



OTTAWA PC NEWS

Vol. 17 number 8

The newsletter of the Ottawa PC Users' Group

October 2000

WHAT'S NEW ON PUB II

Guard your ports! *by Chris Taylor*

Recent issues of the Ottawa PC News have included reviews of software designed to protect your computer from the bad guys on the Internet. I have written about how, if someone wants to connect to your machine (for any purpose, good or bad), your computer must be running some software that opens a port.

The trouble is, it is not easy to tell if you have open ports on your machine. There are some nasty trojan programs out there, such as Back Oriface, that will open a particular port. There are people on the Internet scanning for that open port. If they discover you are running Back Oriface, they can gain complete control of your machine.

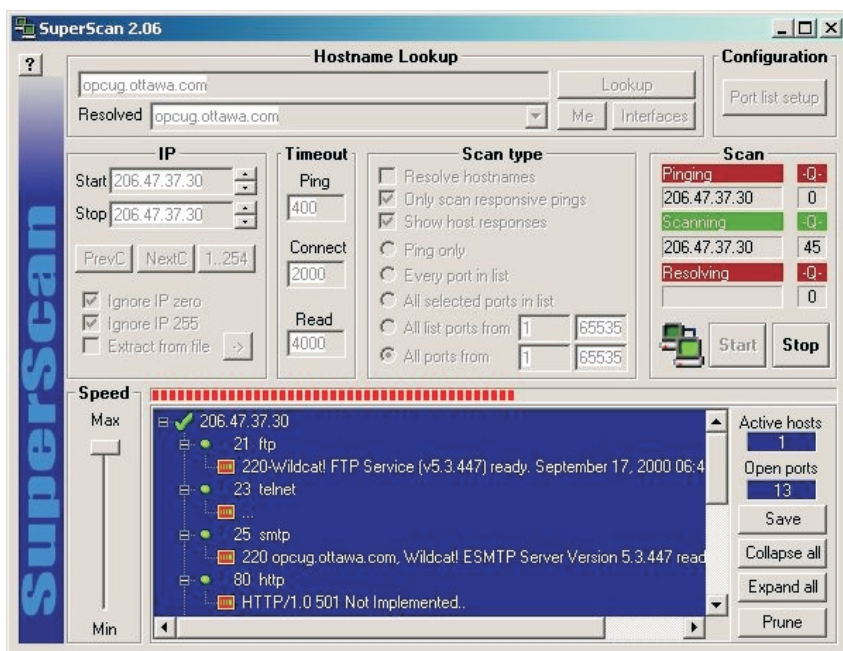
The absence of a trojan does not mean you have no open ports. For example, if you enable file and print sharing on your computer, you may be offering full access to your files to everyone on the Internet whenever you are on-line. This is because enabling file and print

sharing opens port 139. There are programs that will search for computers with an open port 139 and enumerate the shares on those machines. Then, with a simple NET USE command, someone could map a drive letter to your open shares and access your files.

I wrote about a couple of Internet Web sites that will run port scans on your computer, looking for open ports. Probably the most famous of these is the *Shields Up* site run by Steve Gibson at <http://www.grc.com>.

Unfortunately, Gibson's site only scans for a few of the most common ports.

continued on page 3...



INSIDE

Features

- Colossal code of silence broken* 4
- Bringing back the OPCUG past* 8

Club news — Club life

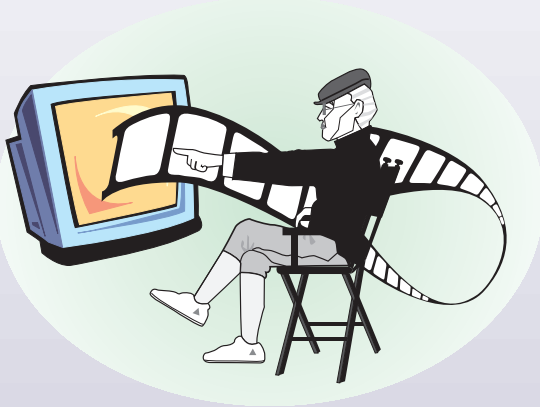
- Coming up / calendar* 2
- Club meeting dates may change* 2
- September winners* 5
- OPCUG honour roll* 6
- Financial figures revisited* 7

Next meeting: **WEDNESDAY, October 11th, 2000**

COMING UP

Fade to the Forefront...

Video editing software



Ian Malcolmson of Forefront Graphics will be making a presentation on video editing software packages for personal and professional use at our October meeting. Forefront Graphics Corporation is a leading Canadian distributor of high performance desktop computer graphics and digital video solutions.



CLUB NEWS

Club meeting dates may change

by Chris Taylor

As you will have noticed, the meeting this month is on the second Wednesday of the month, as it was last month. While, as of this writing, we have not yet received confirmation for all our meeting dates this year, a bit of explanation is in order.

Last year, a number of members expressed interest in also attending the Ottawa Carleton Linux Users Group meetings. They happened to meet on the first Wednesday of the month. Since each summer we have to go to the museum and book our meeting dates for the rest of the year, the Board of Directors decided to try for a different night that would allow members to attend both Groups' meetings. We decided to try to maintain a Wednesday night for the meeting in the hopes that a change to a different Wednesday of the month would result in the least number of conflicts members might have in their schedules.

As soon as we have received confirmation of all meeting dates for the rest of the year, we will let you know.



CALENDAR

Meetings	Date	Time and venue
OPCUG General Meeting	Digital Video Editing (see above) Wednesday, October 11 th	7:30 p.m. - Auditorium of the National Museum of Science and Technology, 1867 St. Laurent Blvd.
Ottawa Paradox Users Group	Third Thursday of each month	6:15 pm - Corel Bldg 1600 Carling Ave.
PIG SIG (i.e., Wing SIG)	October 11 th — An informal social event held after the other SIGs are finished	"Good Times" cafe at Shoppers City West, Baseline and Woodroffe
Internet SIG (I-SIG)	Wednesday, Oct. 11 th from 9–10:00 p.m.	Come and join our discussions!
Developers SIG	Wednesday, Oct. 11 th from 9–10:00 p.m.	Immediately following the main OPCUG presentation the second Wednesday of the month, and occasionally at other locations in the region.

Please note that unless otherwise noted, SIGs meet at 9:00 p.m. (immediately following the OPCUG General Meeting).

Guard your ports! ...continued from front page

However, there is software available that you can run on your own computer to check for open ports. If you are not running any sort of firewall, you can use this type of software against your own machine and get a pretty good picture of what a hacker might see if they were to run a port scan on you. If you are running a firewall, you might get a friend to run a port scan on your machine while you are both connected to the Internet.

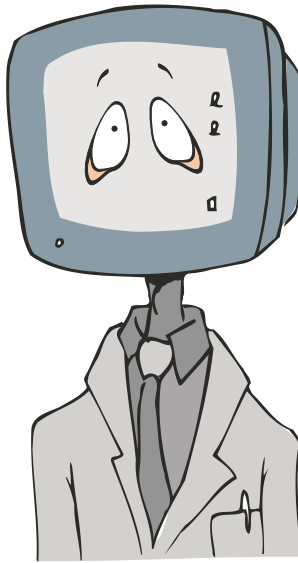
Now to finally get around to the title of this article! SuperScan v2.06 is a free port scanner you can download from PUB II's file area 35 – *Internet*, as *sscan206.zip*. There is no installation routine. Simply unzip the files into a directory and run *scanner.exe*.

There are lots of options, but to do a simple scan looking for any open port on your machine, you can just enter *localhost* in the "Hostname Lookup" box and click the "Lookup" button. Then, in the "Scan Type" section, select the last option, "All ports from" and enter 1 to 65535 in the boxes next to it. Then click the "Start" button. The results box will show any open ports. You can click the "Expand all" button to see additional details.

If you are behind a firewall or want to be certain about what is seen from the hackers' perspective, you can team up with a friend and port scan each other's machines. All you have to do is have both machines connect to the Internet. Then determine what your IP address is by running *winipcfg.exe* (on Win9x machines) or *ipconfig* (from a cmd prompt under WinNT). You can e-mail your IP addresses to each other so you can stay on-line and maintain the same address. Finally, each of you can fire up SuperScan and enter the other person's IP address in the "Hostname Lookup" box and follow all the other instructions above.

So, what do you do if you find open ports? The first thing to do is find out what is opening the port. A good resource for common port usage is RFC 1700. You can download it from PUB II in file area 35 – *Internet* as *rfc1700.zip*. Many applications use non-standard ports, but at least it is a good starting point.

If you have file and print sharing enabled, you should find that port 139 is open. Visit Gibson's site at <http://www.grc.com/su-bondage.htm>. for a good explanation of how to close this open port. Gibson has some other good information available on other pages as well, so browse around.



Some of the other ports you might find open may be harder to close. There is no magic bullet to eliminate the problem. You can try a clean boot and see if the port is closed. You can open programs one at a time and see if you can identify the one opening a port. You can run a good virus scanner that might pick up on a trojan program that is doing it.

You may find that the best solution is simply to install a personal firewall that will block anyone who attempts to connect to your machine. Many of the available firewalls will also block outbound traffic unless you specifically allow it. Since Trojan programs can attempt to do nasty things like send password information to some hacker on the Internet, this can be of great help.

Some programs are free for personal use, such as *ZoneAlarm*, *Sybergen Secure Desktop*, and *PortICE*. All are available on PUB II in file area 35 – *Internet* (*zonalm21.exe*, *ssd21464.zip*, and *portice2.zip*).

There are also a number of commercial products, such as Symantec's *Norton Internet Security*, ZoneLab's *ZoneAlarm Pro*, Tiny Software's *Tiny Personal Firewall*, Network Associates' *McAfee.com Personal Firewall*, and Network Ice's *BlackICE Defender*.

Once you install a personal firewall, you can use a port scanner to verify it is doing its job properly. To do this, you will have to have help from someone outside of your firewall to run the port scan. Running it on your own machine will not tell you what you need to know.

A word of caution on using a port scanner: **NEVER** use a port scanner on anyone but yourself or someone who has asked you to do so. Running a port scan is generally considered to be an attack. If the person on the other end detects a scan, they may report you to your Internet Service Provider. Such a complaint could get your account with your ISP terminated.



Colossal code of silence broken

Submitted by OPCUG member Paul Cooper from the "Electronic Telegraph", the Internet version of the London Daily Telegraph. Story by Roger Highfield.

After 55 years the boffins who shortened the war against Hitler can reveal more of their secrets. THE most important computer upgrade in history, one that enabled the Allies to "read the mind of Adolf Hitler" before D-Day, is about to be revealed in detail after half a century of secrecy.

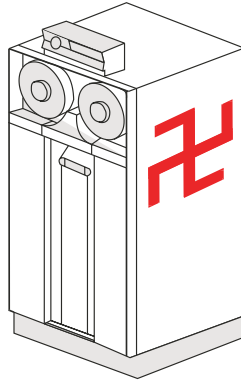
This month, the Government Communications Headquarters at Cheltenham (GCHQ) will release to the Public Record Office, Kew, a 500-page technical report on Colossus, the forerunner of the post-war digital computer and the first practical application of large-scale, program-controlled computing.

Many are familiar with Colossus but the report also contains the specifications for "Colossus II", an upgraded machine which began operation on June 1, 1944. "The modification was very important," said Dr. David Rees, emeritus professor of mathematics at Exeter University, one of the code-breakers.

Colossus II started work in time to decipher high-level messages which confirmed that Hitler had swallowed the Allies' deception campaigns over where the invasion force was to be landed, giving the Allies the confidence to go ahead with the invasion of Europe. By the end of the war there were 10 Colossi at Bletchley Park, the secret establishment in Buckinghamshire that broke German, Japanese and Italian military codes — which some experts believe shortened the Second World War by two years.

"Some will be startled to know that by VE Day Britain had a machine room of some 10 high-speed electronic computers on three-shift operation round the clock," said Dr. Donald Michie, 76, a former Bletchley cryptographer who is emeritus professor of machine intelligence at the University of Edinburgh.

A standard history of computing will probably say that the first electronic digital computer was America's ENIAC, which went into operation in 1946. But the modified Colossus "had a functionality equal to the much later ENIAC, and zillions more data-processing throughput", said Prof. Michie, who co-edited and co-authored the report with the mathematician Dr. Jack Good following the German surrender in 1945. The report details the specifications and conceptual blueprint of Colossus. More important, it describes the upgraded version, Colossus II, which could (unlike Colossus I) be programmed to a limited extent,



marking a key advance in computing of the day, before fully programmable machines were built a few years later in Britain and America.

"The modification gave Colossus an extra bit of brain, so to speak, to extend its repertoire," said Prof. Michie. "There was a crash programme to build it, and more like it."

There were two, quite different, German machine cipher systems: Enigma, for tactical purposes, such as the U boat campaign; and Lorenz, for high-level strategic traffic. It is well known that the Colossus carried out the major step in the decryption of the Lorenz radio traffic, referring to the device developed by the electronics company Lorenz to scramble messages that streamed between Berlin supreme command and some 10 army group HQs.

The Lorenz Schlüssel-zusatz 40, or *Tunny* as the British called it, resembled a mechanical cash register and converted a typed message into code using two sets of five "coding" wheels, among other confounding features, including two "motor" wheels. Even though one was not captured until German capitulation, the Bletchley cryptanalysts were able use the settings found by Colossus to set up a "virtual" Tunny: Bletchley's very own Tunny was deduced by Bill Tutte, a young mathematician, after a mistake made by a German radio operator on August 30, 1941. The operator sent a 4000-character message, after which the receiving station replied "didn't get that, please resend". The operator obliged, but with the same start settings, which was forbidden because the machine then generated the same stream of obscuring characters.

Crucially, these two streams of obscuring characters (or "key"), being exactly the same, cancelled each other out when the two intercepted transmissions were

Continued next page...

Colossal code of silence broken ...continued from previous page

superimposed. But the operator had not fed the plain-text message into the enciphering machine at exactly the same point on the two occasions, displacing them by a 'stagger' of a couple of characters. The result of the superimposition was a message in military German added to itself at a small stagger.

From this error, the code-breaker Brigadier John Tiltman was able to reconstruct the original message and deduce the key. After four months' toil, Tutte could infer the entire Tunny design, a remarkable achievement. But the Germans changed the patterns of ones and zeroes around the circumference of the Lorenz machine's 10 coding wheels, initially monthly, and eventually daily. At first it took the code-breakers days to find the correct combination of start settings to decode a message using known patterns, but months to find a given set of new patterns.

The mathematician Max Newman conceived a way to automate the effort to crack Lorenz codes, one reason why the document on the Colossus, *The Tunny Report*, is often dubbed "The History of the Newmanny". The result — the room-sized Colossus I — was born in 1943, the descendant of a prototype called "Heath Robinson". Containing 1500 valves, 10 times more than electronic machines of the day, Colossus I was built at the Post Office Research Station at Dollis Hill by Dr. Tommy Flowers and colleagues.

The new report fills a gap in the Colossus story: the addition of a new trick for semi-automatically breaking the Lorenz patterns, "wheel breaking", which emerged from a technical proposal by Prof. Michie, then just 20 years old. Because the modification boosted code-breaking by between 10 and 100-fold, it unleashed an all-out effort to crank out Colossus II. No one has described in print the crash programme to get at least one operational before D-day and as many as possible installed as soon after.

"The devil lay in the detailed implementation of the new design," said Prof. Michie. "One of the design engineers in charge of the key hardware modification is still alive, and now at last also free to talk. His name is Harry Fensom."

Fensom, 79, was one of the "lads", the engineers who worked on Colossus and the complicated circuits to conduct the wheel breaking modification, coyly referred to it as the "special attachment." Work on Colossus II, which contained 2,500 valves, began in January 1944. "For Colossus II, we had the resources of the country at our disposal," said Fensom. "We were top priority. We could demand anything and we got it." The machine went into operation on June 1, just in time to decipher messages confirming that Hitler had swallowed the deception campaigns, the phantom army in the south of England, and the phantom convoys. This gave Eisenhower and Montgomery the confidence to go ahead with D-Day.



CLUB NEWS

September Prize winners

by Mark Cayer

The following are prize winners from our meeting September 13, 2000.

A Zero Knowledge T-Shirt to:
Jillian Hyde-Clarke, Duncan Petrie.

A Freedom Software T-Shirt to:
Tim Mahoney, Frank Stokes.

A copy of the Freedom Software package to:
George Monson, Bob Whitla and Albert Wu.

Many thanks to Zero Knowledge for the donation of these prizes.

Raffle winner

Our second raffle was a big success. It raised \$90 to help keep membership fees low. Bob Herres was the winner of the 5-user copy of WinRoute Pro.

Congratulations, Bob!



ERRATUM

The article *Windows Me - Works for me!* from last month's *Ottawa PC News* was supplied by Bob Thomas, however the article originated in Microsoft's Mindshare mailout to the Developers SIG.



The OPCUG honour roll

A volunteer-run organization such as the Ottawa PC Users' Group requires the efforts of a great number of people if it is to be a success. Perhaps the greatest reason for the continued existence of the Group more than 17 years after it was formed is the tremendous number of people who have given of their time over the years.

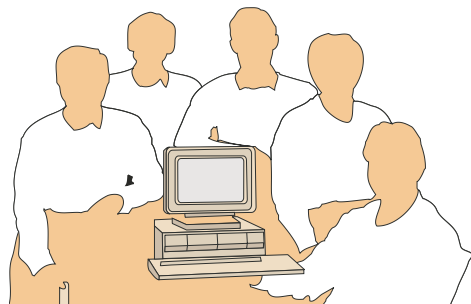
Following is a list of people who have helped to make the OPCUG what it is today. If you know of any errors or omissions in the list, please let us know at opcug@iname.com.

Armstrong, Barry (Software Librarian)
 Baker, Darryl (Treasurer)
 Baker, Philip (SIG Coordinator)
 Baudet, Paul (Newsletter)
 Blain, Suzanne (Editor)
 Breatly, Neil (Newsletter)
 Cayer, Mark (Membership)
 Chambers, Larry (Public Relations)
 Chop, Larry (SIG Coordinator)
 Clyde, Andrew (Newsletter)
 Clyde, Eric (Secretary, Treasurer, SIG Coordinator, Newsletter)
 Curling, David (SIG Coordinator)
 Cross, Bob (Public Relations)
 Cyr, Andre (Treasurer, Publicity, Editor)
 Czerfusz, Mike (SIG Coordinator)
 Dafoe, Norm (Secretary, Software Librarian)
 Doire, Jocelyn (Secretary, SIG Coordinator, Newsletter)
 Dustin, Julie (Newsletter, SIG Coordinator)
 Edwards, Mark (Newsletter)
 Falkner, Anne (Newsletter)
 Fortier, Bonnie (Editor, Sysop)
 Fortier, Jean (Sysop)
 Freise, Harald (Chairman, Membership)

Fridrich, James (Treasurer)
 Frith, Tony (Treasurer)
 Gault, Jerry (SIG Coordinator)
 Gomez, Carl-Henri (Membership)
 Gowan, Bob (SIG Coordinator)
 Green, Paul (Convenor, Membership)
 Green, Thomas (Newsletter)
 Gross, Harry (Chairman, Publicity)
 Guerra, Plato (Newsletter)
 Harris, Sandy (Editor)
 Havrot, Ted (Newsletter)
 Herres, Bob (Public Relations)
 Hibbler, Jackson (Newsletter)
 Hopkins, Gord (Chairman, Editor, Publicity, Software Librarian, SIG Coordinator)
 Hunter, Art (SIG Coordinator)
 Ings, John (Software Library)
 Jarry, Claude (Secretary, Membership, Newsletter)
 Kelland, Herb (Newsletter)
 Kreisman, Murry (Newsletter)
 Ladds, John (SIG Coordinator)
 Laidlaw, Bob (SIG Corodinator)
 Lemay, Jacques (Editor)
 Lemire, Michael (Software Library)
 Lord, Brigitte (Web Master)
 Luckham, Mike (Chairman, Treasurer, Newsletter)
 MacNeill, Andrew (SIG Coordinator)
 Mahood, Paul (SIG Coordinator)
 Mahoney, Terry (Chairman, Bulk Purchasing, Editor)
 Mahoney, Tim (Bulk Purchasing, Meeting Coordinator)
 McElvey, Chris (SIG Coordinator)
 McRoberts, Stan (Treasurer)
 Miller, Bruce (Sysop)
 Mimee, Tom (SIG Coordinator)
 Montpetit, Michael (Newsletter)
 Moxley, Anne (Chairman, Treasurer, Membership)



Moxley, Stu (Chairman, Newsletter, Facilities)
 Parkinson, Robert (Secretary, Newsletter)
 Petrie, Duncan (Editor, SIG Coordinator)
 Philips, Susan (Newsletter)
 Polich, David (SIG Coordinator)
 Poulter, Doug (Chairman, Convenor)
 Przybytek, John (Publicity)
 Rasmussen, John (Software Librarian)
 Reeves, David (Secretary, Web Master)
 Riou, Marc (Newsletter)
 Roy, Mike (Editor)
 Schopf, Bert (Chairman, Editor, SIG Coordinator)
 Schupan, Mike (Software Librarian, Sysop)
 Seal, Chris (Editor, Publicity)
 Seal, Mary (Club logo, Newsletter)
 Sells, Marty (Newsletter)
 Simons, Lynda (Editor, Secretary)
 Smith, David (Newsletter)
 Stekelenburg, Jack (Convenor)
 Svetkoff, Paul (SIG Coordinator)
 Taylor, Chris (Chairman, System Administrator, Software Librarian, SIG Coordinator, Newsletter)
 Terroux, David (Chairman)
 Thomas, Bob (SIG Coordinator)
 Tomlin, Judy (Software Library)
 Turpin, Morris (Director)
 Vandijk, Bill (Treasurer)
 Vaumoron, Jean (Newsletter, SIG Coordinator)
 Walker, Bob (Facilities)



1999 annual report figures re-visited

by James Fridrich, Treasurer

There is a correction for the 1999 figures published earlier this year. Here are the amended figures for the 1999 Annual Report. The original report published in the OPCUG newsletter early in 2000 shows a discrepancy of over two thousand dollars. This is a significant amount, and a correction is in order. The problem lies in the accounting and reporting procedure, not in the actual funds. Our bank records are (and have always been) balanced with our Quicken bank records.

The OPCUG treasurers use an accounting register called Quicken99. The reason for the discrepancy is that I posted a transaction to the incorrect account in Quicken, which balanced the bank account, but not the allocation of funds. There are 37 accounts set up by past treasurers in Quicken, some of which are a mystery to me (mainly boiler accounts generated automatically and not used), and all must be maintained. The discrepancy was found when a transfer of funds went from the Scotiabank account to our current Royal Bank account. When Quicken generated the report this transaction didn't get included. There was never a discrepancy in the paper bank records, only in the generated report.

I apologize for the error, in the 1999 report. My intention was to correct this error after the completion of a review to verify the OPCUG cash flow. This review has been completed and has been accepted by the board of directors. The review was for the past three years; a fair amount of work of which I didn't have the time to take on. Many thanks to Morris Turpin and John Archibald for graciously volunteering their efforts conducting, and completing the review.

Although I am familiar with accounting and bookkeeping principles; area of expertise lies more in manual accounting procedures than financial analysis. I was unfamiliar with Quicken99 when I first took over the treasurer position in November 1999. Since 1999 I have become much more familiar with Quicken99 and have located where the problem was, and fixed the report which now agrees with the accepted figures. The report is as follows:

1. Cashflow for Jan01-99 to Dec31-99

INFLOWS

Interest-bank income	385.00
Membership Dues	4,800.00
Transfer funds to Royal Bank	<u>13,665.73</u>
TOTAL INFLOWS	18,850.73

OUTFLOWS

Bank Chrg-Bank Charge	89.16
BBS-Bulletin Board System	2,660.08
Postage-purchase of stamps	44.31
mailing cost-Other	9.84
Meeting Costs-Meeting Costs	465.17
Membership Costs	233.41
Newsletter-Newsletter	3,504.60
Promotion costs	23.00
Funds transfer from Scotia	13,411.92
Telephone-Telephone Expense	<u>761.24</u>
TOTAL OUTFLOWS	<u>21,202.73</u>
OVERALL TOTAL	-2,352.00

2. Jan01, 1999 Balances

Cash and Bank Accounts	
Checking 97	5,271.10
BNS - GIC's-Investments	<u>10,000.00</u>
TOTAL ASSETS	15,271.10

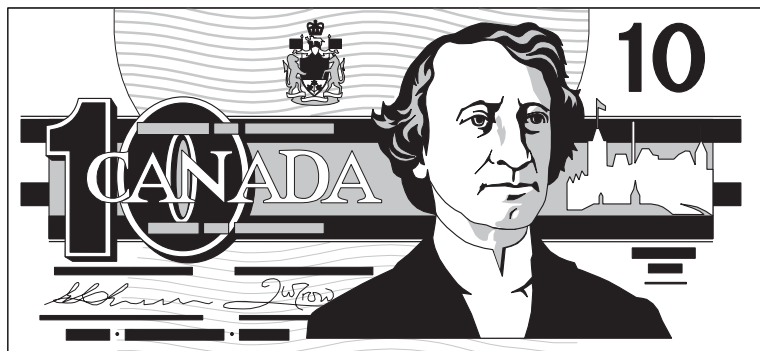
3. Dec31, 1999 Balances

Royal Bank Chequing	7,919.10
Royal GIC	<u>5,000.00</u>
TOTAL ASSETS	12,919.10

Report 3 minus report 2 equals cashflow.
 $12,919.10 - 15,271.10 = -2,352.00$

For further information or to view the OPCUG books, please contact any BOD member or myself at jimbo@magma.ca.

◆◆◆



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 three Saturdays before the general meeting. If you would like to contribute an article to *Ottawa PC News*, please submit it to the newsletter editor.

Group Meetings

OPCUG meets on the second Wednesday in the month, except July and August, at the National Museum of Science and Technology, 1867 St. Laurent Blvd, Ottawa. Meetings are 7:30–9:00 p.m. and Special Interest Groups go until 10 p.m.

Fees

Membership: \$25 per year.

Mailing Address

3 Thatcher St., Nepean, Ontario, K2G 1S6

Web address

<http://opcug.ottawa.com/>

Bulletin board—the PUB II (BBS)

Up to 33.6 kbps V.34 228-8951

Chairman and System Administrator

Chris Taylor ctaylor@nrcan.gc.ca via PUB II

Meeting Coordinator

Tim Mahoney timothy@cyberus.ca 225-2630

Treasurer

James Fridrich jimbo@magma.ca

Secretary

(Mr.) Jocelyn Doire Jocelyn.Doire@opcug.ottawa.com

Membership Chairman

Mark Cayer Mark.Cayer@StatCan.Ca 823-0354

Newsletter

Bert Schopf (editor) bert@blackbirdpcd.com 232-8427

(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

Paradox SIG coordinator

John Ladds laddsj@statcan.ca 951-4581

Webmaster

Brigitte Lord blord@magma.ca

Director without portfolio

Morris Turpin mturpin@igs.net 729-6955

© OPCUG 2000. Reprint permission is granted* to non-profit organizations, provided credit is given to the author and *The Ottawa PC News*. OPCUG requests a copy of the newsletter in which reprints appear.

*Permission is granted only for articles written by OPCUG members, and which are not copyrighted by the author.

CLUB NOTES

Bringing back the OPCUG's past

Calling long-time members! At the suggestion of webmaster Brigitte Lord, we will be featuring stories of our groups' past in coming issues of this newsletter.

We're like to see some of our longer-term members to tell the tales of when the group was founded, periods of rapid growth, when and how the software library operated, changes in the newsletter, the evolution of PUB I and II, history of our Web presence, different locations we met and the reasons for moving, name changes, etc.

Members who can remember as back as far as 1984 and operate a word processor are kindly asked to submit articles to newsletter editor Bert Schopf at bert@blackbirdpcd.com anytime.



CLUB LIFE

Reduce, Reuse, Recycle

Bring your old computer books, software, hardware, and paraphenalia you want to GIVE AWAY to the general meetings, and leave them at the table near the auditorium's entrance. *Please limit your magazines to publication dates of less than two years old.*



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.

