CAEUG

Computers Are Easy User Group

Abort,
Retry,
Ignore....

Founded 1984 **ARI** is the
Official Newsletter of
Computers **A**re **E**asy **U**ser **G**roup

February 2016

Volume XXXIV Issue 2

Confirmed meeting dates

February 27
4th Saturday
~~Room A~~
Story & Craft Rm

March 26
Room A

April 23
Room B

May 28
Room A
:: ::
Check
www.caeug.net
for confirmed
meeting dates
:: ::
MEETING
PLACE
is the
Glenside Public
Library
:: ::
Visitors
Welcome
HOPE TO SEE
YOU THERE!!

Meeting on Feb. 27 (4th Saturday) In the Story and Craft room, located in the Youth Services area.

Our Feb meeting will have members discussing past programs and how they found them helpful. Win 10 can be included in the discussion

Meeting will be held in Story and Craft room,
located in the Youth Services area.

REMINDER

It is that time of year again.
January yearly membership dues are due
For $20.00 yearly membership you will receive:

11 CAEUG (Abort, Retry, Ignore) newsletters
10 informative CAEUG monthly meetings
1 great annual picnic with great food
great coffee breaks
great donuts or bagels
fantastic group of people
and so much more!

See John St. Clair at the meeting to renew your membership
and continue receiving all the benefits or
use our mailing address on page 10

Table of Contents

Page

The Rankin File
10 Ways to Protect Yourself from Identity Theft
By Bob Rankin, Ask Bob Rankin
http://askbobrankin.com/10_tips_identity_theft_protection.html

A new study shows that identity fraud is increasing, affecting over 13 million U.S. consumers in the past year. Big spikes were noted in 'new account fraud' and 'account takeover fraud' -- two of the most damaging types of ID theft. In addition, a series of massive data breaches at major corporations leaves consumers vulnerable to phishing and other forms of fraud. Poor password practices are a factor as well. Read on for my tips on avoiding fraud and identity theft...

Identity theft is one of the most traumatic non-violent crimes to which one can fall victim. When a crook uses your good name to commit fraud or robbery, the impact on your reputation, employability, and credit is severe and can last for years. It's even possible to find yourself arrested for crimes you did not commit. So it's important to protect yourself against identity thieves.

The telltale signs that your identity has been stolen can be subtle and go unnoticed for months, even years. Inexplicable charges on your credit card bill may be chalked up to clerical errors. Letters from creditors you've never heard of and certainly never did business with may be ignored. But eventually, an enormous credit card bill, legal papers or police show up at your door. You are denied a mortgage or a job. Then the real nightmare of proving "I didn't do it" begins.

Prevent Identity Theft

It can be maddeningly difficult to clear your name, costing hundreds of hours and thousands of dollars. That's why it's important to take steps NOW to make it as difficult as possible for a scammer to victimize you. Take action on these ten tips as soon as possible, and you'll tips the scales in your favor:

1. Check your credit report on a regular basis, to see if there is any incorrect information, or accounts you don't recognize. My article Free Credit Reports Online explains how U.S. citizens can get three free credit reports per year, and avoid the credit report scammers.

2. Shred your sensitive personal documents before throwing them away. A battery-powered cross-cut shredder can render your banking and credit card information unreadable and costs less than $30. "Dumpster diving" is a favorite, low-tech way by which ID thieves collect bank statements, credit card numbers, Social Security Numbers, and other bits of your identity from your trash.

3. Be wary of telephone solicitors asking for personal or financial information to "verify your identity." Common scams involve someone who claims to be from your bank or credit card company, claiming that there is a problem with your account. If you did not initiate the call, hang up and call the toll-free number on your statement, then ask for the security department. This happened to me recently, in the wake of the Chase Bank breaches. A person claiming to be from Chase called my unlisted number and asked for me by name. I Googled the number on the caller

Con't pg 3

ID, and found that many others reported similar calls.

4. Keep important documents, such as tax returns, birth certificates, social security cards, passports, life insurance policies and financial statements secure in your home. A fireproof safe is a good idea, but remember to bolt it to the floor or hide it well. Consider using TrueCrypt or Bitlocker to encrypt your personal and financial data, in case your computer is lost or stolen.

5. ATM Safety: Make sure no one is looking over your shoulder when you enter your debit card's PIN at an ATM or point-of-sale terminal. I recommend the "two finger method" where you point two fingers at the ATM keypad, but only press with one. This makes it nearly impossible for someone nearby to discern your PIN while you're entering it. You should also be wary of "skimming" devices at ATMs and gas pumps, which can be used to steal your card information. See All About Skimmers to learn how to identify these devices. **http://krebsonsecurity.com/all-about-skimmers/**

6. Memorize PINs, account numbers, and passwords; do not write them down. And for heaven's sake, do not put such data on scraps of paper kept in your wallet, purse, or laptop case! See my related articles Is Your Password Strong Enough? and Password Managers for Multiple Devices.
http://askbobrankin.com/is_your_password_strong_enough.html
http://askbobrankin.com/sync_your_passwords_on_windows_mac_and_smartphones.html

7. Get blank checks delivered to your bank branch, not to your home mailbox from which they may be stolen. On a similar note, eliminate junk mail which may contain "convenience checks" and credit card offers that can also be intercepted from your mailbox. Visit OptOut Prescreen for help eliminating these dangerous nuisances.
https://www.optoutprescreen.com/?rf=t

8. Credit Cards: Check to see if your online banking service has a feature to notify you by phone, text, or email when you when a credit card transaction exceeding some threshold occurs. Also, when you order a new credit or debit card, mark the calendar and follow up promptly if it does not arrive within 10 business days. Ask the card issuer if a change of address request was filed, and if you didn't do it, hit the panic button.

9. Don't give your Social Security Number to any business just because they need a "unique identifier" for you. Instead, ask if you can provide alternate proofs of identity, such as your driver's license or birth certificate.

10. Consider placing Fraud Alerts with the major credit bureaus, so new accounts cannot be opened without your knowledge. Call Equifax (800-525-6285), and they will pass along the request to both Experian and Trans Union. Fraud alerts expire after 90 days, so you can repeat the process quarterly, or lock down your credit file with a Credit Freeze. A freeze is permanent and free (in most U.S. states) but it may interfere with loans applications, employment screening, signing up for utility or phone service, new insurance policies, and other transactions. (See this Consumer's Union guide to credit freezes.) You'll need to contact each credit bureau (Equifax, Experian, and Trans Union) to request the credit freeze.

Con't Page 4

http://consumersunion.org/research/security-freeze/
https://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp
http://www.experian.com/consumer/security_freeze.html
http://www.transunion.com/corporate/personal/fraudIdentityTheft/fraudPrevention/securityFreeze.page

There are plenty of common sense things you can do to protect against identity theft, but sometimes it's beyond the control of even the most vigilant. The Javelin Research 2014 Identity Fraud Report reports that there is a new identity fraud victim every 2 seconds, and found that data breaches perpetrated on large companies such as Target, Home Depot and JP Morgan Chase are a "treasure trove" of data that could be used to commit identity theft and fraud. Here's a very interesting infographic showing the major data breaches of 2014, and what types of consumer data were affected.

What about LifeLock?

You may be considering LifeLock or a similar identity theft protection service. Although this can be helpful, no company can guarantee that identity theft will never happen. These services monitor your bank account, and look for suspicious online activity done in your name. They'll alert you if they spot any red flags and promise to help you repair the damage. But because of lawsuits filed by the credit bureaus, Lifelock can no longer place fraud alerts on your behalf. Also, all identity protection services are barred from offering Identity theft insurance coverage to residents of New York state.

It can be a nuisance to manage fraud alerts manually. But given the recent focus by scammers on new account fraud and account takeover fraud, a service such as LifeLock, Identity Guard or Trusted ID may still be useful. The downside is that most cost about $10/month, and none of them can claim to prevent all forms of identity theft.
www.lifelock.com
www.identityguard.com
www.trustedid.com

---

* * * * * * REMINDER * * * * * *

It is that time of year again.
January yearly membership dues are due
For $20.00 yearly membership you will receive:

11 CAEUG (Abort, Retry, Ignore) newsletters
10 informative CAEUG monthly meetings
1 great annual picnic with great food
great coffee breaks & great donuts or bagels
and so much more!

See John St. Clair at the meeting to renew your membership
and continue receiving all the benefits or
use our mailing address on page 10

Lamp Post 177

by John Spizzirri
February 2016

By the time you read this, the bald eagles at Decorah, Iowa **(1)** will have a clutch of eggs. At this writing it looks as though there is at least one egg because the eagles are sitting the nest. The incubation from laying to hatching is 35 days **(2)**. The female is larger than the male. The eagles at Berry College in Georgia **(3)** already have one eaglet.

1) http://www.ustream.tv/decoraheagles
2) http://goo.gl/kqN3Qr
3) http://www.berry.edu/eaglecam/

Windows 10 has a new major update **(1)**. The new build has been released to early adopters. The rest of us will have to wait until the early adopter testing identifies the new bugs and Micrsosft (MS **(2)**) fixes them. Then it will be released to the public. It will be our turn to test the new build so it can be certified by MS as a good product for its corporate and governmental customers. It can be said that early adopters are people who want to test new systems on the 'bleeding edge' of technology. The rest of us have the testing forced on us by MS **(3)**.

1) http://goo.gl/oiMsd9
2) https://www.microsoft.com/en-us/
3) http://goo.gl/64hOIU

Ed Bott of ZDnet's Ed Bott Report **(1)** has graded the Windows 10 roll out and implementation from the beginning to the end of 2015 **(2)**. I disagree with some of his 'report card', but he has access to much more insider information than I. For instance, he gave upgrades and updates a 'c-'. I think that when MS released the upgrade on November 15 and then had to recall it almost immediately rates an F for FAIL. First, it took two and a half hours to install (Lamp Post 175 **(3)**). If you had a small office with say 12 computers, do you pay someone to upgrade all those computers during off hours so as to not disrupt your business? What would that free software cost you? Other errors that prevent that installation from completing have been reported (**(4), (5)**). These reports do not give the results of the aftermath. I want to know if the partial install freezes the PC or worse. Does the OS have to be completely reinstalled (deleting all of the victims files, music, and videos)? Bott is much too kind. Bott gives the privacy issue a 'B' grade. He thinks that people like me over blow the privacy issue. I think that privacy should be straight forward. It should be able to be explained in a short English document with no legalese obfuscating the matter. Try reading the privacy document for Windows 10. The first thing you must do is find the document. I have been unable to find the finished product privacy document. I have found a general privacy policy **(6)** and a pre-release policy **(7)**. The pre-release document is almost 1800 words on four and a half pages. It is very non-specific. The reason I find privacy very important is that when it is collected, I have no way of knowing where it is kept, who has access to it, and the security protecting it from crackers. The issue I see is that many different sources can be cracked

Con't pg 6

or freely accessed and the various pieces of information on me can be connected together to steal my identity **(8)**, create credit accounts in my name **(9)**, or perhaps sell my house out from under me **(10)**. Some people say they have nothing to hide. If that is true, they should include their name, address, phone number, Social Security number, and all their credit card numbers in every e-mail or regular mail (postcard) they send. When the IRS data base is cracked **(11)**, the crooks have almost all that information. Some people who work at the IRS have casual access to that information all the time. They could sell it to crooks or become crooks themselves - the possibilities are endless. But if you have nothing to hide, just give that information away. Bott give security an 'A-' grade. He goes on about the Enterprise version of Windows 10 but gives short shrift to the consumer. MS is getting rid of Internet Explorer (IE), a major security hole in favor of Edge. IE is still shipped if you know how to find it. Bott talks about the 'legacy baggage' in IE. Who put the baggage in IE to start with? He talks about full disk encryption provided you 'sign into a Microsoft account.' You give up privacy with a MS account. Things you save to disk are also saved to the cloud (Skydrive or whatever it is called this week). Who knows who or what can view documents in the cloud. In my opinion, Bott is far too lenient with the corporation that can affect so many lives.

1) http://www.zdnet.com/blog/bott/
2) http://goo.gl/xsV7Xc
3) http://goo.gl/DPGHbE
4) http://goo.gl/JVbFon
5) http://goo.gl/yZrC5Q
6) https://privacy.microsoft.com/en-US/
7) http://goo.gl/bHoAZT
8) https://goo.gl/droqWM
9) http://goo.gl/Mxk2HF
10) https://goo.gl/JkJj3B
11) http://goo.gl/OiulsK

Picasa will no longer be supported by Google after March 15, 2016 **(1)**. Picasa was replaced by Google Photos **(2)**. The Picasa desktop application may still be used with some restrictions **(3)**. The web site to use Google Photos **(4)** requires a log in to a Google account. There is no desktop version of Google Photos **(5)**. All your Picasa albums will be available in Google Photos. If you use Picasa, you should check that your photos are available before the Ides of March **(6)**. The DVD of the Month has the Picasa application.

1) http://googlephotos.blogspot.com/
2) https://www.google.com/photos/about/
3) http://goo.gl/zLDv7j
4) https://photos.google.com/
5) http://goo.gl/0XYHn6
6) https://goo.gl/OhfcNQ

You may have heard of the 'Locky crypto-ransomware' **(1)** that is recently been employed by criminals to extort money from (primarily) Americans and Europeans. It comes in the form of an e-mail Word document attachment. The e-mail claims to have an invoice with an invoice number in

Con't pg 7

the subject beginning with J. If an unsuspecting person downloads and opens this document in Word and has macros turned on (the default), the macro downloads a program that executes. The program begins encrypting music, video, image, archive, database, and web application-related files. The encrypted files are renamed with a long hexadecimal **(2)** number with an extension of .locky. It leaves instructions on how to pay in plain text files in each directory that has been encrypted. It stores some data in the Windows registry. It demands one half Bitcoin to unencrypt the files. At this writing Bitcoins are $433US **(3)**. I have personally gotten a number of these e-mails. I rarely get invoices by e-mail, but I know the companies they come from. I do not open e-mail from some one I do not know. I never open attachments without scanning them with anti-malware software. Locky is detected by most anti-malware software.

1) http://goo.gl/21glQZ
2) https://goo.gl/izQKoG
3) http://www.coindesk.com/price/

Emsisoft **(1)** has come up with a program that can derive the decryption key for HydraCrypt and UmbreCrypt ransom-ware **(2)**. These extortion programs arrive on the victims computer by e-mail or malicious web sites or by benign web sites that have been cracked. I have included the decyption key program on the DVD of the Month. Emsisoft also has a malware 'emergency kit' **(3)**. I included it on the DVD of the Month. Both the Windows Club **(4)** and Bleeping Computer **(5)** had articles on this. I have also included CyrptoPrevent **(6)** on the DVD of the Month.

1) https://www.emsisoft.com/en/
2) http://goo.gl/rzRbyi
3) http://goo.gl/2cclyO
4) http://goo.gl/lu9vi8
5) http://goo.gl/Vzr6J8
6) https://goo.gl/c4rno1

Bleeping Computer reported another new cryptoware called CryptoJoker Ransomware **(1)**. This one is delivered via a PDF **(2)** file in e-mail. This extortion is too new to have a free cure. Check out the Bleeping Computer site regularly to see what to do and if there is a free cure.

1) http://goo.gl/UXq6gi
2) https://goo.gl/1xrV7v

PC Magazine had an article last November about how to speed up Windows 10 **(1)**. I held off in hopes that there might be some new material. So far, nothing new. Nine of the ten items will speed any Windows OS. They are uninstall crapware, limit startup processes, clean up the hard drive, add RAM, install a solid state drive, clean up viruses and spyware, change power settings for maximum performance, change appearance to plain (not transparent), and turn off search indexing. The only new item is trouble shoot performance issues. Even that option is similar to other versions of Windows. If you want to speed up your Windows PC, look at the article for the details.

1) http://goo.gl/rsqhSG

Con't pg 8

As reported by SDnet, MS has a new scheme to increase its profits **(1)**. It has Intel **(2)**, Qualcomm **(3)**, and AMD **(4)** on board. The new CPUs **(5)** from these manufacturers will require Windows 10 and vice versa. It will be implemented on the corporate and government customers first. This is a risky move for MS as some corporate and government users have moved to Linux when XP was being phased out. The corporate and governmental customers do not get Windows 10 for free. They must pay for the OS. They must pay for training their users in the new OS. They must pay for the training of their Information Technology (IT **(6)**) departments or external IT expertize. In as much as they pay for all that, they can eliminate the OS cost by switching to Linux.

1) http://goo.gl/okJgD4
2) https://goo.gl/vhXwVt
3) https://www.qualcomm.com/
4) http://www.amd.com/en-us
5) https://goo.gl/ZB0FHc
6) https://goo.gl/jDtcRm

Between you, me and the LampPost, that's all for now.

Mac OS X Tip

BCUG Bytes

By Lee Maxwell, co-leader MacWaves, the Mac/iDevice User Group of the BCUG

August 2015 issue, BCUG Bytes

Leemaxwell [at] gladmaxcom www.bcug.org

Adware is becoming one of the most significant threats to users of computers, both Windows PCs and Macintoshes. Besides causing annoying changes in the performance of a web browser, it can also be used to convince you to allow a nefarious stranger access to your computer.

Case in point: A member of MacWaves, the Macintosh User Group part of BCUG, emailed me about a recent experience. I'm quoting her email:

"This afternoon, when going to a website, I received a message that my computer was infected by a virus — I could not do a force quit from Safari, nor could I get rid of that
message —it wasn't a mail message — it came up right in the middle of my screen —on the message with the warning about the computer being infected by a virus, there was a number to call, which, out of desperation, I called [that number], and was told I reached Apple Support.

"I was told that they were getting a number of calls from people who were receiving the same message — and this gentleman would see what he could do to help — by looking at my desktop!! I've done this a number of times with Apple, and did allow it. (I am kicking myself about doing this—but never had a problem whenever Apple did this in the past.) Not sure what he did — numbers kept appearing, and after 5 or more minutes, he said that he would share the diagnosis with the 'Apple anti-hacking team' and remove the virus — that would take 40 - 50 minutes. He said it was due to a Zeus Malware???

Never heard of it!

Con't pg 9

“When I heard that, I told him that I would prefer to take my computer to the Apple store and have them do whatever — he told me that they would not be able to fix it as it was a network problem —and it was a virus affecting lots of computers in my area.

“I said I had his number and would get back to him after I consulted my Mac User Group or Apple. He said I would have to get back to him within 30 minutes or they would not be able to help; then I knew something was wrong.

“I called Apple — they told me it was a scam — and the gal I spoke to went over everything (checking my desktop, etc. as well as library, apps, documents, etc.) and everything seemed to be fine. I told her I was locked out of Safari and could not even do a Force Quit. Everything seems to be corrected and she also had me install MalwareBytes for Macintosh on my computer.
“Not sure why I was so gullible at first — should have known better than to listen to this guy — especially with his accent, the poor connection which I kind of knew must have been out of the US— but he said he was in California —with the Apple anti-hacking team!!!

“I learned my lesson — hope they were not able to get any info from my computer — Apple said they thought everything was O.K.

“Since then, I changed a couple of my more important passwords just in case — and will probably change a few more.”

The email is pretty self-explanatory, so I will only give some advice to Macintosh users:

If you see a pop-up window like this, do not do what it tells you to do. Instead, try to quit the web browser you’re using. If it won’t quit, click on the Apple Menu icon on the left side of the menu bar, choose the Force Quit command. In the window that appears, choose the name of the web browser and click Force Quit (Command-Option-Escape), then click OK.

If you have a different web browser on your Mac, use it to download MalwareBytes for Mac, the renamed AdwareMedic, install it via opening the downloaded .dmg file and drag-and-drop the MalwareBytes for Mac icon onto the Applications folder icon, then launch it from the Applications folder and use it to scan for and remove adware.

If for any reason you can’t do that, contact Apple Tech Support.

February 2016 DVDOM

ARI - Monthly newsletter
AudioBook - Free audio book

Blender - A free and open source 3D creation suite

ConfigFox - Firefox configue utility
CryptoPrevent - Free crypto malware program

DesktopOK - Remembers desktop icon layout and restore
DVDOMlists - Contents of CDs and DVDs of the Month

EdgeBlocker - Block or unblocks the use of Edge
EmsisoftDecyrpter - Decrypt hydra and umbre crypto malware
EmsisoftEmergencyKit - Remove program
ExactAudioCopy - Copies audio files exactly

GWXControlPanel - Free remove and disable 'Get Win 10'

Kodi - Home theater software

MemberContributions - Things members send me
mp3DirectCut - Audio file editor
MWSnap - Updated screen capture utility
NirLauncher - Updated 180 portable freeware utilities for Windows

OldTimeRadio - Old radio audio files
OpenShotVideoEditor - A video editor

Picasa - Desktop photo application from Google
PopcornTime - Watch torrent movies on line

SpeedyFox - Speeds up Firefox/Skype/Chrome/Thunderbird
VLC - Updated media player

REMINDER:

Your annual CAEUG dues are due.
See John St. Clair at the
January or February meeting or
use our mailing address

Meeting Location and Special Accommodations

The Glenside Public Library address is at 25 E Fullerton Avenue, Glendale Heights, Illinois. Please park away from the building. Thank you. The meeting(s) are not library sponsored and all inquiries should be directed to Mike Goldberg at

Individuals with disabilities who plan to attend this program and who require certain accommodations in order to observe and / or participate in the program are requested to contact CAEUG president, Mike Goldberg at , at least five (5) days prior to the program, so that reasonable accommodation can be made.

Mailing address:
CAEUG
P.O. Box 2727
Glen Ellyn, IL 60138

Members Helpline
Any member with a specific expertise can volunteer to be on the Members Helpline.
Hardware problems, XP,
Win 7, Linux
and Virus Removal
- John Spizzirri

CAEUG OFFICERS

President	Mike Goldberg
	president(at)caeug.net
V.P. (Programs)	Roger Kinzie
Secretary	Al Skwara
Treasurer	John St. Clair
Newsletter Ed	Kathy Groce
Board Member	Frank Braman
Webmaster	John Spizzirri
	webmaster(at)caeug.net