Fiche mémento
« Du bon usage des réseaux sociaux »

1. But de la fiche mémento

Au cours de ces dernières années, les applications de réseaux sociaux sur Internet n'ont cessé de se développer. Rien qu'en Suisse, on compte aujourd'hui 2,48 millions d'utilisateurs actifs de Facebook. A l'échelle mondiale, les fournisseurs de réseaux sociaux tels que Facebook ou autres attirent chaque mois - selon leurs propres chiffres - plus de 100 millions de visiteurs sur leurs pages Web.
Les réseaux sociaux et les profils personnels qu'ils présentent (données) revêtent aujourd'hui une importance non négligeable, dans la mesure où ils représentent les identités virtuelles des internautes. La question est de savoir comment utiliser judicieusement les réseaux sociaux et leurs aspects positifs, sans pour autant sacrifier sa vie privée ?

2. Risques pour l'utilisateur

Que se passe-t-il, lorsque votre (futur) employeur voit les photos de votre dernière fête bien arrosée ? Quel profit pourrait tirer une personne malintentionnée d'informations concernant votre travail ou vos projets de vacances ? C'est le genre de questions que vous devriez vous poser avant de vous créer un profil dans un réseau social et à fortiori avant d'y révéler toute sorte d'informations sur vous-même.

Publication d'informations privées
Sur leurs profils, les utilisateurs de réseaux sociaux peuvent indiquer leurs adresses de courrier électronique, leurs numéros de téléphone, leurs loisirs, leurs préférences et autres informations personnelles. Ces données peuvent être exploitées par des entreprises pour bombarder les utilisateurs de publicité ciblée.
À l'ouverture du compte, les paramètres de confidentialité standard ne sont pas suffisants et l'ensemble des données peut être visualisé par tous les utilisateurs du réseau social. Certains passages des profils peuvent même être partiellement retrouvés par des moteurs de recherche, ce qui les rend accessibles à tous les internautes du monde entier.

Au moment du recrutement, les employeurs utilisent les réseaux sociaux pour obtenir des informations sur leurs collaborateurs potentiels. Photos osées ou déclarations insidieuses les poussent alors rapidement à écarter une candidature. De même, les propriétaires d'appartements à louer et les assureurs peuvent être intéressés par certaines informations révélées.

Informations, textes et en particulier photos sont souvent archivés par les utilisateurs en dehors des réseaux sociaux sur leurs propres ordinateurs. De cette manière, les données peuvent à tout moment apparaître sur d'autres pages Web ou être exploitées à d'autres fins, même après avoir été supprimé du profil.

Vol d'identité
Les cyberpirates tentent de plus en plus de craquer des comptes utilisateurs pour commettre leurs méfaits sous l'identité de quelqu'un d'autre. Une fois qu'ils ont pris possession d'un compte, ils mettent souvent en scène une situation d'urgence et demandent aux amis du réseau de les aider financièrement. Les informations lues en accédant au profil de l'utilisateur peuvent les aider à renforcer leur crédibilité et à tromper les amis. De faux profils sont de plus en plus utilisés à des fins malfaisantes : les voleurs peuvent par exemple apprendre quand quelqu'un part en vacances et laisse ainsi son appartement sans surveillance.

Diffusion des logiciels malveillants
Les utilisateurs font preuve en général d'une grande confiance à l'égard des réseaux sociaux. Les cyberpirates ont donc eu l'idée d'y transposer un bon vieux truc : en postant des messages contenant un lien renvoyant à des sites Web piratés, ils contribuent à la diffusion de logiciels malveillants. Le ver Koobface qui s'était répandu à travers Facebook en est un exemple célèbre. Les utilisateurs reçoivent des messages provenant de comptes précédemment infectés les invitant à regarder une vidéo. En cliquant sur le lien correspondant, le destinataire de l'invitation était renvoyé sur une page piratée de Facebook ou de YouTube, où il devait télécharger le lecteur Flash Player. Mais derrière le programme offert, c'est le ver qui se dissimulait et poursuivait ainsi son inexorable diffusion.

Certains réseaux sociaux offrent des applications supplémentaires que les utilisateurs peuvent ajouter à leur profil. C'est le cas par exemple des mini-jeux auxquels les utilisateurs peuvent jouer en réseau. Mais le problème est que ces applications proviennent de fournisseurs tiers dont les standards de sécurité ne correspondent pas nécessairement à ceux des réseaux sociaux. De cette manière, les maliciels peuvent – de façon volontaire ou non - se diffuser parmi la communauté d'utilisateurs.

Mobbing (harcèlement)

Avec les réseaux sociaux, le harcèlement ou mobbing prend une nouvelle dimension. Des personnes peuvent par exemple être volontairement exclues de groupes d'amis ou voir leurs murs couverts d'insultes. Ce phénomène peut devenir un véritable tourment, tout particulièrement pour les jeunes. Le harcèlement est passible de sanctions.

On se lie plus rapidement d'amitié dans les réseaux sociaux que dans le monde « réel ». Ainsi, des informations parviennent à des personnes auxquelles elles n'auraient peut-être jamais été confiées. Une personne malintentionnée peut mettre à profit ces informations pour compromettre quelqu'un ou manigancer contre lui.

Les « cyberharceleurs » peuvent également se créer de « faux » profils où ils se font passer pour une autre personne, réelle ou fictive. De cette manière, ils peuvent, dans le plus parfait des anonymats, harceler d'autres personnes à travers le réseau social.

3. Règles de conduite pour une fréquentation sûre et sécurisée des réseaux sociaux

Des millions d'internautes nouent des contacts et développent des liens d'amitié à travers le Net. Pour cela ils se créent sur Facebook, ou sur tout un autre réseau, un profil personnel qui peut contenir, au-delà des informations élémentaires les concernant, d'autres renseignements au sujet de leurs loisirs, de leur situation familiale ou de leur carrière professionnelle. L'objectif de ces réseaux sociaux est d'entretenir un réseau d'amis et de partager des contenus. Afin que tous les utilisateurs se sentent bien au sein d'une communauté en réseau, il est important de respecter certaines règles de conduite (qui valent d'ailleurs aussi dans le monde réel). Le réseautage social doit être un plaisir et pour qu'il le reste, il convient d'adopter une attitude amicale et respectueuse envers les autres membres de la communauté. Avec les 12 règles de conduite suivantes, vous voilà armés pour la vie sociale sur Internet !

1. **Faites preuve de réserve lorsque vous révélez des informations personnelles**
   Tout le monde ne doit pas tout savoir sur vous. Faites donc preuve de sens critique pour choisir les données privées que vous voulez réellement rendre « publiques ». Songez par exemple que de plus en plus d'employeurs interrogent Internet pour en savoir plus sur les candidats à l'embauche. De même, les chasseurs de tête, les assureurs ou les propriétaires d'appartements à louer peuvent être intéressés par de telles informations.
2. **Renseignez-vous sur les conditions générales et les conditions de protection des données du réseau social utilisé !**
   Il convient de les lire attentivement et ce, avant de créer un profil. Ne manquez pas d'utiliser les options offertes par le réseau social qui vous permettent de choisir qui peut voir les informations et les images que vous publiez : doivent-elles être accessibles à vos amis seulement, ou bien à vos amis et à leurs amis, ou bien encore à tous les utilisateurs ?
3. **Choisissez bien vos amis et n'acceptez pas toutes les invitations. Les criminels « collectionnent » les amis dans le but de nuire !**
   Pour les personnes que vous ne connaissez pas « réellement », il convient de réfléchir avec esprit critique si vous souhaitez vraiment les ajouter à votre liste d'amis. L'inconnu(e) pourrait également être malintentionné(e) : des malfaiteurs pourraient par exemple essayer de savoir à quel moment votre appartement est vide. Il a été prouvé que les « faux profils » sont utilisés pour nuire aux personnes, que ce soit par vengeance, cupidité ou autre.
4. **Signalez les « cyberharceleurs » qui vous importunent continuellement sur un réseau social !**
   Pour cela, vous pouvez la plupart du temps vous adresser directement aux gérants du réseau social en question. Ces derniers peuvent suivre l'affaire et le cas échéant supprimer le profil douteux. Dans certains cas, il convient également d'informer la police pour engager des poursuites.
5. **Utilisez un mot de passe fort et différent pour chaque application Internet, notamment si vous possédez des profils dans plusieurs réseaux sociaux.**
   Soyez toujours conscient du fait que vos données sont stockées sur des ordinateurs inconnus. Cela signifie que la sécurité de vos données ne dépend pas uniquement de vous, mais aussi des gérants du réseau social : il suffit que leur serveur soit craqué pour que vos données ne soient plus en sécurité. Dès que vous prenez connaissance d'un abus, avertissez-en vos amis.

6. **Ne révélez aucune information confidentielle concernant votre employeur et votre travail !**
   Les informations à caractère professionnel n'ont rien à faire sur les réseaux sociaux. Les espions économiques ont fait des réseaux sociaux un nouveau terrain de jeu et tentent d'y récolter de précieuses informations. Votre entreprise risque d'y perdre de l'argent, et vous votre job.
7. **Examinez avec attention les droits que vous accordez aux gérants des réseaux sociaux sur les images, textes et informations que vous publiez !**
   Tout service a son prix : votre billet d'entrée dans un réseau social est la divulgation d'informations. Beaucoup de sociétés sont prêtes à acheter ces données pour pouvoir envoyer de la publicité ciblée. Si vous cédez les droits de vos photos aux réseaux sociaux, les gérants peuvent théoriquement les vendre à des tiers. Contrôlez également si les droits d'utilisation accordés demeurent, même si vous supprimez votre profil.
8. **Lorsque vous recevez des demandes « douteuses » de la part de personnes connues, enquêtez en dehors des réseaux sociaux sur la fiabilité du message !**
   Le vol d'identité est un risque de l'ère numérique Avec un compte craqué, une personne peut s'approprier une identité et tromper les amis de sa victime. Les pirates peuvent par exemple envoyer des messages dans lesquels ils font état d'une situation d'urgence et demandent une aide financière. Grâce aux informations obtenues à travers le vol d'identité, leur appel au secours apparaît sous une forme des plus crédibles.
9. **Ne cliquez pas au hasard sur tous les links qui vous passent sous les yeux. Les réseaux sociaux sont de plus en plus utilisés pour les attaques de phishing !**
   On a vite fait de cliquer sur un lien. Mais attention ! L'adresse cible pourrait être la page d'accueil falsifiée d'un réseau social. En saisissant sur cette page votre nom utilisateur et votre mot de passe, vos données sont directement transmises aux cyberpirates. Dans la mesure où elles ne permettent pas à l'utilisateur de reconnaître la véritable adresse cible, les URL courtes sont particulièrement prisées par les hameçonneurs.
10. **Parlez avec vos enfants de leurs activités dans les réseaux sociaux et expliquez-leur les dangers qui s'y cachent.**
    La plupart des enfants et adolescents ne sont pas conscients des dangers qui se dissimulent dans les réseaux sociaux. Pour eux, le plaisir l'emporte souvent sur la sécurité. Le renforcement de la « compétence médiatique » est une nouvelle tâche à laquelle parents et éducateurs doivent s'atteler. Mais il serait également souhaitable d'échanger avec ses amis ou d'autres membres de la famille sur les risques.
11. **Les employeurs** qui permettent l'accès aux réseaux sociaux tels que Facebook dans leur entreprise devraient établir une directive « Médias Sociaux » et sensibiliser leurs collaborateurs sur leur utilisation. La directive « Médias Sociaux » devrait compléter le contrat de travail et être signée par chaque collaborateur.
12. En accédant à Facebook à partir d'un **téléphone mobile**, les utilisateurs de Facebook peuvent faire connaître leur état actuel en temps réel. De cette manière, les cambrioleurs savent à quel moment vous n'êtes pas chez vous. Faites en sorte de désactiver cette fonction ou de ne l'utiliser que de façon ciblée.

InfoSurance est une association fondée par de grandes entreprises et la confédération pour la promotion de la sécurité de l'information en Suisse. Son objectif est de sensibiliser la population suisse sur l'utilisation des technologies de l'information.
(v1.0, janvier 2011)

Une initiative de : Soutenue par : Industrie, Administration et Education

InfoSurance
et votre ordinateur est en sécurité.