

## CONSEIL 10

Protégez votre identité en ligne : Limitez les informations personnelles que vous partagez en ligne. Utilisez des paramètres de confidentialité appropriés sur les réseaux sociaux et faites preuve de prudence lorsque vous partagez des informations sensibles.

## CONSEIL 11

Ayez du bon sens : Faites preuve de vigilance en ligne et utilisez votre bon sens. Si quelque chose semble suspect ou trop beau pour être vrai, il est probablement préférable de l'éviter.



Soyez vigilant sur les réseaux sociaux et ajustez vos paramètres de confidentialité pour limiter l'accès à vos informations.

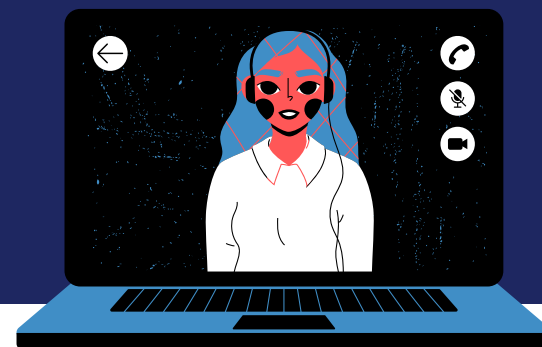


Sensibilisez votre famille et vos collègues aux bonnes pratiques de cybersécurité et encouragez-les à les suivre.



# Guide Cybersécurité

**Pour les débutants**



## CONSEIL 1

Utilisez des mots de passe forts et uniques (12 caractères, majuscule et au moins 1 caractère spécial).

## CONSEIL 2

Activez l'authentification à deux facteurs (A2F), qui renforce la sécurité. C'est une deuxième forme de vérification.

## CONSEIL 3

Méfiez-vous des e-mails et des liens suspects. Le phishing est une attaque courante qui peut voler vos données personnelles. Soyez vigilants quand vous recevez des mails.

## CONSEIL 4

Mettez à jour régulièrement vos logiciels. Les mises à jours peuvent corriger des failles de sécurité.



## CONSEIL 5

Utilisez un logiciel antivirus fiable : Un logiciel antivirus réputé est essentiel pour détecter et supprimer les programmes malveillants tels que les virus, les chevaux de Troie et les logiciels espions. Assurez-vous d'installer un logiciel antivirus de confiance et de le mettre à jour régulièrement pour bénéficier de la meilleure protection possible.

## CONSEIL 6

Activez l'authentification à deux facteurs (A2F), qui renforce la sécurité. C'est une deuxième forme de vérification.

## CONSEIL 7

Soyez prudent sur les réseaux Wi-Fi publics : Évitez d'accéder à des informations sensibles, comme vos comptes bancaires, lorsque vous utilisez des réseaux Wi-Fi publics non sécurisés. Si vous devez le faire, utilisez un réseau privé virtuel (VPN) pour crypter votre connexion.

## CONSEIL 8

Sauvegardez régulièrement vos données : Effectuez des sauvegardes régulières de vos fichiers importants. Cela vous permettra de baisser le risque de pertes de données.

## CONSEIL 9

Sensibilisez-vous et éduquez-vous : Tenez-vous informé des dernières menaces et techniques d'attaque. Apprenez à repérer les signes d'une tentative de phishing ou d'une attaque de logiciel malveillant. Informez vos proches et sensibilisez vous.

