



### It Seemed Like Only Yesterday .....

By Frank Varano

"It seemed like only yesterday that I owned a wire recorder." But it was really about 40 years ago. It seemed like only yesterday that I bought a 128 mb USB flash drive. But it was only 4 months ago. Now we have 32 GB available. The one pictured is \$125.

I talked about the march of progress in storage technology before and I still predict the demise of the noisy hard drive. Who in the world would bother with putting any of your Computer stuff on a CD? Will the CD go first? We'll see.

### An Interesting Observation

By the Editor

Over the past 6 to 7 years that I have been with the CCMV I've notice a gradual transition from a predominantly male membership to predominantly female membership.

Since I help a lot of the Club residents I've also noticed that there are more women using computers than men. Interestingly, in households where both spouses are still alive it is mostly the woman in the house who has and uses the computer.

I wonder if it is a matter of longevity. Hmm.

### A Quick and Easy E-Mail Backup System

Source: Lifetracker

You no doubt know that you should be backing up important files on your computer. But what if you don't have access to your office's server, a flash memory drive, or another backup system?

Well, if you have two e-mail addresses (work and personal, for example), just e-mail a copy of the file to yourself. Because that file will be stored on the provider's server, nothing that happens to your own computer will affect it.

### Your Hard Drive Tree

By F. Varano

I stumbled across this thing the other day and frankly, I think it is a bit of useless information. I wasn't looking for it but since I saw the word 'tree' it intrigued me into thinking that I should branch out my knowledge. Perhaps you can find it useful. Anyway, it is a way to show the contents of your hard drive in a tree form. Exciting, isn't it. Here is how you do it.

Click on Start, Run, and type `Tree >Tree.rtf`. And click OK. You'll see a solid black rectangle flash on the screen for a fraction of a second. And I mean, a fraction of a second. If it was there a millisecond I could read it.

When I first did this I thought it was a joke. But the next instruction said to open a blank Word Document, then click on *Insert | File*, which I did dutifully. I didn't know where the file *Tree.rtf* was located. Heck, I didn't even get a chance to say where to put the *Tree.rtf*. So how could I find the file?

I did the next stupid thing I could think of. I searched for *Tree.rtf*. Guess what? It was located in the root directory of Local Drive C. Going back to *Insert | File* I knew now where to find it. It was in `C:\Tree.rtf`.

OK, all of you now together shout, "Frank, you idiot, that black rectangle was the clue. If you read fast enough you would have seen `C:/Tree.rtf` in that "black box!" or is it `C:\Tree.rtf`?

Now you know how to get the black box, ...no the disk tree. And if you can read what is on that black box please write me an email.



**Board of Directors**

**President**

Jim Richardson  
PRESIDENT@ccmv.net

**Vice President**

(Vacant)  
VP@ccmv.net

**Secretary**

Jim Semanek  
SECRETARY@ccmv.net

**Treasurer**

Chet Hartley  
TREASURER@ccmv.net

**Director at large**

(Vacant)

**Help lines:**

**Windows XP**

Bill Oberg—672-3387  
wobergr@verizon.net

**Microsoft Word, Excel & PowerPoint**

Joannie Lenz—301-6226  
Joannie@RainbowFlair.com

**Newsletter**

E-mail your articles, comments and suggestions and information to:  
EDITOR@ccmv.net or  
tmradius@verizon.net

**Web Page Address**

www.ccmv.net

Good info on our Web Site.  
Read and download the newsletter at the web site.  
(No newsletter in August)

**Club Meetings:**

2nd and 4th Tuesdays  
9:00 a.m. to 11:00 a.m.  
Seventh-day Adventist Church  
29885 Bradley Road,  
Sun City, CA  
Many free magazines, books items and loaners. Pick up a copy of the newsletter

**Web Threats Increase**

The World Wide Web now hosts an unprecedented number of threats, with Sophos discovering a new infected webpage every 5 seconds. This is an average of more than 15,000 every day, three times more than in 2007. Sophos also discovered that a new spam-related webpage appears almost every 3 seconds.

However email threat declines. Only 1 in every 2500 emails are infected, compared to 1 in every 909 in 2007.

In 2007, SophosLabs® – our global network of researchers and analysts – discovered a new infected webpage every 14 seconds – today that figure has dropped to 1 in every 5 seconds; 79 percent of these are legitimate websites.

[Editor: That explains why I am spending a lot of time cleaning out other's computers that have slowed to a crawl.]

**Are You a Password Nut?**

By F. Varano

It is appalling to me how callused PC users are about creating and storing passwords. I find myself remembering passwords for others because they are too careless in creating them and remembering them. Someone gave me a computer to 'clean up' but he couldn't remember the password to access the XP operating system. Believe it or not I was able to get to the Safe Mode and wipe out the users' accounts.

I wrote previously on how to create relatively secure but easy to remember passwords by using patterns. It is not easy to remember a series of random numbers and characters but it is easy to remember a pattern. You can create your own pattern but I use the keyboard. I suggest that you go to the club web page and dig out that article if you are having problems with passwords.

If you forgot a password to access XP OS, try going to the Safe Mode, otherwise email me about the Windows XP Password Reset Disk.

**Profile of the Recovery of a Slow Computer**

By Frank Varano

Here is an actual case I worked on in my area. It is a severe case of the typical problems I have been working on lately.: The computer that has slowed to a crawl. (Next page.)

**Department Leaders**

**Membership**

Dee Morris  
MEMBERSHIP@ccmv.net

**Material Distribution**

Dorothy & George Metcalf  
GWDJM@Verizon.net

**Shareware Distribution**

Position Open  
Need Volunteer

**Newsletter**

Editor: Frank Varano

Newsletter:  
Reporters & Articles:  
E-mail your articles, comments and suggestions to:  
EDITOR@ccmv.net

**Computer Lab Technician**

Jim Richardson

Web Site  
Jim Semanek  
WEBGUY@ccmv.net

\*\*\*\*\*

**Computer Instruction**

**Registrar**

Sonnie Banisch  
REGISTRAR@ccmv.net

**Teachers & Assistants are CCMV members.**

**Would you like to teach?**  
Would you like to help our teachers? Come to the meeting and tell us. Or email Carol.

**Computer Classes:**

**We're in full swing  
Call for class information and sign-ups**



<b>Monthly Income and Expenses</b>		
7/1/2008 thru- 8/31/2008		
Chet Hartley, Treasurer		
<b>Income (\$)</b>	7/2008	8/2008
Contributions	47.00	67.75
Interest	3.17	2.63
Shareware/Freeware Sales	20.00	5.00
Textbook Sales	20.00	155.00
Tuition		315.00
<b>Total Income</b>	<b>90.17</b>	<b>545.38</b>
<b>Expenses (\$)</b>		
Church Usage	125.00	125.00
Newsletter expenses	10.25	
Lab expenses	97.21	
<b>Total Expenses</b>	<b>232.96</b>	<b>125.00</b>
<b>Income less expenses</b>	<b>142.79</b>	<b>\$ 420.38</b>

*(Continued)*

I got a panic call from the user that he simply could not use his computer. He couldn't get his email and had a difficult time accessing the Internet.

Sitting at his computer I found that his anti virus expired long ago. He had no anti malware. I had with me my USB Flash Drive with AVG 8, Spybot, and Ad Aware. Currently these are my standard programs for battling viruses and malware.

When I go on such a mission I first try to get Housecall by Trend Micro to get a thorough scan of the computer. Then I install those three programs and get Windows Defender.

As a general rule, when the infestation is really bad I can't get to Housecall at all. AVG will not install and Spybot will not install. Almost always Ad Aware will install, update and scan. This was what I faced on this call. On top of that it took a long time to do anything on his computer.

Anybody who is so negligent usually has never done any disk scan or defragging. I start there to remove as many obstacles as possible right off the bat to get the computer to speed up a bit. In this case it helped me. I was able to install Ad Aware and run it. I found and removed over 300 malware objects. The computer speeded up a bit so that I felt encouraged to try Housecall. But no. And AVG would not install, either.

But Spybot installed OK. I ran the updates too and then scanned the computer. Keep in mind that these scans take a long time and *(next col.)*

*(From left column)*

I can't sit there and wait for the scan so I leave and schedule a return when the scan is done. I ask the user to call me. In this case I could walk to his house. Spybot found a lot more objects which were 'Fixed' by Spybot. Now the computer had perked up and I successfully installed AVG 8 which I considered as the 'big guns.'

I let it scan and again left. Mind you this is taking place over two days. The complete AVG scan takes hours because it scans for viruses and for malware.

The next day I saw that we were on the road to recovery. AVG did its job and for practical purposes I could have called it done but I decided to get Microsoft Windows Defender and run it too. I am not sure that the Defender is as good as the other three programs. I have never seen Defender say that it found and deleted any malware.

I considered the job done but not without first giving him (by email) a set of written instructions on how to do these scans routinely.

Specifically, AVG and Defender can be programmed to do their thing at any night at 11 PM and 2 AM respectively. That makes it simple to tell the user to leave his computer on one night a week.

His situation was so bad that he was overjoyed to see his computer back and running. He even paid me!



**What you can do:**

If an e-mail message asks you to update your password, account number, or other information, don't take the bait. Access an online account only by using your existing browser bookmark or typing in the institution's Web address. If you suspect that an e-mail is a phishing attempt, forward it to *spam@uce.gov* and *report-phishing@antiphishing.org*.

**Editor's Note:**

I haven't been able to find the time to write about Clipmate that I talked about previously. Clipmate is a pretty sophisticated program and a very powerful one. It is most useful if you need to assemble a lot of stuff to paste to various places.



## Ransomware!

By Frank Varano

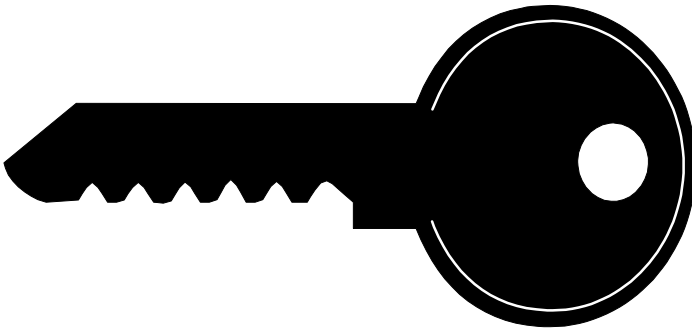
Virus analysts at Kaspersky Lab have intercepted a new variant of Gpcode, a malicious virus that encrypts important files on an infected desktop and demands payment for a key to recover the data.

Egads! Now we have ransomware!

I am going to try to explain something about this but don't feel bad if you don't understand it. I'll go as far as I understand it then assume that beyond that point you and I are both lost.

The Kaspersky people started getting reports from infected victims, analyzed a sample, and added the detection to their antivirus databases (in June.) Although the Kaspersky people could detect the virus itself, they couldn't decrypt files that were encrypted by Gpcode – the RSA encryption in the malware uses a very strong, 1024 bit key.

Here is the explanation. Maybe some of you will understand it. The biggest change in this variant of the ransomware is the use of RSA encryption algorithm with a 1024-bit key, making it impossible to



crack without the author's key. So what are we talking about? Here is the standard explanation: "The RSA encryption algorithm uses two keys: a public key and a private key. Messages can be encrypted using the public key, but can only be decrypted using the private key." At this point just pretend you understand it along with me.

And this is how (this variant of the) Gpcode works: it encrypts files on victim machines using the public key which is coded into its body. The files can only be decrypted using the private key – and guess who has it?

Without really understanding this encryption stuff it appears that after Gpcode encrypts files on the victim machine, it adds `._CRYPT` to the extension of the encrypted files and places a text file named `!_READ_ME_!.txt` in the same folder. In the text file the criminal tells the victims that the file has been encrypted and offers to sell them a "decryptor": And ransomware is born.

*«Your files are encrypted with RSA-1024 algorithm.  
To recover your files you need to buy our decryptor.  
To buy decrypting tool contact us at:*

*\*\*\*\*\*@yahoo.com.»*

The culprit used three Yahoo e-mail addresses with the new version of the ransomware.

Well, does this affect us? I really don't know. It is conceivable that the culprit could have thousands of 'ordinary customers' and rake in millions. Look, I'll study this stuff and if any of you would like to work with me, we can make a mint for CCMV. Contact me at: `decryptor322@yahoo.com`.

---

## Sneaky Charges by Banks— Maximizing Overdraft Penalties

By F. Varano

Let's say the bank has one large check and a bunch of smaller ones to clear. And let's say that clearing all the little checks would not trigger the overdraft. Let's say further that the big check by itself would indeed trigger the overdraft. Now, tell me, which check would the bank clear first? Huh? The big one first, of course, then clearing all the little ones would add penalties. Sneaky?

Bank of America, Citibank, HSBC, Wells Fargo and many other banks engage in the practice. Simply bounce the biggest one first and then the smaller ones. With a fat fee of 30 or 40 bucks for each bounced check and the merchant's charge for a bad check, that can add up equivalently to many prime rib dinners.

Natch, the banks have a rationale for doing this. They are looking out for you because the big checks are the "most important."

The banks claim they do this because large checks tend to be the most important. How about a real example: Five checks you wrote reach your bank on a given day -- four checks for small items followed by a \$1,600 mortgage payment. If there is only \$1,500 in your account, only the final check -- the big mortgage payment -- should bounce. Instead, your bank processes the large mortgage payment first, which means that all five checks will bounce. Rather than a \$30 or \$40 overdraft fee and one upset check recipient, you now face \$150 to \$200 in overdraft fees and five perturbed check recipients. Hey, I am in the wrong business!

What to do? Simply have enough money in your account if you can. Second, learn how to monitor your account online. Then do the simple arithmetic necessary.

A penalty when you bounce a check is one thing -- but some banks also charge another fee of \$5 to \$10 to the sucker that got the bad check. There is a self defense measure you can take. Just don't take checks as payment for something. Insist on cash. Place the burden on the recipient to get the cash. Self-defense: Do not accept checks as payment even if you think you can trust the payer.