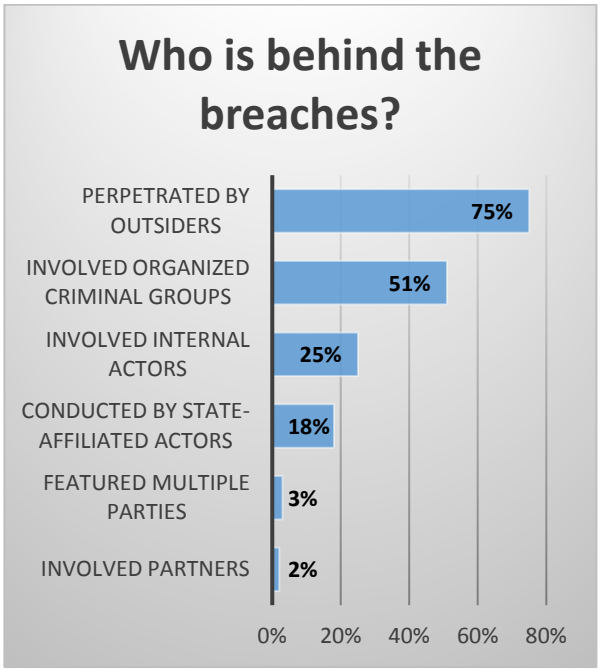
What do I do if I am at risk?

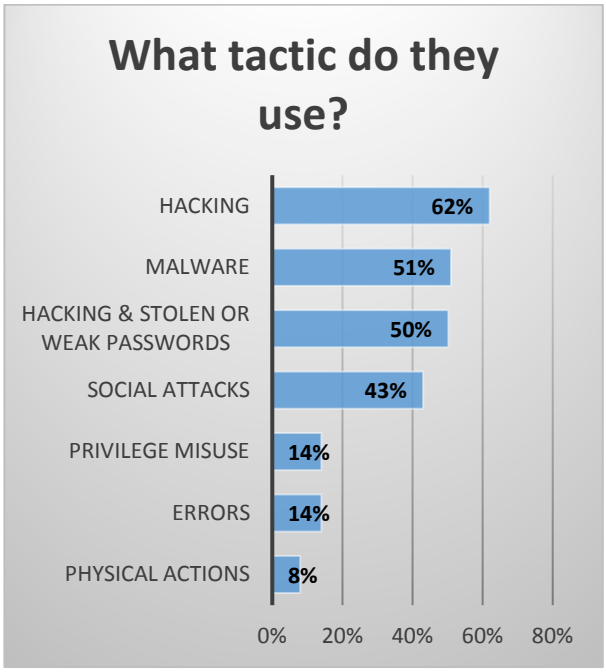
- The Microsoft bulletin cited in the first section, http://tinyurl.com/me8rx8g, contains links to download the MS17-010 patch
- In a highly unusual move, Microsoft has issued security patches for several unsupported Windows versions, including XP and 8.0, which are otherwise not supported with any fixes. Microsoft also offers a patch for Windows Server 2003. However, this is primarily a business installation and it is highly unlikely you have it on your home computer. Links to these downloads are at the bottom of the bulletin.
- If you are running an earlier version of Windows, no fix is available from Microsoft.
- If you are on an unsupported version of Windows, it is highly recommended that you upgrade.

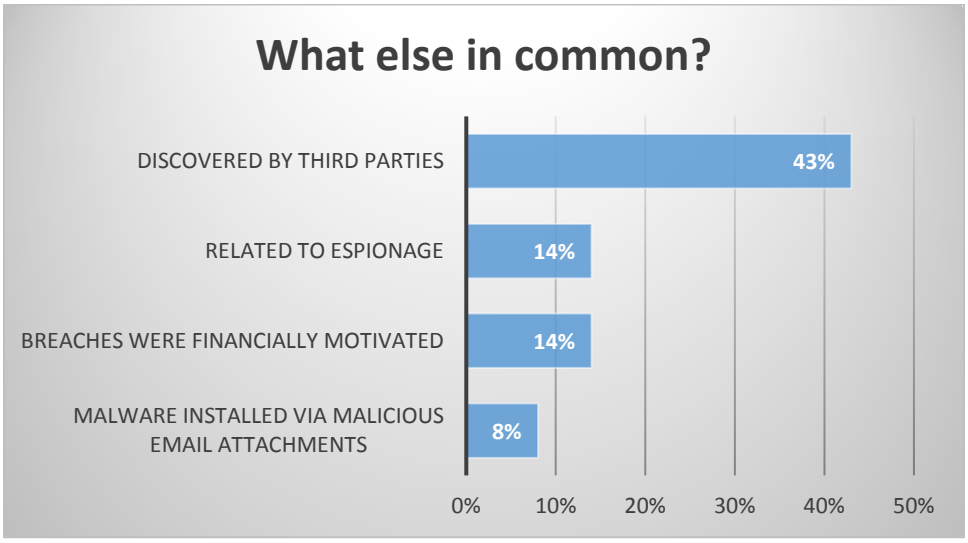
Go to Index

Practicing Safe Computing #21 – "Verizon 2017 Data Breach Report" by Hal Bookbinder
Originally published in the June 2017 issue of *Venturing into our Past* (JGSCV)

For the past 10 years, Verizon has issued an annual Data Breach Report. Here is a quick summary, with thanks to the University of California Information Security department. As the Verizon report is based on actual investigations, it is one of the best sources for data on what is happening.







So, most breaches are perpetrated by criminals outside the organization using a combination of hacking and malware and relying on poor password practices. Most were NOT financially motivated or related to espionage. So, this would imply that most were motivated simply by malicious intent, likely as a challenge. It is also interesting to note that 43% (2 in 5) were not discovered by the targeted organization but rather by outside parties. Bottom line, recognize that your data is at risk and so be careful what you share, practice good password management and keep your virus protection up to date. If interested in reviewing the entire report (which is 73 pages) please go to http://tinyurl.com/mzyk6vt.

Go to Index

Practicing Safe Computing #22 – "Modems and Routers" by Hal Bookbinder
Originally published in the July 2017 issue of *Venturing into our Past* (JGSCV)

A modem (**mod**ulate and **dem**odulate) is a device that accepts a series of analog signals (tones) and converts them into their digital equivalents (represented as 0's and 1's) and vice versa. Digital to analog is "modulation". Analog to digital is "demodulation". Your telephone typically sends and receives analog signals. Your computer recognizes 'digital' streams. The cable or telephone vendor provides you with a modem to interface between the communications line and your digital devices. It is the first device into which you would connect the cable coming into your home.

A router is a network device that takes a digital signal (after being converted by the modem), and intelligently distributes or suppresses it. It may connect directly to a desktop computer and broadcast via Wi-Fi for your wireless devices (laptops, smartphones, tablets etc.). Routers can have rules, including what signals to permit (for example you might bar adult content or specific websites), passwords (to restrict which devices can access it), encryption (to protect transmissions) and a built-in firewall (to protect your devices).

Most routers include built-in firewalls. This article provides easy instructions to check if yours does and, if so how to turn it on: http://tinyurl.com/mt6cfml. Check the user guide that came with your router or the vendor's web page for router-specific instructions.

Wireless routers are those that transmit digital data via Wi-Fi for use by your wireless devices. While not all routers provide wireless transmission, virtually all that are relevant to a home user do. Such routers offer one, two or even three "bands." Bands are the radio frequencies over which the router transmits Wi-Fi signals. If it only provides one band, it may be competing with other wireless devices (e.g. Bluetooth). Most offer two bands, 2.4 gigahertz (2.4 GHz) and 5 gigahertz (5 GHz). A few, offer three. Two is normally adequate. The router automatically switches as needed.

You generally do not need the fastest and most expensive routers since these likely far exceed the data rate from your Internet service provider (ISP). Older routers may be slow and use protocols that do not keep up with today's devices. A current or recent generation router providing 300 million bits per second (300 Mbps) is likely more than sufficient. Consider faster speeds if you are a "gamer", concurrently share several wireless devices, or stream videos.

Wireless routers will generally have one or more antennae. More antennae typically correlate to wider coverage. So, if you have a large area to cover, consider a router with several antenna. If you need to cover an especially large area or need Wi-Fi to go through certain types of walls and doors, you might need a separate range extender. Such a device amplifies the signal to reach additional areas.

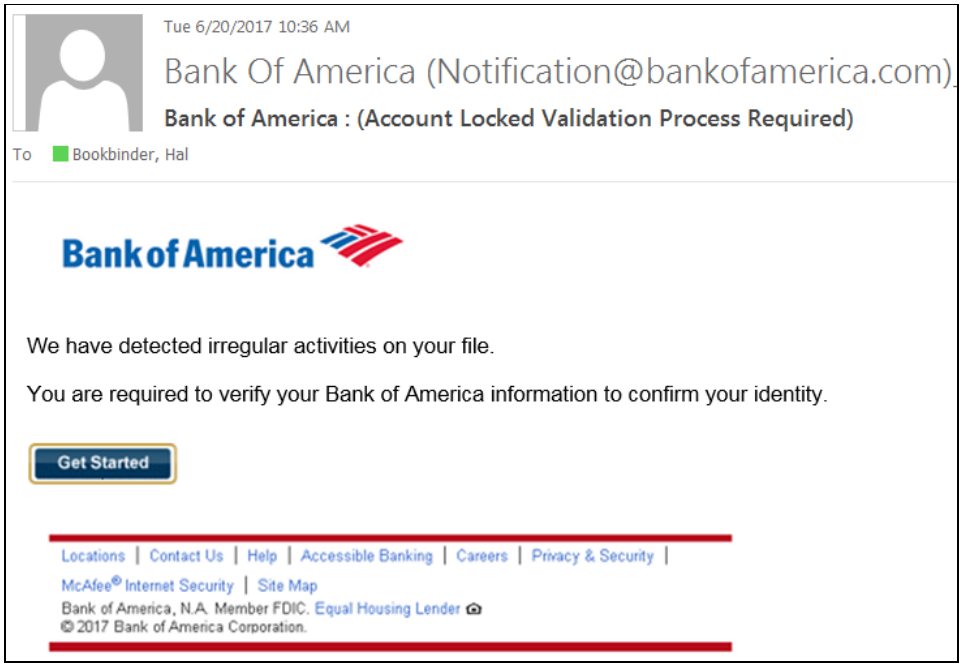
Routers will have one or more USB and Ethernet ports for directly attached devices. This can include a computer, shared storage and printers. If you are connecting a USB 3 capable device, be sure the router has available USB 3 ports. USB 3 devices connected to USB 2 ports will transfer data more slowly.

Review the features before you buy a router and check objective online articles. For comparisons of the best current-generation wireless routers see http://tinyurl.com/n63a3f3, http://tinyurl.com/hoon5qg, or http://tinyurl.com/8xjrafp.

Go to Index

Practicing Safe Computing #23 – Phishing email from your Bank by Hal Bookbinder
Originally published in the August 2017 issue of *Venturing into our Past* (JGSCV)

I recently received the email snapshotted below. Note that the sending email address looks legitimate and the Bank of America name and logo do as well. The "To" address is mine and there are no obvious spelling or grammatical errors. It tells me that my account has been locked which is certainly something I would want to fix quickly. Yet, this is a phishing email sent to obtain my personal information, including my Bank of America ID and Password. It is assuredly not from Bank of America.



Hovering my cursor over the Notification@bankofamerica.com address, the actual source address, "waqar.hussain@descon.com", displayed. Try hovering over the supposed bankofamerica.com link and you will see this. Further, this is likely not even the real address. It is certainly not from Bank of America! Be assured that, if I were to click on the "Get Started" button, I would be taken to a website that looked like a legitimate Bank of America login screen. I will be asked to log in with my ID and Password. However, I will not be identifying myself to Bank of America. Rather this will be sent to "Waqar Hussain" or whoever is actually behind this email. They could then use this to access and drain my account.

Your bank would never send you such an email. DO NOT click on the link. Not only will you be taken to unsafe pages that likely will appear legitimate, but just clicking on the link may result in malware being installed on your computer. If you feel that this warning might be legitimate, call or log in to the bank using your normal method of doing so. NEVER click on a link in such an email.

Most readers will say that they "would never be fooled" by such an email. This is likely true if they thought about it. However, we often go ahead and click on links before thinking them through. Each time we do so we open ourselves to risk. Undoubtedly, thousands or even hundreds of thousands received this email. Some actually have accounts at Bank of America, and some percentage of these will fall for it making it a profitable scam. Think before you click!

Go to Index

Practicing Safe Computing #24 – The Internet is forever by Hal Bookbinder
Originally published in the September 2017 issue of *Venturing into our Past* (JGSCV)

Some truisms to consider

1. "Don't email when angry"
2. "Anything you post may be viewed more widely than you intend"
3. "Deleted files may be recoverable" and
4. "The Internet is forever."

Be careful what you text, tweet, email, post to Facebook, place on a webpage or even save to your computer. Copies may exist on your computer, on servers, in email archives and of course, in the recipient's mailbox or message processor. Deleting or recalling an item does not remove copies and may not even remove the original.

When upset I often proceed to vent my anger in an email. I then set it aside and reread it the next day. 80% of the time I delete it. When I do decide to send it, I generally tone it down. Emails can often convey a harsher tone than intended. Once sent, it is too late to change one's mind.

Items erased from websites, and defunct websites, may not be gone forever. Check out the "Wayback Machine" at http://archive.org/web/web.php (if you forget the URL, just Google, "Wayback").. It periodically snapshots websites, preserving them forever. To date, it has saved over 300 billion web pages. For example, if you enter www.iajgs.org into the Wayback Machine search field you will find that it has snapshots of the website going back to 2000.

If you select 2001, a calendar will show that snapshots were taken on March 31st, April 3rd, July 20th and September 25th. If you click on the September 25th snapshot and select "Officers", you would see that Hal Bookbinder was president, Anne Feder Lee was vice president, Joel Spector was secretary and Michael Posnick was treasurer. The Wayback Machine began operation in 1996. It can be a great research tool. It can also preserve things that you wish would go away.

In the U.S. your employer has the right to monitor your use of company equipment, including your browsing, emails and instant messaging. Some believe that stricter privacy laws in Europe do not permit this. However, according to BBC News, The European Court of Human Rights ruled in January that a company had the right to check on a worker's activities and may read his Yahoo Messenger chats sent while he was at work. It did caution against unfettered snooping.

Even your own computer may contain files you "deleted" and your surfing history. When you delete a file, what you are actually doing is removing the index entry for the item and freeing up the space for reuse. Until overwritten, it continues to exist on your hard drive. Utilities can retrieve such files. Sophisticated utilities may even be able to recover overwritten files. Internet browsers generally preserve your surfing history unless you consciously turn this feature off. You might also consider turning on you browser's "private browsing" option to lessen the trail of crumbs you leave behind.

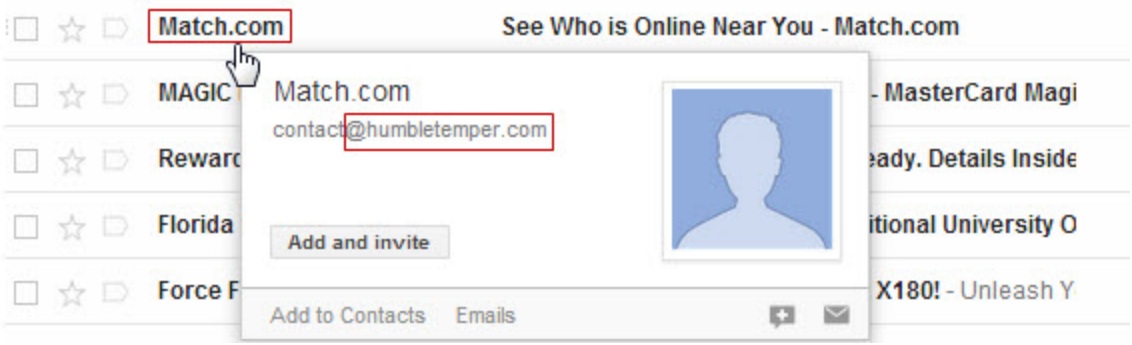
Be careful what you write, save, post, send and the sites you visit. You never know who may be watching – a family member, your company's security department, a co-worker, a friend, an enemy or even a potential boss.

Go to Index

Practicing Safe Computing #25 – Top 10 Tips for Detecting Phishing by Hal Bookbinder
Originally published in the October 2017 issue of *Venturing into our Past* (JGSCV)

Recently, UCLA Health IT Security released the following tips for staff to use to recognize when they are being phished (i.e. the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers). These are good tips for us all.

1. **Hover over the From**
   Probably the easiest way to identify if an email is legitimate or not, is to simply hover your mouse arrow over the name in the "From" column. By doing so, you will be able to tell if the email is from a recognizable domain that is linked to the actual sender name. For example, an email from Match.com should typically have the "From" domain of "match.com" (not "motch.com" or "humbletemper.com").



2. **Are the URLs legitimate?**
   Continuing on with the theme of hovering over certain parts of the email, another place to check would be any URLs the email is trying to get you to visit.

3. **Incorrect grammar/spelling**
   A common practice of many hackers is to use misspelled words on purpose. While it may seem that this would easily reveal an illegitimate email, it is actually a tactic used to find less savvy users. Spammers have learned that if they get a response from a poorly written email, they are on to an easy target and will focus their efforts to bring that user down.

4. **Plain text/Absence of logos**
   Most legitimate messages will be written with HTML and will be a mix of text and images. A poorly constructed phishing email may show an absence of images, including the lack of the company's logo. If the email is all plain text and looks different than what you're used to seeing from that sender, it is best to go with your gut feeling and ignore the message.

5. **Message body is an image**
   This is a common practice of many spammers. Make sure the email is a good mix of text and images. Also, there may be embedded links for you to hover over within the image for an extra step of precaution.

6. **IP Reputation**
   If you can easily identify the sending IP of that email, you can look up the IP's reputation through Return Path's Sender Score site. This tool will reveal a score (0-100) and will be able to

Go to Index

give you some insight into the sending IPs historical performance. The lower the score, the more likely the email is a phishing or spoofing attempt.

7. **Request for personal information**
   One tactic that is commonly used by hackers is to alert you that you must provide and/or update your personal information about an account (e.g., Social Security number, bank account details, account password). Phishers will use this tactic to drive urgency for someone to click on a malicious URL or download an attachment aiming to infect the user's computer or steal their information.

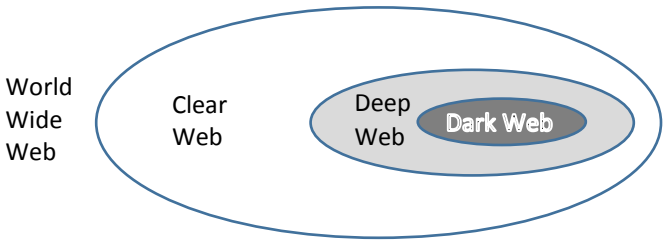
8. **Suspicious attachments**
   Is this new email in your inbox the first time your bank has sent you an attachment? The majority of financial institutions or retailers will not send out attachments via email, **DO NOT OPEN** attachments from senders or messages that seem suspicious. High risk attachments file types include: .exe, .scr, .zip, .com, .bat.

9. **Urgent/Too good to be true**
   If an email seems too good to be true, it most likely is. Be cautious with any message offering to place money into your bank account by simply "clicking here". Also, if the content places any kind of urgency as far as "you must click into your account now", it is most likely a scam and should be marked as "junk".

10. **Is my email address listed as the "From" address?**
    If you notice that your email address is being identified as the "From" address, this is a sign of a fake email message. Along those same lines, if the "To" field shows a large list of recipients, you should also be cautious. Legitimate emails will most likely be sent directly to you and you only. You may see "undisclosed recipients" and this is something to keep an eye on as well. It could be a valid send, but double check by using the other tips identified above.

Go to Index

Practicing Safe Computing #26 – What is the 'Dark Web'?
Originally published in the November 2017 issue of *Venturing into our Past* (JGSCV)



The Internet connects you to the World Wide Web (WWW). This comprises all of the sites on the Internet accessible through their Uniform Resource Locators (URLs). Search engines (like Google or Bing) index only a small portion of the WWW, likely less than 5%. The portion of the WWW visible to these search engines is called the "Clear Web" (or "Surface Web" or "Clear Net").

The 95% that is not indexed is referred to as the "Deep Web" (aka "Invisible Web" or "Hidden Web"). The Deep Web includes database, email and private messaging content. When you access your bank account, download a video on demand, search for your surname in Ancestry, or your town on JewishGen, you are accessing the Deep Web. While your bank's main website, a video sharing site, Ancestry.com and JewishGen.org are public forms and part of the Clear Web, digging into the data underneath takes you into the Deep Web.

The "Dark Web" is that portion of the Deep Web that requires special software to access. Traffic on the Dark Web is typically transmitted through numerous intermediary sites and encrypted multiple times, providing anonymity. This includes small friend-to-friend networks as well as large networks such as "Freenet", "I2P" and "Tor". The Tor Network is the most widely used Dark Web browser. Its URLs end with ".onion" (rather than ".com" or ".org"). Hence, it is sometimes referred to as "the Onion Domain".

It you are in Los Angeles and accessing a Dark Web site hosted in New York you might be routed through Belgium, Russia and Jamaica. New York sees the sending site as Jamaica and you see the send-to site as Belgium. These landing points, or nodes, are referred to as "botnets." They forward your traffic from one node to another, repeatedly encrypting it along the way. This frustrates discovery of who you are, what you are accessing and what you are communicating. A user of the Dark Net can take further steps to hide his/her browsing. While I cannot attest to its accuracy, you might check out https://darkwebnews.com/help-advice/access-dark-web/.

Significant legitimate traffic exists on the Dark Web, including discussion groups, in which peers simply wish to confidentially message, blog or share files. Another use is for "Bitcoin" exchanges and anonymous searching. However, due to its anonymous nature, it is also used for illegal trading, buying and sharing by extremists, drug dealers, hackers, pedophiles and terrorists.

We are all aware of the major hacks of personal data that have occurred in recent months, including the enormous one at Equifax. Some data from these hacks is certainly available for purchase on the Dark Web. To make it more difficult for criminals to gain access to your personal data, maintain strong passwords that you regularly change and instruct the credit bureaus to limit the use of your information. Carefully monitor your financial statements and take quick action when you notice something is amiss.

Go to Index

Practicing Safe Computing #27 - Take care when you use Google
Originally published in the December 2017 issue of *Venturing into our Past* (JGSCV)

We all use search engines like Google and Bing multiple times each day and generally trust that the algorithms they use are taking us to legitimate pages on the Web. We know that the first few links pay for this placement. So, we skip over these and go to the first or second link after the advertisements.

Some malware experts have devised ways to trick the search engines and get their own sites at or near the top. You click on the link and think you are on a legitimate site. After all, you searched for it and used a great tool like Google or Bing. The site then directs you to another and maybe another site. You are still not suspicious.

It now presents you with a button to download a Word document with the information you want. You have no reason to suspect anything and so click on the button. When you open the Word document, it asks you (usually in a banner at the top of the page) to “enable macros”. You have come this far and everything looks legitimate and so you do so.

Microsoft Word defaults to not allowing macros because they can be dangerous. A macro is an executable script that could do almost anything, including installing malware on your computer. You finish your reading and do not realize that you are now infected with software that may be recording and transmitting your keystrokes, displaying adware or deleting your files.

My purpose is not to make you paranoid about search engines. But, when you do search, look at the URL. Does it appear legitimate? If it redirects you several times, be suspicious, never providing personal information. Most importantly, think twice before downloading a file, and if you do and are asked to “enable macros’, run for the nearest exit. This is rarely a good sign.

A class of malware called “Zeus Panda” uses this clever way to cause you to let your guard down. It has been implanted into certain web pages which are designed to display near the top in a Google search. These pages appear completely legitimate, but are infected. You are then directed to a site that asks you to download a Microsoft Word document which contains macros.

Once you agree to “enable macros” they are active and you are at risk. These same Word documents are distributed as attachments to SPAM email. Most of us are rightfully wary of downloading files from SPAM email or agreeing to “enable macros”. However, the hackers know that by offering this after a search you initiate, you might let down your guard. Never agree to “enable macros” unless you are confident that the document is legitimate and permitting it to run scripts is safe.

Want to read more about Zeus Panda? Just Google it. (Yes, I see the irony. Do not abandon Google; just to be careful.)

Go to Index

Practicing Safe Computing #28 – Password Managers, Again
Originally published in the January 2018 issue of *Venturing into our Past* (JGSCV)

In October 2016 I wrote about Password managers, sharing my experience with a free tool, LastPass. I have been using it now for well over a year and remain quite satisfied with its features. It supports my access to over 100 sites with a variety of IDs and passwords. I commend it to you as a tool which can streamline your access to sites on the Internet while providing enhanced security.

Password managers store your login information. They then automatically log you in to the site once you bring up the login page. They often include other valuable security features, like recognizing new sites that you have logged into and offering to save the login information, filling in forms, synchronizing across your devices, generating impossible to remember complex passwords and permitting you to designate a person to obtain your access if you become incapacitated.

LastPass is intuitive, providing "cards" for each website you wish to access and displaying them in logical folders. You enter a description, ID and password into each card. I set up separate folders for email sites, financial sites, genealogy sites, shopping sites, social media sites, travel sites and work sites. I then open the appropriate folder and click on a card. LastPass takes me there and logs me in.

Typically, sites ask for an ID (or email) and a password. Sometimes, however, they ask for a third entry. A site I use asks for my last name, ID and password. LastPass permits you to add a third entry along with the two typical ones. So, you can script it to accommodate unique situations. LastPass resides in the Cloud. So, you can access it from any computer. For computers you typically use, you can link it into the browser (Internet Explorer, Chrome, Firefox, Safari) so that it is immediately available without first logging in. Do not do this if others share the computer as they will then have the ability to log in as you.

Some sites require you to click on a link to the login page and then to enter your information. Consider setting up the card with the login page rather than the initial page. LastPass also generates complex passwords on request which you can use to better secure your most critical sites. You can download it from http://www.lastpass.com.

For excellent comparisons of commercial Password Managers, see "The Best Password Managers of 2018" (https://www.pcmag.com/article2/0,2817,2407168,00.asp) and "The Best Free Password Managers of 2017" (https://www.pcmag.com/article2/0,2817,2475964,00.asp). PC Magazine rates two free Password Managers as "Editors' Choice", LastPass and LogMeOnce. Please do your own investigation to select the right tool for you.

A password manager is a convenient, secure way to maintain different passwords for the various sites that you visit. Of course you must create and remember a password for your password manager. Consider recording it in a secure location, like your safe deposit box - just in case.

Go to Index

Hal Bookbinder bio

Hal lived in the "Catskills" of New York State where his great-grandfather had settled in 1917. He experienced the heyday and decline of the "Borsht Belt" working as a waiter in the resorts. Hal earned his bachelor's degree from New York University majoring in Math and Physics, remaining at NYU to earn a master's degree in operations research.

He then spent four years on active duty with the U.S. Air Force, as a programmer for Space Division (now "Space Command") in the Cheyenne Mountain Complex in Colorado Springs. See the November 2016 issue of *Venturing into Our Past* for an article on Hal's experience there during the 1973 Yom Kippur War. While on active duty, he earned his second master's degree, in business, from the University of Northern Colorado. After active duty, Hal remained in the USAF Reserves, achieving the grade of major.

On leaving active duty, Hal settled in Los Angeles, first working as an IT professional for ARCO and then for UCLA where he is currently the Director of IT Strategic Finance for UCLA Health. He is also a part-time instructor for the University of Phoenix, teaching courses in business, information technology and mathematics. Additionally, Hal created and directs a transition to work training program for individuals in recovery at the Los Angeles Midnight Mission and at its associated Homelight Family Living center.

Hal continues to research eight family lines (Bookbinder, Barenberg, Horwitz/Milstein, Sacharow, Newmark, Yevelson, Biller, Schwartz), identifying 4,000 relatives in 28 U.S. states and 7 other countries. He has traced two of the lines to the late 18th century.

Hal has served as president of the JGSLA and of the IAJGS. He has been a member of the JewishGen Board of Governors and currently serves on the JewishGen Ukraine SIG Board where he is town leader for Dubno. He has co-chaired several IAJGS Conferences, first in 1990 and most recently in 2014. Hal received the IAJGS Lifetime Achievement Award in 2010.

Hal has spoken at most IAJGS conferences over the past 20 years as well as to societies around the U.S. His genealogical interests focus on geography and history. Hal's current presentations include:

- Jewish Fraternal Organizations of the early 20th Century
- Locating Lost Classmates (and Living Relatives)
- One Family's Holocaust Survival Stories
- Practicing Safe Computing
- Ships of Our Ancestors
- The Changing Borders of Eastern Europe
- The Rise and Fall of the Catskills
- U.S. Immigration and Naturalization
- Why did our Ancestors Leave a Nice Place like the Pale?

Hal, his wife, Marci, their four adult children and four grandchildren reside in the Los Angeles area.

You can reach him at hal.bookbinder@ucla.edu.

Go to Index