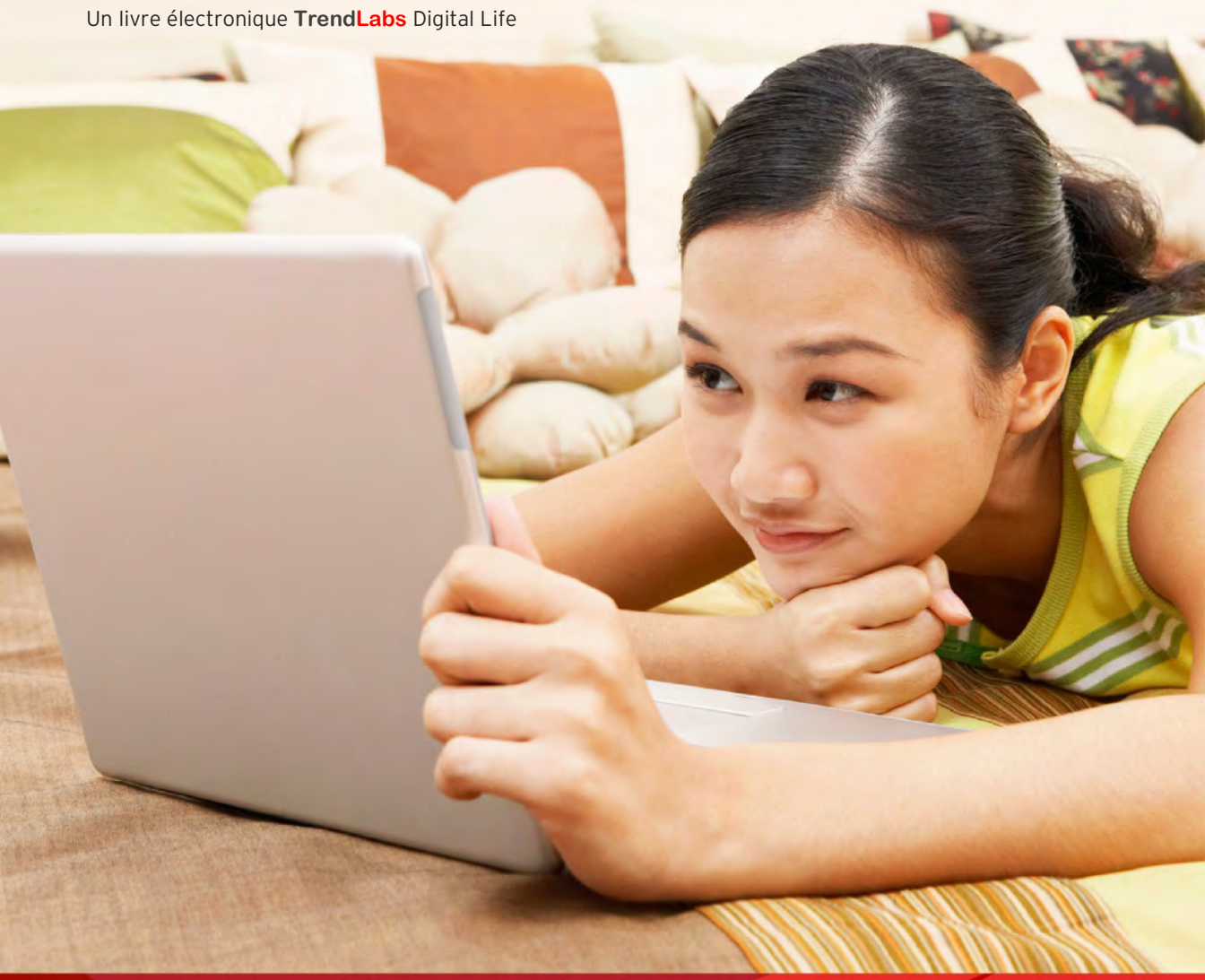
TREND MICRO™

Enjoy your digital life safely

Comment protéger votre confidentialité sur les réseaux sociaux

Un livre électronique **TrendLabs** Digital Life



Comment garder les informations confidentielles sur les réseaux sociaux ? Selon une étude de Trend Micro, seuls 38 % des internautes savent limiter ce qu'ils publient en ligne. Ce faible pourcentage montre que de nombreux utilisateurs partagent plus d'informations qu'ils ne le souhaitent.

Partager trop d'informations en ligne peut porter atteinte à votre réputation. Par exemple, votre famille et votre employeur peuvent repérer des photos de vous dans des situations compromettantes car elles ont été postées de façon négligente. Vos informations peuvent aussi être utilisées pour l'usurpation d'identité, si les cybercriminels les utilisent pour se faire passer pour vous. L'usurpation d'identité est devenue si fréquente que l'on a recensé une victime d'usurpation d'identité toutes les trois secondes l'an passé, aux États-Unis.

Faire confiance aux paramètres de confidentialité d'un site n'est qu'un début. Alors que des paramètres et outils de compte plus stricts peuvent vous aider à protéger votre confidentialité, vos informations personnelles peuvent être rendues publiques de différentes façons. Connaître ces risques potentiels de confidentialité et leur faire face vous aidera à protéger vos données.

Les publications quotidiennes

Si les applications tierces, telles que l'horoscope ou les applications de test de QI, fonctionnent sur les réseaux sociaux, ce ne sont pas nécessairement eux qui les ont créées. Ces applications vous demandent souvent si elles peuvent accéder à vos informations afin de personnaliser votre expérience utilisateur. Si vous doutez de la quantité d'informations demandée par une application, le mieux serait de ne pas l'installer.

Des publicités apparaissent également sur les réseaux sociaux sous la forme de publications sponsorisées. Les entreprises concluent un marché avec les réseaux sociaux qui leur permettent d'utiliser toute activité liée à la marque sur le site, telle que son appréciation, comme publication sponsorisée.

Vérifiez les paramètres de vos applications pour éviter de partager trop d'informations :

Facebook Contrôlez la visibilité relative à l'activité de vos applications sur votre journal et votre flux dans la section Applications de vos paramètres de confidentialité. Vous pouvez aussi gérer les paramètres de chaque application voire les supprimer. Même si vous ne pouvez pas désactiver les publications sponsorisées, vous pouvez ajuster les paramètres de confidentialité de ces publicités.

Google+ Gérez la visibilité des applications ou supprimez-les dans la section Applications et activités.

Twitter Refusez l'accès à votre compte Twitter aux applications tierces dans la section Applications.

L'ensemble des clauses

Les politiques de confidentialité vous donnent une idée de l'importance que les réseaux sociaux accordent à la confidentialité. Vous pouvez découvrir : quelles informations ils recueillent et comment, qui a accès à ces informations, quelles mesures de sécurité sont en place, combien de temps les informations sont stockées et comment les contacter pour tout problème lié à la confidentialité.

Les politiques de confidentialité sont généralement faciles à trouver sur les sites. Il est important de les consulter régulièrement car elles peuvent changer à tout moment. Vous pouvez également utiliser un scanner de confidentialité pour identifier rapidement les paramètres de sécurité susceptibles de rendre vos informations personnelles vulnérables à l'usurpation d'identité, sans avoir besoin de lire l'ensemble des clauses.

Consultez les politiques de confidentialité et ajustez les paramètres à votre convenance :

Facebook	Consultez la page Politique d'utilisation des données pour savoir comment éviter de divulguer vos informations personnelles identifiables.
Google+	Ce site ne vous permet pas de désactiver la divulgation de vos informations personnelles identifiables. Consultez la page Google+ Règles et principes et la page Règles de confidentialité Google.
Twitter	Découvrez comment bloquer l'accès à vos informations personnelles identifiables sur la page Twitter Politique de confidentialité.
REMARQUE **:**	Les organismes d'application de la loi peuvent disposer librement de vos informations personnelles identifiables.

Les identifications

Être identifié dans une publication peut paraître anodin, mais cela peut réduire votre confidentialité. Vos contacts pourront voir lorsque vous êtes identifié dans une publication ou une photo, même s'ils ne sont pas connectés à la source originale. Cela peut nuire à votre réputation si vous êtes identifié sur une photo ou dans une publication peu flatteuse ou sensible.

Vos contacts peuvent également savoir où vous êtes, si un ami décide d'identifier votre emplacement, permettant à quiconque de vous suivre physiquement. Supprimer les identifications ou les mentions peut s'avérer difficile car certains réseaux sociaux ne disposent pas de cette option. Les scanners de confidentialité peuvent vous aider à suivre toutes vos identifications.

Gardez un œil sur toutes vos identifications et mentions :

Facebook Vérifiez les publications et photos identifiées avant qu'elles ne soient ajoutées à votre journal. Vous pouvez aussi supprimer les identifications manuellement.

Google+ Acceptez ou supprimez les identifications sur des images ou sélectionnez une fonction qui accepte automatiquement les identifications de contacts spécifiques.

Twitter Vos contacts peuvent automatiquement inclure votre nom d'utilisateur dans des mentions et des réponses. Toutefois, la visibilité des ces tweets varie en fonction des paramètres de confidentialité de vos contacts. Si vous paramétrez votre compte en mode « privé », les utilisateurs dont les comptes n'ont pas été approuvés ne pourront pas voir vos tweets ni y répondre.

Le partage entre amis

La structure des réseaux sociaux est telle que les paramètres de confidentialité de vos amis ont un impact direct sur votre confidentialité. Si vos amis ont des paramètres moins restrictifs, un public plus large peut voir vos publications.

Les informations que vous postez peuvent toujours être partagées, même avec les paramètres de confidentialité les plus élevés. Certains réseaux sociaux permettent à vos contacts de copier et de republier vos publications originales. Des personnes extérieures peuvent aussi voir vos publications privées si vous y êtes identifié. Souvenez-vous que tout reste en ligne, publiez donc seulement des mises à jour ou des photos que vous acceptez de partager avec des inconnus.

Assurez-vous que vos publications peuvent être vues uniquement par le public souhaité :

Facebook La catégorie « Amis et leurs amis » permet à des gens que vous ne connaissez pas de voir vos publications et vos photos.

Google+ Vous pouvez partager la liste de personnes de votre entourage avec d'autres utilisateurs, exposant les comptes de vos proches à un public plus large.

Twitter Votre compte peut être inclus dans une liste Twitter pouvant être partagée en public. Les utilisateurs auront toujours besoin de votre approbation pour suivre votre compte si celui-ci est en mode privé.

Différences en termes de désactivation

Certains sites font la distinction entre la désactivation et la suppression d'un compte, dans le but de ne pas supprimer définitivement votre compte. Si vous disposez de plusieurs comptes sur le même site, vous devez supprimer chacun d'entre eux séparément.

Désactiver ou supprimer votre compte ne garantit pas qu'il ne laissera aucune trace. Certains de vos profils ou publications cachés peuvent continuer d'apparaître dans les moteurs de recherche. Vos informations peuvent aussi rester stockées sur les serveurs ou les bases de données du site.

Découvrez comment supprimer ou désactiver vos comptes :

Facebook Désactivez ou supprimez votre compte. La désactivation vous permet de réactiver votre compte ultérieurement. En supprimant votre compte de manière permanente, vous effacerez toutes vos informations personnelles, à l'exception de vos messages envoyés.

Google+ Supprimer votre compte Google+ est plus compliqué car celui-ci est connecté à vos autres comptes Google. La suppression de votre compte efface tous vos contacts, commentaires et publications.

Twitter Twitter attend 30 jours avant de désactiver votre compte de manière permanente. Même si votre compte a été désactivé, le contenu reste encore disponible sur le site pendant quelques jours.

AVIS DE NON-RESPONSABILITÉ DE TREND MICRO

Les informations contenues dans le présent document sont fournies uniquement à titre informatif et pédagogique. Elles ne constituent pas et ne doivent pas être interprétées comme constituant des conseils juridiques. Les informations contenues dans le présent document peuvent ne pas s'appliquer à toutes les situations et peuvent ne pas refléter la situation la plus actuelle. Aucune information contenue dans le présent document ne doit servir de base d'action sans l'apport d'un conseil juridique fourni à partir des circonstances particulières et faits présentés ; aucune information contenue dans le présent document ne doit être interprétée autrement. Trend Micro se réserve le droit de modifier le contenu du présent document à tout moment et sans préavis.

Les traductions de tout document vers d'autres langues sont proposées uniquement dans un souci de commodité. L'exactitude de la traduction n'est ni garantie ni implicite. En cas de questions liées à l'exactitude d'une traduction, veuillez vous reporter à la version officielle du document en langue originale. Toute divergence ou différence apparaissant dans la traduction n'a pas force obligatoire et n'entraîne aucun effet juridique à des fins de mise en conformité ou d'exécution.

Même si Trend Micro met en œuvre des efforts raisonnables pour inclure des informations exactes et à jour, Trend Micro ne donne aucune garantie ou représentation d'aucune sorte en ce qui concerne leur exactitude, actualité ou exhaustivité. Vous consentez à accéder, à utiliser et à exploiter le présent document et son contenu à vos propres risques. Trend Micro exclut toute garantie, qu'elle soit explicite ou implicite. Trend Micro ainsi que toute autre partie impliquée dans la création, la production ou la publication du présent document ne sauraient être tenues responsables pour toute conséquence, perte ou dommage, y compris direct, indirect, accessoire ou immatériel, pour toute perte de profits ou pour tout dommage spécial lié à l'accès, à l'utilisation ou à l'incapacité à utiliser, ou en lien avec l'utilisation du présent document, ou pour toute erreur ou omission dans le présent contenu. L'utilisation de ces informations constitue une acceptation d'utilisation dans des conditions « telles quelles ».

Trend Micro Incorporated, leader mondial des solutions et logiciels de sécurité, met tout en œuvre pour sécuriser l'échange d'informations numériques. Pour plus d'informations, consultez www.trendmicro.com.

Enjoy your digital life safely

Created by:
TrendLabs, The Global Technical Support & R&D Center of TREND MICRO