Existence Numerique

Naviguer en sécurité sur internet

1. Utilisez des mots de passe sécurisés :

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

2. Activez l'authentification à deux facteurs (2FA) :

Ajoutez une couche de sécurité supplémentaire avec un code envoyé sur votre téléphone.
Exemple : Utilisez Google Authenticator ou SMS pour 2FA.

3. Mettez à jour vos logiciels :

Installez régulièrement les mises à jour de votre système d'exploitation, navigateur et logiciels.
Exemple : Activez les mises à jour automatiques.

4. Utilisez un antivirus et un pare-feu :

Installez et maintenez à jour un logiciel antivirus et un pare-feu.
Exemple : Utilisez Windows Defender ou Avast.

5. Soyez vigilant avec les emails et les liens :

Ne cliquez pas sur des liens ou n'ouvrez pas des pièces jointes provenant d'expéditeurs inconnus.
Exemple : Vérifiez l'adresse email de l'expéditeur avant de cliquer.

6. Naviguez sur des sites sécurisés :

Assurez-vous que l'URL commence par "https://" et recherchez un cadenas dans la barre d'adresse.
Exemple : https://www.example.com

7. Utilisez un réseau privé virtuel (VPN) :

Utilisez un VPN pour chiffrer votre connexion internet, surtout sur les réseaux Wi-Fi publics.
Exemple : Utilisez NordVPN ou ExpressVPN.

8. Déconnectez-vous après utilisation :

Déconnectez-vous de vos comptes après utilisation, surtout sur des ordinateurs partagés.
Exemple : Cliquez sur "Déconnexion" après avoir utilisé un service en ligne.