Sensibilisation à la sécurité informatique : Bonnes Pratiques

Protégez vos données, restez vigilant et en sécurité en ligne

Conseils basés sur les recommandations de la CNIL et de L'ANSSI

Introduction :

CNIL et ANSSI : Gardiens de la Sécurité Informatique

- CNIL : Commission nationale de l'informatique et des libertés

Créée en 1978, elle protège les données personnelles et les droits liés à la vie privée

- ANSSI : Agence Nationale de la Sécurité des Systèmes d'Information

Créée en 2009 elle renforce la sécurité des système d'information nationaux et protège les données stratégique et les infrastructures essentielles.

Gestionnaire de mot de passe

Pourquoi utiliser un gestionnaire de mots de passe ?

- En seulement 6 minutes, un hacker peut pirater un mot de passe de 7 caractères comprenant chiffres, majuscules, minuscules et symboles.
- L'utilisation d'un gestionnaire de mots de passe, comme Keepass, permet à l'utilisateur de ne retenir qu'un seul mot de passe robuste pour accéder en toute sécurité à l'ensemble de ses mots de passe stockés dans une base chiffrée.
- Les gestionnaires de mots de passe génèrent généralement automatiquement des mots de passe forts, ce qui renforce la sécurité.

Composition du Mot de Passe

Recommandations de la CNIL et de l'ANSSI

- Utilisation de caractères complexes alphanumériques et spéciaux
- Mots de passe d'au moins 12 caractères
- Eviter les informations personnelles
- Mots de passe uniques pour chaque compte en ligne
- Effectuer des modifications régulières des mots de passe
- Utilisation d'outils pour évaluer la force des mots de passe

Vigilance sur les E-mails

Recommandations de la CNIL

- Soyez attentif à qui envoie l'e-mail
- Examinez l'objet pour détecter des signes suspects
- Méfiez-vous des liens et des pièces jointes
- Vérifiez l'orthographe et la grammaire, les erreurs peuvent indiquer un e-mail frauduleux
- Demandez une vérification
- Ne partagez pas d'information sensibles par e-mail
- Éduquez le personnel sur la sécurité des e-mails
- Signalez les e-mails suspects aux autorités ou au service informatique

Des outils tels que 'VirusTotal', qui permet d'analyser une URL ou un dossier, ainsi que 'Have I Been Pwned', qui permet de vérifier si une adresse e-mail ou des mots de passe ont été compromis, sont disponibles pour renforcer la sécurité en ligne.

Le social hacking

Le hacking social est une technique d'attaque qui consiste à manipuler les individus pour obtenir des informations sensibles ou accéder à des systèmes informatiques en exploitant leur confiance, leur curiosité ou leur vulnérabilité.

Pour prévenir et détecter le piratage :

- Utilisez la déconnexion à distance pour désassocier les appareils inutilisés.
- Désactivez les applications non essentielles liées à votre compte.
- Ajustez les paramètres de confidentialité pour limiter l'accès aux pirates potentiels.
- Soyez vigilant en repérant des signes de piratage, tels que des mots de passe invalides ou des comportements inhabituels.
- Signalez immédiatement le piratage et réinitialisez votre mot de passe.
- Explorez les fonctionnalités de sécurité disponibles sur les réseaux sociaux une fois votre compte sécurisé.

Un exemple de la fraude au président est illustré ici :

https://www.cnil.fr/fr/violation-du-trimestre-le-faux-ordre-de-virement-international-ou-fraude-au-president