

Résumé

L'Internet occupe une place de plus en plus prépondérante dans la vie quotidienne. De nombreuses personnes utilisent ce mode de communication pour rester en contact avec leurs amis, pour travailler, pour consulter les nouvelles, s'informer, acquérir des biens ou services, gérer leurs finances, etc. Un des plus grands avantages de l'Internet est que vous pouvez réaliser tout cela aussi bien en vous trouvant à Luxembourg qu'à New-York. De plus en plus de gens utilisent l'Internet sur d'autres ordinateurs que le leur (dans des cyber-cafés pendant leurs vacances par exemple). Par la nature publique des postes de travail dans les cyber-cafés, il est très important de suivre les quelques consignes de sécurité présentées

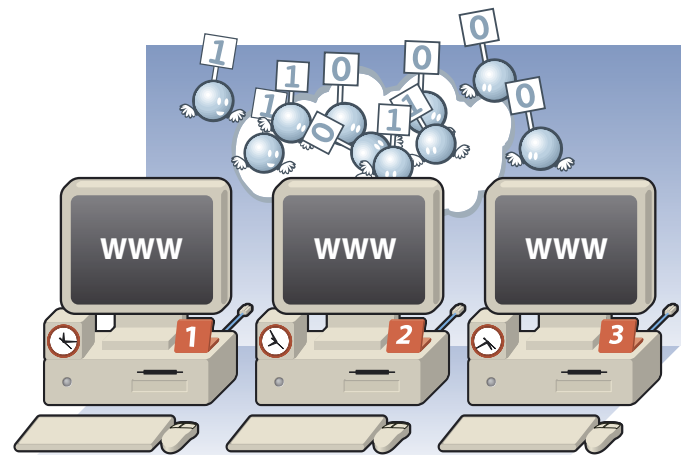
ci-dessous afin d'éviter qu'un attaquant puisse avoir accès à vos données personnelles (ou s'attaque à vos comptes bancaires...).

La meilleure approche pour ne pas subir cette perte de confidentialité ou même d'argent est évidemment de ne pas accéder aux applications importantes ou sensibles depuis des postes inconnus ou suspects. Malheureusement ceci n'est pas toujours possible. Cette fiche vous donne quelques conseils et règles simples à suivre pour réduire les risques liés aux « postes publics ».

Table des matières

1 Problèmes rencontrés

2 Bonnes pratiques



1 Problèmes rencontrés

Les problèmes liés à l'utilisation d'un PC inconnu ou dans un endroit public sont principalement dus au fait :

- ➔ d'un environnement public peu adéquat en matière de sécurité;
- ➔ de l'utilisation d'un ordinateur inconnu;
- ➔ d'une utilisation massive par d'autres personnes.

1.1 L'endroit (l'environnement)

Peu importe si l'ordinateur public que vous utilisez se trouve dans un cybercafé ou au sein de votre entreprise, il est clair que l'environnement dans lequel cette machine se trouve sera peu discret. Vous ne pourrez empêcher que quelqu'un passe (ou s'installe) derrière vous et observe ce qui s'affiche sur votre écran et ce que vous piannotez sur le clavier. Cette technique simple « d'espionnage » appelée « shoulder surfing » est très efficace, et extrêmement courante...

1.2 L'ordinateur inconnu

Si vous utilisez un ordinateur qui n'est pas le vôtre, vous ne pouvez être certain du fait qu'il soit bien installé, géré et sécurisé. Il est tout à fait possible (et même probable dans certains cyber-cafés) que votre machine soit infectée par des virus ou « spywares ».

Le but de ces spywares est de suivre toutes les opérations effectuées sur la machine et d'envoyer ces informations aux malfrats qui s'y intéressent. En général, les spywares prennent la liste des sites que vous avez visités ainsi que les données personnelles que vous avez entrées sur ces sites, comme par exemple votre nom, adresse ou encore vos numéros de cartes bancaires et mots de passe.

Quand vous vous connectez à votre site webmail préféré et que votre ordinateur est infecté par un spyware, vous prenez le risque que votre account email soit lu et utilisé par autrui, ce qui peut vous mettre en danger de poursuites judiciaires !

Dans le cas de l'e-commerce, la situation est encore bien plus grave: la divulgation de votre numéro de carte de crédit peut engendrer des pertes financières importantes ainsi que de gros ennuis lorsque vous vous rendez compte que vous avez soudainement atteint le plafond de votre carte et qu'elle est bloquée!

1.3 L'ordinateur partagé

Quand vous naviguez sur le web, vous laissez des traces de vos activités dans l'ordinateur que vous utilisez. Parmi ces informations se trouve l'historique des sites visités (« history »), le contenu des pages visualisées (ceci est appelé « cache »), les contenus des formulaires que vous avez remplis.

Toutes ces informations peuvent aider une personne malintentionnée à faire votre profil voir même à pouvoir se connecter avec vos coordonnées sur des sites avec authentification (webmail, e-commerce, e-banking). C'est pour cette raison qu'il est primordial de ne pas vous éloigner de votre ordinateur public quand vous utilisez des sites sensibles, même pas pour quelques minutes comme pour aller chercher une boisson ou pour aller aux toilettes.

2

Bonnes pratiques

La solution la plus simple est d'éviter d'effectuer des transactions sensibles sur l'Internet quand vous utilisez un poste de travail inconnu ou public, ou si vous vous trouvez dans un lieu de passage très fréquenté.

Les cyber-cafés, mais également les gares avec accès « wireless », ne sont pas adéquats pour réaliser des transactions financières ou confidentielles.

Si vous devez toutefois utiliser un poste quelconque dans un endroit public, vous pouvez limiter vos risques en suivant les conseils ci-dessous :

2.1 Méfiez-vous des « shoulder surfer »

Si possible, installez-vous dans un coin ou dos contre un mur – Surveillez qu'il n'y ait pas de caméra de vidéo-surveillance qui puisse capter votre écran et/ou votre clavier.

2.2 Vérifiez l'absence de spyware

Assurez-vous, dans la mesure du possible, que votre PC n'a pas été infecté par un spyware. Pour cela vous pouvez utiliser « Ad-Aware » (<http://www.lavasoftusa.com/software/adaware/>) ou « SpyBot Search & Destroy » (<http://www.safer-networking.org/en/spy-botsd/index.html>).

2.3 Utilisez un navigateur sécurisé

Évitez d'utiliser Microsoft Internet Explorer parce que la plupart des attaques spyware se focalisent sur cette plate-forme. Si possible, préférez Mozilla Firefox (<http://www.mozilla.org/>).

2.4 Visitez uniquement des sites sécurisés

Séparez bien votre utilisation du navigateur pour surfer et pour faire des transactions importantes: visitez une seule catégorie de sites avec le même navigateur et fermez-le complètement (File > Quit) avant d'aller sur un autre type de sites. Ceci vous coûte quelques secondes mais cela peut éviter certains vols de sessions.

Les sites importants que vous visiterez devront utiliser le protocole HTTPS, ce qui vous assure que vos données sont transmises de façon chiffrée et vous permet également de vérifier l'identité du site en question (voir la fiche sur HTTPS pour plus d'informations à ce sujet).

2.5 Ne laissez pas de traces

La procédure à suivre dépend du navigateur utilisé :

➔ Internet Explorer :

- Cliquez sur Tools > Internet Options.
- Dans le tab General, cliquez sur Delete Files et Delete Cookies.
- Puis cliquez sur Clear History.
- Sur le tab intitulé Content, cliquez sur AutoComplete.
- Cliquez sur Clear Forms et Clear Passwords.

➔ Mozilla Firefox :

- cliquez sur Tools > Options.
- Dans le tab Privacy, après « Clear all information stored while browsing : » cliquez sur Clear All.

Vous pouvez également utiliser « SpyBot Search & Destroy » pour enlever ces traces de l'ordinateur.

2.6 Protégez vos données personnelles

Les navigateurs courants vous offrent la possibilité de remplir des formulaires automatiquement, et ce, même pour vos mots de passe. Cette fonctionnalité est bien pratique, mais elle n'a pas de place sur un poste qui va être utilisé par d'autres personnes ! Quand votre navigateur vous demande donc si vous voulez qu'il se souvienne de vos mots de passe, répondez Non.

Il est possible de désactiver cette fonctionnalité avant d'entrer vos mots de passe :

➔ Internet Explorer :

- Cliquez Tools > Internet Options.
- Dans le tab Content, cliquez sur AutoComplete. Décochez toutes les cases.

➔ Mozilla Firefox :

- Cliquez Edit > Preferences.
- Dans le tab Privacy, cliquez sur Saved Form Information et décochez la case, ensuite cliquez sur Saved Passwords et décochez la case.

Si vous suivez cette procédure, vos données ne seront pas stockées par le navigateur. Néanmoins, il est toujours possible qu'un spyware (plus spécifiquement, un « keystroke logger ») intercepte votre mot de passe quand vous l'entrez. C'est la raison pour laquelle il est fortement conseillé, quand vous prévoyez de passer par un cyber-café ou autre poste public, de changer temporairement vos mots de passe.

Surtout n'oubliez pas dans ce cas de les rechanger immédiatement après votre retour sur votre poste de travail habituel !