Bits of Bytes

Newsletter of the Pikes Peak Computer Application Society, Colorado Springs, CO

Volume XXXIV | November 2014 | Issue 11

The Prez Sez

by John Pearce, President, P*PCompAS

Watching the video of Bill Gates at the APCUG conference brought back lots of memories about how things were in the Windows 3.1 era. It occurred to me that lots of things have changed for the better but there is still much room for improvements.

As discussed briefly at our last meeting, a Waldo Canyon Fire Memorial dedication to honor former member Bill Everett and his wife Barbara will occur on Saturday, November 22nd. The memorial sculpture will be in Mountain Shadows Park. Bill and Barbara died on June 26, 2012, when the Waldo Canyon fire destroyed 347 homes and burned 18,000 acres. Eileen Gay, a Reno sculputural mosaic artist, was chosen to create the monument. We know Bill liked to hike and was a member of the Saturday Knights Hiking Club. It is only fitting that a hiking trail loop will go through a new plaza and be dedicated as the Everett Memorial Trail. Some more information is at http://gazette.com/waldo-canyon-fire-memorial-begins-to-take-shape-in-colorado-springs-park/article/1538318#BRq7e4RdfHpuJTbJ.99.

The November presentation is by Tim Hoffman of the Information Systems Security Association. His presentation is titled “Cyber Security” and includes topics like best home practices, incident response, home network management, and future risks and white-hat hacking among others. ☺

Next P*PCompAS meeting: Saturday, 1 November 2014

Tim Hoffman, VP of the Information Systems Security Association, will discuss cyber security topics.

Meeting Minutes

by Toni Logan, Secretary, P*PCompAS

The 4 October 2014 meeting was called to order by President John Pearce at 9 am. Due to a miscommunication, there are double goodies today. Also, thanks to Laura at Starbucks at Barnes & Noble for the coffee. The minutes of the last meeting were approved as published in the newsletter.

OFFICER REPORTS

Vice-President Bob Blackledge reported that we would see two videos today and he was working on next month’s program.

Treasurer Dennis Conroy reported that we have a total of $6742.27 in the bank. The only activity this month was a dividend received.

APCUG Representative Joe Nuvolini reported he had received notice of our dues renewal and that there will be a summit meeting in February of 2015. Joe also said the website was looking good.

OLD BUSINESS: None

NEW BUSINESS

John Everett e-mailed that a memorial for Bill and Barbara Everett would be dedicated on November 22. John will send an e-mail and link to an article about this memorial in the Gazette.

There was some discussion on the life of the bulb in our projector. It was decided that it may be a future expenditure. The next meeting is on Saturday, November 1, 2014.

PROGRAM

The members were treated to two videos. The first was a speech given by Bill Gates in 1998. The second was from Steve Gibson on Spinrite. Both were informative and interesting.

DRAWING

T-shirt—Dennis Conroy
Works9—Bob Blackledge
Router—Pete DeMario
iMovie Book—John Pearce
Excel book—Bill Gardner ☺

In This Issue

Officers

President: John Pearce
jlpnet@comcast.net

Vice President: Bob Blackledge
ms5mjkk49z@snkmail.com

Secretary: Toni Logan
bradtonilogan@gmail.com

Treasurer: Dennis Conroy
dennisconroy@comcast.net

Staff

APCUG Rep/Webmaster: Joe Nuvolini
Editor: Greg Lenihan
Librarian: Paul Major
Membership: Ann Titus

Committees

Hospitality: Pat Krieger
Programs: Bob Blackledge
Publicity: Bob Blackledge
Nominating: Vacant

Board of Directors

Vacant
Toni Logan
Norm Miller
Bob Blackledge
Warren Hill

Nybbles and Bits

by John Pearce, P*PCompAS

I have started loading the Windows 10 Technical Preview in a virtual machine on my Windows 7 machine. I am again using the free Oracle VirtualBox software, which is the same approach I used in running the preview release of Windows 8. One benefit to using a virtual environment is the ease of creating and deleting everything. One drawback is the resources the virtual environment requires to run.

There are two articles that provide step-by-step instructions for using VirtualBox as the virtual environment. The first is a Tech Republic article titled "Pro tip: How to install Windows 10 Technical Preview in VirtualBox." The second is in Windows Secrets Newsletter, Issue 453, 10-16-2014.

I had expected to be further along in the project and to have some first comments about Win 10. Unfortunately, I got sidetracked with other things to do. Check back next month for more on my experience with Windows 10. ☺

How to View PowerPoint Presentations without MS Office or Other Software

You can view PPT or PPTX presentations online with the use of a browser:

1. Open your preferred browser, either Chrome, Firefox, Opera, Safari, or IE.

2. Go to http://docspal.com/viewer.

3. From the home page, make sure you are on the View Files tab.

4. Upload the PowerPoint document to be viewed. You can upload the file, or enter a direct link (URL) to the file.

5. After uploading the file, click the View button, and then wait while the Web tool processes your document. ☺

Bob Blackledge and Joe Nuvolini setting up the computer and projector for our main video presentations at the October meeting.

Nuggets from Nuvo

*by Joe Nuvolini, P*PCompAS*

I just returned from my annual sojourn to Italia. I used to do an annual report on the state of Internet access. Well, this year it was great. Every place I stayed had Internet access, even the convent in Assisi and the little hilltop town of Civita di Bagnoregio. One did require you to pay for a certain block of time, but the others were all free. In most places, I was able to stream programs using Dish Network's dishanywhere.com. I used TeamViewer to keep my main desktop computer's e-mail up-to-date since the e-mail is deleted from the server only when it is received on my desktop unit. This also keeps me from having tons of e-mail to go through when I get home. Another thing I noticed was that most eating establishments had free Wi-Fi. Cyber rooms which were common in earlier years were few and far between. Florence used to have some very large cyber rooms for the many students and travelers there, but I saw only one I can remember in my wanderings.

I don't remember if I reported this before but I ran into a Skype problem. I had an early version of Skype on my desktop computer and it could not be uninstalled for some reason. Because of this I could not install a current version of the application. I decided to just use Skype on another computer. However after a period of time I had an idea which I had used to install the Thunderbird e-mail client on my netbook running Windows 7. As I may have reported earlier, I couldn't get my address book from Outlook Express on my XP computer to import properly into Thunderbird on the Windows 7 computer. What I did was to load the Thunderbird Portable Application on my XP computer, import the address book, then just copy the Thunderbird Portable Application folder onto my netbook and create a shortcut. Worked great and I had my full XP Outlook Express address book. Well, remembering this, I loaded the Skype portable application onto my desktop computer, and it works like a charm. A lot of software we use has a portable application version and runs independently. So if you run into a problem similar to mine, give it a shot.

Forget all I have written about Windows 9. Windows is bypassing version 9 and has announced Windows 10, which will be released sometime in 2016. I won't cover all the details here but Jack Dunning has done a very good story on Windows 10 in the October 10 issue of ComputorEdge Magazine. Go to **http://webserver.computoredge.com/online.mvc**, click Archive on the horizontal menu bar, and then select the 10/10/14 issue of Computor Edge to read Jack's article on Windows 10! ☺

You'll notice a very nice turnout of the digerati at the October breakfast. It was such a good time that we may not be invited back, but we'll have to wait and see about that.

With All of the Media Reports About Massive Data Breahes, What Can WE Do?

Published with permission from Ira Wilsker, Golden Triangle PC Club, columnist for The Examiner, Beaumont, TX

WEBSITES:
http://consumerist.com/2014/10/10/kmart-announces-credit-and-debit-card-breach-that-began-in-september/
http://consumerist.com/2014/10/10/do-you-ever-shop-anywhere-congratulations-your-data-will-be-hacked/
http://www.usatoday.com/story/tech/2014/10/02/home-depot-data-breach-credit-card-fast-food/16435337/
https://www.annualcreditreport.com
http://www.verizonenterprise.com/DBIR/2014/
http://www.verizonenterprise.com/DBIR/2014/reports/rp_Verizon-DBIR-2014_en_xg.pdf
http://www.bloomberg.com/news/2014-10-10/sears-s-kmart-says-hackers-stole-payment-card-data-in-attack.html
http://www.kmart.com/en_us/dap/statement1010140.html
http://consumerist.com/2014/10/02/chase-data-breach-hit-76m-households-7m-businesses-account-info-not-stolen/
https://www.creditkarma.com

Tonight (October 12) on the CBS news magazine "60 Minutes," the Director of the FBI, James B. Comey, discussed how the Internet is a very dangerous place. Director Comey explained that because of the massive data breaches, the billions of dollars that can be illicitly accrued by cyber crooks, and how it is often impossible to arrest and prosecute the villains because they are mostly in nations that will generally not cooperate with American law enforcement, that cybercrime on a massive scale is rampant. The most likely source of the malware that has wreaked such havoc on our retail and banking industry has been Russia, where stolen credit and debit card information is readily and openly bought and sold. While most of the high profile data breaches and outright financial crimes are perpetrated against big businesses, it is almost always we the consumers who are actually being victimized.

Just this weekend (October 10), K-Mart acknowledged that its payment system had been compromised (kmart.com/en_us/dap/statement1010140.html). In an official corporate press release, Alasdair James, President and Chief Member Officer of Kmart said, "I am reaching out to inform our loyal Kmart customers of a recent payment security incident. On Thursday, Oct. 9, 2014 our IT team detected that our Kmart store payment data system had been breached and immediately launched a full investigation working with a leading IT security firm. The security experts report that beginning in early September, the payment data systems at Kmart stores were purposely infected with a new form of malware (similar to a computer virus). This resulted in debit and credit card numbers being compromised." Later in the statement Mr. James stated, "There is also no evidence that kmart.com customers were impacted. ... I want our customers to be aware of the situation and I suggest that customers carefully review and monitor their credit and debit card account statements. If customers see any sign of suspicious activity, they should immediately contact their card issuer. More guidance is also available on our website, kmart.com and customers can contact our customer care center at 888-488-5978."

The advice presented by Mr. James that consumers need to carefully monitor credit and debit card statements for suspicious activities is sound, and is a repetition of the guidance previously offered by executives of other corporate victims of similar attacks.

According to an article published online at the "Consumerist" on October 10, the "top five" retailer credit and debit card thefts were the 2008 hack of Heartland Payment Systems where 130 million cards were compromised, followed by TJX Companies (2007, 94 million cards), Home Depot (2014, 56 million cards), Target (2013, 40 million cards and 110 million total records stolen), and CardSystems Solutions (2005, 40 million cards). While these data thefts from large retailers have garnered most of the publicity, again according to the Consumerist, there have also been millions of additional credit and debit cards compromised from smaller retail businesses, including recent breaches at Jimmy John's, Dairy Queen, P.F. Chang's, UPS, Albertsons, Jewel-Osco, ACME, Shaw's, Sally Beauty Supply, Goodwill, some Marriott hotels, Neiman Marcus, and Michael's craft stores. Most of the retailers that were recently compromised had their "POS" or "Point of Sale" systems compromised. Online financial services, as well as other companies with a strong online presence can also be compromised, such as the recent data breach at J.P. Morgan Chase in which personal and private data (but probably not credit and debit card information) from 76 million households and 7 million businesses was stolen, again probably by Russian hackers.

Continued on page 5

10 Tips for Online Shopping Safety

by Sandy Berger, CompuKISS, Sandy (at) compukiss.com, www.compukiss.com

Amazingly, in today's topsy-turvy world, because of vulnerabilities in the processing of credit and debit cards used at retail stores and the hackers who are focusing on those vulnerabilities, right now shopping online can actually be safer than swiping your card at a local store. For safety sake, however, there are a few online shopping rules that you should follow.

1. The first of these is to always have a good antivirus program installed on your computer and to update your antivirus program and other software like the operating system whenever an update is available. When in doubt, don't click on links. This is especially true of e-mail where phishing schemes are prevalent, but you should also be careful when you are surfing the Web or visiting social media websites.

2. Shop at trusted, established websites. Don't use any sites that you've never heard of. If you want to try a new website, check to see if any friends or acquaintances have used it successfully.

3. Pay only through secure sites. Typically the address in your browser will change from "http:" to "https:" during a secure connection.

4. Never e-mail your credit card number, social security number, or personal information to anyone. No reputable seller will request it by e-mail since e-mail is not secure.

5. Do your banking and shopping from home where you are on your own secure network. Wi-Fi hotspots at local coffee shops and other establishments usually do not offer enough protection unless the user takes some added precautions, which can be cumbersome for the average user.

6. Create strong passwords consisting of numbers, letters, and symbols. Do not use words or names. Make the password for each banking and shopping site unique. Keep your passwords private.

7. Credit cards are generally the safest option for shopping online. When using a credit card, you have limited liability and the ability to have the credit card company intervene if something goes awry. Debit cards can also be a good choice as long as you have investigated their liability limits, which may be higher than those of credit cards.

Continued on page 6

Data Breaches (Continued from page 4)

As we approach the peak shopping season of the year, many of us have some rational suspicions or fears about using our credit and debit cards at local and national businesses, as well as online. In the back of our minds may be the nagging doubt, "Will this card information be stolen?" In years past, there was a credible fear of a sales clerk or checker who might swipe our cards twice, once through the legitimate payment system, and then illicitly and immediately a second time through a simple device that reads and saves the magnetic stripe information. This allowed our information to be used by others for nefarious purposes. In last year's Target data theft, malware had been embedded into the payment system itself, such that even if we personally swiped our own cards at the checkout, with our cards never leaving our possession, our payment information was stolen at the instant that we swiped our own cards. International cyber crooks have found that it is much more efficient and profitable to steal credit and debit card information by the millions through compromised payment systems, rather than the small numbers of local thieves stealing our information for predominantly local criminal purposes.

These massive data breaches and hacks beg an answer to the rhetorical, "So what can we as individuals do about it?" According to the Consumerist, "Here's a cheerful thought: there is absolutely nothing that you can do about this situation. Individual consumers are pretty much powerless to prevent retail hacks." That does not mean that we as individuals are totally helpless, or that we must accept some degree of victimization. Certainly, there may be an increasing number of people who may prefer to pay with the traditional and anonymous cash, rather than digitally disclose private information, a sure way to prevent the information from that transaction from being used against us. Even though virtually all major credit and debit card companies offer a "no fraud guarantee" of some type, where the credit or debit card company will absorb any timely and properly reported unauthorized transactions, there is still a lot of aggravation and grief if the user is victimized, even if the losses will eventually be covered by the card issuer.

Continued on page 6

10 ShoppingTips (Cont. from page 5)

8. Keep a paper trail. Let's face it, none of us have perfect memories. Print and save records of your online transactions, including the name of the seller, product description, price, and date of purchase. Most reputable merchants allow you to print a receipt after the transaction is complete. You can use these printed receipts to compare to your bank and credit card statements.

9. Monitor your bank accounts and credit card purchases regularly. Report any discrepancies or unusual charges to your financial institution immediately.

10. Your social security number is the key to your identity. Be miserly about sharing it with anyone, especially online. No reputable merchant will ever ask for your social security number to make a purchase.

Credit card theft is pretty easy to get through. Usually you notify your financial institution and they issue you a new card. Identity theft is much more difficult to handle because a thief can open lines of credit in your name, buy a car, and obtain new credit cards. In order to steal your identity, the thieves needs personal information like social security number, address, phone number and financial information. So be careful when giving out any such information.

Many financial experts say that having your bills sent to you electronically and paying them electronically is safer than sending and receiving them by mail. They also recommend shredding paper documents with personal information. So whether you use a credit card at a physical store, you shop and pay bills online, or you pay bills by mail, the key word is "caution." Our mothers taught us to watch our wallets and keep the doors closed. Now we have a lot more convenience, and also a lot more to watch out for. ☺

Data Breaches (Cont. from page 5)

The Consumerist has several recommendations that we should all implement in order to minimize the threat, and to better recover if we are victimized by these cyber thieves. As has been mentioned many times previously in this column, for online purchases and financial transactions, use complex randomized passwords, which should be changed periodically (many say at least every six months or even more frequently), and never use the same password on multiple websites. Most financial websites offer and utilize a multi-factor authentication process, where in addition to a username and password, an additional security question must be answered, or a randomly selected term or number must be manually entered. When setting up these security questions, avoid using questions and answers that can be readily found on social networking websites (such as Facebook and Twitter), or other simple public information websites. Think about how many times you might have said something on a social network about your first car, favorite color, favorite flower, sibling's name, honeymoon location, favorite vacation spot, pet's name, and other information that could be readily used by others to complete your authentication sequence. Some of the more secure financial institutions actually select questions from old credit reports and other sources that unauthorized third parties will likely have easy access to, such as "what was your street address in the summer of 1983?"

While mostly localized, ATM and credit card skimmers are surprisingly common; these are devices placed by the thieves on the ATM or point of sale device, typically invisible to the casual user, that reads or skims a credit or debit card simultaneously as it is being scanned by the legitimate device. If using a PIN based card, such as a debit card, be sure to cover the keypad as you enter your PIN, preventing dishonest viewing by others, as tiny cameras are often placed with the illegal skimmer in order to read the PIN as the user enters it on the keypad.

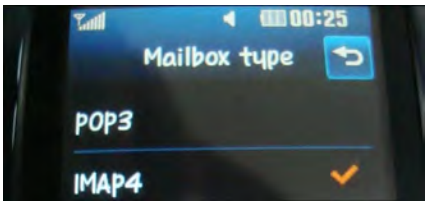
Obviously, be very careful in reviewing monthly credit card and banking statements for questionable transactions. Be cognizant that many fraudulent transactions are in small odd amounts, as they will be less likely to be noticed and questioned by the victim than large, round numbers. If anything questionable is found, contact the financial institution immediately.

It is not just credit and debit transactions that are being used to deprive us of our personal assets, but also other forms of credit and medical fraud. While there are commercials on TV touting a variety of credit reporting and credit score services, be aware that most of those, including some of those with the word "Free" prominently in their name, charge monthly or annual fees for the services that others may offer for free. The real source of free credit reports, as established by law, is Annual Credit Report dot Com (www.annualcreditreport.com), where each individual can get a legitimately free credit report from each of the three major credit

Continued on page 7

E-mail Basics: POP3 is Outdated; Please Switch to IMAP Today

By Chris Hoffman, reprinted with permission from HowToGeek.com
Original article at: http://www.howtogeek.com/197207/email-basics-pop3-is-outdated-please-switch-to-imap-today/



When it comes to accessing your email, POP3 vs. IMAP isn't just a matter of preference. POP3 is old, outdated, and not suitable for the modern world. IMAP is the one you should be using.

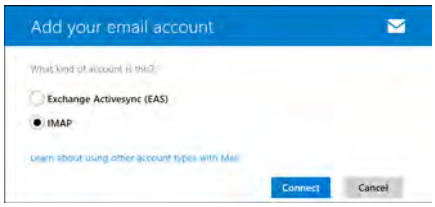
Exchange is also fine—if you have some sort of work e-mail account and it uses Exchange, you're good. Exchange works similarly to IMAP, but is a proprietary Microsoft protocol that isn't available everywhere.

When This Matters

POP3 vs. IMAP is a choice you make when you use an email client to access your mail. That e-mail client is often a desktop program on Windows, Mac, or Linux, but it can also be a smartphone or tablet app.

If you access your e-mail via a Web interface or an official mobile app — like accessing Gmail with the Gmail app on Android or iOS or accessing Microsoft's Outlook mail from outlook.com — you don't have to worry about this. It will just work.

Microsoft refused to support POP3 with Windows 8's included Mail app, requiring workarounds to access a POP3 e-mail account. While this was controversial, they're



at least pushing people in the right direction — away from POP3 and toward IMAP (or Exchange.)

Why POP3 is Bad

POP3 is just outdated. It comes from a time when everyone accessed their e-mail in a desktop e-mail program on a single computer. You probably had an e-mail address through your Internet service provider and they provided a tiny amount of e-mail storage on their server — perhaps 10MB or so. When you opened your e-mail program, it would download all the new e-mails from your e-mail provider and save them to your computer. It would then *delete* the e-mails from your online e-mail account. This was necessary at the time —

Continued on page 8

Data Breaches (Cont. from page 6)

reporting companies (Experian, TransUnion, Equifax), every 12 months. If any improper or unauthorized credit was extended, or erroneous data appears, instructions are provided in order to properly challenge questionable data. While not so much an indicator of fraud, many people like to monitor their credit scores, of which each of us have several different scores compiled for different purposes. Some credit card companies, such as Discover Card, now disclose credit scores directly on the monthly statement, as well as online, while an advertiser supported website, CreditKarma (creditkarma.com) offers free credit scores without ever asking for any form of payment.

Since the credit card companies are absorbing the massive losses from these frauds and scams, they are gradually implementing enhanced physical security directly on the credit and debit cards, such as embedded microprocessors, dual factor authentication, variable account numbers, and other technology that would otherwise make stolen credit and debit card data worthless.

Since many of us will be doing a lot of our holiday shopping online, there is one tactic that may provide substantial protection form online credit card fraud. Most of the credit card companies offer a free service where the user can create some form of virtual wallet, where a unique, one time use credit card number is created for each transaction, and the user can often pre-determine a limit on each of these virtual accounts. Since the account numbers cannot be reused, they would be worthless to data thieves. Some of the new virtual wallets, such as those offered by Google and Apple, may allow us to utilize our mobile devices to make secure financial transactions, rather than by using a plastic card. Some online payment services are offering a USB dongle that creates a new unique account number every few seconds, making previous account numbers obsolete as the new numbers are created.

Inevitably, this will be a classical "cat-and-mouse" game; as new security devices and methods are created, the cyber crooks will find a way or method to defeat them. This is a war that we must win. Our financial health is at stake. ☺

E-mail Basics (Cont. from page 7)

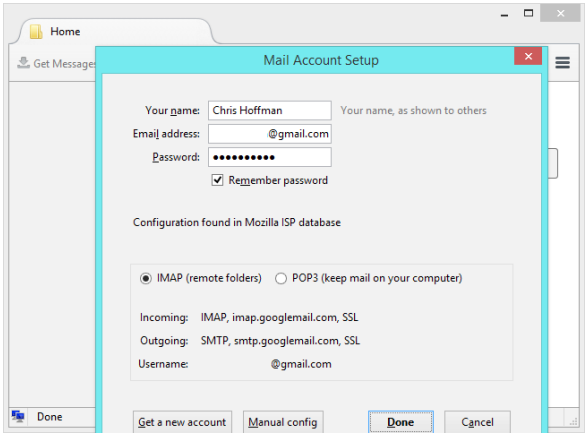
you only had a few megabytes for e-mail storage on the server, and you needed to keep it empty or e-mails directed to your address would start "bouncing" back to the sender.

This made sense in the 90s — given the limitations of the technology — but it's a big problem today. Here's why:

- You can only access your e-mail on one device. After you download the e-mail to that device, you can't access it on other devices. In an age where you probably have at least a smartphone as well as a computer, this is bad.
- POP3 relies on downloading all your e-mails. So, if you have new e-mails with large attachments, you have to sit there and wait while your program downloads all your e-mails to your computer.
- Your e-mails are stored on your computer, not the web server. This means that you have to worry about manually backing up your e-mail program's archive. If your hard drive dies, you'll lose those e-mails!

Some services try to bypass this limitation by not actually deleting e-mails when you access them from POP3. Instead, these services just mark them as read so they won't be downloaded again. This is a dirty hack and it has a big problem, too:

- Your e-mail actions won't synchronize between your devices. For example, if your e-mail client downloads an e-mail and you haven't read it yet, it may just be marked as read on the server. Or, it may never be marked as read on the server, even after you read it. When you change an e-mail's read status, star it, delete it, or organize it into folders, these actions will only be saved in the email program on your computer. They won't be synchronized online to all your other devices.

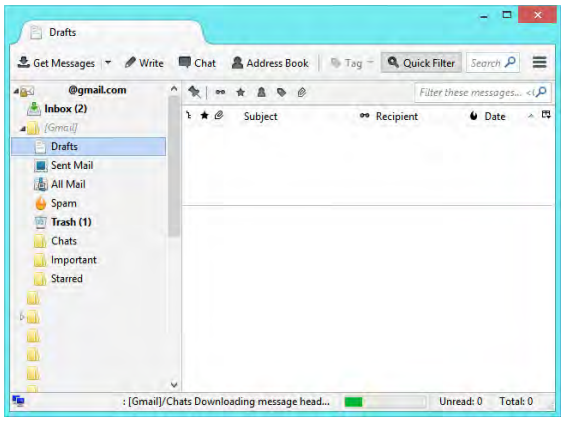


Why IMAP is Better

IMAP is a more modern protocol. Where POP3 just downloads everything to your device and manages it locally, IMAP is more of a syncing protocol. IMAP synchronizes all changes to the server and treats your e-mail server — not your local computer — as the primary place your e-mail is stored.

For example, if you access an e-mail account with 1000 unread e-mails with IMAP, you can access them instantly. They don't actually download until you open them — of course, you can configure your IMAP client to automatically download a certain number of e-mails. E-mail attachments don't download until you view them, unless you configure your e-mail account otherwise. When you open an e-mail, it's instantly marked as read on your device, the IMAP server (for example, in the Gmail or Outlook.com web interface), and every other IMAP client you use. If you organize your e-mails into folders, your organization will be synced online. If you delete an e-mail, it will be deleted everywhere — not just on your local device.

While POP3 downloads all your e-mails and leaves you to manage them on your local device, IMAP just provides a "window" to your e-mail account. In a world where you have more than one device — or just want to leave your e-mail online so you don't have to worry about backing up and importing desktop e-mail archives — IMAP is the best solution.



How to Use IMAP

IMAP is just an option you choose when you set up your e-mail account in a desktop, smartphone, or tablet e-mail program. Older desktop e-mail programs may be configured to use POP3 by default, but even the Mail app on iOS and the E-mail app on Android support POP3 e-mail accounts.

Continued on page 9

Merging Photos

By Larry Piper, President, Midland Compouter Club, MI, mcc.apcug.org, webbyte (at) yahoo.com

Ever see a row of photos at the top of a Facebook or website page? I'll bet it crossed your mind that this would be a good idea for one of your own projects.

I'll bet your next thought was that it would take a powerful photo editing tool, most likely Photoshop, to accomplish this horizontal photo montage. Sure enough, when you did some cursory checking, words like 'layers' and 'flattening' began to appear. Or maybe you found how-to ideas for creating a photo collage, which is NOT what you had in mind.

I too went down this same road. I also discovered that the most recommended solution is to use Paint, a free program that comes with Windows. I found the Paint solution not very intuitive and a little time consuming to use. Then I discovered another solution that had been right in front of me for a number of years. It is also a free program, IrfanView. This little utility has been around since the days of Windows 95. It will open virtually every graphic file type—as well as most sound and video file types. I use it as a fast image resizer. But right there in the opening screen under the Image drop-down menu is the choice Create Panoramic Image. Perfect!

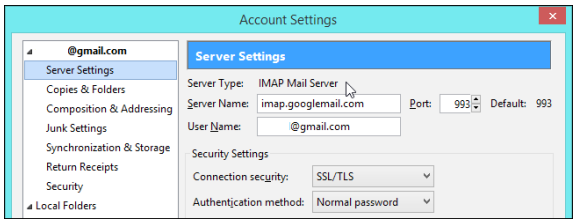
IrfanView gives you the choice of horizontal or vertical merging of photos. You add the photos you want, rearrange their order and then hit the Create key. Save the resulting photo-merge, give it a name and you are good to go. You could even resize the final image if it is too big or too small for your application.

So what about merging photos of different pixel size or resolution. No problem. I ran a few tests where the height dimensions were five times different. IrfanView makes the horizontal photo montage a constant height. The same thing occurred when merging photos of very different resolution. Again, the merged photos were a nearly constant total pixel size. The overall picture quality has been reduced substantially, but who cares when it is being viewed over the Internet.

IrfanView is the product of Irfan Skiljan, who lists himself as graduate of Vienna University. Be sure to get the latest version which is 4.37 as of this writing. ☺

E-mail Basics (Cont. from page 8)

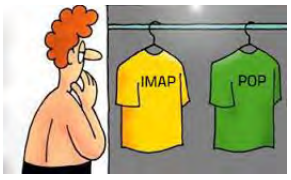
Modern e-mail programs should automatically default to using IMAP instead of POP3. Go into your e-mail app and check to make sure it's using IMAP and not POP3 for your e-mail account!



But My E-mail Program or Service Doesn't Support IMAP!

If you're using an e-mail client that doesn't support IMAP, it's long past time to upgrade. Get a more modern e-mail client today — on the desktop, Mozilla Thunderbird is a solid e-mail client by the makers of Firefox, and Microsoft Outlook is very powerful option if you're already paying for Microsoft Office.

If your e-mail service doesn't support IMAP and only supports POP3, it's also a good idea to move on. For example, if you have an Internet service provider that still offers 10 MB of e-mail storage you can only access over POP3, they probably haven't upgraded their e-mail service in 15 years. You should probably move along to a more modern service. Services like Gmail and Outlook.com can fetch e-mail from your old account over POP3 so you can get it all in one place. ☺



P*PCompAS Newsletter
Greg Lenihan, Editor
4905 Ramblewood Drive
Colorado Springs, CO 80920
e-mail: glenihan@comcast.net

Coming Events:
Next Membership Meeting: 1 Nov, beginning at 9 am (see directions below)
Next Breakfast Meeting: 15 Nov @ 8 am, Country Buffet, 801 N. Academy Blvd.
Newsletter Deadline: 22 Nov.

Check out our Web page at: http://ppcompas.apcug.org