$3.⁰⁰
(membership includes
monthly subscription)

The Digital Viking

Twin Cities PC User Group NEWSLETTER

Minneapolis & St. Paul, Minnesota USA • Vol. 36 No.7 • February 2016

TC/PC Exists to
Facilitate and Encourage
the Cooperative Exchange of
PC Knowledge and
Information Across
All Levels of Experience

February 2016

General Meeting

Tuesday, February 9, 2015
7:00 PM

How is your personal data being used ?

How vulnerable are Students and Seniors to Internet data trackers ?

Presenter: Don Gemberling, J.D.

Location: Summit Place
8505 Flying Cloud Drive
Eden Prairie, MN

Don Gemberling began working with issues of transparency, governmental accountability, the implications of technology on humans, and data privacy in 1973. For over thirty years he was the only staff or managed functions in the Minnesota Department of Administration that involved helping government agencies comply with the Data Practices Act and related law and citizens with exercising their rights under those laws. He is currently on the Board of the Minnesota Coalition on Government Information, and serves as its spokesperson. He graduated from Macalester College and William Mitchell College of Law. He will be bringing us up to date on current issues with data tracking in our schools and our personal lives. This is critical information for you to be aware of. Please join us at the meeting. Special thanks to Jim Grotz for arranging this presentation.💻

Tech Topics 6PM: Tech Topics Book Club with Jack Ungerleider– Books: Design for 3D Printing and the Internet of Things .💻

TC/PC is a Member of APCUG

24-Hour Information • www.tcpc.com
Application form inside back cover

TC/PC Business Members

Friendship Village

Thank You!

The Digital Viking

The Digital Viking is the *official monthly publication of the Twin Cities PC User Group, a 501(c)(3)organization and an all-volunteer organization dedicated to users of IBM-compatible computers. Subscriptions are included in membership. We welcome articles and reviews from members.* The Digital Viking is a *copyrighted publication and reproduction of any material is expressly prohibited without permission. Exception: other User Groups may use material if unaltered and credited.*

Disclaimer: *All opinions are those of the authors and do not necessarily represent the opinions of the TC/PC, its Board of Directors, Officers, or newsletter staff. TC/PC does not endorse, rate, or otherwise officially comment on products available; therefore, readers are cautioned to rely on the opinions presented herein exclusively at their own risk.* The Digital Viking, *its contributors, and staff assume no liability for damages arising out of the publication or non-publication of any advertisement, article, or other item. All refunds in full or in partial, for advertising, membership or any other item shall be at the sole discretion of the Twin Cities PC User Group Board of Directors.*

Advertising

Full page (7½ x 9½)	**$100.00**
Two-thirds page (7½ x 6)	**80.00**
Half page (7½ x 4¾)	**65.00**
One-third page (7½ x 3)	**50.00**
Quarter page (3½ x 4¾)	**40.00**
Member Bus. Card (2 x 3½)	**10.00**

Multiple insertion discounts available.

Contact Sharon Walbran at:: SQWalbran@yahoo.com

Deadline for ad placement is the 1st of the month prior to publication. All rates are per issue and for digital or camera-ready ads. Typesetting and other services are extra and must be requested in advance of submission deadlines.

Payment must accompany order unless other arrangements are made in advance. Place make checks payable to: **Twin Cities PC User Group**

TC/PC Member Benefits

Product previews and demonstrations

Special Interest Groups Monthly Newsletter

Discounts on products and services

Contests and prizes

Business Member Benefits

All of the above PLUS:

FREE ½ page ad on payment of each renewal

20% discount on all ads Placed in the *Digital Viking* Newsletter

Up to 5 newsletters mailed to your site (only a nominal cost for each additional 5 mailed)

TC/PC 2015-2016 Board of Directors

Meets once or twice per year. All members welcome to attend.
Visit www.tcpc.com for meeting details.

President —Bill Ryder	br@rydereng.com
Vice President —Curt Trout	ctrout@troutreach.com
Secretary - Sharon Walbran	sqwalbran@yahoo.com
Treasurer - Sheri Trout	strout@troutreach.com
Membership - - Open Position - -	
Meeting Coordinator- - Open Position - -	
Newsletter Publisher Sharon Walbran	952-925-2726 SQWalbran@yahoo.com
Web Master Curt Trout	ctrout@troutreach.com
Jeannine Sloan	Ambassador for Friendship Village
Joel Hedland	joelh@spacestar.net
Jim Schlaeppi	jschlaeppi@charter.net
Lon Ortner	612-824-4946 csacomp@comcast.net
Steve Kuhlmey	steve@kuhlmeysystems.com
Gary Grau	oxygary2389@yahoo.com
Ross Held	RHeld3745@aol.com
David Van Dongen	davidvandongen@yahoo.com

Newsletter Staff

Editor Sharon Walbran

Contributors:

Jeannine Sloan

Tech Topics SIG: Starting the new year right

The following is the current plan for the Tech Topics SIG in early 2016. Please note that all topics are subject to change.

February 2016 - The Tech Topics Book Club: Design for 3D Printing and the Internet of Things I recently purchased two books that should be interesting in the context of this SIG. The first is a good intro to the terminology and technology of 3D printing. The second is a guide to “smart” technology that is popping up in all areas.

March 2016 - Browsers: Why you want more than one March 2016 will be the six month anniversary of Google turning off support for NPAPI in Chrome. As a result there are some websites that won’t work with Chrome anymore, or at least until they remove the need for NPAPI plugins like Java and Silverlight. Many of Google’s apps work best with Chrome and may lose features in Internet Explorer. We will explore the strengths, weaknesses, and limitations of the major browsers.💻

The "Internet of Things" or IoT - More Common But Hackable

by Ira Wilsker, iwilsker(at)gmail.com

WEBSITES:
http://www.cnet.com/news/internet-connected-homes-open-the-door-to-hackers

https://www.cesweb.org

https://www.cta.tech/Blog/Articles/2015/December/VIDEO-The-Wearables-Making-Us-Smarter-More-Fit-an

https://en.wikipedia.org/wiki/Internet_of_Things

https://nest.com

http://www.forbes.com/sites/josephsteinberg/2014/01/27/these-devices-may-be-spying-on-you-even-in-your-own-home

https://www.shodan.io

A few years at the Consumer Electronics Show (CES) in Las Vegas, I was intrigued by the numbers of both prototype and production items that were evolving into what is now known as "the "Internet of Things", or "IoT". For the majority of us, when we think of the internet, we think of our internet connected computers, tablets, and smart phones. What many of us are not well aware of is that the Internet of Things is beginning to be much more common, and the IoT is already around us in a big way.

When I was last at CES, I was amazed at how internet connections had already made their way into household appliances, and other electronic devices. At CES I saw products being introduced by major appliance manufactures that had connected intelligence built into them.

Among some of the most impressive items that I saw demonstrated were what appeared to be conventional residential kitchen refrigerators that had what appeared to be a flat screen tablet on the front of the door, as well as other types of sensors and readers built into the appliance. The tablet on the front door could be connected to the internet via Wi-Fi and used to order groceries from participating supermarkets, display recipes, and create shopping lists. A small bar code reader was installed on the door that could read the UPC codes on products, adding those items to a digital shopping list that could be remotely printed, or sent directly to the chosen supermarket. The tablet on the refrigerator door would also display digital coupons and other promotions, enabling the owner to instantly add the promoted item to the grocery list.

This internet connected refrigerator, as well as IoT connected washers, dryers, dishwashers, air conditioners, stoves, ovens, microwaves, and other major appliances also incorporated a "service connection" which monitored the physical operating condition of the appliances. These appliances utilizing their internet connection, typically Wi-Fi, would report their operating condition, suggest repairs and maintenance, provide or order a list of replacement parts, display do-it-yourself repair instructions, or contact a repair service if necessary. Most of these devices would actually send an email or text message to the appliance owner alerting him of the issues.

Many auto manufacturers currently offer "OnStar", "BlueLink", or other types of cellular or internet connected monitoring systems that can report on maintenance issues, service reminders, and other issues, as well as providing a method of emergency communications. My wife's car periodically sends her an email listing the mechanical condition of each of the major components on her car.

We are seeing much more of our homes being controlled or secured by the IoT under the general topic of "Building and home automation". Most modern home security systems can be remotely accessed and controlled by cell phone; security cameras can display their images on remote devices anywhere. Lamps can be remotely controlled to turn on or off by remote command. Even our utility usage and thermostats can be accessed remotely. The very popular Nest thermostat, along with an increasing number of competitors, offers internet connected control of household temperatures, as well as smoke detectors and remote cameras. My new "smart TV" is connected to my home data network which allows me to use my smart phone as a fully functional remote to not just control the TV, but to also search through dozens of streaming media services to watch countless movies, TV shows, videos, and other content, all connected by my home Wi-Fi network.

A review of local industry, health care facilities, public utilities, transportation systems, and other commercial enterprises are rapidly becoming more involved with the IoT. Look at your water, gas, and electric meters; many are already internet connected in order to speed automate "meter reading" saving time and money. In the medical field, health monitoring and diagnostic equipment is becoming more connected to the internet. According to Wikipedia, "These health monitoring devices can range from blood pressure and heart rate monitors to advanced devices capable of monitoring specialized implants, such as pacemakers or advanced hearing aids. ... Other consumer devices to encourage healthy living, such as, connected scales or wearable heart monitors, are also a possibility with the IoT. ... Doctors can monitor the health of their patients on their smart phones after the patient gets discharged from the hospital."

While much of this current IoT technology is infringing on what used to be in the realm of science fiction, there is also a dark side to the IoT. Already hackers are breaking into internet connected devices other than the traditional computers and data networks in order to illicitly control these IoT devices, alter or steal data and personal information, or shut them down on demand. In terms of connected medical devices, there have been some serious concerns expressed about complying with HIPAA and other privacy and security rules and regulations.

It has been well documented that some common household smart devices, most notably smart TVs, have actually spied on their owners. This was reported about two years ago in Forbes magazine by Joseph Steinberg, in his expose' "These Devices May Be Spying On You (Even In Your Own Home)" On January 27, 2014, this article in Forbes said, Televisions may track what you watch. Some LG televisions were found to spy on not only what channels were being watched, but even transmitted back to LG the names of files on USB drives connected to the television. Hackers have also demonstrated that they can hack some models of Samsung TVs and use them as vehicles to capture data from networks to which they are attached, and even watch whatever the cameras built in to the televisions see." Internet connected coffee makers, which can be remotely programmed to make morning coffee may disclose to hackers when you may be waking up, and even what time you might be returning home, valuable information for residential burglars. The smart refrigerator may be selling your shopping information to third parties. In an unexpected and unusual case, Joseph Steinberg reported that a smart refrigerator was used to send out spam emails, " ... (P)otential vulnerabilities have been reported in smart kitchen devices for quite some time, and less than a month ago a smart refrigerator was found to have been used by hackers in a malicious email attack. You read that correctly – hackers successfully used a refrigerator to send out malicious emails." Also in that Forbes article, companies providing DVR, satellite, and cable service have been alleged to have sold information of shows and other content watched in the household in order for advertisers to better target their advertising. It is also widely known that many internet service providers compile lists of websites visited; since may people get their TV and internet from the same provider, these companies could combine that information, which Forbes warns, "a single party may know a lot more about you then you might think."

Another popular target for hackers and other miscreants is common household video capture equipment, such as a webcam or a home security camera; remote baby monitors are similarly targeted. Forbes disclosed that malware on a computer can remotely turn on and off the internet connected cameras. In one notable case referenced in the Forbes article was how a Miss Teen USA was allegedly blackmailed by a hacker who controlled her laptop's integral webcam, " ... and photographed her naked when she thought the camera was not on." The images of home security cameras, often transmitted unencrypted over the internet, can be captured by burglars, informing them that not just is the home currently unoccupied, but also the location of the potentially incriminating cameras!

Information about specific items connected to the internet is readily available, and even searchable as easily as any other internet data. The Shanghai based website Shodan (shodan.io) describes itself as, "Shodan is the world's first search engine for Internet-connected devices." On the front page of Shodan is a self aggrandizing statement that says, "Explore the Internet of Things. Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.", followed by, "See the Big Picture - Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!" Just as an experiment, I registered on Shodan with a disposable email address, and did a quick search of my neighborhood; I found nine potentially vulnerable IoT connected devices within a small radius of my house. I also found that some local service stations monitor their gasoline inventory in real time, transmitting their data in real time over an unencrypted internet connection. For example, when searched, one particular major refiner branded station reported, "IN-TANK INVENTORY Regular 7263 (gallons), Temperature 51.74 degrees" as well as other inventory information. This was one of 45 "Automated Tank Gauges" reported by Shodan in this area. This gasoline tank information was just a very small snippet of the millions of such internet connected devices that most of us have no idea even exists.

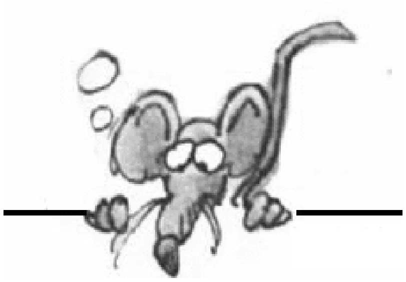
In a December 28, 2015 article published by Cnet, "Internet-connected homes open the door to hackers", with the subtitle, "Baby monitors, thermostats, kitchen gadgets and other "smart" devices add convenience to our daily lives. What are manufacturers doing to make sure they don't make life easier for criminals too?", the author, Laura Hautala, explained the vulnerabilities of our household IoT. In the opening of the article, employees of a Sunnyvale, California cybersecurity company, Fortinet, used the Shodan search engine to find a video stream in Saudi Arabia, 8100 miles away. Using the too common factory default username and password of "admin", they were able to view the streaming video. According to Fortinet engineer, Aamir Lakhani, the Shodan search engine can display, " ... a huge trove of Internet-connected devices, from baby monitors to cars, cameras and even traffic lights." Sadly, many of these devices still use factory default usernames and passwords, and transmit their data over unencrypted internet links. The Cnet article goes on to state, " Billions of sensors will soon be built into appliances, security systems, health monitors, door locks, cars and city streets to help manage energy use, control traffic, monitor air quality and even warn physicians when a patient is about to have a stroke."

The Cnet article stated that a well respected market forecaster, Gartner, predicted that in 2016 there will be 6.4 billion internet connected devices in use. Many new IoT devices will be displayed and demonstrated at this year's CES in Las Vegas. Among some of the risks of an insecure IoT could be a variety of malicious vandalism, as well as outright identity theft, terrorism, and crimes of opportunity. Tanuj Mohan, co-founder of Enlighted, gave one such potential example of vandalism. He was quoted in Cnet as saying, " That connected coffee maker in the office -- it wouldn't be much of a stretch for a hacker to put it into a continuous loop and brew coffee throughout the weekend, flooding the office. ... When computers hold the reins, criminals can grab control in unexpected ways." At present, there is no coordination or uniform standard for IoT security, and many manufactures of IoT devices do not incorporate adequate default security into their devices, making the aggregate vulnerability of the devices potentially catastrophic. Mohan warned that manufacturers are not paying attention to the potential security vulnerabilities of many of their products. "They're not yet aware of how everything they build can be exploited. Safety last."

We, as users of IoT products need to take some personal responsibility for the use of our connected products. We should never use any default usernames and passwords such as the "admin" used to give total access to video link mentioned above, but instead use difficult to guess passwords. Since many of the devices offer some form of encryption as an optional setting, it would be wise for all users to engage that option, and set a complex pass phrase for a decryption key.

The Cnet article closes with a very prophetic statement. "Baby monitors, thermostats, kitchen gadgets and other "smart" devices add convenience to our daily lives. What are manufacturers doing to make sure they don't make life easier for criminals too?"💻

Go to Page 1



NIBBLERS

By Jeannine Sloan

Alleged Hit-And-Run Foiled After Car Calls The Cops

https://nakedsecurity.sophos.com/2015/12/08/alleged-hit-and-run-foiled-after-drivers-car-calls-thecops-on-her/

Weird Science: 10 Strange Tech Stories From 2015

http://www.infoworld.com/article/3017733/

10 'Star Wars' Technologies That Are Almost Here

http://www.infoworld.com/article/3015692/

Bizarre CES tech

Among other stuff the bizarre items on this site include:
· This smart belt will loosen itself if you eat too much… and
· A mirror that 'helpfully" points out all your flaws
http://www.techradar.com/us/news/world-of-tech/here-s-the-most-crazy-awesome-and-weird-tech-atces-2015-1280136

Wearable Waste: Shoes 3D-Printed with Plastic Ocean Trash

http://gajitz.com/wearable-waste-shoes-3d-printed-with-plastic-ocean-trash/

BLITAB First Tactile Tablet for Blind People

https://www.youtube.com/watch?v=AN2QfdvdQiA

Ford's Wacky Idea For A Rear Wheel That Doubles As A Unicycle

http://www.foxnews.com/tech/2015/12/30/check-out-fords-wacky-idea-for-rear-wheel-that-doublesas-unicycle.html

Suitcase Tracks Itself, Locks On Cue

Bluesmart's suitcase has a SIM-card embedded inside it, courtesy of a tie-up with mobile operator Telefonica. That SIM is included in the price of the suitcase, so there's no monthly fee, and it gives you the case's location on a map via the accompanying app, should it get lost.
http://www.cnet.com/products/bluesmart-carry-on/

A Brief History Of Microsoft On The Web

http://www.microsoft.com/misc/features/features_flshbk.htm

Microsoft Feature Archive: A Good Time Wasting Site

http://www.microsoft.com/misc/features/features_archive.htm

Windows Superpowers

Windows has some pretty cool features, but many of them are hidden away, so that average users won't accidentally tinker with their systems in unintended ways. We call these features "superpowers". Here is how to access them:
http://www.makeuseof.com/tag/10-windows-superpowers-access/

IE11 Keyboard Shortcuts

Navigating Internet Explorer 10 and 11 can be super quick if you know what you're doing. Take a look at this list of awesome keyboard shortcuts for Internet Explorer 10 and 11.
http://technomaverick.com/2013/11/04/15-awesome-internet-explorer-keyboard-shortcuts/

Great Idea

By hanging wind turbines under the bridges, the design can capture some of the highest wind speeds while avoiding any impact from construction on land. http://www.fastcoexist.com/3054854/

2016, Intel's Entire Supply Chain Will Be Conflict-Free

We said, we don't want to support conflict, period. Buying electronics used to help fund war in Africa. Now big tech companies like Intel are working to make sure their money isn't used for destruction.
http://www.fastcoexist.com/3055066/

IE11

From January 12, 2016. Internet Explorer 11 is the latest version of Microsoft's browser for Windows 7, Windows 8.1 and Windows 10 and thus, will be the only version to continue to receive support.
http://www.techspot.com/news/63380-microsoft-end-support-internet-explorer-8-9-10.html

Cybersquirrel 1

So, if you are cynical of the word cyberwar, as we are, and you enjoy the occasional piece of amusing satire, you'll love the cute-rodent-of-the-week meme: **Cyber Squirrel 1**.
According to @CyberSquirrel1, the score currently sits at **Squirrels 623, USA 1.**
(You can probably guess what the 1 refers to. It's not known whether this attack actually succeeded, or ended up being a handy excuse for Iran's failed centrifuges, but that doesn't matter now…the 1, of course, is the Stuxnet virus.) http://tinyurl.com/hbzcgbg

Six Tips to Protect Your Search Privacy

1. Don't put personally identifying information in your search terms *(easy)*
2. Don't use your ISP's search engine *(easy)*
3. Don't login to your search engine or related tools *(intermediate)*
4. Block "cookies" from your search engine *(intermediate)*
5. Vary your IP address (intermediate)
6. Use web proxies and anonymizing software like Tor *(advanced)*

https://www.eff.org/wp/six-tips-protect-your-search-privacy

Map Shows How the World's Population is Divided Among Countries

http://metrocosm.com/world-population-split-in-half-map/

List of Features Removed Or Deprecated In Windows 10

With every new release of the Windows operating system, Microsoft, based on user usage data, decides to enhance or deprecate a feature.
http://www.thewindowsclub.com/features-removed-in-windows-10

How to Pin (Almost) Anything To the Start Menu As A Tile

The trick is that anything in the All Apps list is able to become a tile, which then can be pinned to the Start Menu. But how do you get your things on the All Apps list? I got it covered here.
First, navigate to this location:
C:\ProgramData\Microsoft\Windows\Start Menu\Programs

Right click on the empty space and choose New -> Shortcut.

Click Browse to find a file, a folder, or whatever you want to pin.

Then hit Next and OK and you'll have a shortcut.

That's how you put your item into the All Apps list. Just go to the Start Menu, click All Apps and check if you got it in.

From this point, everything will be easy. As you know, to pin item in All Apps to the right side, you just need to right click on it and select Pin to Start.

Voila you got its live tile on the Start Menu. Read more at http://dottech.org/187984/

Windows 10 Recovery Drive

The changes to the self-booting, Windows-recovery system start with the name. Bowing to changes in PC technology, it's no longer a rescue ***disc,*** it's now a rescue ***drive.*** In fact, creating a bootable CD or DVD is no longer an option; you must use a spare USB flash drive with a capacity of at least 512MB. But for a recovery drive with a complete set of tools, you'll need an 8GB or larger drive. http://windows.microsoft.com/en-us/windows-10/create-a-recovery-drive

Tips toTake Good Pictures of Animals

*Get out early and stay out late.
*Shoot in badweather.
*Photograph local subjects… the animals closest to you.
*Bring the wildlife to you.
*Get down low.
*Watch your backgrounds.
*Shoot wide.
*Shoot close.
*Use the rule of thirds.
*Practice makes perfect.
http://tinyurl.com/zdxl4ol

Show/Hide File Extensions

Open File Explorer (Logo+e). Click on View tab and check the "Hidden Items" or "File Name Extension" boxes, and uncheck them when you're done.

Customize File Explorer Search in Windows 10

To do a search in Windows 10 File Explorer simply begin typing when the File Explorer screen opens. There are two options for how File Explorer responds (see below).
To change your preferences you will have to open the Control Panel, then File Explorer Options, then click on the View tab. Under Advanced settings > When typing into list view, you will see the following options: Automatically type into the Search Box
Select the typed item in the view.
I set mine to ‘Automatically type into the Search box’.

Find the Mouse Pointer

Playing "find the mouse pointer" is no fun for anyone with less than 20/20 vision, especially on the latest super-high-resolution laptops. Luckily, there are solutions built into every modern version of Windows. You'll find the necessary settings in the classic Control Panel, under Mouse Options:
On the Pointers tab, choose one of the Large or Extra Large schemes to make the pointer bigger.
The Windows Black (Large) option is the one I prefer.
On the Pointer Options tab, select the Display Pointer Trails check box to make the pointer easier to see as it moves.
At the bottom of that same tab, select the ‘Show Location Of Pointer When I Press The CTRL Key’ option.
Click OK to save your changes and close the dialog box.

Memorize These

If you're running Windows 8.1 or Windows 10, you have a whole batch of new shortcuts, like these:
Windows key + L locks the PC immediately (think of it as the ultimate Boss key).d
Windows key + X opens the Quick Link menu more quickly than right-clicking on Start.
Windows key + I opens the Windows Settings app, where you can begin typing to search for any setting.
Windows key + PrtScrs takes a screenshot and saves it in a subfolder of Pictures.

Adjust Volume for Individual Programs in Windows 10

Right-click on the volume icon to bring up the menu shown at the left.
Any open app will appear in the mixer window with a control slider. Hint from the Windows club.
http://tinyurl.com/zvd5sd9

Read Anywhere, on Anything

From smart phones and tablets to desktop computers and even televisions, ‘Read’ works on anything with an up-to-date web browser. You can download Read books too, so you can read them offline in your web browser.
http://readinfo.overdrive.com/about/faq

Go to Page 1

Special Interest Groups (SIGs)

w Work phone h Home phone c Cell phone
*** Meets at an alternate location**

Most SIGs will meet at Edina Executive Plaza, Conference Room #102, 5200 Willson Road, Edina, MN
Confirm with a SIG group if they meet elsewhere.
For more info contact the SIG Leader(s) listed here.

Get SIG announcements!
Link from www.tcpc.com

Board of Directors*

All members are welcome! Check www.tcpc.com for location.
Selected Saturday mornings

Linux on Saturday

This is for the Linux newbie and those trying to come over from Microsoft to a different operating system.
First Saturday @ 9 AM-Noon
Note: No Meetings June-August

Jack Ungerleider 612/418-3494 c
jack@jacku.com

Tech Topics

Technical presentation/discussion on various technical topics from the following areas:

- **Web/Internet**
- **Mobile Devices and Apps**
- **Playing with Programming**
- **DIY (3D Printing, R-Pi, other hobby electronics, etc.)**

Second Tuesday @ 6:00-7:00 PM
Every month
Right before the general meeting.

Jack Ungerleider 612/418-3494 c
jack@jacku.com

Microsoft Access

All levels. Presentations by expert developers within the group and by MS reps.
Third Saturday 9:00 AM—Noon
Note: No Meetings June-August

Steve Kuhlmey 952/934-8492
skuhlmey@hotmail.com

Microsoft Office

Addresses the use, integration, and nuances of the Microsoft Office applications.
Combined with Systems on Saturday
Third Saturday of the Month
9:00 AM—Noon
Note: No Meetings June-August

Steve Kuhlmey 952/934-8492
skuhlmey@hotmail.com

Directions to **Edina Executive Plaza** for **Systems on Saturday, Access, Word and Picture Perfect SIGs**: Take Highway 100 to the 50th Street/Vernon exit. [If you have come from the north, cross back over Highway 100 to the east side.] Take the first right and go past Perkins [The golf course will be on your left.] and continue on the east frontage road (Willson Road) to the next building—5200 . There is ample parking in the building's lot. Conference Room #102 is on 1st floor.

Directions to **Summit Place** for **General Meetings**:
Proceed to Eden Prairie Center Flying Cloud Drive . [Flying Cloud Drive runs along the West side of the Eden Prairie Center.] Once you have driven past Eden Prairie Center (on the left) along Flying Cloud Drive you will come to a stop light at Prairie Center Drive. The next intersection with a stop light and left turn lane is Fountain Place. Turn left at Fountain Place and go straight into the parking lot. Turn left again to the first covered entry way of Summit Place. There is plenty of parking in the large parking lot in front of the first Summit Place covered entry way. When you enter the door at the first covered entry way, ask to be directed to the Performance Room for the TC/PC meeting. For a map of more detailed directions and ***info on Web SIG and Board meeting***, check the TC/PC website.

Help yourself by helping others!

Join the team & share your knowledge with others.

Contact TC/PC at www.tcpc.com

Meetings start at 7:00 PM (9:00 AM on Saturday) unless otherwise noted. *Meets at Edina Executive Plaza.

February

March

SUN	MON	TUES	WED	THU	FRI	SAT
	1	2	3	4	5	6 Linux and Open Source on Saturdays 9:00—Noon
7	8	9 1Gen Mtg 7:00 PM Data Tracker Issues-Gemberling 6PM Tech Topics: Book Club-3D Printing & IoT	10	11	12	13
14	15	16	17	18	19	20 Windows & MS Office (including Access) 9:00-Noon
21	22	23	24	25	26	27
28	29	1	2	3	4	5 Linux and Open Source on Saturdays 9:00—Noon
6	7	8 1Gen Mtg 7:00 PM TBA 6PM Tech Topics	9	10	11	12
13	14	15	16	17	18	19 Windows & MS Office (including Access) 9:00-Noon
20	21	22	23	24	25	26
27	28	29	30	31		

Go to Page 1

Security Software for your Android Device

by Ira Wilsker, iwilsker(at)gmail.com

WEBSITES:
http://drippler.com/drip/featured-top-10-antivirus-apps-android

http://www.techsupportalert.com/best-free-android-apps.htm?page=0%2C10

http://www.techsupportalert.com/content/best-free-antivirus-app-android.htm

http://www.androidheadlines.com/2016/01/featured-top-10-antivirus-apps-for-android.html

http://www.amazon.com/underground

With over a billion devices currently running the Android operating system, Android has been becoming more of a target for hackers and malware authors.

There is a continuing heavy debate about the need for security software on Android powered devices with one school of thought being that security software is unnecessary on Android devices because of the way that Google created Android with it being (supposedly) impossible for malware infected apps to contaminate other parts of the device because apps run in their own "sandbox" or memory space; the processor time and memory overhead of security software only degrades Android performance without any corresponding benefit.

Many other security experts vehemently disagree, stating that there has been an explosive increase in malware targeting the Android operating system. One of the primary reasons for this explosive in Android targeted malware is the vast number of Android devices running older versions of the Android operating system that have well known security vulnerabilities.

Many of those citing the imperative need for security software on Android devices put some of the blame on the cell phone companies and device manufacturers that do not promptly pass on to their users the latest updates and patches for their Android devices, despite the fact that Google does provide the carriers and makers with these necessary patches promptly and in a timely fashion. Anecdotally, my wife's late model, name brand cell phone connected to a major cellular provider has still not received the upgrade to Android "Marshmallow" 6.0; neither has one of my cell phones (I have two) yet received the upgrade to Android 6. In contrast, my other phone, a Google Nexus 6, connected to Google's Project Fi cell phone service, received the upgrade to Android 6, when it first became available, as well as another upgrade to Android 6.01 a short time later. Now it receives the monthly patches and upgrades directly from Google within days of their release. To be fair, there are a few other brands and models of cell phones that receive prompt Android updates and upgrades shortly after their release, but these are the exception, as most other phones and android devices receive updates and upgrades months after release, if they ever receive them at all.

For those who may feel more comfortable with the greater perceived security having antimalware (antivirus) software on their Android devices, there are a wealth of products available, both free and paid. Almost all of the better known publishers of PC security software also publish Android security apps, and dozens of other app publishers have released Android security software.

While many have their own personal favorite security apps, sometimes based on their experiences with similarly named PC software, there are also several online resources that have tested, evaluated, and rated many of the available security offerings. My personal favorite resource, often mentioned here in earlier columns, is Gizmo's TechSupportAlert.com, a non-commercial, community based resource with over 2000 volunteers who continuously evaluate and rate free software and apps for almost every operating system, including Android. Their recommended Android security apps are listed online at techsupportalert.com/content/best-free-antivirus-app-android.htm, where the Gizmo crew has narrowed down the multitude of available Android security apps, rank ordered them, made recommendations, and even listed several as "Not Recommended".

Gizmo stated that there are several "Aspects to be considered when choosing a Security App for Android." First on the list of necessary or desirable features is obviously the security app's ability to detect, clean, and delete malicious malware and other content, as well as provide real-time protection. Some of the tested security apps also provide "Extra Protection" which may include secure web browsing (prevent malicious content from infected websites), protection from spam and malicious text messages, and protection from "Potentially Unwanted Apps" that may be more threatening than beneficial. Some of the security apps include a "Privacy Advisor" which checks the "permissions" granted to each of the installed apps, informing the user of any potential privacy risks. Several of the security apps include "USSD Exploit Protection" which prevents special "dialed" codes that can be used to exploit internal phone functions, possibly giving a hacker unwelcome access to the device. Some of the security apps also include some "Extra tools" which may include call filtering (blocking spam phone calls and text messages), contact backup and restore, and other useful functions. The final evaluation performed by the Gizmo community is a measure of how much of the system resources (memory and processor power) is used by the security app; less system resources used means better overall performance. Even though Google's free "Android Device Manager" available in the Play Store offers excellent antitheft protection, many of the security apps also offer enhanced antitheft and lost device protection.

All of the apps reviewed by Gizmo are readily available and free for download from the Play Store. Gizmo's top rated security app is CM (Cheetah Mobile) Security, which earned Gizmo's highest five-star rating, and was awarded "Gizmo's Freeware award as the best product in its class!" Gizmo said that CM Security, "Runs as a stand-alone program on a user's computer; Offers an effective and complete security suite in a small package. Full SD Card scan option. Malware scan not limited to APKs. Very RAM friendly. Small installation size." The CM Security app also integrates seamlessly with other products from the same publisher, especially the very popular Clean Master app which is the world's most widely used Android device cleaner.

The number two rated security app was Malwarebytes Anti-Malware, which also had the highest five-star rating. Gizmo says, "Runs as a stand-alone program on a user's computer. Very easy to use. Fast and effective anti-malware engine. Useful set of privacy tools." The only issue that the reviewers had with the Malwarebytes app was the amount of battery power used, and the quirky update check.

The Gizmo reviewer community gave four other popular Android security apps a four-star rating; these apps are avast! Mobile Security & Antivirus, Comodo Mobile Security, Sophos Free Security & Antivirus, and Lookout Security & Antivirus. Another app, 360 Security, earned a three-star rating. Several other security apps, including a few from the major PC security publishers, were reviewed, but not rated for a variety of reasons; three other security apps were rated "Not Recommended".

Another very popular Android resource, "AH", also known as "Android Headlines", published in its January 14, 2016 edition an article "Top 10 Antivirus Apps for Android" (androidheadlines.com/2016/01/featured-top-10-antivirus-apps-for-android.html). Unlike Gizmo's list, this listing from "AH" includes both paid and free security apps, including several paid apps from the well know PC security publishers. As with the Gizmo list, all of these recommended apps are available from the Play Store, but some of them have a subscription charge. The first recommended product is McAfee's (now an Intel product) "Security & Power Booster -free", which is free to download and use, but has some features available as in app purchases ranging in price from 99 cents to $29.99 for such services as phone support, media uploads, and for the removal of ads from the product.

Other "AH" recommend Android security apps which offer paid or optional "premium" features include Norton Security and Antivirus, which is free to download, but has a $29.95 charge in order to use the premium features which include enhanced anti-malware protection, privacy protection, and intrusive behavior, as well as the ability to run this Norton product on multiple portable devices. Another free to download security app that has in-app purchases is Kaspersky Internet Security, a Russian product, which can perform basic security scans and other basic security functions on the Android device. In app purchases ranging from $9.99 to $14.95 per item include real-time protection, cloud based protection to protect against the newest threats, web protection, Phishing (identity theft) protection on incoming SMS text messages, and enhanced privacy protection.

Android Headlines (AH) also recommended several of the same free security apps rated and recommended by Gizmo including Lookout Security & Antivirus, Anti-Virus Dr. Web Light, Malwarebytes Anti-Malware, AVG Antivirus Free, avast! Mobile Security & Antivirus, CM Security, and 360 Security Antivirus Boost.

It should be noted that several of the commercial (paid) multi-license PC and MAC security suites also include a license for the paid version of their Android security apps as one of the available licenses. For those who have an Amazon Prime account, the "Amazon Underground" (amazon.com/underground) app store offers totally free downloads of otherwise paid commercial apps, including all in-app purchases become free, if the app is downloaded from Amazon Underground. Two of my family Android devices have the complete, otherwise paid versions of a major security publisher's security app (regularly $14.95 to $29.95), including all of the otherwise paid premium features, running on our devices, which were downloaded for free when the app was listed on Amazon Underground. While this particular security app is not presently listed on Amazon Underground, it has been listed for a limited time several times since we downloaded it; it may be worthwhile to periodically check Amazon Underground listing of newly listed "totally free" apps to see if any more of the otherwise paid commercial apps are available for free.

It is up to you to decide if your Android device needs a security app. While many believe that they are an unnecessary burden, I am of the school that believes in being safe rather than sorry. The choice is yours. 💻

Go to Page 1

Twin Cities
PC USER GROUP

You have just read an issue of The Digital Viking.

Would you like to receive this delivered directly to your email or business each month?

As a member of TC/PC, the Twin Cities Personal Computer Group, one of the benefits is reading this monthly publication at www.tcpc.com..

As a member of TC/PC, you may attend any or all of the monthly Special Interest Group (SIG) meetings and be eligible for software drawings. The small membership fee also includes access to real-live people with answers via our helplines, discounts, and various other perks.

Does membership in this group sound like a good way to increase your computer knowledge?

It's easy to do! Simply fill in the form below and mail it to the address shown.
(If you use the form in this issue, you will receive an extra month for joining now.)

Here's the info for my TC/PC Membership:

Full name____

Company name____

Address____

City___________________________ State________ Zip_________

❍Home ❍Business ❍Change address: ❍Perm. ❍Temp. 'til __________

Home phone__________________ Work phone__________________

Online address(es) ______________________________________

Where did you hear about TC/PC? ____________________________

❍ I DO NOT want any of my information disclosed.
❍ I DO NOT want to receive any mailings

Administrative Use Only Rec'd__________________ Chk#_____________

2/16

I'm signing up for:

❍ Individual/Family Membership ($18)
❍ Business Membership ($100)
If an existing member your # __________

Make checks payable to:

Twin Cities PC User Group
341 County Rd C2 W
Roseville, MN 55113

http://www.tcpc.com

❍ Check #__________ ❍ Bill me
❍ New member ❍ Renewal ❍ Prior member

I'm interested in:

❍ Training classes ❍ Volunteering
❍ Special Interest Groups: New User, Access, etc.
List here:

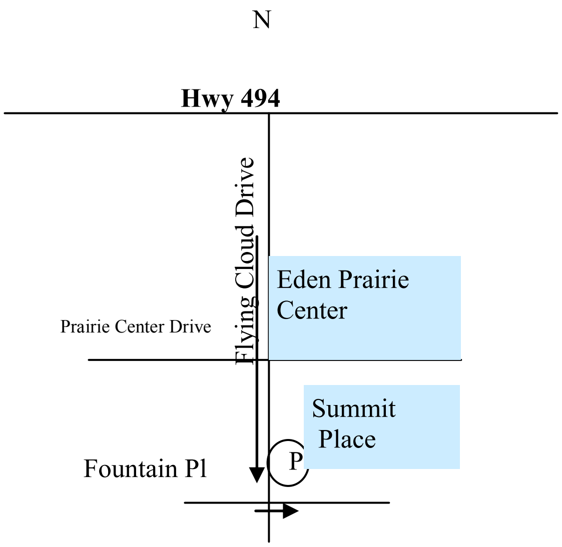
February 9, 2016

General Meeting 7:00 PM

How is your personal data being used ?

How vulnerable are Students and Seniors to Internet data trackers ?

Location: Summit Place
8505 Flying Cloud Drive
Eden Prairie, MN 55344



Twin Cities
PC USER GROUP

341 County Rd C2 W
Roseville, MN 55113

FIRST CLASS MAIL