Le B à B@ de la sécurité informatique pour les nuls

A distribuer sans retenue à tous vos amis non informaticiens

Philippe.Pichon@epfl.ch, EPFL DII-Support

Que ce soit parce que vous avez passé de nombreuses heures à les saisir et à les mettre en forme ou parce que vous n'aimeriez pas communiquer vos données bancaires à tout un chacun, ou encore pour des dizaines d'autres bonnes raisons, **vos données privées sont précieuses**. Chaque informaticien a des amis qui lui demandent régulièrement de dépanner leur ordinateur, et à chaque fois force est de considérer leur manque de connaissances des bases de la sécurité à mettre en place dans le domaine de l'informatique ou l'insuffisance de moyens consacrés par ceux qui sont au courant des mesures à prendre. Certes, la sécurité informatique est un domaine vaste et complexe et les entreprises doivent impérativement la confier à des spécialistes. Mais les privés peuvent aussi adopter quelques comportements évidents, faciles et très bon marché. Permettez-moi donc d'effectuer quelques petits rappels simplistes pour un peu de bon sens.

Tout d'abord, quelles que soient les mesures que vous prenez, ayez toujours à l'esprit que la sécurité absolue n'existe pas.

1er a: b@ckup (copies de sécurité)

Faites-les systématiquement et régulièrement, pour être prêt le jour où vous en aurez besoin. Hélas, en général il faut attendre une catastrophe pour qu'un utilisateur se rende compte à quel point ceci est nécessaire. Au niveau des coûts, il vous suffira de disposer de quelques CD que vous graverez, voire de disquettes; ce n'est pas la ruine.

2ème a: @ntivirus

De nos jours c'est un programme aussi important que le système d'exploitation! Avoir un bon antivirus n'est pas suffisant, encore faut-il mettre très régulièrement à jour le fichier de signatures. Vous trouverez sans peine d'excellents antivirus gratuits à télécharger, ou si vous êtes collaborateur ou étudiant à l'EPFL installez le McAffee VirusScan Home fourni gracieusement par l'EPFL en début d'année.

3ème a: firew@ll (pare-feu)

Ce petit logiciel qui sert de douanier lorsque vous vous connectez à l'Internet: chaque tentative d'entrée ou de sortie requiert votre autorisation préalable. Moins courant sur les PC privés que les antivirus, c'est pourtant devenu une évidente nécessité de nos jours. Là aussi, vous en trouverez des versions gratuites à télécharger.

4ème a: upd@te (mises à jour)

Très régulièrement, des patches (rustines) sont mis à disposition pour combler les trous de sécurité découverts, que ce soit pour votre OS (système d'exploitation), votre navigateur WEB, votre panoplie de logiciels de sécurité et vos autres logiciels. Il est essentiel de colmater ces failles au plus vite avant que de petits malins mal intentionnés ne s'en servent pour attaquer votre système.

5ème a: @ntiSpyw@re (anti-espiogiciel)

Si vous avez par exemple installé de petits (in)utilitaires, sachez qu'ils peuvent contenir des fonctions d'espionnage de vos activités: la liste des programmes que vous utilisez, les sites que vous visitez, vos adresses e-mail, les mots-clés que vous avez tapé sur les moteurs de recherche, etc. Les données collectées sont envoyées sans consentement via Internet à des entreprises peu scrupuleuses avides de ce genre d'informations, par exemple pour de la publicité ciblée. Heureusement, il existe de bons antispyware gratuits à télécharger. Mais attention: certains programmes présentés comme des antispyware ne sont en réalité rien d'autre que... des spywares !

6ème a: antisp@m (anti-pourriel)

Qui n'a pas souffert un jour de ces quantités d'e-mails non désirés qui polluent sa boîte à lettres ? L'Australie vient d'instaurer une loi punissant les spammers d'une amende qui peut atteindre A$ 1,1 mio. par jour, mais les républiques bananières ne vont pas mettre en place de telles lois dans un proche avenir... L'EPFL s'est dotée depuis plusieurs mois d'un excellent filtre à tests heuristiques. Pour les privés, il existe des adresses e-mail sur des serveurs qui filtrent les spams; hélas, ce service est en principe payant. Restent 2 solutions: se connecter à sa messagerie avec un logiciel qui ne lit que les en-têtes et éliminer manuellement les spams avant de télécharger vos messages. Plus pratique, un antispam gratuit, tel que SpamPal par exemple, auquel peut être ajouté un filtre bayésien. Quel bonheur ☺ de supprimer sadiquement ces quantités de pourriels marqués par votre antispam et qu'une règle de votre messagerie déplacera dans une valise dédiée ! Et lorsque vous devez donner une adresse e-mail sur le Web, utilisez des adresses poubelles provisoires tant que faire se peut.

7ème a: inform@tion

Celle que vous communiquez et celle que vous lisez: l'actualité de la sécurité informatique connaît certaines périodes chaudes, et la technologie ne cesse d'évoluer; tenez-vous donc un peu au courant des nouvelles menaces et des moyens pour y faire face.

L'information se traite aussi en évitant de donner fièrement son nom et son pedigree complet lorsque l'on enregistre ses logiciels; dans la mesure du possible, pourquoi ne pas vous appeler M. Privé à l'adresse nospam@nospam.ch par exemple? Quant à votre matériel, c'est à votre vendeur de le garantir. Et n'oubliez pas que si vous devez envoyer des données confidentielles par e-mail, vous pouvez crypter vos données: d'excellents logiciels mettant en œuvre la technologie de la cryptographie à clé publique sont à votre disposition sans bourse délier.

N'oubliez pas non plus que la solidité de la chaîne de la sécurité est égale au maillon le plus faible: donc, ne soyez pas le maillon faible en choisissant bien vos mots de passe mais en les écrivant en clair dans un simple fichier Excel.

Et enfin, de grâce, cessez de transmettre ces chaînes d'e-mails et diverses blagues en laissant visibles toutes les adresses des listes de destinataires...

8ème a: nettoy@ge

Avez-vous vraiment besoin de conserver 20 jours de pages historisées dans votre navigateur Web? Est-il vraiment utile de garder des quantités incroyables de fichiers temporaires ? Et ces centaines de *cookies*, vous évitent-ils vraiment beaucoup de re-paramétrage de pages ? Rien ne vous empêche d'installer un *cookie manager* gratuit et bien pratique si vous ne voulez pas supprimer systématiquement tous vos *cookies*.

9ème a: mesure org@nisationnelle (filet de sauvetage)

Si vous vous connectez à l'Internet en dial-up (vous n'avez pas souscrit à un abonnement à connexion permanente telle que l'ADSL ou le téléréseau) ou si votre ordinateur dispose encore d'un modem analogique ou ISDN, il se peut que vous soyez un jour victime d'un dialer (composeur); de tels programmes vont vous connecter à l'Internet via des numéros à surtarification, et là, bonjour la facture téléphonique ! Une recrudescence mondiale de ces arnaques est actuellement constatée. Et rien ne garantit que personne ne piratera un jour votre opérateur et n'utilisera votre numéro d'appel: le piratrage de centraux devient plus facile à cause de leur informatisation et de leur *complexification*. Or, les opérateurs téléphoniques ont enfin été obligés de vous fournir gratuitement la possibilité de demander sans frais le blocage de ces numéros (0900 et autres). Alors n'attendez pas, exigez immédiatement ceci de votre opérateur !

Bref, investir un peu de temps pour maintenir un niveau de sécurité correct vous semble trop fastidieux ? Pensez alors que ne rien faire reviendrait à laisser une bonne somme d'argent sur la table de votre cuisine, à laisser vos portes ouvertes et à publier un peu partout cette situation. Dans ce cas, ne vous étonnez pas que quelqu'un vienne se servir chez vous ! Donc, un peu de bon sens, ce n'est pas de la paranoïa. Le présent article n'est bien sûr pas exhaustif, je n'y ai volontairement pas abordé les anti pop-up, le paramétrage des systèmes, la désactivation des services inutilisés, etc. Impossible en effet de faire un tour d'horizon complet en quelques lignes.

Pour conclure, voici quelques liens

❶ à propos de b@ckup: un article émanant du TECFA de l'Université de Genève: ***tecfa.unige.ch/themes/FAQ-FL/sauver_sans_perdre/sauver_sans_perdre.html***

❷ à propos d'@ntivirus:
- Grisoft antivirus AVG est gratuit pour les privés: ***www.grisoft.com/us/us_dwnl_free.php***
- **Antivirus perso**, l'article de Christian Raemy, paru dans le FI 7/03: ***dit.epfl.ch/publications-spip/article.php3?id_article=87***
- CD antivirus McAfee EPFL 2004: ***winsec.epfl.ch/core/index.asp?article=54***

❸ à propos de firew@all: ZoneAlarm, dont une version est gratuite: ***www.zonelabs.com/***

❹ à propos de mises @ jour:Windows update, pour mettre à jour cet OS (surtout les mises à jour critiques et service packs): ***v4.windowsupdate.microsoft.com/fr/default.asp***

❺ deux bons @nti-spyw@re gratuits: LavaSoft AdAware, ***www.lavasoft.de*** et SpyBot, ***www.safer-networking.org/*** (don suggéré pour ce dernier)

❻ à propos d'antisp@am:
- l'article sur MailCleaner de Martin Ouwehand, paru dans le FI 8/03, ***dit.epfl.ch/publications-spip/article.php3?id_article=182***;
- la page de MailCleaner à l'EPFL: ***dit.epfl.ch/mailcleaner.***
- le site de l'organisation Spews / Spam Prevention Early Warning System: ***www.spews.org/***
- SpamPal, un anti-spam gratuit pour les privés: ***spampal.corlobe.tk/frame_down.html***

❼ à propos d'inform@tion:
- la page de download de PGP (freeware): ***www.pgpi.org/download/***
- le site de news sur la sécurité informatique et sur les nouvelles technologies: ***www.zataz.com/***
- également un serveur FTP avec plein de logiciels en rapport: ***ftp://ftp.zataz.com/***

❽ à propos de nettoy@ge: Cookie Manager, pour trier les cookies que vous voulez conserver de ceux que vous voulez supprimer: ***www.artisan2k.com/lagratuitheque/securite/cookiesmanager.htm***

❾ à propos de mesure organis@tionnelle:
- l'OFCOM (Office fédéral de la communication), à propos des 0900: ***www.bakom.ch/fr/service/tc/0900/***
- la page de Sunrise sur les 090x: ***www.sunrise.ch/fr/home/support/sup_dia.htm***,
- et la demande de blocage: ***internet.sunrise.ch/fr/general/gen_dial_block_form.asp*** (cochez **tous les sets**)
- la page de Swisscom: ***www.swisscom-fixnet.ch/fx/content/specialservices/outgoingcallbarring/index_FR.html*** ■