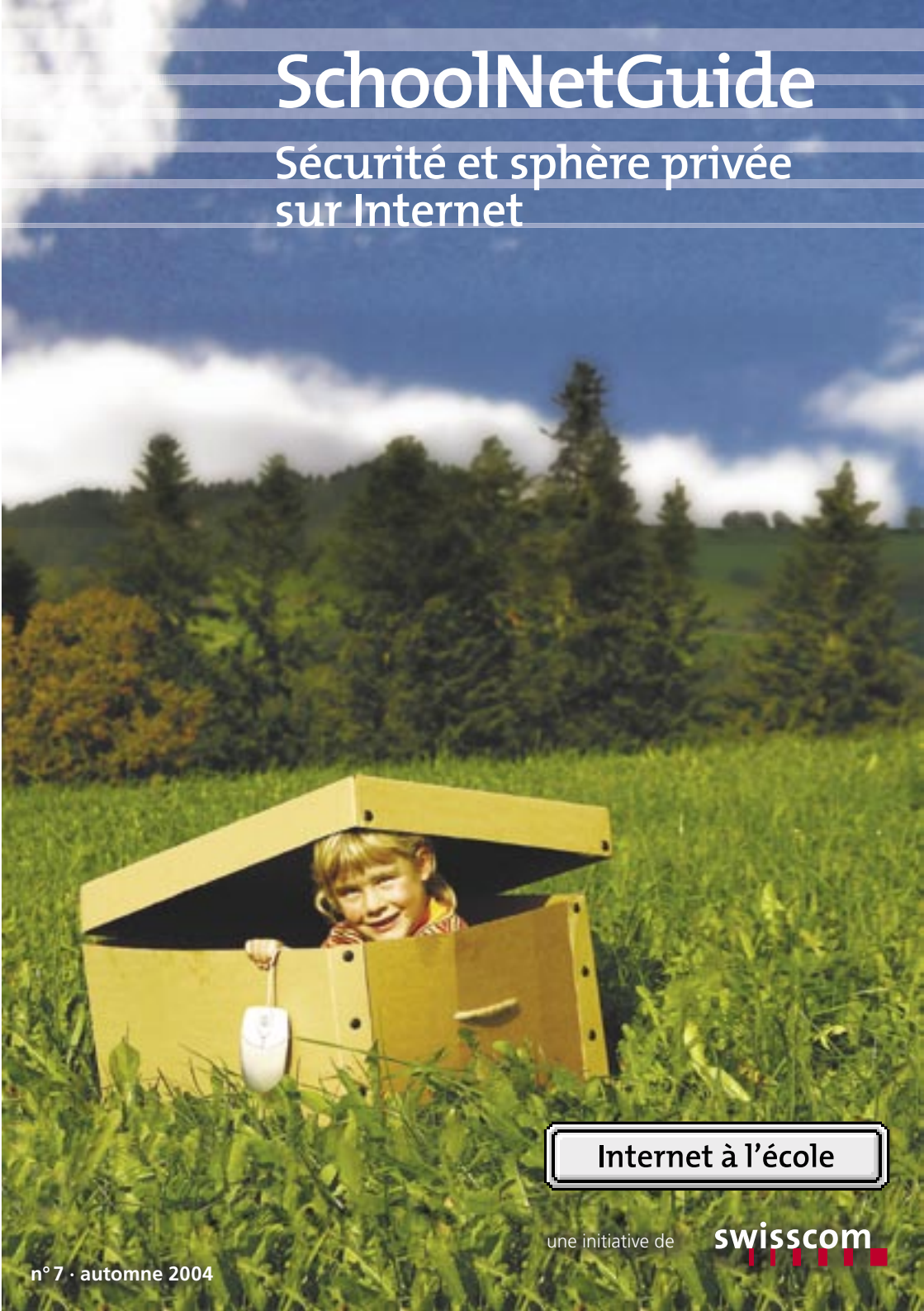
SchoolNetGuide

Sécurité et sphère privée sur Internet



Internet à l'école

une initiative de swisscom

n° 7 · automne 2004

Mot de bienvenue de l'éditeur

Chers utilisateurs Internet,

Avec les derniers numéros du SchoolNetGuide, nous nous adressions en partie aux enseignants et en partie aux parents d'écoliers. Le thème de ce septième numéro – la sécurité – nous concerne tous : à l'école, au sein du cercle familial ou dans la vie professionnelle.

Les questions de sécurité ne se posent pas seulement depuis le succès d'Internet, mais accompagnent notre quotidien depuis toujours ; nous nous y sommes habitués, sommes en mesure d'évaluer les risques et de les gérer. Nous savons que les serrures de sécurité qui verrouillent nos portes ne sont pas inviolables mais nous nous sentons suffisamment en sécurité pour dormir la nuit. Nous ne paniquons pas à la vue du panneau «Attention voleurs» au check-in de l'aéroport et ne décidons pas de renoncer une fois pour toutes à prendre l'avion. Et dans un tram bondé, nous faisons automatiquement plus attention à notre porte-monnaie que lorsque nous nous promenons à la campagne.

Ces principes – connaître les risques, s'en protéger, agir comme il se doit dans les cas particuliers – s'appliquent aussi à la sécurité et à la sphère privée sur Internet. Vous apprendrez aux pages suivantes d'où peuvent venir les risques, quelles sont les précautions de sécurité à prendre et comment vous devez réagir en cas de menace.

Avec ce SchoolNetGuide plus complet, nous contribuons à l'exposition «Cybernetguard» du Musée suisse des transports et des communications de Lucerne, que nous avons soutenue avec plaisir.

Swisscom SA vous souhaite une navigation sûre et sans soucis.

Marc Pfister
Chef «Internet à l'école»

Contenu

PaperLink

Vous pouvez consulter rapidement et aisément tous les liens repris dans cette brochure grâce à « PaperLink » : **f700 www.swisscom.com/sai**

1. Consultez le site **www.schoolnet.ch/guide/f**.
2. Tapez le chiffre à côté du lien, par exemple f700, dans le champ de saisie PaperLink.
3. Vous serez automatiquement transféré(e).

Pourquoi y a-t-il des problèmes de sécurité ?

Pour comprendre les risques de sécurité potentiels, il peut s'avérer utile de comprendre les motifs de l'«ennemi» éventuel. Il convient de faire la distinction entre les **menaces techniques**, qui peuvent être destructrices même quand le responsable n'en profite pas, les **contrariétés**, qui ne peuvent pas endommager vos données mais peuvent vous faire perdre votre temps ou votre calme, et les **activités frauduleuses**, c'est-à-dire quelqu'un «en voulant à votre argent». Nous différencions brièvement ci-dessous ces trois types de problèmes mentionnés à maintes reprises dans le guide.

▲ Dangers techniques

Les logiciels qui peuvent ouvrir les fichiers, afficher des images ou des textes et jouer de la musique sont des programmes. La plupart des programmes installés sur votre ordinateur sont inoffensifs, mais il existe aussi de mauvais programmes introduits clandestinement par quelqu'un qui veut vous nuire. Les virus, vers, chevaux de Troie ou espiogiciels (spyware) sont aussi appelés génériquement «malware» (abréviation angl. de «malicious software» = logiciels malfaisants). Le programmeur de ces mauvais logiciels ne profite en rien des dégâts qui vous sont occasionnés. Pour lui, il s'agit simplement de se mesurer aux fabricants de «contre-mesures» en tous genres ; il veut jouir de la célébrité douteuse d'avoir été, du moins pendant un petit temps, plus malin qu'eux.

■ Contrariétés

Le bien-fondé d'inclure les contrariétés qui ne causent pas de dégâts dans les problèmes de sécurité se discute. Les dégâts se comptent en temps perdu. La publicité qui remplit la boîte aux lettres, les fausses alarmes mettant en garde contre des risques inexistants ou les messages apparaissant soudain à l'écran ne présentent pas de véritable menace mais l'utilisateur s'en passerait bien. Les responsables sont soit des annonceurs peu sérieux comme dans le cas des mails commerciaux indésirables («spam») ou tout simplement des farceurs qui n'ont pas vraiment de mauvaises intentions. Le spam est une zone grise : les mails publicitaires peuvent présenter tant une méthode peu sérieuse de vendre des produits «décents» en soi (ironiquement des filtres anti-spam, p. ex.) qu'une tentative d'escroquerie.

● Activités frauduleuses

Avec Internet, les escrocs ont découvert un nouveau canal par le biais duquel ils essaient de vous soutirer directement de l'argent ou d'obtenir des informations confidentielles pour vous escroquer indirectement. La vie de tous les jours nous a depuis longtemps appris une partie des astuces utilisées – mais, sur Internet, il nous manque encore l'expérience et le flair pour identifier sur-le-champ la tentative d'escroquerie. On peut cependant développer ce flair en faisant tout simplement ressortir les parallèles. Le «vol d'identité», similaire à celui des cartes de crédit et des cartes d'identité, joue p. ex. un rôle important.

● Espions

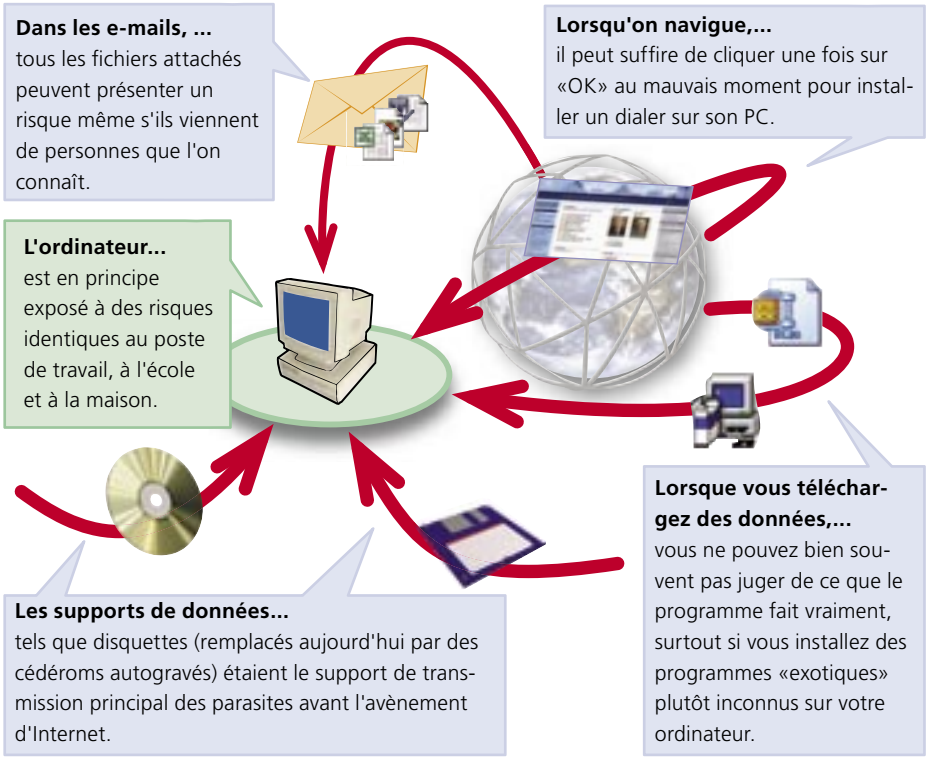
Reportez-vous à la page 14 pour les cas particuliers des pirates, des espiogiciels et des wardrivings.

D'où vient le danger ?

Diverses portes d'entrée

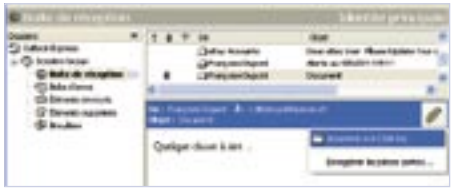
Il existe un danger potentiel en plusieurs endroits. Il est important d'être conscient des activités où la vigilance s'impose.

- Les **e-mails** constituent la porte d'entrée principale aux virus, vers et autres parasites. Les fichiers attachés aux e-mails par des inconnus doivent donc éveiller votre méfiance. Mais des textes purs peuvent aussi être «malfaisants» s'ils souhaitent vous attirer sur des sites Web peu sérieux par de fausses déclarations.
- Vous pouvez aussi attraper des parasites lorsque vous **naviguez** – avant, c'était surtout le cas des sites Web aux contenus «douteux» tels que des offres érotiques, mais aujourd'hui, il y a même des dialers sur les sites proposant des recettes.
- La prudence est toujours de rigueur lorsque vous **téléchargez des données**. Les programmes gratuits en particulier ne tiennent pas toujours leurs promesses.
- Les parasites peuvent aussi atterrir sur votre ordinateur à partir des **supports de données changeables** tels que disquettes ou cédéroms. Ce type de diffusion devient toutefois de plus en plus rare – Internet est tout simplement bien plus pratique, même pour les escrocs.



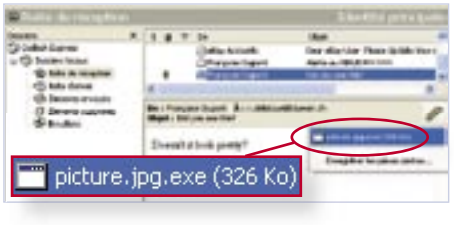
Prudence avec les mails

Dangers techniques
Les personnes qui n'utilisent que le mail et ne naviguent pas beaucoup sont-elles moins en danger ? Non. La plupart des parasites se propagent sous forme de fichiers attachés. Le programme peut démarrer, agresser votre système d'exploitation et essayer de continuer à se propager par l'intermédiaire de votre PC quand vous les ouvrez.



▲ Virus simple F250
Même si vous connaissez l'expéditeur, il est possible qu'un virus soit dissimulé dans le fichier attaché. Si un virus infecte votre PC, il peut à son tour infecter des fichiers que vous envoyez à d'autres personnes.

Mise en danger par…	Prudence avec les fichiers se terminant par …
… l'accès au système d'exploitation	.bat, .com, .exe, .htm, .html, .inf, .js, .jse, .vbe, .vbs
… la lancement de programmes	.chm, .lnk, .pif, .rm, .rt, .scr
… l'exécution d'activités indésirables (cachées dans le document normal)	.mdb, .pps, .wsh, .doc, .xls



▲ Virus camouflé
Les programmeurs de virus camouflent des programmes exécutables en les munissant d'extensions de fichier doubles. Dans Windows Explorer et les programmes de mail, les extensions des fichiers ne sont pas affichées pas défaut de sorte que le fichier **Picture.jpg.exe** ressemble à une image «inoffensive» intitulée **Picture.jpg**. Si vous voulez visionner cette «image», vous installez en réalité le virus sur votre ordinateur.

Les virus s'attachent de préférence à des fichiers d'installation, appellent d'autres programmes ou se nichent sur des disquettes ou cédéroms. Les documents Word ou Excel peuvent eux aussi contenir des virus (= **macrovirus**).

La bonne nouvelle : les virus doivent en règle générale être activés, c'est-à-dire que tant que vous n'ouvrez pas un fichier suspect attaché à un mail, le virus ne peut pas endommager votre ordinateur. Les scanners antivirus actualisés en permanence identifient en outre presque tous les virus.

Il en va différemment des **vers F415** : ils ont certes en fin de compte des effets similaires à ceux des vers mais fonctionnent un peu différemment : Un virus a besoin comme dans la nature d'un «hôte» et l'utilisateur doit, comme on l'a déjà dit, cliquer dessus pour qu'il s'exécute. Il essaie d'infecter des fichiers sur un système. Le ver par contre est un programme autonome qui s'exécute pour ainsi dire lui-même (ce qui est rendu possible p. ex. par des paramètres de sécurité trop relâchés dans le **navigateur F210** ou le programme de mail) et essaie alors de se propager sur différents ordinateurs dans un réseau.

En raison de ces propriétés, les vers se propagent généralement nettement plus vite que les virus et jouissent par conséquent ces dernières années d'une certaine célébrité dans les médias : le premier grand tumulte autour du ver «ILOVEYOU» en 2000 a été suivi de parasites comme «Lovsan», «Sobig» et «MyDoom». Ces vers utilisaient souvent des failles dans les systèmes d'exploitation ou programmes Microsoft, failles contre lesquelles il existait déjà des «antidotes», de sorte que la propagation aurait progressé nettement plus lentement si tous les utilisateurs avaient actualisé leurs ordinateurs.

▲ Ver e-mail
Les vers e-mail sont une combinaison de virus et de vers. Ils essaient de s'envoyer sous forme de fichier attaché à un e-mail à des adresses qu'ils trouvent p. ex. dans le carnet d'adresses du programme de mail. Une adresse e-mail étrangère est souvent utilisée comme adresse (prétendue) de l'expéditeur. Le propriétaire du carnet d'adresses et le propriétaire de l'adresse n'ont aucune idée de ce qui se passe.

Contre-mesures en cas de dangers techniques dans l'échange de courrier
Il est facile de vous protéger contre une attaque virale ou par des vers par mail.

1. Installez un logiciel antivirus (cf. p. 19 à 20).
2. Vérifiez les paramètres de sécurité de votre programme de mail (cf. p. 22 à 23).
3. Pesez le pour et le contre avant d'ouvrir des e-mails ou des fichiers attachés envoyés par des inconnus (cf. p. 28).

La plupart des virus et vers sont programmés avec l'intention de nuire bien que le responsable n'en tire aucun avantage direct. Il y a certes aussi des vers sans «routine destructrice» spéciale. Mais même ces vers peuvent faire des dégâts économiques considérables en accablant p. ex. par leur propagation un réseau de société au point qu'il devient temporairement inutilisable pour tout travail normal.

Contrariétés dans la boîte aux lettres

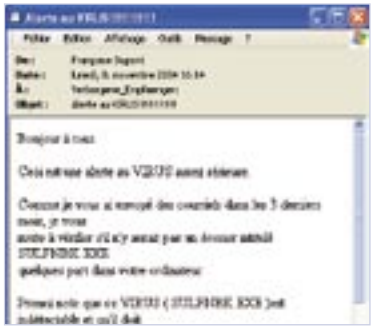
Spam ou junk mail F267

Les mails publicitaires indésirables (= spam) sont envoyés simultanément à de nombreux destinataires et font de la pub pour tous les produits imaginables, du régime amaigrissant aux accessoires de PC. Les intentions derrière ces mails vont de la vente de produits sérieux aux arnaques illégales, en essayant p. ex. de convaincre les utilisateurs d'investir dans des placements douteux en leur faisant miroiter des gains séduisants.

Vous reconnaissez p. ex. le spam à l'adresse insolite de l'expéditeur ou à des lignes de sujet concises («Premier rappel», «Tu te souviens de moi ?»).
Si vous correspondez surtout en français, les mails de spam en anglais sont faciles à reconnaître.
Les mails de spam sont inoffensifs mais peuvent s'accompagner de virus ou renvoyer à un site Web avec un dialer (cf. p. 11).
N'ouvrez pas les mails de spam et n'y répondez pas non plus même pour vous désabonner (lien vers «unsubscribe»), car chacune de ces actions peut avoir pour conséquence de confirmer à l'expéditeur qu'il s'agit vraiment de votre adresse.

Canulars F253

(angl. hoax) Les canulars sont des faux messages d'alerte mettant p. ex. en garde contre un prétendu nouveau danger («mise en garde contre tel virus !!!»). Vous reconnaissez les canulars à l'injonction de les transmettre à toutes les personnes que vous connaissez, à la description inquiétante du dommage («efface tout le disque dur») et à la référence à des autorités apparentes telles que Microsoft, AOL ou la police). Ne procédez à aucun changement sur votre PC sur la base de tels mails.



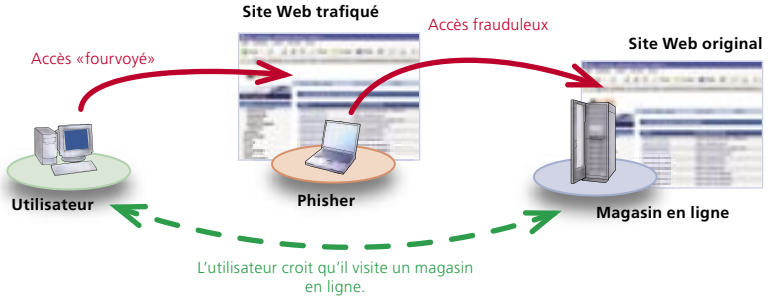
Règles de comportement vis-à-vis des mails indésirables

1. N'ouvrez pas le spam et n'y répondez si possible pas (cf. p. 28).
2. Installez un logiciel de protection antispam (cf. p. 17).
3. Ne transmettez pas de messages de mise en garde contre de prétendues menaces sans les avoir vérifiés (cf. p. 27).

E-mails frauduleux

«Phishing» F407

(de l'angl. «Password Fishing», c'est-à-dire pêche aux mots de passe). Ici, vous pouvez subir des dommages sérieux : les auteurs envoient des e-mails dont les expéditeurs prétendent être votre banque ou un magasin (p. ex. eBay ou Amazon). Dans le mail «hameçon», vous êtes invité, sous un prétexte ou un autre, à vous inscrire sur le site Web de l'offreur avec votre numéro de client ou de compte et votre mot de passe. Mais le lien mène à un site trafiqué qui ressemble à s'y méprendre à l'original. Si vous saisissez effectivement vos données, les responsables peuvent dans le pire des cas accéder à votre compte bancaire ou faire des emplettes en votre nom.



Vous reconnaissez les mails «hameçon» à :

- une salutation impersonnelle telle que «Cher client» (l'escroc ne connaît pas votre nom à la différence de votre véritable offreur)
- l'invitation urgente à vous logger sur-le-champ, souvent liée à une menace (votre compte sera fermé si vous n'obtempérez pas).
- un lien direct dans le texte vers le masque de Login pour éviter que vous tapiez l'adresse du vrai site.
- quelquefois la mauvaise langue. Si vous êtes inscrit chez eBay Suisse, vous ne recevez pas d'e-mail en anglais d'eBay.

Règles de comportement vis-à-vis des e-mails frauduleux:

1. Soyez méfiant si un e-mail vous exhorte à agir immédiatement.
2. Ne cliquez pas sur les liens dans des mails suspects mais tapez l'adresse de l'offreur que vous connaissez.
3. Informez-vous sur le site Web de l'offreur des caractéristiques de sécurité utilisées (pour une banque, p. ex. le certificat numérique correct, etc., cf. p. 33-35).
4. Informez sur-le-champ l'offreur de l'incident.

Prudence quand vous surfez

Dangers techniques

Certains parasites s'installent sur votre ordinateur lorsque vous surfez ou que vous téléchargez des programmes sur Internet.

▲ Vers F415

Les vers – déjà mentionnés dans la section E-mail – peuvent aussi se servir de votre connexion Internet pour se propager. L'un des vers les plus mal famés est le «Blaster», aussi appelé «Lovsan». Les vers profitent souvent de failles de sécurité dans le système d'exploitation pour infecter le PC. Le Blaster peut atterrir sur votre ordinateur sans que vous téléchargiez quoi que ce soit ou ouvriez un fichier attaché à un mail. En cas d'attaque, il cause des redémarrages constants du PC. Une actualisation fréquente du système d'exploitation a pour effet d'enrayer la propagation de la majorité des vers et donc aussi du Blaster.

▲ Chevaux de Troie F251

Les chevaux de Troie doivent leur nom au célèbre cheval du même nom. Ils prétendent être autre chose que ce qu'ils sont en réalité : un programme qui semble utile, servant p. ex. à télécharger plus rapidement de la musique ou à détruire un parasite, contient en réalité un «mauvais» programme.

■ Pop-ups IP / Affichage des messages

Les pop-ups IP (IP = protocole Internet , angl. pop up = surgir) sont des messages Windows apparaissant soudainement et faisant référence à des sites Web. Ils étaient conçus à l'origine pour des messages courts dans les réseaux de sociétés, mais comme le «service de nouvelles» est d'abord activé sur chaque PC sous Windows, tout PC non protégé par un pare-feu peut les recevoir. Les messages sont énervants mais inoffensifs tant que vous ne visitez pas le site Web mentionné (qui contient la plupart du temps un dialer). Un endommagement direct du PC n'est pas possible ; les pop-ups ne connaissent en effet pas de fonction en-dehors du bouton OK.

Règles de comportement vis-à-vis des dangers techniques lorsque vous surfez

1. Actualisez régulièrement votre système d'exploitation (cf. p. 24).
2. Installez un pare-feu (cf. p. 20 à 21).
3. Installez un logiciel antivirus (cf. p. 20 à 21).
4. Désactivez l'affichage des messages Windows (cf. p. 23).

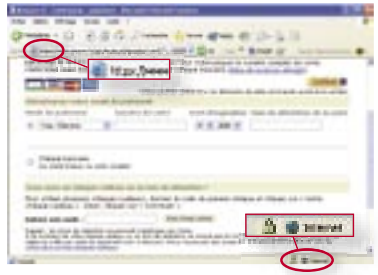
Activités frauduleuses

Il s'agit aussi, lorsque vous surfez ou faites des emplettes en ligne, de reconnaître les signes de tentatives d'escroquerie et de faire preuve d'une méfiance saine mais pas excessive.

● Les dialers F371

offrent la possibilité de se procurer des contenus payants via Internet et de les imputer à la facture téléphonique. Leur utilisation est illégale si le prix de connexion n'est pas indiqué, s'il est dissimulé ou si le dialer remplace la connexion standard à l'insu de l'utilisateur, ce qui n'est possible que dans le cas d'une connexion à numérotation (transmission de données à distance), en cas d'accès par ADSL, les dialers ne peuvent pas faire de dégâts. L'exemple de droite illustre un dialer visible : si vous confirmez, vous approuvez l'installation du dialer sur votre PC. En Suisse, l'utilisation de numéros 0900 par les dialers est interdite. Mais les dialers peuvent toujours établir une connexion Internet par le biais de numéros internationaux payants.

● Utilisation de cartes de crédit



Ne donnez vos informations de carte de crédit (et vos coordonnées bancaires) que sur les sites sécurisés. Les connexions non sécurisées peuvent être «interceptées» et vos informations de paiement peuvent tomber entre de mauvaises mains. Vous reconnaissez les sites sécurisés au petit symbole de cadenas dans la ligne d'état de votre navigateur ou au sigle http**s** dans la ligne d'adresse (cf. p. 29).

● Escroquerie par non-livraison/non-versement

Pour ce qui est des enchères en ligne (p. ex. sur ricardo.ch), votre partenaire commercial est la plupart du temps un particulier ou un petit entrepreneur. Il peut y avoir parmi eux des brebis galeuses. Notez avant de faire une offre de vente ou d'enchère les informations relatives au partenaire et à la protection de l'acheteur ou du vendeur sur le marché respectif.

Règles de comportement vis-à-vis des activités frauduleuses lorsque vous surfez

1. Cliquez «Non» si on vous demande s'il faut installer un programme que vous n'avez pas cherché vous-même à télécharger.
2. Veillez à utiliser des voies de transmission chiffrées lorsque vous effectuez des paiements sur Internet (cf. p. 33).
3. Vérifiez avant d'acheter et de vendre en ligne que l'offreur respectif semble bien digne de confiance.

Prudence avec les données sensibles

Quand vous vous déplacez sur Internet, vous laissez des traces. Certaines d'entre elles sont générées automatiquement alors que vous en «créez» ou encore en retenez d'autres. En principe (tant que vous ne faites rien d'illégal) : vous êtes anonyme sur Internet jusqu'à ce que vous vous identifiez vous-même sur un site Web, p. ex. pour faire des achats ou vous inscrire à un service.

Traces sur le Net

L'adresse IP F107 est l'adresse univoque de chaque ordinateur sur Internet. Lorsque vous connectez votre ordinateur à Internet, votre fournisseur Internet affecte automatiquement une adresse IP à votre PC. En tant que particulier, vous n'avez en règle générale pas d'adresse IP fixe mais recevez à chaque visite sur Internet une autre adresse justement libre.

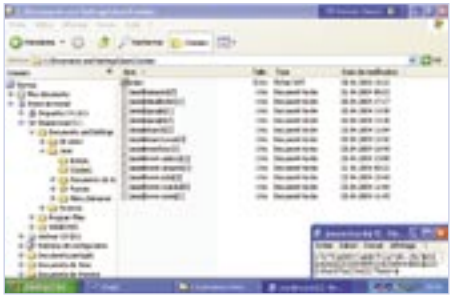
Site Web	Adresse IP
www.swisscom.ch	130.190.1.60
www.creditsuisse.ch	198.240.212.225
www.microsoft.ch	207.46.250.119

Lorsque vous appelez un site Web ou écrivez quelque chose dans un **forum** F408 l'adresse IP actuelle de votre ordinateur est automatiquement enregistrée sur le **serveur** F116 de l'exploitant. Seul votre **fournisseur** F103, p. ex. Bluewin, pourrait déterminer qui naviguait quand avec quelle adresse IP. Vous restez donc anonyme vis-à-vis de l'exploitant du site Web jusqu'à ce que vous vous identifiez volontairement. Le fournisseur doit garder l'information indiquant qui a utilisé quelle adresse IP quand pendant six mois, et la dévoiler – en cas de suspicion d'agissements criminels – à la demande des autorités d'enquête. C'est cependant, on s'en doute, l'exception à la règle.

Cookies F254

Les cookies sont de petits fichiers texte déposés sur votre PC pour que le serveur vous reconnaisse. Nombreux sont les mythes les concernant. La vérité est qu'il en existe deux sortes :

Les **cookies de session** ou temporaires sont recréés à chaque visite. Ils vous permettent p. ex. de remplir votre panier sur plusieurs pages dans un magasin en ligne. Dès que vous quittez le site, le cookie est effacé. Les cookies persistants sont par contre sauvegardés ensuite sur votre ordinateur. Dans les deux cas : le **serveur Web** F353 reconnaît chaque fois votre ordinateur (et votre ordinateur seulement) – il ne sait pas qui vous êtes personnellement jusqu'à ce que vous vous identifiez.



Exemple de cookies persistants

Si vous achetez quelque chose sur Amazon, vous vous enregistrez. Vos données personnelles (nom, p. ex. «Marie Gilbert», adresse, informations de paiement, etc.) sont enregistrées dans une base de données clients – et un cookie qui ne renferme p. ex. que le chiffre 1234567890 est laissé sur votre ordinateur. Ce numéro est aussi enregistré dans la base de données clients. La prochaine fois que vous rendez visite à Amazon, le serveur peut lire le chiffre dans le cookie – et ce chiffre seulement ! La relation entre votre ordinateur et vous est établie par l'intermédiaire de la base de données clients ; l'accueil est personnalisé : «Bienvenue Marie Gilbert» et des zones telles que «Conseils personnalisés» peuvent être affichées.
Amazon donne cependant très simplement à l'utilisateur la possibilité d'effacer le cookie – si vous ne voulez pas être reconnu cette fois-ci ou quand une autre personne utilise le même ordinateur que vous. C'est pour cette raison qu'existe la fonction : «Cliquez içi, si vous n'êtes pas Marie Gilbert.» Le cookie est donc effacé – jusqu'à ce que quelqu'un s'enregistre de nouveau.

Si cette fonction n'existe pas, on peut aussi effacer les cookies à la main dans le navigateur de même que limiter en partie ou totalement l'acceptation de ces derniers (Internet Explorer: menu **Outils > Options Internet > Confidentialité > Bouton Avancé**). Il faudra cependant renoncer aux agréments décrits.

Surfer avec différentes identités

Votre degré d'anonymat sur Internet dépend de la quantité d'informations personnelles que vous dévoilez sur différents sites Web. On appelle aussi un ensemble d'informations «**identité électronique**» F409 . Plus vous donnez de renseignements, moins l'image de votre personne peut être confondue. Il est judicieux de différencier la quantité d'information donnée.
Alors que vous devez obligatoirement donner dans un magasin des renseignements tels que p. ex. votre adresse, vous pouvez rester anonyme dans un chat. Il est toujours plus sûr de faire preuve de retenue. Les renseignements sensibles que vous donnez dans le magasin sont en règle générale protégés d'accès non autorisés.

Exemples de plusieurs identités d'une seule personne

- Magasin en ligne: Marie Gilbert, Av. Guison 1, Nyon, carte der crédit: 1243 …
- Livre des visiteurs: Marie G., marie.gilbert@bluewin.ch
- Chat public: Supermarie29

Faites obstacle aux espions

Les auteurs d'attaques «sournoises» peuvent être très variés.

● Pirates F310

Les pirates sont des programmeurs ayant pour hobby de s'introduire dans les systèmes informatiques étrangers. Ils ne s'intéressent guère à vos données (privées) mais pourraient se servir de votre PC pour attaquer d'autres ordinateurs, p.ex. dans les grandes sociétés.

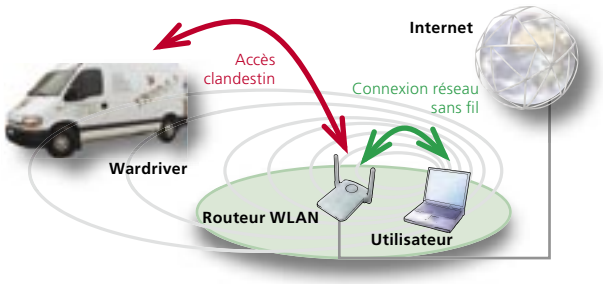
● Un espiogiciel F410

(angl. «spyware») est un logiciel qui s'installe à votre insu sur votre ordinateur. Il y collecte des informations et se sert de votre connexion Internet pour les retransmettre sans se faire remarquer.

Responsable	Effet
Adware	Enregistrent les sites Web visités et initialise les pop-ups publicitaires correspondants.
Keylogger	Enregistrent les saisies de touches (angl. «key» = touche), ce qui peut dérober des données sensibles, comme p. ex. des mots de passe.
Hijacker	Changent les paramètres du navigateur. La page de démarrage ou la liste des favoris sont le plus souvent touchés.
Chevaux de Troie	Introduisent des virus ou permettent la télécommande d'un PC et donc l'accès aux données en mémoire.

● Wardriving F411

angl. Wireless Access Revolution Driving) rappelle le contre-espionnage en temps de guerre consistant à rechercher tout trafic radio interdit avec des voitures munies d'antennes. Les wardrivers essaient par la même méthode de découvrir des réseaux radio non protégés et les trouvent en particulier dans les réseaux sans fil privés (WLAN).
Le wardriver intercepte alors le trafic de données entre les ordinateurs raccordés ou se sert de votre connexion Internet pour envoyer p. ex. des e-mails de spam.



Règles de comportement contre les espions

1. Installez ou activez un pare-feu (= mur de protection contre les indiscrets) et actualisez-le régulièrement (cf. p. 19 à 20).
2. Installez en cas de suspicion un logiciel de protection antispyware provenant d'un site digne de confiance (cf. p. 31).
3. Limitez l'accès à votre réseau sans fil (WLAN) et n'utilisez plus que des connexions radio chiffrées (cf. p. 36 à 37).

Aperçu des menaces

Dangers	Description	Dégâts
▲ **Virus**	Petits programmes ou morceaux de programme nuisibles qui s'attachent à des fichiers ou utilisent les programmes de votre PC pour se multiplier et faire des dégâts.	• Effacement / écrasement de données • Instabilité du système • Transmission de virus
▲ **Vers**	Ont des effets similaires à ceux des virus, mais peuvent se propager de manière autonome.	
▲ **Chevaux de Troie**	Petits programmes prétendant être utiles mais contenant des codes nuisibles.	
● **Spyware (espiogiciel)**	Logiciels installés à votre insu sur votre ordinateur. Ils collectent des informations sur votre PC et se servent de votre connexion Internet pour les envoyer sans se faire remarquer.	• Perte de la confidentialité des données • Abus des données • Abus du PC pour accéder à d'autres systèmes
● **Pirates**	Programmeurs qui infiltrent des systèmes informatiques étrangers.	• Vol de données (surtout chez les entreprises) • Abus des données • Abus du PC pour accéder à d'autres systèmes
● **Wardriving**	Recherche systématique de LAN sans fil à l'aide d'une voiture. Si elle aboutit, le wardriver a largement accès au réseau interne de l'exploitant du WLAN.	
Cookies	Petits fichiers texte créés uniquement pendant la navigation ou déposés sur le PC pendant une période prolongée.	• Les co-utilisateurs de votre PC peuvent obtenir des informations sur votre comportement navigationnel
● **Dialer**	Programmes de numérotation offrant la possibilité de se procurer des contenus payants via Internet et de les imputer à la facture téléphonique. Peuvent être utilisés à mauvais escient en vue d'activités frauduleuses.	• Dégâts financiers dus à des redevances téléphoniques astronomiques (si l'accès à Internet se fait de manière analogique ou par ISDN)
● **Non-livraison**	Non livraison de commandes d'achats Internet effectués auprès de fournisseurs peu sérieux.	• Dégâts financiers
● **Escroquerie à la carte de crédit**	Une liaison Internet non sécurisée peut être connectée pour obtenir des informations sur les cartes de crédit.	
● **Phishing**	Phishing, c.-à-d. escroquerie par e-mail : prétendument vrai message de sociétés à qui vous devez communiquer vos mots de passe, p. ex. pour votre online banking.	
■ **Canulars**	Faux messages, p. ex. fausses mises en garde contre des dangers tels que des virus	• Origine du spam • Endommagement év. du système
■ **IP-Popup**	Messages affichés sur votre écran sous forme de mises en garde.	• Incertitude car les messages sont camouflés sous forme de mises en garde
■ **Spam**	E-mails publicitaires indésirables	• Compte e-mail trop plein • Danger de fichiers attachés infectés • Risque de fausses promesses de gain

Dangers malgré un nouveau PC

Si vous avez un nouveau PC ou installez un nouveau système d'exploitation, tout a certes l'air neuf, mais n'est déjà bien souvent plus actuel car le CD contenant le logiciel date peut-être déjà de quelques mois – synonymes, dans de nombreux cas, d'une petite éternité.

Failles de sécurité dans le logiciel standard
Microsoft Windows et tous les autres produits Microsoft sont particulièrement souvent la cible d'attaques virales ou de pirates, mais les systèmes Apple sont eux aussi de plus en plus souvent attaqués. Les fabricants se livrent en permanence à une course avec les programmeurs de virus pour voir qui sera le premier à trouver les failles dans les systèmes et avec quelle rapidité elles pourront être comblées.

Si vous installez un nouveau PC, la première chose à faire est de prendre quelques précautions de sécurité.

Protection de l'administrateur
Si vous utilisez Windows XP, Windows 2000 ou Windows NT, vous pouvez protéger les comptes utilisateurs par un mot de passe. Il est surtout important de protéger le compte administrateur – le «mode de gestion» de votre PC qui a davantage de droits que l'utilisateur «normal». C'est ce qui rend les droits de l'administrateur particulièrement attrayants aux intrus qui s'aventurent sur votre PC.

Même si vous êtes le seul à utiliser votre PC, vous ne devez pas toujours vous logger comme administrateur mais vous servir, pour l'usage de tous les jours, d'un compte utilisateur assorti de droits restreints. Vous trouverez les étapes à suivre à :
F701 www.microsoft.com/switzerland/fr/security/windows

Pour créer un mot de passe pour le compte administrateur dans Windows XP Home, sélectionnez **Démarrer > Panneau de configuration > Comptes utilisateurs**. Dans Windows XP Professional, vous vous loggez avec le nom d'utilisateur «Administrateur» et confirmez avec «Enter» (si vous n'avez pas choisi de mot de passe lors de la création initiale du compte, la case reste vide). Maintenez enfoncées les touches **Ctrl** et **Alt** et appuyez sur **Suppr**. Cliquez sur «Changer de mot de passe» et saisissez votre nouveau mot de passe dans le masque (pour choisir de bons mots de passe, cf. p. 27, Règles de sécurité concernant les mots de passe).

Règles de comportement lors de la mise en service d'un nouveau PC

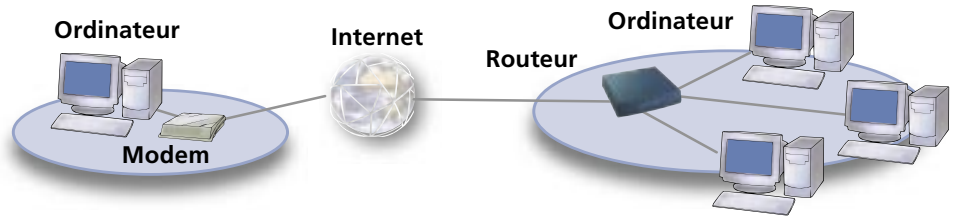
1. Installez un pare-feu avant de connecter le nouvel ordinateur à Internet pour la première fois (cf. p. 19 à 21.).
2. Actualisez ensuite sans attendre votre nouveau système d'exploitation (cf. p. 24).
3. Installez un logiciel antivirus (cf. p. 19 à 21).
4. Sécurisez votre compte administrateur par un «bon» mot de passe (cf. p. 26).

Dangers au niveau de l'accès à Internet

Si vous achetez en même temps que votre nouveau PC une connexion à Internet, il vous faut tenir compte des points suivants pour le choix de votre prestataire Internet.

1. Type de connexion
Plusieurs facteurs jouent un rôle dans le choix du prestataire (p. ex. Bluewin) et du type de connexion (analogique, ISDN ou ADSL). Un accès à large bande rapide augmente non seulement le confort mais protège aussi des dialers car l'utilisation n'est plus facturée par minute. Mais le risque d'une attaque directe, p. ex. par un ver, augmente parce que vous pouvez être en ligne en permanence.

2. Achat du matériel informatique
Pour un accès à large bande, vous avez besoin d'un modem ADSL (si vous n'avez qu'un PC) ou d'un routeur ADSL (si vous voulez accéder à Internet avec plusieurs PC ; angl. router = nœud de transmission, un type de «triage de données»). La fonction du modem ADSL est déjà intégrée dans un routeur ADSL.



Il existe des appareils avec pare-feu intégré. De tels «pare-feu matériels» protègent en règle générale mieux qu'un pare-feu logiciel – mais les différences sont mineures ; l'essentiel est de disposer d'une protection.
Astuce : changez le mot de passe (standard) sans attendre, dès l'installation du pare-feu, pour qu'il ne puisse pas être manipulé par des intrus.

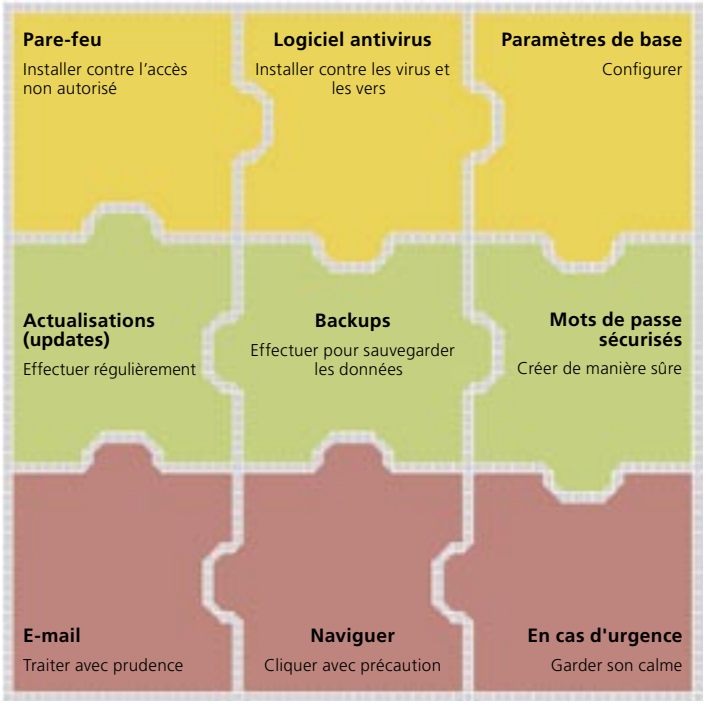
3. Services complémentaires
Certains prestataires Internet proposent des services permettant d'accroître la sécurité de votre PC sans grandes dépenses. Bluewin offre p. ex une protection antispam et antivirus gratuite et un pare-feu qu'il vous suffit d'activer. L'avantage de ces services est que vous ne devez installer sur votre ordinateur ni logiciel ni mises à jour ultérieures et que vous pouvez vous fier à l'appréciation du prestataire quant à la sélection de ce qui est dangereux.

F702 fr.bluewin.ch/services/sicherheit

Les 3x3 règles de la sécurité chez soi

Vous pouvez, en suivant quelques règles de comportement et en prenant quelques mesures techniques, protéger efficacement votre ordinateur et votre sphère privée. Vous ne devez pas être expert en informatique pour exécuter avec succès ces mesures de protection indispensables.

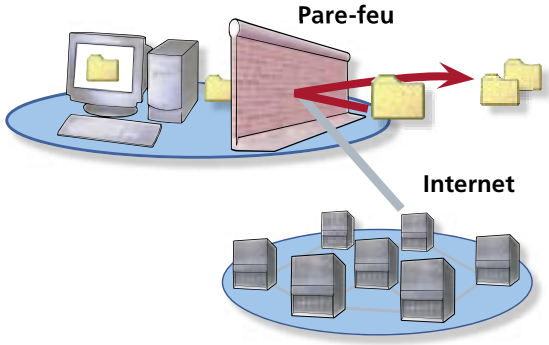
Se protéger complètement grâce aux 3x3 règles de comportement
Nous présentons aux pages suivantes les éléments vous permettant de protéger efficacement votre ordinateur et votre sphère privée. Chaque pièce du puzzle accroît votre sécurité.



Vous trouverez à la fin du fascicule une liste de contrôle qui peut vous aider à protéger votre PC (cf. p. 38).

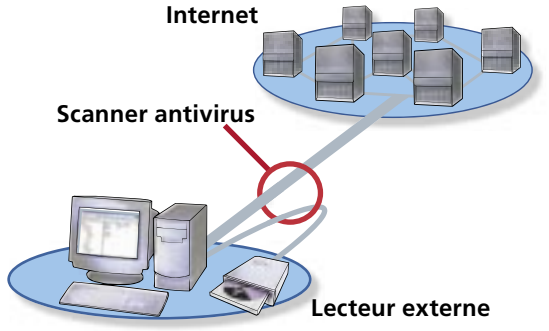
Pare-feu et logiciels antivirus

Que fait un pare-feu ?
Un pare-feu F119 (angl. firewall) est une sorte de garde-barrière qui contrôle individuellement toutes les données qui vont et viennent entre Internet et votre PC. Il protège ce dernier d'un abus par des intrus. Les pare-feu peuvent être intégrés dans les appareils (pare-feu matériels) ou tourner sous forme de programmes sur votre PC (pare-feu logiciels).



Que fait un logiciel antivirus ?
Un logiciel antivirus est un programme qui reconnaît, détecte et détruit les «intrus» tels que les virus et les vers. Un logiciel antivirus comprend les éléments suivants :

- une **bibliothèque de virus** renfermant les caractéristiques de milliers de virus reconnus par le logiciel anivirus,
- un **scanner antivirus**, le programme principal qui recherche à intervalles réguliers les virus, vers et chevaux de Troie sur votre PC et les retire éventuellement et
- un **bouclier** activé en permanence qui surveille toutes les données qui arrivent sur le PC par la connexion Internet (ou par le biais de disquettes ou de cédéroms) pour vérifier qu'elles ne renferment pas de virus, vers ou chevaux de Troie.



Pare-feu et logiciel antivirus – pourquoi vous devez les avoir tous les deux
La tâche principale du pare-feu est de contrôler qui peut envoyer des données sur Internet et en recevoir d'Internet. Par exemple, votre programme e-mail peut envoyer et recevoir des messages – un programme spyware se retrouvant sur votre PC n'est pas autorisé à le faire. Vous voulez recevoir des paquets de données d'un serveur Web à qui Internet Explorer a demandé des contenus, mais bien évidemment pas des données envoyées à votre PC par un pirate via un serveur inconnu.
En règle générale, le pare-feu accorde cette autorisation à un programme – votre logiciel e-mail est sur la liste «blanche». Mais le pare-feu ne connaît pas le type des données qu'il laisse passer, il ne sait pas si elles renferment malgré tout des virus, des vers ou des chevaux de Troie. Il laisse cette responsabilité au logiciel antivirus.

Installation de logiciels de protection

Les nouveaux ordinateurs sont souvent livrés avec des versions d'essai de pare-feu et de logiciels antivirus. Un pare-feu que vous devez d'abord activer est déjà inclus dans Windows XP. Vous pouvez acheter dans le commerce ou télécharger gratuitement (souvent avec une limite dans le temps) sur Internet des pare-feu et des logiciels antivirus. Notez les points suivants si vous optez pour un téléchargement :

- des chevaux de Troie qui installent des virus ou des espiogiciels peuvent aussi se cacher derrière des programmes de protection prétendument gratuits.
- le téléchargement dure longtemps si vous vous connectez à Internet par le biais d'une liaison téléphonique «normale» (analogique) ou par ISDN. Dans ce cas, il vous faudra vous procurer les logiciels de grande taille sur CD.

Le **pare-feu de Bluewin** tourne non pas chez vous mais «à l'extrémité Bluewin» de la liaison ADSL, un peu comme la Combox de votre portable qui n'est pas non plus un appareil mais un service. Vous n'avez ni besoin de l'installer ni de l'actualiser, il vous suffit de vous y abonner.

Vérifiez avant d'installer un logiciel antivirus qu'il n'y en a pas déjà sur votre PC. Il vous **faut obligatoirement le retirer** avant d'installer un nouveau programme de protection, sinon il peut y avoir des conflits. (Suppression avec **Démarrer > Panneau de configuration > Ajout/Suppression de programmes** ; recherchez-y une entrée avec «antivirus», p. ex. de McAfee, Norton ou Symantec (tous sont des fabricants connus de logiciels de protection). Cliquez sur **Ajouter/Supprimer** pour effacer les entrées inutilisées.

Antivir est un logiciel antivirus éprouvé que peuvent utiliser gratuitement les utilisateurs privés. Disponible en allemand et en anglais.
Demandez-vous avant de télécharger des programmes de protection individuels s'il ne serait pas plus judicieux d'acheter tout de suite une solution complète vous donnant p. ex. droit à une aide téléphonique.

F703 **www.free-av.de**

F704 **free.grisoft.com/freeweb.php/doc/2** – «AVG Anti-Virus» est un logiciel antivirus gratuit de langue anglaise caractérisé par des fichiers d'actualisation particulièrement petits. Il vous conviendra donc spécialement si vous vous connectez à Internet par téléphone (analogique, ISDN).

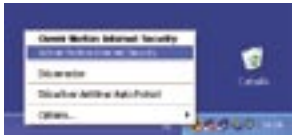
Solution complète de Norton

Les paquets logiciels combinés en valent la peine dès le moment où vous en achèteriez de toute façon deux composants. Norton Internet Security est une solution de sécurité combinée de ce type qui renferme la protection antivirus, le pare-feu, le filtre antispam, une protection pour les données confidentielles (Privacy Control) et un logiciel de protection des enfants (Parental Control).

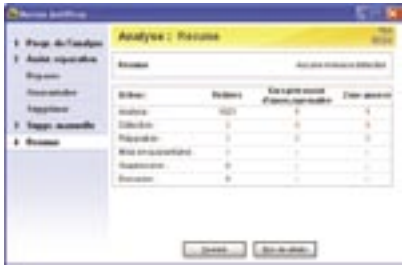
Version d'essai de 30 jours
Vous avez à votre disposition une version d'essai gratuite de ce paquet logiciel à télécharger. Vous pouvez décider après 30 jours si vous voulez l'acheter ou le désinstaller.
F705 **www.schoolnet.ch/norton**

Installation de la version d'essai
N'oubliez pas de retirer au préalable d'autres logiciels antivirus éventuellement sur votre PC. Loggez-vous en outre comme administrateur. Téléchargez le fichier et lancez l'installation. Suivez pour ce faire les recommandations données dans les fenêtres d'installation. Tous les paquets de sécurité sont installés en même temps.

Contrôle de l'activité
En bas à droite, à côté de l'heure, dans le «system tray» (littér. «plateau système») un symbole vous informe de l'état de Norton (= activé; = désactivé). Vérifiez périodiquement si le logiciel est bien activé. Si ce n'est pas le cas, cliquez sur le symbole avec la touche droite de la souris et sélectionnez **Activer Norton Internet Security**.



Mise en garde en cas de menace
Le programme affiche dans la même zone un message si la sécurité de votre PC est compromise. Des messages du programme vous informent généralement qu'un problème de sécurité s'est présenté mais qu'il est déjà maîtrisé. Vous pouvez en lire davantage sur le comportement à adopter en cas d'attaque à partir de la page 30.



La question du paramétrage sûr

Tous les programmes prenant part au trafic de données avec Internet peuvent être paramétrés de manière à être moins sensibles aux attaques :

- système d'exploitation (= «unité de gestion» de l'ordinateur)
- navigateur (= programme de visualisation Internet, p. ex. Internet Explorer)
- programme e-mail (p. ex. Outlook, Outlook Express, Eudora, Thunderbird)
- programmes d'application comme Word et Excel

Tout comme dans le monde réel, il faut souvent s'accommoder d'une perte de confort au profit de la sécurité et vice-versa. La modification de ces paramètres représente en outre un réglage de sécurité fin – il ne doit en aucun cas remplacer l'installation d'un pare-feu et d'un logiciel antivirus ni les mises à jours (= actualisations) régulières du système d'exploitation.

1. **Débusquez les virus cachés**
   Comme nous l'avons déjà mentionné à la p. 6, les programmes infectés se camouflent en fichiers inoffensifs caractérisés par une fausse extension double («Picture.jpg.exe»). Vous pouvez, à **Poste de travail > Outils > Options des dossiers > Affichage**, désactiver l'option dangereuse «**Masquer les extensions des fichiers dont le type est connu**».

2. **Adaptez les niveaux de sécurité d'Internet Explorer**
   Vous pouvez modifier les paramètres de sécurité du programme dans le menu **Outils > Options Internet**. Cliquez pour ce faire sur l'onglet **Sécurité**, **Personnaliser le niveau** et choisissez le niveau désiré. Vous modifiez le niveau de sécurité en cliquant sur **OK**. Le niveau maximum («élevé») rend cependant la navigation pénible car des pages entières ne sont plus affichées même si elles ne sont pas du tout «peu sûres». Tout permettre (niveaux «bas»/«très bas») vous rend par contre vulnérable. Vous pouvez aussi sélectionner ici des paramètres individuels de manière ciblée.

Vous trouverez d'autres paramètres de sécurité pour les programmes les plus courants à **F706** **www.microsoft.com/switzerland/fr/security/settings**

3. **Contrôlez l'enregistrement des mots de passe dans Internet Explorer**
   L'enregistrement de mots de passe, p. ex. pour le Webmail ou les comptes clients, dans Internet Explorer est certes pratique, mais annule l'effet sécurisant. C'est à vous de décider si vous souhaitez l'autoriser. Vous pouvez désactiver l'option à **Outils > Options Internet > Contenu > Saisie semi-automatique**.

4. **Désactivez l'affichage des messages.**
   Loggez-vous sur votre PC en qualité d'«Administrateur». Cliquez ensuite (dans Windows XP) sur le menu **Démarrer > Panneau de configuration > Outils d'administration > Services.** Dans Windows 2000 cliquez au menu **Démarrer > Paramètres > Panneau de configuration > Outils d'administration > Services**. Cliquez alors avec la touche de droite de la souris sur **Affichage des messages** et choisissez **Arrêter** dans le menu Contexte. Cliquez une nouvelle fois sur **Affichage des messages** avec la touche de droite de la souris et choisissez **Propriétés**. Cliquez sur l'onglet **Général** et cochez **Désactivé** pour le «Type de démarrage».

5. **Sécurisez votre programme d'e-mail.**
   Certains types de virus s'activent déjà à l'affichage dans le volet de visualisation d'Outlook Express lorsque vous sélectionnez le courrier en question dans la boîte aux lettres. L'idéal est donc de désactiver la visualisation automatique. Choisissez pour ce faire le menu **Affichage > Disposition** et désactivez la case «Afficher le volet de visualisation». Confirmez la modification avec **Appliquer** et ensuite **OK**.
   Depuis la version 6 d'Outlook Express, vous pouvez en outre empêcher le programme d'ouvrir des fichiers attachés potentiellement dangereux en activant dans le menu **Outils > Options**, sur l'ongle **Sécurité**, l'option «Ne pas autoriser l'ouverture ou l'enregistrement des pièces jointes susceptibles de contenir un virus».

Actualisations (updates)

Comme de nouvelles variantes de virus et de vers ne cessent d'apparaître, le pare-feu, la protection antivirus et le système d'exploitation doivent être actualisés en permanence, c'est-à-dire qu'il faut procéder à des «updates» (angl. update = actualisation). Voici quelques valeurs de référence pour les intervalles :

Logiciel antivirus	Au moins une fois par semaine, si vous utilisez moins souvent votre ordinateur, nous recommandons de le faire à chaque démarrage, avant toute autre chose.
Système d'exploitation	Actualisation au moins une fois par mois, idéalement plus souvent, en fonction de la disponibilité de nouvelles mises à jour.
Pare-feu	Actualisation au moins tous les trois mois.

Le chargement et l'installation ne durent que quelques minutes et peuvent tourner en arrière-fond pendant que vous continuez à travailler.
Astuce : servez-vous des services de rappel : La plupart des programmes ont des fonctions qui vous préviennent automatiquement dès qu'une nouvelle mise à jour est disponible.

Conseil : les mises à jour ne sont jamais envoyées par e-mail. Si vous recevez un tel message, effacez-le car il s'agit probablement d'un virus.

Il y a pour les systèmes d'exploitation Windows 2000, ME ou XP des «mises à jour automatiques» qui actualisent aussi des composants importants comme Internet Explorer et le pare-feu XP. Vous avez le choix, en fonction de la version de Windows, entre différents niveaux d'automatisation. Le niveau que vous choisissez n'a pas d'importance du moment que vous l'actualisez. Vous trouverez des instructions à **F707 www.microsoft.com/switzerland/fr/windowsupdates**

Pour MAC OS, vous pouvez faire les mises à jour au menu **Pomme > A propos de ce Mac > Mise à jour de logiciel**.

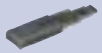
Actualisation du logiciel de protection
Norton contient une fonction d'actualisation automatique qui vous aide à maintenir l'actualité des composants. Cliquez sur le symbole du logiciel et vérifiez à **Options** si la case «Activer LiveUpdate automatique» est cochée. Dans la négative, activez l'option correspondante.

Copies de sauvegarde (backup)

Quelles que soient les autres mesures de sécurité que vous preniez, nous vous recommandons de créer régulièrement des copies de sauvegarde de vos données les plus importantes. Vous pouvez ainsi limiter les dégâts si votre ordinateur est infecté. Il vous faudra différents supports en fonction de la quantité de données que vous sauvegardez.

Pour évaluer la taille des classeurs de données que vous souhaitez sauvegarder en mégaoctets, cliquez avec la touche de droite de la souris sur un classeur, puis sur **Propriétés**.

Additionnez les mégaoctets et choisissez le support adéquat. Les supports de données suivants conviennent à la sauvegarde de données d'utilisateurs privés :

Supports de données	Quantité de données	Description	Coûts
Sticks mémoire USB ou cartes mémoire 	128 à env. 512 MB (p. ex. pour grands exposés, photos)	• peuvent être enfichés et utilisés comme un lecteur • écrivables aussi souvent qu'on le souhaite • plutôt pour le transport et la sauvegarde à court terme	• grandes différences de prix en fonction de la capacité • 256 MB à partir de CHF 75.– env.
CD, DVD 	• CD : 700 MB (souvent suffisant pour les utilisateurs privés) • DVD : env. 4 à 5 GB	• enregistrement avec graveurs de CD/DVD • le graveur peut aussi s'utiliser pour les CD musicaux • les CD-R ne peuvent être gravés qu'une seule fois, les CD-RW plusieurs fois.	• les graveurs de CD/DVD sont intégrés aux nouveaux PC, sinon, disponibles à partir de CHF 150 • CHF 0.50–1.00 par CD vierge • CHF 1.00–5.00 par DVD vierge
Disque dur externe 	à partir de 20 GB (beaucoup d'espace pour de la musique, des films, des photos numériques)	• taille pratique • certains ont plus de mémoire que le disque dur du PC • peut aussi être raccordé au besoin à d'autres ordinateurs	• à partir de CHF 200.–

Il existe, pour des répertoires complets et de grandes quantités de fichiers …

- **des programmes backup** qui vous aident à sauvegarder les données, p. ex. «Cobian» : **F708 www.pcastuces.com/logitheque/cobian.htm** ou
- **des programmes image** , qui vous aident à créer une copie complète du disque dur, p. ex. «Norton Ghost» : **F709 www.symantec.com/region/fr/product/ng_index.html**

Faille de sécurité au niveau du mot de passe

Le nom d'utilisateur et le mot de passe nous accompagnent dans toutes nos emplettes, dans nos comptes e-mail et dans bien d'autres services sur le Web. Voici quelques tuyaux pour vous aider à rendre difficile l'accès de vos données ou de vos mots de passe aux personnes non autorisées :

Bon	Mauvais
Mot de passe simple : il faut que vous puissiez vous souvenir facilement de votre mot de passe – il doit en même temps être difficile à deviner par les autres. Exemple : la chanson enfantine «Mon chapeau a 3 corne» sous forme de mot de passe : **Mca3c**	**Pas dans le dictionnaire :** n'utilisez pas de mots qui se trouvent dans le dictionnaire. Le mieux est d'inverser plusieurs lettres (p. ex. cèractares, iretiondicna).
Combinez lettres et chiffres : p. ex. **t0b1as** (au lieu de Tobias).	**Rien d'évident :** n'utilisez en aucun cas le nom de votre partenaire, animal domestique ou domicile sans l'altérer.
Différents comptes, différents mots de passe : si un agresseur découvre p. ex. le mot de passe pour votre compte e-mail, il ne faut pas qu'il découvre en même temps le mot de passe pour votre compte eBay.	**Pas de Post-it sur le moniteur :** si vous voulez noter vos mots de passe, surtout ne les conservez pas directement sur le moniteur ou dans le tiroir du dessus.
Changez vos mots de passe : il est souvent recommandé d'en changer tous les mois. A vous de décider si c'est réaliste pour vous. Il vaut mieux changer de temps en temps que jamais.	**Garder le mot de passe secret :** ne donnez pas vos mots de passe à des tiers, même s'ils vous les demandent. Aucun prestataire sérieux ne vous demandera jamais votre mot de passe par e-mail ou au téléphone.
Prudence avec les caractères spéciaux : ces derniers ne sont pas sur les mêmes touches dans tous les pays. Si vous ne trouvez pas le caractère # dans un cybercafé à l'autre bout du monde, vous êtes dans le pétrin.	**Pas de répétitions, pas de combinaisons logiques de caractères :** comme p. ex. **lalala**, **abcdefg** ou **azerty** (ordre sur le clavier)
Utilisez des variantes de votre mot de passe principal : Si vous devez gérer plusieurs comptes, utilisez des variantes de votre mot de passe : p. ex. mat0b1as (mail), bat0b1as (banking), sht0b1as (shopping). Le système ne doit toutefois pas être identifiable au premier coup d'oeil.	**Ne pas sauvegarder sur votre ordinateur :** par exemple dans un document intitulé «mots_de_passe.doc».

Règles pour le mail

Dans les questions de sécurité, rien ne remplace le bon sens – c'est pourquoi nous redonnons ici un aperçu de tous les conseils de comportement. Vous évitez ainsi aussi les attaquants et casse-pieds qui passent outre les précautions techniques.

1. N'ouvrez pas les fichiers attachés envoyés par des inconnus, en particulier si ces fichiers ont des extensions comme .exe, .vbs ou .bat ou des extensions doubles (p. ex. .doc.exe).

2. Aucun fournisseur de logiciels, en particulier Microsoft ou Apple, n'envoie d'actualisations par e-mail. Il s'agit de contrefaçons aux contenus dangereux.

3. Un fournisseur sérieux ne vous invitera jamais à vous logger sur-le-champ sur un site avec une adresse bizarre ou à faire connaître par e-mail des mots de passe ou des informations concernant votre compte.

4. Réagissez de manière critique aux mises en garde contre des virus envoyées par mail, même par des personnes que vous connaissez.

   a. N'effacez pas prématurément des fichiers si c'est recommandé dans la mise en garde.

   b. Essayez de voir si le message est déjà connu comme canular : chez le fabricant du logiciel ou p. ex. à F710 **www.hoaxbuster.com**).

   c. Ne transmettez pas le mail aux personnes que vous connaissez, en particulier si vous y êtes invité.

   d. Informez l'expéditeur de fausses mises en garde dans la mesure où vous le ou la connaissez en personne.

5. Utilisez plusieurs adresses e-mail dont une comme adresse «personnelle». Ne la communiquez qu'à vos amis et connaissances.

6. Créez au moins un autre adresse, p. ex. pour vous abonner à des newsletters, pour vous enregistrer ou contribuer à des forums publics. Si vous y recevez trop de spam, changez d'adresse.

7. Evitez les répertoires d'adresses. Des services e-mail gratuits offrent en cas d'abonnement l'inscription dans des «annuaires téléphoniques» ; il est facile de venir y «chercher» des adresses.

8. N'ouvrez pas, si possible, les mails contenant du spam car ils peuvent informer l'expéditeur de la réussite de la transmission.

9. Ne répondez pas au spam et n'utilisez pas d'éventuelles fonctions de désabonnement («unsubscribe») dans le texte. En ce faisant, vous ne faites que confirmer que votre adresse e-mail est utilisée.

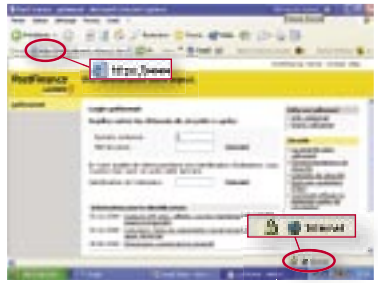
10. Si vous voulez être tout à fait sûr, servez-vous de méthodes de codage pour vos mails (ce point s'adresse aux utilisateurs avancés).

Règles de navigation

1. Actualisez régulièrement Internet Explorer. L'actualisation du système d'exploitation («Windows Update», cf. p. 25) permet aussi de supprimer des failles de sécurité dans Internet Explorer qui pourraient faute de quoi être exploitées par des vers p. ex. C'est particulièrement important si vous – p. ex. après les vacances – n'avez pas utilisé votre ordinateur pendant longtemps.

2. Evitez les sites Web «peu sérieux». Sont p. ex. gages du sérieux d'un site

- un impressum facile à trouver avec adresse postale et numéro de téléphone de l'offreur.
- une indication claire des coûts éventuels (p. ex. pour informations/articles, pour logiciels, pour envoi), des conditions de livraison et de paiement.
- la transmission des informations sensibles par l'intermédiaire d'un codage SSL (identifiable par http**s** dans la ligne d'adresse et au symbole de cadenas dans la barre d'état de la fenêtre du navigateur).



Si vous atterrissez sur un site Web suspect, fermez sur-le-champ la fenêtre. Utilisez la croix en haut à droite de la fenêtre ou la combinaison de touches **Alt-F4**, ne vous servez en aucun cas des boutons à l'intérieur du site Web douteux (qui font éventuellement autre chose que ce qu'ils prétendent).

3. Soyez méfiant vis-à-vis des téléchargements qui vous sont «imposés» par un site Web. N'appuyez pas sur **OK** ni sur **Interrompre** dans une fenêtre Web (cliquer sur Interrompre peut avoir pour conséquence l'installation), mais fermez la fenêtre.

4. Qui a, en plus de vous, accès à votre PC : ne laissez p. ex. pas de mots de passe, même masqués par **** sur votre poste de travail ou dans un cybercafé. Evitez d'utiliser des magasins en ligne avec des cookies permanents sur des PC publics (c'est-à-dire des sites Web qui vous réservent p. ex. toujours un accueil personnalisé ou affichent automatiquement vos données client). Ceci s'applique en particulier à la combinaison de cookies avec des mots de passe sauvegardés.

5. En cas de commandes sur Internet, n'indiquez des données de compte et de paiement que par des voies de transmission codées.

Comportement à adopter en cas d'urgence

Quelquefois, un virus, cheval de Troie ou dialer «gagne» à court terme la course contre les experts en sécurité des sociétés logicielles et peut se nicher sur votre ordinateur malgré toutes les mesures de prévention. Les **symptômes** d'une attaque virale sont p. ex. que

- le PC tourne à une lenteur inhabituelle,
- des problèmes surgissent au démarrage,
- des messages incompréhensibles sont affichés sur l'écran,
- des données que vous êtes certain de ne pas avoir effacées disparaissent.

Ne paniquez en aucun cas.
Gardez votre calme. L'effacement précipité de fichiers prétendument dangereux ou même l'effacement de toutes les données sur le disque dur risquent de causer des dégâts importants. Une perte complète des données est très rare. Comme les virus et les vers sont des logiciels, ils peuvent certes paralyser temporairement votre ordinateur mais ne peuvent pas l'endommager physiquement de manière permanente.

Retrait en cas de symptômes :

1. Sauvegardez les fichiers ouverts et les données importantes sur disquette ou cédérom (il vaut mieux des données infectées que l'on peut «nettoyer» plus tard que pas de données du tout).
2. Informez-vous des virus actuels et des possibilités de remédier aux dégâts. Servez-vous à cet effet du site Web du fabricant de votre logiciel antivirus ou de portails d'information spécialisés (cf. p. 32).
3. Actualisez votre logiciel antivirus. Normalement une mise à jour correspondante du logiciel de protection est disponible quelques heures après l'apparition de nouveaux virus.
4. Lancez ensuite votre logiciel antivirus. Ne vous effrayez pas s'il annonce la présence d'un virus – il est très probable qu'un intrus identifié puisse être effacé sur-le-champ ou mis en quarantaine.

Après avoir remporté la lutte :

1. Vérifiez tous les fichiers que vous avez sauvegardés ces derniers temps sur des disquettes ou des cédéroms pour empêcher une «propagation» du virus.
2. Informez les connaissances à qui vous avez envoyé des fichiers récemment.

En cas d'échec :
En fonction de l'urgence, vous pouvez …

- faire appel à un spécialiste
- mettre en oeuvre un logiciel anti-spyware (cf. page suivante),
- attendre qu'il y ait une mise à jour correspondante (maxi. 2 jours).

Attaque par spyware ou chevaux de Troie
Un spyware est en général bien dissimulé sur votre PC. Il arrive la plupart du temps sur ce dernier sous forme de fichier invisible attaché à des produits gratuits. Des **symptômes** sont:

- détérioration de la performance du système (c'est-à-dire temps d'attente plus longs que d'habitude)
- fenêtres Web de publicité s'ouvrant souvent ou
- paramètres changés du navigateur (p. ex. autre page de démarrage).

Retrait :

1. Si le scanner antivirus trouve le cheval de Troie, il peut certainement aussi le retirer.
2. En cas d'échec, installez un programme anti-chevaux de Troie. Vous trouverez des informations à ce sujet à : **F711 www.commentcamarche.net.** Le logiciel de Spybot Search and Destroy vous aide en cas d'attaque de Spyware (à télécharger gratuitement sous **F712 spybot.safer-networking.de/fr)**.
3. En cas de nouvel échec, adressez-vous à un spécialiste.

Attaque par des dialers peu sérieux
S'il y a un dialer sur votre PC et que vous soupçonnez (sur base de votre facture de téléphone, que vous pouvez toujours consulter via la «facture réseau fixe en ligne») qu'il a déjà fait des dégâts financiers, «amassez des preuves» avant d'effacer le dialer. Vous avez ainsi quelque chose de concret en cas de contestation. En cas de dégâts occasionnés par des dialers : **F713 www.bakom.ch/fr/service/tc/0900**
Preuve de connexion en ligne : **F714 www.swisscom-fixnet.ch/factureonline**

Retirer des dialers visibles (le dialer a visiblement installé une nouvelle connexion)
Windows XP : choisissez dans le menu **Démarrer > Panneau de configuration > Connexions réseau**. (anciens systèmes : **Démarrer > Panneau de configuration > Connexions à distance**)

1. S'il y a à côté des entrées de votre prestataire Internet, p. ex. Bluewin ou autre, des entrées que vous ne connaissez pas, supprimez-les. (Touche de droite de la souris **> Supprimer**)
2. Vérifiez le numéro de votre fournisseur (touche de droite de la souris **> Propriétés**, onglet «Général»)
   Davantage à : **F715 www.microsoft.com/switzerland/fr/security/dialer**

Retirer des dialers camouflés (le dialer n'est pas identifiable sur-le-champ)
Certains dialers se «camouflent» vraiment. Les nouveaux logiciels antivirus renferment déjà des fonctions spéciales pour détecter et éliminer ces dialers.

1. Actualisez votre logiciel antivirus et servez-vous de la fonction correspondante.
2. En cas d'échec, installez un programme antidialer, p. ex. de
   F716 www.swisscom-fixnet.ch/fx/privatkunden/dienste/dialerschutz
3. Si l'emploi d'un programme antidialer est inefficace, faites appel à un spécialiste.

Liens d'entraide

Aussi nombreux les programmeurs de virus aimeraient-ils être – ils ne sont en fin de compte qu'une faible minorité. Il y a sur Internet de nombreuses adresses qui vous soutiennent. En voici une sélection :

Annonce-virus des entreprises
Les sites de Microsoft et Apple ainsi que les fabricants de logiciels de protection renferment toujours des informations actuelles sur les virus, p. ex.
F717 **fr.mcafee.com/virusinfo**

Presse spécialisée en ligne
Les sites Web de la presse informatique spécialisée renferment toutes les annonces de virus et sites spéciaux consacrés à la sécurité, p. ex.
F718 **fr.bluewin.ch/services/sicherheit/index.php/sicherheits-lage_fr**
F719 **www.secuser.com**

Hoaxbuster
Diverses plates-formes recueillent des messages d'utilisateurs concernant en particulier le spam et les canulars (faux messages de mise en garde contre des virus). Vous pouvez y consulter la liste mais aussi «dénoncer» de nouveaux malfaiteurs :
F710 **www.hoaxbuster.com**

L'union contre le spam : SpamNet
Les gens reconnaissent mieux le spam que les logiciels : si de nombreux utilisateurs du logiciel SpamNet marquent un mail entrant comme étant du spam, il est communiqué à une base de données centrale et cette dernière le bloque pour tous les autres utilisateurs. Version d'essai gratuite à : F720 **www.cloudmark.com/products/spamnet**.

Contrôles de sécurité en ligne
Testez gratuitement votre configuration en ligne si vous n'êtes pas sûr d'être bien protégé.

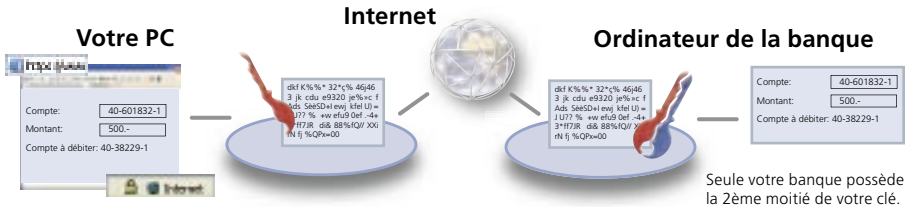
F721 **www.kaspersky.com/remoteviruschk.html**
F722 **www.symantec.com/region/fr/avcenter**

Le bon client – la société authentique

Quand il s'agit de faire des achats, ou plus précisément de payer, sur Internet, les expéditeurs et destinataires veulent être sûrs que l'autre personne est vraiment ce qu'elle prétend être.

Authentification simple
Dans la vie de tous les jours, on demanderait à voir la carte d'identité de son vis-à-vis ; sur Internet, cela se fait par le biais d'un contrôle d'identité électronique (= authentification). Le client crée avant son premier achat un compte utilisateur composé d'un nom d'utilisateur et d'un mot de passe sur le site Web du vendeur et s'identifie chaque fois au moyen de ces renseignements (= login).
Le nom d'utilisateur est unique et identifie donc l'utilisateur. Le mot de passe est une combinaison alphanumérique qui n'est connue que de lui seul. Le nom d'utilisateur est souvent lisible alors que le mot de passe est masqué sous forme de **** lors de la saisie.

Encryptage SSL pour garder le secret
Le secret des données de paiement est préservé grâce à l'«**encryptage SSL**» F217 (abréviation de «Secure Sockets Layer», un protocole de transmission développé par la société Netscape) de la connexion. SSL est la procédure d'encryptage standard des transmissions de données sur Internet qui deviennent alors illisibles pour des tiers. Les connexions SSL sont identifiables au symbole de cadenas dans la barre d'état du navigateur ainsi qu'au sigle https (s comme dans «secure», fr. sécurisé) dans la ligne d'adresse.

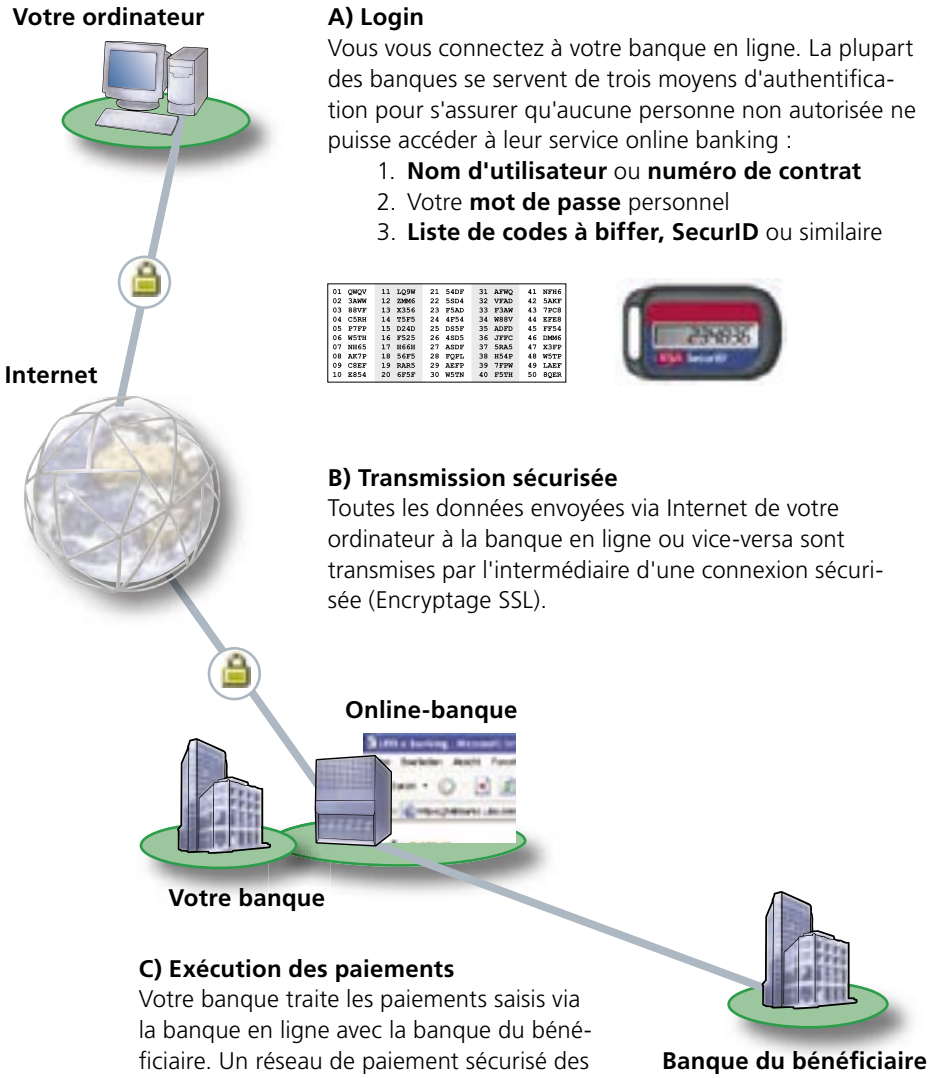


Certificats numériques
En cliquant deux fois sur le symbole du cadenas dans la barre d'état, vous pouvez visionner le certificat numérique de tous les sites Web encryptés. Il s'agit d'une attestation électronique de l'identité d'une organisation. En cas de doute, vous pouvez vérifier ainsi si vous saisissez vraiment vos données sur le bon site Web.

Conseil : si la fenêtre de votre navigateur n'affiche pas la ligne d'état, vous pouvez la faire apparaître à **Barre d'état** au menu **Affichage**.

Paiement sécurisé

Authentification triple dans l'online Banking
C'est dans l'online Banking que l'on trouve le summum des mesures de sécurité pour les paiements via Internet. Les clients peuvent ainsi accéder en toute sécurité, à tout moment et partout, à leur propre compte via Internet. Les mesures de sécurité des banques et de Postfinance renferment trois moyens d'authentification au lieu de deux :



A) Login
Vous vous connectez à votre banque en ligne. La plupart des banques se servent de trois moyens d'authentification pour s'assurer qu'aucune personne non autorisée ne puisse accéder à leur service online banking :

1. **Nom d'utilisateur** ou **numéro de contrat**
2. Votre **mot de passe** personnel
3. **Liste de codes à biffer, SecurID** ou similaire

01	QWQV	11	LQ9W	21	54DF	31	AFWQ	41	NFH6
02	3AWW	12	ZMM6	22	5SD4	32	VFAD	42	5AKF
03	88VF	13	X3S6	23	F5AD	33	F3AW	43	7PC8
04	C5RH	14	T5F5	24	4F54	34	W88V	44	EFE8
05	P7FP	15	D24D	25	D55F	35	ADFD	45	FF54
06	W5TH	16	F525	26	4SD5	36	JFFC	46	DMM6
07	NH65	17	H66H	27	ASDF	37	5RA5	47	X3FP
08	AK7P	18	56F5	28	FQPL	38	H54P	48	W5TP
09	C8EF	19	RAR5	29	AEFP	39	7FPW	49	LAEF
10	E854	20	6F5F	30	W5TN	40	F5TH	50	8QER

B) Transmission sécurisée
Toutes les données envoyées via Internet de votre ordinateur à la banque en ligne ou vice-versa sont transmises par l'intermédiaire d'une connexion sécurisée (Encryptage SSL).

C) Exécution des paiements
Votre banque traite les paiements saisis via la banque en ligne avec la banque du bénéficiaire. Un réseau de paiement sécurisé des banques est utilisé à cet effet.

Exemple de Direct Net

Quand vous vous abonnez au service Direct Net du Credit Suisse, vous recevez un numéro de contrat (correspondant au nom resp. à l'identification utilisateur) et un mot de passe initial généré automatiquement qu'il vous faut changer lors du premier login. (Notez les recommandations pour des mots de passe sûrs à la p. 26). Vous avez besoin, en guise de caractéristique de sécurité supplémentaire pour l'accès à votre compte, d'un autre «mot de passe» qui change à chaque connexion :

La **SecurID** est une carte à affichage qui génère toutes les minutes une série aléatoire de six chiffres. Quand vous vous connectez, la série de chiffres actuelle constitue votre seconde caractéristique de sécurité. Comme cette séquence chiffrée change en permanence, personne ne peut copier les chiffres pour les utiliser plus tard.

La **liste de numéros à biffer** est une liste de 100 codes alphanumériques. A chaque connexion, vous vous identifiez avec le code suivant. Les banques se servent de ces listes comme d'une troisième caractéristique de sécurité ; également dans la variante où l'on ne biffe plus mais où l'endroit est déjà donné.

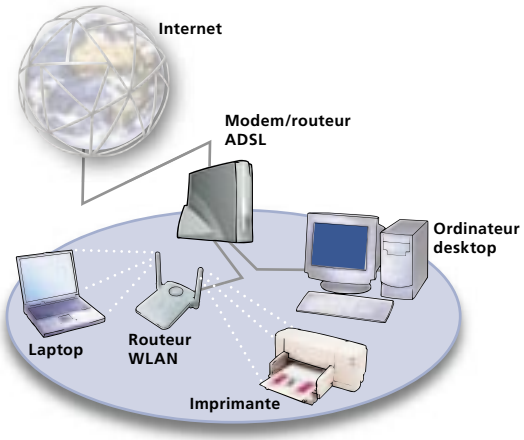
01	QWQV	11	LQ9W	21	54DF	31	AFWQ	41	NFH6
02	3AWW	12	ZMM6	22	5SD4	32	VFAD	42	5AKF
03	88VF	13	X3S6	23	F5AD	33	F3AW	43	7PC8
04	C5RH	14	T5F5	24	4F54	34	W88V	44	EFE8
05	P7FP	15	D24D	25	D55F	35	ADFD	45	FF54
06	W5TH	16	F525	26	4SD5	36	JFFC	46	DMM6
07	NH65	17	H66H	27	ASDF	37	5RA5	47	X3FP
08	AK7P	18	56F5	28	FQPL	38	H54P	48	W5TP
09	C8EF	19	RAR5	29	AEFP	39	7FPW	49	LAEF
10	E854	20	6F5F	30	W5TN	40	F5TH	50	8QER

Vous pouvez contribuer au fonctionnement optimal des précautions de sécurité :

- Utilisez toujours pour vous connecter l'adresse officielle de votre banque, ici **www.credit-suisse.com** ou **www.directnet.com/fr**.
- N'ouvrez pas d'autres pages Internet tant que vous utilisez le online banking.
- Lisez attentivement les conseils de sécurité affichés sur votre écran tels qu'informations concernant votre dernier usage de l'online banking.
- Veillez à vous déconnecter après chaque session (bouton : **Sortie**).
- Videz les fichiers Internet temporaires de votre navigateur après la session (**Outils > Options Internet > Général > Supprimer les fichiers**).
- Utilisez toujours la version de navigateur actuelle et recommandée par votre banque.

Vous trouverez des conseils plus complets sur la sécurité de Direct Net et des renseignements détaillés sur le certificat à **F723 www.directnet.com/fr/media/pdf/dn_fr_sicherheit_10_04.pdf.** Toutes les banques et Postfinance ont maintenant, sur leurs sites respectifs, des pages d'information de ce type relatives à la sécurité de leur online banking.

Sécuriser les réseaux sans fil



Si vous avez installé chez vous un WLAN (abréviation de l'angl. Wireless Local Area Network = réseau sans fil), il vous faut le protéger tout spécialement. Si le réseau n'est pas protégé, n'importe qui se trouvant dans son rayon d'action peut y accéder.

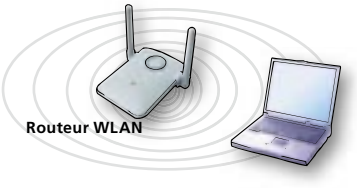
Nous montrons les réglages nécessaires à l'exemple du routeur WLAN (angl. router = noeud de transmission) de Netopia exploité par Bluewin. Si vous utilisez un autre appareil, réalisez les étapes de manière analogue en vous aidant du mode d'emploi.

Etape 1 : changer de mot de passe
Les intrus connaissent les mots de passe réglés côté usine des routeurs et pourraient accéder de cette manière à votre appareil. Créez donc votre propre mot de passe sûr (cf. p. 26, «Faille de sécurité Mot de passe»).

1. Tapez **http://192.168.1.1** dans le champ d'adresse de votre programme Internet pour accéder aux réglages du routeur Netopia. (Remarque : cette adresse d'accès fonctionne pour beaucoup de routeurs courants)
2. Inscrivez-vous avec le nom d'utilisateur (p .ex. «Admin») et le mot de passe indiqué côté usine. Vous les trouverez dans le mode d'emploi.
3. Changez ce mot de passe au menu **Mode expert > Configurer > Mot de passe routeur**.

Conseil : les appareils disposent en règle générale d'une fonction de télémaintenance donnant aux techniciens de service accès à votre routeur via Internet. Les agresseurs peuvent également s'en servir. Sur les routeurs Netopia, cette fonction (angl. «Remote Management») est déjà désactivée de manière standard pour des raisons de sécurité de sorte que vous devez d'abord l'activer si quelqu'un doit vous aider via la télémaintenance.

Etape 2 : «isoler» le réseau
Quiconque souhaite pénétrer dans un réseau sans fil doit connaître son «nom», la «SSID» (Service Set ID, quelquefois aussi «ESSID» pour «Extended...»). Empêchez donc que votre routeur communique son SSID à tous les appareils sans fil dans son rayon d'action.



Sur le routeur Netopia, ce réglage se trouve à **Mode expert > Configurer > Sans fil > Etendu**. Activez-y l'option «Permettre le mode système fermé».

Etape 3 : coder le trafic radio

1. Réglez à **Mode expert > Configurer > Wireless > Etendu** le codage «codage WEP» sur «Activé – automatique».
2. Inventez une phrase avec au moins 26 caractères (p. ex. «Un chasseur sachant chasser sans son chien est un bon chasseur»). Le système utilise alors cette phrase pour coder les données.
3. Réglez la taille du code à 128 bits (un codage encore plus élevé ralentirait votre PC).
4. Sauvegardez vos changements.

Important : procédez aux réglages analogues suivants sur tous les ordinateurs utilisant le réseau sans fil :

1. Présentez-vous comme l'administrateur aux ordinateurs et cliquez sur **Démarrer > Liaisons réseau**. Cliquez avec le bouton droit de la souris sur **Liaison réseau sans fil** puis sélectionnez **Propriétés** dans le menu. Dans **Réseaux préférés**, cliquez sur le bouton **Ajouter**.
2. Inscrivez votre SSID dans la case prévue et choisissez le même canal de transmission (ici : canal 7) que pour le réglage du routeur à l'étape 2.
3. Inscrivez aussi ici la même phrase de codage («Un chasseur sachant... »).
4. Sauvegardez vos changements.

Autres informations sur WLAN :
F724 **fr.bluewin.ch/accesinternet/index.php/wlan_traveller**
F725 **www.figer.com/publications/network.htm**

Liste de contrôle

	A faire	fait	Notes	Cf. page
	Type et version du système d'exploitation constatés p. ex. dans Windows : Démarrer > Programmes > Exécuter. Saisir «winver», OK.	☐	Type	
1.	**Télécharger actualisations pour le système d'exploitation** (attention : se logger comme «administrateur»)	☐		24
2.	**Télécharger version d'essai pour solution complète de logiciel de protection** ou	☐	*Norton Internet Security 2005*	21
	Se procurer un pare-feu sur XP: pare-feu activé ? autres systèmes d'exploitation: pare-feu acheté/téléchargé ?	☐	*Microsoft XP Firewall*	19/20
	Se procurer un logiciel antivirus	☐		19/20
3.	**Actualisation automatique du système d'exploitation et préparé pour le logiciel de protection ?**	☐		24
4.	**Autres mots de passe vérifiés**	☐	Ne pas noter !	26
5.	**Compte administrateur sur Windows protégé par mot de passe ?**	☐	Ne pas noter !	16
6.	**Paramètres de sécurité vérifiés ?** • Option Fichiers dont l'extension est connue activée • Adapter les niveaux de sécurité d'Internet Explorer • Saisie semi-automatique des mots de passe désactivée • Service de nouvelles Windows désactivé • Programme mail (ici : Outlook Express) sécurisé	☐		22/23
7.	**Copies de sauvegarde créées** • Besoin de mémoire calculé • Support mémoire sélectionné et acheté • Notes dans agenda pour prochaines copies de sauvegarde	☐	Nouvelles copies toutes les _____ semaines	25
8.	**Services de rappel activés** (ou propres rappels notés dans l'agenda)	☐		24
	Uniquement pour réseau sans fil 1. Mot de passe changé 2. Réseau protégé (SSID) 3. Trafic radio encrypté	☐		36/37

f726 www.schoolnet.ch/checkliste.pdf.

«Education routière» pour l'autoroute de l'information

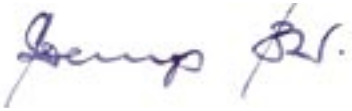
Chères enseignantes,
Chers enseignants,

Les questions de sécurité décrites dans ce SchoolNetGuide nous intéressent tous et constituent bien entendu un thème idéal pour l'école. Nous nous rappelons l'éducation routière scolaire nous apprenant le comportement sûr à adopter dans la circulation routière. C'est maintenant l'heure de l'«éducation routière» pour les autoroutes modernes de l'information, en d'autres mots celle du maniement sûr d'Internet.

Ici aussi, il est utile de ne pas seulement pouvoir lire les étapes nécessaires, mais de les «toucher» et de les essayer dans la mesure du possible. C'est pourquoi je me réjouis que l'exposition «Cybernetguard» du Musée suisse des transports et des communication de Lucerne offre cette possibilité. Permettez-moi de vous recommander une visite de l'exposition avec votre classe. Elle n'est pas seulement intéressante du point de vue informatique ; elle montre avant tout les risques et règles de base du maniement des technologies de l'information et de la communication qui revêtent pour nous une grande importance dans la vie de tous les jours.

Profitez aussi de la possibilité d'aborder les aspects économiques, sociaux et éthiques de la diffusion d'Internet, p. ex. par des discussions en vue de la préparation à la visite de l'exposition, discussions sur des thèmes tels que l'équilibre entre la sécurité et la sphère privée ou la motivation des programmeurs de virus à qui leur créativité destructive n'apporte aucun bénéfice direct. Profitez-en si vous avez des passionnés d'Internet dans votre classe : la structure modulaire de l'exposition permet de faire expliquer ces contenus sur place par les écoliers.

Je vous souhaite beaucoup de plaisir et de succès à l'occasion de cette excursion.



Beat W. Zemp

Président central LCH
Enseignant(e)s de Suisse

Index

Autres liens

F727 **www.cybernetguard.ch** – Site Web de l'exposition sur le thème de la sécurité informatique et la sphère privée sur Internet au Musée suisse des transports et des communications de Lucerne. Les enseignants peuvent visiter le musée gratuitement pour préparer les visites de leurs classes. La halle COM 1 peut être réservée sur place pour des cours.

F728 **www.microsoftsecurity.ch** - Portail de Microsoft Suisse consacré à la sécurité et donnant des informations actuelles sur les virus et des instructions détaillées pour tous les paramètres de sécurité.

F729 **www.inoculer.com** - Site web qui offre des dossiers et des trucs tout autour de la sécurité informatique.

F730 **eservice.free.fr** -Site Web privé sur les thèmes de la sécurité.

Impressum

Editeur Swisscom « Internet à l'école »

Rédaction et textes Zeix SA, Zurich

Numéro SchoolNetGuide n° 7 · automne 2004

Tirage 400 000 (a/f/i)

Impression Zollikofer SA, St-Gall

L'édition n° 8 de SchoolNetGuide est envisagée pour le printemps 2005.

envoyer dans une enveloppe affranchie S.V.P

Swisscom SA
Internet à l'école
Alte Tiefenaustrasse 6
Case Postale
3050 Berne

Pour les écoles de Suisse, que le monde est petit!

Ces trois dernières années, Swisscom a déjà connecté gratuitement à l'Internet plus de 3000 écoles dans le cadre de son engagement en faveur de l'«Internet à l'école».
Et ce n'est pas terminé. Les écoles qui souhaitent bénéficier de cette action de Swisscom en sauront plus en visitant le site www.swisscom.com/sai.

www.swisscom.com/sai

Internet à l'école

swisscom