Pôle Ressources Numériques de l'Ondaine

III. **Utiliser les services de l'Internet**

- *1. Se repérer et naviguer sur Internet*
- *2. Effectuer une recherche*
- *3. Utiliser des services en ligne*

3 comment utiliser des services en ligne

Explications avec Franck Baudot, ingénieur-expert à la CNIL.
LexTimes.fr : Expliquez-nous le principe de cette nouvelle rubrique "Vos traces" sur le site de la CNIL.
Franck Baudot : La finalité est de sensibiliser les internautes au sujet. Au cours de leurs navigations sur le web, des données techniques sur eux peuvent être récupérées. Il s'agit déjà de les en informer, et aussi de leur faire quelques recommandations simples afin qu'ils ne soient pas trop exposés à l'utilisation de ces données.

Comment laisse t-on des traces sur le web ? en faisant quoi ?
En naviguant sur n'importe quel type de site, et c'est pour cela qu'il vaut mieux éviter si possible de fréquenter ceux sur lesquels on n'a pas d'informations, dont on ne sait pas qui les gère. Le conseil est de ne rentrer aucune donnée personnelle sur ces sites-là.

Quelles formes prennent ces "traces" que l'on laisse sur internet ?
Elles sont de différentes formes. Quand on se connecte à un serveur, des informations de configuration de l'ordinateur, comme l'adresse IP par exemple, peuvent être transmises. Et l'on peut être capable d'identifier quelqu'un de manière quasi unique sur la base de la configuration de son ordinateur ! Autre moyen: les *cookies*. Ce sont de petits fichiers textes que les sites peuvent déposer sur les ordinateurs pour réidentifier la personne quand elle se reconnectera sur le même serveur. Plus insidieux, il y a maintenant les cookies "flash". 98% des ordinateurs "grand public" possèdent le logiciel "flash", et c'est encore plus facile d'être identifié par ce biais, car plus difficile de supprimer les cookies.

Qui peut utiliser ces "traces" et dans quel but ?

Il y a plusieurs cas de figures. Parfois ce sont de simples programmes informatiques. Quand vous vous connectez à un moteur de recherche comme par exemple Google, un programme va déposer des cookies pour être capable de vous réidentifier par la suite. Il pourra ainsi savoir qui vous êtes, connaître vos centres d'intérêts et affiner la qualité de réponse à vos recherches.

Mais cela peut aussi être des personnes, parfois mal intentionnées. Évoquons ainsi les attaques du genre "phishing". Par des moyens frauduleux, des escrocs peuvent accéder à vos informations, notamment au site de votre banque. Ils peuvent substituer quelques minutes le site internet de votre banque à un autre site factice dans le but de récupérer vos identifiants de connexion. Ils vont ensuite vous renvoyer sur le vrai site de votre banque, et vous ne vous serez même pas rendu compte de l'opération. Rappelons aussi que si quelqu'un saisit votre ordinateur, il pourra avoir accès à son historique.

Comment contrôler et éventuellement effacer ou supprimer ces "traces" ?

Il faut commencer par appliquer des recommandations simples: ne pas accepter tous les cookies, refuser notamment les cookies tiers (ceux qui ne sont pas rattachés au site que l'on est en train de visiter), et supprimer régulièrement l'historique de son ordinateur.

Source : http://www.lextimes.fr/5.aspx?sr=379#wluOARFxyYolHu15.99

Le saviez-vous ? Lorsque vous naviguez sur Internet tous les jours, vous laissez des traces. Les sites que vous visitez, les mots que vous tapez dans les barres de recherche, les liens sur lesquels vous cliquez, tout cela est potentiellement enregistrable et utilisable.

La Commission nationale de l'informatique et des libertés (CNIL) s'est penchée sur le sujet et en parle sur son site internet. Dans la rubrique "Vos traces", vous pouvez savoir quelles informations personnelles peuvent être accessibles lorsque vous naviguez sur le web.

Il faut s'assurer que vous possédez une protection contre les logiciels malveillant, ils en existent plusieurs.

Les attaques sur les comptes bancaires en lignes sont très fréquentes.

Il y a plusieurs raisons cohérentes pour la popularité grandissante des attaques sur des comptes en ligne. Les pirates ont un accès immédiat au compte et arrivent sans détour à leur but : votre argent. Cet accès reste souvent inaperçu pendant une longue période. Ceci est dû aux raisons suivantes :

- Absence de logiciels de sécurité, de protection en temps réel ou d'analyse de comportement. L'époque des pièces jointes aux mails qu'il fallait ouvrir pour causer une infection sont bel et bien révolus. Aujourd'hui, ce sont plutôt des points faibles ("exploits") dans des applications bien répandues telles que l'environnement d'exécution *Java, Adobe Acrobat* et *Flash Player* ou des logiciels de *Microsoft* tels que *Windows* ou *Internet Explorer* dont les criminels se servent.

- Si vous utilisez des logiciels démodés ou dépourvus de mises à jour récentes. Il suffit de vous rendre sur un site web préparé à cet effet pour infecter votre ordinateur. Il ne doit même pas s'agir d'un site web peu sérieux des zones grises sur Internet. Il y a des nouvelles régulières sur des cas dans lesquels des exploits passent par des réseaux de publicité ou des sites web fréquentés par de nombreuses personnes tels que des portails d'information.

- Si un ordinateur est directement connecté sur Internet, c'est-à-dire sans router ou *pare-feu*, il est possible de profiter directement de ces points faibles depuis l'extérieur. Votre PC sera infecté sans que vous ne vous en rendiez compte.

La plupart des logiciels de sécurité gratuits ne proposent pas de composants de protection en temps réel essentiels. Parmi ceux-ci comptent par exemple une analyse de comportement efficace qui détecte les variantes nouvelles et inconnues de *malware* de manière fiable qui sont, d'habitude, installées à travers ces exploits. Si vous vous contentez d'un nettoyage hebdomadaire à l'aide de logiciels *anti-virus* ou *anti-malware* gratuits, vous pourriez de même afficher ouvertement vos détails de compte et la liste TAN sur Facebook.

Les connexions sécurisées ne suffisent pas toujours

Quelques forums et directives de sécurité recommandent diverses règles de conduite pour utiliser Internet en toute sécurité. Une astuce fréquente : Utiliser des connexions sécurisées (HTTPS pour "sécurisé") pour les services bancaires en ligne en particulier. Cette méthode ne vous protège néanmoins pas du tout contre les méthodes d'attaque les plus récentes, telles que celles employées par les *malware* bancaires, les attaques de "l'homme dans le navigateur". Car les logiciels se servent directement du navigateur de l'utilisateur alors que les connexions sécurisées, telles que celles par SSL ou TLS, ne protègent que les communications entre le navigateur et le serveur de votre banque.

Imaginez : vous téléphonez sur une ligne sécurisée. Cela ne sert pas à grand chose si un espion a installé un microphone directement dans votre combiné.

La mise en page des sites de services bancaires en ligne est peuvent être manipulée.

Certaines variantes de logiciels malveillants bancaires s'attendent à ce que vous effectuiez une transaction pour la manipuler ensuite de manière spécifique. Vous faites, par exemple un virement pour payer le loyer du mois prochain de votre appartement et saisissez un TAN. Le virement s'effectue comme d'habitude, mais le numéro de compte cible sera modifié. Une personne dite "money mule" aura votre argent sur son compte. C'est un tiers qui aide les criminels, sans s'en rendre compte, à s'emparer de l'argent volé, et aura une provision pour ce service. Votre solde bancaire sera manipulé de façon à ce que vous ne voyez pas la transaction modifiée. Rien de suspect non plus sur votre relevé de compte, étant donné que le numéro de compte falsifié sera remplacé par celui du compte de votre propriétaire.

Personne ne saura rien jusqu'à ce que votre propriétaire vous appelle après quelques semaines. Suffisamment de temps pour vider votre compte et trop de temps pour encore annuler les transactions effectuées.