ORANGE COUNTY PC USERS GROUP

NIBBLES & BITS

annual christmas
fundraising raffle

raffle rules
on page 2

list of prizes
*will be given
to members
at meeting*

RULES OF THE RAFFLE

by Mike Lyons, ORCOPUG President

The Christmas raffle has always been the club's biggest money maker. The Tuesday, December 10 meeting at Coco's Bakery Restaurant in Fullerton is the only meeting of the year where you have to be a member to participate. If you don't see your name at the badge table, it means your dues have lapsed. Everyone needs to wear their name tags to place bids.

Starting at 6 p.m. all the raffle items will be put out on display. Each item will have a yellow sticky note with a number on it (corresponding to the number on the raffle prizes list) and a dish in front of it.

At 6:30 p.m., we will name each vendor and give a brief description of each donated item. Once we have finished describing the prizes, tickets will go on sale. Tickets are one dollar each.

There are two pieces to each ticket. Put one side of the ticket in the bowl and keep the stub. Your name badge will have a number on it. Write that *number* on the ticket you deposit in the bowl. This will speed up the process.

Please keep the ticket stubs you hold intact. It makes easier to check your numbers for winners. Members can put as many tickets as they choose into the bowls in front of each item. All tickets will be deposited into the bowls no later than 8 p.m.

At 8 p.m., we will check the bowls and add "ORCOPUG' ticket(s) to any bowl with less than five tickets until the count hits five. Our club ticket will be a different color for easy identification. If a club ticket is drawn, the club wins the prize and it is set aside for use in the monthly raffles.

This meeting is always a lot of fun. So, bring your smile and your wallet or purse and join us for a great meeting.

**PLEASE NOTE –
Members will receive a list of
the prizes at the meeting.**

feedback

Frank Bollinger
ORCOPUG, California

The wills and trusts presentation generated lots of questions (My usual method for determining the success of a presentation). Since I updated my trust earlier this year, a technical subject would have been better for me, but I was impressed by the presenter. She was friendly and patient, very different from my image of most attorneys.

Pim Borman
Evansville, Indiana

I made a public version of the Krupuk (an Indonesian food) video, http://sn.im/krupuk_public, with the addition of the nutritional data

Screenshot
from video

on the package. Feel free to forward this to anyone you think who might be interested! I plan to put it on my Facebook page also.

The taste is very mild (unless you get a spicy version, less popular). A bit similar to pork rinds, but not nearly so strong, with a subtle taste of shrimp.

Each chip has about 30 calories, with a negligible amount of fat. Deep frying is what adds the calories, of course. It would be best to carefully blot each chip with paper towels as it comes out of the fryer to remove as much oil as possible.

Indonesia used to be a Dutch colony, until after WWII when they fought for their independence. Poor populations often have the most diverse, tasty food since they have been forced to eat anything edible, finding out along the way what tastes unexpectedly good. The opposite is true too - the USA has about the worst cooking in the world, unimaginative, monotonous, and unhealthy to boot.

Dutch colonials, and after WWII Dutch soldiers returning from trying to quash the rebellion, brought a taste for Indonesian food back with them, and it remains an important addition to Dutch cuisine. Almost anywhere in Holland you can find Indonesian restaurants, especially popular since every-day Indonesian meals are tasty and inexpensive.

The meals are based on rice, with the addition of an endless variety of spices, condiments, sauces, and what have you. Krupuk is often added as a side dish, something to nibble on.

A rudimentary meal, called Nasi Goreng (literally"fried rice") consists of cooked and fried rice mixed with ham and some Indonesian spices, such as Sambal Oelek, an Indonesian equivalent of Tabasco. The dish is usually served topped off with a fried egg. Side dishes may be Sateh, pieces of pork or chicken stuck on small sticks, fried bananas, peanut sauce, and many other items I can't remember after all these years.

The famous Indonesian Rijsttafel (Rice Table) is usually served to a group of people or in a large restaurant, since it requires enormous effort. It consists of literally dozens of small dishes of tasty stuff, served with a small helping (to leave room for the rest) of rice.

I once enjoyed a minor version of that while in the military service. Our battalion commander was a former Dutch Colonial Army officer. He arranged a rijsttafel dinner in the officer's mess with the help of a military cook he had found who knew Indonesian cooking. A meal I'll never forget!

There are also Chinese-Indonesian meals, quite distinct from regular Chinese cooking. I did not eat it as often. Much of it is based on noodles ("Bami") instead of rice, with different spices and condiments. Very tasty also.

Favorite Shot

T his was taken while I was standing in front of (our) Uncle Lee's house, looking at the covered drive. It was January 12, 2005. Uncle Lee's house was in a small town called Confidence in California. It is a couple of miles from Twain Harte.

**Photo by
Edith Parker, Oakdale, California**

november keyword explained
cryptolocker prevention kit

CryptoLocker is Trojan horse malware which surfaced in late 2013. A form of ransomware targeting computers running Windows, a CryptoLocker attack may come from various sources; one such is disguised as a legitimate email attachment. When activated, the malware encrypts certain types of files stored on local and mounted network drives using RSA public-key cryptog-raphy, with the private key stored only on the malware's control servers. The malware then displays a message which offers to decrypt the data if a payment (through either Bitcoin or a pre-paid voucher) is made by a stated deadline. —Wikipedia

Bitcoin is a virtual currency. Image is for illustration only.

cryptolocker prevention kit

The SMBKitchen Crew and Third Tier staff have put together…a kit (that) includes an article on cleaning up after infection, but more importantly provides materials and instruction for deploying preventative block using software restriction policies. The articles provide instruction for installation.

In these documents Susan Bradley has added new information about additional methods to block it and explains the why and how used in the GPO and also summarizes the blog posts that we've made on how to exempt your frequently reinstalled apps or those that MUST run from the blocked location from your policies.

It is zipped up into a single file at www.thirdtier.net/downloads/CryptolockerPrevention-Kit.zip

This kit updated on a frequent basis. Check the updates at www.thirdtier.net/2013/10/cryptolocker-prevention-kit-updates and download the kit again.

cryptolocker thieves likely making 'millions' as bitcoin breaks $1,000

It's a classic phishing attack, except the malware is sophisticated in getting past antivirus programs, infecting computers via several surreptitious steps: after victims get the first spam email, the attachment that a victim opens downloads a separate application, which downloads malware that finally downloads Cryptolocker, Uttang Dawda, of the security software firm Fire-Eye, said.

Dawda says that tens of thousands computers have been affected and that the perpetrators, who appear to be in Russia based on domain name tracing, are likely bringing in millions of dollars in ransom payments.

…Bitcoin is key to Cryptolocker's continuation — the currency is anony-mized and means ransom payments can't be traced — but it was also a problem for Cryptolocker at first. Initial victims of Cryptolocker were willing to pay the ransom but couldn't because they didn't know how to make payments through Bitcoin or Moneypak, which was another form of accepted payment.

Earlier this month, the perpetrators changed tack, giving victims a second chance to pay the ransom. The ransom demands are now typically at 2 Bitcoin (roughly $2,000 today). The second-chance ransom rises five fold to 10 Bitcoin.

Meanwhile the value of Bitcoin has more than tripled since mid-September, when Cryptolocker was first detected, reaching an all-time high of $1,070 on November 27. That means the perps behind Cryptolocker will see the value of their collected ransoms get a boost too. http://onforb.es/18M82Cl

12 Tips
for a Hoax-Free Holiday

by Brett Montgomery

*I*n song, the 12 days of Christmas include *partridges, turtledoves, French hens, calling birds, geese and swans. In reality, scammers fly high on unsuspecting pigeons vulnerable to their holiday hoaxes. To avoid getting plucked, follow these tips for safe spending and a hoax-free holiday:*

1. PAY ATTENTION TO WEBSITE URLs. Online searches can lead you to scammer-run websites that unleash computer malware or collect credit card numbers for identity theft. Carefully read website domain names. Watch for unfamiliar vendors or missing letters, misspellings or other tweaks to the name of a legitimate company.

Pay special attention to the last letters: For example, www.tiffanyco.mn indicates a Mongolia-based website, not the legitimate, website for Tiffany & Co., www.tiffany.com.

2. STEER PAST SITES THAT LACK CLEAR TERMS AND CONDITIONS. Before ordering, check the "Contact Us" page for a phone number and physical address, and the "Term and Conditions" link detailing return policies and such. Unlike legitimate vendors, bogus websites are less likely to post these—or they'll provide them in a suspicious manner, such as via a faxed request only.

3. AVOID BUYING UNTENDED GIFT CARDS. Buy gift cards from a store's attended Customer Service counter or its website, rather than display racks, which are less secure. Fraudsters can peel off stickers to glean gift card codes, replace them in envelopes and wait for an unsuspecting shopper to buy them. Once purchased and activated, they enter stolen codes at the retailer website to make

online purchases – leaving the intended recipient with a useless card.

4. Shop on https sites only.

When buying online, don't provide your credit card or other information on any page without an "https://" instead of merely "http://". The "S" is for "secure." Even with an "https://" avoid using public hi-fi hotspots for online shopping or other financial transactions.

5. Beware of post-auction offers.

When shopping at online auction sites, never trust offers that arrive after you've lost a bid, such as when a seller claims to offer you the merchandise off-site.

6. Take care on Craigslist.

At Craigslist or when answering classified ads, deal only with sellers who provide a phone number that you can verify. Don't rely solely on email correspondence. Assume any request for wire-transfer payment is a scam; also be suspicious of prepaid debit card transactions. Using Paypal or a credit card are your safest bets.

7. Avoid deals that are too good to be true.

Stay clear of prices from private sellers that are too good to be true or tied to hard-luck stories, such as a need to sell quickly because of divorce or military deployment). These are common scams to get advance payment—and you'll likely get no merchandise.

8. Beware of holiday e-cards from unnamed

friends or admirers. Delete these if you don't know the sender or even if they're from webmaster@ hallmark.com. These mass-sent greetings likely contain malware. Legitimate card notifications should include a confirmation code to safely open the card at the issuing website.

9. Avoid emails claiming that FedEx, UPS, DHL or

the U.S. Postal Service has an undeliverable package with links for details. The links will install malware that can log keystrokes to steal computer files and passwords. Unless you previously provided an email address, courier services won't contact you this way.

10. Don't fall for a mailed postcard about an

undeliverable package. Hmmm, funny that the courier has your address but couldn't provide delivery. This scam baits you to call for details—at which point you'll be tricked into making an expensive overseas call and/or to revealing your personal and financial information. Look up the callback number yourself if you're curious.

11. Be mindful of charity scams.

Be suspicious of email solicitations unless you have previously provided your email address to a charity. Never give cash to charities. And request proof materials be provided and authenticated before providing a credit card to callers or a check to door-to-door solicitors.

12. When giving or receiving computer

devices, secure them with comprehensive security suite software before use. Do an online check of vendor reputations before installing mobile apps. When transferring files with a flash or portable hard drive, use a secure USB stick that encrypts information.

Used with permission from Identity Theft 911. Source http://www. idt911blog.com/2013/11/12-tips-for-a-hoax-free-holiday/ Identity Theft 911, www.idt911.com, is the nation's premier consultative provider of identity and data risk management, resolution and education services.

converting automatic numbering to manual numbering

by Allen Wyatt

Steve notes that Word's auto-numbering is not suitable for documents that are to be imported into page layout programs such as Adobe InDesign. He wonders if there is a quick way to replace auto-numbering with manual numbering, in the same way that you can convert field text to plain text.

The answer is yes, there is a quick way. Simply follow these steps:

1. Open the document whose numbering you want to convert. (You may want to open a copy of the document so that you don't mess up the original document.)
2. Press Alt+F11. Word displays the VBA Editor.
3. Press Ctrl+G. This opens the Immediate window.
4. Type the following in the Immediate window:

ActiveDocument.Range.ListFormat. ConvertNumbersToText

5. Press Enter.

That's it; all the auto-numbered lists are changed to manual numbering. There are a couple of gotchas related to this approach, however. First, it may appear that your numbered lists no longer line up properly. This is because any custom tab stops set for the lists are deleted and Word reverts to using the default tab stops. This shouldn't be a huge problem, as you are doing this conversion in preparation for importing the document to a page layout program. (The tab stops in that program should take precedence over any you have set in Word.)

The second gotcha is that if you applied the auto-numbered styles using lists, then the numbering isn't really gone. You can apply it again by simply selecting the paragraphs in the lists and pressing Ctrl+Q.

If you would rather not mess with the VBA Editor, then there is another approach you can try out—save your document in RTF format. Many page layout programs (such as InDesign) use a different filter for importing RTF files, with the result that the numbered lists are converted automatically to regular numbers.

WordTips is your source for cost-effective Microsoft Word training. This tip at http://word.tips. net/T010247_Converting_Automatic_Numbering_to_ Manual_Numbering.html applies to Microsoft Word 97, 2000, 2002, and 2003. You can find a version of this tip for the ribbon interface of Word (Word 2007 and later) at http://wordribbon.tips.net/T010248_ Converting_Automatic_Numbering_to_Manual_ Numbering.html

csv file opens with data in a single column

by Allen Wyatt

Jan uses a program to create a CSV file. This file can then be opened in Excel for further analysis. When Jan double-clicks the CSV file in Windows, Excel starts and then loads the file. The problem is that the file, when opened, isn't parsed by Excel. Instead of the comma-separated values being in different columns, every record appears in a single column.

The reason for this behavior is probably quite simple and has to do with the format in which the data is stored in the CSV file by the non-Excel program. To understand that, it is critical to understand how Excel opens CSV files.

When you open a CSV file in Excel (either by double-clicking in Windows or by using File | Open in Excel), the program treats any commas in the file as delimiters. This makes sense; after all, the file is supposed to contain comma-separated values (CSV). You cannot override this automatic filtering when opening the file.

So, how does Excel treat the incoming data? Consider, for a moment, if the CSV file contains the following four records:
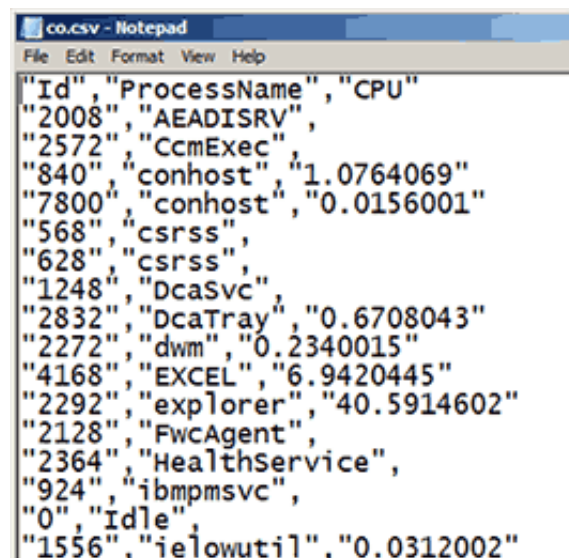
> a,b,c,d,e
> "a,b,c,d",e
> a,"b,c",d,e
> "a,b,c,d,e"

As far as Excel is concerned, the first record has five fields, separated by commas. The second record has only two fields, "a,b,c,d" and "e." The inclusion of the quote marks around "a,b,c,d" causes Excel to treat the string as a discrete unit. In other words, Excel ignores any commas that may appear between the quote marks.

Given the effect that quote marks have, you can probably figure out how Excel interprets the third and fourth records. In this case, the third record has only four fields, and the fourth record is interpreted to have only a single field.

What does this have to do with the CSV file that seems to be loading incorrectly? It is very possible that the program creating the CSV file is putting a pair of quote marks around each record. This would cause everything in the record to be treated as a single field by Excel, which means it ends up in a single column when the CSV file is loaded.
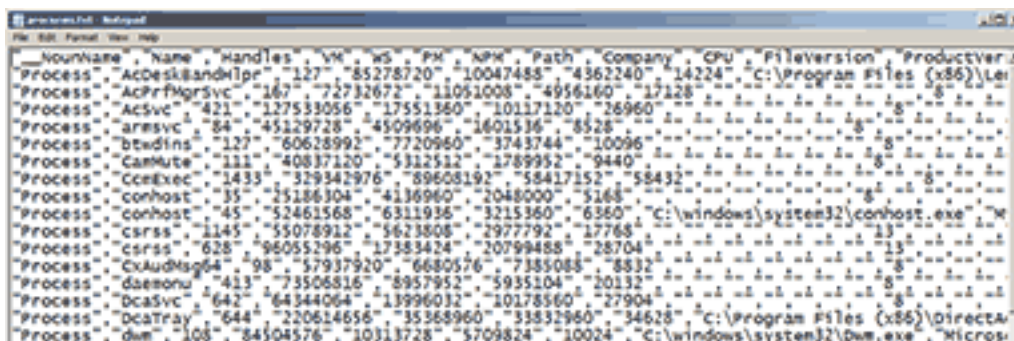
There are a couple of ways to verify this. The first is to simply open the CSV file with Notepad and look at each record. (Right-click on the CSV file in

Sample CSV file in Notepad

Sample of an extensive CSV file with delimiters in Notepad

Windows, choose Open With | Choose Program, then choose Notepad.)

Another way is to rename the CSV file so that its extension is not .csv but .txt instead. When you choose to open this file within Excel, the Text Import Wizard is started. Choose Delimited, click Next, and then you can see what delimiters are chosen. Pay attention to the Text Qualifier; if you change it, you can immediately see at the bottom of the dialog box how Excel interprets the file's records.

If you find that there are extra quote marks around each record in the CSV file, there are three things you can do. The first is to change the program that creates the CSV file so that it doesn't add the extra quote marks—you'll then be able to import with no problem. The second is to go ahead and load the CSV file into Excel, such that each record is in column A. Note that the surround quote marks are gone, stripped out by the import process. This means that you can

now use the Text to Columns wizard to separate the data in column A into individual columns.

Finally, the third thing you can do is to create a macro that will open the CSV file and parse it for you. This is particularly helpful if you will be opening, over time, many CSV files that have the exact same format. Your macro could be as elaborate as desired, even formatting columns and processing data as it is imported. Ways to create macros such as this are found in other issues of ExcelTips.

ExcelTips is your source for cost-effective Microsoft Excel training. This tip at http://excel.tips.net/T003002_CSV_File_Opens_with_Data_in_a_Single_Column.html applies to Microsoft Excel 97, 2000, 2002, and 2003. You can find a version of this tip for the ribbon interface of Excel (Excel 2007 and later) at http://excelribbon.tips.net/T011264_CSV_File_Opens_with_Data_in_a_Single_Column.html

Other tips on the Excel.tips.net website

CSV files—

you'll like what they can do for you

CSV is a common, relatively simple file format that is widely supported by consumer, business, and scientific applications.

by Linda Gonse

You may not have heard about CSV files, or you may have heard of them but don't know anything about them. So, of course you don't use them.

But, if you use a spreadsheet program, such as Excel, OpenOffice Calc, Quattro Pro, Calc XLS, Gnumeric, LibreOffice Calc, Numbers, Google Spreadsheets, Calc XLS, among others, you would find CSV files can be very useful to you.

Before explaining why, let's take a look at what a CSV file is. CSV stands for Comma Separated Values. Sometimes it is called Character Separated Values, because the separa-tor character does not have to be a comma, but can be a semicolon, tab, space, or another character the user may designate.

The CSV file is based on an existing spreadsheet file. The CSV format converts the tabular data into a simple, single line of plain text which typically represents one record (row). Within each line of plain text, commas separate each of the data that appears in adjacent colums in the spreadsheet.

Each spreadsheet program has the capability of saving a spreadsheet as a CSV file. CSV files can also be saved as TXT files, because they only contain text without any formatting or program coding.

CSV files are not a new invention and even predated personal computers by more than a decade. The comma separated lists were used by IBM FORTRAN compilers in the 1960s, as well as later computers and programs. When punched cards were used for input in earlier corporate computers, the CSV format was easier to type than columnar data. And, incorrect results due typing data in the wrong column was largely eliminated.

A simple spreadsheet such as this:

States	Abbreviations	Capitals
Alabama	AL	Montgomery
Alaska	AK	Juneau
Arizona	AZ	Phoenix
California	CA	Sacramento

would look like this in a CSV format:

> States,Abbreviations,Capitals
> Alabama,AL,Montgomery
> Alaska,AK,Juneau
> Arizona,AZ,Phoenix
> California,CA,Sacramento

The top row is the header row and the records following it each have the same sequence as the headings (called fields).

(Additional rules for separating data in CSV files and simple explanations for implementing them appear at http://en.wikipedia.org/wiki/Comma-separated_values)

Now, you might wonder why you would want to reduce a spreadsheet to its bare bones data anyway.

Suppose you need to share a spreadsheet with someone, and you are using Excel and they are using Numbers. They will not be able to open, view, and edit your spreadsheet. Or, if your file was created on a Mac and your friend is using a Windows computer — the spreadsheet file will not open. How can you share the spreadsheet you created with someone who is not using the same program as you, or is not using the same platform as you are?

Or suppose you want to save your email program's address book on another disk, another computer, or in another email program. How do you do that?

This is when CSV files are necessary and invaluable. Whatever program you are using, on whatever machine or platform you are using, you can open and view a CSV file created elsewhere. Proprietary database formats in email programs (such as Outlook) also rely on CSV files to convert their data to plain text so it can be easily read by you.

"CSV is a common, relatively simple file format that is widely supported by consumer, business, and scientific applications," Wikipedia said.

In addition, CSV files may be significantly smaller when large amounts of data are contained in a spreadsheet. For that reason alone, a CSV file can more conveniently be sent in an email than the spreadsheet itself.

Details on how to import (open) and export (save) a CSV file in Excel, are at Microsoft's support page at http://bit.ly/1bXKA22 For other programs, go to the software developer's webpage, or do a search using Google or Bing for creating a CSV file in your spreadsheet program.

Sample of a large database saved to the CSV format and viewed in Notepad

Image from http://www.pubassist.com/articles/convertfromquickbooks.asp

adventures in video making and youtube

by Pim Borman

Windows Live Movie Maker is a pretty nifty program. It lets you edit, rearrange, and combine individual movie clips, I used my Canon Powershot G15 camera, which has nice image stabilization available for movie taking.

Next time I'll know not to use the camera in portrait mode, to avoid the awkward vertical clipping of the oil frying shots, although for those scenes it was not too limiting.

The Windows program converts your edited movie to different wmv (Window Movie Format) files, differing in size according to what you want to do with it. Output for email ends up as a 35+MB file, with enormous quality loss, and still too big to attach to most emails. The default wmv output was over 460MB, with good retention of image quality.

I have used Any Video Converter in the past to convert movie files. It is pretty good, but no longer free. At least, the current free trial version is badly crippled. I found another, better, and completely free video converter, called Video Converter by SweetPacks, that worked just fine. I think it may be an Open Source program, since it is also available for Linux.

I converted the movie to AVI (Apple) format, but that file was still 380+ MB. I compressed that AVI file to a smaller AVI file of about 35 MB, but that again suffered from loss of quality. I tried to mail it using Google Mail, but it was deemed too large.

Google suggested sending it via the Google+ Cloud, but that procedure seemed to take forever. However, it reminded me of YouTube.

Recently I had extricated myself from Google+ (for the second time!) because I got tired of all the unsolicited messages it kept sending me. It warned me at the time that it would cut off my YouTube access.

Sure enough, I was not allowed back to YouTube until I reinstated Google+. My old videos were still there, and YouTube gladly sucked up the large wmv file of my Krupuk movie. That took about 45 minutes while I did something else.

I forgot that YouTube takes care of converting your video to its own format.

Once in place, YouTube noticed some (residual) shakiness in my video, that it offered to correct — accepted. Afterwards it even did some image stabilization for me. I forgot what a great program it is.

I made a second version of the video suitable for unrestricted publication, omitting some personal data and adding nutritional information. I uploaded it to YouTube with a "public" setting. I used Snipurl to convert the impossible URL of the video to easier http://sn.im/krupuk_public. And there it stands.

When I tried to upload a link to the YouTube video to Facebook, it would not accept the snipurl version. I guess there have been instances where these URL simplifiers were used to introduce malware. The awkward URL provided by YouTube worked just fine.

Pim Borman is a retired chemist. He was newsletter editor and webmaster of the SW Indiana PC Users Group before it disbanded in December 2008. His email address is swipcug@gmail com.
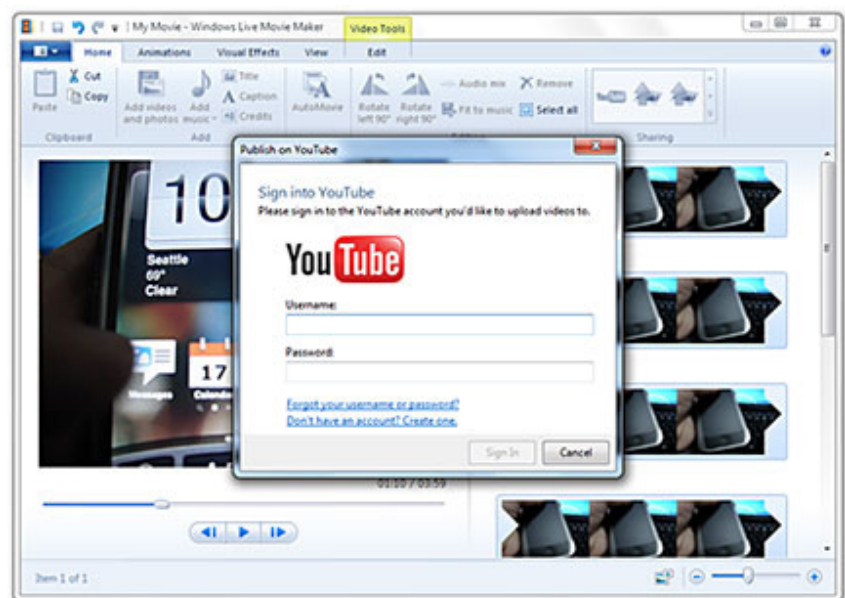
ask leo!
by Leo A. Notenboom

will a new computer burn dvds faster?

Will a new computer be a lot faster at making a homemade single-layered DVD? Today, it took five hours for DVD Flick to process the memory already stored on my computer. The video is in mp4 format; the DVD-R was a 4X single layer.

When you're burning a CD or DVD, the computer isn't typically the weakest link; it's the CD/DVD burner. When they write, CD/DVD burners operate at some maximum speed of rotation and how quickly a burner spins depends on its hardware and how fast it can write the data to that disc.

But I think something else might be going on here. You mentioned that your original video is in MP4 format. That's not a format that is written to DVD.

writing to DVD

DVD format is definitely encoded and compressed, and sometimes encrypted, but it's a different format. It's certainly a very different format from MP4.

In your case, the DVD-burning operation may have taken a long time because the computer's processor had to first convert it from one video format to the other. That can be a very CPU-intensive operation. In fact video conversion is often used as an example of a process that demands a lot from a computer's CPU.

If that is the limiting factor, then a new computer with a faster processor might well be the answer. Depending on the video conversion software being used a multi-core processor can sometimes dramatically reduce the amount of time that the conversion process takes.

Again, that depends on the specifics of your current CPU: how fast it is, how much RAM you have, and how fast your disk is. Your current computer may already be able to handle the conversion process and a new computer won't make that much of a difference.

If it's not the conversion process, then it is the speed of the drive that's limiting how quickly the bits can actually get written. You may want to try burning another type of file (say any type of files to create a data CD or DVD) to make sure that it's not the drive.

But I strongly suspect from your description that it's the conversion process.

Used with permission of Leo A. Notenboom, Ask Leo! http://ask-leo.com.

Source: http://askleo.com/will-a-new-computer-burn-dvds-faster/

there was a
ghost in my computer!

by Linda Gonse

R ecently, I participated in an online help forum at Hewlett Packard regarding a printer I no longer had. But, one of its files was still loading on my computer, and at shutdown it had to be forcibly closed. I was looking for a solution on where the "ghost" file was located so it could be deleted. The following is a days-long series of discussion board posts between HP and me. You may never have the exact problem, but many of the steps I followed may come in handy for you to use to troubleshoot your ghosts.

Me

10-04-2013 — I upgraded my OfficeJet 7300 All-in-One printer to an OfficeJet 8600 All-in-One.

The problem is just before shutdown on my Windows XP SP3 computer a message pops up saying a program file did not close. It is HPSilentPatch_Wnd5370c.

I researched it and it appears to be a leftover file from the (HP OfficeJet 7300 All-in-One) scanner. Although I made sure all the old HP-related startup files have been unselected in MSCONFIG, this file continues to be an annoying holdover. Where is it located, so I can delete it? Or, is there a registry key that can be changed to keep this file from appearing on shutdown?

HP

10-07-2013 — The HPSilentPatch_Wnd5370c file would have been a patch that you downloaded and installed, so it should be a file somewhere in your programs.

So use the Search function in Windows XP and search for that specific file and then it will tell you where it is located so you can remove them all.

Once you've done this, restart the computer and everything should be resolved with this file.

And with that answer, my saga began!

The "ghost" file stayed hidden despite all my attempts to exorcise it.

Me

10-07-2013 — I did a computer-wide search, including system files and hidden files, for HP SilentPatch_Wnd5370c without results.

HP

10-08-2013 —*The reason it didn't find anything may be because the file could have been renamed at some point.*

To search for it you would need to know the name, so do the same search, but look for 7300 instead of the file name you tried before. If you can remember the exact name of the printer (such as 7310, or 7310xi) then search that instead of just 7300.

Me

10-10-2013 — I deleted a couple of folders for the 7310 that contained many files. The folders and paths are:

C:\Drivers\HP Officejet 7310
C:\708ef726d0fe278e16\1_downloads\hpscanjet-upgrade
I rebooted.
The file message appeared again at the next shutdown.

HP

10-11-2013 — *Run a disk cleanup on the computer. Then once you've performed the disk cleanup, please restart your computer.*

If the file is still there after this step, download and run the HP Print and Scan Doctor. It should hopefully be able to get rid of the file or move it so that it stops popping up.

Me

10-11-2013 — Before running Disk Cleanup, I followed Microsoft's directions and deleted several application files:

- HP PSC & OfficeJet 4.7 (related to the 7310 printer)
- Java 6 & Updates
- Java 7 & Updates
- J2SE Runtime Environment 5.00 Update 11

I rebooted and ran the disk cleanup. Rebooted again, and ran CHKDSK for several hours.

Next, I ran the HP Diagnosis Tool but only the in-stalled printers were shown in the list — not the 7310 printer.

Finally, I ran CCleaner and cleaned out file problems in the Registry: Shared dlls, Unused file extensions, Active X & Class Issues, Type Libraries, and Installers.

Before shutdown, however, I got the popup saying that the old HP file still had to be closed!

HP

10-14-2013 — *The only other option is to perform a system restore on your computer to a time before the Office-Jet 7310 was installed. Any files that have been added to the computer since then would be gone, so it is up to you if this is a step you want to take.*

Me

10-14-2013 — A system restore to a time before the Office-Jet 7310 was installed is not possible. The 7310 was purchased some years ago and removed possibly six months ago, and I am using an 8600 OfficeJet.

HP

10-14-2013 — *Please call into HP Tech Support for your area and see if they have any other information on this file.*

My final post three days later—

10-17-2013 — **The problem has been solved!** I downloaded Ashampoo Startup Tuner, a free program recommended by several computer users online. It detects all the programs in the startup folder, categorizes them, and shows the icons for the programs they belong to. It was easy to see a folder for the 7310 with its update.exe file associated with the 5370c error. I didn't suspect the folder before, because it was named sj666. (CCleaner also displays similar information, but the Ashampoo program allowed me to pinpoint the location of the problem.)

At last, there is no popup. What a relief!

ask pamela

How do I transfer Kindle e-books to my Apple iPad?

You can move the books from one device to another via "Manage My Kindle" on amazon.com using a web browser.

1. Sign into your account
2. Select Manage My Kindle
3. Next to the Digital Content Column on the left, find the book that you want to move to the iPad and select action on the right. You can move the content from device to device there.

Alternatively: You can use the application that Amazon provides for users to download and read Kindle books on iPad or iPhone called "Kindle."

After you downloaded the Kindle for iPad APP, you can use it to re-download your kindle books from the Amazon store into an iPad. You can find this application in the App Store on your iPad. Just type in "Kindle for iPad" in the App store search box and the free "Kindle" app will usually be the first app that appears.

by pamela tabak

I have a flatbed scanner and I notice that when I copy or scan it cuts off about ¼ of an inch at the top of the page; what is the reason?

Check the icons displayed on the case of your scanner. They will show you where you should place your original and also if the printed side should be on the top or underneath. If the printed scan is being cut short each time you scan, it is probably because you are putting the paper to be scanned at the wrong end of the glass.

I have been using Adobe Reader for many years and now I am unable to open PDF files when they are sent to me by email. Can you explain what has happened?

If you have not updated Adobe Reader recently you may not be able to open the PDFs that are written in the latest version. In addition, if you are trying to open them on your mobile device, like an iPad, you will need to download the Adobe Reader APP that is available free from the App Store. With these in place you will be able to open all PDF files that are sent to you.

Used with permission. For more questions and answers check the ComputerTutor's site at http://www.computertutorinc.net/ frequently-asked-questions-2/

phishing

identity theft now considered the #1 web threat

by Ira Wilsker

In several past columns, I have warned readers about the various methods and techniques that cyber crooks use in order to steal their identities. According to Wikipedia (en.wikipedia.org/wiki/Phishing), "Phishing is the act of attempting to acquire information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication."

While phishing has been around for several years, it has now become the major method of online identity theft; according to the cyber security service Webroot, "Phishing 2.0" (the latest iteration of this type of phishing) is currently the #1 web threat facing computer users.

In the past, it was thought that only inexperienced and unknowing computer users were vulnerable to the original "Phishing 1.0" level of phishing attacks, as these unfortunate users would blindly click on any links in an email, and give personal and credit card information to all who asked.

In order to protect these highly vulnerable individuals, as well as other more experienced users, the computing industry has upgraded web browsers and security software with the capability to detect most phishing attempts, and alert the user of the risk, or otherwise stop the phishing attempt in its tracks.

Not to be impeded by the security improvements incorporated into newer browsers and security suites, and losing a major source of substantial but illicit revenue, the cyber crooks who profit handsomely by stealing the identities of others have created new and improved Phishing methods referred to by the security industry as "Phishing 2.0."

According to Webroot, in discussing Phishing 2.0, "(Phishing 2.0 is) ... a new generation of sophisticated phishing attacks now target(ing) businesses. These phish evade traditional antivirus and anti-phishing products. Using targeted information —often gathered from social media sites — they fool even security-savvy employees into divulging sensitive information or visiting websites that infect machines with dangerous malware."

One very recent example of such a phishing expedition has been the recent deluge of emails directed against the faculty and staff of Lamar University, simultaneously directed

Turn to next page

at both their official ".edu" email addresses and their private email addresses.

These multiple emails addressed to many of the employees are an apparent attempt to eventually bypass the security systems that are already in place; it does not really matter how good the university or corporate firewall or protective software, as many of the employees are also receiving redundant Phishing 2.0 emails at home, where the security may be likely to be weaker (or non-existent) than the professional security systems employed by the organizations.

While the sophistication of the Phishing 2.0 attacks are intended to penetrate most common security methods, the simpler Phishing 1.0 still can wreak havoc on individuals and their employers.

Over the past few days, I have been made aware of multiple university employees, as well as employees of some of the other nearby colleges, receiving the following email at both their work and home email accounts; this email arrived numerous times over a two-day period at my home and work email addresses, as well as many of my acquaintances, both Lamar University faculty and staff and the faculty and staff of the other local lower division colleges:

From: Lamar Help Desk <helpdisk@lamar.edu>

To: Recipients <helpdisk@lamar.edu>

Sent: Thursday, November 21, 2013 2:20 AM

Subject: Mailbox Re-Validation
Your Lamar Password will expire in two (2) Days, click the link below to validate your e-mail http://lamar(xxxxxxx).eu.pn/login.php

Thanks
Lamar Help Desk

Knowing that a percentage of recipients will always click on email links, it is inevitable that some users will be duped into doing that. At first glance, this email appears to be legitimate, unless the targeted victim looks closer at it.

The item that attracted my primary attention is that I do not have a "lamar.edu" email address, as I teach at one of the other local colleges, but my wife, who does have a "lamar.edu" email address also received multiple copies of this Phishing email; I had also received inquiries for other college faculty and staff who received this email.

While the simple header on this email appears to indicate that it is from the "Lamar Help Desk," notice that the word "helpdisk" is misspelled, with the suffix being "disk" rather than the correct "desk."

The web link included in the email would also raise suspicion as to the real destination of the reply.

While the beginning of the web address (URL) clearly says "lamar," there is a three word suffix (which I purposely redacted) creating a

Source of phishing emails. Is a Texas university located on Pitcairn Island?

compound word after the prefix "lamar."

Generally, the abbreviation ".eu" might indicate Europe, but this website actually has an upper level domain of ".pn" indicating that it is registered in the Pitcairn Islands.

For those who may recognize the Pitcairn Islands in a historical context, these southern hemisphere, western Pacific islands are the home of the descendents of the mutineers of the famous British ship "The Bounty."

I really do not see a Texas university having a major help desk located there.

Examining the full headers of the phishing email, it appears to have originated on a server at the University of California — San Diego (UCSD), and been questioned

by an IronPort spam filter, but still was delivered to many of its intended recipients.

Many of these phishing emails also were not stopped by the generally very good spam filters utilized by several of the popular webmail providers, such as Gmail and Yahoo mail. It is possible that a hijacked account at UCSD was "milked" for information, providing the cyber crook with a list of attractive target ".edu" domains; it is also quite possible that the hijacked account at UCSD became a "zombie," unknowingly sending out spam emails at the request of a "Zombie Master" who may control thousands of compromised computers.

I also performed a basic digital trace of the link on the email, and found that the server that it is using is actually located in Kiel, Schleswig-Holstein, Germany. The registered owner of the server has a Russian sounding name, probably a pseudonym.

Only generic information about the webhost was available, rather than the more common detailed contact information (also often bogus) of the actual website owner.

Using a "sandbox" on my computer (a virtual machine where nothing can get out and threaten my home computer), I tried to access the phishers'

website, but was blocked by my memory resident security suite; even though I was likely safe, I decided not to continue to load the bogus website.

Based on prior experience, the website would likely appear to be a legitimate Lamar University website where users would be asked to enter their username, old password, and new password. Since this is a bogus

website, the new password would likely not be implemented, but either of two events will be likely to occur,

Top image: Destination of the phishing emails.

Bottom image: Destination details of the phishing emails.
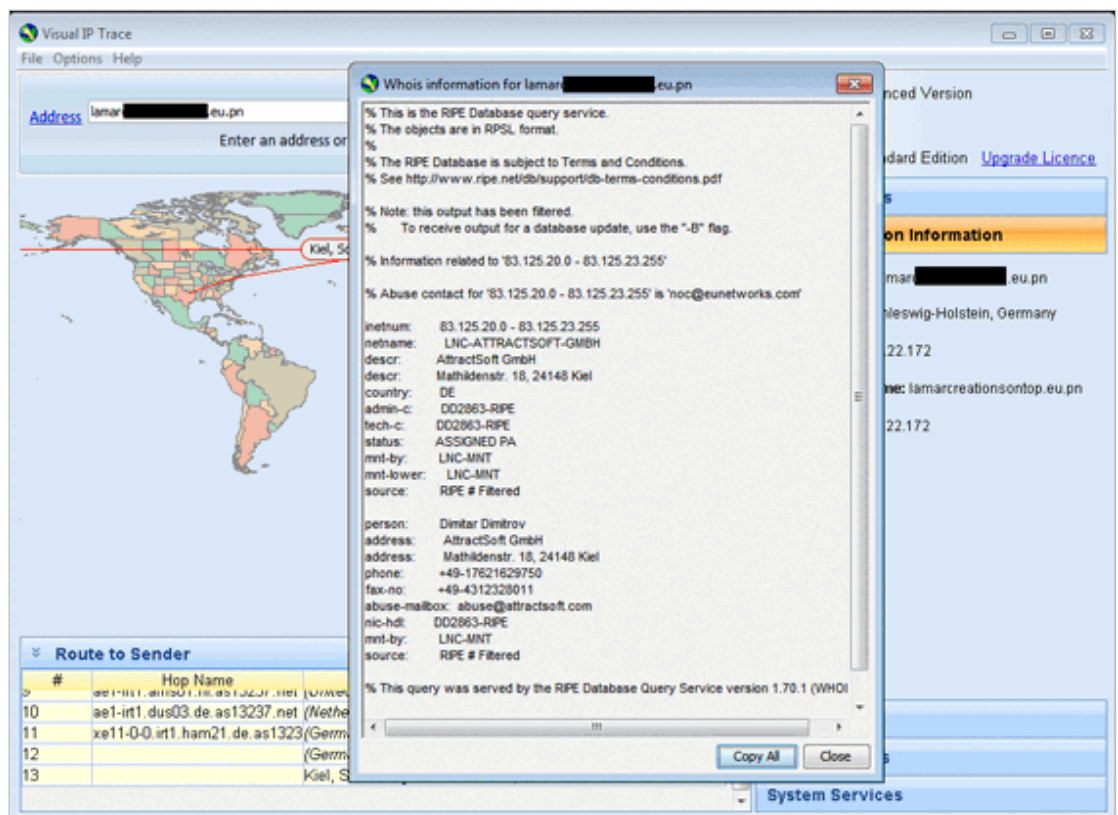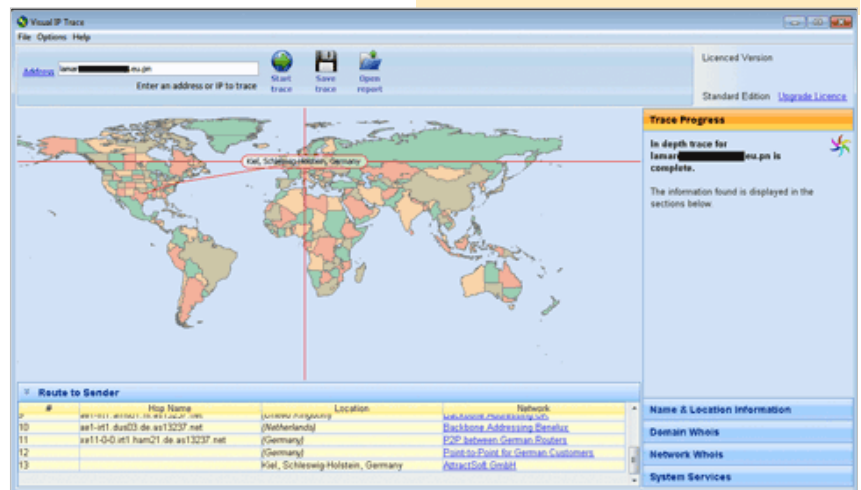
both leading to the same nefarious results. The cyber crooks could either use the current username and password entered by the victim, or can change the password to one unknown to the legitimate user, preventing his access to any Lamar University system.

This username and password is the necessary first step to logon to any computer at the university, allowing for email access as well as access to other data components at the university. Since the cyber crook now has an apparently legitimate Lamar University username and password, the email system now becomes available to the crook, as well as access to any accessible network drives.

The amount of valuable data that can be stolen is immeasurable.

The entire email history of the individual can now be downloaded, giving the crook information about students, family, and any other content, including passwords to external web services.

It would be quick and easy for the crook to determine external web accounts that are connected to the now stolen Lamar.edu email accounts, go to those websites, click on the "forgot password" links, and have the external password or a reset link sent to the purloined email box.

Not just would this process continue until the legitimate user contacts the real helpdesk and resets his password, but the identity theft will likely continue, until the legitimate user also changes any other external passwords linked to that compromised account.

WEBSITES and SOURCES

- http://hosteddocs.ittoolbox.com/Phishing_and_Web_Security_WP_Mar13.pdf

- http://resources.idgenterprise.com/original/AST-0102181_EECDatasheet_from_KnowBe4.pdf

- https://en.wikipedia.org/wiki/Phishing

- http://www.consumer.ftc.gov/features/feature-0014-identity-theft

- https://www.annualcreditreport.com

This might just seem like a local issue, but Lamar, like most other universities, has faculty and staff engaged in research, such that the theft of the research (intellectual property theft) could result in financial loss, loss of a competitive advantage, and even a threat to national security, all because an employee clicked on an email link and thought that he was resetting an expiring password.

If anyone has ever clicked on this or the millions of similar emails asking for passwords, usernames, or credit card number confirmation, or responded to phone calls or text messages informing the victim that his debit card number and PIN needs to be confirmed in order to reactivate the card, that person is likely to be the victim of identity theft.

While Phishing 2.0 is primarily intended to steal information from businesses and other organizations,

the crude technology of the archaic, simple, but still effective Phishing 1.0 will still snare plenty of prey. In addition to the immediate changing of passwords (after scanning and removing any malware that may have been planted by the cyber crooks), it will likely be necessary to change other passwords, check credit bureau reports (totally free from annualcreditreport.com) and challenge any questionable postings.

Complete information on dealing with identity theft can be found on the Federal Trade Commission website at www.consumer.ftc.gov/features/feature-0014-identity-theft.

Play it safe; be suspicious, adopt a policy of never clicking on links in emails, social networking sites, or instant messages (text messages).

If, for example, you get an email apparently from your bank or a major retailer asking you to click on a link to verify information or sign up for something, do not perform that task by clicking on the link, but instead going directly to the known website of the source.

Be careful of what you click on; the results may be devastating.

Read Ira Wilsker's weekly computer and technology column in the Examiner at http://www.theexaminer.com/feature/ira-wilsker You can email Ira at iwilsker@sbcglobal.net

Dealing with this factor caused some stress along the way.

my toughest computer
support request

by Frank Bollinger

From time to time, friends and neighbors who know I've worked with computers ask me for help. One such request, although ultimately successful, was both a technical and emotional challenge.

One of my neighbors had a phone message from a lady friend who had subsequently passed away. The message was stored on a centralized voice mail system, so he did not have a physical copy of it. He wanted to preserve the message and provide copies to two acquaintances. Although he could still play the voice mail on his phone, the message would eventually be purged by the system. Having a laptop PC with a modem and remembering the days of dial-up bulletin boards and Internet, I thought it would be fairly easy and told him we could do it.

Initially I tried to get a computer readable copy of the voice mail, but the support technician said they couldn't do it.

Next, I began researching PC software that could call the voice mail system then play and record the message. Unable to find a single program capable of doing the entire job, I looked for ways to do various subtasks. The audio recording and editing program, Audacity, would record the message but I couldn't find anything able to respond to the voice mail system's prompts for things like password and menu choices.

So, I tried using an actual phone with a device that connects the handset to a PC microphone jack. This allowed me to control the voice mail system and record the message with Audacity. Unfortunately, this method generated background noise that was louder than the actual message. Although I now had retrieved and recorded the message, the result was unusable.

The emotional element involved the relationships between the people who were part of this story. Apparently my neighbor and another man both had been interested in the deceased woman. On top of this, my neighbor had promised a copy of the message to his competitor. I knew both men and dealing with this factor caused some stress along the way.

After a couple frustrating months without useful results on the software side, l attached a voice recorder to the phone and recorded the message without the computer. The recorder came with software that copied the recording to a PC in .wav and .exe formats. I used the .wav file to create CDs and sent the .exe file as an email attachment. That gave my neighbor two ways to distribute the message.

In conclusion, mission accomplished, even though it proved more challenging than expected.

Christmas Gift Ideas

PetChatz

PetChatz allows you to interact with your pet while you're away. Using your phone or computer you can alert your cat or dog to go to the device where you can communicate through video and sound, your personal scent, and deliver treats.

(Video demo) http://www.incrediblethings.com/tech/petchatz-greet-treat-your-pup-while-youre-away/

Driftwood iPhone Charging Dock

Docks for iPhone and iPod are handcrafted in Maine from natural driftwood. Velvety smooth from the stony shores of Maine. The juxtaposition of organic and artificial, contemporary and timeless transforms personal electronics into functional art. http://www.uncommongoods.com/product/driftwood-iphone-charging-dock

Creative Outlet

Pivotable Surge Protection with an adjustable power strip that holds large adapters in EVERY outlet! Six adjustable outlets. Finally, every plug fits. http://www.quirky.com/shop/best-sellers

Multipurpose Sensor

What's going on at home? Stay updated with Spotter on—from anywhere. Monitor motion, sound, light, temperature, and humidity from your mobile device. Use for baby monitoring to washer/dryer notifications; the possibilities are endless. http://www.quirky.com/shop/609-Spotter-Multipurpose-Sensors

Push MAG Lights

Small lights with magnets attach to refrigerators, hallways, or anywhere you can use magnets. Use as lighted markers to highlight important things around your office or home. Just push the top to turn on and again to turn off. http://www.coolstuffexpress.com/push-mag-lights.html

Gift ideas compiled by Linda Gonse

email addresses

Bollinger, Frank
frbollinger@earthlink.net
Boutwell, Lloyd
Boutwell65@yahoo.com
Gonse, Linda
editor@orcopug.org
Jackson, Walter
wvjaxn@charter.net
Kaump, LeRoy
leroy_kaump@hotmail.com
Klees, Larry
lklees@dslextreme.com
Leese, Stan
stanleese@dslextreme.com
Loehr, Lothar
lothar@orcopug.org
Lyons, Mike
mike@orcopug.org
Moore, Charlie
charlie@orcopug.org
Musser, Dave
dmusser@worldnet.att.net
Westberg, Carl
carl@orcopug.org
Wirtz, Ted
twirtz@pacbell.net

time for renewal?

NOVEMBER 1	Louise Applequist
DECEMBER 1	Bob McDonald
	Carl Westberg
JANUARY 1	Linda Gonse
	LeRoy Kaump
FEBUARY 1	Charlie Moore
MARCH 1	Frank Bollinger
	Kevin Joe

submitted by Charlie Moore

november raffle winners

Mixcraft Pro Studio	Value $50
Bob Schmahl	Winner
Mixcraft Pro Studio	**Value $50**
Frank Bollinger	Winner
Mixcraft 4	**Value $39**
Bill Bowman	Winner
Mixcraft Pro Studio	**Value $50**
Charlie Moore	Winner

submitted by Charlie Moore

cryptolocker updates for ug members

The Greater Cleveland PC Users Group, a fellow APCUG member, has created a special CryptoLocker page at http://bit.ly/GCPCUG-CryptoLocker and updates it regularly with articles, software, tips and video links.

thank you!

A big thank you to our member presenters: Frank Bollinger, Bill Bowman, Larry Klees, and Ted Wirtz. THANK YOU! And a grateful thank you to Program Chairman, Lothar Loehr, who is making arrangements for our programs.

We need YOUR help, too. Please contact Lothar Loehr and sign up to do a presentation.

Give Your Computer A Gift! JOIN ORCOPUG!
For About $2 A Month You Can Belong to Our User Group!

membership application

New Member ☐ Renewal* ☐

Expired members are not eligible to win raffle prizes or to access the Members' Only web page.

Last Name _____ First Name _____ Nickname _____

Mailing Address _____ City _____ State ____ Zip _____

Home Phone ( ) _____ Work Phone ( ) _____ E-mail Address _____

Areas of Interest/Comments _____

Make checks payable to: ORCOPUG — Dues are $25 per year
ORCOPUG, P.O. BOX 716, Brea, California 92822–0716
Meetings are the second Tuesday of every month. See www.orcopug.org for more information.

how stores use your phone's wifi to
track your shopping habits

Every smartphone these days comes equipped with a WiFi card. When the card is on and looking for networks to join, it's detectable by local routers. In your home, the router connects to your device, and then voila — you have the Internet on your phone.

But in a retail environment, other in-store equipment can pick up your WiFi card, learn your device's unique ID number and use it to keep tabs on that device over time as you move through the store.

This gives offline companies the power to get incredibly specific data about how their customers behave. You could say it's the physical version of what Web-based vendors have spent millions of dollars trying to perfect — the science of behavioral tracking.

Thousands of customer interactions a day are logged and uploaded to the databases of third-party companies that specialize in retail analytics. **Estimates vary as to how big this industry is, but according to Polonetsky, nine major players account for the vast majority of tracking activity.** Others estimate there could be as many as 40 major and minor firms.

Thwarting this tracking yourself can be impractical. One option is simply to turn off your wireless cards whenever you enter a store. But that might still not prevent a retailer from snatching your MAC address (a unique, 12-digit code that helps routers send data to the right recipient) while you're walking by the promotion in the window outside. Some retail analytics companies — including New York-based Nomi, which this week raised $10 million in venture capital — offer an opt-out function on their Web sites where you can type in your MAC addresses and state your desire not to be tracked. Doing this for every device you own can be exhausting, however. And some retail analytics companies don't provide the opt-out feature.

That's where Bradish and The Wireless Registry's other co-founder, Patrick Parodi, come in. Together with the Future of Privacy Forum, the two hope to build a kind of central Do Not Call list for MAC addresses. **At least in theory, consumers will be able to visit a single Web site, register their MAC addresses for free, and the major tracking companies that have committed to the project will pledge not to follow those addresses around brick-and-mortar stores.** It's a form of potential self-regulation that should look familiar if you've been following the debate over online tracking, where web browsers have begun letting users tell commercial web sites they don't wish to be followed.

Excerpt from Brian Fung's blog at http://www.washingtonpost.com/blogs/the-switch/ wp/2013/10/19/how-stores-use-your-phones-wifi-to-track-your-shopping-habits/ or http://wapo.st/1ir4Sty

The gift of love, the gift of peace, the gift of happiness... may these be yours this Holiday Season

Orange County PC Users Group

computer users helping computer users

Member of

apcug

An International Association of Technology & Computer User Groups

ORCOPUG
Post Office Box 716
Brea, California 92822-0716

714-983-2391 • www.orcopug.org

President, Mike Lyons *mike@orcopug.org*
Treas/Membership, Charlie Moore *charlie@orcopug.org*
Editor/Webmaster, Linda Gonse *editor@orcopug.org*
Programs, Lothar Loehr *lothar@orcopug.org*
Membership, Carl Westberg *carl@orcopug.org*

Nibbles & Bits is electronically published and distributed by Orange County PC Users Group to its members and vendors. Opinions expressed herein are the writers and are not reflective of the Orange County PC Users Group position, nor endorsed by inclusion in this newsletter. Submit newsletter items to: editor@ orcopug.org. Reprint Policy: PAGE LAYOUTS AND IMAGES MAY NOT BE USED. User groups MAY REPRINT UNALTERED, UNCOPYRIGHTED TEXT, WITH CREDIT TO THE AUTHOR AND NIBBLES & BITS.

www.orcopug.org

• program of the month • newsletters • tech & help links • pdf & on-site search • map • online review form • contact info • membership application • Members' Only! page

our website has everything you need!

benefits of
User Group Membership

- Product & "How To" demos
- Free raffles and magazines
- Help from other members
- Newsletter and web site
- Special offers & discounts
- Monthly meetings
- Affiliation with worldwide group

User groups represent the spirit of the frontier, a community getting together to do things that no individual ought to have to do alone. The pioneers of the American west got together for barn raisings, cattle roundups, and the occasional party. The pioneers of new technology get together for installfests, new user training and support, and just plain fun. Being part of a user group is the best way to get more out of your computer, and lets you make friends while you're at it.

Tim O'Reilly, President
O'Reilly Media

where are the meetings, when are they held?

next meeting: Tuesday, December 10, 6 p.m. to 9 p.m. — Coco's Bakery Restaurant

Regular meetings are held the second Tuesday of the month at 6 p.m. at Coco's Bakery Restaurant, 1011 North Harbor Blvd., Fullerton, CA. Meetings are free and the public is welcome!
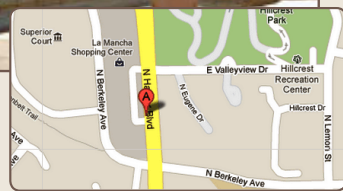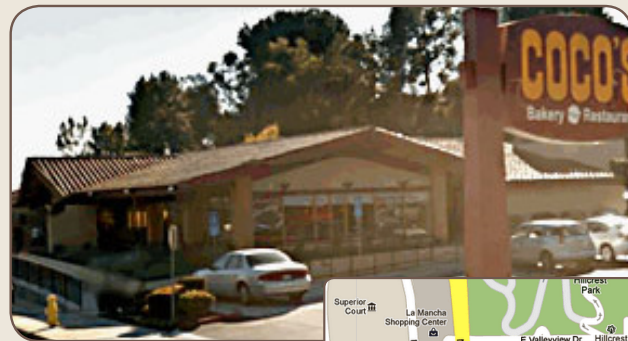
Planning meetings *are held the second Wednesday after the regular meeting every month at 6:30 p.m. at Carl's Jr., 3240 Yorba Linda Boulevard, Fullerton, CA 92831. All members are welcome to attend planning meetings! Check with Charlie Moore in advance to be sure the planning meeting has not been cancelled.*