# QBITS

## QCS Review:
## From Chalkboards to Tablets...

**Campus Technology
in Transition
presented by
Chris Vaughan
Chief Information Officer
Augustana College**
*chrisvaughan@augustana.edu*

by Joe Durham

Chris Vaughan, the Chief Information Officer (CIO) for Augustana College described the changes and challenges of operating a network for the today's tech savvy college students. For 16 years he has worked for Augustana's information technology department.

Chris worked in several government and business areas before assuming his present position. He likes the work and enjoys living in the Midwest.

Since 1980, the nexus of computing and education has grown. We went from Chalkboards, and text-books to White erase boards, to List-serve bulletin boards, to email, to the World Wide Web. Chris notes that each technological leap has challenged higher cation to remain relevant, and useful in today's fast paced data age.

Apple's creativity with the iPod is a game changer. It is mobility with music. The music industry had to rapidly change its business model to survive this technological tsunami.

Now there are iPads and Tablets. To these are added the computer laptops and cellphones. Compound this number with the fact that students use all of these devices, and the CIO's administration becomes more complex. Augustana's 2500 students use a least 3 devices each. So the network has to serve and manage 7500 devices daily.

A CIO's job is never static. The "Cloud" is another transformational branch on the web. Now CIO's have to decide how much of the "Cloud" is a part of their services and work.

On one level Chris noted that putting things on the cloud reduces your hardware footprint and resources for storing and managing data. In his opinion the cloud's security has not risen to the level where college networks can be comfortable with it, because they have to maintain and support several laws to protect student privacy, in matters of grades, coursework, and health information. Since Augustana's network additionally supports its Dining service, financial aid, business accounting these security issues remain predominant.

As it now stands Augustana has a 3 terabyte (TB) server which is RAID (**R**edundant **A**rray of **I**ndependent **D**isks) supported. RAID is a real time back up of data on servers which equates to a data storage size of 12 TB's size. Until the cloud's security issues are addressed Augustana maintains its own server of data.

Augustana's network time line is comprised of many interesting changes.

Four years ago they transitioned from Microsoft Exchange for email to Google mail which is cloud based.

Augustana's network originally supported a data speed rate of 100 megabytes per second (mbps). Then a 300 mbps data rate was installed. By December of this year a 800 mbps rate will be achieved. In the summer of 2014 Augustana will be using a data rate of 1.5 gigabytes per second.

A CIO's work is never finished.

**QBITS** December 2013

The QCS is a member of

apcug

Within the last year colleges have begun to create and support Massive Open Online Courses ( MOOC). **goo.gl/MGO0Pk** Instructors are now able to place their syllabus, textbooks, and lectures online. At this stage the lectures are being offered in for  no credit, no fees.

Chris observed that this type of educational model will probably gain influence in conjunction with the traditional in-class instruction. An instructor can offer this online component that students can study at their own pace. In class the professor can then focus on a real world application of the knowledge have gained online. He did say that this online approach to education requires a self-directed student who can remain focused to online preparation in addition to the in-class presentation.

By answering questions from the audience, Chris explained network administration in detail:

### What do you do when a college student uses too much bandwidth?

He described that a CIO can monitor bandwidth use, not the content. If it is discovered to be out of the norm from the student population, then the CIO knows that the student is using it improperly: playing online games excessively for example or downloading a great deal of music online. In which case they can throttle that person's use of the network so that other students have their fair share of network access.

### Why are textbooks so expensive?

Chris' college bound daughter has just recently paid $329 for a chemistry textbook. So these volumes are expensive at the college level. He said that the business model of textbooks has begun to change.

Amazon has offered new, used, rental textbooks online at reduced rates. He sees the eBook model becoming the norm in the near future in college education with a reduction is pricing. Although college textbook publishers and authors continue to find ways around this approach by offering up new editions yearly in attempt to make the used version obsolete.

### Why not charge for network bandwidth used?

Augustana doesn't charge for network use, because it not their goal to nickel and dime the parents and students. It is simply seen as a part of their tuition.

Student network use is not static. He said that on Monday and early in the morning, network activity is low. It begins to pick up around 10 AM then increases during the day as the student begin their course work. Then it rises to it highest level after 6 PM until 10 PM.  Each day the network load increases until by Thursday and Friday it becomes the greatest.

Chris said they seek to offer bandwidth speeds that are often greater than the load requires because when it is needed it has to be there. As a result a fee based system doesn't support their educational objectives.

As a sidelight they discovered that keyword censorship of network use doesn't work at the college level either. Some students required access to the censored keywords for the course work and research. As a result Augustana removed those limitations.

For the near term, Chris sees more computing mobility, more cloud use, and more online courseware for the higher education com-

munity: Blended Learning. More challenges await CIO management of the Augustana network, it never ends. The QCS would like to thank Chris for his fine presentation about college network use today.
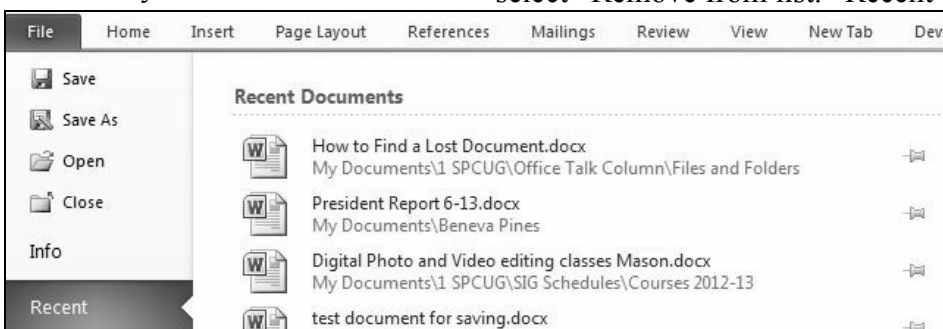
**Editor's note: As part of his presentation Chris used an online presentation tool called Prezi ( prezi.com ). It is a visually appealing and his ideas transition easily with this program. There is a free version for the public. Here is a link to Chris' Prezi presentation online : goo.gl/GZChfv**

---

# How to Find a Lost Document and Other Filing Tips

By Nancy DeMarte,
1st Vice President,
Sarasota PC Users Group, FL
August 2013 issue, *PC Monitor*
**www.spcug.org**
**ndemarte (at) Verizon.net**

I suppose you're thinking this could never happen…until it does. You have a large number of folders full of documents and photos on your computer. One day you need to find a letter that you wrote and saved a week ago, but can't remember what name you gave it or which folder you saved it in. Here are some ways to find that document:
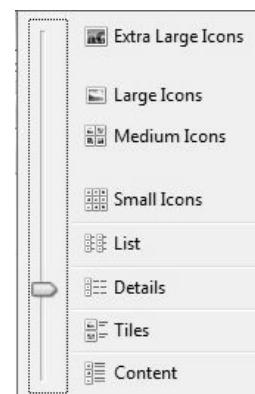
Look in your Recent Documents list: Open Word 2010 or 2007 and click File, and you will see a list of documents you opened recently. If you haven't opened more than about 20 documents since you saved the letter, it will be on the list. If you find the letter, you can open it from the Recent Documents list. But before you do that, it's a good idea to take note of its "path," so you'll know exactly where it's stored. The path of a document file in Word 2010 is shown below its name in the Recent Documents list. It is represented by a string of folders, starting with the largest folder, My Documents, and ending with the sub-folder in which the document is stored. As shown, the path for this article is "My Documents\1 SPCUG\Office Talk Column\ Files and Folders." In Word 2007, the path is missing in the Recent Documents view, but with a few steps, you can find it. Open Word 2007 and click the Office button to open the Recent Documents list. Click a recent document to open it. Then click Office button – Save As. In this window the path of the document appears in the address bar across the top. The last folder in the string of folders is where the document is stored.

You can keep or "pin" any Recent Document to the list for easy future access by clicking the pushpin icon next to it. You can also right click a recent document in Word 2010 and select "Remove from list." Recent files lists exist in most 2070 and 2010 Office programs.

Search your computer: In Windows 7, click the Start button at the left end of the taskbar, then type in the search box one or more words which you guess are part of your lost letter's name. If your guess is correct, the letter should appear in the Files list and can be opened from there. Sometimes, however, a Windows 7 search does not find files stored too deeply in sub-folders. Windows 8 offers a more targeted search. Open the Charms from the Start Screen and click the category of item you're looking for, such as Mail or, in this case, Files. Then type your search words in the Search box. This tool searches inside all levels of sub-folders in the category and returns a list of possibilities. It searches not only file names, but also the body of the document.

Make use of File Views: The contents of any folder on the computer can be viewed in various ways, but some views fit certain kinds of files better than others. It's easiest to find a document in a file list using the Details view, which is a list which includes File Name, Date Modified, File Type, and Size. A photo is best viewed as an Icon or Tile, which shows a thumbnail of the photo, its name, and file size. To change the view of a file list in Windows 7, open a folder, then click the Views icon at the right end of the menu bar. By moving the slider, you can

preview how different views affect your list before making your selection.

If your letter does not appear in Recent Documents and is not found with a Search, you can open My Documents and scroll to the bottom of the list of folders to see unfiled documents. If it isn't there, then open a sub-folder where you guess it might be. Set the view to Details, and sort the list by Date Modified, which will put recently opened files at the top of the list. To sort, click the heading of the Date Modified column. Reverse the sort order by clicking the heading again. File names sort alphabetically; dates chronologically.

Add folders to your Favorites: Much like the Favorite websites list you keep in your Internet browser, Windows provides a convenient spot for you to park folders that you open frequently. Open Libraries. In the Explorer Window, at the top of the navigation pane on the left, you'll see a section called Favorites. A few folders are listed there by default, but you can customize this list with your own folders. I keep my SIG Schedules and Office Talk Column folders there because I open them frequently, and because opening a Favorite folder takes only one click. To add a folder to Favorites, make it visible in the main Explorer window (but don't open it), then click and drag it left onto the word Favorites, or use Copy and Paste. A Favorite folder is synchronized with the original one. Whenever you make a change to files in the original folder, the change will also appear in the Favorites version and vice versa.

File Management is one of the most difficult skills to master in a Windows environment. And each new version of Windows changes the system just enough to cause confusion.
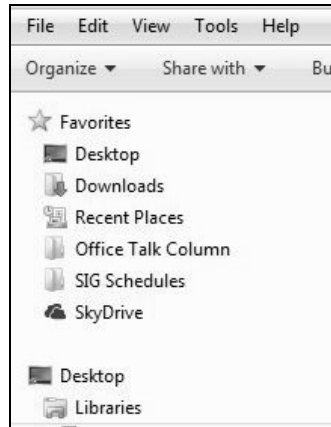


The more you understand how-files and folders are stored and organized on your computer, the more control you'll have of your documents and other important files. You won't have many lost documents, either.

---

# D-Link Update on Router Security Issue
**www.dlink.com/uk/en/ support/security**

**(Editor's note: a QCS member brought this vulnerability to our attention, consult this article if you have a D-Link router that matches these fixes.  Consult the above url for the latest firmware updates and information )**

### Security for your D-Link router

Various media reports have recently been published relating to vulnerabilities in network routers, including D-Link devices. Security and performance is of the utmost importance to D-Link across all product lines. This is not just through the development process but also through regular firmware updates to comply with the current

safety and quality standards.

We are proactively working with the sources of these reports as well as continuing to review across the complete product line to ensure that the vulnerabilities discovered are addressed.

We will continue to update this page to include the relevant product firmware updates addressing these concerns.

In the meantime, you can exercise the below cautions to avoid unwanted intrusion into your D-Link router.

### Unsolicited emails

• If you receive unsolicited e-mails that relates to security vulnerabilities and prompt you to action, please ignore it. When you click on links in such e-mails, it could allow unauthorised persons to access your router. Neither D-Link nor its partners and resellers will send you unsolicited messages where you are asked to click or install something.
• Make sure that your wireless network is secure.
• Disable remote access to your router if it is not required (this is disabled by default).

### Security patch for your D-Link router.

These firmware updates address the security vulnerabilities in affected D-Link routers. D-Link will update this continually and we strongly recommend all users to install the relevant updates.

**As there are different hardware revisions on our products, please check this on your device before downloading the correct corresponding firmware update. The hardware revision information can usually be found on the product label on the underside of the product**

**next to the serial number. Alternatively, they can also be found on the device web configuration.**

Please make sure you follow the firmware install guide provided within the ZIP firmware package.

**DI-524 Revision A1**
**Wed, 16/010/13**
The new firmware 1.06b01 that fixes the security vulnerabilities will be available by the 31st of October

**DI-524UP Revision A1/A2**
**Wed, 16/010/13**
The new firmware 1.08b01 that fixes the security vulnerabilities will be available by the 31st of October

**DIR-100 Revision A1**
**Wed, 16/010/13**
The new firmware 1.14b01 that fixes the security vulnerabilities will be available by the 31st of October

**DIR-120 Revision A1**
**Wed, 16/010/13**
The new firmware 1.05b01 that fixes the security vulnerabilities will be available by the 31st of October

**DIR-300 Revision Ax**
**Mon, 29/04/13**
The new firmware 1.06b02 that fixes the security vulnerabilities
DIR-300 Revision Ax 1.06b02
**goo.gl/rJVdKz**
Please note: In the ZIP firmware packages, there are instructions in TXT that guides you on the firmware update.

DIR-300 Revision B1
Wed, 06/02/13
The new firmware 2.14b01 that fixes the security vulnerabilities
DIR-300 Revision B1 2.14b01
**goo.gl/XBmci3**
Please note: In the ZIP firmware packages, there are instructions in TXT and PDF that guides you on the firmware update.

DIR-600 Revision B1 and B2
Wed, 06/02/13
The new firmware 2.15b01 that fixes the security vulnerabilities

DIR-600 Revision B1 and B2
2.15b01
**goo.gl/l8xVcx**
Please note: In the ZIP firmware packages, there are instructions in TXT and PDF that guides you on the firmware update.

DIR-600 Revision B5
Mon, 27/05/13
The new firmware 2.16b05 that fixes the security vulnerabilities
DIR-600 Revision B5 2.16b05
**goo.gl/7uKgKK**
Please note: In the ZIP firmware packages, there are instructions in TXT and PDF that guides you on the firmware update.

DIR-615 Revision Dx
Mon, 29/04/13
The new firmware 4.14b02 that fixes the security vulnerabilities
DIR-615 Revision Dx 4.14b02
**goo.gl/1DxgPG**
Please note: In the ZIP firmware packages, there are instructions in TXT that guides you on the firmware update.

DIR-645 Revision Ax
Mon, 29/04/13
The new firmware 1.04b05 that fixes the security vulnerabilities
DIR-645 Revision Ax 1.04b05
**goo.gl/k5EnUu**
Please note: In the ZIP firmware packages, there are instructions in TXT that guides you on the firmware update.

DIR-815 Revision Ax
Mon, 29/04/13
The new firmware 1.04b02 that fixes the security vulnerabilities
DIR-815 Revision Ax 1.04b02
**goo.gl/Xlc9jy**
Please note: In the ZIP firmware packages, there are instructions in TXT that guides you on the firmware update.

DIR-845L Revision Ax
Mon, 29/04/13

The new firmware 1.01b02 that fixes the security vulnerabilities
DIR-845L Revision Ax 1.01b02
**goo.gl/0qyKzj**
Please note: In the ZIP firmware packages, there are instructions in TXT that guides you on the firmware update.

DIR-865L Revision A1
Thu, 18/07/13
The new firmware 1.05b07 that fixes the security vulnerabilities
DIR-865L Revision A1 1.05b07
**goo.gl/DZi8Yq**
Please note: In the ZIP firmware packages, there are instructions in TXT that guides you on the firmware update.

DSL-320B Revision D2
Mon, 29/04/13
The new firmware 1.25 that fixes the security vulnerabilities
DSL-320B Revision D2 1.25
**goo.gl/cAAQpm**
Please note: In the ZIP firmware packages, there are instructions in TXT that guides you on the firmware update.

DSL-321B Revision D2
Mon, 29/04/13
The new firmware 1.02 that fixes the security vulnerabilities
DSL-321B Revision D2 1.02
**goo.gl/dU0TDE**
Please note: In the ZIP firmware packages, there are instructions in TXT that guides you on the firmware update.

---

## *Interesting Internet Finds*

Compiled by Steve Costello, President
Editor, Boca Raton Computer Society, FL
September 2013 issue,
*Boca Bits*

In the course of going through the more than 200 RSS feeds, I often run across things that I think might be of interest to other user group members.

The following are some items I found interesting during the month of August 2013.

Sandboxes Explained: How They're Already Protecting You and How to Sandbox Any Program
**goo.gl/hLDBkc**

Print Files Remotely in Windows with Google Cloud Print
**goo.gl/unuqH0**

Don't Get "Smished": How Scammers are Targeting Your Smartphone
**www.dailybits.com/sms-phishing/**

How to install a fully portable desktop on a USB for on-the-go access
**goo.gl/fmwXoa**

How To Use Skype to Share Your Computer Screen
**goo.gl/vujX5M**

Ultimate Windows 8 Wi-Fi Troubleshooting Guide
**goo.gl/si4acg**

Stop Android 4.3 from always scanning for Wi-Fi networks
**goo.gl/IO4J4i**

How to Return a Lost Phone in Four Easy Steps
**goo.gl/4nzYse**

How to Fix Annoying Multi-Page Articles All Over the Web
**goo.gl/TjuiMb**

Most Fridays, more interesting finds will be posted on the Computers, Technology, and User Groups Blog, under Creative Commons licensing.

Recent posts:
CTUBLOG

August 23, 2013
**goo.gl/3pqECP**
August 16,2013
**goo.gl/PrNNAM**
August 9, 2013
**goo.gl/5exnQY**
August 2, 2013
**goo.gl/Zdc1a1**

---

## Take One Tablet and Text Me in the Morning

By Greg Skalka,
President, Under the Computer Hood User Group
September 2013 issue, *Drive Light*
**www.uchug.org**
**president (at) uchug.org**

I've been pretty lucky with contests this year. My winning started at our group's January meeting, where I won the copy of Office Professional 2010 that Microsoft gave away at our party at the Microsoft store. Then at a local electronics component trade show in May, I won a drawing for an iPad Mini. Though it was the low-cost 16GB Wi-Fi version, it was still a more expensive tablet than I would have bought for myself.

I had been thinking of getting a new tablet, as the low-cost Velosity Micro Cruz reader I bought a few years ago was never more than fair at getting on the Internet. Since my wife had gotten a Kindle Fire HD for Christmas and my son bought himself a Google Nexus 7, I felt left out of the tablet world. I initially considered selling the iPad and buying a Nexus 7, but in the end kept it, concluding that this was probably the only way I was going to own an Apple product.

I have nothing against Apple; I think they make very good products, but feel they are overpriced. Though I may admire BMW automobiles, I'm fairly certain I'll never own one for the same reason. For me, it is all about value. I'd never considered buying an iPad Mini, as I felt there were a number of alternatives that were at least almost as good, but at 2/3rds of the price. I've known a number of Apple fanatics, some acting like cult followers. I figured this windfall would allow me to more fairly review an Apple product and perhaps give me some insight into the cult.

Though I've had the iPad for a few months, I have not really made much use of it. Its ability to browse on the web is excellent, beating my old Cruz reader by at least an order of magnitude. The iPad easily displays any web page and allows me to bypass those horrible mobile-oriented pages that seem so neutered. Still, I favor wired network connections at home, so I've used the iPad mostly when traveling. I also have not yet figured out how to transfer files to or from the iPad easily. It appears to have a great camera, but I have not been able to transfer photos. Problems with my Apple ID are contributing to the lack of wider use, and I'm still confused as to how to easily bridge the Apple and PC worlds.

In spite of relatively little use, the iPad did work well for me while on two weekend getaways with my wife early this summer. I'm accustomed to taking my laptop with me when traveling (I prefer a smaller 14" screen for greater portability), but on these trips I also brought the iPad along as it is so small. Since it is so quick to start up, the tablet became my preferred device for web

searches for nearby restaurants and attractions. Once back home, however, I went back to my PC ways.

A few weeks ago I learned that I was a winner once again. I had entered a web contest with Littelfuse, a manufacturer of electronics protection components, and got the call that I was one of 10 winners of their Speed2Design contest (**www.speed2design.com/contest**). The prize was a trip to the NASA Ames Research Center in Mountain View, CA, for an all-day engineering-oriented tour on August 15.

Prior to this, I had not considered my streak of luck in contests so significant that I should block out the time in my schedule for the prize trip when entering. I received notice that I had won only two weeks before the NASA trip, so was fortunate that the trip did not interfere with the family mini vacation to Catalina Island I had scheduled for two days afterwards. Since I had already scheduled vacation for the Catalina trip, I decided to minimize the vacation needed for the NASA trip and fly up to San Jose in the afternoon on Wednesday, the day before the tour. I needed to be there at the hotel by 6 PM for a reception, and felt flying mid-afternoon on Southwest Airlines would get me there in time. I'd flown to San Jose many times for business and was very familiar with the airport and area, justifying my lack of much margin on the travel arrangements.

Air travel used to be fun, but now with all the security scrutiny, crowded airports, baggage restrictions and added fees, it has become something like going into battle. I signed up for flight updates by text message with Southwest and with my favorite flight tracking website, Flightaware (**www.flightaware.-**

**com**). While still at work on my departure day, I received messages that my flight's departure would be delayed by 35 minutes. Since I believe delays breed delays, I started getting anxious about arriving in time for the evening reception.

I had planned on bringing my laptop and checking a bag (I like to be prepared, which often means bringing more stuff than I typically use), but with the news of my flight delay, I decided to see if I could just carry everything on and eliminate the time waiting in the baggage claim area in San Jose. Since this seemed more reasonable if I left the laptop at home, I decided to take only the iPad. I rushed home from work, repacked my bags to take only the tablet, and headed for the airport. Fortunately, my flight was not delayed further, and I made it to the reception in time.

Littelfuse really treated us great, and put us up at the Santa Clara Marriott. My only gripe with the hotel was that they charge $6 per day for in-room Internet access ($13 for bandwidth enough for video chat and streaming video). The hotel did provide free Wi-Fi in their lobby, but once again it is indicative of this added-fee culture in the travel business. I've stayed in hotels all over the Bay Area and had always found free in-room Internet access. And this is in the city of Santa Clara, which provides free public Wi-Fi over most outdoor areas of the city (when Santa Clara switched to smart power meters this year, it provided the free Wi-Fi in conjunction with the wireless network needed to read the meters). I was able to sit in the Jack In the Box across the street from the hotel Friday morning after the tour and surf the web on the Santa Clara city

network while having breakfast (sorry, I'd forgotten my other Marriott gripe: their hotel breakfast was $22).

The NASA tours arranged by Littelfuse on Thursday were the experience of a lifetime. Our day was packed with tours and presentations on nine different topics, all of which were excellent. In addition to touring the world's largest wind tunnel and learning about NASA's latest efforts to sustain humans in the closed environment of a space station though forward osmosis filtration of waste liquids, I saw several items that would have been of particular interest to our group. One was the Hyperwall display and Pleaides supercomputer.

Pleaides is a 1.79 petaflop supercomputer, made up of 130,000 cores in 182 racks. To make sense of the results of the complex simulations run on it, NASA uses the Hyperwall, a matrix of displays 12 wide and 7 high. It can all be devoted to the display of one simulation, like a world-wide view of ocean currents, or instead display the outputs of many simulations at once (**vimeo.com/71358105**). And I thought my dual display of 23" monitors at work was hot stuff.

Another interesting project we saw was the PhoneSat. To try to reduce costs and gain more knowledge quickly, NASA has developed small cube satellites (approx. 4" x 4") based on cell phone processors (**vimeo.com/71356259**, **www.-phonesat.org**). In early incarnations, there were actual cell phones built into the cubesat. The phones they prefer to use are based on the open source Android operating system (sorry, Apple).

On the flight back from San Jose, I was on a Southwest plane with in-

flight Wi-Fi. They of course wanted a fee for web browsing ($8 per day), but on that flight they also had some free live and on-demand TV shows courtesy of Dish Network. The iPad Mini provided a great display for the TV, but since I had not brought headphones, I had to settle for watching their free flight tracker for most of the flight. Installing this Wi-Fi system in their planes is a win-win situation for Southwest, as they can get the extra revenue from the Internet and movie fees as well as save flight weight, as they are making their passengers bring their own screens for movies.

The iPad Mini worked so well on the Littelfuse NASA trip that I again took it in place of my laptop on the Catalina trip. With Wi-Fi at our hotel, it again was great for checking on activities and dining on the web. It is certainly a lot lighter and easier to travel with than a laptop. It does not fill all the travel needs that a laptop does, however.

One thing I have used my laptop for on travel is for photo storage. When my camera's memory card is full, the photos can be transferred to the laptop's hard drive. With the iPad Mini, which has no SD card slot and limited internal memory, I had to bring enough spare SD memory cards for the camera. Another thing I do frequently is to create a document before each of my trips, which contains all the trip information (flight, hotel and rental car times and confirmation numbers, planned activity details and other trip info). I typically keep this document on the USB Flash drive I always carry with me, and then can view it on my laptop if I lose the paper copy. With no USB capability on the iPad, I have to rely only on the paper copy. I suppose I could have put the document in the cloud so it could be viewed on the tablet, but I don't think I want all my travel details in the cloud. For a short trip, the tablet works well, but the laptop might be better on longer ones.

---

# CryptoLocker
From Wikipedia, the free encyclopedia

| CryptoLocker | |
|---|---|
| Classification | Trojan horse |
| Type | Ransomware |
| Subtype | Cryptovirus |
| Operating system(s) affected | Windows |

**CryptoLocker** is Trojan horse malware which surfaced in late 2013, a form of ransomware targeting computers running Microsoft 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 cryptography, 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, and says that the private key will be deleted and unavailable for recovery if the deadline passes. If the deadline is not met, the mal-ware offers to decrypt data via an online service provided by the malware's operators, for a signifi-cantly higher price in Bitcoin.

Although CryptoLocker itself is readily removed, files remain encrypted in a way which researchers have considered infeasible to break. Many say that the ransom should not be paid, but do not offer any way to recover files; others say that paying the ransom is the only way to recover files that had not been backed up. A few people who have paid have had their files decrypted, as a way of increasing hope, although the number is very few.

### Operation
CryptoLocker typically propagates as an attachment to a seemingly innocuous e-mail appearing to have been sent by legitimate company, or is uploaded to a computer already recruited to a botnet [1] by a previous Trojan infection. A ZIP file attached to email contains an executable file with filename and icon disguised as a PDF file, taking advantage of Windows' default behaviour of hiding the extension from file names to disguise the real .EXE extension. Some instances may actually contain the Zeus trojan instead, which in turn installs CryptoLocker.[2][3] When first run, the payload installs itself in the Documents and Settings folder with a random name, and adds a key to the registry that causes it to run on startup. It then attempts to contact one of several designated command and control servers; once connected, the server then generates a 2048-bit RSA key pair, and sends the public key back to the infected computer.[2][4] The server may be a local proxy and go through others, frequently relocated in different countries to make tracing difficult. [5][6]

The payload then proceeds to begin encrypting files across local hard drives and [mapped network drives](#) with the public key, and logs each file encrypted to a registry key. The process only encrypts data files with certain [extensions](#), including [Microsoft Office](#), [OpenDocument](#), and other documents, pictures, and [AutoCAD](#) files.[3] The payload then displays a message informing the user that files have been encrypted, and demands a payment of 300 [USD](#) or [Euro](#) through an anony-mous pre-paid cash voucher (i.e. [MoneyPak](#) or [Ukash](#)), or 2 [Bitcoin](#) in order to decrypt the files. The payment must be made within 72 or 100 hours, or else the private key on the server would be destroyed, and "nobody and never [sic] will be able to restore files."[2][4] Payment of the ransom allows the user to down-load the decryption program, which is pre-loaded with the user's private key.[2] [Symantec](#) estimated that 3% of users infected by CryptoLocker chose to pay.[6] Some infected users claimed that they paid the attackers but their files were not decrypted.[1]

In November 2013, the operators of CryptoLocker launched an online service which claims to allow users to decrypt their files without the CryptoLocker program, and to purchase the decryption key after the deadline expires; the process involves uploading an encrypted file to the malware site as a sample, and waiting for the service to find a match, which the site claims would occur within 24 hours. Once a match is found, the user can pay for the key online; if the 72-hour deadline has passed, the cost in-creases to 10 Bitcoin (which, in early November 2013, was valued at over $3500 USD).[7][8]

### Mitigation

While security software is designed to detect such threats, it might not detect CryptoLocker at all, or only after encryption is underway or complete, particularly if a new version unknown to the protective software (a [zero-day exploit](#)) is distributed.[9] If an attack is suspected or detected in its early stages, it takes some time for __encryption to take place; immediate removal of the malware (a rela-tively simple process) before it has completed would limit its damage to data.[10][11] Experts suggested precautionary measures, such as using software or other security policies to block the CryptoLocker payload from launching.[2][3][4][6][10]

Due to the nature of Crypto-Locker's operation, some experts reluctantly suggested that paying the ransom was the only way to recover files from CryptoLocker in the absence of backups (in particular, [offline](#) backups that are inaccessible from the network, or from a [continuous data protection](#) system such as Windows' [Shadow Copy](#) mechanism).[1] Due to the length of the key employed by CryptoLocker, they considered it practically impossible to use a [brute-force attack](#) to obtain the key needed to decrypt files without paying; the similar 2008 worm Gpcode.AK used a 1024-bit key that was believed to be large enough to be computationally infeasible to break without a con-certed [distributed](#) effort, or the discovery of a flaw that could be used to break the encryption.[2][8][12][13][1]

In late October 2013 security vendor [Kaspersky Labs](#) reported that a [DNS sinkhole](#) had been created to block some of the domain names used by Crypto-Locker.[14]

### See also

[PGPCoder](#)
["CryptoLocker Scan Tool"](#).

### References

1. *a b c d* [Security Week: Cryptolocker Infections on the Rise; US-CERT Issues Warning, 19 November 2013](#)
2. *a b c d e f* Abrams, Lawrence. ["CryptoLocker Ransomware Information Guide and FAQ"](#). Bleeping Computer Retroeved 25 October 2013 . Retrieved 25 October 2013.
3. *a b c* ["Cryptolocker: How to avoid getting infected and what to do if you are"](#). *Computerworld*. Retrieved 25 October 2013.
4. *a b c* ["You're infected—if you want to see your data again, pay us $300 in Bitcoins"](#). *Ars Technica*. Retrieved 23 October 2013.
5. Destructive malware "CryptoLocker on the loose here's what to do. Maked Security Sophos Retrieved 23 October 2013
6. *a b c* ["CryptoLocker attacks that hold your computer to ransom"](#). *The Guardian*. Retrieved 23 October 2013.
7. ["CryptoLocker crooks charge 10 Bitcoins for second-chance decryption service"](#). *NetworkWorld*. Retrieved 5 November 2013.
8. *a b* ["CryptoLocker creators try to extort even more money from victims with new service"](#). *PC World*. Retrieved 5 November 2013.
9. [The Yuma Sun, on a CryptoLocker attack](#): "... was able

to go undetected by the antivirus software used by the Yuma Sun because it was Zero-day malware"

10. [a] [b] Leyden, Josh. "Fiendish CryptoLocker ransomware: Whatever you do, don't PAY". *The Register*. Retrieved 18 October 2013.

11. Cannell, Joshua. "Cryptolocker Ransomware: What You Need To Know". *Malwarebytes Unpacked*. Retrieved 19 October 2013.

12. Naraine, Ryan (6 June 2008). "Blackmail ransomware returns with 1024-bit encryption key". *ZDnet*. Retrieved 25 October 2013.

13. Lemos, Robert (13 June 2008). "Ransomware resisting crypto cracking efforts". *SecurityFocus*. Retrieved 25 October 2013.

14. "Cryptolocker Wants Your Money!". *SecureList*. Kapersky. Retrieved 30 October 2013.

### External links

* "Threat Outbreak Alert: Email Messages Distributing Malicious Software on October 11, 2013". *Cisco Security Intelligence Operations Portal*. San Jose, CA, USA: Cisco Systems. 2013-10-14. Retrieved 2013-10-30.

* "CryptoLocker Scan Tool".

This page was last modified on 21 November 2013 at 00:04.

---

# Jeff Foxworthy Comments on Iowa

If you buy a TV that doesn't fit in your car and the man in the van next to you says, "Put it in my van, I have to pick up a few things and then I'll drop it off. What's your address?" And about 1/2 hour later, the van pulls up, the man helps you get the TV in the house, refuses any form of pay, except "Thank You". Drives away and you still don't know his name ... **then you live in Iowa**. (Good folks here!)

If you've worn shorts and a parka at the same time ... **you live in Iowa**.

If you've had a lengthy phone confersation with someone who dialed a wrong number ... **you live in Iowa.**

If you know several people who have hit a cow more than once ... **you live in Iowa.**

If you have gone from "heat" to "A/C" in the same day and back again ... **you live in Iowa**.

If you design your kid's Halloween costume to fit over a snowsuit ... **you live in Iowa**.

# SIG and Event Calendar
## December 2013

Dec 2nd – Mon    5:30 PM    **Beginners SIG**    EDC   Jim Kristan      309-755-8277
                 7:00 PM    **Best Buy**    EDC
                       **Showroom Tech!**

Dec 16th – Tue    **NO SIG**    Genealogy SIG    -------    **---->NO SIG<----**    563-359-9672
                 **NO SIG**    Internet SIG    -------    **---->NO SIG<----**    309-792-9470

Dec 23rd – Mon    **NO SIG**    Digital Media SIG    -------    **---->NO SIG<----**    309-787-2239
                 **NO SIG**    Windows SIG    -------    **---->NO SIG<----**    309-787-5574

| Location Key | | Location Key | |
|---|---|---|---|
| **BCL** | Library of Butterworth Home | **MVC** | Moline Vikings Club |
| **CRA** | Craft Room of Butterworth Home | **OAK** | Oak Room of Butterworth Home |
| **EDC** | Education Center of Butterworth | **ORC** | Orchid Room of Butterworth Home |



BUTTERWORTH HOME
8th St & 11th Ave  Moline, IL
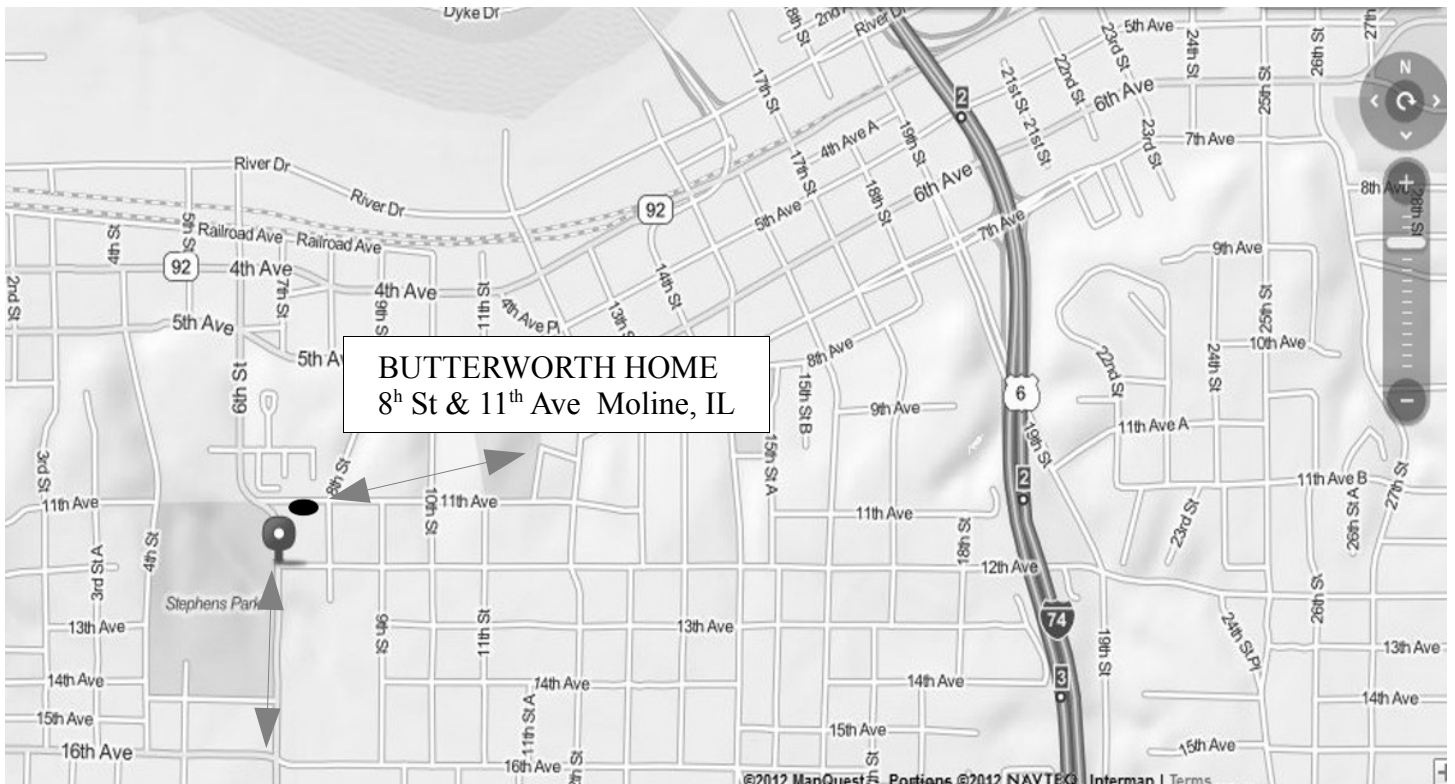
EDUCATION CENTER OF BUTTERWORTH
7th St & 12th Ave  Moline, IL

Quad Cities Computer Society
c/o Dave Tanner
3449 - 52nd St
Moline IL  61265
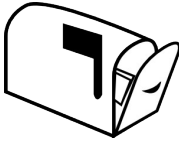
Moving? Send an
address change to:
**felspaw@sbcglobal.net**

**This Month in** *QBITS* **....**

*Monday*
**December 2nd**
**7:00 PM**
*Best Buy*
*Showroom Tech!*
**presented by**
*Tim Kress*
*Manny Martinez*
*Carol Perezemza*
*Austin Kargl*