Launceston Computer Group INCORPORATED NEWSTREAM

The Journal of the Launceston
Computer Group Inc
ABN 41 451 764 376

Volume 10 Issue 4
May 20112011

INSIDE THIS ISSUE:

Next Meeting

Wednesday 4th May 2011

at7.30 PM Workshop

Dennis will show the power of Excel Workbook

Happy Mothers Day to all Mums

Newstream Articles

Deadline : 10 Days before Meeting

Editors Contacts:

Address: 8 Cadorna Street Mowbray Heights 7248 Phone 6326 5824

email address editor@lcg.org.au

Correspondence

Address all Correspondence to: Launceston Computer Group Inc PO Box 548
Launceston 7250

Membership

Single $15, Family $20 (Includes Email edition Newstream)

Printed & Posted Newsletter $20 extra

Disclaimer: *The articles in this newsletter may be reprinted as long as credit is given to the original author. Opinions expressed are those of the author & not necessarily the views of the Editor or the Group. Unless otherwise noted material is copyright 2004 for the Launceston Computer Group Inc.*

LCG COMMITTEE

President: Ivan Turmine
Vice President: Janet Headlam
Minutes Secretary: Iris Meek
Treasurer: Laraine Rist
Assistant Treasurer Open
MAC Librarians: Ivan Turmine
PC Librarian: Julie Hjort
Newstream Editor: Ron Baker
Public Officer Judy Hall
Publicity Officer: Iris Meek
Maintenance Co-ordinator; Dennis Murray
OPEN Co-ordinator: Robert Tierney
Webmaster/Content: Tom Olsen
Auditor: Ron Baker
"VICTOR" Co-Ordinator: Robert Tierney
Liason Officer Eleanor Horder
General Committee: Glenn Gilpin,
Reinhard von Samorz Harvey Tavener
Barry Symonds

OPEN Committee 2011

Chairperson	*June Hazzlewood*
Co-ordinator	*Rob Tierney*
Vice Chairperson	*Rob Tirney*
Minute Secretary	*Eleanor Horder*
Treasurer	*Laraine Ridst*
Assistant Treasurer	*Open*
O Learn Co-ordinator	*Eleanor Horder*
Tutor Co-ordinator	*E Horder*
Assist Treas.	*Laraine Rist*
Membership Co-ord.	*K Wicks*
Newsletter Editor	*Iris Meek*
Publicity	*I Meek*
Committee:	*Heather Loffell,*

Marie Cleaver, Kay Dawson, Irmgard Rosenfeldt, Pauline Hardy, Sandra Viney, Janet Headlam

OPEN NEWSLETTER May 2011

Coordinators Corner

Rob will inform the class about various aspects of internet security.

A must do session in present times.

Friday May 27

10 am—noon

Graphic Workshop Classes

May 4 10–noon

June 1 10–noon

A big thank you to the willing hands who turned up to the "Working Bee" in the club rooms Saturday April 30.

We now have a much tidier work place.

.

PSP XI Graphics

Advanced graphics with Eleanor, Karia, Sandra, Margaret & Laraine

May 25 1 pm—3 pm

June 22 1 pm—3 pm

July 27 1 pm —3 pm

SPECIAL CLASSES

Using the new Print Artist Software.

Learn to make Notices, Cards, Banners etc.

Computer Security with Rob TierneyMay

OPEN COMPUTING TELEPHONE 63434928

Between 10 am and 3 pm weekdays.

VICTOR mobile 0408 174235

FAMILY HISTORY ON-LINE

Until further notice, two morning classes in Family History are held each month at OPEN.

Students use either the internet or the club's own CD based history links to locate their ancestors and relatives.

Places are limited so make sure you put your name on the Registration Form near the front desk.

May 18 and 25	10 am 'til noon
June 15 and 22	10 am 'til noon

Please have a basic chart made out. Father, mother or grandparents with perhaps a birth, baptism or death date or two to begin with.

Another session on how to use Family History Links will be held at a later date.

Basic Graphics

with Judy, Karia, Laraine & Sandra

May 11 10am to noon

June 8 10am to

noon

OPEN Session Times

Studioworks, 1 Pipeworks Rd, L'ton

Standard Sessions $5.00

		Beginners
	1 pm – 3 pm	**Beginners & PC Support**
Tuesday	10 am –12	P C Support & Beginners + Mac
	1 pm – 3 pm	**As above**
	7 pm—9 pm	PC Support (Night Class)
Wednesday	10 am—noon	Special sessions or Meetings
	1.pm—3 pm	As for mornings (see rosters)
	3.30—5.30	P C Support
Thursday	10 am –12	General & Beginners
	1 pm – 3 pm	General & Beginners
	3.30—5.30	Absolute Beginners
Friday	10 am –12	General & Beginners
	1 pm—3 pm	Beginners

OPEN NEWSLETTER – May 2011

SPECIAL WEDNESDAY SESSIONS

Please register on the sheets – numbers may be limited

Date	Time	Topic	Details
May 4	10 am—12 noon	Graphics Workshop	Judy, Karia, Laraine & helpers
	1 pm— 3 pm	**OPEN MEETING**	**It's your club...Have a say in it.**
May 11	10 am—12 noon	Basic Graphics	Judy, Margaret, Laraine & Sandra
	1:00—3 pm	**Print Artist 23**	Eleanor, Karia, Laraine, and Snadra.
May 18	10 am—noon	Family History	Finding your ancestors on line with Judy
	1 pm— 3.00	**Level 2—3 Graphics**	**Using PSP 7 and 8**
May 25	10 am –noon	Family History On Line	Judy, Margaret, Laraine & Sandra
	1 pm— 3pm	**PSP X!**	**Advanced Graphics with Eleanor, Karia, Judy, Laraine & Sandra**
June 1	10 am-3pm	Graphics Woprkshop	**Refresh lessons learned so far this year.**

Open meetings 1pm onwards May 4 & June 1

OPEN COMPUTING & LAUNCESTON COMPUTER GROUP

May 2011 Roster

	Monday	Tuesday	Wednesday	Thursday	Friday
10 am to 12 noon	**Beginners/** **PC Support**	**PC and Mac Support** **Beginners/**	**Second Step Tuition** ***Please Register on Board***	**Beginners/** **PC Support**	**Begin-ners/** **PC Sup-**
	Laraine Karia Heather Tony	Rob Eleanor Tom Jenny Tony Sandra V *(Mac)*	WEEK 1 May 4 Graphics Workshop WEEK 2 May 11 Basic Graphics WEEK 3 May 18 Family History WEEK 4 May 25 Family History	June Kari Jenny Tom	Rob Robin B
	Up to 12	Up to 12	Judy, Eleanor, Karia, Laraine, Sandra, Margaret, Iris	Up to 12	Up to 12
12 noon to	Lunch	Lunch	Lunch	Lunch	Lunch
1 pm to 3 pm	**Beginners and** **PC Support**	**Beginners and** **PC & MAC** **Support**	**Second Step Tuition** **(1 to 3:00 pm)**	**Beginners** **and PC** **Support**	**O Learn**
	Laraine Karia Tony Jenny	Rob Eleanor Tony Ron Tom Jenny *(Mac)*	WEEK 1 May 4 OPEN MEETING WEEK 2 May 11 Print Artist WEEK 3 May 18 Level 2-3 Graphics WEEK 4 May 25 PSP X1 Graphics WEEK 1 June 1 OPEN MEETING	June Tom Karia Tony Jenny	Robert Eleanor
3.30-5.30	Up to 12	Up to 12	Judy, Karia, Laraine, Sandra V, Margaret, Eleanor and Tony	Up to 12	
Evening	3.30 – 5.30 O Learn Robert		LCG Meeting May 4 at 7.15 pm Followed by Workshop on Excel Workbook	3.30 – 5.30 O Learn Robert	

LizaMoon infection: a blow-by-blow account

By Fred Langa

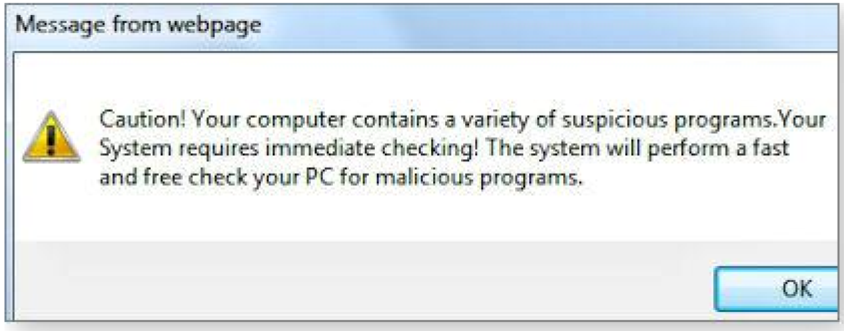
Fortunately, LizaMoon is easy to avoid if you know what to look for.

Using rogue-AV scare tactics, LizaMoon tries to trick you into running bogus security-scan and virus-cleanup tools on your PC — but it's pure malware.

If allowed onto your PC, this particular ploy is especially troublesome because it can partially disable the Windows Security Center and change the Registry so that the full WSC can't be restarted. It also interferes with Microsoft Security Essentials, if MSE is running. (You'll find lots more LizaMoon news coverage via Google.)

My encounter with LizaMoon started unexpectedly one evening when a suspicious warning popped up on my screen. As discussed in a previous Top Story, I use Microsoft Security Essentials and the Windows 7 firewall to protect all of my PCs. In over a year of constant use, I'd never had any malware trouble. But that abruptly changed.

That evening, I was searching for something through Google — I don't recall what. When I clicked a link, a blank page overlaid with the dialog in Figure 1 popped up instead of the site I was expecting.



Message from webpage

Caution! Your computer contains a variety of suspicious programs.Your System requires immediate checking! The system will perform a fast and free check your PC for malicious programs.

Figure 1. A real LizaMoon initial dialog, captured in the wild.

My mental alarm bells immediately started ringing — the dialog was identified as a **Message from webpage.** But why was a random, external webpage displaying what looked like a local security message?

Also, how could a random webpage know what was installed on my system (suspicious programs or not)? The warning made no sense.

There was plenty more to suggest that the dialog was bogus. For example, the third sentence is in fractured English — Microsoft dialogs aren't like that. And the kicker: I keep my system very clean, so the odds that it would suddenly contain "a variety of suspicious programs" are virtually nil.

Then it struck me. I'd encountered a for-real LizaMoon page hijack, in the wild!

Typically, when you encounter any suspicious webpage dialog, the correct procedure is to immediately dismiss it via the **red-X close box** in the upper-right corner of the dialog box or to simply close the browser. (If needed, you also can use Windows' Task Manager to kill offending software or its processes.)

Next, if you think you might have a security problem, you should manually launch known-good security tools directly from reliable sources. In no case should you ***ever*** launch unknown software triggered by visits to random websites.

In my case, however, this was exactly the kind of malware I'd been looking for to test. In the past few months, readers reported encountering new malware that masquerades as a security tool — malware that disables or bypasses Microsoft Security Essentials. I'd been trying to track it down for weeks. And suddenly, there it was.

Living dangerously: taking the malware's bait

Given this unexpected opportunity, I took a deep breath and clicked OK, knowing full well that I was voluntarily giving the webpage permission to interact with my PC.

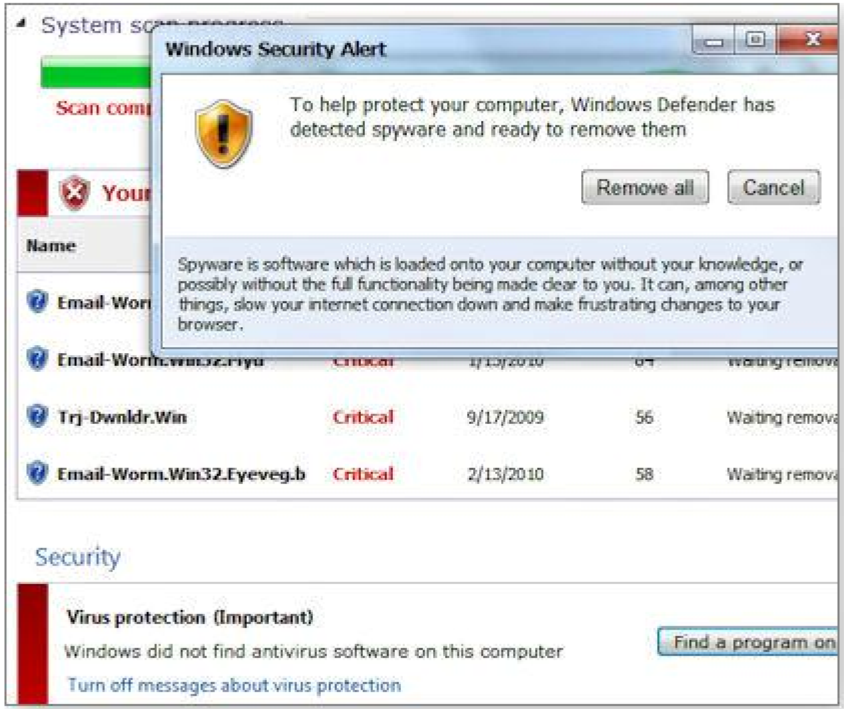
A new webpage opened, showed a flurry of fake "scanning" activity (most likely, just an animated **.gif**), and then reported a huge number of discovered viruses and security problems.

(Continued on page 7)

(Continued from page 6)

I knew my system was clean, so this report of widespread infection was clearly fake. But because the page layout and icons closely mimic those of familiar Windows tools, it could easily fool casual users into thinking that the alert was real.

After a minute of fake scanning activity, a new dialog opened — offering to "Remove all" the threats (see Figure 2).



Windows Security Alert

To help protect your computer, Windows Defender has detected spyware and ready to remove them

Remove all | Cancel

Spyware is software which is loaded onto your computer without your knowledge, or possibly without the full functionality being made clear to you. It can, among other things, slow your internet connection down and make frustrating changes to your browser.

Trj-Dwnldr.Win	Critical	9/17/2009	56	Waiting remova
Email-Worm.Win32.Eyeveg.b	Critical	2/13/2010	58	Waiting remova

Security

Virus protection (Important)

Windows did not find antivirus software on this computer

Find a program on

Turn off messages about virus protection

Figure 2. Clicking "Remove all" on this fake security dialog starts the malware download. Find a way to close the dialog, as discussed in the text.

The new dialog set off more of my internal alarm bells. Windows normally identifies the software or subsystem involved in security alerts — such as the Action Center, the Security Center, Security Essentials, or whatnot. A dialog simply labeled "Windows Security Alert" is suspiciously generic.

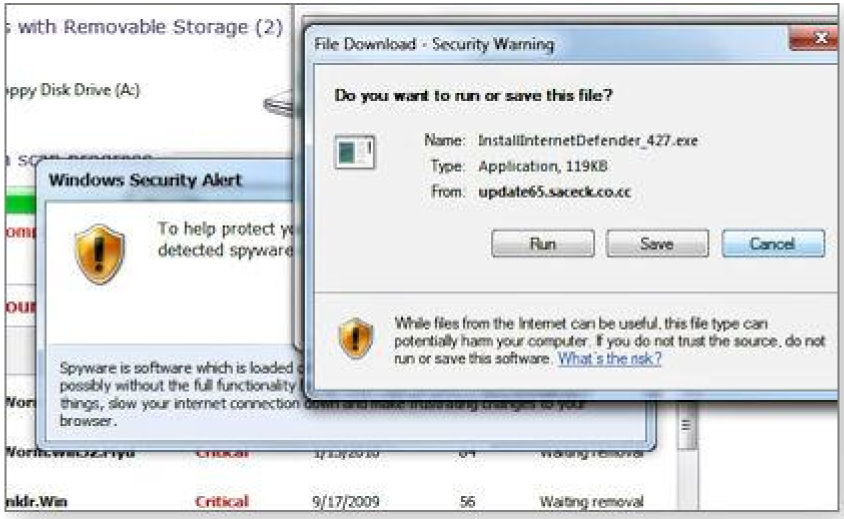
And what's this about "Windows Defender"? That's Microsoft's standalone anti-malware tool that ships with Vista and Win7 and is available as a free download (page) for XP. The forerunner of the more complete Microsoft Security Essentials, it's deactivated when you install MSE. Since I have MSE active on my system, I shouldn't be hearing from Windows Defender.

At that point, you'd normally try to dismiss the warning by clicking on the red X. To see what would happen next, I clicked "Remove all," knowing I was inviting trouble.

(If you're keeping count — and I did — you'll know this was my second entirely voluntary action leading to infection.)

A real and quite legitimate Windows file-download security warning opened, as shown in Figure 3. But while the previous dialog discussed "Windows Defender," this dialog box asked permission to download an installer for "Internet Defender." What's more, the dialog clearly showed that the file was from a site called update65.saceck.co.cc — not Microsoft!

Clearly, the LizaMoon authors are confident that people do not pay attention to these details.



File Download - Security Warning

Do you want to run or save this file?

Name: InstallInternetDefender_427.exe
Type: Application, 119KB
From: update65.saceck.co.cc

Run | Save | Cancel

While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not run or save this software. What's the risk?

Windows Security Alert

To help protect y
detected spyware

Spyware is software which is loaded o
possibly without the full functionality
things, slow your internet connection down and make frustrating changes to your
browser.

Figure 3. This dialog box has several naming in-

(Continued on page 8)

(Continued from page 7)

consistencies: the previous dialog mentioned Windows Defender, but this one offers something called Internet Defender. It also isn't coming from a known address, such as Microsoft.com.

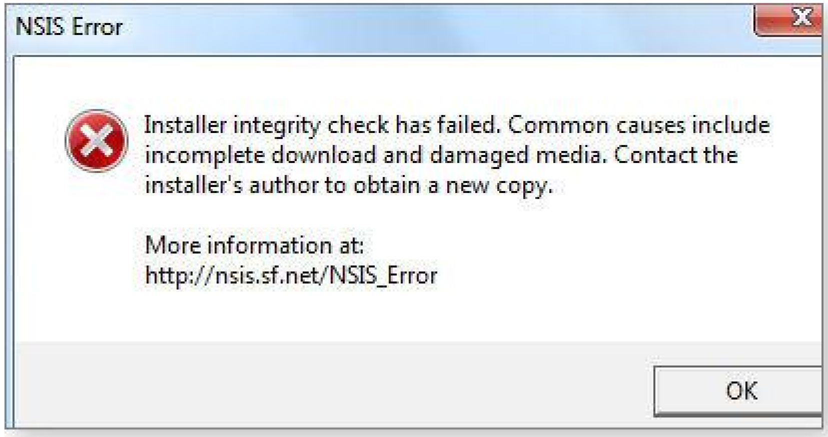
Ignoring yet another opportunity to bail out before being infected, I clicked the Save button and entering the location where the file should be saved (the third voluntary action on the path to infection).

My hard-drive light flickered briefly and I swallowed hard, knowing that a malicious payload had just been delivered to my personal PC. (Yes, my system was fully backed up and my sensitive data encrypted.)

Ready or not, the malicious payload arrives

I intended to disconnect my PC from the network before the malware ran, assuming that going offline would keep any system damage local and no personal data could be exported.

But there must have been a script running somewhere, because the malware installer immediately attempted to self-start. Fortunately, Windows reported an **NSIS error** (see Figure 4). NSIS is SourceForge's Nullsoft Scriptable Install System, and the error means that an installation script failed an integrity check.



NSIS Error

Installer integrity check has failed. Common causes include incomplete download and damaged media. Contact the installer's author to obtain a new copy.

More information at:
http://nsis.sf.net/NSIS_Error

Figure 4. The first sign of trouble after downloading the malware

Following the link given with the NSIS Error opens a sourceforge.net page advising you to "Update your anti-virus software" and to "Scan for, and remove malware and viruses on your system."

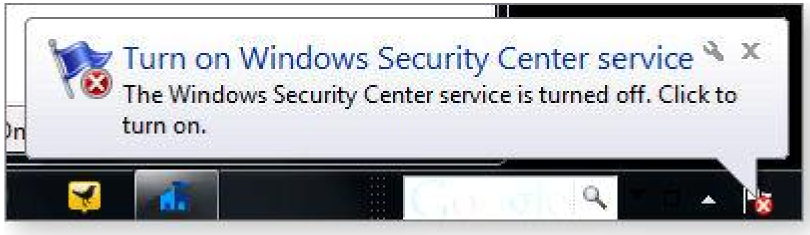
Microsoft.com's "NSIS Error" page states that, among other possible causes, "Your PC is infected with a virus." It adds, "Thoroughly scan your PC for possible virus or spyware infections." The page even provides a direct link to Microsoft's free online safety scanner (site) and to a discussion of how to remove viruses and malware.

I took none of that advice but did disconnect from the network. Taking yet another deep breath (and my fourth voluntary action), I clicked OK, which let the malware installer run to completion.

The malware goes active and disables my security

Immediately after I clicked OK, my system went haywire.

First, the Windows Security Center was compromised (see Figure 5), and I could not manually relaunch it — proof that my system was infected.



Turn on Windows Security Center service

The Windows Security Center service is turned off. Click to turn on.

Figure 5. The infection immediately disabled the Windows Security Center.

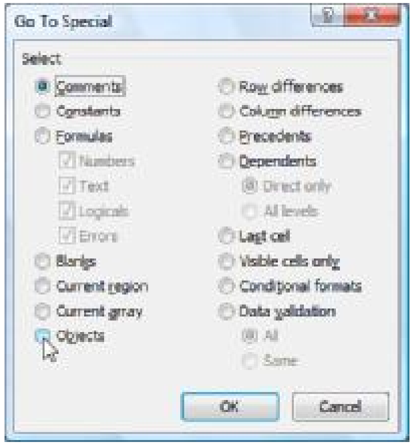
Next, the downloaded malware opened a new, fake, scanning window. Calling itself "System Defender," it claimed to have discovered numerous malware apps. Trying to learn what I could about the bogus software, I opened its Help/About menu, as shown in Figure 6.

(Continued on page 13)

Deleting All Graphics

Excel allows you to easily add graphics to a worksheet. This can be helpful at times, but at other times you may want to delete all the graphics in a worksheet. The easiest way to delete all the graphics is to follow these steps:

1. Press **F5** to display the Go To dialog box.
2. Click on the Special button. Excel displays the Go To Special dialog box.



Go To Special

Select

● Comments
○ Constants
○ Formulas
☑ Numbers
☑ Text
☑ Logicals
☑ Errors
○ Blanks
○ Current region
○ Current array
○ Objects

○ Row differences
○ Column differences
○ Precedents
○ Dependents
● Direct only
○ All levels
○ Last cell
○ Visible cells only
○ Conditional formats
○ Data validation
● All
○ Same

The Go To Special dialog box.

3. Make sure the Objects radio button is selected.
4. Click on OK. All the graphics in your worksheet are selected.
5. Press the **Del** key. All the graphics are deleted.

This solution works only if there are no other objects (besides graphics) in your worksheet. If you have other objects that you don’t want deleted, then all you need to do is perform steps 1 through 4, and then hold down the **Ctrl** key as you use the mouse to click on each object you don’t want deleted. When you are satisfied with the objects selected, finish up by following step 5.

Selecting an Entire Paragraph

If you are using the mouse, Word provides several quick ways to select an entire paragraph. First, you can simply triple-click anywhere within the paragraph. This is perhaps the fastest and most common method of selecting an entire paragraph.

Second, you can move the mouse pointer to the left of the first character in any line of the paragraph you want to select. The mouse pointer turns into an arrow pointing up and right. Double-click the mouse, and the paragraph is selected.

Finally, if you are using the style area, you can also move the mouse pointer into the style area to the left of the paragraph you want to select. Click once on the left mouse button, and the entire paragraph is selected.

If you like to use the keyboard instead of the mouse, you can select the current paragraph by pressing **Ctrl+Up Arrow** (which moves the insertion point to the beginning of the paragraph) and then pressing **Ctrl+Shift+Down Arrow**.

How to Stay Safe in Public

Let's face it, there comes a time in everyone's life, whether they like it or not, when they are compelled to use a public computer. This might be in an Internet café, public library an airport or in a hotel. Sometimes you just have to deal with it - indignity or not. Here are a few public house policies to follow so you don't end up in the slammer or worse than that - your private info absconded. Let's try and keep the private stuff private-okay?

Rule Numero Uno: Do Not, I repeat Do Not - don't save your login on a public computer. This is just too tempting for the next guy. He may not be able to read your mind but he sure may guess at the password or have some device that feeds fifty gazillion entries into the wazoo and he steals your money. We don't want that. So don't under any circumstances allow your public computer to save your logon. Got it? Good!

Rule Numero Dos: After you have logged into a site, it is really a good practice to actually logout of that site when you are done. Don't just close the browser and walk away. That I can assure you my friends is not a bright thing to do. You can experiment with this at home. Log into Facebook or your other favourite site, now just close the browser and then open the browser. Son of a gun - you are still logged into Facebook. So by all means unless you want someone posing as you and posting photos you don't want to admit to, log the heck out of there.

A further point to make on this is that many of your social networking sites, web mail, etc. have an automatic login. When you are using a public computer, please don't check that box, and if it is already checked when you are logging in just uncheck it.

And if you have to use the facilities in the midst of your online public computer experience; logout of everything, close all the windows, don't leave anything alive and running. Don't leave the computer to its lonesome self, it might find company from most unattractive places.

Rule Numero Tres: Let no one follow you - erase your tracks! Today's browsers have a private mode where you can surf the web and leave without a trace. Chrome calls it Incognito, Firefox calls it Private Browsing and Internet Explorer has InPrivate. Here's a cool article that explains how to use the private browsing feature in each of these browsers.
http://www.sunbeltsecuritynews.com/1HB475/110427-Private-Browsing

Another thing, you know that little feature in browser that asks you if you want to save the password after you login to a site. Unless you have a death wish - don't click okay.

As a final precaution erase your temporary Internet Files and your history. Let's face it, computers have long memories and funny places to store things. We don't want some robber guy, checking into the computer you just departed and searching out your history. Aside from any potential blackmail situations this could evolve, you just don't want to leave a trace. Go into the options part of your browser and usually in the security area it will tell you how to delete where you been. This is a very good practice to follow. However, if you have been using the private browser mode, you got yourself covered.

Rule Numero Quattro: Someone looking over your shoulder? You just might be surprised at just how many peaking Toms there are. When computing in public take a moment to look over your own shoulder to see who is watching you and copying down your passwords from afar. Especially, look out for those guys with binoculars, they are not studying birds in the airport proper, of that I can assure you.

Rule Numero Cinco: So after reading all this and you still want to do your banking in public (I advise not to do this) - it is really not a good idea because after all your precautions are just that precautions. You do not know who was playing at this computer before you sat in front of it. Some black-hat may have installed some rather nefarious software with the sole purpose of logging your passwords and other private info. Don't make it easy for these guys. Just don't do it!

(*From Sunbelt Software*)

As disasters spread, so do online scammers

By Jan Bultmann

\

The outpouring of generosity from people all over the world following the earthquake in Japan has been accompanied by a profusion of donation scams.

These scams no longer prey on the simply gullible but have moved to less obvious ruses such as malicious websites that use ***clickjacking*** and ***drive-by*** attacks.

Natural disasters bring out extremes of human behavior. Workers at the devastated Japanese nuclear power plants place themselves in harm's way trying to protect other people from explosions and radiation poisoning. Military and social services staffers work days without sleep under horrifying conditions.

And in response, strangers around the world ask how they can help, what they can do, what they can send. Unfortunately, predators also respond, seeking to exploit the suffering and generosity of others for personal gain.

Online donation scams are not new, but they became really evident in 2005 in the aftermath of Hurricane Katrina. Most of those scams were e-mail–based phishing, also known as 419 scams. The least sophisticated claimed to be from victims; they explained complicated and peculiar circumstances leading them to write e-mails asking individuals for money. More advanced phishing scams imitated the look and feel of reputable charities' Web presences.

Thanks to the increasing efficiency of spam filters, e-mails such as these reach fewer users today — and most Web users have learned to recognize and discard them quickly.

Since 2005, online scams have grown in sophistication. So it should be no surprise that, in the wake of Japan's crisis, donation scams are harder to spot. Clickjacking and drive-by threats don't depend on our charitable impulses — they target our interest in the unfolding events, using such common sources as news photographs, links to YouTube videos, and information updates.

Since March 11, 2011, scores of domain names have been registered — names containing terms such as Japan help, tsunami, or nuclear disaster, according to a Forbes report.

Often, these URLs are similar to the Web addresses of popular sites or are based on common misspellings. These malicious sites are also heavily seeded with now-familiar search terms (Japan, tsunami, nuclear disaster, radiation, Japan help, and so on) to draw the clicks of (or clickjack) people searching for information. This practice is known as **search engine optimization poisoning.**

A TrendMicro blog shows a search return list that reportedly includes fake sites.

Sometimes the scams are relatively innocuous; scammers register these bogus Web addresses as a way to earn money through advertising or delivering traffic to online survey sites. But others are far more dangerous. Clicking malicious drive-by sites, for example, can easily result in an infected PC.

Search-engine companies watch for these sites and eliminate the dangerous ones as quickly as possible. But so many have appeared in the aftermath of Japan's disaster that even Google is having difficulty keeping up with them, reports Bojan Zdrnja at Internet Storm Center.

PC users can also be directed to drive-by sites through links circulated on Twitter, Facebook, and other social-networking sites as well as in discussion forums. Wall posts, IMs, and messages represent themselves as containing links to newly uncovered disaster videos that might be tsunami simulations, doctored images, and worse.

As Graham Cluley, senior technology consultant at Sophos, wrote on the Sophos blog "Facebook users are being tricked into clicking on links which claim to be raw CNN footage of the Japanese tsunami by cold-hearted scammers — as part of a plot to earn money by driving Web traffic to take online surveys. The videos, which in the examples seen by Sophos exist on a website called spinavideo, purport to be footage of the horrifying tsunami which hit parts of Japan on Friday."

Clicking the link takes users to a spoof website that looks like YouTube. Users are tricked into agreeing to 'Like' the page on Facebook, which spreads the scam even further on Facebook.

But misdirection to online surveys and **likejacking,** as Cluley describes above, can be the least of a deceived user's problems. A user who activates a clickjacking link is taken to a drive-by website that might (or might not) look legitimate but that automatically downloads malware onto the user's machines. The most frequently

(Continued on page 12)

(Continued from page 11)

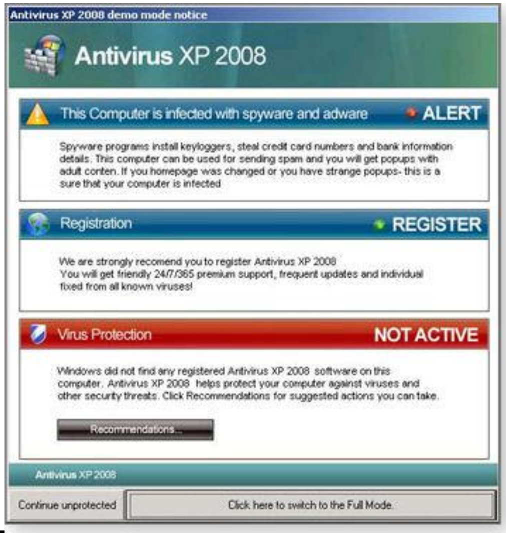
downloaded type of malware is rogue security software, often also called rogue antivirus software (or rogue AV).

Rogue security software masquerades as legitimate security software. Sometimes it even imitates legitimate security software interfaces, such as Microsoft Update. After it's installed on your machine, antivirus malware might simply pretend to detect viruses and then entice you into paying for a ***subscription*** to have your machine ***cleaned***.

Or it might install more malicious software — keyloggers, password recorders, or rootkits — that can go undetected while stealing your data. This software might lie dormant until it detects a specific event, such as when you enter a bank account number. Then it comes to life and starts collecting your keystrokes: recording your passwords, social security number, date of birth, and other personal data.

The scammers resell your credit card numbers or passwords to other criminals. Then they change their company name, change the credit agency they're using to bill you for your "malware subscription," and vanish before they can be identified. Rogue security software costs the banking industry billions of dollars a year, a cost borne by consumers.

Figure 1 shows an example of rogue security software that's disguised as a Microsoft alert.


Antivirus XP 2008 demo mode notice
Antivirus XP 2008
This Computer is infected with spyware and adware
ALERT

Spyware programs install keyloggers, steal credit card numbers and bank information details. This computer can be used for sending spam and you will get popups with adult conten. If you homepage was changed or you have strange popups- this is a sure that your computer is infected

We are strongly recomend you to register Antivirus XP 2008
You will get friendly 24/7/365 premium support, frequent updates and individual fixed from all known viruses!

Windows did not find any registered Antivirus XP 2008 software on this computer. Antivirus XP 2008 helps protect your computer against viruses and other security threats. Click Recommendations for suggested actions you can take.

- How can you avoid clickjacking scams and drive-by websites? It's simple, but in the heat of a disaster, it can be harder than it sounds. Sophos's Cluley wrote, "Remember to always get your news from legitimate news websites, and if you're hunting for a video, make sure that you go to the real YouTube website rather than a replica set up by scammers."

Meanwhile, old-fashioned donation fraud, featuring spoofed charity sites and phishing e-mails, has not gone away. ScamWarners has reported detecting a fake Salvation Army site. FBI spokeswoman Jenny Shearer told MarketWatch.com that a fraudulent e-mail, purportedly from the British Red Cross, is soliciting wired donations.

How to keep yourself safe in disastrous times

Here are tips to help you protect yourself from donation fraud:
Make informed choices about where to donate. Before turning over the personal information needed to process your donation, visit an online watchdog site such as charitywatch.org to evaluate the receiving organization's legitimacy.

- Don't click links in online forums, e-mails, or IMs that say they are from charity organizations — even well-known ones such as the Red Cross or Red Crescent, Mercy Corps, World Vision, or others. These e-mails could easily be spoofs that will direct you to a website that looks like the real thing but steals your data.
- Do not respond to unsolicited requests for donations, particularly from people who claim to be victims. "Symantec has observed a classic 419 message targeting the Japanese disaster," said researcher Samir Patil in a post to the company's security blog. "The message is a bogus 'next of kin' story that purports to settle millions of dollars owing to an earthquake and tsunami victim."
- To get to the website of a charitable organization you want to support, type its web address into your browser's address bar yourself — don't rely on links, however professionally designed they may look, to take you there.
- When you are on a charitable site, take a moment to check the spelling of the organization's website in the address bar. Scammers often use common typos or misspellings to create URLs that fool an unwary eye.
- Make sure the page where you enter your credit card or other personal information is encrypted. The beginning of the address should read **https://**

(Continued on page 13)

(Continued from page 12)

instead of **http://.**

a Make sure any site that you donate through has a written privacy policy.

a Get your news about events in Japan from reputable news sites.

If you believe you have been a victim of a charity-related scam, contact the National Center for Disaster Fraud by telephone at (866) 720-5721, by fax at (225) 334-4707, or by e-mail at disaster@leo.gov.1.

You can also keep an eye on samples of fraudulent e-mails and messages by watching the forums at ScamWarners, a reputable Internet Fraud Center that will also examine and evaluate material you submit and post samples to help other people avoid being scammed.

BREAKING NEWS!!

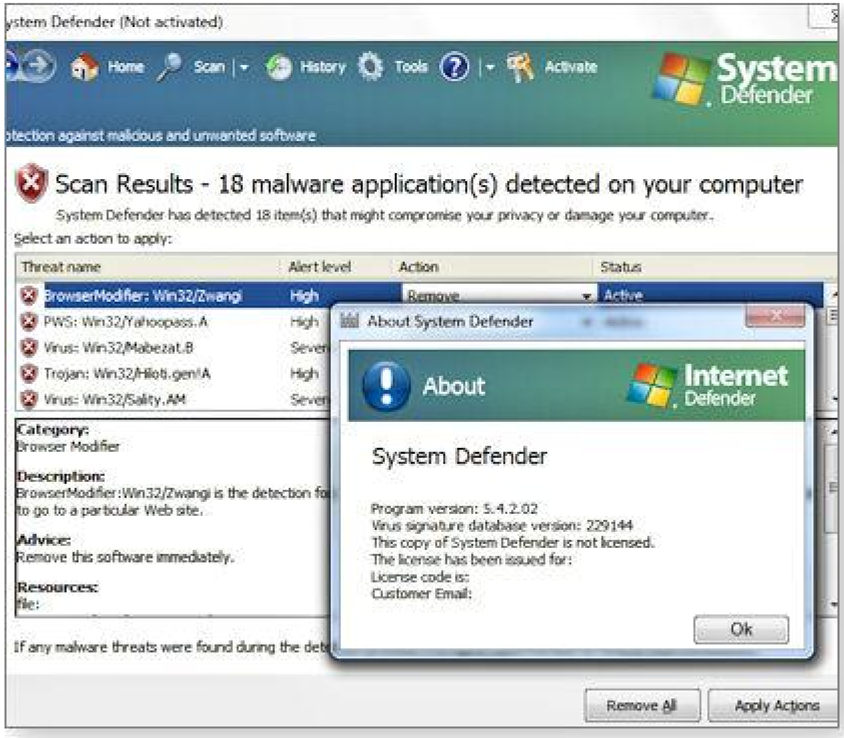
To save the economy, in May, 2011, the Gillard government will start deporting old people (instead of illegals) in order to lower Social Security and Medicare costs

RUN YOU OLD BUGGER, RUN!!

Well....what can I say? Someone sent it to me

And I'm *not* going alone!

(Continued from page 8)


ystem Defender (Not activated)

otection against malicious and unwanted software

Scan Results - 18 malware application(s) detected on your computer

System Defender has detected 18 item(s) that might compromise your privacy or damage your computer.

Select an action to apply:

Threat name	Alert level	Action	Status
BrowserModifier: Win32/Zwangi	High	Remove	Active
PWS: Win32/Yahoopass.A	High		
Virus: Win32/Mabezat.B	Sever		
Trojan: Win32/Hiloti.gen!A	High		
Virus: Win32/Salty.AM	Sever		

Category:
Browser Modifier

Description:
BrowserModifier:Win32/Zwangi is the detection fo
to go to a particular Web site.

Advice:
Remove this software immediately.

Resources:
file:

If any malware threats were found during the det

About System Defender

System Defender

Program version: 5.4.2.02
Virus signature database version: 229144
This copy of System Defender is not licensed.
The license has been issued for:
License code is:
Customer Email:

Figure 6. Superficially, this dialog looks quite legit. But it fails closer inspection — it can't even keep its name straight!

In previous dialog boxes, the malware identified itself as "Windows Security" and "Windows Defender." Now it's simultaneously "System Defender" and "Internet Defender." No valid software product goes by four separate names in the same instance.

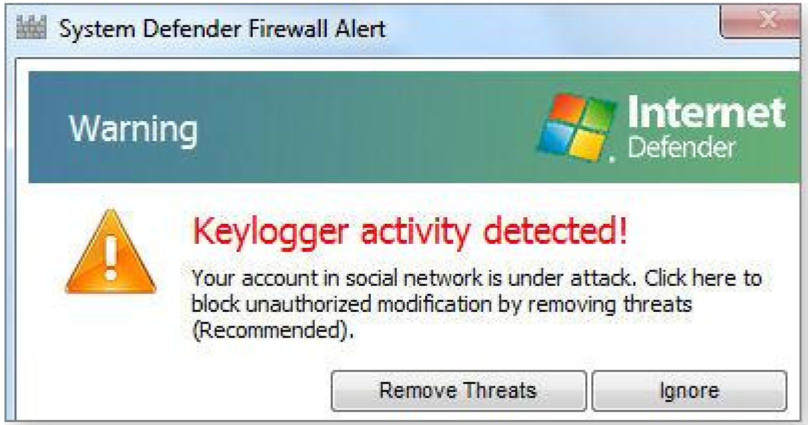
Of course, the point of all this smoke-and-mirrors chicanery is confusion — to extort you into ***paying*** to activate the software and "remove" the supposed infections. But the only real infection is LizaMoon itself.

I was certain that clicking the malware's Remove All button would bring me to a payment site. But because I didn't want to reconnect to the Net while the malware was still active on my machine, I left the above dialog alone and waited to see what would happen.

(Continued on page 14)

(Continued from page 13)

Every few minutes, the malware would pop up other warnings, such as the one in Figure 7. There were many others.



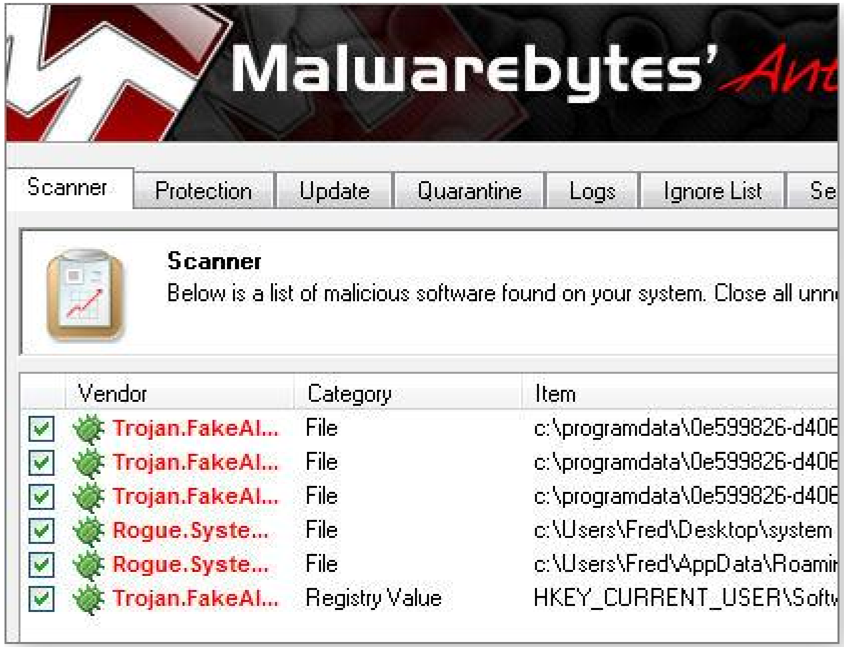
Keylogger activity detected!

Your account in social network is under attack. Click here to block unauthorized modification by removing threats (Recommended).

Figure 7. The fake virus warning got more urgent — and more illogical and ungrammatical. This nonsensical message states that a firewall has somehow detected keylogging in a social network.

Throughout this time, Microsoft Security Essentials was silent — a major disappointment. However, every few minutes the Windows Security Center would wave the flag (via a dialog box) and urge me to "Turn on Windows Security Center service (Important)."

LizaMoon blocked attempts to restart the Security Center service and hid itself from MSE. To clean up the mess, I needed to use another tool, Malwarebytes Anti-Malware (site/download), which disabled and removed most of the malware (Figure 8). When I rebooted the newly cleaned PC, I ran MSE again, which discovered more pieces (Figure 9).

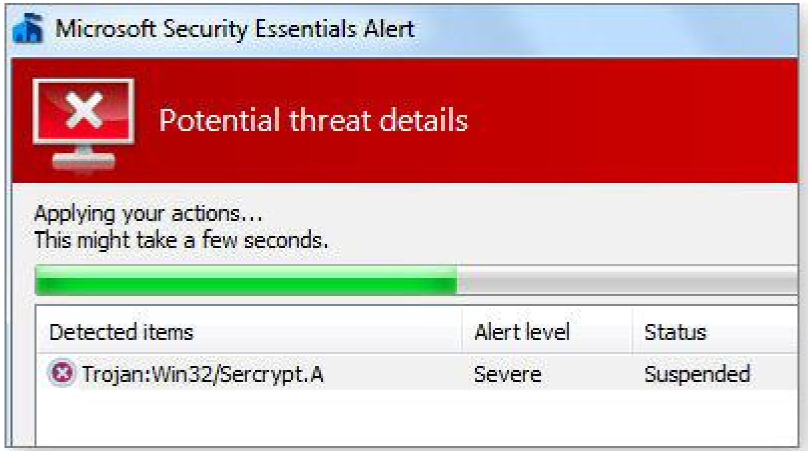


Scanner

Below is a list of malicious software found on your system. Close all unn

	Vendor	Category	Item
☑	Trojan.FakeAl...	File	c:\programdata\0e599826-d40E
☑	Trojan.FakeAl...	File	c:\programdata\0e599826-d40E
☑	Trojan.FakeAl...	File	c:\programdata\0e599826-d40E
☑	Rogue.Syste...	File	c:\Users\Fred\Desktop\system
☑	Rogue.Syste...	File	c:\Users\Fred\AppData\Roamir
☑	Trojan.FakeAl...	Registry Value	HKEY_CURRENT_USER\Softw

Figure 8. Malwarebytes' Anti-Malware disabled and removed most — but not all — of the malware.



Potential threat details

Applying your actions...
This might take a few seconds.

Detected items	Alert level	Status
Trojan:Win32/Sercrypt.A	Severe	Suspended

Figure 9. MSE was able to remove the threats that Malwarebytes missed.

I followed up with scans using ESET's online scanner, McAfee's Security Scan Plus, TrendMicro's HouseCall, and Microsoft Windows Live OneCare scanner. All agreed that my PC was now clean.

(Continued on page 15)

(Continued from page 14)

Just in case, I continued to run additional extra scans for the next few days. Nothing untoward turned up, and my system has behaved normally ever since.

Microsoft Security Essentials: first failure

I have to say I'm disappointed that Microsoft Security Essentials didn't detect or prevent this infection. It should have, and I hope Microsoft patches MSE pronto.

On the other hand, deliberate choices and actions by a user can defeat ***any*** software. LizaMoon required my active, voluntary involvement ***four different times*** before the infection took hold.

LizaMoon wasn't even subtle: I had plenty of warnings and opportunities to abort the process, the malware itself provided abundant clues to its own bogus nature (such as an inability to keep its aliases straight).

The lesson? Using security tools is no substitute for common sense. Malware like this is actually very easy to avoid, ***if*** you pay attention to what's going up on your screen.

Thoroughly read all dialogs — especially unexpected ones and ones pertaining to installing new software. Ask yourself if the warning really make sense. If you have any suspicions at all, dismiss such dialogs via the red-X close box or, if that fails, by using the aforementioned built-in Task Manager (more info).

Immediately run your favorite suite of security tools, such as the ones mentioned above.

Remember: You won't get infected with LizaMoon (and similar malware) unless you allow it!

Solving Memory Problems

By Fred Langa

Free tools from Microsoft, other software publishers, and RAM vendors all can work together to solve your PC's memory troubles.

In Windows 7 and Vista, an easy-to-use Memory Diagnostic Tool is built right into the operating system; XP users have other choices.

a **New RAM and new OS — and new trouble**

Reader Robert started having blue-screen reboots after he upgraded his XP PC:
"There are not many things that beat me these days, but I do have an annoying problem. After testing Win7 on a very old computer, I thought it would be a piece of cake to install it on a much newer Acer Aspire E650 that was running XP. "So I installed Win7 and brought it up to 2GB of RAM. "Now it will go for a day or two, and then it Blue-Screens and reboots. I clean the Registry and use a file cleaner, and away it goes again. All the drivers seem to be fine. What would you do here?"

a Your system apparently was running fine under XP, so let's assume the original hardware was OK. That leaves us with two changed items to look at: your new operating system and your new RAM.

Possibly you have a subtle compatibility issue with your new Windows 7 setup. Most XP systems can run Windows 7 fine, and you did in fact get it up and running. But it still would be worth your while to back-check for trouble with Microsoft's Win7 Upgrade Advisor (info/download).

If the Advisor finds trouble, your first task is to resolve that problem, whatever it is. But I suspect the Advisor will tell you that your system is fine — and that's good. Now you can focus on the RAM, with some assurance that you're on the right track.

Start with the physical RAM. Remove and reinstall your new RAM stick(s), making sure all the electrical contacts are clean, there's no dust or lint in the socket, and that the RAM seats and locks properly when you reinstall it. (If

(Continued on page 16)

(Continued from page 15)

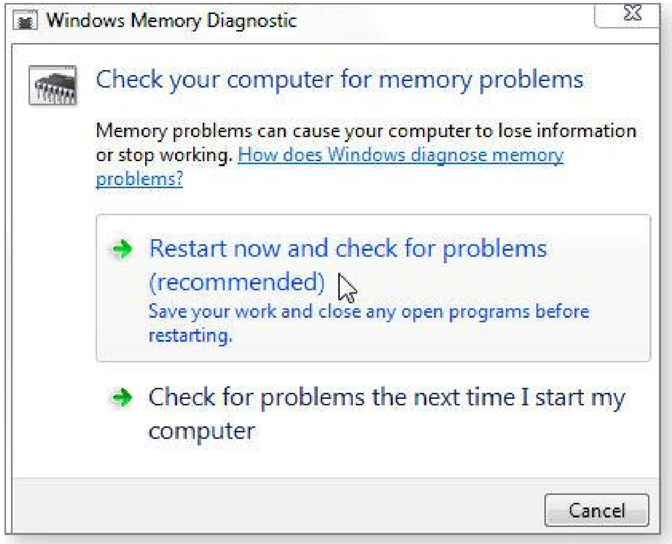
you need or want more detail on these purely physical steps, HelpWithPCs.com has a nicely illustrated how-to article on replacing laptop RAM.)

Often, the simple act of removing and reinstalling RAM cures many kinds of minor installation issues. For example, a system's unused RAM socket may be slightly oxidized, causing poor electrical contact. Removing and replacing the RAM scrapes through the oxide, restoring good contact to fresh metal.

While your RAM is out in the open, double-check its markings to make sure it's really the right type and speed. Your PC manufacturer's site should list the exact specs for your system.

If you can't find RAM specs from your system maker, try a RAM vendor. For example, Crucial.com offers two useful RAM-specification tools (site), either of which can usually tell you the RAM specs for most PCs. Naturally, Crucial wants you to buy their RAM, but specs are specs, and you're not obliged to make your purchase there.

If the RAM is the right type for your system and has no installation issues, it's time to run some tests.



Check your computer for memory problems

Memory problems can cause your computer to lose information or stop working. How does Windows diagnose memory problems?

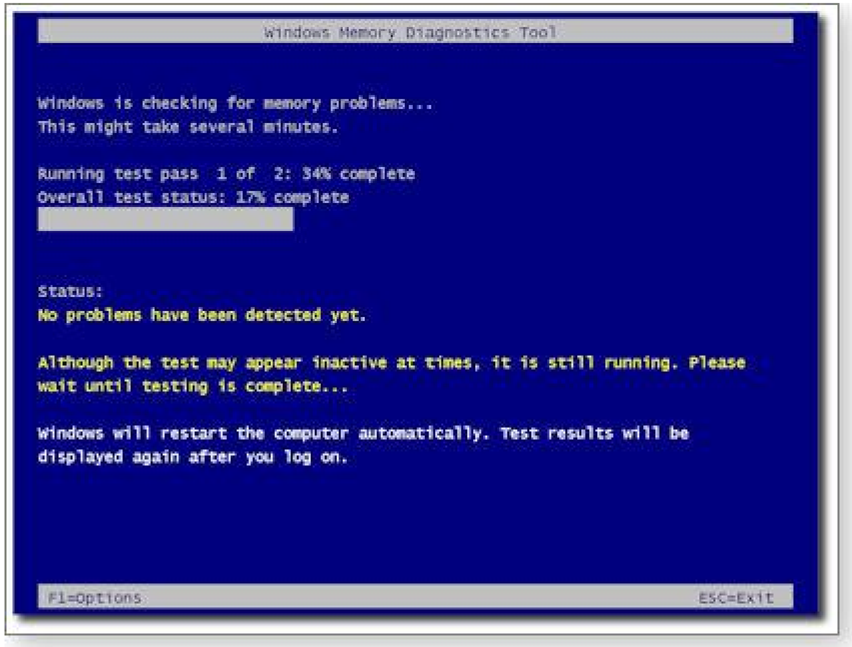
Restart now and check for problems (recommended)
Save your work and close any open programs before restarting.

Check for problems the next time I start my computer

Windows 7 and Vista have a built-in tool named Windows Memory Diagnostics. To use it, click the Start orb, and then type the word **memory** in the **Search programs and files** or **Start search** box. Press Enter, and the tool runs, simple as that. (See Figure 1.)

Figure 1. The Windows Memory Diagnostic tool built into Windows 7 and Vista makes it easy to track down RAM errors.

When you reboot, the diagnostic software takes over — exercising all your RAM in several ways, running through the test two full times, collecting the results, and looking for problems. (See Figure 2.)

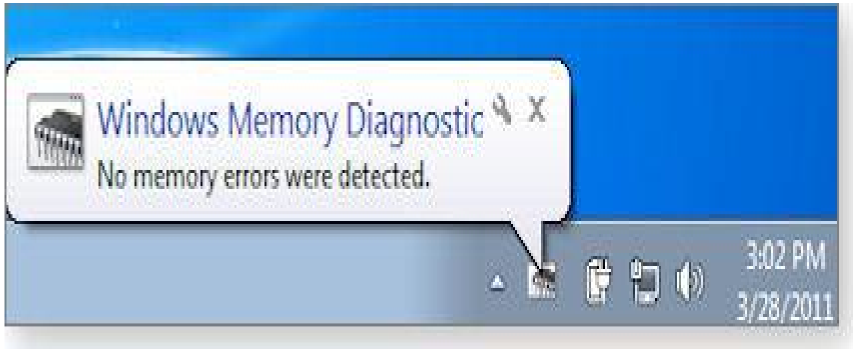


```
                 Windows Memory Diagnostics Tool

Windows is checking for memory problems...
This might take several minutes.

Running test pass  1 of  2: 34% complete
Overall test status: 17% complete


Status:
No problems have been detected yet.

Although the test may appear inactive at times, it is still running. Please
wait until testing is complete...

Windows will restart the computer automatically. Test results will be
displayed again after you log on.



F1=Options                                                          ESC=Exit
```

Figure 2. The actual memory testing takes place at reboot, before any other software loads.

(Continued on page 17)

When the testing is done, your system reboots itself normally. A minute or two after Windows is up and running, the Windows Memory Diagnostic tool opens a small tooltip balloon (see Figure 3) to tell you the results of the tests.



Windows Memory Diagnostic

No memory errors were detected.

Figure 3. After reboot, the Windows Memory Diagnostic tells you, via a tooltip, what it found. In this case, the tested RAM was fine.

If you want more control over the testing, you can adjust the Memory Diagnostic Tool's settings by pressing F1 when it starts. You'll be presented with options for various test types, number of test passes, and so on; the choices are described onscreen as you use the tool. For more information on these options, see this Microsoft Help & How-to page.

XP users note: A standalone version of the Windows Memory Diagnostic is available on a Microsoft webpage. It works very similarly to the version built into Windows 7 and Vista.

You can also find numerous third-party, standalone memory diagnostic tools. For example, see PCsupport.com's write-up of the "Top 5 free memory testing software tools" or ComputerHope.com's article, "How can I test my memory to determine if it is bad?"

With luck, simply removing and reinstalling your new RAM solves the problem. But if the diagnostic tests show ongoing trouble, or if your random reboots continue, your best bet is probably to return the new RAM and get a replacement.

Wanted! Your top SMB security tips

Windows Secrets is planning a special issue focused on online security, specifically in small and home businesses.

What do you do to keep yourself and your work-related systems/data/financial info/etc. safe from Web attack?

Please share your security tips via tips_mail@langaonline.com (note the underscore).

I hope to select and publish a collection of your best tips in the special issue.

Thanks for your help!

Windows 7 SP1 Remote Admin Tools failure

Dave encountered an incompatibility among Microsoft's own tools:
"RSAT (Remote Server Administration Tools) does not work with Win7 Service Pack 1 yet, and you can't roll back the Service Pack if you install from a slipstreamed package with SP1 integrated. Just ran into this problem at work."

a You're right, Dave: thanks for the heads-up.

Microsoft says it will have a corrected release of the Tools available sometime this month (April 2011). In the meantime, a TechNet Blog post suggests this workaround:

1. Install Windows 7

a **2.** Install the RSAT tools [info/download]

a **3.** Install Service Pack 1 via the standalone package

a The "Comments" section of the same blog page also offers some additional suggestions.

A separate but related "Community Content" section of TechNet's "Remote Server Administration Tools for Windows 7" page offers several free workaround scripts.

Siphoning data off an old laptop drive

Howard Potash has a new laptop but kept his old drive.
"I sold my older laptop (Windows 7 Ultimate 32-bit) but kept the hard drive. "My new laptop is the same brand but has Windows 7 Home Premium 64-bit

software and two hard drives in it. "There is some info that I would like that is on the old drive, but it is 32-bit. Can I and should I get files off the old drive? Can I install the drive in the other bay?"

a Laptops with open drive bays are rare, but if yours has one and the old drive fits, sure — give it a try. Turn off the laptop, open the bay, plug in the drive, close the bay, and restart. The system should still boot from the new drive, but "see" (and give you access to) the old one.

If that doesn't work — or, more likely, isn't possible — you can connect your old drive to the new PC via an inexpensive **USB laptop drive adapter** (that's the phrase to search and shop for). The adapters typically cost $10 to $20 or so.

Once your new PC can see and access the old drive, you should be able to move (or copy and paste) your data files and personal information off the old drive without trouble.

Can't revert to Firefox 3 if 4 fails?

John Hill needed a source for older versions of his browser after he ran into trouble with Firefox 4.

"Just downloaded Firefox 4.0, and it deleted my Norton Internet Security toolbar. It's incompatible with Firefox 4. Norton says they'll 'release an update for NIS/NAV 18.5 and Norton 360 v5 in early May that will address the problems found in both Internet Explorer 9 and Firefox 4.' "But I want it to function now, so I tried System Restore and soon found out that that's not going to work. System Restore wiped out Firefox 4.0, but it did not give me a way to replace it with the version I was using, 3.6.15. "Went looking on the Net to see if I could find a 3.6.15. No luck. Everything directs you back to Mozilla's 4.0 download. "So the reason for this message, besides 'heads up on Firefox 4,' is do you have a way for me to access a copy of 3.6.15?"

Older versions of Firefox are still available online, and they are still current. Mozilla even says, "Firefox 3.6.x will be maintained with security and stability updates for a short amount of time." The most recently updated version of the 3.x series — currently Firefox 3.6.16 — is available on this Mozilla page.

Some independent sites, such as Oldversion.com and OldApps.com, also maintain complete back-libraries of browsers and of many other apps.

But don't go too far back: Very old versions of browsers (and all the other software offered on those old-software archives) are mainly of academic interest: Ancient software is unsupported and may not be safe or current for today's conditions and standards.

If you need installation help once you've found what you want, check out Mozilla's instructions for "Installing a previous version of Firefox."

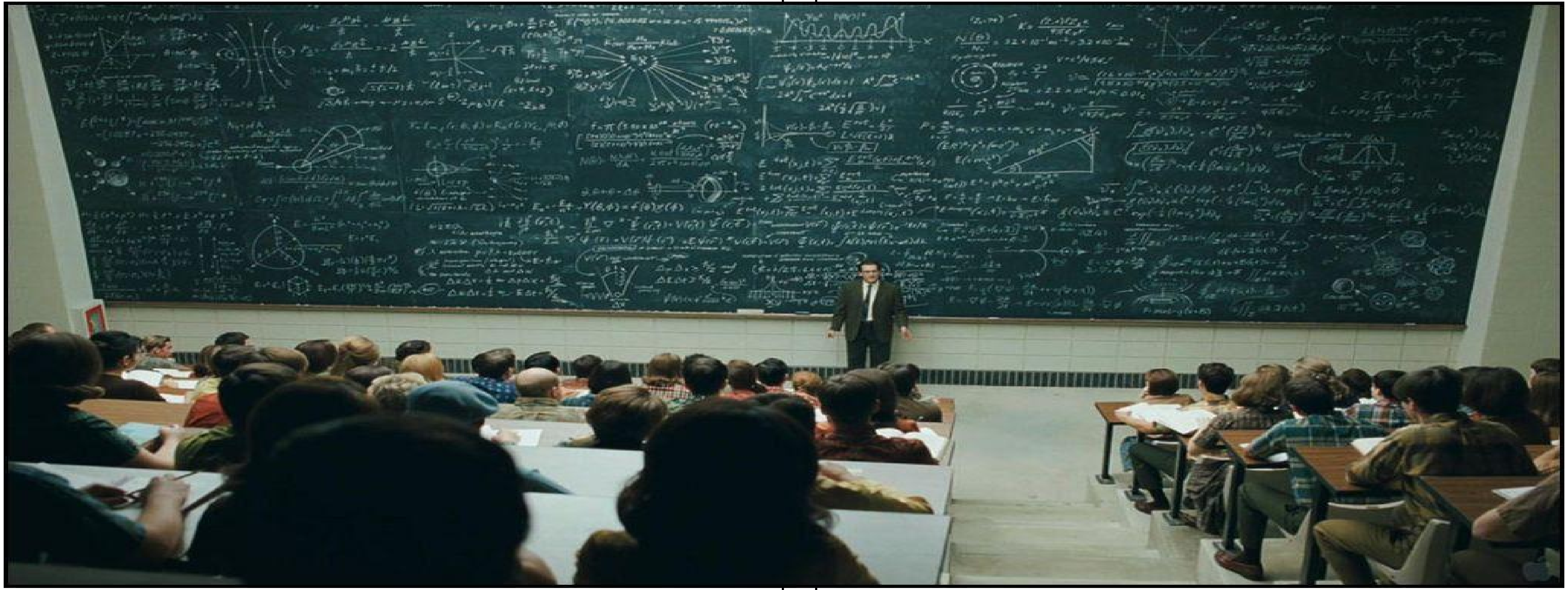
You'll then be all set until your toolbar maker finally catches up with browser tech!

WHY MEN ARE NEVER DEPRESSED:
Men Are Just Happier People.
Your last name stays put.
The garage is all yours..
Wedding plans take care of themselves.
Chocolate is just another snack.
You can never be pregnant.
Car mechanics tell you the truth.
The world is your urinal.
You never have to drive to another gas station restroom because this one is just too icky.
You don't have to stop and think of which way to turn a nut on a bolt.
Same work, more pay.
Wrinkles add character.
People never stare at your chest when you're talking to them.
New shoes don't cut, blister, or mangle your feet.
One mood all the time.
Phone conversations are over in 30 seconds flat.

(Continued from page 18)

You know stuff about tanks and engines.
A ten-day vacation requires only one suitcase.
You can open all your own jars.
You get extra credit for the slightest act of thoughtfulness.
Your underwear is $8.95 for a three-pack. Three pairs of shoes are more than enough. You never have strap problems in public.

You are unable to see wrinkles in your clothes.
Everything on your face stays its original colour.
The same hairstyle lasts for years, maybe decades.
You only have to shave your face and neck.
You can play with toys all your life.
One wallet and one pair of shoes -- one colour for all seasons.
You can wear shorts no matter how your legs look.
You can 'do' your nails with a pocket knife.



And thus, dear students, we have arrived at the basic formula for understanding women