News Journal

Lake County Area Computer Enthusiasts

PROGRAM OF THE MONTH NOVEMBER
"COMPUTER & INTERNET SECURITY"

Presented by:

Charles Prince of Avast Software

L.C.A.C.E. to celebrate 30th anniversary April 6th!

Food, fun, and festivities will mark LCACE's gala 30th anniversary party. The day will begin with the election of officers, to be followed by Show and Tell and Ask the Gurus. Members must be present to win one of many door prizes. Some lucky person will win first prize, a Western Digital 2TB USB 3.0/2.0 silver My Passport portable hard drive. Remember you have to be a member to participate in the prize drawing. No party is complete without refreshments; birthday cake and fresh fruit will head the "goodie" list.

Robin's RAMblings

LCACE welcomed 6 guests to our January 5th meeting. One person heard about us through the library; the others learned of our club through newspaper articles. Our publicity chair, Linda Koudelka, has been working hard to publicize our club. A photographer from the Chicago Sun-Times took photos at the January meeting, and a very nice article with his photos appeared in the Waukegan News-Sun on Monday, January 7th. http://news-sun.suntimes.com/17367239-417/computer-enthusiasts-members-helping-members.html

The question of the day was "Have you downloaded any interesting smartphone apps lately?" Ellen Smatlak introduced us to "Lake County Passage", www.lakecountypassage.com/, which shows traffic tie-ups in real time. I mentioned "Google Goggles", www.google.com/mobile/goggles/, and Fred Barnett said there was a way of downloading smartphone apps to your computer.

If you have suggestions for the question of the day, please email them to me at president@lcace.org

When he saw a picture of a $20 bill in the agenda, newsletter editor Mike McEnery asked how I was able to scan it, since most scanners today will not copy U.S, currency. I had downloaded the image from the internet several years ago when I wanted to print currency with pictures of my grandchildren on them. I figured no one would think that color pictures of the children printed on one side of heavy paper could possibly be real money.

This brings up an important point. Just because you find something on the internet does not mean you have the right to reproduce it. Better to be safe than sorry.

Alex Lopez and Tyler came from Best Buy of Gurnee to show us the latest in mobile computing: smartphones, tablets, and ereaders. They told us of the services Best Buy offers including free classes on Windows 8 and Apple devices. I plan to take the Windows 8 class so I can learn if there is a reason I would want to use this latest Microsoft operating system.

Best Buy also brought us 20 door prizes which our members were happy to collect.

Our February speaker, Charles Prince of Avast software, will speak about internet security. It doesn't much matter these days what operating system you use; you need to be very careful on the internet.

In February we begin our three part election process. Richard Eisenmann has volunteered to conduct the election again. We take nominations for board positions February 2, March 2, and April 6. We elect our board at our April 6 meeting, and then choose our president from the people elected to serve on the board. All nominees must be members in good standing-i.e., their membership dues must be paid to date. Please start to think of who you would like to nominate. You can nominate yourself.

Our March 2 program will feature Linux expert Julie Bell who will present GnuCASH, an accounting software program that works on Windows, Linux, and Mac OS X. She will just show the checkbook portion. GnuCASH is similar to Quicken for Windows but it is open source and free.

Has anyone tried www.ninite.com for downloading and installing software in batches?

Do you know how to save to a flash drive? Do you use a flash drive to move data? Our gurus can show you. Each paid member family at the March 2 meeting will receive a flash drive (One flash drive per family.). Preference will be given to those who did not receive one at our August meeting. Be sure not to miss the meeting.

Do you have some doubts about getting a new computer because it will be running Windows 8? Apparently there are still a lot of Windows 7 computers left for sale. I recently noticed some HP laptops in a Tiger Direct ad that were dual boot. This means they open in Windows 7 Professional but they also include Windows 8 Professional. This sounds like a very interesting idea.

I just saw an attention grabbing headline online: **"Pope tells church leaders: Get tweeting!"** "Pope Benedict XVI has told Catholic Church leaders they must engage with social networking sites like Facebook and Twitter if they want to spread the faith to the next generation."

If you are going to make a purchase on Amazon.com, please remember to sign in through our LCACE home page, www.lcace.org

Click on the Amazon logo to connect and start shopping. LCACE will receive a small commission for all purchases made when people have connected through our home page. Please ask your family and friends to use this link as well.

We have exciting programs scheduled for 2013:
February 2, 2013-Charles Prince of Avast Software will present "Internet Security", nominations
March 2, 2013-Julie Bell will present "GnuCASH", flash drive demonstration, and nominations

April 6, 2013-Nominations, election, Show and tell, Ask the Gurus, 30th anniversary party

Our meetings are always open to anyone with an interest in computing. Bring family and friends.
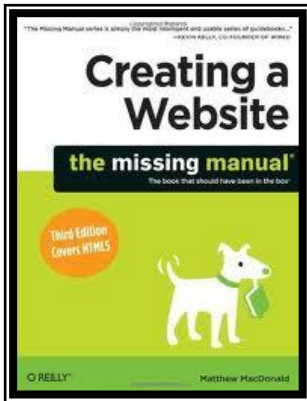
Happy computing!

Creating a Website
The missing manual

Book Review

Submitted by: Lester Larkin

This book, by author Matthew MacDonald, has the two most important characteristics of any book: it is comprehensive, and easy (and fun) to read. It weighs in at about 575 pages measuring 7" by 9". I am reviewing the third edition, printed April 2011.

The book is divided into 5 parts, each with several chapters:

Part One is "Welcome to the Web". Its 4 chapters cover newbie type subjects such as website planning, basic HTML, selecting a website hosting company, and web-page editing software.

Part Two is "Building Better Web Pages". These 6 chapters deal with more advanced HTML concepts and practices, like Cascading Style Sheets (CSS), adding pictures, linking pages within your website, and creating slick standardized page layouts.

Part Three is "Connecting with Your Audience". What good is a really great website if no one knows it exists? Chapters 11 through 13 help you bring in traffic, and keep them interested. Chapter 14 helps you make some money with your website.

Part Four is "Website Frills". Don't you love it when a website actually DOES something? Chapters 15 and 16 cover the application of JavaScript mini programs that can bring your website to life. Chapter 17 deals with adding music and video to your website.

Part Five is "Appendixes". Unlike its readers, this book has 2 appendixes. The first is a handy HTML reference. The second is some useful links for more info, free stuff, and some available services. Don't like to type links? No problem! Well, you have to type one:

http://www.missingmanuals.com/cds/caw3

But that is if you have only a paper copy of this review. Otherwise, just click on the above link.

I really like this book. It lists for $30 in the U.S. And $35 in Canada. Tightwad that I am, I may actually buy a copy so I can create better websites!

Les Larkin

1/19/2013

Ira is a member of the Golden Triangle PC Club, an Assoc. Professor at Lamar Institute of Technology, and hosts a weekly radio talk show on computer topics on KLVI News Talk AM560. He also writes a weekly technology column for the Examiner newspaper <www.theexaminer.com>. Ira is also a deputy sheriff who specializes in cybercrime, and has lectured internationally in computer crime and security.

Secure Your Wireless (Wi-Fi) Connection

by Ira Wilsker

WEBSITES:
http://www.makeuseof.com/tag/7-important-features-wireless-router
http://compnetworking.about.com/od/wirelesssecurity/tp/Wi-Fisecurity.htm
http://wiki.answers.com/Q/How_do_I_change_my_wireless_netw_ork%27s_security_settings
http://en.wikipedia.org/wiki/Wi-Fi
http://www.wi-fi.org
http://en.wikipedia.org/wiki/War_chalking
http://www.blackbeltjones.com/warchalking/warchalking0_9.pdf
(Pocket War Chalking Card)
http://en.wikipedia.org/wiki/War_driving

Almost all newer laptop computers as well as tablets, smart phones, video game consoles, and home entertainment systems utilize Wi-Fi as a primary or secondary method of connecting to the internet or some other network. According to published reports from several sources, the majority of home internet users have some form of Wi-Fi in their homes, and Wi-Fi is very commonly used in business, commercial, and academic environments. While the basics of Wi-Fi security apply to almost all Wi-Fi networks, home users have become especially vulnerable because many have never implemented anything more than the minimum default security settings when installing and setting up the hardware.

The Wi-Fi Alliance (www.wi-fi.org) defines Wi-Fi as any "wireless local area network (WLAN) products that are based on the Institute of Electrical and Electronics Engineers' (IEEE) 802.11 standards." Wi-Fi is a fan-

cy radio device that sends and receives streams of data through the air, just as any other 2-way radio device. As consumers, we often see the presence of Wi-Fi in terms of its standard designations, such as 802.11b, g, or n (as in 802.11n), each of these terms indicating the speed, bandwidth, and channels available under those industry standard protocols. While new speeds and protocols are always being developed and tested, the fastest and most powerful of the current widely available standards is 802.11n, which is capable of a theoretical speed of 540 Mbps. A portion of the standard provides for downward compatibility, meaning that devices made for one of the newer standards, such as the "n" standard, must also be capable of communicating with lesser devices, such as the "b" and "g" standard devices.

For home use, most of us have some form of Wi-Fi access point, typically either a free standing device directly connected to the internet, integrated with a wired (Ethernet) router, integrated with some form of modem (common with cable and DSL internet services), or as a combination unit of "all of the above." In my home I have a major name-brand integrated unit that combines a broadband modem, 4-port router (four Ethernet ports for Ethernet cable connected devices), a USB port to connect a printer or other USB devices to the network, and an 802.11n wireless Wi-Fi with MIMO (MultipleInput-Multiple-Output technology) for improved performance. Pur-

chased from one of the big box electronics stores for about $70, my multi-function device replaced the less-capable modem supplied by my internet service provider (ISP), and offers more features, speed, and security than the one provided by my ISP. On my laptop computer and on my smart phone I can see several nearby homes that have Wi-Fi, some of which are not properly encrypted and accessible to anyone within range for any purpose, including illegal or other illicit activities. I cannot easily see networks with a hidden SSID. The unprotected household Wi-Fi networks are so vulnerable, when one neighbor had his home broadband connection out of service, and was waiting for the ISP to come and repair it, he illegitimately used another neighbor's Wi-Fi until his was repaired. Do you really want someone else using your network without your permission or knowledge? Secure your Wi-Fi, or face the possible consequences.

For me, enhanced security was one of the primary reasons for replacing the older technology modem provided to me from my ISP just a few years ago. This older broadband Wi-Fi modem from my ISP incorporated the mid-speed 802.11g wireless access point, with archaic security and encryption capabilities. Being fully cognizant that home (and business) Wi-Fi networks are common targets of hackers and crackers, I wanted to harden my system from attack, and the newer integrated Wi-Fi ac-
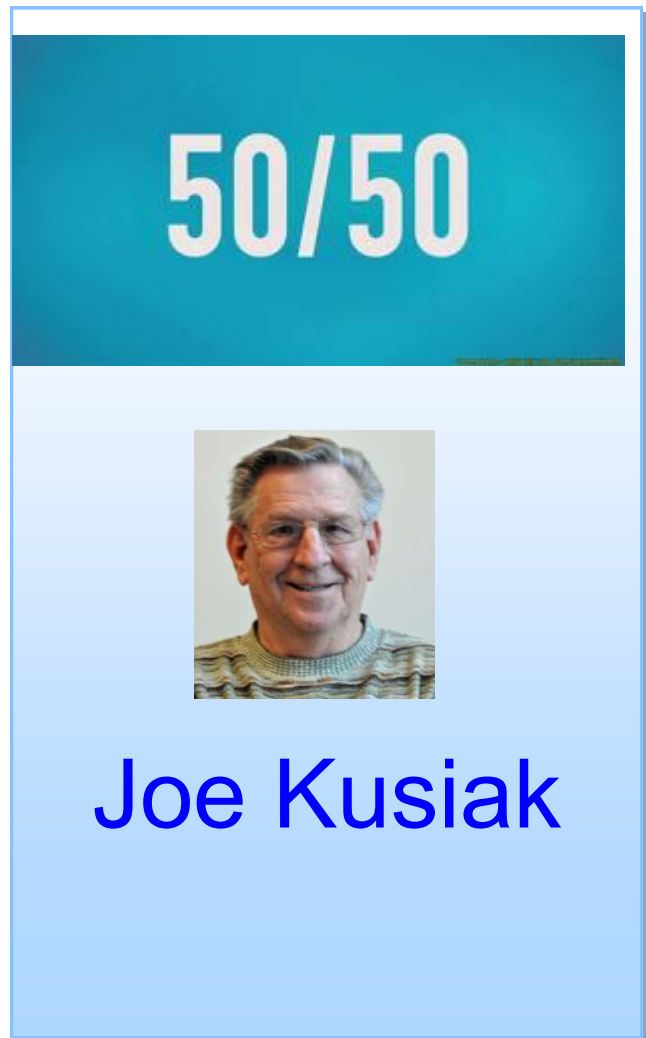
cess point offered far superior protection than did my ISP provided unit.

One of the first requirements of a reasonably secure Wi-Fi network is to implement the best encryption available on that particular device, such that unauthorized individuals who pick up the Wi-Fi signal will only find random garbage, rather than a useful stream of data. Since only Wi-Fi devices with the proper encryption key can exchange readable data, enabling the best type of encryption compatible with both devices (access point and remote device) will help protect the personal Wi-Fi network from intrusion. Unencrypted Wi-Fi leaves the entire network open to attack which can be used to steal personal data, passwords, user names, credit card information, and other information that can be illicitly used for a variety of malevolent purposes, including identity theft. At a minimum, an unencrypted home Wi-Fi network works like a free open network at a coffee house, where anyone can "leach" (steal or otherwise use) your internet access, slowing your connection, as the crooks are using your bandwidth. This "leaching" or theft of internet service may lead to unintended consequences, as it is not unknown for illicit drug dealers, pedophiles and child pornographers to use an innocent persons unprotected Wi-Fi in order to conduct their evil enterprises; if law enforcement tracks the bad guys, it typically leads to the innocent Wi-Fi owner, rather than the miscreant who purloined the system.

A common game of hackers and crackers is "War Driv-ing" (en.wikipedia.org/wiki/War_driving) where people with Wi-Fi computers and some readily available software drive around an area picking up and recording the locations of all detectable Wi-Fi networks, and posting the locations on a GPS coordinated electronic map. Even Google compiled a massive listing of Wi-Fi networks as its specialized vehicles travelled up and down virtually every street in the country for its Google Maps "Street View" service, creating a massive firestorm with privacy and security specialists. While Google has graciously removed public access to its "war driving" database, there are a myriad of websites that post the maps and data found by amateur War Drivers, such that anyone can easily locate and tap into an unencrypted Wi-Fi system. Parallel to war driving is war chalking, war walking, war jogging, and war bicycling, which is common in densely developed urban areas. The simplest iteration of these is to use chalk on the side of a building or sidewalk to show the presence of a vulnerable Wi-Fi system, telling anyone on the street about the unfettered broadband internet access, compliments of an often unwilling provider. There is actually a standardized list of chalk symbols indicating the type and availability of Wi-Fi signals, these symbols being available from en.wikipedia.org/wiki/War_chalking.

50/50

Joe Kusiak

Virtually all Wi-Fi access points offer some form of encryption. During the initial setup of the Wi-Fi system, the user is often requested to select an encryption method, or else "no encryption" is often the default setting, making the network accessible to anyone within range. The most common forms of encryption for Wi-Fi access points are WEP, WPA, and WPA-2. WEP (Wireless Encryption Protocol) is the oldest and least secure of the common encryption methods; while only having slight degradation in performance and speed, it is virtually useless against all except the least sophisticated hackers, with instructions on how to crack and defeat WEP being readily available on the internet. WPA (Wi-Fi Protected Access) is better than WEP in terms of security, but degrades performance a little more than WEP. On most contemporary home Wi-Fi access points, WPA-2 is the best of the commonly available encryption methods, but is slower and requires more computing resources then WPA; except for the most bandwidth intensive uses, the majority of users will not really notice the slightly slower performance of WPA-2.

Another security trick embodied in almost all Wi-Fi access points is the "Hide SSID" setting. SSID means "Service Set Identifier", also called "Network Name". At a minimum, the user should change the

network name to some meaningless name that is not readily connected to the particular system. The reason for changing from the factory default name (often the name of the manufacturer, such as "Linksys") to a non-descript name is that there are online directories with default encryption and password settings for unmodified Wi-Fi access points; hackers can easily break into networks that are only using the factory default settings. An even better trick, if available on the Wi-Fi access point, is to totally hide the SSID, meaning that the network name is not openly transmitted, and only those in range who know the network name can connect to it. While not foolproof or totally secure, hiding the SSID is a simple way to make it more difficult for hackers to find your network. If war driving through your neighborhood, hackers may likely miss networks with a hidden SSID, while picking up the other, possibly more vulnerable neighborhood networks.

Another feature that can be enabled to restrict unauthorized access to your home network is "MAC address filtering" (Media Access Control). Every device that can connect to the internet has a unique MAC address, usually a series of about six two-digit alphanumeric characters separated by periods. While MAC addresses can be counterfeited or spoofed, filtering only allows selected devices, as indicated by their individual MAC addresses, to access the network. By entering the authorized MAC addresses into the filter, and enabling the filter, only those approved devices can connect to the network. Likewise, the filter can prevent specific devices from accessing the network.

On my laptop computer and on my smart phone I can see several nearby homes that have Wi-Fi, some of which are not properly encrypted and accessible to anyone within range for any purpose, including illegal or other illicit activities. I cannot easily see networks with a hidden SSID. The unprotected household Wi-Fi networks are so vulnerable, when one neighbor had his home broadband connection out of service, and was waiting for the ISP to come and repair it, he illegitimately used another neighbor's Wi-Fi until his was repaired. Do you really want someone else using your network without your permission or knowledge? Secure your Wi-Fi, or face the possible consequences.

Up Coming Meetings

March 2, 2013-Julie Bell will present GnuCASH, a free open source program that works with Windows, Linux, and Macs. Julie will demonstrate the checkbook portion of GnuCASH, which is similar to Quicken for Windows. Members in good standing will also have a chance to win one of a number of 8GB USB 2.0 flash drives that are preloaded with free software.

April 6, 2013-Food, fun, and festivities will mark LCACE's gala 30th anniversary party. The day will begin with the election of officers, to be followed by Show and Tell and Ask the Gurus. Members must be present to win one of many door prizes. Some lucky person will win first prize, a Western Digital 2TB USB 3.0 silver My Passport portable hard drive. Remember you have to be a member to participate in the prize drawing. No party is complete without refreshments; birthday cake and fresh fruit will head the "goodie" list.

"How shall I torture you today? Put you on the rack? Boil you in oil? Make you call a technical support line?"

Door Prizes

January Winner

DeBorah Sirilla

Happy Birthday

February Birthdays

Tracy Berry

Winnie Frost

Mike Mc Enery

This months Recipes submitted by: *Linda Koudelka*

Recipe of the Month

Taco Salad
Serves 6-8

1 pound ground beef
1 package Taco Seasoning Mix
1 can (16 ounce) kidney beans, rinsed, drained, dried
1 medium head lettuce, torn, shredded, or cut up
2 medium tomatoes, chopped
1 medium onion, chopped
½ avocado, chopped (optional)
½ cup green pepper, chopped
1 cup shredded cheddar cheese – not sharp
2 cups coarsely crushed Taco Flavored Tortilla Chips a
(5 ½ ounce bag)
¼ cup (or more to taste) **Tasty French Dressing**
Salt (optional) and pepper to taste

Fix ground beef according to Taco mix directions. Cool.
Put all rest of ingredients in a very large bowl and toss with dressing.

Tasty French Dressing For Taco Salad
1 quart approximately

½ cup sugar
⅓ cup tarragon or wine vinegar
1 teaspoon Worcestershire sauce
1 teaspoon salt
2 or 3 small onions or dehydrated onions--regular onions better
2 cloves garlic, minced
⅔ cup ketchup or to taste.
2 cups salad oil (canola not olive oil)

Combine all ingredients in blender – mix until smooth.

Linda Koudelka

Lake County Area Computer Enthusiasts

Do you have computer questions
or need help with your computer?

Visit Lake County Area Computer Enthusiasts'
help desk for one on one help

Open to all

11:15 a.m.-12:15 p.m.
Grayslake Area Public Library
Rooms A-C

Saturday, February 2 Saturday, March 2
Saturday, April 6

Next Meeting

Saturday

October 13th

Meeting Agenda: http://lcace.org/agendas.htm

"L.C.A.C.E. Meetings are held at the Grayslake Area Public Library, 100 Library Lane, one Saturday a month unless otherwise posted on our web site and in the News Journal. Everyone is welcome. Doors open at 11:15 am for the help desk; the meetings start at 12:30 pm.

Future Meetings 2012

March 2
April 6
May 11
June 8