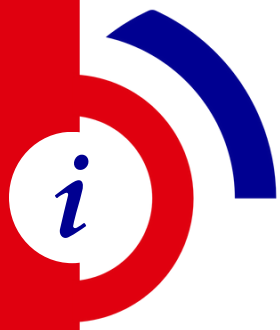
FICHE RÉFLEXE



BONNES PRATIQUES À ADOPTER POUR LA SÉCURISATION DE COMPTE SUR LES RÉSEAUX SOCIAUX

CYBER RÉUNION

CYBER RÉUNION

LA SÉCURISATION DE COMPTE SUR LES RÉSEAUX SOCIAUX

Les réseaux sociaux sont devenus des outils incontournables pour communiquer et partager des informations. Cependant, ils sont aussi des cibles privilégiées pour les cybercriminels. Un compte mal protégé peut être compromis et utilisé pour voler des données, diffuser du contenu frauduleux ou escroquer vos contacts.
Adoptez ces bonnes pratiques pour protéger vos comptes.

UTILISEZ DES MOTS DE PASSE FORTS ET UNIQUES

Un mot de passe solide est la première ligne de défense contre la compromission de votre compte. Il doit être **unique** pour chaque compte :

- **Optez pour un mot de passe d'au moins 12 caractères avec lettres, chiffres et caractères spéciaux**.
- **N'utilisez jamais le même mot de passe** sur plusieurs sites.
- **Privilégiez un gestionnaire de mots de passe** pour stocker et gérer vos identifiants en toute sécurité.

ACTIVEZ L'AUTHENTIFICATION À DEUX FACTEURS (2FA)

L'authentification à deux facteurs ajoute une couche supplémentaire de sécurité en exigeant une deuxième forme de vérification, comme un code envoyé par SMS ou généré par une application dédiée, en plus de votre mot de passe.
Cette mesure rend l'accès à votre compte beaucoup plus difficile pour les cybercriminels, même s'ils connaissent votre mot de passe.

- **Utilisez une application d'authentification** (ex. Google Authenticator, Microsoft Authenticator ou équivalent).

VÉRIFIEZ ET AJUSTEZ VOS PARAMÈTRES DE CONFIDENTIALITÉ

Par défaut, les réseaux sociaux peuvent rendre vos informations personnelles visibles à un large public. Il est crucial de configurer vos paramètres de confidentialité pour contrôler qui peut voir vos publications, vos informations personnelles et votre liste d'amis.

- **Révisez régulièrement ces paramètres** pour vous assurer qu'ils correspondent à vos préférences en matière de confidentialité.
- **Limitez la visibilité de vos informations personnelles** (date de naissance, adresse, numéro de téléphone).
- **Restreignez l'accès à vos publications** et à votre liste d'amis à vos contacts de confiance.

LIMITEZ L'ACCÈS DES APPLICATIONS TIERCES À VOS COMPTES

Certaines applications ou jeux demandent l'accès à vos comptes de réseaux sociaux.

- **Accordez ces autorisations avec prudence et révoquez l'accès aux applications que vous n'utilisez plus ou en lesquelles vous n'avez pas confiance.**

MÉFIEZ-VOUS DES LIENS ET MESSAGES SUSPECTS

Ne cliquez pas sur des liens provenant de messages non sollicités, même s'ils semblent provenir d'un ami.

- **Vérifiez toujours l'expéditeur et privilégiez les sites officiels pour toute connexion**.

SURVEILLEZ LES CONNEXIONS ET ACTIVITÉS SUSPECTES

Vérifiez régulièrement l'activité de vos comptes pour détecter des connexions ou des publications suspectes. La plupart des réseaux sociaux offrent des options pour consulter les appareils connectés à votre compte et les sessions actives.

- **Si vous remarquez une activité inhabituelle, déconnectez les sessions suspectes et changez immédiatement votre mot de passe.**

SOYEZ VIGILANT(E) AUX DEMANDES D'AJOUT D'INCONNUS

Accepter des demandes d'ajout ou de suivi de personnes que vous ne connaissez pas peut exposer vos informations à des individus malveillants.

- **Soyez sélectif et n'acceptez que les personnes que vous connaissez et en qui vous avez confiance.**

CYBER RÉUNION

LA SÉCURISATION DE COMPTE SUR LES RÉSEAUX SOCIAUX

Les réseaux sociaux sont devenus des outils incontournables pour communiquer et partager des informations. Cependant, ils sont aussi des cibles privilégiées pour les cybercriminels. Un compte mal protégé peut être compromis et utilisé pour voler des données, diffuser du contenu frauduleux ou escroquer vos contacts.
Adoptez ces bonnes pratiques pour protéger vos comptes.

ÉVITEZ LES CONNEXIONS SUR DES WI-FI PUBLICS NON SÉCURISÉS

Les réseaux Wi-Fi publics peuvent être moins sécurisés et faciliter l'interception de vos données par des cybercriminels.

- **Si vous devez vous connecter sur un réseau public, évitez d'accéder à des informations sensibles ou utilisez un réseau privé virtuel (VPN) pour sécuriser votre connexion.**

DÉSACTIVEZ OU SUPPRIMEZ LES COMPTES INUTILISÉS

Les comptes inactifs peuvent être des cibles faciles pour les cybercriminels.

- **Si vous n'utilisez plus un compte de réseau social, il est préférable de le désactiver ou de le supprimer pour réduire les risques.**

QUE FAIRE EN CAS DE COMPROMISSION ?

1. **Changez immédiatement votre mot de passe et activez la 2FA.**
2. **Vérifiez les sessions actives et déconnectez celles que vous ne reconnaissez pas.**
3. **Prévenez vos contacts pour éviter qu'ils ne se fassent piéger.**
4. **Contactez le support du réseau social pour récupérer votre compte.**
5. **Révoquer les autorisations d'applications tierces**
6. **Conserver l'ensemble des éléments de preuve : contenu diffusé, messages envoyés aux contacts**
7. **Dépôt de plainte dans le cas d'une usurpation d'identité, chantage, escroquerie ou propagation de contenu illégale**

RESSOURCES UTILES

- Cybermalveillance.gouv.fr – Sécuriser ses comptes
- Guide officiel Facebook
- Guide officiel Instagram
- Guide officiel X/Twitter
- Guide officiel LinkedIn

RETROUVEZ TOUTES NOS PUBLICATIONS SUR
www.cyber-reunion.fr