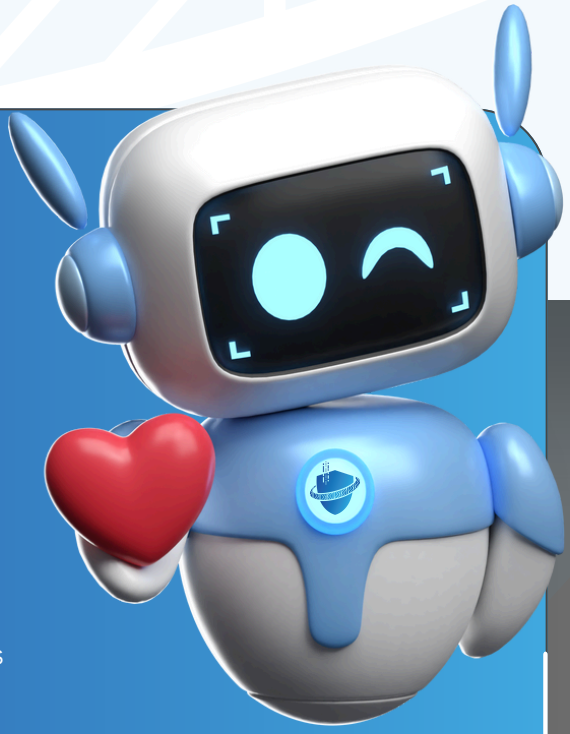
SÉCURITÉ SUR LES RÉSEAUX SOCIAUX

CENTRE CYBER DU PACIFIQUE

EN BREF

POURQUOI C'EST IMPORTANT ?

Les réseaux sociaux sont des outils de communication et d'information puissants et facilement accessibles. Aujourd'hui installés dans les usages personnels des internautes, mais aussi dans les usages professionnels des entreprises qui les utilisent comme vitrine de leur activité, ils n'échappent pas aux activités malveillantes. Escroquerie, usurpation d'identité, chantage, vol d'informations, cyberharcèlement, désinformation, diffamation… sont autant de dangers auxquels sont confrontés les utilisateurs de ces réseaux.



Voici 10 bonnes pratiques à adopter pour votre sécurité sur les réseaux sociaux

1. PROTÉGEZ L'ACCÈS À VOS COMPTES
2. VÉRIFIEZ VOS PARAMÈTRES DE CONFIDENTIALITÉ
3. MAÎTRISEZ VOS PUBLICATIONS
4. FAITES ATTENTION À QUI VOUS PARLEZ
5. CONTRÔLEZ LES APPLICATIONS TIERCES
6. ÉVITEZ LES ORDINATEURS ET LES RÉSEAUX WIFI PUBLICS
7. VÉRIFIEZ RÉGULIÈREMENT LES CONNEXIONS À VOTRE COMPTE
8. FAITES PREUVE DE DISCERNEMENT AVEC LES INFORMATIONS PUBLIÉES
9. UTILISEZ AVEC PRUDENCE L'AUTHENTIFICATION DE VOTRE COMPTE RS SUR D'AUTRES SITES
10. SUPPRIMEZ VOTRE COMPTE SI VOUS NE L'UTILISEZ PLUS

▶ Voir détail page "10 BONNES PRATIQUES A ADOPTER"

SÉCURITÉ SUR LES RÉSEAUX SOCIAUX

CENTRE CYBER DU PACIFIQUE

10 BONNES PRATIQUES À ADOPTER

1. PROTÉGEZ L'ACCÈS À VOS COMPTES

Vos comptes de réseaux sociaux contiennent des informations personnelles sensibles (identité, adresse, numéro de téléphone, etc.), convoitées par des cybercriminels. Utilisez des mots de passe différents et robustes. Activez la double authentification si possible.

2. VÉRIFIEZ VOS PARAMÈTRES DE CONFIDENTIALITÉ

Par défaut, vos informations personnelles sont souvent très accessibles. Réglez la visibilité de vos données pour maîtriser ce que les autres utilisateurs voient de vos activités. Vérifiez régulièrement ces paramètres, qui peuvent changer sans notification.

3. MAÎTRISEZ VOS PUBLICATIONS

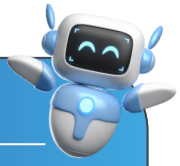
Les réseaux sociaux permettent de communiquer à un large public. Même dans un cercle restreint, vos publications peuvent vous échapper. Ne diffusez pas d'informations personnelles ou sensibles. Faites attention à ce que vous partagez sur votre travail, cela pourrait vous nuire ainsi qu'à votre entreprise.

4. FAITES ATTENTION À QUI VOUS PARLEZ

Les cybercriminels utilisent les réseaux sociaux pour voler des informations. Soyez vigilants même avec vos contacts, qui peuvent partager des contenus malveillants sans le savoir. Ne transférez jamais d'argent ou de photos sensibles à des contacts virtuels.

5. CONTRÔLEZ LES APPLICATIONS TIERCES

Certaines applications demandent des autorisations pour accéder à vos informations. Ne les installez que depuis des sources officielles. Si une application semble intrusive, évitez de l'installer. Pensez à révoquer les autorisations des applications que vous n'utilisez plus.



LE SAVIEZ-VOUS ?

En vertu de la loi n° 2018-493 du 20 juin 2018 – Article 20, un mineur peut consentir seul à un traitement de ses données à caractère personnel à partir de quinze ans. Avant cet âge, le consentement du titulaire de l'autorité parentale est requis.

RESPECTEZ LA LOI

Internet n'est pas une zone de non-droit et l'anonymat n'y est pas absolu : les propos incitant à la haine ou à la violence, la pédophilie, le cyberharcèlement, l'atteinte au droit à l'image ou au droit d'auteur… sont punis par la loi.

SÉCURITÉ SUR LES RÉSEAUX SOCIAUX

CENTRE CYBER DU PACIFIQUE

10 BONNES PRATIQUES À ADOPTER

6. ÉVITEZ LES ORDINATEURS ET LES RÉSEAUX WIFI PUBLICS

Se connecter via un ordinateur en libre accès ou un réseau WiFi public présente des risques. Un cybercriminel pourrait voler votre mot de passe et pirater votre compte. Si vous devez utiliser un tel réseau, assurez-vous de vous déconnecter après utilisation.

7. VÉRIFIEZ RÉGULIÈREMENT LES CONNEXIONS À VOTRE COMPTE

La plupart des réseaux sociaux vous permettent de voir les connexions actives sur votre compte. Consultez ces informations et déconnectez les sessions inconnues. En cas de doute, changez immédiatement votre mot de passe.

8. FAITES PREUVE DE DISCERNEMENT AVEC LES INFORMATIONS PUBLIÉES

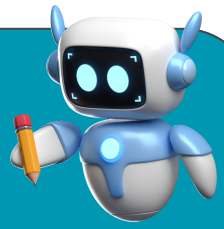
Les réseaux sociaux sont des outils puissants, mais les informations publiées peuvent être fausses. Avant de partager une information, vérifiez sa véracité pour éviter de relayer des fausses nouvelles qui pourraient causer du tort.

9. UTILISEZ EN CONSCIENCE L'AUTHENTIFICATION AVEC VOTRE COMPTE DE RÉSEAU SOCIAL SUR D'AUTRES SITES

Certains sites permettent de se connecter via votre compte de réseau social, mais cela partage des informations entre les deux. Si votre compte est piraté, tous les sites liés pourraient être compromis. Vérifiez toujours les autorisations avant d'utiliser cette fonctionnalité.

10. SUPPRIMEZ VOTRE COMPTE SI VOUS NE L'UTILISEZ PLUS

Pour éviter que votre compte ne soit piraté ou utilisé à votre insu, supprimez-le si vous ne l'utilisez plus.



QUE FAIRE EN CAS DE PROBLÈME ?

- Réagir en cas de piratage de votre compte de réseau social – Les conseils de la CNIL : www.cnil.fr/fr/prevenir-reperer-et-reagir-face-au-piratage-de-ses-comptes-sociaux
- Demander la suppression d'une publication gênante ou compromettante sur les réseaux sociaux – Les conseils de la CNIL : www.cnil.fr/fr/publication-genante-sur-les-reseaux-sociaux-signalez-pour-supprimer
- Être conseillé face à une situation de cyberharcèlement : contacter gratuitement le 3018 par téléphone ou sur 3018.fr.
- Signaler un contenu illicite sur les réseaux sociaux – Internet Signalement/Pharos (ministère de l'Intérieur) : www.internet-signalement.gouv.fr