



OTTAWA

PC NEWS

Volume 23, Number 2

February 2006

ARTICLE

How Internet Predators Can Harm Your Computer

By Gene Barlow, User Group Relations, Copyrighted August 2005 (reprinted with permission)

This is the first of a two part article on Internet Security. This article will focus on the harm that predators can do to your computer while you are attached to the Internet. The second article addresses what you can do to protect your computer from these predators. You need to read both articles to get the whole story.

Introduction

The Internet was originally designed as a communication tool between users of a few mainframe computers located inside some Universities and Government offices. To access this early Internet, you had to use a terminal that was inside these secure locations and attached by cable to one of the mainframe computers involved. The outside world could not get access to this early Internet system. Because the original Internet was limited to a very secure environment, no security measures were designed into the Internet. Later, as the scope of the Internet was broaden and became available to almost anyone around the world, additional security features were not added to the Internet. The Internet was initially designed without security and security was never added to the Internet as it grew.

The Internet has become one of the most useful features of our computers. Almost all computers can be connected to the Internet through phone lines, wireless, or via many types of broadband connections. Today, we keep in touch with our families and friends via Internet email, chats, and Internet phones. We find enormous amounts of information on almost any topic by researching the Internet. We locate hard to find items on the Internet and can order them and have them delivered to our door. We access our bank and investments using the Internet to handle our financial affairs. The

Internet has brought us tremendous benefits in the past few years.

That is the bright side of the Internet. Unfortunately, there is also a dark side to the Internet that many of us are not fully aware of. The simple fact is that while you are connected to the Internet and can access thousands of locations, thousands of predators on the Internet can access your computer at the same time. As our connection time to the Internet increases, the risk of having harm done to our computers is skyrocketing. Broadband Internet connections greatly speed up our use of the Internet, but these are always connected and so our computer is always available to these predators. The purpose of this article is to identify who these predators are and how they use your computer for their own needs. The following article will show you what you can do to protect your computer from these predators.

Internet Predators

Who are the Internet predators that cause harm to your computer? They are called Hackers and they come in a variety of types. Taking a cliché from the old western movies, these hackers are often distinguished by the deeds they do. If you remember the old western movies, the cowboys that wore white hats were usually the good guys. The bad cowboys normally wore black hats. Likewise, you have the White Hat Hackers and the Black Hat Hackers. They both break into your computer, but the White Hat Hackers do no harm and only do it for the challenge. The Black Hat Hackers are not as kind and will do all sorts of damage to your computer once they break into it. Finally, you have the Script Kiddies who are young kids learning to become hackers.

Where do these hackers hang out? There are hundreds of hacker web sites around the world and the hackers use these sites to exchange ideas and things they have learned about hacking into certain computers. They also brag about their hacking accomplishments once they have broken into a special computer. This brings them the admiration of their fellow hackers. Young kids from 10-14 years old learn to become the future hackers of the world on these web sites. So these web sites are the training ground for new hackers to learn and develop.

Taking Over Your Computer

What do these Internet Predators do to your computer? The Black Hat Hackers go through a number of steps to break into and harm your computer. The first step is to scan for a target. They want to find a computer that has fast internet access, has enough empty space on their hard drive for storage of their hacker tools, and is a fast computer. While this is the ideal target, they will take a less valuable target if they can access it easily. They have special computer

(Continued on page 6)

Inside this issue:

Calendar / Coming Up / Raffle	2
Article: Internet Predators	1, 6
Article: To (US)B or not...(Part 2)	3, 7
Treasurer's Report 2005	4-5
President's Report 2005	7
Accounts-Audit 2005	8
IT-Pro SIG Activities	8

Next Meeting: **FOURTH** Wednesday, February 22nd, 2006

February Raffle

At the February meeting, thanks to the generosity of Morris Turpin, we have [WordPerfect Office 12](#) for re-raffle.

This full-featured suite of applications includes the venerable WordPerfect word processor, Quattro Pro spreadsheet for crunching numbers, Presentations for creating stunning ... well, presentations, and the Pocket Oxford English Dictionary.

WordPerfect Office 12 has a street price of \$350.

Raffle tickets are \$1 for one, \$2 for three, or \$5 for ten.

January Raffle Winners

Our lucky winners at the January meeting included:

Claude Jarry and **Wayne Houston** who each won a copy of MAKE magazine and **Jocelyn Doire** and **Irene Kwik** who each won a copy of Photoshop Elements.

But the evening's big winner was **Kevin Kavanagh** who not only won a door prize, a copy of Adobe Acrobat 7.0 Pro, but also won the evening's raffle prize of a copy of CorelDraw Graphics Suite 12.

Congratulations to the winners and thanks to Adobe, Corel and O'Reilly Publishing for the prizes.

Upcoming meetings

NOTE: The February meeting takes place on the FOURTH Wednesday.

► February 22, 2006 (**FOURTH** Wednesday)—Elliott Finkleman, Practical Computing, "Protect Your Computer from Virtual Crime"

March 8, 2006—Chris Taylor, "How to configure a secure (enough) home wireless network "

April 12, 2006—DBx GEOMATICS, "Web Mapping with Scalable Vector Graphics" <http://www.dbxgeomatics.com>

CALENDAR

Meetings	Date	Time and Venue
OPCUG General Meeting	FOURTH Wednesday, Feb 22 nd	7:30 p.m. Auditorium of the Canada Museum of Science and Technology , 1867 St. Laurent Blvd. http://www.science-tech.nmstc.ca/english/index.cfm
Beginners' SIG	FOURTH Wednesday, Feb 22 nd	Immediately following the OPCUG General Meeting.
IT-Pro SIG	FOURTH Wednesday, Feb 22 nd	Immediately following the OPCUG General Meeting.
PIG SIG (Wing SIG West)	FOURTH Wednesday, Feb 22 nd	10:00 p.m. (after all other SIGs) at Chances "R" restaurant, Baseline Rd. at Woodroffe Ave. (College Square Shopping Centre)
Beer BOF (Wing SIG East)	FOURTH Wednesday, Feb 22 nd	10:00 p.m. (after all other SIGs) at Liam Maguire's, St. Laurent Blvd. at Innes Rd. (formerly Hooters')

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

ENTRY FOR BEST NEWSLETTER ARTICLE

Dunc's article continues below from [last month](#). For contest details, visit <http://opcug.ca/public/Articles/contest2005.htm>.

To (US)B or not to (US)B, That Is the Question (Part 2)

(with apologies to the bard) *by Dunc Petrie*

Hubs

1. Avoid external hubs if possible. If you must, a powered hub (using an external "brick" power supply) is preferable to a self-powered (no external power supply). If you only have a self-powered hub (I believe that this is the norm for compact, portable computer hubs) resist using it with a power-hogging peripheral. Some devices will absolutely refuse to work if a hub is present in the data path. For powered hubs, check that the power supply is capable of providing sufficient power (that is, a minimum of 500 milliamps per port x number of ports). While uncommon, a few manufacturers forgot to do the math.
2. Some keyboards or monitors offer built-in hubs. Invariably, they are self-powered and are probably low speed/full speed: intended for a USB mouse and not a digital camera! The trend towards optical mice diminishes the convenience of the keyboard hub since many optical mice draw more power than a self-powered hub can sustain.
3. USB Version 1.1 and Version 2.0 hubs have important internal differences. Unless you are using only Version 1.1 devices make certain that you obtain a USB 2.0 hub (should state on the package). Be willing to spend a bit more to purchase a Version 2.0 hub that uses a chip called a transaction translator for each port. To avoid the inevitable, long-winded, technical discussion suffice to say that these little goodies smooth out the data transfers; unfortunately, the USB technical specification dictates minimally a total of one per hub, not the ideal one per port (costs extra: read the package).
4. USB Version 2.0 Hi-Speed hubs and USB Version 1.1 Full Speed ports do not work well together. The technical discussion will be avoided. Keep a

chain from the root hub to the final peripheral "pure"; that is, all the same speed. Instead, given the bandwidth foibles of hubs, an expansion card is probably money better spent.

Isochronous hardware

These devices ignore system pleas to divide bandwidth equitably; instead, they demand a constant, dedicated block that does not fluctuate. Webcams or video cameras are the traditional examples; the recent arrival of sound cards and digital sound as USB come-latelies makes the future interesting. Each one of these devices will most likely require its own root hub. That means the other port of the root hub pair must remain idle.

Thumb drives

Despite their diminutive size some are real power hogs: a situation unlikely to improve as capacity increases. Power consumption can be determined from Device Manager. Lack of adequate power might be one explanation (but not the sole one) for data corruption or loss. Thumb drives usually trigger the "Safely Remove Hardware" icon in the System Tray (beside the clock). Looking around the Internet I have found many posts stating that failure to use this icon did result in data loss or corruption. Conversely, other posts claim that clicking on the icon to obtain consent can be ignored. I believe that it depends on personal practices. As a minimum, I would recommend that the device never be removed if its indicator lamp indicates activity. A further possible explanation: drive caching is usually implemented at the system level by default.

Faithfully using this icon would prevent removal of the thumb drive before the cache was emptied and written to flash memory. To turn off drive caching (trust the indicator light exclusively) you should "Optimize for Quick Removal", as follows:

- Connect the USB flash drive to the computer's USB port
- Go to My Computer and Right-click on the drive
- Select Properties, then Hardware
- Select the USB drive in the list and click on Properties button below
- Click on the Policies tab and select "Optimize for Quick Removal"
- Click OK, and from now on all data will be written to the flash drive immediately (and not cached). Now all you need to remember is to wait until the LED on the drive goes out each time before removing it! Personally, I stick with the tried and true but now you have a choice.

Disconnecting USB devices results in a system reboot

I saw this one posted on the Internet and swallowed hard - say what? The first and simplest cure posted by Microsoft was to always use the safe removal icon. If the problem persists Microsoft suggests: <http://support.microsoft.com/kb/883517/> and <http://support.microsoft.com/kb/884868/>

Problems with device recognition

1. Intermittent recognition of USB-attached devices can often be traced to the devices requiring too much start-up current at system boot. Try distributing the heavy hitters across different root hubs. Replace a self-powered hub with a powered one (has a transformer brick) or add an expansion card.
2. Windows power management may shut down unused root hubs to conserve power. Sometimes, Windows does not wake up the ports correctly. To disable this "feature", go to Control Panel | System | Hardware tab | Device Manager. Scroll down to the Universal Serial Bus controllers and click the "+" sign immediately to the left. Scroll

(Continued on page 7)

TREASURER'S REPORT 2005



Balance Sheet, 2005

Assets

Current Assets

1000	Cash Account (TDCT)	2,457.70
1100	Investment Account (ING)	17,149.24
1200	Membership float	40.00
Total Assets		19,646.94

Equity

Owner Equity

OPCUG, Capital December 31, 2004	17,218.59
Total revenue	7,821.11
Total expenses	5,392.76

Net income **2,428.35**

OPCUG, Capital December 31, 2005	19,646.94
-------------------------------------	-----------

Total Equity **19,646.94**

Notes to financial statements:

1. Membership Income includes a total of \$ 1,550.00 derived from membership fees associated with the 2005 Digital Imaging Workshop. This included both fees for new members and fees for existing members participating in the workshop.
2. Miscellaneous Income resulted from bonus payments received from ING Direct for OPCUG members who signed up for new accounts.
3. The expenses for PUB II in 2004 included a one-time charge of \$ 941.85 for the purchase of a new computer to host the club's on-line system.

(Continued on next page)

TREASURER'S REPORT 2005

Income Statement, 2005

Revenue	2005 (\$)	2004 (\$)
2100 Bank Interest (ING)	370.11	336.41
2200 Membership Income	4,425.00	3,950.00
2300 Raffle Income	1,463.00	1,403.05
2400 Merchandise Income	0.00	135.00
2500 Workshop Income	1,550.00	840.00
2900 Miscellaneous Income	13.00	26.00
Total revenue	7,821.11	6,690.46
Expenses		
3100 PUB II Expense	1,386.17	2,071.04
3200 Newsletter Expense	2,555.64	2,833.02
3300 Office Supplies Expense	143.09	17.09
3400 Bank Charges	79.28	83.51
3500 Barbecue Expense	267.52	257.51
3600 Facility Rental	200.00	150.00
3700 Workshop Expense	616.17	544.12
3800 Merchandise Expense	0.00	967.81
3900 Miscellaneous Expense	144.89	166.19
Total operating expenses	5,392.76	7,090.29
Net income	2428.35	-399.83

Notes to financial statements *(Continued from previous page)*

4. Expenses for office supplies included customs brokerage fees for software shipped to the club, and a new supply of bank cheques.
5. The Facility Rental charge is imposed by the Museum of Science and Technology for the club's use of meeting rooms.
6. The Merchandise Expense of \$ 967.81 in 2004 consisted of a one-time charge for the purchase of clock-calendars to be used for gifts to guest speakers, and to be made available for sale to club members.
7. Miscellaneous Expenses resulted from extending our special thoughts to club members and their families.

(Accounts-Audit 2005 on page 8)

Internet Predators *(Continued from page 1)*

programs that scan and test computers connected to the Internet. Did you know that your computer is tested on average of 17 times each day by hackers looking for a target? When will they stop at your computer and decide to use it for their purposes? One in four computers will be hacked this year, so your turn is not far off.

Once the hackers find a target, their next task is to break and enter into that computer. Unfortunately, this task is very easy to do, since most computers have no security protection at all to keep the hackers out. Some users will have a firewall set up to prevent hackers from entering their computers. These firewalls have doors in them called ports. A firewall may have 256,000 doors or ports in them with some of these doors wide open. When a hacker finds a firewall, all he needs to do is to scan these ports until he finds one that is open and available for him to enter into your computer. Finally, hackers know of weaknesses in your operating system and Internet browser. He can take advantage of these weaknesses in the software and break through any security you think you have in place. It may take him a bit of time, but eventually, a hacker will find a way to break into your computer without you even knowing that he is doing this.

Once inside your computer, the hacker goes about setting up shop in your system. He may first look around for anything of value that he can steal from you. It may be as dangerous as your social security number, credit card numbers, or other financial information that he can use in the theft of your identity. Identity Theft is the number one consumer problem today and the number of thefts is growing each year. If your identity is taken and used, it will cost over \$10,000 in goods and services to resolve the problems from this crime. The hacker may find your personal digital photos saved on your computer and share them with others on the Internet. Finally, the hacker may help himself to copies of any software he finds on your computer.

Next the hacker will make changes to your computer to fit his needs. He will store his hacker tools on your hard drive so that it is available for him to use in a moments notice. These tools may include viruses and worms to send out from your computer, key loggers to watch the keys you press as you enter your password to get into your online banking, email monitors to read your email messages, and other devious tools he has available to use from your computer. Once he gets all of his tools loaded on your com-

puter, he will make your computer secure from other hackers. He will close up all of the open ports and operating system weaknesses in your computer so that other hackers will not be able to break into it. He wants your computer for his own use and not to share it with other hackers. He will leave one very well hidden back door open so that he can get back in to your computer at any time he wants to. The hacker now has your computer all ready for his future use.

Using Your Computer

Having set up your computer for his needs, what things will a hacker do with your computer? First, he may set up your computer to send out viruses to other computers. He will start with your email address book and send out these viruses to all of your friends and family members. After all, he does not want to have his computer identified as the source of the virus. Junk mail is also sent out mostly from hacked computers. My computer was hacked a couple of years ago and thousands of SPAM messages were sent out late one night using my computer. The next morning my inbox was filled with bounced messages from email addresses that were no longer valid. Just emptying these bounced messages from my inbox took hours to accomplish. Working with my ISP, we found the faulty code that let my system be hacked and fixed it. I quickly learned that these hackers are serious. Another favorite hacker use of your computer is to send out porn pictures. It would really embarrass me to learn that my computer had been used to distribute porn to others. I may even be held legally liable for permitting this porn to be distributed from my computer.

Some hackers pride themselves in bringing down main computers, like eBay, Yahoo, or AOL. Other hackers go after mainframe computers at banks, stock markets, and government offices. To do this, they need to use more than one computer. Hackers will break into and set up hundreds of computers which are called Zombie systems. The hacker can activate these Zombies to do what it wants in a few seconds. Your computer may be sitting as a Zombie computer waiting to be activated to attack some large government defense computer. When it is activated with hundreds of other Zombie computers, they all send messages at the same time to the large computer under attack. When the mainframe computer is hit at the same time by hundreds or thousands of Zombies, it can't handle the load and will shut down to protect itself. Just what the hacker wanted. The shutdown of a major computer may take hours to bring back up

and can cost hundreds of thousands of dollars in lost businesses to these companies. This is serious hacking and your computer might be involved without your knowing it.

Check Out Your Computer

So, how do you know if your system has been affected by a hacker? Hackers pride themselves in doing their mischief without anyone knowing that they have been hacked. So, finding out that you have been hacked is not easy to do. There are a few excellent software tools that have been designed to find and remove hacking tools from computer systems. The second article of this series will identify all of the things you need to do to protect your computer from hackers and to remove their mischief if you have already been hacked. Watch for this article to be sent to you in a few days or you can find it on my web site (<http://www.usergroupstore.com>) in the Newsletters section after September 1, 2005. In the meantime, you can check to see if your computer has hacker tools on it by accessing my Invisus web site at <http://www.myinvisusdirect.com/usergroupstore>. Look for and click on the small red button that is titled, "Test Your PC Now". This will take you to a page where you can download a trial of the hacker tool removal program and see what hacker tools are located on your computer. You will probably be surprised at what you find.

I hope you have learned more about the harm that can happen to your computer on the Internet. If you have questions about this article or Invisus tools, please email them to gene@ugr.com and I will try to answer them for you. Watch for my following article on protecting your computer from Internet predators.

Gene Barlow is the president of User Group Relations, a consulting firm specializing in promoting computer products to the user group community. He has over 40 years of experience with computer systems. He worked for IBM for 34 years and managed IBM's user group support organization for 14 years. He helped hundreds of user groups get started and is sometimes called the Father of User Groups for his involvement. When he left IBM, he set up his own consulting firm and has represented many software vendors to the user group community the past 9 years. He is an outstanding speaker, writer, and helper of end users and loves working with user groups. You may contact him at gene@ugr.com.

PRESIDENT'S REPORT 2005

It is nice to reflect back on the previous year and think about what was accomplished. Overall, I think it was a good year for the OPCUG.

A wide variety of topics was presented at the main meetings. Our own Don Chiasson told us about emulators. Sylvain Dumas from McAfee let us know about the evils of spyware and other "potentially unwanted programs" and came back in the fall to talk about a personal interest of his – home theatre. We learned about Voice over IP. OPCUG member and Microsoft IT Pro Advisor Rick Claus presented on upcoming technologies and later in the year on Vista, the next desktop version of Windows. Our 4th annual BBQ was a success and afterwards we learned of

software that can protect your computer from unknown malware. Michael Ondrechak from the Ottawa Canada Linux User Group showed us some of what Linux can do for us. All in attendance got to take away a "Live Linux" CD which lets you try out Linux without disturbing your current operating system. Rounding out the year, Harley Bloom from Bloom MicroTech was back with his 7th annual Christmas Wish List.

SIGs were consolidated down to the two current SIGs – IT Pro and Beginners. Both meet after the general meeting and are quite active. And we saw the formation of the Wing SIG East with members meeting at Liam McGuire's just north of the Museum.

The SIG seems to have a small but enthusiastic and growing following.

In the fall, it was announced that there would be a contest for the best member-authored newsletter article. The contest is still on, so you still have a chance to win the prize.

Our fall workshop changed theme in 2005. This year it was on digital imaging and was a huge success. If you have ideas for next fall's workshop, talk to any member of the board for directors. Planning will begin soon.

I hope 2006 will be every bit as great as 2005. Happy computing one and all.

Chris Taylor

To (US)B or not to (US)B... *(Continued from page 3)*

down to a USB Root Hub entry (may be several) and double-click on it. Go to the Power Management tab and uncheck the box beside "Allow the computer to turn off this device to save power." Repeat as required. For portable users this will increase battery power consumption.

3. Plugging and unplugging the same device can confuse Windows and the device may not be recognized immediately. Have patience: Windows, in a worst-case scenario, could require several minutes to straighten itself out.

Chipset conflicts

Conflicts exist in some cases between the embedded USB chipset (integrated onto the motherboard) and the operating system. This occurred frequently with earlier chipsets but is uncommon now. Still, if you have one of these motherboards then upgraded drivers are the most likely cure. You should also visit <http://www.guidenet.net/resources/usb.html>.

Several motherboard chipsets (particularly non-Intel) and the USB chipset (for example, one is VIA VT6212L) on the USB expansion cards do not peacefully co-exist. In some cases updated chipset drivers will resolve this; however, this depends upon the motherboard-chipset combination. Unfortunately, many of these cases are mired in the all-too-frequent scenario: "The other party is at fault and bears the responsibility for crafting a solution." Consequently, no solution is apparent for the harried end user. There are many expansion chipset manufacturers (for example, VIA, NEC, Adaptec); you should be able to find a compatible card. Obtain compatibility assurances - or money back - before you purchase.

Problems and Solutions - FireWire

Despite its more recent appearance on the Windows scene, FireWire has managed to create its own impressive list of problems. Personally, I have experienced only one (see below) on my Windows XP SP2 system. I suspect that older Windows versions and

systems/motherboards/ chipsets may experience more problems due to inadequate drivers. Visit

<http://www.pcbuyer beware.co.uk/USBProblems.htm#firewire> to find ready access to solutions from Microsoft's Knowledge Base.

Chipset conflicts (experienced this one myself)

Several ASUS boards (other makes /models I don't know) and the VIA chipset (VIA VT6306) used on many FireWire expansion cards do not peacefully co-exist. There are many expansion chipset manufacturers (for example, VIA, Texas Instruments, Adaptec); you should be able to find a compatible card. Specifically, for my Asus board, I found that the Texas Instruments chipset worked perfectly.

Conclusions

1. The more recent your hardware/operating system is the less likely you will experience problems.
2. Try to avoid using hubs for USB. An expansion card will likely be close in cost and will probably result in fewer hassles.
3. Distribute the "heavy hitters" - either power or bandwidth - across all the ports.
4. While disabling write caching is an option, I recommend that you always click the icon and await the safety message.

Additional websites

<http://www.quepublishing.com/articles/article.asp?p=339086>
(Retrofitting USB 2.0 to your system)

<http://www.quepublishing.com/articles/article.asp?p=339069>
(Configuring your system to use USB and IEEE 1394 peripherals)

http://www.tech-pro.net/intro_usb.html (How USB works)

This is the final part of Dunc's article. The entire article can be viewed online in Rich Text Format at:
[http://opcug.ca/public/Articles/\(US\)B_or_not.rtf](http://opcug.ca/public/Articles/(US)B_or_not.rtf)

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.

Member participation is encouraged. If you would like to contribute an article to Ottawa PC News, please submit it to the newsletter editor (contact info below). Deadline for submissions is three Sundays before the next General Meeting.

Group Meetings

OPCUG meets on the second Wednesday in the month, except July and August, at the Canada 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:	OPCUG membership:	\$25 per year
Mailing Address:	3 Thatcher St., Nepean, Ontario, K2G 1S6	
Web address:	http://opcug.ca	
Bulletin board — PUB II (BBS)	http://opcug.ca/default.htm	

President and System Administrator

Chris Taylor chris.taylor@opcug.ca 727-5453

Meeting Coordinator

Bob Gowan bob.gowan@opcug.ca

Treasurer

Alan German alan.german@opcug.ca

Secretary

(Mr.) Jocelyn Doire jocelyn.doire@opcug.ca

Membership Chairman

Mark Cayer mark.cayer@opcug.ca 823-0354

Newsletter

Brigitte Lord (editor/layout) brigitte.lord@opcug.ca
(Mr.) Jocelyn Doire jocelyn.doire@opcug.ca
 (e-mail distribution)

Public Relations

Morris Turpin PR@opcug.ca 729-6955

Facilities

Bob Walker 489-2084

Webmaster

Brigitte Lord opcug-webmaster@opcug.ca

Privacy Director

Bob Thomas privacy@opcug.ca 820-6835

Director without Portfolio

Wayne Houston wayne.houston@opcug.ca

Beginners' SIG

Chris Taylor chris.taylor@opcug.ca 727-5453

IT-Pro SIG

Bob Thomas ITProSIG@opcug.ca 820-6835

© OPCUG 2006.

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.

IT-Pro SIG Activities

January's SIG meeting saw attendees receiving free 1 year magazine subscriptions to their choice of Windows IT Pro or the SQL Server magazine donated to the group by Penton Media.

Free-ranging discussions centered around the new CTP (Beta II) release of the Vista Operating System, Linux varieties, multi-boot and virtual management approaches, photo management applications, disk management applications and recovery techniques, the upcoming DevTeach (Montreal, May 8-12) and TechNet (Ottawa, January 26) sessions.

We're watching to see the attendees rushing to take over the SIG's Coordinator's role because I'll be moving to B.C. this year.

Serving as your Coordinator for this SIG, the DevSIG and FoxPro SIGs over the years has been a pleasure. I hope you have equally enjoyed them.

Happy Computing,
Bob Thomas,
IT-Pro SIG

Accounts-Audit

2005 was a profitable year for the OPCUG. The Group is considered to be in good financial health and has been well managed by the Board of Directors.

An increase of \$2,428.35 is available in cash assets to begin 2006 compared with a cash short-fall of \$399.83 recorded at year-end 2004.

Report Dated 23 Jan, 2006 and certified by:

John Archibald,
Member,
OPCUG