Interface

Lorain County Computer Users Group
www.LCCUG.com
info@LCCUG.com
Volume 28 Number 1 December 2015

2015

Inside This Issue

Tuesday
January 12, 2016

ANTI-VIRUS / MALWARE / SPYWARE
What you need to know now!

Presented by

Derek Widdowson

Of

Empirical Computers

RAFFLE ITEMS

Infoguard 8 sheet Cross-Cut Shredder
8GB Flash drive
Malwarebytes Software
Container of screen wipes

☺Meeting in Amherst☺

Meetings are held at
The Amherst Church of the Nazarene
210 Cooper Foster Park Rd. Amherst, OH
Doors will open at 5:30 PM, program starts at 6:30 PM

A Word From Our President

A new year is upon us!! Every year brings more and more new technology. I'm sure we'll see things in 2026 that we can't imagine right now. What an exciting time we live in.

We should start the year doing everything we can to have a successful computing year. Derek Widdowson, Owner of Empirical Computers, will be presenting a program on protecting your computer from malware, spyware and viruses. This is basic information that is important for every computer owner. We will all have a much better year if we have our computer protected in these areas.

It is also a good time to remind ourselves not to fall for one of the many scams floating around out there. Some of these will come as a phone call and others could be an email or popup on your computer. Be very suspicious if you get a phone call from anyone saying you owe money or won money. Just don't give out personal information on the phone or fill out forms online. If we initiate the transaction it is another matter. It seems any more it is best to always step back and don't trust anyone who contacts you with an offer, a deal or a threat.

Right now **Tax Scams** are at the top of the list. Followed by:
Debt Collections,
Sweepstakes/Prizes/Gifts
Tech Support
Government Grant
Advanced Fee Loan
Credit Cards
Work from Home
Fake Check/Money Order
Lottery

You can read more about these dangers at:
https://www.bbb.org/top10scams/#sthash.8D5glsk4.dpuf

So be aware and be safe by educating yourself and securing your computer.

One of my New Year's Resolutions is to take advantage of the many online classes there are out there. The winter is a great time to do this when we are inside more. I am updating earlier lists that I had assembled of where to find these kinds of opportunities. Many of them are available through the libraries and a large number of those being offered will expand your computer skills. You will also find great classes, webinars and tutorials on everything imaginable.

Here is one such master list:
http://www.openculture.com/freeonlinecourses

There you will find links to online college courses, online certificate programs, business courses and free online learning of all kind. You can learn about everything from an introduction to a foreign language, a math review, how to use digital pictures, look up your family history, gardening, sewing, science, music and on and on. Many local libraries offer free high-quality courses and career training programs online for their library's card holders.

LCCUG Officers For 2014

President	Sandee Ruth president@lccug.com
Vice President	Carole Doerr vicepresident@lccug.com
Secretary	Don Hall secretary@lccug.com
Treasurer	Micky Knickman treasurer@lccug.com
Newsletter Editor	Pam Rihel newsletter@lccug.com
Web Page Editor	Richard Barnett webpage@lccug.com
Statutory Agent	Sandra Ruth statutory_agent@lccug.com
Director of Membership	Dennis Smith membership@lccug.com
Director of Advertising	Richard Barnett advertising@lccug.com
Director of Public Relations	**Open**

Khan Academy (https://www.khanacademy.org/) allows you to take control of your **learning** by working on the skills you choose at your own pace with their free **online** courses. These include math, science, computer programming, history, art, economics, and much more. These are great for students and adult learners alike.

And then there is always Youtube.com. You can find a video there on doing just about anything imaginable! Take advantage.

Another learning opportunity will be an APCUG conference that is being planned for outside Columbus October 21-23 this year. More information on this event as available.

We have NO excuses! What a great time to be a learner. The world is ours from anywhere if we have a computer and an internet connection.

Let's start the year together at our first meeting of the year on January 12 when we will learn to secure our computers.

Sandee Ruth
LCCUG President

Tuesday
January 12, 2016

Presented by

Derek Widdowson
Of
Empirical Computers

To the average home computer user, a virus can be very damaging in terms of personal data loss: the complete loss of family photos, resumes, your children's school work and other valuable items is a large price to pay if you're not protected. With several basic antivirus programs available for free and "good" products and programs typically averaging about $30 a year, there is no excuse to go unprotected. Having virus protection is important, of course, but just as important as the virus protection itself, is keeping that program or application updated.

Please join us as Mr. Derek Widdowson, Owner of Empirical Computes and one of our newest sponsors, explains to us the many different aspects of virus protection. Derek will not only discuss virus protection, but also protection against Malware, spyware, ransomware and other nasty computer programs. Please join us for what promises to be a very informative and useful presentation.

L C C U G

MEETING CANCELLATION NOTICE

When a meeting is cancelled, the notification will be on our Websites and emails will be sent out to our members.

Our Websites are: **www.lccug.com**
www.lccug.com/members

If you think the weather is too bad to drive in then don't try to come to a meeting that may already be cancelled. Please check your email boxes and our websites.

Thank You

Attention! Attention! Attention!

Now you can get a 5 year membership subscription to LCCUG for only $75.00.

This is a savings of $50.00. Can't beat this price.

So talk to Micky Knickman our Treasurer and get started on your 5 year membership today.

Don't wait until this great offer disappears. Sign-up today...

Executive Board Meeting Minutes

DECEMBER 1, 2015

The board meeting was attended by Sandee Ruth, Don Hall, Micky Knickman, Pam Rihel, Richard Barnett, Dennis Smith, Carole Doerr and Neil Higgins.

The board discussed possible programs for the coming year along with possible field trips on non-meeting days. We have tentative programs thru this coming June.

Sandee renewed our membership in APCUG for the coming year.

Neil Higgins and Carole Doerr will be added to the proposed slate of officers in the December election.

Responsibilities for the December Christmas meeting were assigned.

The January board meeting will be held on Google Hangout.

Dennis moved, Micky seconded the meeting be adjourned.

General Meeting Minutes

DECEMBER, 2015

President Sandee Ruth called the meeting to order. Sandee proceeded to read the proposed slate of officers for the coming year and asked if there were any nominations from the floor. There were no nominations so Sandee moved the existing slate be approved by unanimous ballot, motion approved.

Sandee read a letter from the widow of recently departed loyal LCCUG member Enio Fernandez telling how much he enjoyed the friendships made with club members.

The Annual Holiday Party began with members enjoying all the delicious food supplied by members.

Members were very generous in their purchasing ticket for the raffle which raised $129 for the Church of the Nazarene Food Bank.

Dennis Smith moved, Pam seconded the meeting be adjourned.

Newsletter Editor: Pam Rihel using Microsoft Publisher, Corel Paint Shop Pro X3, CreataCard 8.

This Month's contributors: Micky Knickman, Sandra Ruth, Pam Rihel, Don Hall, Dennis Smith, Dick Eastman, Ira Wilsker, Larry McJunkin, Steve Costello, Bill Sheff, Scambusters, Ask Leo, http://www.familytreequotes.com/categories/Family-Tree-humor/

Microsoft Office art online,
Newsletter is now
Online at
lccug.com/newsletters or **lccug.com**

LCCUG Members Page

Don't forget to check the Members' page for up-to-date information about programs & events:

http://www.lccug.com/members

Pam Rihel prihel1947@gmail.com

Dick Eastman http://www.eogn.com

Don't Use QR Codes on Tombstones!

I had an experience a while ago that got me thinking about today's tombstone technology and what it might be like in the future. A company that shall remain nameless asked that I write about the company's product: long-lasting display plates containing QR codes. The company's products can be attached by adhesive, either to a tombstone (which I am strongly against) or to an urn, marker, or other nearby object that can be inserted into the ground near the tombstone. (I can live with that second idea.)

NOTE: For an explanation of QR codes, see https://en.wikipedia.org/wiki/QR_code.

The second part of the company's product occurs when a future visitor to a cemetery uses a QR code reader in an Apple iPhone, Android phone, or similar mobile device to read the QR code. That person would use the device's wireless Wi-Fi or cellular data Internet connection to display an associated web page that is stored on a web server someplace. This product requires the QR code to point to the dedicated web page on the company's web server. Each QR code points to a different page on the server, and each page contains information supplied by the family that purchased the QR code display plate. That tribute page could either display information directly or redirect the visitor to another web site, such as a charity of the family's choice or a family tree posted on some other web site.

At first, this sounds like a good idea; but, then I wondered, "What happens if the company goes out of business and their web site goes offline?" I assume the answer is that the customer has wasted the money he or she spent. While I hope this company remains in business for a long, long time, I still don't like the idea of depending upon any one corporation's future success.

The discussion I had with a company rep revolved around a possible endorsement of the product from me. In return, the company would offer a discount to readers of this newsletter.

I declined the company's offer, and I will explain why I am not offering discounts on this product to newsletter readers. The bottom line is that I don't approve of this product as it presently exists. However, I will also offer explanations and describe three of my concerns. I will say that minor product changes could quickly remove my objections. However, I think I have an even better idea, which I will also describe.

In fact, I believe there is a better technology that can achieve the same results without the use of adhesives or any other method of defacing the tombstone.

First, there is the concept of attaching a QR code (or any other foreign object) directly to a tombstone. I am against that for a variety of reasons. When discussing historic tombstones, most tombstone scholars would be aghast at the idea of using adhesives or any other means to attach a new object to an existing tombstone.

NOTE: Adhesives are commonly used to repair broken tombstones. However, only certain types of adhesive are used because an improper chemical mix in the adhesive can actually accelerate the tombstone's decay. Some adhesives also expand or contract with changes in temperature. That would hasten the destruction of the tombstone—the exact opposite of what was planned.

If you are thinking of using an adhesive of any sort on any tombstone for any purpose, please first consult with an expert who knows what to use and especially what not to use! Even then, adhesives are normally only used to restore a tombstone as closely as possible to its original condition, not to add new attachments.

I do think the use of a nearby "marker" of some sort is a good idea, however. In many cemeteries we already see in-ground markers or flags placed by veterans' organizations, fraternal organizations, the Daughters of the American Revolution, church groups, and others. These nearby markers are subject to occasional theft or lawnmower damage, but most of them seem to remain in place for decades. If the item deteriorates or is stolen, it is easily replaced without damaging anything else. These markers make me think that a **SEPARATE** marker containing a QR code could be used in any cemeteries that allow separate markers.

Acceptable use of a QR code

My second objection revolves around the question, "What web page or URL should the QR code point to?" I would never purchase a QR code marker that points to a corporation's web site, even if that site then redirects the web browser elsewhere. The QR code should not be dependent upon the lifetime of any corporation.

I would prefer to have the QR code point directly to a web site of my choice, preferably to a web page that I own or control and a web site that I

(Continued on page 6)

(Continued from page 5) Dick Eastman

can pass on to one or more younger family members who can make sure it lasts until QR codes are replaced by some newer technology. To be sure, even pointing to one of my own web sites is an imperfect idea; but, at least it remains under my direct control. I like that better than depending upon some corporation where I have no control at all. If I have direct control and want to change the web page later, I can do so.

My third objection concerns technical longevity. While QR codes are a great solution today, I doubt if my grandchildren or great-grandchildren will use them. I'm reminded of the old proverb, "This too shall pass." That's another reason against permanently attaching anything to a tombstone: if the technology becomes obsolete, the tombstone is left with a permanently-attached memorial of someone's failed use of the technology of that time. That would be embarrassing, even if the person who attached the foreign object has long since departed this world.

If a QR code becomes no longer relevant, a surviving family member could visit the grave and replace the QR code with something more useful. Of course, that can happen only if the QR code is **NOT** attached to the tombstone with some sort of permanent adhesive.

A Better Solution

In fact, I think I see a better technological solution on the horizon, a solution that is non-destructive and doesn't require any attachments. It also doesn't require an in-person visit to the cemetery by future "visitors." It even solves the "problem" I have because all of my ancestors' tombstones are buried in the snow for about four or five months every year. You may or may not have the same "problem."

Tombstone experts have always questioned the practice of using any sort of adhesive to attach anything to a tombstone. Today's smartphones have cameras and internal GPS receivers that make QR codes obsolete by replacing them with the one thing that never changes: latitude and longitude. In fact, future descendants and others can obtain the gravesite information without even visiting the cemetery, unlike a "solution" that requires an in-person visit to view and use QR codes.

Tombstone apps

for BillionGraves.com and FindAGrave.com already provide cemetery visitors the power to easily find genealogical information about a deceased individual without the use of QR codes or other displays at the grave site. This is done when one volunteer visits the cemetery and snaps a quick photo of a particular gravesite's monument from the app's interface. (I assume the volunteer is not snapping pictures when snow obscures the information.) The photo normally includes longitude and latitude information embedded in the photo's metadata, supplied by the mobile device's internal GPS. That photo and its embedded information can then be uploaded to BillionGraves.com, FindAGrave.com, MyHeritage.com, FamilySearch.org, Ancestry.com, WeRelate.org, a personal web page devoted to a deceased relative's memory, or to any of hundreds of other web sites. In fact, it can be uploaded to ALL of those sites and even more, should the photographer wish to do so. As part of the upload, still more textual information can be added beyond the embedded metadata. This might include the exact location of the tombstone, complete with a picture, a transcription of the tombstone's text, instructions on how to find the cemetery, and any other information as well as web link(s) the uploader wishes.

If enough people start using longitude and latitude information, I am sure dozens of similar apps will appear in the future. I also know of only one web site today that encourages the use of longitude and latitude information for tombstones: BillionGraves.com. FindAGrave.com also accepts latitude and longitude information but doesn't require it. Many of the tombstones listed on FindAGrave.com do not have geographic coordinates listed. This could change quickly; if customers were to start asking for the capability to **AUTOMATICALLY** record the coordinates already stored in a smartphone at the moment a picture is taken, I bet dozens of web sites would soon add new search capabilities.

A smartphone or any desktop or laptop computer could then access the online photo and its included metadata. Any app COULD (in the future) instantly recognize the exact tombstone in question and then display all known information about the stone and the person it commemorates. If the first page were to contain links to the individual's information stored on other web sites, such as on BillionGraves.com, FindAGrave.com, MyHeritage.com, FamilySearch.org, or others, the person viewing the information could easily click to visit those additional sources of information.

Once the longitude and latitude information is automatically extracted from each picture's metadata, I would envision the possibility of also clicking on an option that says, "Display nearby tombstones" or something similar. That would simplify the search for possible relatives of the first person, even in the largest of cemeteries. Today you can find lots of web sites that list a cemetery's tombstones alphabetically, but very few of them will provide a listing of nearby tombstones. However, that capability would be simple to add if all tombstones' longitude and latitude information were included as searchable database fields. That information already is embedded in most iPhone and Android photos and can be added to photos taken by a number of other cameras as well.

Theoretically, this information also could be added manually, but I wouldn't want to do that to hundreds of photos at a time. That would be a tedious task! It's much better to let technology perform mundane tasks for us. Let's use cameras that embed that information for us automatically. Most of today's smartphone cameras already do that anyway.

This technology should work when the information seeker is in the cemetery as well as when at home or at other locations. If used while in a cemetery, the process is simple. Since today's smartphones usually include a GPS, an app written for that smartphone or tablet computer could easily determine where you are located and then show you information about nearby tombstones, more information than what is engraved on each stone. If you are at home or elsewhere when you use the app, you would have to enter the name or the latitude and longitude of each cemetery of interest. Perhaps the app would also automatically look up the cemetery's name as well as its latitude and longitude.

(Continued on page 7)

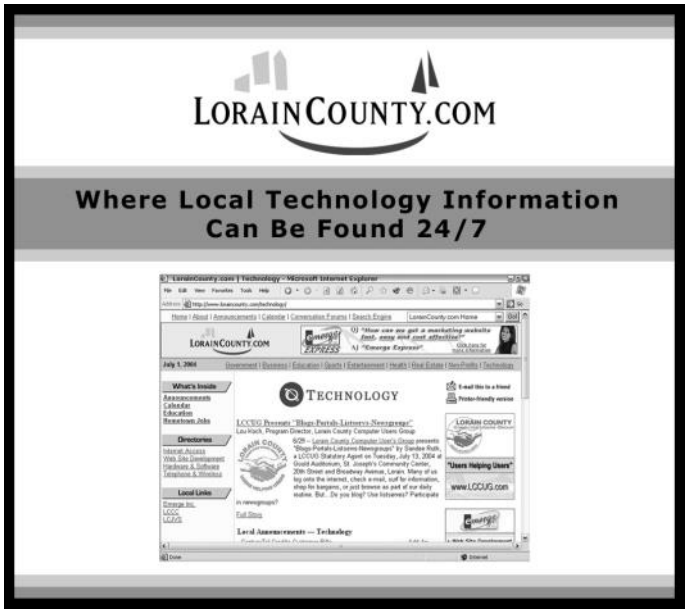
(Continued from page 6) Dick Eastman
The result should be nearly instant identification of any recorded tombstone from any location in the world, accompanied by all known information about the person buried there. That will even work in mid-winter as a personal visit should not be required. All of this can be done without attaching any foreign devices or adhesives to the tombstone.

I would love to go to a web site and say, "Show me all the tombstones containing the word 'Eastman' in the Pine Grove Cemetery in Bangor, Maine, plus all tombstones located within twenty feet of an Eastman tombstone." The required technology is already available today. All we need is customer demand to encourage the programmers.

In summary, I doubt if any technology will last more than ten or twenty years. While QR codes are a great solution today, I doubt if my grandchildren or great-grandchildren will use them. I am sure an even better technology of some sort will eventually replace QR codes. I wouldn't mind adding a QR code to a small marker that is nearby, but not attached to, a tombstone. However, let's recognize that this would still be a short-term solution. (When talking about tombstones, "short term" means ten or twenty years.)

I will suggest that the use of latitude and longitude will probably never change and is also non-destructive to the memorials. Even if latitude and longitude were to drop out of favor at some future date, a web site containing that information could easily be converted to use whatever new location identification methods become popular in the future. Using latitude and longitude also allows for searches for information without a personal visit to a (distant) cemetery. I doubt if the use of longitude and latitude will be perfect forever, but it sure sounds good to me for use in the next few decades.

When documenting the past, let's also look to the future to make sure information will always be available as easily as possible, limited only by our abilities to predict future technologies. And let's make sure we don't deface any tombstones!



ScamBusters.org

Could School Information Lead to Children's Identity Theft?

By Keith

Warning signs of ID theft and actions you can take to protect and inspect your child's school information: Internet Scambusters #682

Carelessly guarded school information could provide a route for crooks to steal identity information about your children. But there's a law that enables you to inspect that info and opt out of it being shared with third parties, as we explain in this week's issue.

We also have an urgent alert about a new scam that aims to steal your bank information by inviting you to participate in a bogus store quality-control program.

Every time you fill in a form or provide school information about your children, you're putting them at risk of identity theft.

It's a shocking thought, isn't it? And of course, most schools have tough security rules in place to protect data about their students.

But, in an age where hacking and other forms of data theft has become commonplace, it's important to think about protecting your children's information. Because, chances are that they won't!

According to a 2012 survey*, 1 in 40 U.S. families with children under age 18 had at least one child whose personal information had been compromised.

(*Identity Theft Assistance Center and Javelin Strategy & Research Group)

As we've previously reported in Identity Theft Update: Kids, Students and Medical Services Are Key Targets for 2010, thieves mostly target children's Social Security numbers because youngsters don't have credit histories, so they haven't been flagged for any problems with the credit scoring agencies.

The crooks use the SSN, changing date of birth details to make credit and loan applications and for other criminal purposes.

In some cases, according to the study referred to above, the misuse of these numbers can go on undetected for years and can take even longer to repair.

The Federal Trade Commission (FTC) recently warned parents about the dangers of giving away too much information about their children when they fill in forms for things like school directories, scholarships, sports teams, scouts, and so on.

(Continued on page 8)

(Continued from page 7) Could School Lead to Identity Theft.

Parents also should not carry their children's Social Security card or give out the number to anyone unless absolutely necessary.

But how do you know what information a school is storing about your children (or other kids in your family) and what's being done to protect it?

Most parents and guardians may not be aware of the provisions of a law known as the Federal Educational Rights and Privacy Act (FERPA), which is intended to protect the privacy of student records.

Under FERPA, schools must notify parents and guardians about their policy on school directories and give them the right to opt out of releasing directory information about their children to third parties.
The law also:

- Forbids improper disclosure of personally identifiable information derived from education records.
- Allows parents (or students aged 18 or over) to inspect and review education records and to provide a copy of them if required.
- Provides the right to have records amended.

However, it's important to know that FERPA only covers publicly funded schools. Private schools are not included.

There are also a lot of exclusions and exceptions even within the law, so it's worthwhile getting acquainted with its provisions.

There's a fairly readable summary, which also details the complaints process.

But of course, it's not just the information you provide to schools that puts children's identities at risk of theft.

Most kids today are walking around the schoolyard with a veritable mine of information about themselves stored on mobile devices.

So it's vital that parents teach children both to limit the information they share online and to protect their smartphones and tablets with passwords that they absolutely must not share.

If you have college students in the family, consider giving them a crosscut shredder for their room, especially if they're in a shared accommodation, encouraging them to shred all documents including credit card offers.

Indeed, shredding should be a must on the list of everyone who wants to protect their identity against theft.

See this useful Scambusters issue on that subject: Shredding: A Key Weapon in Your Document Security and Identity Theft Prevention Strategies.

The FTC lists three key warning signs that someone might be misusing personal information about your children:

1. An application for government benefits is rejected because someone using your child's name is already receiving them.
2. The IRS notifies your child that they haven't paid any income tax or that their SSN has been used on another tax return.
3. You receive bills addressed to your child for products you or they didn't order or receive.

Apart from monitoring the use of personal information at school, the other key action you can take is to regularly check for a credit report in your children's names.

You can find details of how to do this and much more about protecting your children's identities in this downloadable guide.

The message is clear: your children are just as vulnerable to identity theft as you are, so think twice and be sure it's essential every time you're asked to provide school information or details about them to any other organization.

Alert of the week: Watch out for a scam letter pretending to be from Walmart saying you've been selected for their Quality Control Program.

The phony letter is accompanied by a check you're supposed to "activate" online before depositing it into your bank account.

But the supposed activation requires you to enter details of your bank account and — bingo! — the crooks have the info they need to drain your account, including the notional value of the bogus check you deposited before it's identified as a fake.

Meanwhile, you might also be in Walmart spending some of that money you don't really have, money that your bank will eventually demand back.

More Security Vulnerabilities Disclosed for Phones, Carriers

Ira Wilsker, *Assoc. Professor, Lamar Institute of Technology; technology columnist for The Examiner newspaper www.theexaminer.com; deputy sheriff who specializes in cybercrime, and has lectured internationally in computer crime and security.*

If you are like me, I carry my cell phone everywhere, carrying on voice conversations, sending and receiving text messages, utilizing countless apps, and surfing the Web. Until recently, I gave very little heed to the security of these external communications as our smart devices are supposed to be somewhat secure. GSM carriers like AT&T and T-Mobile utilize encryption to make communications secure; CDMA carriers like Sprint and Verizon also claim to have secure networks. Yes, I do have a major security app on my Android phone that scans new apps and text messages for malware, as well as protects from hazardous websites. Google created Android to be secure, with apps running in a somewhat closed memory space, called by some a "sandbox," which is supposed to prevent purloined apps from talking over the phone. IPhone fanatics, along with many Apple fans in general, believe that their devices are immune to attack, as Apple would not dare to allow any threats to harm their beloved devices.

Now welcome to the world of stark reality. In a recent column, I wrote about two newly revealed vulnerabilities, known as "Stagefright" and "Certifi-gate," that may threaten the security, safety and privacy of nearly a billion smart phones and tablets. Since then, others have come forward demonstrating previously unannounced security vulnerabilities that threaten the security of our smart phones, often including both iPhones and Android devices in their threat assessments.

One of these newly disclosed threats explicitly targets the most technology innocent and uninformed among us. Appropriately called "grandma malware," this clever piece of malware sneaks onto Granny's phone using a compound method of infection designed to defeat many of the simplest security precautions. While recently updated Web browsers and desktop security software, as well as updated phone operating systems, have likely patched the vulnerabilities, Granny's often older and unpatched computer and phone may be vulnerable. The first step in the infection sequence occurs when the victim downloads an innocent looking app, often a game or simple photo utility, onto their computer using any one of the older versions of most of the common Internet browsers, which are still in wide use. This small utility, explicitly designed to appeal to a "grandma," does not itself contain any malware, and will pass the scrutiny of many of the less sophisticated desktop security products. This utility sits quietly and apparently innocently on the victim's computer, often performing its intended tasks. The app surreptitiously monitors Web surfing until Granny logs on to an app store, such as the Google Play Store. The malicious utility captures the logon and connection information from the app store; with this information, the malware is invisibly downloaded wirelessly to the smart device, installing itself on Granny's phone. Once installed, this malicious app immediately gathers personal data from the phone and sends it to parties unknown. Even if this malware is detected and removed in a subsequent security scan by a third party security utility, it is too late; all of the personal information was stolen within seconds of the app being installed on granny's phone. Granny's private information has just been stolen, and she might very well become an identity theft victim; as is common in criminal enterprises, the most vulnerable among us are more likely to be victimized.

Despite the travesty of purposely going after Granny, it is not one of the most insidious of the newly announced threats imperiling our smart phone usage. In recent days, a pair of IBM cyber security analysts, Or Peles and Roee Hay, uncovered a flaw in the Android operating system still being used in over a half-billion Android smart phones. This vulnerability, not yet formally named but referred to as a type of "masque" attack, could allow hackers to take over and remotely control vulnerable Android phones. According to these researchers, "Masque attacks are defined as malicious apps uploaded, say, from e-mails directing victims to fake Web links." According to Peles and Roee, Google has issued patches for devices running Android 5.1, 5.0, 4.4, and Android M, but as often the case for many Android devices (except some Nexus phones), it is up to the phone manufacturer or cell phone carrier to push these patches to their users, meaning that although the patches are available, over half of Android phones do not yet have the patches installed.

This "masque" attack vulnerability allows hackers to control the security privileges that are a part of the Android operating system, allowing compromised or counterfeit apps to access information on the phone that would otherwise be unavailable to the hacker. According to the researchers, this vulnerability allows the data thieves to steal personal information, capture banking information including logins and passwords, access the phone's cameras, download contact lists, and pilfer stored files and e-mails, sending the stolen information to a remote server. While this particular Android vulnerability was recently discovered by IBM cyber security experts, it is very similar to one discovered several months ago by FireEye that explicitly targets Apple's iPhones. The mechanism and modus operandi, as well as the data thefts, are almost identical between the Android and iPhone vulnerabilities.

A "masque" attack can occur when smart phone users download any of 11 authentic looking but counterfeit or contaminated apps that also appear to work properly

(Continued on page 11)

NEED HELP?

Here's Who to Contact:

Neil Higgins
440-967-9061 - higgins.neil@gmail.com
Evenings 6 p.m. -10 p.m. + Weekends
Hardware, Linux & Windows Operating Systems, Tweaking your system

Micky Knickman
440-967-3118 - micky@knickman.com
Evenings 4:00 pm to 6:00 pm + Weekends
General Software Configuration, Hardware Installation, Basic to Advanced Windows

Richard Barnett
440-365-9442 - Richard216@aol.com
Evenings & Weekends
General Software Configuration, Hardware Installation, Basic to Advanced Windows & Web Page Design

Sandee Ruth
440-984-2692 - sandee29@gmail.com
Basic Word Processing, Windows, & Web Design
Advanced Internet

Pam Casper Rihel
440-277-6076
6:00 p.m. to 10:00 pm Monday thru Thursday
Genealogy help
prihel1947@gmail.com

If any of our members are interested in helping other users with what programs you are adept at, please contact any of our officers with you name, what program or programs you would be willing to give help with, you email address and or phone number and when you would like to have them call you. Thanks

LCCUG Ongoing Workshop

All Are Free And Open To The Public

Problem Solving Workshop

Date: Tuesday - January 19, 2016
Time: 5:30 - 8 pm **Instructor: Micky Knickman & Richard Barnett**
Place: Amherst Church of the Nazarene
210 Cooper Foster Park Rd.,44001

Learn how to repair or update your computer by changing hard drives, memory, CD ROMs, etc.

Members are encouraged to bring their computers anytime before 7:30 pm for assistance from Micky & Richard.

Learning About Electronics

Date: Tuesday - January 19, 2016
Time: 5:30 - 8 pm **Instructor: Sandee Ruth**
Place: Amherst Church of the Nazarene
210 Cooper Foster Park Rd.,44001

Learn how use you electronic devices.

Members are encouraged to bring their tablets, iPod, kindles, etc. at 5:30 pm for assistance from Sandee and any other knowledgeable members. Public is welcome to sit in these classes.

Learning About Raspberry Pi

Date: Tuesday - January 19, 2016
Time: 5:30 - 8 pm **Instructor: Neil Higgins**
Place: Amherst Church of the Nazarene
210 Cooper Foster Park Rd.,44001

Neil will assemble one of these new inexpensive "Raspberry Pi" computers. If you want to participate in that and get copies of the material he is assembling, please let him know you are coming (higgins.neil@gmail.com).

Computer Club News

Don't Forget to Bring in Your Used Ink Cartridges

LCCUG is collecting empty ink cartridges.

Our Club is recycling used ink cartridges and using the rewards we earn to buy more prizes for the club raffle.

If you have empty ink cartridges laying around, please bring them to our meetings and any officer will gladly take them off your hands. ***Recycle & Help Our Club, Too!***

The Lorain County Chapter of OGS

is having it's next meetings on :

January 11 - "How to Prepare a Lineage Application" Margaret Cheney will discuss the basic information, documentation, and organization needed to successfully complete an application to any Lineage Society.

February 8 - "Researching Your Italian Ancestors" - Tom Cinincione, President of Cleveland Italian American Organization (CIAO) will discuss the resources available to research Italian ancestors.

REGULAR MEETING LOCATION
North Ridgeville Library, 35700 Bainbridge Rd. North Ridgeville, Ohio. Meetings are free and open to the public. Social time is at 6:30 PM and the program begins at 7:00 PM.

Jean Copeland: **jecopeland1975@gmail.com**. or
Pete Hritsko: **hritsko@centurytel.net**

More About Raspberry Pi:

The Raspberry Pi is a low cost, credit-card sized computer that plugs into a computer monitor or TV, and uses a standard keyboard and mouse. It is a capable little device that enables people of all ages to explore computing, and to learn how to program in languages like Scratch and Python. It's capable of doing everything you'd expect a desktop computer to do, from browsing the internet and playing high-definition video, to making spreadsheets, word-processing, and playing games.

Genealogy Insights:

We've uncovered some embarrassing ancestors in the not-too-distant past.
Some horse thieves, and some people killed on Saturday nights. One of my relatives, unfortunately, was even in the newspaper business.
Jimmy Carter

Some family trees have beautiful leaves, and some have just a bunch of nuts.

Remember, it is the nuts that make the tree worth shaking.
~Author Unknown

Families are like fudge... mostly sweet with a few nuts.
~Author Unknown

(Continued from page 9) More Securities Vulnerabilities...

when downloaded and installed. Among the most commonly downloaded iPhone and Android apps that enable this vulnerability are modified copies of Facebook, Twitter and WhatsApp. According to FireEye, iPhones are as vulnerable to these masque attacks as Android devices. According to Zhaofeng Chen, a senior research engineer and scientist at FireEye, the 10 tainted apps that most threaten Apple devices are "WhatsApp, Twitter, Facebook, Facebook Messenger, Google Chrome, Blackberry Messenger, Skype, WeChat, Viber, Telegram and VK." These apps are often downloaded from genuine-appearing links in e-mails or SMS text messages, and mimic the functionality of the genuine app, but allow for the remote access to this valuable personal content. FireEye was quoted as stating that this iPhone vulnerability can steal or access a variety of information from compromised phones. Among the dastardly deeds that this masque vulnerability can perform include recording and forwarding phone calls placed on Skype, Wechat and other voice apps; intercept text and SMS messages from iMessage, WhatsApp, Facebook Messenger, Skype and other SMS apps; send real-time and historical GPS locations; access website histories; steal contact information and lists; and download photos from the phone. Apple has created patches and upgrades closing this vulnerability, and pushed these patches to many of its users, but there are inevitably iOS device users who have not received or installed these patches.

In recent days, on the Australian version of the "60 Minutes" news magazine, another cell phone vulnerability was demonstrated where hackers in Germany were easily able to listen in on a cell phone chat between individuals in Australia and the UK. This ability to readily capture live calls is known as the "SS7 Vulnerability." SS7 technology is widely used, legitimate and necessary for cell phone carriers to properly direct calls and text messages to their intended recipients. ComputerWeekly.com said, "Like any protocol, SS7 is vulnerable to exploitation by sophisticated and well-funded third parties with criminal intentions." In another ComputerWeekly.com story titled "Security flaw exposes billions of mobile phone users to eavesdropping," the online magazine says, "Hackers, fraudsters, rogue governments and unscrupulous commercial operators are exploiting flaws in the architecture of the mobile phone signaling system known as SS7. ... Billions of mobile phone users around the world are at risk from covert theft of data, interception of their voice calls and tracking of their location." SS7 is not a vulnerability in the phones themselves, as the vulnerability is not brand or operating system dependent, impacting Android, iPhone, Blackberry and other systems equally, but is in reality a vulnerability in the switching system utilized by the cell carriers themselves.

For those of us who routinely use Android, iOS or Blackberry devices without much thought about the inherent security vulnerabilities of the phones and cellular carriers, keep at least a spark of consideration in mind. While I am fully cognizant of the risks, I will continue to use my smart devices pretty much as I have in the past.

Siri for Seniors (or Anyone)

By Larry McJunkin, The Retired Geek
http://retiredgeek.net/2015/06/03/siri-for-seniors-or-anyone/

If you have an iPhone 4s or later, iPad with Retina display, iPad mini, or iPod touch (5th generation), meet your new best digital friend – Siri. You've probably been ignoring Siri a lot simply because you may not be comfortable using it. But if you'll just talk to Siri as you would a friend, you'll be amazed how much it will help you during your day. Let's take a look at some of the most helpful things you can do.

Things like sending messages, reading email, placing calls, setting reminders (very important for those of us with short memories) or even finding a restaurant or making dinner reservations. You can ask Siri to show you the Orion constellation or even how to flip a coin. Siri works hands-free, so you can ask it to show you the best route home and what your ETA is while driving. And it's connected to the world, working with Wikipedia, Yelp, Rotten Tomatoes (movie reviews), Shazam (song & artist recognition), and many other online services to help you find even more answers. The more you use Siri, the more you'll realize just how great it is. And just how much it can do for you.

How to Use Siri

Press and hold the HOME button on your iOS device until you see "What can I help you with?" accompanied by a double-beep tone. Then, in a normal speaking voice tell Siri your command. Wait for Siri to respond to your request and display it. If you're driving, don't try to read it, but reply to Siri again, saying "I can't read it". Then Siri will read back your command for verification, which is very helpful with texts or emails, especially while driving.

Set Reminders, Alarms, Add to Your Calendar & More

– "Set the timer for 10 minutes"
– "Stop the timer"
– "Reset the timer"
– "Pause the timer"
– "What time is it?"
– "What is the date?"
– "Wake me in 30 minutes" (one of my favorites for a power nap)
– "Remind me at 8am tomorrow morning to put out trash"
– "Remind me to record American Idol at 8pm"
– "Remind me to call Jack next Friday"
– "Set up a tee time for next Friday at 9am"
– "Add Yoga to my calendar for next Monday at 10am"

Location Based Reminders (Location must be enabled in Settings)

– "Remind me when I arrive home to defrost the turkey"
– "Remind me when I arrive here to buy gas" (use "here" as the "place" at which you want to do something)
– "Remind me when I arrive in Knoxville Tennessee to call Sam"

Read and Send Emails or Texts (Use actual "First Last" names from your Contacts)

– "Read my emails" (Siri will read aloud the time the email was sent, sender's name and subject)
– "Send an email to James Brown" (Siri will then ask you "what would you like to say to James Brown"?
– "Email Bob and say I cannot play golf this weekend"
– "Send a message to Dave on his mobile and tell him I'll be 10 minutes late" (assumes Dave has a mobile phone in his contact)
– "Read my most recent email message"
– "Read my new text messages"
– "Text Brenda See you soon smiley exclamation point"

Create Notes

– "Note, the grandkids will be here the last week in July"
– "Create a shopping list note" (substitute any name for your list)
– "Add bread, milk, and salami to the shopping list note"
– "Find the shopping list note" (Siri will display your shopping list note)

Some Other Things You Can Ask/Tell Siri (Use your imagination for more…Siri will likely know the answer)

– "What movies are playing today at the Regal Cinema in Knoxville?"
– "What is the temperature?"
– "What is the current weather in Kansas City?"
– "What is the forecast for tonight?"
– "Search for Italian recipes that use bowtie pasta"
– "Find a table for four tonight in Dallas Texas"
– "What time does the sun set tonight in Paris tomorrow?"
– "What are names of the band members in Three Dog Night?"
– "Did the Tennessee Vols win last night?" (I sure hope they did!"
– "Are there any Mexican restaurants near me?"
– "Where's a good Indian place around here?" (Siri understand slang and will assume you mean an Indian restaurant)
– "How many cups are in a gallon?"
– "Who starred in the movie Gravity"

Special Tip

Here's a really helpful Siri tip you can apply in any way you want, to any contact.

– Tell Siri "Brenda Smith is my wife".

This explains to Siri how people in your contacts are related to you, like your mom, dad, or wife, and it will know who you're referring to the next time you ask Siri to contact someone. Then just tell Siri to "Call my wife".

Siri is nothing more than artificial intelligence, maximized in a way to help you with obtaining answers, finding tips and tricks, locating entertainment, staying organized, staying in touch, keeping up with your favorite sports teams, and much, much more. Experiment by simply asking Siri any question that comes to mind and you'll quickly realize just how helpful it is.

Ask Leo! by Leo Notenboom

How Long Should I Keep Backups?

I can't tell you how long you should keep backups, but I can give you some guidelines and examples of the implications of your choice.

In your books you suggest that we keep backups for 2 months, as an example. I feel very comfortable keeping no more than 3 days. Is there any drawback in using such a short time, or is it OK?

Ultimately, this is an unanswerable question in a general sense. By that, I mean three days might be enough… or it might not.

It actually depends on a number of factors that range from your comfort level to your risk tolerance, as well as your personal back-up scheme.

To understand how long you might want to keep backups, we'll want to look at those risks.

When in doubt
If you don't want to put a lot of thought into it, I would absolutely fall back to my two-month recommendation. In slightly more detail, that means:

Without knowing more about your requirements, this represents a balance between recoverability – anything in the last two months can be recovered – and disk space – only two months' worth need be kept.

It's also what I do.
Implications of how long you keep backups.

The key to understanding how long you want to keep backups is to understand exactly what happens after whatever time period you choose passes.

In your proposal, exactly what happens after three days? What's lost?

Think of each backup as a representation of your computer "as it was" when the backup was taken. As a result:

- Yesterday's backup: everything on your machine as it was yesterday.
- The day before yesterday's backup: your machine as it was two days ago.

The day before that: your machine as it was three days ago.

Your machine as it was four days ago? Well, if you only keep backups for three days, then that backup was deleted to make space. Older versions of anything that changed in the three day window will be lost.

Let's look at some examples of what that implies.

Malware
Let's say your machine becomes infected with malware. As I've stated many times, restoring to a recent backup taken prior to the malware's arrival is probably the fastest and most reliable way to completely remove it.

Ideally, you would notice quickly, and restore the previous day's backup.

But… what happens if you fail to notice for, say, a week? Perhaps you don't use your computer for a while. Maybe it takes a week to figure out that the odd behavior you're experiencing is, indeed, malware.

With only three days of backups, all you have is a back-up of your machine as it was three days ago – *after* the malware arrived. That backup – in fact, all three back-ups you have – are infected. You no longer have a clean backup you can restore to.

Accidental deletion
Accidents happen, and sometimes we change our minds.
Let's say on Monday you delete a file you believe you no longer need. You're done with it, or so you think.

Then, later that week – perhaps Friday – you suddenly realize that not only were you not done with it, but it turns out to be critical.

With three backups, you have backups of your machine "as it was" on Thursday, on Wednesday, and on Tuesday. But not on Monday. As a result, you no longer have a back-up copy of the file you deleted: it's gone.

(Continued on page 14)

(Continued from page 13) **How Long Should I Keep My Back-ups?**

File corruption
Either software or hardware can fail in such a way that a perfectly good file can be damaged so it can no longer be opened or used. The file may be present, but it contents are so much garbage.

As above, let's say on Monday your computer experiences an unexpected power loss, and shuts down without warning.

Come Friday, you suddenly realize that a file you rely on to perform some end-of-week processing every Friday can no longer be opened – the application that tries to open it reports it as being broken, or of the wrong format. It looks like that power problem earlier in the week caused your hard disk to damage the file beyond repair.

Once again, with only three days of backups you have your machine "as it was" on Thursday, on Wednesday, and on Tuesday; all *after* the damage had happened. You no longer have a backup copy of the undamaged file.

So, how long should you keep backups?
As I said, there's no general rule I can apply that would make sense for everyone.

Clearly, the first few days are important. Things like lost files, malware and the like are often discovered very quickly, and typically you'll need go back only a day or two when that's the case. Of course, a sudden and total hard disk failure makes itself known quite quickly.

In situations like that, your three-day proposal is quite sufficient.

The questions I'd have you ask are:

- How confident are you that you'll discover whatever it is you might want from your backup within those three days?
- What would be the cost – be it monetary, emotional, or just the time to re-create it – should you be unable to recover something because you didn't discover you needed it before your three-day backup period passed?

Is there any reason you can't just throw more disk space at it and increase the number?

I'm using your three-day proposal as my example here, but the questions apply for any time period you might choose to keep backups, be it three days, three months, or three years. For various reasons and in various situations, the proper retention period could be any of those, or even longer.

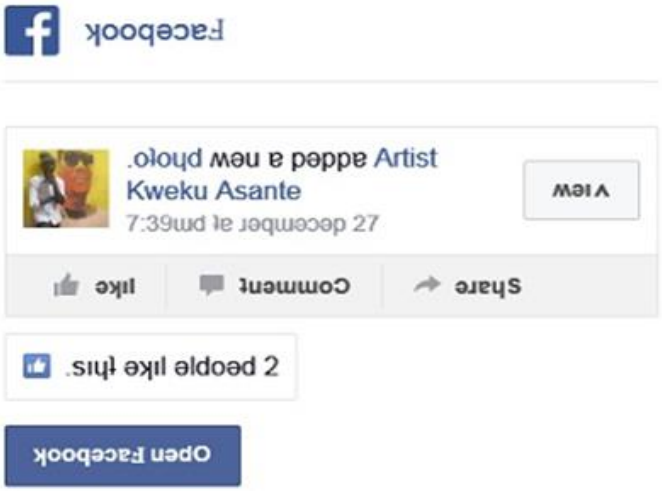
Ultimately, I can't answer this question for you, but hopefully I've given you a few things to think about.

WS Tech Tips

Backwards Facebook Scam

Tuesday, January 5th, 2016 by **cynthia** | Filed Under: **E-Mail Help**, **Security Help**, **Social Networking**

In this week's edition of *Facebook Scams To Watch Out For,* we bring you a combination e-mail/Facebook fraud. Eleanor, has been receiving some strange e-mail notifications about her Facebook account. She writes: *"What is happening with these backward Facebook messages? I often don't even know the sender listed."*



What this is, Eleanor, is a scam and not even a well-executed phishing expedition. They want you to click on that backwards "open Facebook" button thinking you're opening your Facebook account, but actually taking you to a web page of their choosing. That web page could contain malware that could infect your PC and steal your information. It could also look very much like a genuine Facebook page and prompt you to enter your password or other information the spammers would like to steal from you.

By saying that someone has added a photo they'll hope you'll want to get a look at that photo.

These folks don't seem to be trying too hard, since they managed to get the image of the Facebook graphic backwards. Except for the name of the person who is s. That's probably because English isn't this scammers first language and he/she probably didn't know how the letters were supposed to look.

This is certainly Spam, and you should mark it as such immediately. You can't stop spam from being sent to you, but hopefully you can teach your e-mail account to filter it out so you don't have to be bothered with it.

Never click on a notification that seems wrong to you. You can just open of your Facebook account in your browser to see if you actually have any real notifications from people you do indeed know.
~ Cynthia

Amherst Church of the Nazarene

210 Cooper Foster Park Road, Amherst, Ohio 44001 (440-988-9014)

To: Sandra Ruth, President
Lorain County Computer User Group
Jan, 6, 2016

It is with great pleasure that we received your generous donation to the Amherst Church of the Nazarene food pantry. Your support and donation has enabled us to help the poorest of the Lorain County are and for the coming year.

The donation that we received allowed us to purchase over 600 pounds of fruits, vegetables and other non-perishable food items for senior citizens and families with children in our area. This is a significant amount of food for our community.

It is through the generosity of groups like yours, with a heart for the poor and disenfranchised, that we are able to serve not our fellow citizens but to answer the call of our faith to serve the poor.

Sincerely,

Aurelie A. Higgins

Aurelie Higgins RN, Pastor of Compassionate Ministries
Site Director for Amherst Church of the Nazarene

What are Websites Doing with Your Personal Information?

By Ira Wilsker, *Assoc. Professor, Lamar Institute of Technology; technology columnist for The Examiner newspaper www.theexaminer.com; deputy sheriff who specializes in cybercrime, and has lectured internationally in computer crime and security.*

WEBSITES:
http://www.govtech.com/data/How-Do-Websites-Use-Your-Data.html
https://identity.utexas.edu/privacycheck-for-google-chrome
https://identity.utexas.edu/idwise
https://identity.utexas.edu/strategic-partners
https://chrome.google.com/webstore/detail/privacycheck/poobeppenopkcbjejfjenbiepifcbclg
https://www.ghostery.com

You have likely noticed that the banner ads and other forms of advertisements on many of the web pages visited appear to "coincidently" be for many of the same items that you have recently searched for online. You may even notice that many of these ads are also from many of the same online sellers whose web pages you have recently visited. In some cases, you may also see online ads for direct competitors of previously visited websites, offering many of the same or similar products that you have looked at on other websites. It should not be surprising that the owners of many websites, as well as many third party advertisers, use a variety of tracking technologies to gather information on you, as an individual, the types of websites that you visit, and the products and services viewed. While many users find this targeted advertising interesting and useful, and even possibly necessary in order to support "free" web sites and online services, many others consider the gathering of such personal information as a gross violation of personal privacy.

Some of the more common methods of compiling and distributing this personal information and shopping preferences are the placement of "tracking cookies" on the user's device; web bugs or web beacons (small graphic files which transmit information when opened, often 1 pixel in size); and the dissemination (sale) of personal information entered on a website. Cookies are small, alpha-numeric and text based pieces of data which are by default, placed on the hard drive or other storage of the device being used to view a website; while some types of cookies are benign and necessary to compile shopping carts, store passwords and other login information, and save other information that can speed the web process, some other types of cookies may not be so desirable.

The most common type of unwanted cookies is often known as "tracking cookies", which are typically placed on the hard drive or other storage medium, just as other cookies, but these cookies can also be read by other third parties as a method of gathering information about the user, mostly for targeted marketing purposes. There are many companies that have a lucrative and highly profitable business selling access to the tracking cookies which they have previously been placed in storage, most often by simply visiting a web page. Almost all browsers give the users the option to control which cookies can be saved and accessed, but the default is to accept all cookies. Tracking cookies that are currently saved in the device storage can often be easily and quickly removed by most of the reputable (and often free) security scanners, such as Malwarebytes (malwarebytes.org) and SuperAntiSpyware (superantispyware.com).

What many users might find shocking is that they unknowingly and explicitly allowed many of the websites that they visit to place tracking cookies and other marketing information on their computers and smart devices. When I mention this to users at some of my security and privacy presentations, some of those present get very agitated, and vehemently deny that they ever gave permission for websites to place such information on their computers and other devices. My typical response is something to the effect of "Did you ever read the privacy statement on those websites when displayed, or simply click on the "I Agree" box when first visiting them?" Most of the honest, but still aggrieved users, acknowledge that they never fully read the privacy statements on the websites visited, with the typical response being that the privacy statement is too long to read, or it is written in "legalese" which they cannot readily understand, so they simply "agree" in order to get access to that particular website.

Complex privacy statements, often blindly agreed to, have been a popular tool to legitimize the placement of that website's or other third party commercial tracking information on your computer, smart phone, tablet, or other device. These tracking devices are often a significant source of revenue for the website owner, and are often utilized by some of the largest and most reputable online vendors. In a recent article by Omar L. Gallaga, of the Austin American-Statesman, dated May 11, 2015, and reprinted by "Government Technology", Gallaga wrote, "How Do Websites Use Your Data? A new tool in Google

(Continued on page 17)

(Continued from page 16)
Chrome puts website privacy policy language in plain English, letting you easily know whether your email address is shared or the site has access to your Social Security number, and if it tracks your location."

This free new tool, currently only available for Google's Chrome browser, is "PrivacyCheck", a Chrome browser extension (plug-in) which was developed by the Center for Identity at the University of Texas - at Austin (identity.utexas.edu). According to the Center for Identity, "PrivacyCheck is a browser add-on intended to provide consumers an overview of the ways in which companies use their personal data in a graphical, 'at-a-glance' format. ... PrivacyCheck surpasses existing add-ons, apps, and certifications by using a Data Mining algorithm to access the text of any webpage. The user provides the URL for the company's privacy policy and PrivacyCheck searches the page, returning icons that indicate the level of risk for several types of PII (Personally Identifiable Information)". PrivacyCheck can be downloaded for Chrome from the Chrome web store at chrome.google.com/webstore, and entering "PrivacyCheck" in the search box. The latest version of PrivacyCheck, as I am typing this, is version 1.0.5, dated May 14. It is important to know that federal and state laws require businesses with a web presence to post their privacy policies, and there are often harsh penalties for violating those posted privacy policies.

To use PrivacyCheck to determine the degree of privacy risk on a particular web site, download and install PrivacyCheck from the Chrome web store (chrome.google.com/webstore). Once installed, open the selected website using the Chrome browser, and locate the privacy statement, often linked at the very bottom of the webpage; open the privacy statement page. On the top right of the Chrome address bar is a small icon which is light brown in color, and has what appears to be a lower case "i" within a brown circle; click on that icon. Once clicked, "Browse to a privacy policy and click Start". Within seconds a series of 10 larger icons will appear, with an easy to comprehend green, yellow, and red coloration, indicating the degree of privacy risks associated with that privacy policy and website.

Moving the cursor over each of the large icons will explain what it represents: the "envelope" icon represents what the website does with the user's email address, red indicating that the website uses, sells and shares the email address to others; the second icon represents the magnetic stripe on a credit card, and indicates what the site does with credit card information; the three asterisks "***" represent what is done with the user's social security number, green indicating that it is not collected or otherwise used; the "megaphone" indicates the marketing use of your private information, red indicating that the website sells your information to others for marketing purposes; the "compass" icon indicates what the website does with detected location information, red indicating that the website sells the user's location information to third parties; the sixth icon, circular with two eyes, indicates the policy on information gathered from children; the "badge with star" icon indicates the distribution of information to law enforcement, red indicating that the site will provide information to law enforcement without a warrant or subpoena; the "open book" indicates the policy on posting privacy policy changes and giving the opportunity for users to opt-out; the "pie chart" icon indicates whether or not the user can modify his own information; the tenth icon, which looks like a cloud with directional arrows, indicates what the website does with aggregated information, yellow indicating that aggregated information is distributed, but personally identifiable information has been removed.

PrivacyCheck is an excellent method to determine what commercial websites are really doing with your personally identifiable information (PII), but its major weakness is that it (currently) only works with the Chrome web browser. Users of other browsers may find some privacy utilities that provide significant privacy protection while online.

On all of my PCs, as a browser add-on, I have been using a free, popular browser extension called "Ghostery" (www.ghostery.com), which will seamlessly run on computers using any of the major and popular browsers including Firefox, Chrome, Opera, Safari, and Internet Explorer, as well as on mobile devices running the Android and iOS operating systems. According to its website, Ghostery claims to have, "The largest tracker database on the internet, constantly growing; Ghostery has the largest tracker database available on the web. We meticulously select, profile and cull over 2,000 trackers and 2,300 tracking patterns." Ghostery displays the tracking information on almost every web page opened, and gives the user the ability to allow or block trackers as desired.

Our personal privacy should be taken very seriously. Once third parties have access to our personal information, it is virtually impossible to get it back. Most of the browsers offer an option or setting to control privacy, which may be called "Do Not Track", "Reject Third Party Cookies", or some similar name. By using PrivacyTracker, Ghostery, browser privacy settings, and other utilities, our individual privacy may be better protected.

Interesting Website

Interesting Internet Finds

Compiled by Steve Costello, President / Editor,
Boca Raton Computer Society, FL
May 2015 issue, Boca Bits
www.brcs.org / http://ctublog.sefcug.com/
editor@brcs.org

In the course of going through the more than 300 RSS feeds, I often run across things that I think might be of interest to other user group members.

The following are some items I found interesting during the month of April 2015.

VPNs the next big browser feature?

http://www.ghacks.net/2015/03/30/vpns-the-next-big-browser-feature/

This ghacks post explores the idea of VPNs being included as a browser feature. Opera acquired VPN provider SurfEasy, and the TOR browser is already based on Firefox, so this is something that just might come to pass.

Get Your Free eBooks Here

http://askbobrankin.com/get_your_free_ebooks_here.html

Bob Rankin lists some places to get free ebooks. I am always being asked where I get my free ebooks, so this should be of interest to anyone who read ebooks.

6 Amazon Prime Benefits You Might Be Ignoring Right Now

http://www.makeuseof.com/tag/6-amazon-prime-benefits-might-ignoring-right-now/

I am an Amazon Prime member, and there were a couple of things I didn't even know about. If you are an Amazon Prime member too, or thinking about becoming one, you should check out this Make Use Of post to get the most out of your membership.

Force Close A Chrome Tab When It Becomes Unresponsive

http://www.addictivetips.com/web/force-close-a-chrome-tab-when-it-becomes-unresponsive/

It doesn't happen often, but sometimes I have a Google Chrome tab that becomes unresponsive. Until I ran across this post at addictive tips I had to close down the browser completely, now I can use this tip and continue what I am doing.

How to Share a Wired Ethernet Internet Connection With All Your Devices

http://www.howtogeek.com/213638/how-to-share-a-wired-ethernet-internet-connection-with-all-your-devices/

There may be times you can connect via Ethernet, but there is no Wi-Fi or cell service available. If you follow the instructions in this HowToGeek post you will be able to work with all your devices.

Why I'm (slowly) Switching to OneDrive

https://askleo.com/why-im-slowly-switching-to-onedrive/

Leo Notenboom explains some differences between Google Docs and Microsoft Office Online, as well as backup handling in OneDrive and Google Drive. Check it out, maybe it can help you decide what works best for you.

The Tip Corner

By Bill Sheff, Lehigh Valley Computer Group, Pennsylvania
May 2015 issue, The LVCG Journal
www.lvcg.org
nsheff@aol.com

Print part of an email or other text?
At a recent meeting the question came up. "How can I print a portion of an email?" Here are a couple of ways of achieving this.

One way is to highlight the section of the email you'd like to print. Select copy and paste to a word document. This method is good if you want to do some editing of the text.

Another method is to highlight what you want, right click, select PRINT. When the print dialog box comes up, in the "Print Range" box, place a check mark in the box that says "SELECTION". Finally, highlight what you want, right click and select PRINT PREVIEW. Select the "As laid out" option click the drop-down button, and click 'As selected on screen' and you will see only the selected portion of text, ready to print. That will print out just what was highlighted.

MEMBERSHIP WITH LCCUG:

Yearly dues are $25.00. For more information contact:

Dennis Smith
Director of Membership,
membership@lccug.com.

Directions to Meetings:
A map and directions to our meetings can be found on our Members' web page:

www.lccug.com/members. Just click on the link "Meeting Locations & Directions"