Interface

Lorain County Computer Users Group

Users Helping Users

2016

Inside This Issue

**Tuesday
September 13, 2016**

TECHNOLOGY...
FROM A DIFFERENT PERSPECTIVE

Presented
By

Bob Gosticscha
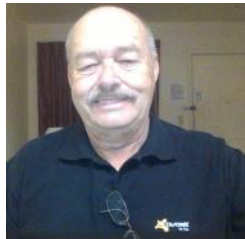
RAFFLE ITEMS

iHome USB Mouse w/Retractable Cord
16 GB PNY Flash Drive
Staples Gift Card
Ream of Printer Paper
2-in-1 GEL Pen & Touch Screen Stylus

☺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

This summer I've been thinking a lot about the capabilities of a smartphone. I especially found my smartphone useful on my mini vacation this year.

Although, I did make my flight reservations on my home computer, I used my phone to pull up my boarding pass in my airline's phone app. All the flight information could be tracked there and reminders are sent to me there as well. It did not have to be done that way, but it was convenient to have this option.

I also used my home computer to select and book a bed and breakfast through Airbnb. I wanted to spend 2 nights near Seattle to do some sightseeing. Housing in the Seattle area is extremely expensive and staying in a B&B seemed like a good decision. Once I had made my choice, which I could have done on the phone, all my interaction with the service and the host were done on the phone. Reminders, directions questions….. was all done on the smartphone.

I researched where I wanted to do sightseeing by exploring online and once I decided what I wanted to do in the morning, I booked a bus tour of the city for that afternoon.

Then I checked off another item on my list of things to experience when I scheduled an Uber ride to pick me up and take me into the city. This has to be done on a smartphone and once you are signed up, calling for a ride is very simple. Within 2 minutes of requesting a ride to my first destination, the driver was there as promised. The phone showed me a that was coming, the make of their car and their license plate number and a picture of the driver. Later I used the service to return from the city to the B&B and that wait was exactly 8 minutes. He even called me to check and make sure 8 minutes would be OK. The next morning I requested an Uber to take me back to the airport and the wait for that ride was exactly 5 minutes as the app on the phone told me.

Of course, I used the phone for all my photo's as did everyone else around me (with few exceptions). I used Google directions to give me walking navigation help from the shopping site I started at to lunch and to the hotel to meet the tour bus! It guided me easily street by street.

The phone also provided me with music to listen to and books to read in the evening. Email and facebook could be checked easily. I even took a couple phone calls from home reminding me of an upcoming dentist appointment and such… which is a funny feeling. You can't escape some routines even when you are out of state.

I was able to text back and forth with my brother when the last leg of the flight home was delayed because of weather. I could then remind him to check online to judge exactly when my plane would land so he could pick me up.

LCCUG Officers For 2016

President	Sandee Ruth president@lccug.com
Vice President	Carole Doerr vp-programs@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 Education	Neil Higgins education@lccug.com

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

TECHNOLOGY...
FROM A DIFFERENT PERSPECTIVE

By
Bob Gosticscha

This is a very new presentation. Looking back and comparing it to now, it is an enjoyable and funny comparison combined with the stark reality of what you need to do to keep safe in the modern world. This presentation will cover: Computer (Windows and Mac), tablets and Smart Phones.

Join presenter Bob Gostischa, as he takes a comical look back in time and then explains what you need to know to stay safe in the present. He will make your Internet experience and Computer operation safe, secure and, enjoyable.

After a successful career in banking, Bob enjoys his retirement as an enthusiast IT security expert, most notably for Avast Software. Avast is the creator of avast! antivirus software. He has contributed over 30,000 forum interactions.

This should be a very interesting and informative program for members and guests.

(Continued from page 2)Presidents column

I also had my tablet with me but I didn't take a laptop as I might of other times. It was a short trip but I was able to do everything between the tablet and the smartphone. I even had downloaded a couple movies from the library service, Hoopla, but never had a chance to watch them. The BnB had very good Internet strength available but didn't offer Television, which added to its charm in my estimation. An interesting experience .

Such is a small look at traveling in the year 2016!!

Sandee Ruth
LCCUG President

Executive Board Meeting Minutes

AUGUST 1, 2016

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

A brief discussion was held on ideas for future programs. We must finalize the October program for this year.

The club has a new account with the Amazon Smile Program where we get credit for purchases made thru our club website. We will explain more to members at future meetings.

Prizes for the August 8 software/hardware raffle were selected. Sandee will pickup $10 gift certificates from Staples and Pam will pickup 32 GB flash drives from Sam's.

Dennis gave a seven step recommendation on how he felt the newsletter could be improved by shortening. The board welcomed his thoughts and will discuss this issue further.

Pam moved, Richard seconded the meeting be adjourned. Motion passed.

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"

Member of
apcug
Association of Personal Computer User Groups

General Meeting Minutes

AUGUST 8, 2016

President Sandee Ruth called the meeting to order. A motion to accept the minutes as shown in the August issue of the *INTERFACE* was made by Pam Rihel, seconded by Micky Knickman. Motion passed by voice vote.

Sandee reminded members to turn in their used ink cartridges so the club may get credit from Staples. She mentioned the $25 roll over raffle, Neil's Windows 10 help at next weeks workshop and the credit we get from ordering under the Amazon Smile program.

Dan Hornby presented his program "Smart Investment Strategies" under the title "INVESTING 101".
He then explained the workings of the $90 a year subscription from www.betterinvesting.org which provides you with historic data on individual stock performance so you can make an informed decision when selecting a stock to buy or sell.

Dan made no recommendations on which stocks to buy, only how you may evaluate them.
There were many questions from the attendees which were very well answered.

There was no attendance raffle winner. Lorna Middendorf won the roll-over raffle, Carole Doerr won the software/hardware raffle.

Joe Harrold moved, Bud Ennis seconded the meeting be adjourned.

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**

New Genealogy Service Poised to Fill Critical Gap in Genealogy Industry

This looks interesting. You can now obtain personalized coaching for your genealogy searches. The following announcement was written by the folks at genealogyDOTcoach:

CEDAR HILLS, Utah - August 29, 2016 - A new family history service launched today that will fill a critical gap in the multi-billion dollar genealogy industry. genealogyDOTcoach(SM) is a new online service that matches up professional genealogists (called Genealogy Coaches) with people who want to have all the fun of making family history discoveries for themselves but just need a little assistance from someone they can trust.

"With do-it-yourself sites like Ancestry.com and FamilySearch.org it has become so easy for anyone to start climbing their family tree," says co-founder, Janet Hovorka. "But, sometimes people get a little stuck in the process. The traditional option at that point has been to purchase a 10 or 20 hour research package from a professional genealogist. Many people can't afford that kind of help. Others are reluctant to do so because they want the joy of making those family history discoveries themselves. genealogyDOTcoach aims to fill that gap."

The service launches with 25 coaches across 47 different categories. Topics include: getting started; genetic genealogy/DNA; tree analysis and writing a research plan; and document translation. Coaches also specialize in research for different regions of the world and different ethnic groups. The initial group of coaches have an average of 25 years of training and experience a piece. They are researchers, authors, and lecturers. The impressive list of coaches includes some of the most well-known genealogists in the industry.

On the genealogyDOTcoach website, users can select a topic and see a list of coaches who specialize in that topic. They can review comments and ratings from previous clients, to help them select a coach they would like to work with. Sessions can be scheduled for 15, 30 or 60 minutes. Pricing starts as low as $15 for 15 minutes.

Shortly before the coaching session, an email link is sent that allows the user to log in to a private video chat room. There they meet face to face, via video chat, to share screens and documents with the genealogy coach, and receive the help they need to keep them moving along in their family history journey.

"Clients leave the coaching sessions with a game plan for how to move forward in their family history research," says Hovorka. "Just like life coaches or athletic coaches, genealogy coaches can give you the boost you need to be better at what you enjoy."

Funny Mottos, funny quotes and phrases

"Everything is funny as long as it is happening to somebody else."
Will Rogers

"I feel sorry for people who don't drink. When they wake up in the morning, that's as good as they're going to feel all day."
Frank Sinatra

"If you can smile when things go wrong , you have someone in mind to blame."

"The saddest aspect of life right now is that science gathers knowledge faster than society gathers wisdom."
Isaac Asimov

"Sometimes the questions are complicated and the answers are simple."
Dr. Seuss

"Good friends, good books, and a sleepy conscience: this is the ideal life."
Mark Twain

"Don't cry because it's over, smile because it happened."
Dr. Seuss

"Life is short, don't waste time worrying about what people think of you. Hold on to the ones that care, in the end they will be the only ones there."
http://www.mottos.info/life/

Computer Attacks

By Dick Maybach, Member, Brookdale Computer Users' Group, NJ
June 2016 issue, BUG Bytes
www.bcug.com
n2nd@ att.net

An important factor in defending your computer is to understand how it might be attacked. This topic fascinates many computer owners and has been the subject of many articles, books, advertisements, and discussions. One result of this is a jumble of terminology with words having meanings almost as slippery as the programs they are trying to describe. In this article I'll attempt to untie the terminology knot with brief definitions of the most common terms. You can learn (much) more with an Internet search for any of these terms, provided you read with skepticism. We'll start by using **attack** to describe any malicious act directed at a computer, the data it contains, or its user. We can classify attacks in three different ways:

1) their **attack method** (how they access your PC, your data, or you),
2) their **behavior** (how they get established and perhaps spread), and
3) their **payload** (what they do).

To a great extent, these characteristics are independent, and we can look at each in turn. Much of the confusion about malware arises because authors don't make it clear whether what they are describing is an attack method, a behavior, or a payload.

First consider network attacks, which may not affect your computer at all. The first type, **network monitoring**

is passive and is a digital version of a phone tap; everything you send and receive is recorded by a third party. This is easily done at a public hot spot, and requires only a laptop and widely-available software. It also can occur at ISPs and Internet relay points, either by the facility owner or by government agencies. A second type, the **man in the middle** attack, is active and is much more specific. Here, a computer is set up to mimic, for example, your Internet bank. If you can be fooled into logging into it, the attacker can capture your password and other account details before forwarding your traffic to the bank site you think you are using. This is more difficult to set up than simple network monitoring and is thus less common.

Let's now look at computer attack methods, which include

1) physical access,
2) social engineering,
3) Trojan horses, and
4) unethical suppliers.

Someone with **physical access** to your PC can install malicious hardware or software. Although this is sometimes called the **evil maid** attack (presumably because it's done by a hotel's housekeeping staff), it more commonly occurs when someone uses your PC with your permission and inadvertently infects it during, for example, a careless Internet browse. You now have a compromised PC for such tasks as your Internet banking. **Social engineering** or **phishing** occurs when someone tries to convince you to disclose sensitive data or perform some action that compromises your computer. You might receive a phone call or an e-mail message claiming to be from your credit card company requesting your account information, or one from tech support offering to remove a virus they somehow have detected remotely. Many attacks occur as **Trojan horses**, where malevolent software hides inside something that appears useful, interesting, or at least harmless. Examples include e-mail (often appearing to be from somebody you know) with an attachment that installs software, Web pages that run programs on your PC, and macros embedded in office files. Finally, there are **unethical suppliers** that include software you neither need nor want with their products. Although the most common culprits are Websites, it can take the form of **shovelware**, useless and sometimes intrusive programs installed on PCs, and malicious software on supposedly blank media.

Once **malware** (which malicious software is often called) infects your PC, it can behave in four different ways:

1) reside there as a normal program file,
2) attempt to hide by changing its form or the operating system configuration,
3) spread through your computer by attaching a portion of itself to other files, or
4) send copies of itself to other computers, usually

via the Internet.

Type (2) programs are called **stealth software** or **root-kits**, type (3) programs are called **viruses**, and type (4) are called **worms**. An interesting form of virus resides in office document as a **macro**, for example written in Visual Basic and included in an MS Word or Excel file. These can migrate to your master template and infect every document you compose after that. When they first appeared around 2000 macro viruses were serious problems, but office suites now have effective safeguards against most; however, you may wish to check your preferences to be sure. (Although many people use the term virus for all malware, only 17 per cent of it really behaves this way and another eight per cent acts as worms.) Combinations are also possible; for example, a virus can have stealth features. Since rootkits and viruses can affect system programs, their installation often, but not always, requires that the user grant them administrator privileges. A number of vendors offer applications to detect rootkits, but removing one sometimes requires erasing the computer's hard drive and reinstalling the operating system. Many people call type (1) programs Trojan horses, but I prefer to use that term for a malicious program's attack method rather than it's behavior after it becomes active.

Note that network attacks, social engineering, and macro viruses are operating-system agnostic. OS X and Linux users are just as vulnerable to them as are Windows users.

The object of most malware is to deliver a payload that is to perform some action to harm the computer owner or benefit the malware supplier. The payload is independent of the attack method and also of the malware's behavior. Examples are:

1)ransomware,
2)adware,
3)spyware,
4)key loggers,
5)botnets, and
6)hijackers.

Ransomware restricts your access to your PC and displays a message on how you can purchase instructions or software to remove the limitation. In some cases it encrypts files and demands the fee in return for the password to regain access to them. Sometimes there is just a threat, such as pay a fee within 10 days or your hard disk will be formatted. **Adware** continually displays advertising messages on your screen, although this can be legitimate (if annoying) when it's associated with trial software and seeks to sell you the paid version. **Spyware** transmits sensitive information, such as account information and passwords to an Internet location without your permission. Some people lump adware and spyware together and call both spyware, but I prefer to keep them separate, since spyware is more costly. A

key logger records your keystrokes and forwards them to an Internet location with the intent of capturing log-in information; it can be implemented by either hardware or software. Malware can make your PC a component of a **botnet** (also called a zombie army), a computer network sometimes used to distribute spam or to attack other Internet sites by trying to overwhelm them. Other payloads, having a variety of names that often include the term **hijack**, change the configuration of your browser by changing your home page or your search engine or by adding menu bars.

By far the best time to defend your computer is in the attack phase, where healthy suspicion is your friend. Be careful reading e-mail, surfing the Internet, and using your laptop in public places. Note that some form of social engineering is a component of most attacks. After the attack, an anti-virus program may be able to recognize the malware's behavior and prevent it from delivering its payload. Here, you depend on the malware spreading relatively slowly, so that anti-virus vendors have had time to develop a defense before you encounter it, and fortunately this is most often the case. Once the payload has been delivered, the damage has been done, and you will have to stop using the computer until it can be cleaned, change your passwords, and work with your bank, credit card vendors, and others to repair the damage.

We usually think of malware defense only for PCs, but it also infects all computer-driven devices, such as smart phones and network routers. It's important that you include these in your safe computing plan.

Your ultimate defense against all malware is a backup made before your PC became infected. Wiping and restoring your hard disk will almost always restore your system, except in the rare cases where the malware resides in your PC's BIOS firmware, in which case you probably need expert help. Unfortunately, the Unified

Extensible Firmware Interface (UEFI) adds a new vulnerability as it includes a writable boot

partition on your hard disk. Since the code residing here executes before your operating system; any malware installed there becomes active before any anti-virus program. Re-installing the operating system will probably leave the infected partition unchanged. So far, this is only a theoretical threat. I mention it only to make the point that threats evolve continuously, which requires that you keep all your software, not just your anti-virus programs updated, and conscientiously practice an effective back up discipline.

To summarize, we can classify computer threats according to their attach method, their behavior, and their payload. Attack methods include physical access to a computer, social engineering, Trojan horse software, and unethical suppliers. Once established, malware can behave as normal software, a rootkit, a virus, a worm, or a combination of these. Typical payloads are ransomware, spyware, key-logger, botnet, and hijacking. Network attacks are special in that they occur outside your computer.

Our next months meeting will be

To Be Announced

?

How the Internet of Things Threatens Your Security

It seems like just when we're coming to grips with one new piece of technology, something new comes along to bamboozle us again.

And the trend is not likely to change anytime soon as more and more devices in our homes get connected to us and to each other via the Internet.

This is what people refer to as the Internet of Things (IoT), a topic we touched on recently in our article Technology Delivers New Hacking and Key Copying Threats when we discussed how hackers have been trying to access and gain control of these devices.

Right now, IoT is mainly focused on business, notably networks of machines and industrial robots. But, we're already seeing IoT devices in homes — on smart TVs, security systems and domestic appliances.

The idea is quite simply to give us greater control over the things that are supposed to make life easier in our homes. Soon, electrical items that break down will be able to tell us what's wrong and how to get it fixed — surely a great time and money saver.

Using an Internet door entry system, we can also answer a knock on the front door and view who's there even when we're not at home, we can set and unset security alarms, switch appliances on and off and even switch on the heating and draw the drapes to create a cozy atmosphere for when we get back home.

In the process, most of us probably don't give a second thought to the question of securing access to these systems. After all, who but you would want to mess around with that remotely controlled thermostat in the entryway?

The answer is probably no one. But the trouble is that the thermostat or any other IoT controlled device is potentially connected to all the others via your Wi-Fi network, including your home security or alarm system. Potentially, any one of them is a gateway to all the rest.
In fact, Google actually has a service called Thread whose purpose is to link all your online appliances and devices together.
If you're technically-minded, you can read about Thread on Wikipedia.

The problem is that most of us aren't technically minded, yet we are increasingly allowing, or being asked to allow, Internet-accessible things — the workings of which we don't understand — in our homes.

This is a challenge that won't be going away, so we may as well knuckle down and learn how to make these devices and networks as secure as possible.

In fact, there are a few simple things you can do, without being a techie, to minimize the risk of security breaches.

Five Key Tips

Here are 5 tips to follow:

1.Be sure you know which devices in your home are actually Internet-accessible. Sometimes you may not realize when you buy them and, increasingly, you may not have a choice of whether the feature is included or not, though you might be able to switch off the connection. If it's an electronic product, ask the salesperson or check the manual.

2.If you decide you want to buy a connected device, check reviews and get a clear idea of price and capabilities. This should help you steer clear of counterfeits (usually much cheaper), which may have security weaknesses or even intentionally embedded malware that can spy on your wireless system.

3.When researching connected devices, establish if they come with "embedded security." Manufacturers are starting to add this feature.

4.Keep all appliances/devices up to date. The "brains" of IoT devices, from smart TVs to intelligent refrigerators, are often built into circuitry known as "firmware" — which means it can be reprogrammed or updated. As security risks are identified, manufacturers often update the firmware. Unfortunately, sometimes updates must be done manually; check your manual or the manufacturer's website on how to do this.

5.Make sure your home network is secure. The manual that came with your router — the device that distributes Wi-Fi signals in your home — will tell you how to set the highest possible security level, change the password and even make your network invisible to snoopers.

And ensure that the Internet security software on your PC is also up to date.

Right now, you may think you don't have any IoT devices at home. But if you have a smart TV, a wireless thermostat or newer video doorbell systems, you almost certainly do.

In a recent investigation, security firm Proofpoint found that some home-based non-computer devices were already being linked into a botnet — an illegal, remotely controlled network used to spy on computer systems and to send out spam.

Currently, there are estimated to be around 50 billion connected devices worldwide, and the number is rocketing.

The Internet of Things is going to be a central part of everyday life soon. So, make the time now to find out if or how your current TVs and other devices connect to the Internet and take action to secure them.

Alert of the Week

The Federal Trade Commission (FTC) has released four new videos dealing with imposter scammers — people who pose as officials, lonely-hearts, relatives and others supposedly in need of your cash.

The videos, also available in Spanish, are short and easy to watch — so, well worth the time to view.

Ask Leo!
by
Leo Notenboom

Why can't I boot from an SD card?

I have noticed many times in publications that we can use a USB flash drive to boot from under certain situations. But what about SD cards? Can we also use SD cards in the same way as we can use USB drives? I have noticed on my computers that the computer seems not to differentiate between the different types of drives. Does Windows really care if you use a USB drive versed to an SD drive for doing these sorts of things like booting from?

Windows doesn't really care at all, for reasons that we often overlook.

We need to start by clarifying something: the initial steps of booting your computer have nothing – or at least very little – to do with Windows.

Let's have a look at booting, who does what at boot time, and why you probably can boot from an SD card if you really want to.

What it means to boot
To "boot" something is a term derived from "bootstrapping", which in turn came from the phrase "to pull one's self up by one's bootstraps".

In the realm of computing, to boot something means the process of starting up a computer or similar device from some inactive, initial state, to a working, functional state. It's mostly about loading the operating system software, such as Windows, but can involve not only that but any software configured to run when a computer starts.

Note that I said "load the operating system software". That's our clue as to why Windows doesn't so much

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

---

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!

LCCUG ONGOING WORKSHOP
ALL ARE FREE AND OPEN TO THE PUBLIC

Problem Solving Workshop

Date: Tuesday - September 20, 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 - September 20, 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.

Learn About

Questions About Windows10

Date: Tuesday - September 20, 2016
Time: 5:30 - 8 pm Instructor: Neil Higgins
Place: Amherst Church of the Nazarene
210 Cooper Foster Park Rd.,44001

If you want to know more about Windows 10, we will be demonstrating this newest version of Windows and answering your questions.

Class materials (PDF files and Word documents about Windows 10 features and settings) will be available.

Please bring a flash drive with a least 500 MB of space to copy these items to it. If you would like to participate please let Neil know by sending an email too.

If you would like to participate and get copies of the material for this class, please let Neil know by sending an email toEducation@lccug.com

Class Ideas?

Please tell Neil or one of the other officers what you would like to learn and we will be happy to hold classes on your subject./subjects.

The Lorain County Chapter of OGS

is having it's next meetings on :

⇒ **September 12 - "Looking For Lizzie" - Debra Lape, author of "Looking for Lizzie", will discuss her journey to discover the family secret surrounding her 2nd great-great grandmother, Lizzie Rogers Lape, while Mary Kathleen Tripp portrays the main character.**

⇒ **October 10 - "When Descendents Become Ancestors" - David Kendall**

⇒ **October – Annual banquet – for information click HERE (hold down the crtl tab & hit enter.)**

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**.

WOW LCCUG IS OPEN TO THE PUBLIC

While you are on Facebook look us up and check out what our meetings are about, are workshops and much, much more. You can learn about new programs, what's new with computers, tablets, phones, anti-virus's, etc.

The Lorain County Computer Users Group has been around since 1990. I have been a member since about 2003 and I am now the Newsletter Editor and have been for about 8 years.

Since joining this group I have learned a lot about many programs, like the one I use for our newsletter. I started out knowing very little and I knew nothing about Publisher or Power Point programs and so much more.

So please join our Facebook page and be informed.

Newsletter Editor
Pamela M. Casper Rihel

---

care about what you boot from.
Boot time chicken and egg

Windows doesn't control the initial state of the boot process because Windows isn't running yet. The boot process loads Windows[1], but booting starts before Windows is around.

In fact, it doesn't have to be Windows at all. Your machine could boot into Linux, or even some other operating system entirely. Not only is Windows not involved at that point, it may be nowhere near the machine.

BIOS and UEFI

What controls the booting process is the computer's BIOS, or UEFI, the more powerful and secure BIOS-replacement on newer-model computers. I'll simply refer to both as BIOS.

The computer's BIOS is built in to the hardware. Aside from some housekeeping when it starts, it's there and running the instant you turn on your computer.
A BIOS has several different jobs, one of which is to load the operating system.

In other words, it's the BIOS that does the booting.

Boot devices

It's your computer's BIOS that determines what devices you can boot from.

If your computer has a built-in SD card reader, and your computer's BIOS supports booting from that reader, then you're good. It should, in theory, work.

In reality, most computers don't have a built-in SD card reader. Most computers do have USB sockets, though. As a result, it simply makes more sense to make the USB interface the next most logical boot device after the hard disk itself, or any optical drive.

That being said, most SD card readers are, themselves, external devices you connect to your computer via a USB interface. Therefore, you should be able to create a bootable SD card if you treat that external SD card reader as if it were a USB thumbdrive.

But if you need to have an external card reader and a SD card, it's probably just easier to use a plain old USB thumbdrive to begin with.

Boot order

Where many people get hung up, particularly since the introduction of UEFI, is boot order.

When you turn on your computer, the BIOS essentially asks itself a series of questions to figure out what to boot from:

Is there a hard disk? Is there an operating system[2] on the hard disk?

> ο Yes? Great, let's boot that.
> ο Is there a CD or DVD drive? Is there a CD or DVD inserted? Does it have a bootable operating system on it?
> ο Yes? Great, let's boot that.
> ο Is there a USB drive? Does it have a bootable operating system on it?
> ο Yes? Great, let's boot that.
> I give up. No bootable devices.

As you can see, if there's a bootable operating system on the hard disk, the USB drive will never be used for booting.

Most BIOS's let you change the order it checks. A very common alternate order is to check the CD/DVD drive first, then USB, and then lastly the hard drive. As long as both CD/DVD drive and USB drives don't have anything bootable inserted[3], the machine boots from the hard drive; otherwise, the inserted disk or thumbdrive is used.

How you change the boot order depends on the BIOS in your machine, and naturally, different machines have different BIOSes. You'll need to check the documentation that came with your machine.

UEFI can make things more complicated, because it provides a mechanism to prevent changing the boot order at all, or to prevent booting from anything other than the hard disk.

And this is also where Windows can get involved in the boot process, kind of.

UEFI, booting and Windows

With the advent of UEFI, many of the choices we might make at boot time are now made in Windows itself instead. For example, to reboot into a recovery mode, to repair Windows, or even to change many different start-up options, Windows 8 and 10 use the Settings app to make those choices. Then, under the control of the UEFI, the machine reboots and whatever was selected happens.

To me it feels somewhat like putting the cart before the horse. You have to boot into Windows, (usually proving you're the administrator – an added security measure), in order to run the settings app to make some of the choices affecting how the machine boots the next time. But it's still a reboot. It's the UEFI that determines

what happens, though at the instructions of a previously running copy of Windows.

One of the more frustrating aspects of UEFI is that it can disallow booting from external media at all. This is a security measure that prevents people from walking up to your computer, inserting a disc, and forcing a reboot to bypass all of your other security. Unfortunately, it's a hassle if you have a legitimate need to boot from something other than the hard disk.

Once again, this also all depends on your specific computer and exactly how your computer manufacturer configured the UEFI used in your machine.

If it looks like a USB drive

One of the nice aspects of the USB interface is that it more or less hides the technology being used from the computer. If your USB SD card reader looks like a USB flash drive, you should be able to use it as a boot device. Similarly, one of my recommendations for booting from DVDs and CDs for machines that don't have optical drives is to get an external USB DVD reader. Most look like any other USB device at boot time, and if the BIOS supports booting from USB, they can be used for exactly that purpose.

So, sure, you can boot from an SD card if you like. You probably just need to treat it like a USB flash drive. I just don't see any huge advantage to doing so.

Interesting Internet Finds – June 2016

Steve Costello, Boca Raton Computer Society
editor@brcs.org   http://ctublog.sefcug.com/

How to Set Up and Use Open365, an Open Source Alternative to Office 365

http://www.howtogeek.com/256450/how-to-set-up-and-use-open365-an-open-source-alternative-to-office-365/

If you are using LibreOffice, and would like to try out the Open365 (beta at this time) alternative to Office 365, this post from *HowToGeek* is a must read.

Seven Tips on Keeping Your Phone Safe While Traveling

http://www.cnet.com/news/seven-tips-on-keeping-your-phone-safe-while-traveling/

This is the time of year for vacation travel, so check out this post to refresh yourself on how to keep your phone safe while you are out there.