Réseaux sociaux

Introduction : Le principe des médias et réseaux sociaux est le partage d'informations, photos et autres données personnelles avec des «amis». Mais ces informations peuvent aussi être interceptées par des escrocs du web. Il importe donc de bien réfléchir aux informations que vous publiées sur votre profil. Rappelez-vous que tout ce que vous publiez sur un site de réseau social est permanent.

Pour se protéger

	A faire	A éviter
Niveau 1	• Se limitez à publier des informations personnelles • Acceptez les invitations d'«amitié», uniquement des personnes que l'on connaît vraiment dans la vie réelle. • Se méfier des messages d'une personne que l'on ne connait pas. • Utilisez des mots de passe différents pour chaque compte/service. • S'assurer que les programmes informatiques sont parfaitement à jour (navigateur, système d'exploitation, antivirus, etc.). • Si l'on doute de la quantité d'informations demandée par une application, le mieux serait de ne pas l'installer. • Décocher la case « maintenir la connexion »	• Ouvrir les liens (documents, photos, vidéos, etc.) provenant de source douteuse et toujours les vérifiez avant de cliquer dessus. • Envoyer croire à tous les messages que l'on reçoit (ex : concours pour gagner un IPhone, demande urgente d'argent…), même s'il s'agit d'un ami. Il se pourrait que le compte de ce dernier ait été piraté ou copier.
Niveau 2	• Utiliser des logiciels anti-virus • Adapter des paramètres de confidentialité en fonction des besoins • Utiliser des connexions sécurisées « http:// » • Supprimer les cookies • Supprimer les photos, statuts sur lesquels vous êtes tagué et qui pourraient vous porter préjudice dans le futur	• Publier sa date de naissance • Publier ses dates de vacances (pour éviter les cambriolages) • Publier trop de photos • Activer le géolocalisation • Accepter tout le monde • Laisser ses coordonnées bancaires • Laisser ses amis parler sur soi (dire n'importe quoi) • Cliquer sur les liens pirates • Utiliser les bornes wifi publiques

Application :

- Supprimer les cookies
  - Paramètres/ historique/ effacer/ cookies et plug-in

- **Facebook :**
  - Paramètres de sécurité (connexion) :
    - **Alertes de connexion** (quand quelqu'un se connecte à votre compte sur un nouvel appareil ou un nouveau navigateur)
    - **Générateur de codes** Activer la fonctionnalité « approbation de connexion. Ainsi pour vous connecter à votre compte sur un nouvel appareil, il vous faudra saisir votre mot de passe et un code. Le code est fourni par l'application Facebook et le renouvelle toutes les 30 secondes.
    - **Contacts de confiance** : ce sont des amis qui peuvent vous aider en toute sécurité si vous avez des problèmes d'accès à votre compte. Ces derniers doivent simplement confirmer votre identité avant de vous donner les codes de sécurité. Il vous suffira ensuite de saisir les codes pour pouvoir vous connecter.
    - **La double authentification** est une option activable sur la plupart des réseaux sociaux. Lorsque vous vous connectez depuis un poste informatique inconnu, le réseau social vous demandera de confirmer l'accès en entrant un code que vous aurez reçu par sms ou par mail. D'autres fonctions proposent simplement de vous alerter si une personne extérieure tente de se connecter à votre compte depuis un terminal inconnu (PC, smartphone, tablette, mac).
    - **Vérifier le nombre d'appareils reconnu et de sessions actives**
  - Confidentialité :
    - Limiter le nombre de personnes ayant accès à votre profil, vos publications.
  - Journal et identification :
    - Limiter le nombre de personnes pouvant publier sur votre journal
    - Activer, examen des publications dans lesquelles vous êtes identifié.
    - Limiter l'accès à votre journal (ex// amis uniquement)
  - Blocage :
    - Si un utilisateur vous harcèle, il peut être intéressant de le bloquer. Pour cela allez dans le menu Compte puis paramètres de confidentialité, cliquez sur modifier vos listes dans la partie Listes de personnes et applications bloquées. Saisissez le pseudo de la personne puis cliquez sur Bloquer cet utilisateur.

Rq: il est possible par la suite de débloquer cette personne par la suite en effectuant la même manipulation.

- **<u>Twitter</u> :**
    - Paramètres / profil / confidentialité :
        - Notifications de photos (seuls les personnes qui me suivent peuvent me mentionner)
        - Protéger mes tweets
    - Bloquer quelqu'un :
        - Appuyer longuement sur un tweet (sur le téléphone) ou clic droit (sur ordinateur), ensuite bloquer ou signaler ou ne plus afficher
- **<u>Google+</u> :**
    - Paramètres
        - Limiter l'accès

          => Partage / visibilité / contacts et cercles
        - Ne pas partager sa position

      Partage de position

      =>off

Fiche réalisée par : Ruben Atlani, Guillaume Adiceam, Léni Alilat, Côme Dacien, Valérie Douangphrachandr et Manohari Goarin.