

Cours Bonus

Sécurité

Mots de passe & accès

- Premiers exemples

- Utilisez un mot de passe différent pour chaque service important.
- Choisissez des mots de passe longs (au moins 12 caractères).
- Évitez les mots évidents : prénom, date de naissance, "123456".
- Ne notez jamais vos mots de passe sur un papier visible.
- Activez la double vérification (code par SMS ou appli) quand c'est possible.
- Ne communiquez jamais votre mot de passe, même à un proche ou à un "service client"

Emails, SMS et appels

- Nouveaux Exemples

- Méfiez-vous des emails alarmants (“compte bloqué”, “urgence”).
- Ne cliquez pas sur les liens dans les emails ou SMS suspects.
- Vérifiez toujours l’adresse de l’expéditeur.
- Les banques, impôts et administrations ne demandent jamais vos codes par email ou téléphone.
- Supprimez les messages douteux sans répondre.
- Attention aux faux colis, faux remboursements, faux gains

Navigation Internet

- Encore ?
 - Vérifiez que les sites commencent par `https://` (le petit cadenas).
 - Évitez les sites inconnus ou mal écrits.
 - Ne téléchargez rien depuis une fenêtre qui “clignote” ou fait peur.
 - Fermez les pages qui disent “Votre ordinateur est infecté”.
 - Utilisez un moteur de recherche connu (Google, Safari, Edge).

Logiciels & mises à jour

- Nouveaux Exemples
 - Installez un antivirus reconnu et laissez-le actif (Windows Defender)
 - Faites les mises à jour de l'ordinateur et du téléphone régulièrement.
 - Téléchargez les applications **uniquement** depuis les boutiques officielles (Play Store, App Store).
 - Désinstallez les programmes que vous n'utilisez plus.
 - Évitez les logiciels "gratuits miracles".

Téléphone & applications

- Nouveaux Exemples
 - Verrouillez votre téléphone avec un code ou empreinte.
 - Ne donnez pas toutes les autorisations aux applications.
 - Méfiez-vous des applications qui demandent trop d'informations.
 - Faites attention aux faux messages WhatsApp ou SMS de proches

Données personnelles

- Nouveaux Exemples
 - Ne publiez pas trop d'informations personnelles sur internet.
 - Faites des sauvegardes régulières de vos photos et documents.
 - Ne branchez pas de clé USB inconnue.
 - En cas de doute : ne faites rien et demandez conseil à quelqu'un de confiance

Cours Bonus

Bravo !

Vous avez terminé ce cours !