CYBER RÉFLEXES

Vous protéger sur Internet

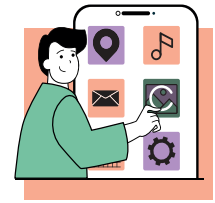
DES MOTS DE PASSE SOLIDES ET DIFFÉRENTS POUR CHAQUE COMPTE VOUS CHOISIREZ

Un mot de passe, c'est comme une clé propre à chaque porte : elle vous protège de l'intrusion. Si vous vous faites voler un mot de passe que vous utilisez pour différents sites web ou applications, ils pourront tous être piratés !

BONNES PRATIQUES

- Utilisez des mots de passe suffisamment longs, complexes et surtout différents pour chaque compte.
- Gardez-les secrets et privilégiez un gestionnaire de mots de passe sécurisé pour les conserver.

LES MISES À JOUR DE VOS APPAREILS SANS TARDER VOUS FEREZ

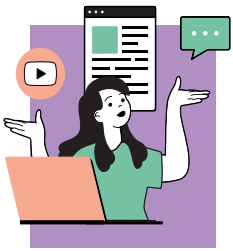


Les failles de sécurité de vos logiciels, applications et matériels sont comme des portes laissées ouvertes pour les pirates. Ils peuvent les utiliser pour accéder à vos données personnelles ou les voler.

BONNES PRATIQUES

- Faites les mises à jour des logiciels, applications et appareils, dès qu'elles vous sont proposées pour corriger leurs failles de sécurité.
- Activez les options de mises à jour automatiques chaque fois que c'est possible.

EN LIGNE, LE MOINS POSSIBLE SUR VOTRE IDENTITÉ VOUS DIREZ



Publier et partager vos données personnelles sur Internet (nom, prénom, adresse mail, photos, vidéos, vocaux…) peut les exposer à une utilisation malveillante.

BONNES PRATIQUES

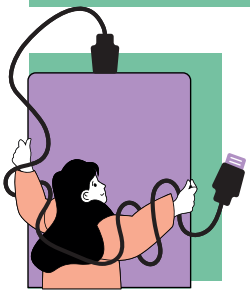
- Évitez de divulguer vos données personnelles et celles de vos connaissances.
- Vérifiez les paramètres de confidentialité de vos comptes pour définir ce qui peut être visible par les autres.
- Utilisez des pseudos quand c'est possible.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE GOUV.FR
Assistance et prévention en sécurité numérique

CNIL.
COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

EN LIEU SÛR, UNE COPIE DE VOS DONNÉES VOUS CONSERVEREZ



Copier vos données, c'est les sauvegarder pour éviter de les perdre en cas de piratage, de vol, de panne ou de casse de vos appareils.

BONNE PRATIQUE

• Pensez à faire régulièrement des sauvegardes de vos données sur un autre support (clé USB, disque externe, cloud...) pour pouvoir les retrouver en cas de problème.

DES MESSAGES INATTENDUS ET ALARMANTS TOUJOURS VOUS VOUS MÉFIREZ

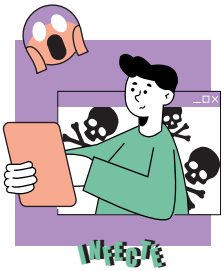
L'hameçonnage ou *phishing*, ce sont des messages (courriels, SMS, réseaux sociaux) ou appels d'escrocs qui se font passer pour un organisme familier (banque, administration…). Ces arnaques visent à vous voler des informations personnelles et bancaires, vous faire télécharger un virus ou directement vous escroquer.

BONNES PRATIQUES

• Restez méfiants et ne vous précipitez pas pour cliquer ou répondre.

• Vérifiez toujours l'information par vous-même, en vous connectant à votre compte sur le service concerné.

LES CONTENUS PIRATÉS OU NON-OFFICIELS VOUS ÉVITEREZ



Des virus qui peuvent pirater vos appareils ou vos comptes sont souvent présents dans les logiciels ou jeux piratés, les extensions de triche de jeux vidéo, les sites de *streaming* illégaux...

BONNES PRATIQUES

• Ne téléchargez pas de contenus illégaux ni des solutions non officielles.

• Installez uniquement des applications depuis les sites ou magasins officiels des éditeurs.

PLUS DE CONSEILS SUR :

CNIL.FR

CYBERMALVEILLANCE.GOUV.FR