



Agenda de janvier

8 *SIG Questions (PC)*
Organiser son disque dur

8 *SIG Cours (PC et Mac)*
Disques durs amovibles



9 *SIG Macintosh (Mac)*
BeOS

13 *SIG Jeunes (PC)*
Hellfire & Ultima Online
Centre Communautaire de 9h00 à 11h30 am

15 *SIG Cours (PC et Mac)*
Trucs et gadgets

18 *SIG Général (PC et Mac)*
Party de Noël (voir annonce page 8)

Dans ce numéro

In This Issue

P2. Damn Graphics

Andrew Trumper

P2. Photos du 8 novembre

Kristine Paul

P3. Message du Président

Ken Wood

P4. What's New

Don Druce

P4. Sig Jeunes

Michel Paul

P5. Aperçu de www.microsoft

Michel Paul

**P6. La sécurité sur le Net:
Le cambriolage**

Michel Paul

P8. Party de Noël

Ken Wood



Venez voir la version HTML du CHIP sur la page d'accueil Internet du Club à :

<http://www.cimbcc.qc.ca>
Page web du SIG Mac home page
<http://home.ican.net/~dondruce/>

Come and see the HTML version of the CHIP on the Club's Internet Home Page.

Damn Graphics!

by Andrew Trumper

Sometimes I feel like strangling my Dad. He comes into the room while I'm on the Internet, looks over my shoulder and says things such as "My, this is a tad slow, isn't it" over and over until I wish he would leave. The trouble is, he's right. Pages with large graphics files are glacially slow to load, and the sites of some large corporations are particularly bad. I go to the Apple site, for instance, and wait literally two minutes while everything loads. Worse still, the graphics you get are either advertisements or something ridiculous like a pair of eyes following your cursor around nagging you to buy something you don't want.

I suppose this impatience comes from working with Lynx on a 64 Kbps connection (one half of an ISDN line). Lynx is a Unix web browser. Since it's text-only, you can use it through, say, Zterm or a regular Telnet terminal. When I use it, my computer is acting as a virtual terminal and the program is running on a server, downloading at the server speed instead the poky 14.4 Kbps of my modem. Connections seem instantaneous, and pages load in the blink of an eye. Even the Apple page mentioned above, which takes 30 seconds to load with graphics off on my system, comes up like a flash.

**Atelier d'initiation à l'ordinateur du
8 novembre 1997**

Voir toutes les photos sur le site du Club à:
<http://www.cimbcc.qc.ca>



Le Club informatique Mont-Bruno The Mount Bruno Computer Club

ADMINISTRATEURS/OFFICERS

President	Ken Wood	514-446-9552
Vice-president	Roland Babin	514-653-9657
Treasurer	Lise Renaud	514-441-2140
Secretary	Ellen Clare O'Gallagher	514-446-9552
Past President	Bill Petrie	N/D
CHIP editor	Michel Paul	514-461-0953
Correction du français	France Doré	514-461-0896
Publicity	Geneviève Renaud	514-653-8925
SIG General	Roch Lafrance /	514-441-2343
SIG Mac	vacant	
SIG Course PC	Gérard Carignan	514-653-1811
SIG Questions	Robert Paradis	514-653-3458
SIG Internet	Roland Babin	514-653-9657
Logo Design	Jacques Dessarts	514-467-1428
Adresse postale	18 Beaumont E, St-Bruno J3V 5K6	
Internet	http://www.cimbcc.qc.ca http://home.ican.net/~dondruce/ (Mac)	

Le Club informatique Mont-Bruno a été fondé en mai 1983 en tant qu'organisme à but non-lucratif, autorisé par le conseil municipal de Saint-Bruno-de-Montarville.

The Mount Bruno Computer Club was founded in May 1983 as a non-profit organization authorized by the City Council of Saint-Bruno-de-Montarville.

CHIP is the newsletter of the Mount Bruno Computer Club. The opinions presented in CHIP are those of the authors and not the club. Articles submitted for publication must be signed and should not be longer than 1000 words. Please proof read your articles before submitting them. The last date for submission is the 12th of the month.

CHIP est le bulletin du Club informatique Mont-Bruno. Les articles présentés dans CHIP ne reflètent pas forcément l'opinion du club. Ils n'engagent que la responsabilité de leurs auteurs. Les articles doivent être signés et ne pas dépasser 1 000 mots. Les articles sont sous la responsabilité de leurs auteurs quant aux fautes. La date limite pour soumettre vos articles est le 12 du mois.

CHIP is published using Microsoft Word for Windows, Microsoft Publisher, Corel Draw 6.0 and a Hewlett-Packard HP-4L laser printer.

President's message

By / Par Ken Wood

Message du président



It's Saturday, November 8th. I've just come back from Genevieve Renaud's "Initiation to Computers" session. When I arrived at 10:30 I walked into a large room with three computers set up. At the far end, five or six people sat around Roland Babin while he explained how to open and close files and how to set up your desktop.

A little further down, a similar group sat round Robert Paradis, who was demonstrating how to copy an object from one application to another in Windows95. No one stirred from his seat during the two hours.

Next to Robert, Michel Paul sat with a somewhat larger group. He went through the business of organizing files, moving and copying files, using shortcuts and formatting floppy disks. In the background sat Michel's twelve-year old daughter, who probably knows more than anyone else in the hall, waiting for her father to finish.

While all this was going on Hélène Lortie was collecting data on the visitors and helping with the organizing. You couldn't help but be impressed by the smoothness of the operation.

In another part of the building there was a presentation for Mac beginners, given by Eric Gravel, a newcomer to the club. I didn't go in; the door was closed, and there were no chairs left, a pretty good indication of how things were going.

Next door a group of people from the Mac SIG were planning their strategy for the coming sessions. Seated around the table were Don Druce, Emmanuel Sapena, Wilfrid Sauv , Yolande L'Homme, Jean Guillet and Bernard Lambert. These are people with good ideas who are committed to keeping the Mac SIG going; I think it will do well in their hands.

Passing on to another topic, G rard Carignan now has a list of Mentors, for those who need help with their computer. His

number is given in the masthead on page 2.

J' cris ces lignes en ce samedi 8 novembre, alors que je reviens tout juste des ateliers d'"Initiation   l'informatique" organis s par Genevieve Renaud.   mon arriv e,   10 h 30, je me suis retrouv  dans une grande pi ce o   taient

install s trois ordinateurs.   l'autre bout de la pi ce, cinq ou six personnes  taient rassembl es autour de Roland Babin qui leur expliquait comment ouvrir et fermer un fichier, et comment organiser leur dossier Bureau.

Dans un autre coin, un groupe entourait Robert Paradis qui faisait une d monstration sur la fa on de copier un objet d'une application   l'autre dans Windows 95. Et personne n'a quitt  avant la fin de la pr sentation qui a dur  deux heures.

Tout pr s de Robert, se trouvait Michel Paul avec un groupe un peu plus nombreux. Il a abord  l'organisation des fichiers, le d placement et la copie de fichiers, l'utilisation des raccourcis et le formatage des disquettes. Assise au fond, la fille de Michel, qui a 12 ans en savait probablement plus que tous les autres participants, attendait sagement que son p re ait termin .

Pendant ce temps-l , H l ne Lortie faisait la collecte de donn es sur les participants et donnait son coup de main. Tout marchait comme sur des roulettes: c' tait vraiment tr s impressionnant!

Dans une autre partie du b timent,  ric Gravel, un nouveau venu, s'adressait   un groupe de novices en syst me Macintosh. Je ne suis pas entr . La porte  tait ferm e et il ne restait plus de chaises, ce qui en dit long sur l'int r t suscit  par cet atelier.

Dans la pi ce suivante, des membres du groupe Mac planifiaient les prochaines rencontres. Autour de la table  taient r unis Don Druce, Emmanuel Sapena, Wilfrid Sauv , Yolande L'Homme, Jean Guillet et Bernard Lambert. Ces personnes ne manquent pas de bonnes id es et elles veillent   la survie du groupe Mac. Je ne suis pas inquiet, le SIG Mac est entre bonnes mains avec eux.

Par ailleurs, veuillez prendre note que G rard Carignan poss de maintenant une liste de mentors   la disposition de ceux qui ont besoin d'aide avec leur ordinateur. Vous trouverez son num ro de t l phone dans l'encadr  administratif de la page 2.

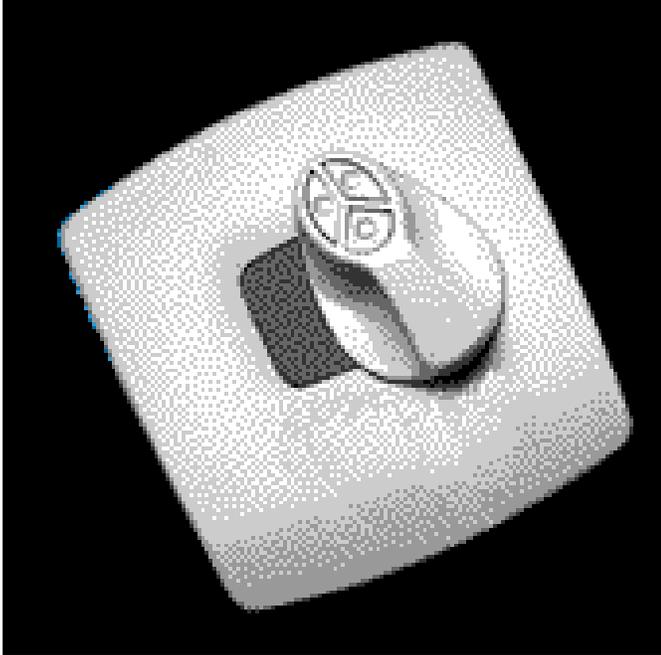
What's New

by Don Druce

Here we are back again with an assortment of new finds and facts. Items are available for both the Macintosh and PC platforms.

Felix

I have been using a Felix on my Macintosh for



several years. Much to my pleasure, I recently discovered that there is a Felix for the PC.

Felix is what Altra feels that a mouse should be. It combines some of the advantages of both the mouse and trackball. Felix has the advantages of a trackball in that it uses very little desk space and can be used anywhere - on your lap as easily as on your desk. It has the advantages of a mouse in that you control the cursor by sliding the Felix's handle - like a very small mouse. The control zone is just one inch square, reducing wrist, arm and shoulder movement and strain. You can use it all day without strain or pain.

On the PC, the Felix works with your Windows mouse drivers. Just unplug your old PS/2 mouse or trackball, plug in Felix and you are ready to go. The three buttons are conveniently placed on the handle for easy fingertip control.

Felix uses advanced optical tracking technology,

an on-board microprocessor and 640 dpi resolution to provide cursor control with precision you must try to believe. It senses your finger speed allowing you to zip across the screen, yet easily find your cursor by moving the handle to one of the corners.

As with any input device, give it a try before deciding; individual preferences certainly apply in this area.

Visit <http://www.altra.com> or contact Altra at 520 West Cedar Street, Rawlins, WY 82301-5639 Tel (307) 328 1342 for more information.

SIG Jeunes

par Michel Paul

Un nouveau SIG a vu le jour dernièrement: il s'agit d'un groupe d'intérêt dirigé par des jeunes, et pour des jeunes (de 7 à 99 ans). Les sujets abordés porteront surtout sur les jeux et sur Internet. Les réunions se tiendront au Centre communautaire le samedi matin, de 9 heures à 11 heures 30, à la fréquence de une par mois.

Au programme de la première réunion du 13 décembre prochain:

- Présentation des membres de l'équipe et de la façon dont ils envisagent le déroulement des réunions;
- Démonstration du jeu *HellFire* de Sierra On-Line, un module d'expansion pour le populaire jeu *Diablo* de la compagnie Blizzard; Démonstration du jeu *Ultima Online* de la compagnie Origin;



- Échange de trucs et conseils sur divers sujets.



Aperçu de www.microsoft.com



par Michel Paul

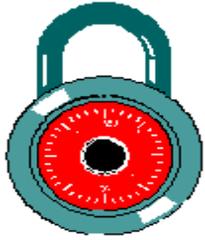
Voici quelques renseignements sur un site que tous connaissent sûrement, <http://www.microsoft.com>, et qui, je crois, pourraient vous intéresser:

- **www.microsoft.com** est l'un des sites les plus vastes et les plus actifs du World Wide Web; il est l'objet de près de 120 millions de visites par jour.
- Le site Web de Microsoft est distribué sur 44 ordinateurs.
- Des ordinateurs Compaq servent de serveurs de contenu, de recherche, de téléchargement et de bases de données.
- La mémoire vive totale des 44 serveurs est de 3,3 Go (milliers de Mo).
- L'espace disque disponible est de plus de 2 téraoctets (2000 Go).
- 8.7 Go de logiciels gratuits
- 200,000 documents HTML

Service	Rôle	Nombre de serveurs	Nombre de processeurs	Mémoire vive	Disque dur utilisé	Remarques
www.microsoft.com	Stockent le contenu du site Web général	14	4 processeurs P6	512 Mo	50 Go	155 000 pages HTML et ASP
search.microsoft.com	Répondent aux recherches du site	4	4 processeurs P6	256 Mo	30 Go	150 requêtes par min, par serveur

LA SÉCURITÉ SUR LE NET

par Michel Paul



Voici le dernier des articles ayant pour sujet la sécurité sur le Net. Nous y verrons les différentes façons dont les cambrioleurs peuvent s'y prendre pour dérober des données, de l'argent ou des secrets au moyen d'Internet.

Le cambriolage

Comme plusieurs personnes, vous conservez probablement des données confidentielles sur vous et votre travail dans votre ordinateur (mots de passe, numéros de cartes de crédit, états financiers, portefeuille de placement, contrats d'assurance, etc.). Mais vous n'avez aucune idée du risque que cela comporte.

À l'occasion d'un sondage dont les résultats ont été publiés à la fin de 1996 par *WarRoom Research*, les dirigeants de plus de 200 compagnies ont donné une idée de l'ampleur des intrusions et cambriolages électroniques dont ils ont été victimes.

Plus de la moitié des répondants ont révélé que les systèmes informatiques "vitaux" de leur entreprise ont fait l'objet d'au moins une tentative d'effraction. Le quart d'entre eux ont subi plus d'une douzaine de tentatives. Plus de la moitié de ceux qui ont déclaré avoir été attaqués ont avoué que les systèmes ont bien été infiltrés.

Habituellement, ces intrusions se font dans le cadre de l'espionnage industriel, mais on fait aussi état de vol d'argent, de mots de passe et de données. Plus de la moitié des répondants ont calculé que ces intrusions ont coûté en moyenne 50 000 \$ en pertes ou frais engagés pour la mise en place de mesures de sécurité plus strictes. Plus de 30 répondants ont révélé que les coûts ont dépassé le million de dollars.

Ce crime n'est pas insignifiant et ne donne qu'un mince aperçu de l'importance du problème réel. La plupart des crimes informatiques, incluant les cambriolages, ne sont pas rapportés. Pour faire des affaires, il faut avoir la confiance de sa clientèle, et c'est encore plus vrai lorsqu'il s'agit de transactions par Internet. Si vous admettez que votre système a été menacé, vous risquez de perdre beaucoup plus que ce que les voleurs ont pris. En fait, seulement 33 % des professionnels utilisateurs d'Internet ayant participé au sondage ont répondu qu'ils rapporteraient une intrusion de leur système informatique.

Fait encore plus troublant, plus de 25 % des répondants ont révélé que leur compagnie n'était pas en mesure de savoir si leur système avait fait l'objet d'une intrusion. Mais vous pouvez probablement faire mieux...

Facile d'entrer

Vous avez sûrement vu la scène suivante dans des centaines de films et programmes de télévision: un adolescent s'assoit devant son ordinateur, tape sur le clavier comme un malade et réussit à déjouer les systèmes de sécurité des plus grands réseaux informatiques en quelques secondes. Les effets spéciaux ont peut-être été réalisés à l'aide d'ordinateurs, mais

les créateurs ignorent ce qui se passe réellement.

La plupart des intrusions sont planifiées très minutieusement à partir d'un autre ordinateur, qui peut être situé dans un autre pays. La stratégie consiste à effectuer des demandes prudentes sur le système ciblé pour trouver des portes de sortie ou des failles qui peuvent être exploitées.

Virtuellement, tous les systèmes possèdent certaines faiblesses, et l'accessibilité qu'offre Internet rend leur exploitation presque trop facile. Lorsqu'un pirate découvre une faille, par exemple, il peut "déguiser" son ordinateur pour faire croire au réseau qu'il en fait partie, et avoir ainsi accès aux données enregistrées dans le système.

Que peut-il y trouver? D'abord votre mot de passe et votre nom d'utilisateur, dont vous avez besoin chaque fois que vous devez brancher votre ordinateur au réseau, par exemple. L'intrus pourrait aussi trouver les fichiers maîtres contenant tous les mots de passe, données financières et secrets de fabrication – en d'autres termes, à la circulation sanguine électronique de votre organisation ou compagnie.

Érigez un mur de protection

Des compagnies se protègent contre ce genre d'exploration et d'intrusion en utilisant les mêmes moyens que les intrus: ils mettent leur système informatique à l'épreuve et essaient de le casser. Malheureusement, les outils dont une compagnie se sert pour ériger ses défenses peuvent aussi permettre aux intrus d'essayer de forcer ces mêmes systèmes de défense.

Par exemple, le *System Administrator's Tool for Analyzing Networks*, ou SATAN (<http://www.fish.com/satan/>), s'est révélé aussi efficace pour les compagnies que pour les cambrioleurs. Facilement disponible sur Internet, le logiciel SATAN (basé sur le système UNIX) a permis de découvrir un grand nombre de failles dans les systèmes d'architecture de réseaux. Sa popularité a été telle qu'elle a déjà permis le développement de *Courtney* (<http://ciac.llnl.gov/ciac/ToolsUnixNetMon.html#Courtney>), un programme de surveillance continue visant à détecter les tentatives d'intrusion de SATAN. Les intrusions sont devenues tellement répandues que nous avons besoin d'outils pour nous protéger contre nos outils!

Mais les concepteurs de SATAN proclament qu'un réseau convenablement protégé ne devrait pas craindre l'utilisation de SATAN à des fins malhonnêtes. Cette protection adéquate s'appelle "coupe-feu" (firewall (<http://www.ncsa.com/library/firefacts.html>)).

Dans son expression la plus simple, un coupe-feu est un ordinateur qui utilise un logiciel conçu pour filtrer l'information qui entre ou sort d'un système. Le coupe-feu est conçu pour empêcher les intrus de pénétrer dans le système et rendre impossible la sortie non autorisée des données.

Votre fournisseur de service Internet ou le réseau informatique de votre compagnie ont besoin d'un coupe-feu très sûr et efficace, mais ce n'est sûrement pas le cas pour vous à la maison. À moins que vous n'utilisiez un serveur Internet, il est probable que votre fournisseur Internet vous assigne une adresse IP différente chaque fois que vous vous branchez.

Ainsi, le risque d'une attaque contre votre système est très faible. Si vous utilisez une adresse statique, ou permanente, ou que vous permettez à des personnes de l'extérieur d'accéder à votre ordinateur, vous avez alors besoin d'un coupe-feu.

Jouer à "mot de passe"

Votre mot de passe est votre première défense contre le vol électronique. Malheureusement, c'est peut-être aussi le point faible de votre défense.

Vous avez probablement plusieurs mots de passe: un pour votre compte chez votre fournisseur Internet, un pour votre ordinateur à la maison, un pour votre ordinateur au bureau... et bien d'autres. Et il y a fort à parier qu'ils sont écrits à un endroit facile à trouver en cas de besoin. Dès que vous écrivez un mot de passe quelque part, vous augmentez le risque qu'il puisse être découvert.

Ne divulguez pas votre mot de passe, non plus. Peu importe la confiance que vous accordez à quelqu'un, la divulgation d'un mot de passe augmente le risque de vol.

N'inscrivez pas votre mot de passe dans un fichier non codé dans votre ordinateur. Si jamais vous quittez le bureau alors que votre ordinateur fonctionne, et nous faisons tous cela à un moment ou à un autre, vous prenez un risque. Les ordinateurs portables sont encore plus vulnérables: ce sont les objets que l'on vole le plus dans les aéroports. Vous serez déjà assez malheureux de vous être fait voler votre ordinateur; inutile d'empirer les choses en donnant aux voleurs les clés de votre vie.

Si vous conservez vos mots de passe et autres renseignements importants dans votre ordinateur, encodez-les à l'aide de programmes tels que PCCrypto (<http://www.cnet.com/Content/Reviews/Hands/020397/pcc.html>) ou PGP (<http://www.cnet.com/Content/Features/Howto/Privacy/index.html>). Les renseignements qui font l'objet d'un encodage adéquat devraient être en sécurité, même contre les voleurs les plus déterminés. Il existe plusieurs utilitaires d'encodage et de mots de passe pour les Mac (<http://www.download.com/Mac/Result/TitleList/0,2,0-d-78-99,00.html>) et les PC (<http://www.download.com/PC/Result/TitleList/0,2,0-d-78-99,00.html>).

Cacher tout simplement vos mots de passe ne suffit pas. Vous ne voudrez pas non plus remplacer tous vos mots de passe par un seul, facile à mémoriser, sinon un voleur qui se renseigne un peu sur vous pourra facilement le deviner. Les mots de passe les plus efficaces sont ceux formés d'une série de chiffres et de lettres pris au hasard et qui utilisent le maximum d'espace prévu à cet effet (par exemple, si vous pouvez utiliser un mot de passe de 12 caractères, trouvez-en un de 12 caractères).

Les parents ont aussi une autre petite fuite à colmater. Les cambrioleurs potentiels se tiennent souvent dans les sites et services que les enfants utilisent. Si vos enfants passent suffisamment de temps en ligne dans des salons (*Chat rooms*) ils seront presque sûrement abordés par quelqu'un qui essaie d'obtenir des renseignements personnels (mots de passe, numéros de téléphone ou de carte de crédit, etc.). Prévenez vos enfants que les honnêtes gens ne demandent jamais ce type de renseignements et qu'ils ne doivent jamais fournir de

renseignements personnels sur Internet.

Enfin, changez fréquemment de mots de passe. Ainsi, même si un cambrioleur arrive à trouver un mot de passe à votre insu, il ne pourra pas s'en servir longtemps.

Protégez-vous... protégez vos valeurs

1. Assurez-vous que votre fournisseur de service Internet et/ou que le réseau de votre compagnie sont munis d'un coupe-feu efficace.
2. Rapportez toute intrusion électronique aux personnes responsables.
3. N'écrivez pas vos mots de passe.
4. N'enregistrez pas vos mots de passe ou autres renseignements importants non encodés dans des ordinateurs qui risquent d'être volés ou utilisés par des personnes non autorisées.
5. Assurez-vous que chaque usager d'un même ordinateur a sa propre partition et son propre mot de passe.
6. Changez souvent de mot de passe.
7. N'utilisez pas de noms ou de chiffres faciles à deviner comme mots de passe.
8. Dites à vos enfants de se méfier des cambrioleurs en ligne ou des camarades de classe trop curieux.

Voilà qui met fin à la série d'articles sur la sécurité et Internet. Je ne prétends pas avoir tout dit sur le sujet, car il est très vaste, mais j'espère que vous vous serez rendu compte que le cyberspace n'est pas sans danger, même s'il est relativement nouveau. Plus de 50 000 000 usagers utilisent régulièrement Internet et, même si quelques individus peu scrupuleux cherchent à nuire, la plupart sont là pour aider et sont honnêtes. Sur ce, bon surf...



NOËL 1997
Venez nous trouver
au Centre Communautaire
53 Rabastalière
le 18 décembre, à 18h30

Pour renseignements contactez
Larry Garinther
au 441-6829

Hope you`ll find a way to come to