CYBER RÉFLEXES

Se protéger sur Internet

1 DES MOTS DE PASSE SOLIDES ET DIFFÉRENTS POUR CHAQUE COMPTE TU CHOISIRAS

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

BONNES PRATIQUES

- Utiliser des mots de passe suffisamment longs, complexes et surtout différents pour chaque compte.
- Les garder secrets et privilégier un gestionnaire de mots de passe sécurisé pour les conserver.

2 LES MISES À JOUR DE TES APPAREILS SANS TARDER TU FERAS

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

BONNES PRATIQUES

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

3 EN LIGNE LE MOINS POSSIBLE SUR TON IDENTITÉ TU DIRAS

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

BONNES PRATIQUES

- Éviter de divulguer tes données personnelles et celles de tes connaissances.
- Vérifier les paramètres de confidentialité de tes comptes pour définir ce qui peut être visible par les autres.

4 EN LIEU SÛR, UNE COPIE DE TES DONNÉES TU CONSERVERAS

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

BONNE PRATIQUE

- Penser à faire régulièrement des sauvegardes de tes données sur un autre support (clé USB, disque externe, *cloud*...) pour pouvoir les retrouver en cas de problème.

5 DES MESSAGES INATTENDUS ET ALARMANTS TOUJOURS TU TE MÉFIERAS

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 te voler des informations personnelles et bancaires, te faire télécharger un virus ou directement t'escroquer.

BONNES PRATIQUES

- Toujours te méfier et ne pas te précipiter pour cliquer ou répondre.
- Vérifier toujours l'information par toi-même, en te connectant à ton compte sur le service concerné.

6 LES CONTENUS PIRATÉS OU NON OFFICIELS TU ÉVITERAS

Des virus qui peuvent pirater tes appareils ou tes 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 pas télécharger des contenus illégaux ni des solutions non officielles.
- Installer uniquement des applications depuis les sites ou magasins officiels des éditeurs.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique

CNIL.
COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

CYBER MOIS

PLUS DE CONSEILS SUR
CNIL.FR
CYBERMALVEILLANCE.GOUV.FR