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

October 2015

Volume XXXIII Issue 10

Confirmed meeting dates

Oct 24
4th Saturday
Room A

:: ::

We do not have a date for the Nov/Dec meeting

Check www.caeug.net for confirmed meeting dates
MEETING PLACE is the Glenside Public Library

:: ::

Visitors Welcome
HOPE TO SEE YOU THERE!!

The October 24, 2015 (4th Saturday)
presentation video:
APCUG Computer Maestro to
discuss backing up strategies

Meeting will be held in Room A
10/24/15 4th Saturday

October is National Cyber Security Awareness Month

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

For the past 14 years, I have been promoting the annual National Cyber Security Awareness Month, encouraging individuals, schools, colleges, governmental agencies, corporations, clubs, and other groups to get involved. Every year since its founding in 2001, this annual event has been recognized by bipartisan presidential proclamations declaring October as National Cyber Security Awareness Month. While many organizations around the country hold a myriad of events during the month of October promoting cyber security, locally the premier event is hosted by the city of Port Arthur and its most capable information technology manager, Fay Young.

In recent weeks, hundreds of thousands of taxpayer records have been digitally stolen from the IRS; a multitude of financial institutions have had their

Con't pg 2

Table of Contents

Page

customers' account data purloined by hackers for nefarious purposes; and millions of individuals have been victimized by a variety of online attacks from hackers who steal their personal information, hold their data for ransom, and trick individuals into disclosing usernames and passwords. Sensitive military data has been stolen by hackers and other data thieves, and unfriendly foreign government hackers have stolen hundreds of billions of dollars' worth of American intellectual property and used it to unfairly undercut American industry or to dissect and copy our most advanced military weaponry.

I am amazed that despite years of imploring individuals to use different and complex passwords for each of their online accounts, many people still use the same easy-to-guess passwords to access all of their accounts. Hack or crack any one of those, and all of the victim's accounts now belong to the hacker. Bank accounts are drained, multiple illicit purchases are made from online sellers and delivered to parties unknown (all of which are then billed to the victim); inappropriate e-mails are sent to people of authority and power, traceable back directly to the victim; and scams can be perpetuated on the friends, relatives, and acquaintances of the victim by sending spam that is apparently coming from a trusted sender.

Now that so-called "smart devices," mostly Android, Windows, and iOS powered phones and tablets, are taking over roles previously performed on desktop and laptop computers, they have become the targets of choice of dishonest people out for the fast buck, at the expense of the otherwise innocent users. A popular online pundit, Kim Komando, recently posted the "7 Worst Apps That Violate Your Privacy." Some of these questionable apps are popular games played by kids all over the world, but these are more than just games, as they compile and send extensive personal information, contact lists, microphone and camera captures, and other content from the phone to third parties for questionable purposes. Immensely popular social media apps are being inappropriately utilized by pedophiles engaging in "victim acquisition." While for many of us our smart phones are addictive, we must also be aware of the risks that these wonderful devices impose upon us.

It is not too late for people to promote the concepts of cyber security awareness right now, and is also certainly a worthwhile project for next October. An abundance of material including brochures, videos, lesson plans for all age and academic levels, and other content is readily available for free from Stay Safe Online (staysafeonline.org). For teachers, college professors and administrators from K-12 to graduate school, Stay Safe Online offers prepared information that is ready to present to appropriate audiences. The website lists age-appropriate concepts for which the organization provides complete and free instructional content and media. It's easy to participate and use.

Businesses have become prime targets for cyber crooks who have stolen enormous amounts of money directly from the businesses as well as their customers. Hundreds, if not thousands, of small and midsized businesses have fallen prey to scams that illicitly transferred funds from their bank accounts to distant thieves, mostly in Russia, Eastern Europe, China, Nigeria, Iran, Pakistan, and other locations where the likelihood of recovery or even of prosecution is nil. In recent history, we are all aware of the massive credit card thefts from many other well-known retailers. Millions of those credit card numbers, complete with enough additional information to conduct unlawful online transactions, as well as to produce excellent quality counterfeit credit

Con't pg 3

cards, were widely available for sale online, mostly on Russian websites. Within days of the massive Target breach, thousands of counterfeit credit cards bearing data stolen from Target were confiscated by Customs and other law enforcement agencies along the Mexican border, many of those cards already used to purchase thousands of dollars of goods from American merchants, and then carted back across the border. Richard Clarke, a renowned cybersecurity expert who advised several presidents, has written that all of the Fortune 500 corporations have been the victims of hackers, and billions of dollars' worth of intellectual property have been stolen, mostly by the Chinese. Obviously, businesses and their employees need to be made aware of the cyber risks that they face on a daily basis, and be adequately trained in safe cyber practices.

Businesses can utilize the free materials and teaching guides available to them under the "RE: Cyber" program from the alliance. Executives and managers up to the top executive level as well as the board of directors may find the educational information available at staysafeonline.org/re-cyber appropriate for their degree of fiduciary responsibilities, as the information covers Cyber Threat Trends; Getting Started (with a corporate cyber security program); Board Oversight; Cyber Risk Assessment and Management; Cybersecurity Maturity Model; Cyber Regulation; Legislation and Policy; and Creating A Culture of Awareness. For employees, the material available online at staysafeonline.org/business-safe-online will cover many of the most important topics that the rank and file (as well as managers and executives) may need to be safer while online.

The general public will also find valuable information available at staysafeonline.org/stay-safe-online. Topics covered include, Malware & Botnets, Spam & Phishing, Hacked Accounts, and Securing Your Home Network. I cannot emphasize enough the utter necessity for everyone to become familiar with these most basic home cyber security and safety concepts not just to protect our computers and our personal finances, but to also protect our most valuable assets – our children.

I am offering an open invitation for everyone to attend a free, public celebration of "National Cyber Security Awareness Month," which will be held on Thursday, Oct. 1, at the Port Arthur City Hall, 444 Fourth Street, 5th Floor, starting at 9 am.

Kudos go to Fay Young, the Port Arthur Information Technology Manager, who has so ably promoted these annual National Cyber Security Awareness Month events for the past several years. We need many more like her doing much of the same in our schools, colleges, businesses, computer clubs, and other organizations. Individuals also need to be better aware of proper cyber security in order to protect their personal computers and other smart devices.

While I personally applaud and commend those who are involved with promoting and implementing these most useful and valuable events, I personally believe that cyber security is too important to "only" be a monthly event. Protecting our cyber world needs to be a continuous practice.

Those interested in attending the Port Arthur event should preregister online at registration.cityofportarthurtx.net.

Lamp Post 174

by John Spizzirri
October 2015

You may have heard of the Save WiFi campaign **((1), (2))**. The Federal Communications Commission (FCC **(3)**) is considering a rule change that will require router manufacturers to lock down the firmware so that consumers will not have a choice of firmware. Most consumers only use the software provided by the manufacturer on their routers. There are open source software choices available that control the router with a more friendly interface, more stable operation, and maximum through-put. Most consumers have never heard that there was software other than the manufacturers. A very few people write that type of software. Fewer still do naughty things in the writing of that type of software (2 or 3 incidents). The proposed rules apply to the 5GHz WiFi spectrum which includes cell phones. ThinkPenguin **(4)**, the Electronic Frontier Foundation (EFF **(5)**), Free Software Foundation (FSF **(6)**), Software Freedom Law Center **(7)**, Software Freedom Conservancy **(8)**, OpenWRT **(9)**, LibreCMC **(10)**, and Qualcomm **(11)** are the active participants in the campaign. The electronic comment period is apparently over. I searched the FCC and the Federal Register web sites for the closing dates and found three different dates. The official comment period does not preclude a snail mail letter to the head of the FCC (Chairman Tom Wheeler, Federal Communications Commission, 445 12th Street, SW, Washington, DC 20554). This rule change is unnecessary because the two to three incidents were already violations of FCC rules. This proposed rule change will prevent experimentation and inovation. Currently there are two popular router controlers - OpenWRT and DD-WRT **(12)**. Here is a list **(13)** of open source router software.

1) https://goo.gl/BFGGGr
2) http://goo.gl/WtrS8W
3) https://www.fcc.gov/
4) https://www.thinkpenguin.com/
5) https://www.eff.org/
6) http://www.fsf.org/
7) https://www.softwarefreedom.org/
8) https://sfconservancy.org/
9) https://openwrt.org/
10) https://librecmc.org/
11) https://www.qualcomm.com/
12) http://www.dd-wrt.com/site/index
13) https://goo.gl/FjY5sP

PBS Nova had a recent show that should be of interest to us all called Cyber War Threat **(1)**. The program had interview snippets with Shane Harris **(2)**, Richard Clarke **(3)**, James Bamford **(4)**, Edward Snowden **(5)**, General Michael Hayden **(6)**, Kim Zetter **(7)**, and others. Interestingly, they called Edward Snowden a whistle blower and not a traitor. If you watch the whole program, you may note that General Michael Hayden lied about knowing about the Stuxnet **(8)** malware. (He was the head of the agency that developed it with the help of the Israeli government.) Nova mentioned the National Security Agency (NSA **(9)**) and Cyber Command (USCC **(10)**) projects

Con't pg 5

like Nightstand, Howler Monkey, Picasso, and Ragemaster (**(11), (12)**). Here are some of the details of those projects;
NIGHTSTAND: Portable system that wirelessly installs Microsoft Windows exploits from a distance of up to eight miles.
HOWLERMONKEY: A RF transceiver that makes it possible (in conjunction with digital processors and various implanting methods) to extract data from systems or allow them to be controlled remotely.
PICASSO: Software that can collect mobile phone location date, call metadata, access the phone's microphone to eavesdrop on nearby conversations.
RAGEMASTER: A concealed $30 device that taps the video signal from a target's computer's VGA signal output so the NSA can see what is on a targeted desktop monitor. It is powered by a remote radar and responds by modulating the VGA red signal (which is also sent out most DVI ports) into the RF signal it re-radiates; this method of transmission is codenamed VAGRANT. RAGEMASTER is usually installed/concealed in the ferrite choke **(13)** of the target cable. The original documents are dated 2008-07-24. Several receiver/demodulating devices are available, e.g. NIGHTWATCH
The ferrite choke is an item you have seen on your own equipment. It is the cylindrical object that the cable passes through near the end of data cables. The whole video program is on the DVD of the month.

1) http://goo.gl/TYgTVi
2) https://goo.gl/pQNFiM
3) https://goo.gl/LTzRrF
4) https://goo.gl/Bn7J7Q
5) https://goo.gl/fIL8uY
6) https://goo.gl/40q7Z8
7) https://goo.gl/PF0Civ
8) https://goo.gl/vrzmKF
9) https://www.nsa.gov/
10) http://goo.gl/E0r3Oy
11) https://goo.gl/W05lxf
12) https://goo.gl/0Wyrqd
13) https://goo.gl/DRFEJz

The Motion Picture Association of America (MPAA **(1)**) and the Recording Industry Association of America (RIAA **(2)**) must be smiling. WikiLeaks **(3)** revealed that a deal between Internet service providers (ISPs **(4)**) and the semi-secret Trans-Pacific Partnership (TPP **(5)**) has been reached. ISPs will hand over copyright infringer details (identities) to the TPP **(6)**. The details of the agreement are sketchy **(7)**. The agreement seems to obligate the governments of the TPP to enforce the copy write nonsense the MPAA and the RIAA seem to think is their birth rite. That means that 'infringers' may be dragged into a foreign country's court for ajudication. It is interesting that civilian owned ISPs get to determine who is a 'law breaker' and who is not. The agreement seems to give ISPs immunity from liability from 'infringers' and copy write holders. The TPP is another agreement like the North American Free Trade Agreement (NAFTA **(8)**) or the General Agreement on Tariffs and Trade (GATT **(9)**) - no good for anybody except the super rich.

1) http://www.mpaa.org/
2) https://www.riaa.com/

Con't pg 6

3) https://goo.gl/1QDq9T
4) https://goo.gl/WjFS5b
5) https://ustr.gov/tpp/
6) http://goo.gl/UmIdOQ
7) https://goo.gl/lmysvs
8) https://goo.gl/7b88KV
9) https://goo.gl/j8Na1q

Marc Rotenberg, the Executive Director of Electronic Privacy Information Center **(1)**, testified before the United States Senate Special Committee on Aging **(2)** hearing on Protecting Seniors from Identity Theft: Is the Federal Government Doing Enough? He specifically testified about Social Security number (SSN **(3), (4)**) privacy issues. His testimony **(5)** is on the DVD of the Month. He talked about how the SSN is used for identity with disastrous results. (If you read you SS card, it says that the number is NOT to be used for identification.) He cited a 1973 government report (Report of the Ware Commission) that outlined the problems we are having today due to the use of the SSN for identification. The Privacy Act of 1974 which specifically states that the SSN is not to be used for identification was the response to that report. He told the committee that the SSN is a unique identifier because of its widespread [and illegal] use that connects numerous personal records. He testified, "Elderly Americans are most at risk of identity theft and the problem is getting worse." Further the SSN appearing on Medicare cards is not helping. He cited a study **(6)** that stated that 91% of all healthcare organizations have had a data breach in the last 24 months. He also cited the Federal Trade Commission's **(7)** Consumer Sentinel Network Data Book (CSN **(8), (9)**) which stated that 39% of all identiy theft victims are over 50 years of age. He cited numerous examples of government and private health insurance providers removing SSN from identification cards. He went on recommending that the Centers for Medicare & Medicaid Services (CMS **(10)**) remove SSN from Medicare cards. The CSN Data Book is on the DVD of the Month.

1) https://epic.org/
2) http://www.aging.senate.gov/
3) https://goo.gl/TUdkqK
4) https://epic.org/privacy/ssn/
5) https://goo.gl/j4Z5wL
6) https://goo.gl/HZwYhZ
7) https://www.ftc.gov/
8) https://goo.gl/oAV9Kq
9) https://goo.gl/JVOEmZ
10) https://www.cms.gov/

Business Insider reported **(1)** that the NSA may be able to crack 1024 bit AES encrption like that used on virtual private networks (VPN **(2)**) and Secure Sockets Layer (SSL **(3)**). This is a major revelation. Edward Snowden revealed that the NSA records almost all communication in America. Now there is suspicion that everything can be decrpted **(4)**. This decrption is accomplished by using an error in the Diffie-Hellman key swap algorithm **(5)**. The Electronic Frontier Foundation (EFF **(6)**) has some tips on how to protect your privacy.

Con't pg 7

1) http://goo.gl/wnXpaH
2) https://goo.gl/vDTnFx
3) https://goo.gl/elkVkZ
4) http://goo.gl/9gmnx1
5) https://goo.gl/1QGHcy
6) https://goo.gl/oNMqQe

The Edge **(1)** is the new browser from Microsoft (MS **(2)**). It is included with Windows 10. According to Quantcast **(3)**, a company that measures browser, OS, and web usage for advertizing purposes, reported that Windows 10 users use Chrome over Edge 63% to 15% with IE accounting for 5% and Firefox tracking 2 to 3 percent more **(4)** than Edge. Computerworld magazine reported (CW **(5)**) that Edge's "unfinished status" may account for its poor performace. It does not have cut and paste, lacks support for add-ons, and does not have the Save As function. I would not be able to write the Lamp Post or produce a DVD of the Month without those functions. CW said that MS income will be impacted if Edge is not accepted because Bing **(6)** is the search engine of Edge. Bing like Google **(7)** produce ads which generate income for the engine's owner by tracking where and what you search. That tracking is annoying to me. That is why I use StartPage **(8)**, IXQuick **(9)**, and Duck Duck Go **(10)**. Those engines do not track and have easily identifiable advertising. If you do not think that is important, try searching on Google for a unique product. Open at least three web sites where that product is sold. You will find that over the next two to three days of Google use that ads for that product will be on the search results. I find that annoying.

1) https://goo.gl/JF5Gpv
2) https://www.microsoft.com/
3) https://www.quantcast.com/
4) https://goo.gl/e7fkal
5) http://goo.gl/KWzsHB
6) https://www.bing.com/
7) https://www.google.com/
8) https://startpage.com/
9) https://www.ixquick.com/
10) https://duckduckgo.com/

Forbes Magazine reported that the spying done by MS users of Windows 10 has now been added to Windows 7 and 8 through Windows Update **(1)**. The article has the Knowledge Base (KB) numbers if you care to remove them through the Add Remove Programs function. You would have to be vigilant in that Update will try to re-install these KBs every day if you have automatic updates turned on. To turn off automatic updates follow these instructions for Windows 7 **(2)** and Windows 8 **(3)**.

1) http://goo.gl/ePlnkH
2) http://goo.gl/Kzsu33
3) http://goo.gl/r5GTTy

Getting into Safe Mode On Windows 8 or 10 have changed from the way it was done in Windows

Con't pg 8

7. Windows 8 and 10 have Automatic Repair that is used as the default mode for fixing Windows. Safe Mode is not readily available because MS wants you to use Automatic Repair. On occasion, Safe Mode is necessary. Follow the directions at How To Geek in order to access Safe Mode **(1)**.

1) http://goo.gl/SMYkKG Between you, me and the LampPost, that's all for now.

Password Generation Hint

By Jerry Goldstein
Member, The PC Users Group of Connecticut
August 2015 issue, The Program
http://www.tpcug-ct.org/ Adrabinowitz (at) att.net

Thanks to the lack of safety of those holding our passwords, we are often notified of user information and password theft occurring by those we provide our information to. Banks, stores, and other major corporations announce data thefts and loss regularly. As a result we need to be constantly on vigil and update our passwords regularly.

Remembering passwords is difficult enough without having to change them at least twice a year. Password manager programs are great but even they can fail and then you can lose all your passwords.

A new password theme has been worked out that helps you to remember your ever changing password scheme. The method uses a consistent password coupled with the name of the site you are at. Create a base password like: Qstn&16^, and combine it with the website you are visiting to create a unique password for that site. So if you go to the TPCUG Yahoo Forum site you would use, for example, Qstn&16^tpcg. This combines the usage of leaving out vowels in a word to remember the password better while making the password harder to break, using numbers and characters, one capital letter, and using at least an eight part letter/character basic password for better protection. You use the same basic Qstn&16^ with all your sites and just add in the website's name without vowels. You now have a single password to remember that can be used everywhere.

Since the likelihood of one of the sites you use that password is going to be hacked this year you want to take one extra step to avoid having to revise all your passwords every time a hack occurs. Value your sites according to Low, Medium, and High security needs. For low value sites, like the shoe store or grocery store you add LV to your password. That would be: Qstn&16^LV as your base password for low value sites. Medium value sites add MV and high value sites, like banks and credit cards, add HV.

For high value sites it is recommended you also use secondary authentication, such as having to answer a question after your user name and password are approved. Remember not to use your correct information on your authentication answers. Your correct information is too easily available on the internet to use as an authentication. Dates of birth, schools you attended, and family and pet first and maiden names are readily found on many people's Facebook profiles and postings. Use something different that you can easily remember instead.

Con't pg 9

Protecting yourself is never going to be as easy as locking your doors and windows any more. Banks lose your data regularly as laptops filled with information are left behind by bank employees when they stop off for their morning coffee. Thousands of hackers work feverishly to break your passwords and steal your identity. The methods offered here are just methods to help you protect yourself. Doing due diligence in the battle against identify theft is an ever ongoing battle. Stay alert and you may get lucky and not hacked, for a while.

The Rankin File What is Medical Identity Theft?

Bob Rankin, bob (at) rankin.org September 22, 2015 Column

Medical Identity Theft on the Rise

Your credit and bank account balance are not the only valuables that identity thieves are after. As health care costs have soared, so have incidents of “medical identity theft” in which crooks steal the credentials that enable one to obtain health care and sell them to other crooks. Here's what you need to know...

Medical identity theft is on the rise. And sadly, it is much more difficult to guard against this type of ID theft, and much harder to clean up the havoc it can create for a victim.

The Medical Identity Theft Alliance estimates that over 2.3 million Americans have been victims of medical ID theft, and 2014 saw 500,000 more cases than the previous year. That bad news is sure to get much worse. The MITA’s latest survey was conducted in November, 2014, before the disastrous leak of 80 million patients’ personal health information from Anthem. And just yesterday, I read that an "error" on Amazon's Web Services platform exposed 1.5 million people's private medical records.

Criminals can use victims’ birth dates, Social Security Numbers, and the ID numbers found on insurance cards to obtain medical services and prescriptions at hospitals, clinics, and doctors’ offices. While medical providers today routinely scan your driver’s license, you may notice that they aren’t very diligent about verifying its authenticity.

Medical Identity Theft

A fake license that wouldn’t fool a liquor store clerk can be used to rack up thousands of dollars in health care costs very easily. Insurance cards, generally, don’t bear photos or signatures. Using stolen medical credentials, a crook may visit multiple hospitals, pharmacies, and doctors to obtain services and drugs – often narcotics.

The records of these transactions are added to victims’ health care records, and should be visible on your Explanation of Benefits letters, but bogus healthcare transactions often go undetected for months or even years.

The MITA’s survey found that the average victim did not learn of medical ID theft until three months after it happened, and 30 percent victims could not determine when their health care credentials were improperly used. Health care privacy laws force victims to be intensely involved in investigations of medical fraud.

Can't Get No Satisfaction

If you’ve ever challenged a hospital bill, you know how hard it can be to prove that you did not authorize or receive the treatment claimed. Only 10 percent of victims in MITA’s survey indicated they were “completely satisfied” with the resolutions of their cases. About 65 percent of respondents said they ended up paying an average of over $13,000 to resolve disputed claims.

MITA estimates that medical ID theft crimes are a $5.6 billion industry. Larry Ponemon, head of The Ponemon Institute that conducts MITA’s annual surveys, believes that “a medical record is considered

Con't on pg 10

more valuable than everything else" to cybercrooks. Credit cards expire and are replaced frequently, rendering them useless to fraudsters after a short time. But Social Security numbers and personal health information don't change; a crook can use them practically forever.

There is no way to "freeze" health care credentials as one can freeze a credit card account. There are no centralized reporting agencies analogous to Experian, TransUnion, and Equifax that collect health care activity and can monitor it for suspicious patterns. Health care providers are trained to be helpful to patients, not skeptical of their identities.

In short, there are very few protections against medical ID theft and little help resolving its consequences. My 10 Tips to Avoid Identity Theft will help you safeguard your personal and financial records.

Aside from that, the most important thing you can do to guard against medical ID theft is reactive: read all of those "explanation of benefits" letters that come from your health care providers and insurance company as soon as they arrive. If you see anything suspicious, do not delay in challenging it.

Are you concerned about other forms of identity theft? Your best defense is knowledge and a proactive stance. See my articles Free Credit Reports Online and 10 TIPS: Identity Theft Protection to learn what steps you can take, both online and offline, to protect yourself.

October 2015 DVDOM

AdwCleaner - Updated malware cleaner
ARI - Monthly newsletter
AudioBook - Free audio book

ConfigFox - GUI for Firefox configuration
Cyberfox - Web browser based on Firefox

DVDOMlists - Contents of CDs and DVDs of the Month
HDBackupImage - Back up program
JRT - Updated malware cleaner
Kmeleon - Updated light weight web browser

MemberContributions - Things members send me
OldTimeRadio - Old radio audio files
Pixia - English version of a Japanese graphics creator

RadioRipper - Copies streaming audio to the hard drive
SlimBrowser - Light weight web browser
UsbFix - Cleans malware from flash drives

WindowsUpdateMiniTool - 3rd party control of Windows Update
WinUtilities - System performance and optimization suite

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	Billy Douglas
Webmaster	John Spizzirri
	webmaster(at)caeug.net