September 2017 (Makeup Issue)

PATACS Posts

Newsletter of the Potomac Area Technology and Computer Society

Editorial Note

By Geof Goodrum

Co-Editor, Potomac Area Technology and Computer Society

First, my apologies to the PATACS membership about the delay in getting this September 2017 makeup issue out. As many of you know, I retired as newsletter editor (as of this issue) so I can hike the 2,189 mile Appalachian Trail in 2018 (my journal is at https://goo.gl/qDDXHf), and preparation of this newsletter was a victim of my shift in priorities.

Note that the meeting calendar and articles herein were current when submitted in 2017, but contents have been overcome by events. This is not the fault of the authors. I decided to provide the content as-is for retrospective context.

Also contributing to the delay in this issue, I decided to invest the time to recreate the newsletter template to be compatible with the word processors included in the free LibreOffice (https://www.libreoffice.org/) and OpenOffice (https://www.openoffice.org/) office suites. Prospective new editors familiar with word processors should find this template easier to use than a desktop publishing program. This template is also exportable to Microsoft Word format.

Please consider contributing to the PATACS Posts newsletter as an author or editor. The newsletter is one of the key benefits to our members, but requires your support. The articles are contributed by members of APCUG member groups, like you (email articles to editor@patacs.org). The editor's role involves selecting articles and pasting them into the newsletter template, which takes about six hours time per issue (more or less, depending upon how finicky you choose to be). If you are interested in helping as an editor, contact one of the Board members listed on the inside back cover. Thanks!

Musings of an Apple Tyro

By Lorrin R. Garson

Columnist, Potomac Area Technology and Computer Society

macOS High Sierra Coming

Sometime this fall, probably in October, Apple will make available the next version of its computer operation system, macOS High Sierra (version 10.13). The most important feature will be the new file system called APFS (**Ap**ple **F**ile **S**ystem). APFS replaces the HFS+ file system, which has been in use since 1998. The new file system is optimized for flash and solid state drive storage with a focus on encryption. APFS will be used for all of Apple's products (macOS, iOS, tvOS and watchOS). This new operating system does have some drawbacks. It can't be used with startup disks or Apple's Fusion Drives. APFS formatted drives won't be recognized by computers running OS X 10.11 Yosemite and earlier, which means files can't be transferred to such machines using APFS drives. It's conceivable that High Sierra will require a clean installation, but probably not. See http://apple.co/2ve9ZXe for more information. Also see http://bit.ly/2tm9NYJ and http://bit.ly/2uvI8o9.

Table of Contents

Editorial Note....1
Musings of an Apple Tyro....1
Rational Backup Strategy....4
What is PayPal and how does it work?....7
Customer Support by Erica....9
Back to the Basics: Easy Spreadsheets for Home Finances....11
QCS Meeting Review: Scams, Frauds, and Identity Theft....12

Because of this new file system, I suggest being more cautious than usual in installing High Sierra. Of course, make sure your Mac and its current operating system are compatible with High Sierra and you have a full, recent backup of your system… just in case. And, very important, be sure the programs and apps essential to you can function with High Sierra.

Hear Your Mac Speak

"Speech" is macOS's function to read aloud selected text. "Speech" works with Microsoft Word, Microsoft PowerPoint, Adobe Acrobat Reader DC[1] (for .pdf files), Apple Mail, Apple Calendar, Web browsers Google Chrome, Firefox and Safari, etc.

To setup/activate Speech, do the following:

System Preferences ➔ [Select] Accessibility ➔ [Select] Speech ➔ [Check box] "Speak selected text when the key is pressed"

The default "Key" to start "Speech" is Option+Esc, but that can be changed. You can select the "System Voice" between Alex, Fred, Samantha and Victoria. Alex is the default. Pressing the "Play" button provides a sample of the selected speech. You can also adjust the "Speaking Rate" by adjusting the slide bar. To use "Speech", Highlight the text for "Speech" to be read aloud then press Option+Esc. For more information see http://apple.co/2talgXR and http://bit.ly/2rDwQZe.

Is Your Mac Computer Overloaded?

If you suspect that your Mac is overloaded for some reason, i.e., running slow, there is a way to quantitatively ascertain if this is the case. Overloading can be caused by (a) over-burdening the CPU with processes, (b) running out of physical RAM memory so that a lot of swapping to and from disk storage occurs, (c) excessive writing to and reading from your hard disk, and other factors.

The procedure to determine overloading is as follows:

1. Go to the Utilities folder and double-click on "Terminal.app".
2. At the [Unix] prompt, key "uptime" [without quotes] then press Return and you will see something like: 13:10 up 3 days, 6:15, 2 users, load averages: 2.18 1.95 1.81
   a. 13:10—is the current time.
   b. up 3 days, 6:15—is the time since the computer was last booted-up (3 days, 6 hours and 15 minutes).
   c. 2 users—is the number of users[2].
   d. load averages 2.18 1.95 1.81—the system load averages after one minute (2.18), after five minutes (1.95) and after fifteen minutes (1.81), all of which requires further explanation (*vide infra*).

It is necessary to determine the number of logical CPU cores your processor has. The procedure is as follows.

1. Go to the Utilities folder and double-click on "Terminal.app", or if you already have Terminal running from the proceeding operation…
2. At the [Unix] prompt, *carefully* key sysctl hw.ncpu | awk '{print $2}'
3. The result will be a single number, the number of logical CPU cores, 8 in the case of my iMac, a 3.1 GHz Intel Core i7 processor[3].

1 Surprisingly, it does not work well with macOS's Preview. The function starts speaking from the beginning of the document and not with selected (highlighted) text.

2 This is a bit confusing. This is a case of a single user running two sessions (the normal logon session and the Terminal session), which results in 2 users being shown. In reality, there is only one user running two sessions.

3 A little more confusion. My Core i7 processor has only 4 cores but because of hyper-threading it has 8 logical CPU cores.

Now, what does all this mean? Dividing each of the three load averages by 8 gives:

1. 2.18÷8 = 0.273 (one minute)
2. 1.95÷8 = 0.244 (five minutes)
3. 1.81 ÷8 = 0.226 (fifteen minutes)

If any of these resulting numbers exceed a value of 1 (one), that is an indication of your computer being overloaded. Don't be too concerned if you get a number greater than one for the one minute value; it is the fifteen minute value that is the most indicative. This is a test that should be run at a time you think your computer is overloaded. Don't run the test if the computer has been sitting idle for several minutes.

All of this is not as complicated as it seems from the directions. Give it a try.

For more information, see http://bit.ly/2uySAdT.

Apple's WWDC 2017

Apple held its annual 2017 World Wide Developer's Conference on June 5-9 in San Jose, California. Last month I described the newly introduced Mac computers. See http://bit.ly/2tCsItE for details.

Password Managers

Much has been written and discussed about how to manage, or mismanage, passwords. Since passwords are the keys to your private information, serious thought should be given to managing them. If you organize your passwords using slips of paper or in an unencrypted Word file on your computer, you're going down a ski jump on one ski, blindfolded with your hands tied behind you—what could go wrong? Give serious thought to adopting a password manager and carefully evaluate the software of your choice. Verify that the product will work with the Web browsers you use. The products described in Table 1, except iCloud Keychain, work on PCs and Macs. Some have a one-time price others are subscription based. Some have a free application and most have a free trial period. Most of these systems also have applications for iOS and Android. No endorsements or recommendations are made or

Table 1: Password Managers

Product	Company	Reviews & Related Links	Comments
1Password	https://1password.com/	http://bit.ly/2q4smKv http://bit.ly/2r0K8mU	$4.99/month
Dashlane	https://www.dashlane.com	http://bit.ly/2r0VgAl http://bit.ly/2pTO34J	Free & $3.33/month. Doesn't support Microsoft Edge
iCloud Keychain	http://apple.co/2pTI5AL	http://bit.ly/2ucPJYC http://bit.ly/2rAgPE1	Free with the OS. Works only with Safari
KeePass	http://bit.ly/2rmspWZ	http://bit.ly/2r0FWUm http://bit.ly/2qFvIWj	Free. Also for Linux
Keeper	https://keepersecurity.com/	http://bit.ly/2qCgtPO http://bit.ly/2q4EPhi	$29.99 to $59.99/yr.
LastPass	https://www.lastpass.com	http://bit.ly/2tBz0Lt http://bit.ly/2t2UaEN	Free & $1.00/month
RoboForm	https://www.roboform.com	http://bit.ly/2rJU2G0 http://bit.ly/2t2oVJP	$19.95/yr.
True Key	https://www.truekey.com	http://bit.ly/2rJVEQc http://bit.ly/2tW2HWR	Free & $19.99/yr.

implied. Also see http://bit.ly/2rJEyC4 and http://bit.ly/2sJkfG7.

Rational Backup Strategy

By Dick Maybach

Member, Brookdale Computer Users' Group, NJ
January 2017 issue, BUG Bytes

www.bcug.com
n2nd (at) att.net

In developing a plan to defend against the loss of data and software from operator, hardware, and software failures and malicious acts, it's important to take a systematic approach rather than responding to the latest sensational article or alarming ad. Your first step should be to identify the threats. Otherwise, you could end up with a Maginot Line, an expensive defense against an attack that didn't occur and was ineffective against the one that did.

Common threats to PCs and the information they hold include the following:

- Operator errors are common. You mistakenly delete a file, a directory, or an entire partition. If this involves your software, it may disable the PC.
- Software sometimes contains coding errors that create problems, which if serious enough can crash the operating system. Simply repairing the resulting damage doesn't cure the root cause. However, often symptoms appear only under rare conditions, which means you can only repair the damage and hope these don't recur.
- Hardware malfunction often immediately disables the PC, and the solution is to repair the failure and then restore any damaged data. Some problems, such as intermittent RAM failure can be difficult to identify and may require a visit to the shop. Disk failure is common and this requires replacement of the disk and then restoration of the software and data it held.
- Malware is software that is designed to cause damage. Individual programs acquire colorful names, such as virus, ransomware, rootkit, and Trojan horse. Each newly discovered name results in a new commotion, but the remedy is the same for all – remove the malware and then repair the damage. A worry here is that the malware may reside for some time before damage appears, so that you back up the problem as well as your software and when you restore from a backup, you also restore the malware.
- PC loss can occur when traveling with a laptop or when one fails to the extent that repair isn't economically practical. You must replace not only the hardware, but any original equipment manufacturer (OEM) software that is licensed only for the lost machine. You can restore only your data from backup.
- Environmental catastrophe most commonly results from burglary, fire, storm, or flood. Here you lose not only the PC, but perhaps all the material associated with it, including documentation and backup media. At some level, perhaps nuclear holocaust or asteroid strike, you probably decide you don't care as the loss associated with your PC is trivial compared to other damage.

You will surely find that no single approach will protect against all of these, and you may decide to ignore some threats.

You have two software and data repair approaches: reinstall from the original sources or recover from a snapshot of your disk taken previously. Only the latter is possible with data; the receipts needed to recreate your 2012 tax return are long gone, as are the vacation photos on your camera's SD card. However, with software, you have choices:

- Use the original distribution media to create a fresh installation, configure it, and apply any updates for the OS and all the applications. This is tedious, but the result is a clean system, free of whatever problem (assuming it's not with your hardware) that corrupted your system. Most PCs are delivered with the operating system already on the disk and without its installation media; they have instructions on how to create a repair disk, although you may have to dig to find them. Most also have a recovery partition on the disk that you can use to recreate the initial configuration. In my experience, the hard disk is the PC component most likely to fail, which of course makes the recovery partition unavailable. The software supplied with a PC is almost certainly sold as OEM products, which means it is licensed only for that hardware, and it often includes a feature to prevent it from being used elsewhere. As a result, you need a separate set of recovery media for each PC, and you need to be able to identify to which hardware each set belongs.
- Recovering the software from a backup is far simpler, because it restores all the software in one step, which has already been configured and updated. However, if the failure was the result of a developing software problem, you also install its root cause. For this reason, many keep backups made at different times, hoping that if they go back far enough, they'll find a clean one. Of course, when you restore an old backup, you most likely also restore your old data, destroying any acquired since. Your recovery plan must include a remedy for this.

There are several choices of backup media:

- a backup directory on your system disk,
- a backup partition on your system disk,
- a separate internal backup hard disk,
- an external backup disk, and
- a cloud service.

Only hard disks and cloud services have the capacity to back up modern disks. Optical media capacities have not kept up with those of hard disks, and far too much of it has poor reliability. Cloud service adds security concerns, both because your data travels over the Internet and because you have entrusted it to an outside entity.

As with the backup medium, you have choices about what to back up. These include:

- a complete disk image,
- all the data files in the home directory, and
- only those data files in the home directory that have changed since the last backup.

Some strategies include backing those OS and application files that have changed, but this can be risky, as these often depend on each other. If you replace a file but not something with which it interacts, the result can be an inoperable system. With software, it's safer to replace everything.

Some backup program developers recommend that your PC have constant access to the backup medium. While this insures that all your data is backed up as soon as its created, it also insures that malware also always has access to the backup. This is a good scheme for protecting against operator error, but less so for protecting against malware and software errors. For the latter, you want your backup medium to be accessible for only very short periods of time. You may decide to use two methods, one

that backs up continually to protect against operator error, which are common, and a second that backs up only periodically to protect against such threats as malware.

Backup software is a poor area in which to experiment. Obtain it from well-known vendors with good reputations. Consider only products with favorable reviews from responsible experts. Microsoft includes a suite of recovery software with its operating systems, and you should have a good reason for using something different. I discussed their Windows 7 version of this in the February 2012 issue of BCUG Bytes and the Windows 10 version in the May 2016 issued, available at www.bcug.com.

After obtaining your choice, test it as best you are able. For a thorough test, you would have to erase your disk and restore a backup, but don't do this. Instead, make a copy of just one file or directory; then backup, delete, and restore it. Compare the original and restored versions. If the recovery software includes a bootable disk, test it on the PC where you will use it to be sure it does boot. This will probably require that you make some changes in your BIOS. Record these before you change them back, as frequently, the BIOS settings must be different for internal disks and external media. You may also wish to obtain and test a reliable repair utility disk. If you suspect a virus infection, you can boot with it and the virus won't be active. This will allow you to copy your data files to an external drive without its interference. I discussed some of these tools in articles in the April, June, July, and August 2012 issues of Bytes.

My strategy is that every week I have a scheduled backup of all the data files that have changed since the previous backup. This is to an internal hard drive, separate from my system and data drives. As a result, I limit my loss from most causes to the data I generate in one week. Once a month, or when I think of it, I back up to an external hard disk, all the data files that have changed since my last external backup. My operating system is Linux, and I have its installation USB memory stick. Almost all my applications are available from the distribution's repositories. As a result, it's convenient to restore all my software as a fresh install, and I do this every two years, even if I have no problems, just to clean out the accumulated cruft. Reviewing this plan against my list of threats, we see the following:

- An operator error can destroy at most a week's work.
- Similarly, most software errors and hardware failure can delete up to weeks of work. Although if one affects both the service and the on-line backup disk, I could lose up to a month's worth, but this is very rare.
- Malware could cost me up to a month, if it affects all the disks. But malware in Linux is uncommon and, so far, I have not had this problem.
- Although I do have a laptop, I transfer any data to my desktop as soon as I get home. As a result, losing it would lose only the data acquired on that trip.
- The weak point in my plan is environmental catastrophe, as all my PC gear resides in one room, and I could lose all of it in one incident. I could improve by adding a backup file server to our home network and locating it in the basement or better by storing a backup drive at a neighbor's or in my bank deposit box or using a cloud storage service.

You should make a similar assessment of your backup plan against your own list of threats to see if it needs adjustment.

Your recovery approach of course depends on what is damaged. Your data resides in what is often called the home directory, and this can be restored only from a data backup. However, Windows may store some of your data (such as Internet favorites and e-mail data) in the system area, and recovering them

requires a system restore. The operating system and applications reside in what's known as the system area. They can be recovered by restoring a system backup or by making a fresh install from the original distribution media.

If you use Microsoft's backup software, system backups are in the form of full disk images. If your system won't boot, it may be because the boot loader, or in new PCs the UEFI partition, has been damaged. These can be repaired in Windows system using the Windows recovery disk. See the MS Website for instructions. If the BIOS ROM is corrupted, a competent shop may be able to help, but you may have to return the machine to its manufacturer.

How you recover depends of course on how you backed up:

- The fastest is to restore from backup as the result will be software that is updated with the last version of your data. If this includes restoring the OS, you must be able to boot from live media, which means you have to properly set up your BIOS. Later PCs use UEFI, which adds complexity.
- If you decide to re-install the OS you can try to restore from the PC vendor's recovery partition, which places your computer to its state when you first purchased it. You will have to reinstall all your applications from their distribution disks and your data from a recent backup.
- If the recovery partition isn't available, you'll have to use the OS distribution disk if you purchased it separately or its recovery disks if the OS was installed by the PC vendor. (This of course assumes you created these.)
- As a last resort, if the former isn't possible or if you doubt your abilities you can take your PC back to the vendor who sold it to you or to an independent shop to have the OS re-installed. You then must restore any applications and your data yourself. It should be clear that record-keeping is a very important component of your plan. In particular, be sure to label your external backup media and any notes. You don't want to restore from the wrong computer.

Creating and following a good backup discipline require more than trivial knowledge, thought, and time. Many computer owners choose to take a "Do nothing and hope for the best" approach or they follow the advice in the latest article or ad they've read, and neither approach is sound. As a last resort, there are commercial firms that will attempt to recover data from damaged or corrupted storage media, but the results aren't certain and the costs are high (up to multiple thousands of dollars).

TechBoomers™

What is PayPal and how does it work?

https://techboomers.com/t/what-is-paypal

At Techboomers, one of the most common security questions that we get from our users is with respect to websites that require you to pay for something: "is it safe to put my credit card details into this website?" Often, the answer is "yes," but some people are still a little uncomfortable with entering their credit card details into every single website that requires payment, either for a subscription to a service or an item that they want to buy from someone. And with all of the horror stories about how permanent information on the Internet is, and how often others try to steal it (and sometimes succeed), we totally understand that.

That's where a website like PayPal.com is useful. Just enter a few of your personal and financial details into PayPal, and you can use it as a payment method on millions of websites across the Internet, including eBay.com and OverStock.com! And here's

the kicker: you don't have to reveal your credit card or bank account details to any of those websites. That's right; authorization of your PayPal account is all that you need to seal the deal!

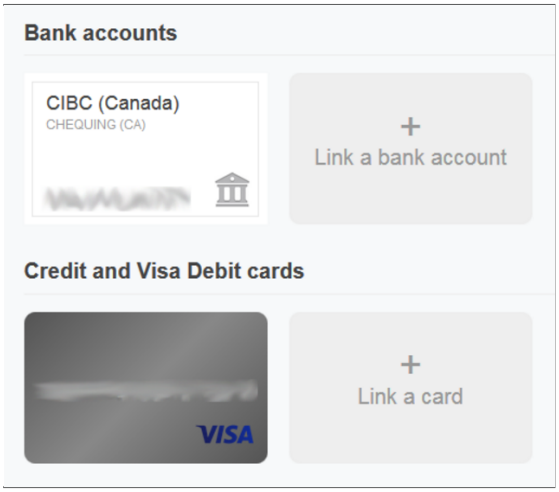
So what exactly is PayPal?

PayPal is a financial tool that lets you conduct transactions online without entering your financial details into every website you deal with. Link your credit card and/or bank account to PayPal, and then add to (or withdraw from) a secure money pool, shop at retailers who accept PayPal, or send money to other PayPal users.

How does PayPal work? 5 key ways to use PayPal

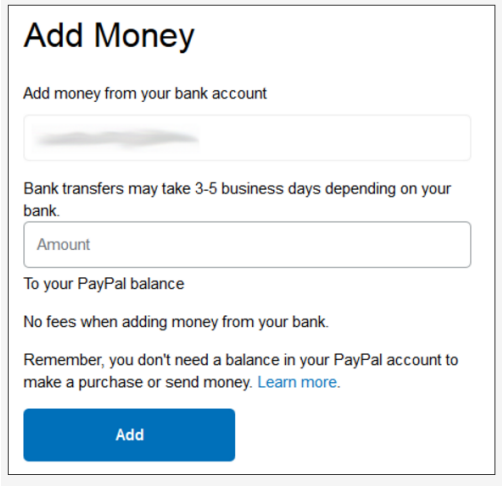
1. Pay from your credit card or bank account

When you sign up for PayPal, you can link your credit card account, your bank account, or both to your PayPal account. That way, when you pay for something using PayPal, you get to choose where the money comes from!



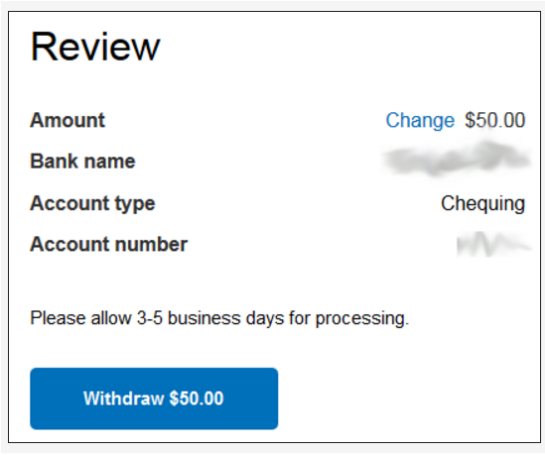
2. Create a secure pool of money

You can transfer money from your bank account to your PayPal account. That way, when you want to send money or pay for something with PayPal, you can just use the money in your PayPal account. You don't have to involve your credit card or bank account details at all in the transaction!



3. Draw money from your PayPal account when you need it

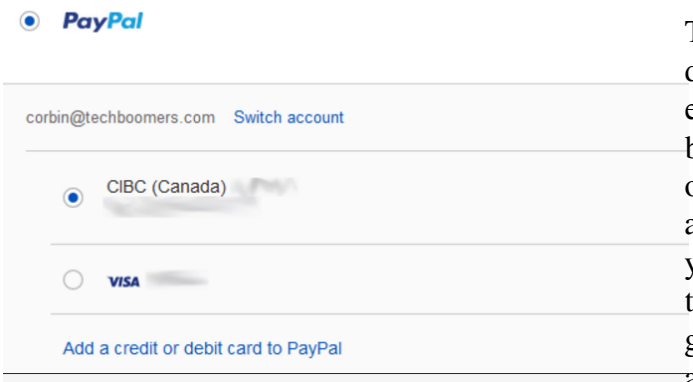
If you need to make a purchase that can't be completed with PayPal, don't sweat it! PayPal allows you to easily transfer money back into your bank account from your semi-anonymous pool on PayPal if liquid cash would be more useful to you in a certain situation.



4. Seamless online shopping through PayPal

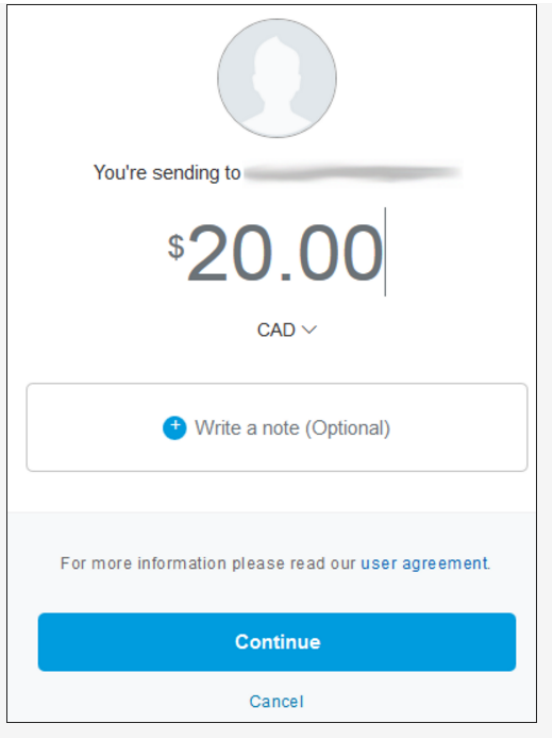
Millions of websites accept PayPal as payment, and shopping with PayPal is a snap on sites like eBay.com, OverStock.com, and HomeDepot.com! When you go to check out, simply select PayPal as your payment type, log into your PayPal account,

and select where you want the money to come from: your bank account, your credit card, or your balance on PayPal. No credit card details required!



5. Transfer money quickly and easily to other PayPal users

If your friends or family members use PayPal, too, then you can send them money when they need it with just a few quick clicks! Just type in their email address or phone number, choose how much money you want to give them (and in what currency), write them a note if you want, select where the money's going to come from – your credit card, your bank account, or your PayPal balance – and send your gift off!



That's an introduction to what PayPal is and what it does! Throughout our PayPal course, we'll teach you everything you need to know to make PayPal your best friend when it comes to transferring money online. We'll show you how to sign up for a PayPal account, transfer money to your PayPal account, use your PayPal account for online purchases, and do all this and more as safely as possible. Let us be your guide for using PayPal to move money online safely and quickly!

TechBoomers' PayPal course: https://techboomers.com/p/paypal

Customer Support by Erica

By Dan Douglas
President, Space Coast PC Users Group, FL
April 2017 issue, PC Journal
www.scpcug.org
ringram28 (at) cfl.rr.com

My daughter Erica was visiting this week and I told her that sometimes I get stumped on what to write for the journal each month. She came up with what I think was a great idea – what actually happens when you call a Customer Support line and how to make those calls more effective for you to get the help that you need. I spent most of my career working on software to log the critical parts of a customer call for service and she reviews and manages people who actually take those calls at an AT&T call center. Here's Erica's take on Customer Service and how to get better results!

You know that message when you call customer service that says the call "may be monitored or recorded for quality assurance"? My job is to listen to those calls and give feedback to customer service agents and their management about areas to improve and where they excel. So yes, someone really does listen!

Calling in to customer service or tech support is never how you want to spend your day, but there are a few things that you can do to help make sure the person you're talking to gives you the best service they can. So here are a few tips to make your next call go as smoothly as possible.

1. Don't skip the automated voice or you will need to be prepared to be transferred. No one likes to navigate all the options the automated system gives you, and the voice recognition can be frustrating, but giving it as much information as you can rather than just skipping it can make your call shorter and better. It will get you to a department you need, or where there is an account matching information you provide, and it will often (but not always) auto-load that information for the person who answers your call. If you do skip it, be patient with the person who answers and understand that they may have to transfer you – be clear about what department you need or what services you have, so as to waste as little time and save as much bother as possible.

2. Know your information, and give what is asked. You may want to go straight into telling your agent what the problem is, or vent about how long it has been happening, but there are a few things the agent must do before they can really help, the most important of which is to find your account. If the person is asking only for your name or security question, then they probably have your account loaded up thanks to you taking time with the Interactive Voice Recognition system (IVR) or the robot as we call it, but they need to confirm it's right before they can start making changes or troubleshooting. If they ask for your account number, let them know if you don't have it, and ask what other information they can use to find you. If you have phone or email services with the company you're calling, that's what they would normally use to contact you; that's probably the information they need.
3. Be patient and try not to ramble. You may hear long periods of silence, or the phrase "I am just running some tests" which is a favorite in the tech support calls. It can be hard to wait this out, if you are the customer, when you're mad that it's the 2nd time your Internet has gone out today. But this time is when your support agent is checking your account, letting their system check for damage in the area or other reported problems, and when they are figuring out what steps to do next. If silence goes on for longer than a minute, feel free to ask for an update, but if you are talking the entire time it will be harder for the agent to concentrate on their job.
4. Leave honest feedback, good or bad. You might be offered a supervisor or ask to speak to one, or you might get a survey email or text after your call. This data is crucial for the company to figure out if there are patterns of good or bad service, and figure out how to give you more of what you like. Ratings of your satisfaction with the result, the wait time, and the service are good points of reference for the company and service as a whole. If you have the option for a short-answer or a free response, that is the

best place to give your specific thoughts about the agent you worked with rather than the company as a whole, that section usually goes to the agent's supervisor and is a big part of how they are evaluated.

Back to the Basics: Easy Spreadsheets for Home Finances

by Jim Cerny
Forum Leader, Sarasota Technology User's Group, FL
May 2017 issue, Sarasota Monitor
www.thestug.org
jimcerny123 (at) gmail.com

Tax time has come and gone and this is always a good time to review your financial status. Over the years I have found that two easy spreadsheets have helped me a great deal in keeping track of my finances and I would like to share them with you. It is important that you know that it is NOT difficult to keep a spreadsheet, especially if you are only doing basic calculations. My first spreadsheet tracks all my expenses, month by month, and the other spreadsheet tracks my investments, also monthly. (See the two samples with this article – I am showing only three months instead of twelve, but you will get the idea).

By using these two spreadsheets I can easily see what bills I have paid (or not), the past amounts paid for each, and I can see those quarterly or annual payments as well. For my investments status, I can see the amount and percent gain/loss each month and the overall gain/loss for the year. Color shading of the rows of cells in each spreadsheet is very helpful, easy to do, and makes the data easy to view. All "formulas" that I use are only totals, differences from the previous month column, and percentages. Really easy stuff for a spreadsheet!

The only spreadsheet "skills" that you need to know for all of this are listed here, and you can find instructions by looking them up on Google:

1. Merge cells to create titles on your spreadsheet that span multiple columns. This makes the spreadsheet look nice.
2. Enter a number (dollar amount) in a cell.
3. Enter text into a cell.
4. Color a background to a cell, row, or column.
5. Enter a summation formula in the bottom cell to add all the cells in that column above. The formula: SUM(b2:b15) will add all the values in the cells in column B from B2 through B15. This formula should be entered in the last cell in the column which would be B16 in this example.
6. Just change the numbers to add the cells you want.
7. Add and/or delete a row or column of cells.

And that's about it. Of course, there is always more to learn if you want, but just these skills will work just fine for the basics.

Let's begin with my "Monthly Expenses" spreadsheet (Figure 1) and how you can modify it to suit your situation. I have each billing company or organization in the first column "a," followed by a column for each month across the sheet "b" through "m," twelve months. The last column on the right "n" is a total column.

F16

	A	B	C	D	E	F
1	My Monthly Expenses					
2	COMPANY	JAN	FEB	MAR	TOTAL	Average
3	Electric	68.22	75.93	63.86	208.01	69.34
4	Gas	34.25	39.76	37.72	111.73	37.24
5	Phone	48.32	48.32	48.32	144.96	48.32
6	Water & sewer	55.93	60.72	58.44	175.09	58.36
7	VISA bill	387.93	487.73	433.87	1309.53	436.51
8	Pest control			35.88	35.88	11.96
9	Dentist		478.5		478.5	159.50
10	Medications		35.86		35.86	11.95
11					0	0.00
12	TOTAL	594.65	1226.82	678.09	2499.56	833.19

Figure 1: Monthly Expenses

Basically, I have grouped my bills that come due each and every month at the top of the sheet, followed by those bills I consistently pay by credit card (a different color). These are then followed by those odd bills, the ones I pay quarterly or annually, and one-time bills such as for home improvements, etc. Don't forget to keep your medical bills clearly indicated in another color too. Usually it is a good idea to use your charge card for many bills because you can separate out the medical, food, and other charges as you need to for tax purposes. I usually do not track my cash payments out of my pocket (lunches, misc. expenses, etc.) but I DO track how much I take out from the bank in cash for those expenses. By looking across each row I can see how that bill went up or down and how much I have been using in gas or electric, etc. If my water bill jumps up, for example, maybe I have a leak or maybe I just filled up my pool too much. At the end of the year I can see how much I paid, total and monthly average, for all my expenses.

For my "Financial Status" or "Investments" spreadsheet (Figure 2) I do pretty much the same thing, one row across for each investment or account, and a column for each month. I enter the numbers into the spreadsheet based upon my monthly account statements. On my example, I have one row that is all negative as it is a loan or debt. The rows at the bottom contain the totals and the percent difference (up or down) from the previous month. Whenever you enter a new number in a cell, the totals, averages, and percentages are all automatically calculated for you. The column at the far right tells me the percentage gain/loss for the year so far for each investment.

D18

	A	B	C	D	E
1	MY ASSETS				
2	Investment	JAN	FEB	MAR	% + or -
3	Edward Jones	50,678	53,124	58,402	15.2%
4	Stock A	35,673	30,483	31,383	-12.0%
5	Stock B	15,478	17,123	18,058	16.7%
6	IRA	100,673	102,841	109,984	9.2%
7	House equity	50,738	50,738	50,738	0.0%
8	Checking acct	1,027	1,507	1,183	varies
9	Savings acct	20,675	19,839	20,108	-2.7%
10	Debt on loan	(4,893)	(4,772)	(4,633)	-5.3%
11	TOTAL	270,049	270,883	285,223	5.6%
12	% from prev month		0.3%	5.3%	

Figure 2: Investments

Remember you can just add more rows as you need. It fits nicely on my computer screen and, if I print it out in "landscape" mode, it looks great. Learning how to use the basics of a spreadsheet is a great way to find out if spreadsheets can help you in other areas as well. There is free spreadsheet software on Google Drive and OpenOffice, and free help on using them on Google and YouTube. Why not give it a try? – it's a lot easier than keeping written records by hand!

QCS Meeting Review: Scams, Frauds, and Identity Theft

Presented by Cpl. Hank Jacobsen, Davenport Police Department

Review by Joe Durham

Co-Editor, QBits, Quad-Cities Computer Society, IA
joseph85_us (at) yahoo.com

Cpl. Hank Jacobsen visited our club to share insight and advise from a policeman's perspective on the evolving scourge of the 21st Century: scams, fraud, and identity theft.

First, he described how these technological threats affect everyone when not prevented. Most victims realize something is not right and fall for the theft anyway. Young people don't realize that the theft of their Social Security Number will affect them in manifold ways in the future: car loans, credit applications, employment complications. Older citizens can lose money that they cannot afford to miss. He said that once your money has been lost it is very difficult to recover, it is usually lost for good.

So, it is incumbent upon everyone to learn about these current financial and personal threats.

What is the scope of the criminal's approach to technological crime? Hank observed that criminals do this work, because it is easy for them. They are fishing for that one victim out of thousands that will succumb to their wiles. They target places and people that have a great deal of money: individual, companies and banks. So, by following his simple, commonsense solutions you can protect yourself from this mayhem.

He stated that we often say to ourselves and others:

"Everything has been fine thus far, nothing has happened to me."

It only takes that one time and you will be sorry for it right then.

The thief is always seeking that one piece of information that they need to complete their work. Our names, addresses and phone numbers are usually public. These pieces are not what they need to advance their crime. They need your social security number to give that automatic access to your account, create new accounts and transfer funds to them.

Social Security Number

Hank stated that we should keep our Social Security Number private and protected. This means that we do not carry our Social Security card with us in our wallet or purse. Some members of the audience mentioned that their Medicare card has the SSN# on it. He said that, by next year, Medicare cards will not have that full information on it. In the interim, he suggested you make a photocopy of your Medicare card and use a permanent marker to black out all but the last four digits of your number.

To follow this trend of protecting your identity, he said you should remove or shred documents that have any personal information on it. Thieves will go through dumpsters looking for information like this. Shredding this information is best. It is always a good idea to keep a separate inventory of your wallet and your purse so you can figure out what may have been pilfered by a thief.

Personal Checks

Another financial vulnerability is checks. Whenever possible, don't use checks for payment when you are out and about. Checks provide thieves with just the information they need. And, if you do use a check, just take one with you not the whole checkbook and make a notation of its use when you get home.

If possible, mail your checks by taking them to the Post Office or a USPS mailbox yourself. There is a chance a thief will look in your personal mailbox and help themselves while it is sitting there waiting to be picked up by the letter carrier.

Hank noted that banks and financial institutions mail out statements with your information on it. HIs hope is that, in the future, they correct this oversight. For the near term, make a note of when your statements arrive in the mail each month, and notify the bank if they do not arrive on the usual date.

Credit Cards

Whenever possible, use credit cards for your daily transactions. And travel with no more than two credit cards in case your wallet or purse are pilfered or stolen. It is easy for you to then contact your provider and notify them it was stolen and you can obtain a new card.

Hank does not like Debit cards. These cards have access directly to your money. If these are compromised or stolen you will immediately surrender your funds. With credit cards, you have the opportunity to notify the credit card company and your liability is limited to $50.

Credit card skimmers are the latest financial threat to our money. Thieves will surreptitiously install a card reading device on an ATM machine or a gas pump. They will also install a small pinhole camera that is very hard to see with them; so that the skimmer will read your credit card strip information while the camera records the password you enter on the numeric keypad. Once that information is matched, the thief can do anything with it.

To protect yourself against this fraud, Hank suggested that you examine the credit card slot closely to see if it is physically secure. Often times you can physically pull out these skimmer devices. On gas pumps, some thieves have placed these skimmers inside the machine to avoid detection. He suggested that you examine the state seals on the pump to make sure that they are not broken or tampered with. If they are compromised notify the authorities immediately and do not use that pump.

Unfortunately, there are hand-held skimmers that are on the market. These devices will allow someone to get close to you and in a wireless fashion obtain the strip information from your card. You protect yourself form this approach by placing your cards in a metal case or placing them inside aluminum foil.

Hank said that there are occasions when large companies have had the security of their credit card databases broken. In this event, you request a new card immediately, and closely monitor your credit card statement for any irregularities and report them.

Phishing

This is an email with content that looks like an official company website that also, conveniently asks for your site password or personal information. He said never to do anything with these emails, put them in your spam folder or trash folder.

Emails

Hank described how we should handle emails in general. Do not open link attachments in your email even if they are from a known contact. When you open up these attachments, you have given permission for their malicious code to enter your computer. Make sure to contact your sender directly to confirm that they have just sent you this particular email and attachment before opening up an attachment from a friend.

Passwords

He noted that it is difficult to keep multiple passwords and remember them. This is always a continuing challenge for the average user. Create a couple of good long passwords, write them down and keep them in a safe place and use those.

Hank closed with 4 simple rules:

1. Do not answer the phone to anyone who is calling on behalf of an institution that you use. They will never start a request over the phone.
2. Don't answer the phone. Let people leave a message. If they really want to get in contact with you they will leave a message.
3. Do not make any hasty decisions or permit anyone to intimidate you into doing so. Take your time and check all areas of the request if it needs to be made.
4. You have the right to obtain a copy of your credit report once a year from the three top credit rating agencies and he recommended that you do so. One of the unfortunate drawbacks is that you have submit your SSN# to identify yourself when making the request.

 Monthly Circulation: 100

Posts is an official publication of the Potomac Area Technology and Computer Society (PATACS), a Virginia membership corporation (SCC ID: 02722890). PATACS is a tax exempt organization under section 501(c)(3) of the Internal Revenue Code. Contributions are gratefully received and tax deductible.

E-mail article submissions and reprint requests to editor(at)patacs.org

Membership Policy: PATACS membership dues are $30.00 (U.S. Funds) per year, with a $15 surcharge for international mail. PATACS membership includes a subscription to the Posts published twelve times per year and distributed by US Mail and PDF download. The membership application is available at any PATACS meeting, by downloading from http://www.patacs.org/membershippat.html, or by written request. A sample newsletter, membership application and related information may be obtained (for US addresses only) by mailing a check in the amount of $2.00 made payable to 'PATACS' with your request. Please do not send cash by mail. Payment and applications may be submitted at any meeting, or by mail to PATACS Membership, 4628 Valerie CT, Annandale VA 22003-3940.

Advertisement Policy: Ads are accepted from members for non-commercial purposes at no charge. Copy should be sent to the Editor in the same format as article submissions. Ads are accepted from commercial advertisers at the rate of $40 per full page, per appearance, with discounts for multiple insertions. Smaller ads are priced accordingly. Payment for ads must be made in advance of appearance. Advertisers must supply a permanent address and telephone number to the editor.

Reprint Policy: Permission to reprint articles from **PATACS Posts** is given to school, APCUG member, and non-profit organization publications, provided that: (a) PATACS Inc. receives a copy of the publication; (b) credit is given to **PATACS Posts** as the source; (c) the original author is given full credit; and (d) the article author has not expressly copyrighted the article. Recognition is one means of compensating our valued contributors.

PATACS, Inc.
201 S Kensington St
Arlington VA 22204-1141

TEMP-RETURN SERVICE REQUESTED

FIRST CLASS MAIL

AFFIX
FIRST
CLASS
POSTAGE

Arlington Carlin Hall Community Center 5711 4th St South 22204		**September 2017** **PATACS Event Calendar**			Fairfax Osher Lifelong Learning Institute 4210 Roberts Road 22032	
Sunday	**Monday**	**Tuesday**	**Wednesday**	**Thursday**	**Friday**	**Saturday**
27	28	29	30	31	1	2
3	4 Labor Day	5	6 Arlington Meeting, 7-9p	7	8	9
10	11 Remembrance Day	12	13 Online Meeting 7-9p	14	15	16 Fairfax Meeting 12:30-3:30p
17	18 Board Meeting 7-9p	19	20	21	22	23
24	25	26	27 Arlington Help Desk Meeting, 7-9p	28	29	30
1	2	3	4 Arlington Meeting, 7-9p	5	6	7