June 2014

Visit our website at www.pcs4me.com Ken Johnson, Newsletter Editor

CALENDAR

SIG = Special Interest Group

This Week's Schedule:

June 14 - Saturday - 1:00-3:00 PM
General Meeting - Leader: Ray Carlson
Location: Prescott Public Library

First Hour: Transferring Money over the Internet

Some members have asked for a discussion of ways to transfer money over the Internet. During the first 30 minutes of this meeting, we will briefly review some of the alternative methods you can use including banks, Paypal, Google Wallet, Amazon Payments, Dwolla, Venmo, and Square Money. We will discuss how each works, their costs, limitations and risks. New efforts to make these services fast, easy to use and free will be described. The rest of this initial hour will be an open question and answer session using questions raised by those attending the meeting or submitted to the website prior to the meeting.

Second Hour: Phil Ball will begin by responding to questions left over from the first hour, and then will add his famous "Tips and Tricks" with insights into various topics that assist with regular computer use.

In addition to the presentations, the following are typical events which take place at our General meetings:

1) We hold an informal Flea Market in which you are encouraged to bring in your excess computer equipment or software and make them available for others to enjoy at no charge. Please deposit give-away items on the table in the back marked "Free Stuff." Any items left here at the end of the meeting are subject to disposal.

2) If you have items that are just too good to give away, you may set up a separate table and hold your own sale.

3) We conduct a raffle of new computer items at the end of the meeting, so make sure to get a pair of tickets from whoever is in charge and place one on the item you'd like to win.

4) We will also accept your used ink and toner cartridges for recycling. They are turned in to Think4Inc for credits which PCS uses to purchase office supplies from them.

Calendar *Cont on Pg 2*

Future Meetings

June 21 - Saturday - 1:00-3:00 PM
Joint meeting with PMUG (Prescott Mac User Group) - Leader: John Carter
Location: Prescott Public Library

Topic to be announced.

June 28 - Saturday - 1:00-3:00 PM
SmartPhone SIG - Leader: Murray Smolens
Location: Prescott Public Library

First Hour: For the inaugural SmartPhone SIG, Murray Smolens will present during the first hour a potentially interesting expose on the workings of a typical smartphone, the various device types, the top ten reasons for getting a smartphone, the difference between apps and widgets, and many other wondrous tidbits.

Second Hour: We will have a smartphone Q&A session with Alan Paradis, owner of Paradis Cellular, a local mobile phone dealer. If you have any specific smartphone questions for Alan that you would like an-

Note that these dates are correct at time of publication but are subject to change.
Up to date information can be found on our website, www.pcs4me.com

Unless otherwise noted, our meetings are usually held in the Founder's Suite at the Prescott Public Library.

Smart Device Users Beware: Fraud May Be Just a Click Away

A Heads Up e-mail from the Southeastern Wisconsin Windows User Group

Reprinted with Permission from:

porte brown, Certified Public Accountants

www.portebrown.com / www.sewwug.org

email (at) sewwug.org

This was forwarded from a CPA Member of SEWWUG. Even if you don't have a described "smart device," it explains a lot about the QR Codes we often see.

You've installed anti-virus software to protect your personal computer and business network. You know the signs of phishing scams (including unfamiliar senders, poor grammar and misspelled words). And like most people who use the Internet today, you never open a suspicious e-mail or download files from a questionable website.

But what have you done to protect your iPhone, Android or tablet from cyber theft?

Many smart devices currently operate without anti-virus and malware protection. Although there haven't been many high-profile fraud cases involving smart devices, opportunistic hackers are targeting these devices as the world of quick response (QR) codes grows.

Scammer's Delight

QR codes appeal to fraudsters for several reasons:

They're easy and cheap to create. All you need to do to set up a QR code is go to an online service and enter a web address. The site generates a QR code in seconds for free.

Malicious codes can be printed on stickers and placed on top of legitimate QR codes. Or a fraudster might post the code on a subway station bulletin board or a tourist monument and wait for curious victims to click on the image.

The human eye can't decipher QR codes. People can't tell a legitimate QR code from a malicious one. So it's easier to hide a "click jacking" scam than a phishing scam or virus. Smart devices don't usually slow down or show any other signs of "infection" until the user's data has long-since been compromised.

QR codes are relatively new, but rapidly growing. Hackers will increasingly exploit QR codes as more people purchase smart devices and more businesses use them for marketing purposes.

Users new to the QR code world may be unfamiliar with the risks of clicking on malicious codes and may not be security-conscious enough when using their smart devices.

What are QR Codes?

QR codes are square, two-dimensional barcodes that were originally used by auto manufacturers in the 1990s to track vehicle parts. Today, QR codes have become a popular marketing tool for businesses to connect with customers using smart devices.

You've probably seen QR codes in magazine ads, on business cards and product packaging -- even in taxis. Instead of remembering a web address and typing it into your browser, you can simply snap a photo of a QR code with your smart device.

Once clicked, QR codes perform all kinds of functions, quickly and easily. For example, a code might link to product specs on the company's website, enter the user into a prize contest, provide directions to an event, purchase a product using a PayPal account, "like" a company on Facebook or download coupons.

Unfortunately, QR codes can also be used to commit fraud.

Anatomy of a QR Code Scam:

Some QR codes are self-contained. That is, all the product information is coded into the image. If you have a QR reader on your smart device, it auto-converts the image and directs you to a website.

Other QR codes require you to download or purchase an application (app) to access an online server, which looks up the desired information or performs some other function. Both types of QR codes -- direct and indirect -- are susceptible to fraud.

Scammers can, for example, embed shortened URLS into QR codes to misdirect victims to cloned websites, where the fraudster sells product without ever fulfilling the contract or installs malware to gain control over the device. The next time the user accesses his or her mobile wallet or PayPal account, the malware captures that information and makes fraudulent charges.

Alternatively, proprietary apps pose a security risk by allowing the QR code author to install measurement and tracking systems onto the smart device.

Continued on page 4

Continued from pg 3:

Most QR code apps require consent to a user's agreement -- which many people fail to read -- and these could authorize the QR code author to track your cell phone usage, access your contacts and other personal information, or ring up charges for premium texts on your cell phone bill, for example.

An even bigger threat occurs when the user connects the smart device to a computer to charge it or sync data. The malware can "leap" to the PC, infecting it and any networks to which the computer is linked. This security risk is one reason some companies are leery of implementing bring-your-own-mobile-device (BYOD) programs.

Users Provide the First Line of Defense

Surprisingly few iPhone, Android or tablet users have taken steps to protect against fraud. Here are four simple things you can do to protect your smart device starting today:

Never click a QR code in a public place, such as a bus stop or mall. Only scan QR codes from trusted sources or vetted by third parties. Be especially careful when traveling overseas where QR code "click jacking" scams tend to be more common.

Always check a QR code for a sticker before scanning it. Use your fingernail. If it looks like a sticker, it could be a scam.

Never provide personal information or passwords if requested by a website linked to a QR code, even if the site appears to be legitimate.

Install a QR code scanner app that screens URLs before directing you to the site. These apps block unsafe sites and stop online threats before they're downloaded to your device. Search for "secure QR reader" on your smart device. Read the reviews and select one from an anti-virus software provider you know and trust.

The end result of all this is simple: Your smart devices are personal computers. Treat them that way. Don't wait for a major cyber threat to occur to prove that smart devices are vulnerable to viruses and malware. Contact an information technology professional for more information.

What is a 'CAPTCHA'?

by Phil Chenevert, member and instructor for Computer Lab Workshops

Cajun Clickers Computer Club, LA

December 2013 issue, Cajun Clickers Computer News

www.clickers.org

Have you ever found yourself grinding your teeth because you can't make out those weird words in something like this? All you want to do is get somewhere on the internet to do something and then, Wham! They hit you with this silliness!

Well, they are not there just to annoy us or have fun at our expense. They are there to save everyone a lot of misery so be patient with them. CAPTCHAs, or Completely Automated Public Turing Tests to Tell Computers and Humans Apart, exist to ensure that user input has not been generated by a computer. These peculiar puzzles are commonly used on the Web to protect registration and comment forms from spam.

To understand the need for CAPTCHAs, we should understand spammers' incentives for creating and using automated input systems. For the sake of simplicity, we'll think of spam as any unwarranted interaction or input on a website, whether malicious or for the benefit of the spammer (and that differs from the purpose of the website). Incentives to spam include:

Advertising on a massive scale;

Manipulating online voting systems;

Destabilizing a critical human equilibrium (i.e. creating an unfair advantage);

Vandalizing or destroying the integrity of a website;

Creating unnatural, unethical links to boost search engine rankings;

Continued on pg 5

Cont'd from page 4

Accessing private information;

Spreading malicious code.

A captcha is a challenge-response test that determines whether a user is human or an automated bot. A typical captcha includes an image of distorted text and a form field for the user to enter the text. Captchas are commonly found at the end of website forms, and must be filled out in order for the form to be submitted. By requiring users to decipher and enter the captcha text, webmasters can prevent automated programs from sending spam or other unwanted data through online forms.

It is estimated that 80% of email is actually spam and captcha's protect us from most of 'em. Be patient, use the 'give me another one' symbol that looks like two arrows, or the little speaker symbol to have it pronounce the word if you continually fail to type it correctly. It is kind of like seatbelts, irritating to put on but for our own safety.

A new software contrivance was discussed at the Build-or-Buy SIG on Wednesday, January 22. Previously, when free software was offered, one was frequently referred directly to the programmer's website. In more recent times, one would notice that the desired software was accompanied by boxes to select additional software to download and install. At least you had a chance not to download the add-ons.

Member to Member Tip

HAL-PC, Texas www.hal-pc.com

Free-Software ALERT

A new software contrivance was discussed at the Build-or-Buy SIG on Wednesday, January 22. Previously, when free software was offered, one was frequently referred directly to the programmer's website. In more recent times, one would notice that the desired software was accompanied by boxes to select additional software to download and install. At least you had a chance not to download the add-ons.

Then came the "installers." Here you couldn't directly access the desired software, but had to be subjected to advertisements and also other software you were virtually trapped into downloading in order to get to the free software that you wanted. CNET is infamous for this. Some of this unwanted software is almost as bad as viruses, Trojans, and worms.

The most common "additives" include taskbars, driver updates, and performance improvers. It can be extremely pervasive.

Joe Whinery, a Co-Chair of the Build or Buy SIG, along with Gill Boyd, discussed a process to counter this:

1. Always check the download order to uncheck any unwanted software. Look for "boxes."
2. To install, select Custom instead of "Default" or "Automatic" or "Recommended" when downloading, so you can select what is to be downloaded.
3. Read each screen of the install operation.
4. Look for a "Decline" option (which may appear to be grayed out, but is functional).
5. Decline these options.
6. When the download is complete, Install, but DO NOT RUN the downloaded software, instead: Go to Control Panel, then Add/Remove Programs (Programs and Features in Win7 and 8).
7. Then SORT by date.

Examine the listing for the software that you WANTED. If there is anything else with the same date/time that you did not intentionally install, delete it.

Now you can safely run your desired program. This may seem like a chore but it is much easier than trying to undo something that infiltrated your machine.

Continued on pg 6

Continued from pg 5

Fun and Knowledge with YouTube

By Jim Cerny, 2nd Vice President, Sarasota PCUG, Florida

February 2014 issue, PC Monitor

www.spcug.org

jimcerny123 (at) gmail.com

Whether you have a tablet, smart phone, or any kind of computer, YouTube is one application that can, all by itself, really justify the purchase of your device. YouTube can be found on the internet at youtube.com (that's easy to remember, right?) or you can download the free YouTube application for any device. Since Google has acquired YouTube, it can also be found on the Google web site (it used to be Google videos).

YouTube is your access to millions of videos made by almost anyone who wants to make them available to you for free. Many of the videos are fantastic and some are just a waste of time. But YOU decide. You search for the videos you want to see simply by entering your search criteria (regular English words) in the search box. Do you have a favorite entertainer? Just enter their name and you will have access to hundreds of their videos. How about a home improvement project? Just enter what it is you want to do and see a video of how to do it. Almost anything you can think of, there is probably a video on that subject on YouTube.

Here are just a few examples of fun things to see and explore on YouTube: Famous people, science experiments, college lectures, cartoons, news, products, companies, cooking, travel, painting, and, well just about everything.

The only thing it seems that YouTube does not give you is fairly recent free movies and TV shows. If you searched for a movie or TV show by its title, YouTube will probably only show you the "trailers" for free. However, YouTube does offer some movies and TV shows for a price. But the real fun for me is seeing all that is available to you at no cost whatsoever – and you do not have to join anything.

You could think of YouTube as the ultimate "window to the world" and all that is in it by just using your computer or device. Why read a printed article or view pictures? YouTube can SHOW you what other sources only TELL you. Click on the right-pointing arrow to play the video. You can click on any point on the progress bar to go to that point in the video. And you can click on pause (usually the double vertical line symbol), just like you used to do with the old video VHS tape players. After clicking on "pause" you can go back to the list of videos just like you do with Google. Some videos may have a short advertisement the plays before the real video starts.

There is really no limit to what YouTube has to offer. I have yet to search for something that did not have some kind of video to watch on that subject. So do not limit your imagination either. Here are just a few things I have found – each of which can provide hours and hours of videos:

- Enter your favorite game and learn how to play the game or sport better.
- Enter "How to…" and learn a new skill or improve the skills you have.
- Tour your favorite city, park, or attraction.
- Ride all the roller coasters you want, at any park, and never have to wait in line or get dizzy.
- Attend a class lecture at a famous university.
- View long-forgotten videos of famous people and entertainers.
- View videos of how to use your digital camera or tablet or any device or contraption.
- See dangerous stunts, magic tricks, and stupid jokes.

Discover new things about your favorite hobby.

So don't hold back – be adventurous and explore the world! Your brain will thank you for it.

Need Help With Computers?

Did you know that the Prescott Public Library has a program of Computer mentoring on a one-on-one basis? They have several experienced volunteers who will work with you using one of the Library computers.

All you need to do is make an appointment with either the "Ask a Librarian" personnel or go to:
http://www.prescottlibrary.info/.