The PULP
Newsletter of the Hartford User Group Exchange

http://www.huge.org Volume 35 Issue -- 10

October 18th General Meeting:

Computer Security Month

Rev. Fleming Hall
2533 Main Street,
Glastonbury, CT

Q&A Session: 7 PM–7:15PM
Meeting starts at: 7:15PM

Member of apcug
An International Association of Technology & Computer User Groups

The **PULP** is published monthly by and for members of the Hartford User Group Exchange, Inc. (**HUGE**). **HUGE** is a nonprofit organization whose aim is to provide an exchange of information between users of personal computers. The **PULP** is not in any way affiliated with any computer manufacturer or software company.

MEETING LOCATIONS

Rev. Fleming Hall
2533 Main Street,
Glastonbury, CT

From The Editor

by Stuart Rabinowitz

Since October is National Cyber Security Awareness Month, that's the topic. We'll try to cover securing your router & computer, privacy (or lack thereof), encryption, and etc. November is party-time and open forum. December is for gift suggestions.

In the news: A researcher was able to spoof a USB Ethernet adapter, he could steal credentials from locked

Windows (98 se through 10 Enterprise) and Mac computers. He's working on a Linux version.

Cyber-reasoning platform Mayhem (from Carnegie Mellon University spin-out All Secure) won the $2 million first prize in a DARPA- sponsored Cyber Grand Challenge competition that pitted 6 entrants against each other in the classic hacking game Capture the Flag, never before played by programs running on supercomputers. It was entered in the DEF CON Capture the Flag competition for human teams and finished 15th (of 15).

Automatic braking system performance varies widely. In a real world test by AAA the systems were able to avoid a crash successfully 60% of the time. But they were able to reduce the energy of impact by 50%+.

Apple is surveying MacBook Pro customers about the headphone jack?

A researcher found that attackers could steal millions through online phone verification systems by tricking the systems to call premium-rate numbers.

Audis will be able to talk to traffic lights this year and drivers will be able to find out how long they have to wait for a signal to change

DOE scientists' discovery may boost solar cells' energy output by up to 40% The photovoltaic cells are easy to create -- and inexpensive

On Aug. 27, astronomers discovered a new asteroid, 2016 QA2, as it missed the Earth by less than a quarter of the distance to the Moon.

The long-standing tradition of getting cheaper ink by buying "off brand" cartridges just hit a snag for HP printer owners. A recent firmware update for bans third-party ink .

MIT researchers have discovered a method to triple wireless speeds.

New battery technology from SolidEnergy could double capacities for consumer electronics

Hackers can snoop and even type keystrokes from at least 8 wireless keyboard vendors

A U.S. court ruled that the FBI can hack into a computer without a warrant.

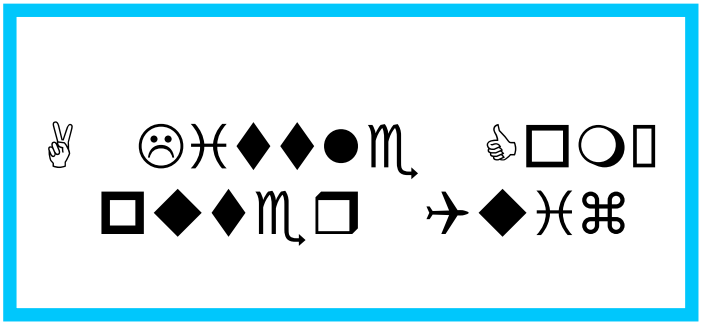
Send your comments to editor@huge.org

Until next month…Happy computing!!

Stuart Rabinowitz, Editor

Here is the appropriate copyright citation and a link to the full text. articles from "Tidbits"

http://creativecommons.org/licenses/by-nc-nd/3.0/



In honor of October being "National Computer Security Month" —

1 In what movie (circa 1983) did a teen hack into a government computer? And what was the name of that computer?

2 What type of computer did he use?

3 What was the password that allowed the security breach?

4 Yes computer hacking is a crime now, but when was the first computer crime legislation passed?

5 "Star Trek: The Wrath of Khan" also depicted computer hacking (into a starship computer). How many characters were in the password used to hack the computer? And what command was entered?

Sept. Quiz Answers

1 Once upon a time there were emoticons :), and now we have emoji's. Developed in the '90s there are now about 1800, but like all things there is a coordinating body. What organization sets the standards for emoji?

A The Unicode Consortium sets the basic B&W structure, designers for OS, websites, etc design their own graphic. There is no schedule for the release of new ones. You can see all of them at:

http://unicode.org/emoji/charts/full-emoji-list.html

2 Where does the word "emoji" come from?

A Japanese; e ≅ picture, mo ≅ writing, ji ≅ character

3 Making the news a lot recently is "ransomeware", but what was the first recorded instance of ransomeware?

A The "AIDS Trojan" released in 1989

4 Who coined the term "Net Neutrality"?

A Tim Wu, a law professor at Columbia

5 Google was started at Stanford, but where was Yahoo started?

A Trick question (sort of) it was also Stanford

Internet Security
By Dick Maybach, Member, Brookdale Computer Users' Group, NJ
February 2016 issue, BUG Bytes
www.bcug.com
n2nd (at) att.net

In my January 2016 article (available at http://www.bcug.com), I discussed Internet privacy, which in closely related to Internet security. Many of the topics fall into both categories and the choice of the article in which they appear was quite arbitrary.

A personal computer is secure until you connect it to the Internet, which is why the title of this article isn't "Computer Security;" however, without communications, a PC loses much of its value. Yours is almost certainly connected, but you can take steps that greatly reduce the risks. First recognize that the greater risk is not to your computer but to the personal information it holds. We'll consider two types of defense, preventing attacks and recovering from any that do occur.

The most important step you can take is to keep your operating system and your applications up to date. This can be automatic for your operating system, although I prefer to have the vendor tell me when updates are available and decide for myself whether to install them. You will probably have to check each application separately, but this is surely worth the trouble. While you're in a housecleaning mindset, remove all those applications you no longer use, as each one represents a potential vulnerability. Until you've completed this, updating your anti-virus software is wasted effort.

In particular, if you're still using Windows XP, disconnect that PC from the Internet now, and never reconnect it while XP is running. If you must check your e-mail or your bank balance, use a secure operating system, such as Tails, http://tails.boum.org/, on a live DVD or (better) on a memory stick. Tails, which I discussed last month for a slightly different use, includes a nice suite of applications, including an Internet browser, an e-mail client, an office suite, graphics designer software, media players, a screen reader for the visually impaired, and a password manager. While using Tails you can't run any XP software, but you can read and write files on your XP disk. Tails is Linux, but as the screen-shot below shows, its user interface is similar to XP's, and you should feel comfortable using it. (In the shot, Tails has opened an image on the Windows 7 disk of the netbook on which it's running.) Furthermore, since Tails resides on a live medium, you can safely use it from almost any PC, regardless of how insecure it might be. Tails is designed for high security, and it's worth considering for such tasks as Internet banking, even if your present operating system is up to date.

Once your software is updated, you should secure your Internet connection with an effective firewall, which monitors your communication stream and blocks malicious traffic. At the least, install a software firewall on your PC, which many anti-virus suites contain, but a hardware one is more effective. Most broadband modems that include routers also have firewalls, but often ISPs don't keep these updated, with the result that you may prefer to install an Ethernet router that contains a firewall with the latest firmware available from the vendor. Keeping your router and firewall software updated is as important as for your operating system and applications. If your router includes Wi-Fi, be sure you have enabled WPA encryption and changed both the Wi-Fi and the administrator passwords. Otherwise, passersby and your neighbors have free access to your computers and your Internet connection.

Next address the least secure component in your system, yourself. Establish a process to generate secure passwords and store them securely and use it everywhere, and never use the same password for different places. A good application for this is KeePassX, http://www.keepassx.org/, which both generates secure passwords and stores them in an encrypted file. You have no doubt heard that you should never use as a password anything that can be linked to you, such as you mother's maiden name, your college, or a pet's name. Yet your bank insists on recording your answers to "security questions" that have these very things as answers, so that they can be used in case you lose your password. If you follow this irresponsible advice, an intruder looking at your Facebook page can probably find the answers needed to compromise your account. The solution is to use secure "answers" to these silly questions. For example the name of your high school could be x9$Aw*_35{py. You'll of course have to store such obscure answers in your password program.

From my experience, most malware is installed on computers by users tricked by unscrupulous Internet sites. Be very careful when downloading software, as many sites include unwanted extras with the program you want. When making a search, I often find that the official source of an application is far down the list returned, and that the top choices often try to masquerade as the official source. Windows users have to be especially careful, both because Windows is vulnerable to malware and because being the most popular operating system makes it the most attractive target.

E-mail is another risk. The only safe way to deal with a message from someone you don't know is to delete it im-

mediately. Don't open any attachments and don't follow any links. This is good advice even if you think you know the sender, as e-mail addresses are easily forged. Unless you are expecting it, treat any e-mail with an attachment or a link as toxic. This is especially true of forwarded messages, since people in the habit of doing this seldom have the expertise to check them for hazards. Be especially careful of official looking e-mail claiming to be from your bank, the government, Microsoft, or similar entities and demanding immediate attention to avoid serious consequences. These folks seldom use e-mail to sound alarms. If you are concerned, contact them using the phone number or e-mail address you obtained directly from them, not the one in the e-mail.

A common risk is euphemistically known as "social engineering" or "phishing," but is just swindling using techniques that have been around for thousands of years. You can often recognize these because they are one of the following:

- an unexpected email with a link or an attachment,
- a request that you forward emails, attachments, or links to others,
- a promise too good to be true,
- an email that isn't addressed to you by name,
- a sender who isn't specified, isn't someone you know, or doesn't match the "from" address,
- one with spelling or grammar errors,
- one with a link that doesn't match where the email says the link will take you, or an attachment with an incorrect or suspicious filename or a suspicious file extension,
- one with a link or attachment to view an unexpected e-card or track an unknown package, or
- one that includes links to pictures or videos from people you don't know.

Other common techniques include e-mails or phone calls asking for sensitive information or asking that you perform some task, such as the following:

- a request for your name, account information, date of birth, Social Security number, address, and the like,
- a request that you click on a link or open a file to resolve a problem with your account or to repair a problem with your computer,
- a security alert in an email, pop-ups, or a Facebook notice warning that your computer is at risk of being infected, or
- someone (probably an acquaintance) in another country needing assistance
  accessing a large sum of money, or stuck without any money,
- an IRS agent claiming that you owe taxes and must pay immediately.

Anytime you are using the Internet, you should be as cautious as if you were on the street in a foreign country, because you are. It is easy to be lulled into a false sense of security because you are physically sitting in the familiarity of you own home.

You may be surprised that this far into the article, I haven't mentioned anti-virus programs. That's because prevention is far more effective than correction. Relying an anti-virus software as your only defense is like relying only on surgery and drugs to maintain your health; where a good diet, exercise, and sensible personal habits are more effective. However, as with your health, even with good preventive measures, your computer can be compromised, and a common cure for Windows malware is a good anti-virus program. Just keep in mind that these aren't cure-alls, because they can only detect, and often but not always remove, that malware they know about. They can't prevent problems resulting from unpatched software or careless users. The only sure cure is a good backup regimen, which will allow you to recover not only from malware infection, but also hardware and software failure, and user mistakes. There are many anti-malware programs from which to choose, ranging in cost from free upward, and an Internet search will show good reviews of these. Although they're not well rated, I use only the native Windows firewall and Microsoft Security Essentials. I feel that my preventive measures are effective, and I have frequent backups for recovery although I've seldom needed to resort to them. Although you should know that I usually do my Internet browsing from Linux, using Firefox with several protection add-ons enabled.

By making preparations and staying alert you can enjoy the Internet with minimal risk, and if you are attacked, you can recover with little or no loss.

Computer Attacks
By Dick Maybach, Member, Brookdale Computer Users' Group, NJ
June 2016 issue, BUG Bytes
www.bcug.com
n2nd (at) att.net

An important factor in defending your computer is to understand how it might be attacked. This topic fascinates many computer owners and has been the subject of many articles, books, advertisements, and discussions. One result of this is a jumble of terminology with words having meanings almost as slippery as the programs they are trying to describe. In this article I'll attempt to untie the terminology knot with brief definitions of the most common terms. You can learn (much) more with an Internet search for any of these terms, provided you read with skepticism. We'll start by using **attack** to describe any malicious act directed at a computer, the data it contains, or its user. We can classify attacks in three different ways:

(1) their **attack method** (how they access your PC, your data, or you),
(2) their **behavior** (how they get established and perhaps spread), and
(3) their **payload** (what they do).

To a great extent, these characteristics are independent, and we can look at each in turn. Much of the confusion about malware arises because authors don't make it clear whether what they are describing is an attack method, a behavior, or a payload.

First consider network attacks, which may not affect your computer at all. The first type, **network monitoring** is passive and is a digital version of a phone tap; everything you send and receive is recorded by a third party. This is easily done at a public hot spot, and requires only a laptop and widely-available software. It also can occur at ISPs and Internet relay points, either by the facility owner or by government agencies. A second type, the **man in the middle** attack, is active and is much more specific. Here, a computer is set up to mimic, for example, your Internet bank. If you can be fooled into logging into it, the attacker can capture your password and other account details before forwarding your traffic to the bank site you think you are using. This is more difficult to set up than simple network monitoring and is thus less common.

Let's now look at computer attack methods, which include

(1) physical access,
(2) social engineering,
(3) Trojan horses, and
(4) unethical suppliers.

Someone with **physical access** to your PC can install malicious hardware or software. Although this is sometimes called the **evil maid** attack (presumably because it's done by a hotel's housekeeping staff), it more commonly occurs when someone uses your PC with your permission and inadvertently infects it during, for example, a careless Internet browse. You now have a compromised PC for such tasks as your Internet banking. **Social engineering** or **phishing** occurs when someone tries to convince you to disclose sensitive data or perform some action that compromises your computer. You might receive a phone call or an e-mail message claiming to be from your credit card company requesting your account information, or one from tech support offering to remove a virus they somehow have detected remotely. Many attacks occur as **Trojan horses**, where malevolent software hides inside something that appears useful, interesting, or at least harmless. Examples include e-mail (often appearing to be from somebody you know) with an attachment that installs software, Web pages that run programs on your PC, and macros embedded in office files. Finally, there are **unethical suppliers** that include software you neither need nor want with their products. Although the most common culprits are Websites, it can take the form of **shovelware**, useless and sometimes intrusive programs installed on PCs, and malicious software on supposedly blank media.

Once **malware** (which malicious software is often called) infects your PC, it can behave in four different ways:

(1) reside there as a normal program file,
(2) attempt to hide by changing its form or the operating system configuration,
(3) spread through your computer by attaching a portion of itself to other files, or
(4) send copies of itself to other computers, usually via the Internet.

Type (2) programs are called **stealth software** or **rootkits**, type (3) programs are called **viruses**, and type (4) are called **worms**. An interesting form of virus resides in office document as a **macro**, for example written in Visual Basic and included in an MS Word or Excel file. These can migrate to your master template and infect every document you compose after that. When they first appeared around 2000 macro viruses were serious problems, but office suites now have effective safeguards against most; however, you may wish to check your preferences to be sure. (Although many people use the term virus for all malware, only 17 per cent of it really behaves this way and another eight per cent acts as worms.) Combinations are

also possible; for example, a virus can have stealth features. Since rootkits and viruses can affect system programs, their installation often, but not always, requires that the user grant them administrator privileges. A number of vendors offer applications to detect rootkits, but removing one sometimes requires erasing the computer's hard drive and reinstalling the operating system. Many people call type (1) programs Trojan horses, but I prefer to use that term for a malicious program's attack method rather than it's behavior after it becomes active.

Note that network attacks, social engineering, and macro viruses are operating-system agnostic. OS X and Linux users are just as vulnerable to them as are Windows users.

The object of most malware is to deliver a payload that is to perform some action to harm the computer owner or benefit the malware supplier. The payload is independent of the attack method and also of the malware's behavior. Examples are:

(1) ransomware,
(2) adware,
(3) spyware,
(4) key loggers,
(5) botnets, and
(6) hijackers.

Ransomware restricts your access to your PC and displays a message on how you can purchase instructions or software to remove the limitation. In some cases it encrypts files and demands the fee in return for the password to regain access to them. Sometimes there is just a threat, such as pay a fee within 10 days or your hard disk will be formatted. **Adware** continually displays advertising messages on your screen, although this can be legitimate (if annoying) when it's associated with trial software and seeks to sell you the paid version. **Spyware** transmits sensitive information, such as account information and passwords to an Internet location without your permission. Some people lump adware and spyware together and call both spyware, but I prefer to keep them separate, since spyware is more costly. A **key logger** records your keystrokes and forwards them to an Internet location with the intent of capturing log-in information; it can be implemented by either hardware or software. Malware can make your PC a component of a **botnet** (also called a zombie army), a computer network sometimes used to distribute spam or to attack other Internet sites by trying to overwhelm them. Other payloads, having a variety of names that often include the term **hijack**, change the configuration of your browser by changing your home page or your search engine or by adding menu bars.

By far the best time to defend your computer is in the attack phase, where healthy suspicion is your friend. Be careful reading e-mail, surfing the Internet, and using your laptop in public places. Note that some form of social engineering is a component of most attacks. After the attack, an anti-virus program may be able to recognize the malware's behavior and prevent it from delivering its payload. Here, you depend on the malware spreading relatively slowly, so that anti-virus vendors have had time to develop a defense before you encounter it, and fortunately this is most often the case. Once the payload has been delivered, the damage has been done, and you will have to stop using the computer until it can be cleaned, change your passwords, and work with your bank, credit card vendors, and others to repair the damage.

We usually think of malware defense only for PCs, but it also infects all computer-driven devices, such as smart phones and network routers. It's important that you include these in your safe computing plan.

Your ultimate defense against all malware is a backup made before your PC became infected. Wiping and restoring your hard disk will almost always restore your system, except in the rare cases where the malware resides in your PC's BIOS firmware, in which case you probably need expert help. Unfortunately, the Unified Extensible Firmware Interface (UEFI) adds a new vulnerability as it includes a writable boot partition on your hard disk. Since the code residing here executes before your operating system; any malware installed there becomes active before any anti-virus program. Re-installing the operating system will probably leave the infected partition unchanged. So far, this is only a theoretical threat. I mention it only to make the point that threats evolve continuously, which requires that you keep all your software, not just your anti-virus programs updated, and conscientiously practice an effective back up discipline.

To summarize, we can classify computer threats according to their attach method, their behavior, and their payload. Attack methods include physical access to a computer, social engineering, Trojan horse software, and unethical suppliers. Once established, malware can behave as normal software, a rootkit, a virus, a worm, or a combination of these. Typical payloads are ransomware, spyware, key-logger, botnet, and hijacking. Network attacks are special in that they occur outside your computer.

Ransomware - Protecting your ability to recover from an attack
By John Langill, Newsletter Editor, STPCC (Southern Tier Personal Computing Club) June 2016 issue, Rare Bits
http://www.pageorama.com/?p=stpcc1979jlangil1 (at) stny.rr.com

A recent posting to Yahoo.com reminded me that the key element to recovering from a ransomware attack is to have a reliable system image backup. Most computer users — you among them, I'm sure — are aware of this and have diligently performed regular backups. Some may have chosen to back up their systems to a Cloud-based service for which, if their backup files are sufficiently large, they pay a monthly fee based on the storage capacity required. Others have preferred to keep things "close to the vest" and store their backup files on a local external hard-drive (never, ever store backup files on an internal hard drive) for which one with a three-terabyte capacity, for example, presently costs about $100.

I fall into the latter group.

Cost aside, both methods provide protection but also have their own particular drawbacks that are too often overlooked. What will happen, for instance, if some enterprising ransomware purveyor one day successfully manages to hijack (encrypt) all the client files that have been stored with the cloud-based service. Not possible, such services say. Well, that may be but just how sure of that are you really — or are they, for that matter? And, as sure as God made little green apples, you can bet that there is at least one someone somewhere trying to do just that.

The uncertainty of cloud-based services is what led me to rely on a USB-connected external hard-drive for storing my backup files; and I have been doing so for years with a blissful — and perhaps a false — sense of confidence that they would be secure and uncorrupted should they be needed. Ok, so what's the drawback in this method? The fact is that a ransomware attack will — along with all files stored on the internal hard-drives — also hijack the backup files stored on an external hard-drive unless the drive is either powered off or physically disconnected from the computer at the time of the attack. Not a problem, said I — my USB 3.0 external hard-drive is equipped with an On-Off switch and I power it ON only for the time it takes to create a backup.

There's one other precaution I take and that's to set my cable modem to "Stand by" mode to disrupt Internet traffic during the time that a backup is created; thereby assuring that my system and external hard drives will not be vulnerable to attack while a backup is in progress.

Accordingly, I considered the risk of the backup files becoming corrupted was minimal.
And all was fine and dandy until I decided to swap a relatively low-capacity external hard-drive over to my laptop PC and to install two larger capacity USB 3.0 hard-drives on the desktop PC. The problem with doing this was that the newer drives did not have On-Off switches; and rummaging around behind my desktop PC (which, despite what it's called, is actually located under a desk) to connect and disconnect the USB cables from either the drives themselves or the PC was a real pain — it's a rats-nest back there, as many will probably know.

My solution: I purchased a powered 4-port USB 3.0 hub (under $20) specifically for use with the two newly installed external hard-drives. Now, all I have to do is connect/disconnect the one cable between the hub and the PC. Fortunately, a USB 3.0 port on the front of my PC that makes this convenient and easy. The only thing I need to be careful of is making sure that the external hard-drives have both completed their respective operations before disconnecting the hub from the PC which, by the way, also removes power to the drives (i.e., acts as a de-facto power On-Off switch).

Of course, if you use just one external hard-drive to store your backup files, and it has an accessible On-Off switch, you've no problem. Even if the drive doesn't have an ON-Off switch it's likely that restricting Internet access to it will be simply a matter of disconnecting the USB cable from the back of the device and that should not be much of a problem either.

Why do I have two external hard-drives? One is used to directly store backup files — which by the way, are always full system image backups — as they are created. The other serves to archive copies of previously created backups; that is, to back up my backups.

OK, so I'm paranoid when it comes to protecting my system image backups — it's not the worst of my faults. Admittedly, over the past 25 years or so, I can recall only once having to restore a system from a backup. I consider myself lucky on that score. But, with the chance of suffering a malicious attack rapidly increasing at the rate at which it is in today's world — and the risk will only get worse with time — I'd rather be overly cautious than suffer the consequences that could result from a lack of vigilance.

Back to Basics
Changing to another Email Service
By Jim Cerny, Chairman, Forums Committee, Sarasota Technology UG, Florida
June 2016 issue, Sarasota Technology Monitor
www.thestug.org
jimcerny123 (at) gmail.com

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

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

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

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

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

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

PULP Staff

Editor Stuart Rabinowitz

Distribution George Carbonell

Membership: Anyone may become a member. Dues are $12 per year and includes a one-year subscription to The Pulp. Meeting topics, times and places can be found on page 1 of this issue.

Officers & SIG Leaders

Leader:	George Carbonell	860 568–0492	george.carbonell@comcast.net
Secretary:	Stuart Rabinowitz		
Treasurer:	Charles Gagliardi	860 233 6054	epencil@aol.com
Director at Large:	Phil Manaker	860 659-4584	amanaker@earthlink.net
Director at Large:	Ted Bade	860 643-0430	tbade@cox.net
Director at Large:	Stuart Rabinowitz	860 633–9038	s.e.rabinowitz@att.net
Web Manager:	Bob Bonato		bob@bonatodesign.com
Membership:	Richard Sztaba		richer1@aol.com
Integrated SIG:	Stuart Rabinowitz		

		October	2016			
						1 1982 Lotus 1-2-3 announced
2	3 *Techies Day*	4	5	6	7	8
9	10 1st World Series radio broadcast	11	12	13	14 1957 British Computer Society founded	15
16 Ada Lovelace Day	17	18 General Meeting 7 PM	19	20	21	22
23 **Mole Day**	24	25	26	27	28	29 1956 IBM invents Disk Drive
30	31 Halloween					