Existence Numerique

Sensibilisation face aux menaces en lignes

1. Reconnaître les Emails de Phishing :

Méfiez-vous des emails non sollicités demandant des informations personnelles.
Exemple : Un email prétendant être votre banque demandant votre mot de passe.

2. Protégez vos Informations Personnelles :

Ne partagez pas vos informations sensibles sur des sites non sécurisés.
Exemple : Ne donnez pas votre numéro de sécurité sociale en ligne sans vérifier la légitimité du site.

3. Utilisez des Mots de Passe Sécurisés :

Créez des mots de passe forts et uniques pour chaque compte.
Exemple : "S3cur!t3P@ssw0rd!"

4. Méfiez-vous des Téléchargements :

Ne téléchargez que des logiciels et fichiers à partir de sources fiables.
Exemple : Téléchargez des applications uniquement depuis les boutiques officielles comme Google Play ou l'App Store.

5. Gardez Vos Logiciels à Jour :

Installez régulièrement les mises à jour de sécurité pour tous vos appareils.
Exemple : Activez les mises à jour automatiques pour votre système d'exploitation et vos applications.

6. Activez l'Authentification à Deux Facteurs (2FA) :

Utilisez 2FA pour ajouter une couche de sécurité supplémentaire à vos comptes en ligne.
Exemple : Recevez un code de vérification sur votre téléphone lors de la connexion.

7. Utilisez un Antivirus et un Pare-feu :

Protégez vos appareils avec des logiciels antivirus et un pare-feu à jour.
Exemple : Utilisez Windows Defender ou Norton.

8. Soyez Prudent avec les Réseaux Wi-Fi Publics :

Évitez de saisir des informations sensibles sur des réseaux Wi-Fi publics non sécurisés.
Exemple : N'effectuez pas d'opérations bancaires sur un Wi-Fi public sans utiliser un VPN.