OTTAWA
# PC NEWS

Vol. 16 number 11 | The newsletter of the Ottawa PC Users' Group | December 1999

Software review

# BlackICE Defender *by Chris Taylor*

## The threat

At work, our firewall logs thousands of attacks from the Internet every week. That made me start thinking about protection for PUB II. Since it is connected to the Internet 24x7, I thought it would be a likely target for the random attacks from the script kiddies: those individuals who attack computers on the Internet using pre-compiled scripts targeting well-known vulnerabilities. I concluded we were not the target of professionals for a couple of reasons. First, we don't really have anything to attract them and second, well...PUB II is still operational. I don't think it would have stood up well against the crackers who really know what they are doing.


The NT security log showed some periodic failed attempts to log on as Administrator, Guest, PUB2, Root, Admin, etc. I was unaware that this is a tell-tale trace of attacks. I could see no other evidence of tampering. I knew we could not afford something like the firewall we use at work, which costs thousands of dollars and is a bear to configure. But recently, there have been a number of personal firewall products released on the market at under $100. One getting rave reviews from people such as Ziff-Davis' Bill Machrone and Steve Gibson of SpinRite fame is BlackICE Defender from NetworkICE.

## Background

To understand how firewalls work, it is necessary to have a basic understanding about how computers communicate over a TCP/IP network, such as the Internet. You get services on other machines through virtual connections known as ports. There are TCP and UDP ports. UDP connections are similar to TCP but UDP does not include error correction.

When your web browser tries to load a web page, it tries to connect to port 80 on the remote machine. If a web server is listening at port 80, it sends the default web page to your browser. To send e-mail to a remote server, you try to connect to port 25 on the other machine. If an SMTP daemon is listening on port 25, it answers with a standard greeting. Services can listen on

*Continued on page 3*

## INSIDE



Next meeting: **WEDNESDAY, December 1st, 1999**

# Digital Cameras

For the feature presentation at the December meeting, OPCUG welcomes John Stephens, the General Manager of The Focus Centre, as our guest speaker.

Initially an expensive curiosity, digital cameras now command a significant presence in the retail market. Technical features abound, high-quality optics (often zoom lenses) and image resolution have increased from sub-VGA to the current megapixel-capable devices. More dramatically, despite the increased technical sophistication, prices have plummeted. To accommodate the increased memory demands of these high-quality images manufacturers are offering a variety of on-line and near-line storage devices that range from memory chips to disk drives (Iomega's Clik).

If there is a digital camera in your future, bring your curiosity—and your questions—to this meeting.

✧✧✧

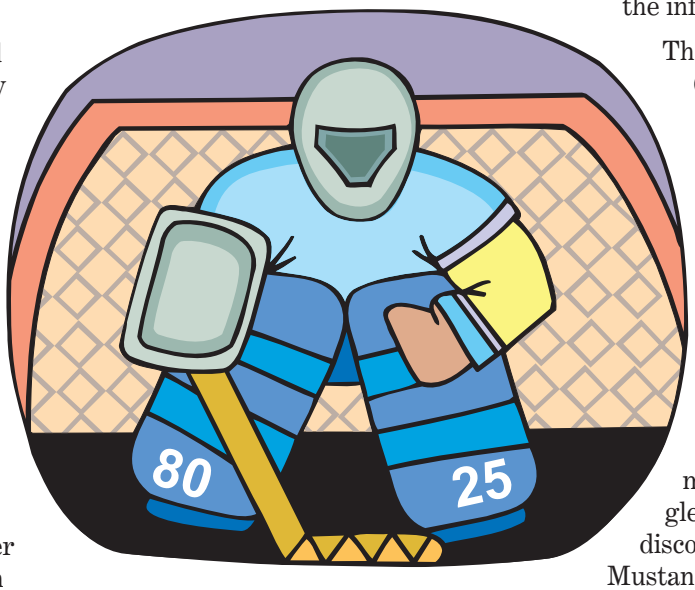
## Calendar

| Meetings | Date | Time and venue |
|---|---|---|
| OPCUG General Meeting | December 1st: **Digital Cameras** | 7:30 p.m. - National Museum of Science and Technology, 1867 St. Laurent Blvd. |
| Ottawa Paradox Users Group | Third Thursday of each month | 6:15 pm - Inly Systems, 1221a Cyrville Rd. |
| FOX Pro/Developers SIG | To be announced | 7:15 pm - Sir Jean Talon Building Conference room, Tunney's Pasture, Holland Ave. (north of Scott St.) |
| PIG SIG<br>(or is it WING SIG?) | December 1st, after all the other SIG's - All questions, be they serious or not | "Good Times" cafe at Shoppers City West, Baseline and Woodroffe |

non-standard port numbers, but in most cases this defeats the purpose, since the machine connecting to them must know to attempt the connection on the different port number. PUB II uses this capability to support an extra FTP server used to maintain web pages.

There are a total of 64K ports available. These are categorized as system ports (those under 1024) and application ports (those over 1024). System ports are generally more powerful. This comes from the fact that, under Unix, only processes running under the root context (the most powerful account on the system) may open ports under 1024.

Enter BlackICE Defender. It has four basic configurations. The most open is Trusting, where no ports are blocked and a connection may be made to any listening port. Other settings are Cautious, Nervous, and Paranoid. Each setting blocks more inbound TCP and UDP ports. Paranoid blocks all inbound ports. If someone can't connect to a port on your computer, they can't exploit a weakness there. The more ports you block, the more secure the machine will be.




The manual says outbound connections are never blocked, meaning you can connect from a BlackICE-protected machine to other computers without interference from BlackICE. Tech support tells me that due to UDP's connectionless nature, all outbound UDP ports are blocked when set to Paranoid, meaning some applications like ICQ will not work at Paranoid.

If BlackICE does not block a port, it must try to determine if the packets of data are normal traffic or an attack. This is not a simple task and this ability, more than anything else, separates a good firewall from a bad one. Even set to Trusting BlackICE has a lot of work to do. It must allow all connections to happen normally. It then has to decide if the traffic is legitimate or an attack which it must block. BlackICE can detect and block over 250 different types of attacks.

The default configuration is Cautious which blocks TCP and UDP ports under number 1024. PUB II hosts a web server, two FTP servers, a POP3 mail server, Telnet services and an SMTP daemon, all of which listen on port numbers under 1024. One alternative was to use Trusting, where no ports are blocked, and rely on BlackICE's ability to detect and block attacks. A better alternative was to use a customized firewall.ini file that allows the use of the Cautious configuration while opening the specific ports we need for proper PUB II operation.

## Installation and configuration

The installation of BlackICE was about as simple as any install could be. After installation, I replaced the customized firewall.ini file. To test if BlackICE is working, the NetworkICE web site can send a simulated Back Orifice probe, one of the attacks that BlackICE can detect and block. When I tried this, the tray icon for BlackICE immediately began to flash. A single click on it opened the console where I could see the information about the attack.

The Gibson Research site (www.grc.com) has a page called Shields Up. It will do a port scan on your machine looking for common listening ports. On PUB II, it found the ports purposely left open, but nothing else. BlackICE was effective at concealing more details.

I disabled BlackICE Defender to see how much more information could be gleaned. Shields Up discovered the NetBIOS names Mustang, PUB2, and UserGroup (user name, machine name and workgroup.) It enumerated the shares and discovered they were password protected. It also determined the MAC address of the network card. Keep in mind that the more information you provide a cracker, the better their chances of breaking in.

When BlackICE detects an attack it does a back trace to gain as much information as possible about the intruder. In addition to the IP address, depending on the attacker, it may be able to determine the NetBIOS name, the Workgroup or Domain name, the DNS name, and the MAC address of the network card. Attacks are categorized as Informational, Non-threatening (but worthy of note), Suspicious (non-threatening but maybe an indication of someone probing for vulnerabilities), Serious (attempts to access information but not damaging), or Critical (a deliberate attack designed to damage or crash your machine). A button on the Attacks

*Continued on page 4*

page takes you to the NetworkICE web site and provides more information on the attempted intrusion.

BlackICE has a history tab where you can see graphs of frequency of attacks and network traffic. As well, there is a summary of the total number of Critical (actually, both Critical and Serious) and Suspicious events. Informational events are not plotted.

The configuration menu allows you to configure packet logs, which log all TCP/IP traffic, as well as evidence logs, which log just the traffic during an attack. These files are not human-readable but may be useful to an ISP or law enforcement. You can configure addresses you want to trust. BlackICE will completely ignore traffic from these hosts. This may be appropriate for machines on a LAN.

A menu option connects you with NetworkICE to check for updates. If an update is available it downloads automatically. Otherwise it sends you to a page that tells you your version number. A bug in the current version prevents the system from understanding you already have the latest release. It will be fixed in the next release, but it might be a bit of a challenge getting word out about a new release after customers repeatedly download an update file only to discover it's always the same version they already are running.

## The acid test

I expected the first real attack to come within minutes of installing BlackICE Defender. Well, it was not quite that fast, but a computer in Australia did a port scan within an hour. Over the last week we have had a couple of dozen attacks. So far, attacks not initiated by me have included port scans, NetBIOS Port scans, Back Orifice pings, PC Anywhere pings, TCP Trojan horse probes, NetBus probes, RPC port probes and SOCKS Port scans. We have had attacks from Israel, Germany, France, Russia, the Netherlands and Canada, as well as computers in the .NET and .COM domains.

Overall, I am very impressed with BlackICE Defender. We now have a good level of protection against crackers trying to crash PUB II or use it as a launching pad to attack other systems. I've noticed no performance problems. It only takes a couple of megs of RAM and even in the middle of an attack, BlackICE never took more than 1% of CPU cycles. Right now, PUB II has been up for over 100 hours and BlackICE has used 81 seconds of CPU time. Considering PUB II is running on a Pentium 200, that's impressive. The tweaker in me would like to see more documentation about tuning BlackICE: according to NetworkICE, that may be coming.

## do you need one?

Do you need a firewall? I would have to say a definite maybe. If you have an always-on connection to the Internet, consider the fact that you are almost certainly scanned every day for vulnerabilities. Even dial-up connections are at risk, since people "out there" are scanning millions of addresses. If you are connected to a LAN as well, you almost certainly have shares on your computer than may be discovered and accessed: especially if your shares have no passwords. It may only take seconds or a few minutes to grab password information and credit card numbers or destroy data and more.

The least you should do is determine how vulnerable you are. Go to www.grc.com, www.dslreports.com, www.it-sec.de/vulchke.html, and www.hackerwhacker.com. All of these sites will do a scan on your machine looking for vulnerabilities. Most of them will also tell you how to make your machine more secure.

## Purchase details

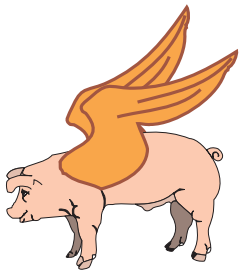
BlackICE Defender may be purchased for US$40 at www.networkice.com. This includes updates for a year. Updates are very important when it comes to security products since new vulnerabilities are discovered all the time and defenses must be devised to protect against new attacks. Subsequent yearly subscriptions for updates cost US$20. The 111-page manual (over 60 pages are short descriptions of the attacks BlackICE can block) comes in Adobe Acrobat format and must be downloaded from the web site. BlackICE Defender requires a Pentium and Windows 9x or NT.

NetworkICE is interested in providing a discount to members of the OPCUG, but it might be a couple of months before their program is set up. They have been overwhelmed with the response to BlackICE Defender and are struggling to keep up with the demand right now. I will let members know as soon as I know more.

✧✧✧

## Club Life

# Fly West



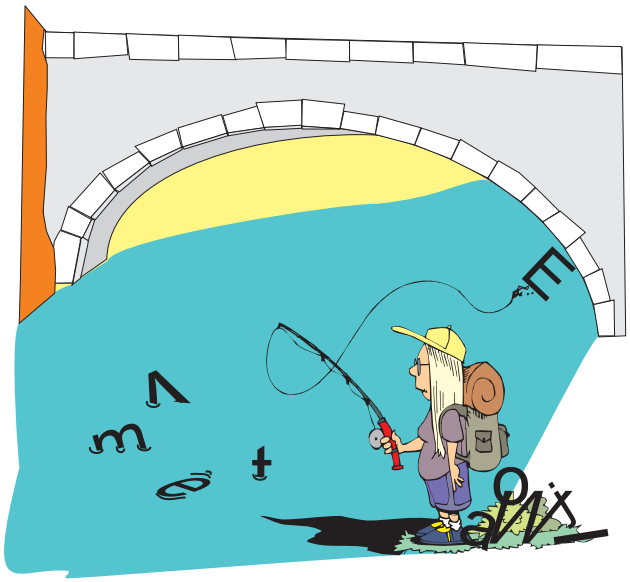
The "Good Times" cafe at Shoppers City West, Baseline and Woodroffe, for chicken wings and a drink after the General meeting: may be the best and most informative SIG meeting of the evening. See you there!

✧✧✧

# TextBridge Pro 9.0 *by Gary Schweinshaupt*

[Editor's note: this review complements the Caere Omnipage Pro review in the October 99 newsletter.]

ScanSoft's TextBridge Pro 9.0 is a complete OCR package. It preserves all document formatting and even automatically converts tables into Microsoft Word or Corel WordPerfect cell formats. It also saves color graphics, including their sizes and page positions. To help improve recognition accuracy, TextBridge both sharpens characters and removes the background tinting, which often confuses OCR routines. In addition, the program can recognize text in 56 languages. Lastly, Webmasters will appreciate TextBridge 9.0's automatic conversion of documents into Hypertext Markup Language (HTML). This product continues to improve in several ways, now claiming a 99% accuracy (the Pro 98 product claimed 82%).



## Features

Like previous versions, TextBridge Pro 9.0 integrates well with other applications, and it can be called up from within Microsoft Word, WordPerfect, Microsoft FrontPage and similar programs. TextBridge also saves converted text files to all major word processor formats and exports to Adobe Acrobat PDF files and HTML files. To add an application to the Instant Access OCR list, you just open that application and select the TextBridge Instant Access Control Panel. If the program is compatible, it appears on the list — all you have to do is check the box and TextBridge will now appear in the File menu of that application and also on the Tool Bar of many applications.

PC Magazine says: "TextBridge 9.0's most pronounced improvement is its interface. Previously, the program's spartan interface had few toolbar buttons and confusing menus that made it difficult to figure out how to perform some tasks." I concur, the interface is much improved. Now a finished scan/recognition Insert Button is available on the toolbar, before you had to pull down the function from the Menu Bar/File—much better. TextBridge has obviously been listening to their users.

Installation was simple and uneventful. The last time I installed TextBridge, the default driver for the scanner was the ISIS driver, this time TextBridge defaulted to the more prevalent Twain. With the Adobe Acrobat user's manual, it takes up 32MB on my hard disk.

The default scanned image is now grayscale and it seems to work well. Before it was a setup option. There is an advantage with grayscale, as more of the character is captured during the scan. If the image is captured in black and white there is usually a 50% dropout point. Content less than 50% of full black would be lost; poor copy can lose enough detail that it can make characters unintelligible to the OCR software.

## Improvements

A function I consider a necessity, the built-in proofreader, looks similar to a spell-checker but now it has a built-in dictionary lookup. TextBridge still has a training mode and you can save the results to use with similar documents. In the previous version, I had some problems with the way the Proofreader works with the Original Image window. I think the Original Image window is one of the most helpful features. It lets you compare the scanned image with the recognized text. It's much easier to correct unrecognized text when you can compare it to what's on the original document right on the screen. Now the page image window comes up automatically; it is also a much larger window that covers the full width of the TextBridge Window. Also, the image of the target word appears directly under the 'actual scanned image' of that same word. Another new feature is Word Popups; when you scan across a 'recognized text page' whatever word your cursor stops at causes a popup window to appear with the scanned image of the word—much more positive than the previous method. These are significant improvements over the previous version.

Other significant new or improved features include:

- improved color and grayscale abilities (it can recognize text on a colored background for more accurate results),

*Continued on page 6*

## TextBridge Pro 9.0 (Continued from page 3)

● new AccuMorph Technology (improves the recognition of faxes and second-generation copies),

● TextBridge Scheduler (allows you to schedule large OCR jobs to occur while you are away from your computer), and

● output OCR results to over 25 file types.

Now you can convert paper to formatted Web pages without losing page layout—almost. My experiments showed simple pages converted well, but more complex documents with multi-columned text and randomly placed images formatted poorly in the final HTML page. However, most of the elements were there. It maintains the format by using cascading style sheet technology. It will dynamically analyze each page of the scanned document and create a table of contents and buttons that provide easy hypertext navigation of the documents when they are viewed with a browser.

### Recommendations

I am very satisfied so far with TextBridge Pro 9.0 and would recommend it to any novice or serious user. Everyone should have a scanner and a good OCR program; the prices are low now, there is really no excuse. The street price is $99 (US—about $150 Cdn).

If you have an interest in TextBridge Pro 9.0, you will be interested in visiting the Web page, it really covers everything you need to know at http://www.scansoft.com/products/tb90/index.html.

Requirements: Windows 95, 98, 2000 or NT 4.0, Intel (or compatible) 486 or Pentium PC with VGA, SVGA, or multi-sync color monitor, 24MB of RAM (32 recommended), 20MB hard drive (took 32MB on my system), scanner, input device drivers: TWAIN.



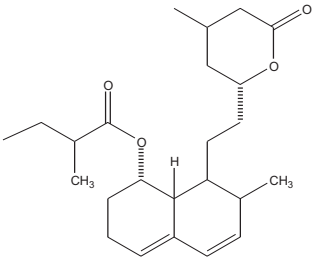
## Sofware review

# Cambridge Chemistry

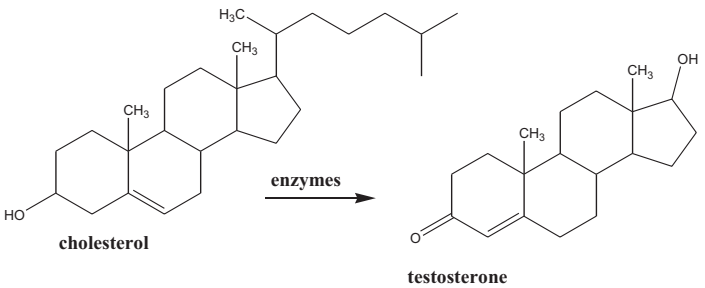
*by Jean Vaumoron*

Drawing programs such as Corel Draw are becoming more and more efficient and can be used for many tasks. At least if you have the patience… and are only considering producing a single drawing for an article or illustrating a newsletter.

Professionals who edit articles for scientific magazines generally do not use fancy programs for the text itself. They rely almost exclusively on safe workhorses such as WordPerfect or Word, which are readily available to most authors. When it comes to drawings though, the softwares get a lot more involved. In the Chemical field, for example, editors must be able to insert into the text neatly drawn figures, formulae and reactions. The drawing skills necessary to produce these works of art are out of reach of most computer users and they have to be replaced by specialized tools which do all the calculations for you. A good example is ChemDraw, the *de facto* standard chemical structure drawing program manufactured by CambridgeSoft (more information at www.camsoft.com). Usable in both Mac and PC platforms, it can save you a lot of time and produce absolutely perfect drawings with minimum work. ChemDraw has a proprietary file format but also exports through .wmf files into any text environment.



Compactin



cholesterol

testosterone

The basics can be learned in a few hours, and its intuitive approach is quite impressive. You can almost draw freehand and yet everything just falls into place. All the basic shapes such as benzene rings, and all kinds of chemical links and chemical symbols are available from the tool bar. All drawings can be modified and integrated into chemical equations. Although these first steps are already impressive, the program can take you much further with the use of molecular modeling, search engines for instant access to huge databases of ready-drawn chemicals, each with a list of their physical properties and lots more, … but you need to have the finances of a chemical firm if you hope to tap all their resources!

✧✧✧

Internet site recommendation

# Web-based image editing

A number of image-oriented companies (including Extensis, the subject of this article) have cooperated to set up a wide-ranging site that will interest members who use image editors. Visit www.creativepro.com and join (free). Once you are a member you can go to www.creativepro.com/intellihance/welcome/1,2190,,FF.html for a unique opportunity (yes, the commas are part of the URL and not a misprint).

Extensis (I wrote about their almost-free Mask Pro filter in the October issue) has made available, on-line at this URL, their Intellihance filter. This is not a download of the filter per se although a Java applet will be downloaded to your computer to facilitate the process. According to the website's instructions, you:

- specify which image you want to Intellihance (must be a JPEG, TIFF or BMP file),
- adjust the settings for your image (or use the enhancement settings that Intellihance suggests), and
- save your "Intellihanced" file as a JPEG, TIFF, or BMP file.

Aside from the cost savings, this is an easy way to learn by doing. While automatic settings might be tweaked further (in experienced hands) to yield better results the default results are impressive. New scanner owners and digital camera users might want to try it out. To my knowledge, there is no limit imposed on the number of images that you can process.

You could also download a time-limited demo from www.extensis.com to use on your own system.

✧✧✧

Virus alert

# More woes in the "Office"

Again, my Internet explorations have found trouble.

Microsoft may have garnered the lion's share of business application software with its Office suite; however, users must remain vigilant. Office applications are prone to malicious macro viruses. Recently, another unwelcome guest looms. To the best of my knowledge, at this time the threat is theoretical; however, once the genie is out… Consider the following scenario.

It is possible to embed an executable file within Microsoft Word. Double clicking it, or copying and pasting it to the Windows Desktop, would allow it to run: nothing new here.

This strategy has a weak link. Microsoft has a file type "Scrap" that uses the SHS extension. This is a product of cut and paste operations from within a file to the Desktop. This file type is obscure; Windows makes little mention of it.

To make matters potentially worse, in a default Windows installation Windows recognized file extensions are suppressed. To show all file extensions you must, in an Explorer window, go to View | Folder Options | select the View tab and uncheck the box titled "hide file extension for known file types."

"What if" that SHS file is really an executable in disguise? Now we have an innocuous (apparently) file that is waiting to spring the trap. To camouflage the deceit further suppose that the file is renamed: for example, a Microsoft Scrap file (the extension is SHS) is renamed to become a BMP (an image) or a text (TXT) file: some of these icons are similar and the unwary may not suspect. Double-clicking the icon (regardless of the file type that it "claims" to be) to "open" the file for viewing the image or text instead has an unexpected but predictable result: the file will execute.

While it could be attached to e-mail, the extension is normally displayed in the filename. Hence, the possibility is diminished although not eliminated.

To counteract this, you should review your anti-virus software settings and make certain that it will scan all SHS files by default. You should also consider the added security that is provided by a firewall (see Chris Taylor's excellent review in this issue). Regrettably, I know that this is just "waiting to happen" to the unwary when he/she least expects it.

✧✧✧

## OTTAWA PC NEWS

*Ottawa PC News* is the newsletter of the Ottawa PC Users' Group (OPCUG), and is published monthly except in July and August. The opinions expressed in this newsletter may not necessarily represent the views of the club or its members. Deadline for submissions is four Saturdays before the general meeting.

**Group Meetings**
OPCUG normally meets on the first Wednesday in the month, except in July and August, at the National Museum of Science and Technology, 1867 St. Laurent Blvd, Ottawa. Meeting times are 7:30 p.m. to 10 p.m.

**Fees**
Membership: $25 per year.

**Mailing Address**
3 Thatcher St., Nepean, Ontario, K2G 1S6
Telephone answering machine . . . . . 723-1329

**Web address**
`Http://opcug.ottawa.com/`

**Bulletin board—the PUB (BBS)**
Up to 33.6 kbps V.34 . . . . . 228-0665

**Chairman**
Bert Schopf **bert@blackbirdpcd.com** . . . . . 232-8427

**Treasurer**
James Fridrich `jimbo@magma.ca`

**Secretary**
David Reeves `dlreeves@iname.com` . . . . . 723-9658

**Membership Chairman**
Mark Cayer `cayemar@statcan.ca`. . . . . 823-0354

**BBS Sysop**
Chris Taylor `ctaylor@nrcan.gc.ca`. . . . . 723-1329

**Newsletter**
Duncan Petrie (editor)
`gdpetrie@accglobal.net`. . . . . 841-6119
(Mr. ) Jean Vaumoron (layout)
`vaumojav@magi.com` . . . . . 731-7847
(Mr.) Jocelyn Doire (distributor, electronic version):
`Jocelyn.Doire@opcug.ottawa.com`

**Publicity**
Chris Seal `cseal@istar.ca`. . . . . 831-0280

**Facilities**
Bob Walker `skywalk@iname.com` . . . . . 489-2084

**Beginners' and Windows SIG coordinator**
Duncan Petrie `gdpetrie@accglobal.net` . . 841-6119

**Fox SIG coordinator**
Andrew MacNeill `andrew@aksel.com` . . . . . 851-4496
Fox SIG web page: `www.aksel.com/foxsig`

**Internet SIG coordinator**
Bob Gowan `gowanb@inac.gc.ca`

**OS/2 SIG coordinator**
(Mr.) Jocelyn Doire; please contact via PUB:
`Jocelyn.Doire@opcug.ottawa.com`
OS/2 web address: `http://os2.ottawa.com`

**Paradox SIG coordinator**
John Ladds `laddsj@statcan.ca`. . . . . 951-4581

**Graphics SIG coordinator**
(Mr. ) Jean Vaumoron
`vaumojav@magi.com` . . . . . 731-7847

**Director without portfolio**
Terance Mahoney `terancep@cyberus.ca` . . . 225-2630
(Mr.) Jocelyn Doire `Jocelyn.Doire@opcug.ottawa.com`

**Club news**

# Great Computer Swap Meet

With the imminent arrival of "2000" our host, the National Museum of Science and Technology is actively planning the fifth Great Computer Swap. This event has consistently drawn crowds of more than 1,600 persons who are eager to enjoy information sessions, technology displays and the opportunity to buy and sell computer products.

For OPCUG, this event offers excellent exposure, a chance to fulfill our pledge "Users helping Users" and an opportunity to thank the Museum for its hospitality.

- Date: January 15, 2000
- Time: 10:00 to 4:00

Once again, OPCUG will set up a display. If you are willing to provide assistance, please see Dunc Petrie or Bert Schopf at the December meeting.

✧✧✧

**Club life**

# Reuse, recycle

Bring your old computer magazines, books, or any other computer paraphernalia you want to GIVE AWAY to the general meetings, and leave them in the area specified. If you don't bring something, you may want to TAKE AWAY something of interest, so look in on this area. Any item left over at the end of the meeting will be sent to the… recycle bin.

✧✧✧

**Club News all about Club Life!**

To receive the newsletter by e-mail, send the message "subscribe Newslettertxt" or "subscribe NewsletterPDF" (without quotes) to `listserve@opcug.ottawa.com`.

Did you know that the PDF issue was in color ?