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

November/December
2013
Volume XXX Issue 11

Confirmed meeting dates

Nov/Dec
December 14
2nd Saturday

January 18
3rd Saturday

February 22
4th Saturday

Check
www.caeug.net
for confirmed
meeting dates

MEETING
PLACE
is the
Glenside Public
Library
*** ***
Visitors
Welcome
HOPE TO SEE
YOU THERE!!

* * * November / December meeting * * *

Nov/Dec meeting -- December 14

Frank Braman's presentation Nov/Dec meeting will be
"Fast Answers On the Internet"
- this presentation will take us to amazing sites for information and answers.

CD-R and DVD+–R Longevity: How Long Will They Last?

By John Langill, Newsletter Editor
Southern Tier Personal Computing Club, NY
August 2013 issue, Rare Bits jlangil1 (at) stny.rr.com

Although there are today many data storage alternatives, I'm sure that there are many such as me who in the past stored various kinds of information on optical media, CD-Rs in particular. To cite just two examples; I have scanned hundreds of family slides, organized the digital images, and saved them on CD-Rs. Similarly, I did the same with several hundred of digital photos from my two-month visit with my son and daughter-in- law in Australia in 2003. The purpose of doing so was to have a convenient form in which archive the digital images and to share them with other members of the family; while at the same time conserving space on the hard-disk—then a more precious commodity than it is today.

Thinking back 10 or more years, one may recall that a single CD-R then offered a relatively large data storage capacity in a form that could be easily and inexpensively mailed anywhere in the world—something that could not be accomplished via the Internet or with other "portable" media at the time.

Con't pg 2

Table of Contents

While acknowledging that the images stored on these CD-Rs—and others even older—could now be transcribed to another medium, I confess that I'm reluctant to devote the time and effort to doing so at this point. Accordingly, the durability and life-expectancy of the CD-Rs that I created 10, 20, and even 30 years ago, has become an increasing concern.

In the early '90s when the first CD-R discs were introduced manufacturers said the media had a data life in excess of 40 years. In the late '90s when the first DVD-R discs appeared on the scene producers proclaimed a data life of at least 100 years. However, in the time since their introduction it has been discovered that these early discs are susceptible to media "rot" (i.e., "bit rot") that can eat your information—audio, video, or data—in as little as two years after it is written. (According to research fairly recently conducted by J. Perdereau, CD-Rs may have an average life expectancy of not more than 10 years—Journal de 20 Heures, March 2008.)

Because CD-R and DVD+–R media is used to archive nearly everything today, it does make one worry; especially if these discs are the only repository in which your precious, and irreplaceable, family memories— photos and movies—as well as vital family, personal, and company data/documents are stored.

So where does the truth lie? Somewhere across the complete spectrum.
Most people who successfully burn a disc believe they have quality media. Unfortunately that only tells you the disc will be compatible (able to be played) in the vast majority of CD or DVD players. More importantly all better quality CD and DVD burners include technology called over burn/under burn protection making "coaster production" a thing of the past. The basic construction of both disc technologies enable you to burn your data in a very precise, very controlled manner.

Test Options
There are only two foolproof ways of proving the data life of the discs you use:
1. Write a few CD-Rs or DVD+–Rs, then wait about 25-50 years and check if they still hold the correct data.
2. Use a CD/DVD analyzer that is specially designed to retrieve very accurate information about your media and your data after accelerated aging in test chambers where the discs are subjected to excessive temperature and humidity tests.

The first is typically impractical. Nonetheless, from personal experience I can attest to the fact that the first CD-R I ever burned—selections from a vinyl LP album—plays just fine and the music still sounds great 25 years later. However, I have also had some CD-Rs become unplayable in just a matter of months. Fortunately, such occurrences have been few.

The second provides only theoretical limits and doesn't take into consideration how you use, handle, and store the media. However, even assuming proper handling, temperature and humidity can adversely affect the data-life of even quality media.
Between the CD-R discs produced in the early 1980s and today's double-layer DVD+-R discs there has been considerable progress in write performance, capacity, quality, and cost.

Following the test procedures of the International Standards Organization (ISO), quality media manufacturers have been able to predict data-life spans ranging from 50-200 years. But keep in mind there are wide differences between low-budget media manufacturers and quality media

Con't pg 3

manufacturers. In addition variations in manufacturing methods, materials and processes/procedures can dramatically affect the data life of the media you use.

Or as auto manufacturers like to say... “Your mileage may vary.”

Understanding Your Discs

It isn’t vital that you understand the construction of CD-R or DVD+–R media to produce a quality disc that can be read years from now any more than you need to understand the internal combustion engine to drive a car. But understanding the difference between quality and cheap media may help you avoid losing family photos or videos later on.

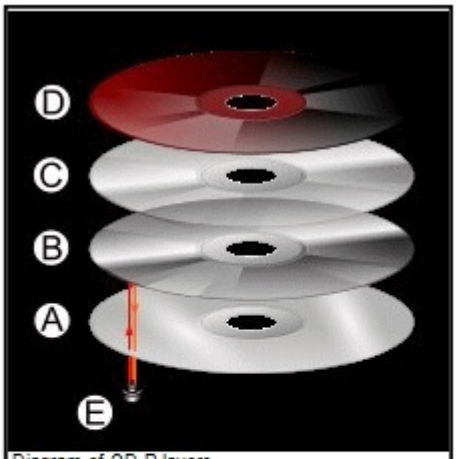

Diagram of CD-R layers.
A. A grooved polycarbonate disc layer to which a dye layer is applied to enable the encoding of data..
B. A shiny layer reflects the laser.
C. A layer of lacquer protects the shiny layer.
D. Artwork is screen printed on the top of the disc.
E. A laser beam reads the CD and is reflected back to a sensor, which converts it into electronic data

Most people consider DVD+–R discs little more than overgrown CD-Rs but, while they are similar, they are also quite different. In particular, the grooves are narrower and more closely spaced and the structure (pattern) of “pits” and “lands” is very much smaller with a DVD+–R in order to enable a greater data storage capacity. Precision is very critical.

Writable CD-R and DVD+–R discs start with a piece of polycarbonate substrate into which very precise grooves are molded to guide the tracking of the laser beam. A dye layer is then precisely applied to the substrate followed by a reflective layer and one or more protective layers. A few of the leading media manufacturers have initiated the policy of applying two very resistant layers for added data protection when the discs are used, handled, and stored.

Because of the faster read/write performance users now expect, leading manufacturers have developed new stamper technology for optimum groove (storage area) shape and ultra-precise molding technology. The molding is critical when the media must withstand being rotated at extremely high speeds during the write process—up to 52x for CD-Rs, and 8x to 16x for DVD+–Rs. The engineering margin that was once reserved for manufacturing tolerance has been used for data capacity instead, leaving no tolerance for manufacturing; for these discs to be truly compliant with the Orange Book standard, the manufacturing process must be perfect.

Media Problems

The quality of your media is directly related with the time the media will last without losing information. As you can see there are a number of areas where manufacturers can shave a few cents in the overall cost of the media and areas where production can go amiss to dramatically shorten the data life of your stored information.

There are conflicting claims and consumer beliefs on which media is best for data retention of 30, 50, 100 years—green, gold, or blue dye; and gold or silver reflective layer. It is somewhat immaterial today. Manufacturers of quality writable discs have developed significantly improved, more sensitive and more stable dyes, and better reflective materials that virtually eliminate data loss during high-speed read/write processes and enhance long-term reliability.

CD and DVD rot (i.e., bit rot) is not the problem today that it was with earlier LaserDiscs because the

media use different dye technologies to store data and make it much less susceptible to that kind of degradation. The truth is that deterioration arising from delamination and oxidation is the greater problem.

Delamination and oxidation usually occur at the outer edge of the disc and are often the result of the adhesive not being properly applied and cured during the production process. This usually happens when price-oriented manufacturers use equipment that is 2 to 3 generations old and the least expensive materials possible.

When it does happen the laser is unable to read the data on the reflected layer. It is usually caused by:

- Oxidation when air comes in contact with the reflective layer
- Galvanic reaction between the layers and coatings
- Chemical reaction caused by impurities in the disc's adhesive or aluminum coating.
- Excessive heat and humidity are known to accelerate and exacerbate delamination and oxidation.

The Real Culprit

If you have purchased quality media from a quality manufacturer, you are still not assured of 50-100 years of data life!

The greatest danger to the data longevity of your personal, family, and business information is you alone; that is, by the way you handle and store your discs. The environment—temperature and humidity—can stress the materials. Gravity also can bend and stress the discs. Fingerprints and smudges can do more damage than scratches.

But by following a few Do's and Don'ts you can ensure your precious family and friend pictures, movies, family records, and business files have the maximum data life.

Do not

Touch the surface of the disc.
Bend the disc... especially when removing it from its case as this can cause a fine crack to develop at the rim of the hub-hole which will render the disk useless. This is a particular problem with DVDs.
Store discs horizontally for a long time (years).
Open a recordable optical disc package if you are not ready to record.
Expose discs to extreme heat or high humidity.
Expose discs to rapid temperature or humidity changes.
Expose recordable discs to prolonged sunlight or other sources of UV light.
Write or mark in the data area of the disc (the shiny side that the laser "reads").
Clean in a circular direction around the disc.

Do

Handle discs by the outer edge or the center hole.
Use a nonsolvent-based felt-tip permanent marker to mark the label side of the disc.
Keep dirt or other foreign matter from the disc.
Store discs upright (book style) in original jewel cases that are specified for CDs and DVDs.
Return discs to their jewel cases immediately after use. Because the label side is more delicate and susceptible to damage, I recommend storing any CD or DVD disc label-side down in its jewel case.
Leave discs in their spindle or jewel case to minimize the effects of environmental changes.
Remove protective wrap only when you are ready to record data on the disc.

Con't pg 5

Store in a cool, dry, dark environment in which the air is clean—relative humidity should be in the range 20% - 50% (RH) and temperature should be in the range 4°C - 20°C (approx. 40 to 70EF).
Remove dirt, foreign material, fingerprints, smudges, and liquids by wiping with a clean cotton fabric in a straight line from the center of the disc toward the outer edge.
Dampen the cloth with a lens cleaner to clean your discs. Dry with photo lens tissue. For tough problems use Windex or a similar glass cleaner, diluted dish detergent, or rubbing alcohol. Rinse and dry thoroughly with a lint-free cloth.
Check the disc surface BEFORE recording.

Reliable Medium
There is a lot of cheap CD-R and DVD+-R media that has marginal quality. For some applications like games, quality isn't critical. For irreplaceable, vital data like family photos, special events, vacations, and family/friends memories quality does matter. If you are backing up mission-critical data on your home or business computer, quality matters. Then it is important to select a brand of media that will keep your data safe, secure and available for years to come.

Quality and low prices just don't seem to mix!

The next step to long-term data reliability is to handle and store the media with the respect your data deserves.

What to do if you think your email has been hacked

John King, Contributing Editor, Golden Gate Computer Society
July 2013 issue, GGCS Newsletter
www.ggcs.org editor (at) ggcs.org

The first thing to do if you worry about email hacking is to change your email account password to something more complex than 123456. For best security, use a password such as Q*93im#&qrR-57$. You'll never remember it and won't have any more email problems [insert snicker].

My Hotmail account was hacked a while ago. A human hacker or automated bot was indeed sending spam from my account on Hotmail. My local computer wasn't involved. Everything was happening on the Hotmail computers.

Spammers like to use other people's email accounts to send spam because it's free and makes the spam harder to block. After I changed my weak Hotmail password to a stronger one, the spammer/bot couldn't access my account; and the problem ended.
Alternatively, a spammer may be simply spoofing the return address of the spam using your email address to make the message less likely to be blocked. There's nothing that you can do to stop that. You could stop using that email address, but the spammer can keep using it as the return address anyway.

Fortunately, spam with your spoofed return address usually stops in a few days or weeks at the most. The spammer probably found your address without hacking your account, for example, from the address book of a friend, an intercepted email, etc. Nonetheless, changing your email password is

Con't pg 9

Lamp Post 153
December 2013
by John Spizzirri

There is already talk on the net about the 2016 presidential election. One quote comes to my mind. "We're all going to have to rethink how we deal with the Internet. As exciting as these new developments are, there are a number of serious issues without any kind of editing function or gatekeeping function." That quote was said by a person that will likely be a presidential candidate in 2016. "editing function or gatekeeping function" will probably amount to licensing of speech or censorship of the Internet. If you like the Internet as it is or if you want "editing function or gatekeeping function", you should investigate the positions on the Internet of all the candidates for the presidency. If you want to know who said the quote, copy it to Google. About fifteen articles mention that quote in totality.

CryptoLocker **(1)** is a new extortionware (ransomware) that was first reported in August **(2)**. If you see the cryptolocker screen (see Figure 1), it is too late to do anything about it. What it does is encrypts all of your office suite files, picture files, and sound files. It also encrypts files on any drive attached to

computer. If you were to stick a USB drive into the computer, it would encrypt those files as well. There are some reports of all files on the hard drive being encrypted. After all files are encrypted, it presents you with a window that informs you the files have been encrypted. The window also has a count down clock with about 72 to 80 hours on the clock. There are instructions about how to pay the ransom. Some of the criminals want the ransom paid in BitCoin (**(3)** see next paragraph). Others will

Con't pg 7

take a credit card or MoneyPak **(4)** of U.S. dollars or Euros. MoneyPak is a prepaid credit card. Those that want payment in BitCoin are the most problematic for the victim, as BitCoin changes value every day. As of this writing a single BitCoin is worth $1039 U.S. What should you do if this screen shows on your PC? First disconnect from the Internet physically (unplug or turn off the wi-fi). Do not insert any USB devices. Determine if you want to pay the ransom. There is only one means of recovery without paying the ransom - reformat the drive and restore your files from a backup disk that is NOT connected to your PC except when backing up files. That could be a cloud backup like Carbonite **(5)**, Norton Online Backup **(6)**, Backblaze **(7)**, CrashPlan **(8)**, MozyHome **(9)**. Cloud backup solutions will only work if they do not connect to your machine as if they are an additional hard drive. Other considerations of cloud backup include; how much the service costs, when backups are done, are the previous backups overwritten or are multiple copies of your files kept on their servers, are the cloud servers all in one physical location or in multiple locations, are your files encrypted on their servers, is the backup done without user intervention. If a back up drive is connected to the PC at all times, cryptolocker will encrypt those files, too. The Swansea, Massachusetts Police Department got cryptolocker and decided to pay the ransom **(10)**. They also have the FBI **(11)** investigating the infection. I don't think the FBI will do the same for you. If you decide to reformat, you must have a restore CD or DVD of the operating system (OS). CDs or DVDs of all purchased programs installed and a clean backup of all your personal files. Expect to spend upwards of 4 to 8 hours installing the OS, purchased programs, and personal files. If you decide to pay the ransom, you must do so within the time limit. After the time limit expires the files will never be able to be unencrypted. The warning page says that payment processing could take up to 48 hours because it is done by hand and not automatically. After the unencryption begins, you must maintain connection to the Internet or the process stops - so a power failure could cost you your files. On the DVD of the month there are a number of videos that describe how to pay the ransom, how to 'remove' the infection, what the infection looks like, and the pitfalls that can happen if you pay. I would suggest never paying the ransom. Paying will only encourage this virus maker and his or her copycats to continue to prey on consumers. How do you get infected? CryptoLocker comes as a zipped or plain PDF attachment to an e-mail. It will claim to be from from FedEx **(12)**, UPS **(13)**, DHL **(14)**, or someone you know. If you are expecting a package, FedEx, UPS, and DHL will NOT send you an e-mail with an attachment. Go to their web site by searching for it using Google. Do NOT click on any links within an e-mail. Erase e-mail from any shipping company. If you receive an e-mail from someone you know with an attachment and you suspect anything about it may be 'not right', call or e-mail that person and ask if they sent it and what the attachment is. If their answer is satisfactory, then you may open the attachment. If you have a satisfactory backup of your files, I would suggest that you do not try to remove the virus (trojan). Instead, format the hard drive and reinstall everything. After you are satisfied that all is working properly, change every password you have. Make the passwords strong **(15)** and memorable (**(16), (17)**). There is a free program called CryptoPrevent **(18)** on the DVD of the Month. I do not know if it works however the site that produced it is known for quality products.

1) https://en.wikipedia.org/wiki/CryptoLocker
2) http://sn.im/28acs5a
3) http://sn.im/28acs6l
4) https://www.moneypak.com/
5) http://www.carbonite.com/
6) http://us.norton.com/online-backup/
7) http://www.backblaze.com/
8) http://www.code42.com/crashplan/

Con't pg 8

9) http://mozy.com/product/mozy/personal
10) http://sn.im/28acs8e
11) http://www.fbi.gov/
12) http://www.fedex.com/us/
13) http://www.ups.com/tracking/tracking.html
14) http://www.dhl.com/en.html
15) http://www.passwordmeter.com/
16) https://www.grc.com/haystack.htm
17) http://sn.im/28acs9h
18) http://www.foolishit.com/vb6-projects/cryptoprevent/

Bitcoin **(1)** is a cryptocurrency **(2)**. As of this writing one Bitcoin's value is $1039.00 U.S. **(3)**. BitCoin is an Internet currency that has no fixed value and has no government taxing, controlling, or inflating it. It requires a certain amount of expertise to use. It was started by a nebulous person or group of people called Satoshi Nakamoto **(4)** in 2009. Nakamoto established the Bitcoin protocol which results in the creation of Bitcoins by doing various difficult computational work. That work has been dubbed 'mining' **(5)**. Bitcoins have certain attributes that are unique in the area of money; there will never be more than 21 million Bitcoins (currently 12 million), they are impossible to counterfeit, they can be divided into as small of pieces as you want (actually 10 ^-8), and they can be transferred instantly across great distances via a digital connection such as the Internet. Bitcoin is not the only cryptocurrency. Litecoin **(6)** and others are already making headway. When the maximum amount of Bitcoins have been 'mined', other cryptocurrencies will fill the gap. Many people think that Bitcoin is only used in illegal trade (drugs and other countraband), tax evasion, or money laundering. As Bitcoins are not physical, the U.S. Government cannot confiscate them for using the restricted term 'coin'. The U.S. Government has in the past confiscated great quantities of competing currencies. They hold the monopoly and want to maintain it. I assume that Bitcoin and other cryptocurrencies will eventually fall victim to government hegemony. Bitcoin fact **(7)** and myth **(8)** pages have explanations of just about anything you might want to know.

1) http://bitcoin.org/
2) https://en.wikipedia.org/wiki/Cryptocurrency
3) http://bitcoincharts.com/
4) https://en.bitcoin.it/wiki/Satoshi_Nakamoto
5) https://www.weusecoins.com/en/mining-guide
6) https://litecoin.org/
7) https://en.bitcoin.it/wiki/FAQ
8) https://en.bitcoin.it/wiki/Myths

Two million passwords of Facebook, Twitter, Yahoo, FTP, LinkIn, and Gmail were compromised **(1)** by the illegal Pony botnet **(2)**. If you think you have been compromised, change your passwords on anything that involve money. They collected keyboard keystrokes on the botnetted PCs. This could lead to identity theft or just plain stealing.

1) http://sn.im/28acsbc
2) https://en.wikipedia.org/wiki/Botnet

I think Brad Reed **(1)**, a home computer pundit, makes some interesting points regarding consumer resistance to Windows 8 **(2)**. He points out that customers either hate or love this version of Windows

on a more or less equal basis. In past versions most customers were on one side or the other.

1) http://bgr.com/author/brad-reed/
2) http://sn.im/28acsci

A division of Samsung, the TV, tablet, hard drive maker, also builds ships **(1)**. They have built the largest ship in the world at about 1,600 feet long and 240 feet wide. This ship dwarfs the Great Lakes 1,000 foot ore boats. This ship is designed to collect natural gas from the sea bed and process it for compact storage (cool it to -260 F degrees). The ship is called Prelude is powered by three 6,700 HP diesel engines.

1) http://sn.im/28acse8

If you have been affected by the Tuvaro **(1)**, Snapdo (**(2), (3)**), or the Sandori (**(4), (5)**) redirection viruses here are the methods to remove them. These are known as Browser Helper Objects (**(6)** BHO)

1) http://botcrawl.com/remove-tuvaro-virus/
2) https://support.mozilla.org/en-US/questions/944832
3) http://malwaretips.com/blogs/snap-do-toolbar-removal/
4) http://www.2-spyware.com/remove-sendori.html
5) http://sn.im/28acsfu
6) https://en.wikipedia.org/wiki/Browser_Helper_Object

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

---

continued from pg 5

still a good idea.

If your email is a POP account, as opposed to a web mail account such as Hotmail or Gmail, the odds are higher that your computer has been hacked, which is a much larger problem. The best solution is to restore a backup system image made well before the hacking was suspected. The chance that you have a backup image to restore is as likely as the intruder putting money into your bank account, but this instance is when
you want backups. Lacking a backup, you can thoroughly scan your system with several antimalware products in addition to your normal antivirus product.

Again, you should change the passwords for your Internet Service Provider, router, and
email, and be sure that your Wi-Fi network is protected with the highest level of security possible. People often hate passwords on computers; but if any computer on the network was hacked, all computers on the network should have logon passwords. Fortunately, protecting the network is enough in most cases.

Personally, I'd suggest you change your email password, scan your computer with your up-to-date antivirus software, and wait to see what happens. If possible, do not do any online shopping or banking until some time has passed to confirm that only your email was hacked. Also watch for any suspicious activity on credit card and bank accounts.

November / December 2013 DVD of the Month

AdwCleaner - Updated malware remover
ARI - November / December newsletter
AuslogicsDefrag - Updated HD defrag program
BlackBeltPrivacy - Program to ensure privacy on the Internet
CainAndAbel - A password recovery tool
cCleaner - Updated HD cleaner
Chameleon - Updated a program to run Malwarebytes when block by malware
CryptoPrevent - Program to prevent Cryptolocker infection
Firefox25 - Updated web browser
FoxitReader - Updated PDF reader
FreeSoundRecorder - the name says it all
HijackThis - Updated malware investigation tool
JRT - Updated Junkware removal tool
LibreCAD - Free CAD program
MalwarebytesAntiExploit - Protects MS before security patches are issued
MalwarebytesAntiMalware - Updated anti malware program
MboxImport - Thunderbird backup tool
MemberContributions - Things e-mailed to me from members
MozBackup - Backup and restore bookmarks, mail, contacts for Mozilla products
MP3Tag - Tool to change tag information in MP3 files
MyEventViewer - Tool to make sense of Windows log files
NotepadPlusPlus - Updated text editor
OldTimeRadio - Old time radio broadcasts
PDF24Creator - Create and edit PDF files
Recuva - Updated undelete tool
RogueKiller - Detect and remove generic malwares, rootkits, rogues, worms, etc.
Sandboxie - Updated Sandbox protection
ScreenshotCaptor - Take screen shots of all or part of the screen
Speccy - Updated hardware inventory program
StartupDelayer - Tool to delay programs from starting immediately at startup
SyncBack - Synchronizes your files to the same drive, a different drive or medium
SyneiPCCleaner - PC HD cleaner
TeamViewer - Remote control software
TightVNC - Updated remote control software
Tweaking - Control of Windows firewall
VirtualBox - Updated virtual machine
VLC - Updated media player
Wavosaur - Audio editor
WhyICantConnect - Diagnose TCP/IP connection problems
WinAmp - Media player

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 MikeGold60137(at)yahoo.com. 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 MikeGold60137(at)yahoo.com, at least five (5) days prior to the program, so that reasonable accommodation can be made.

Members Helpline
Any member with a specific expertise can volunteer to be on the Members Helpline.

Beginner Helpline
- Billy Douglas

Beginner hardware problems
- Dick Fergus

Hardware problems, XP, Win 7 & Linux
- John Spizzirri

CAEUG OFFICERS

President	Mike Goldberg
V.P. (Programs)	Roger Kinzie
Secretary	Al Skwara
Treasurer	John St. Clair
Newsletter Ed	Kathy Groce
Board Member	Billy Douglas
Webmaster	John Spizzirri