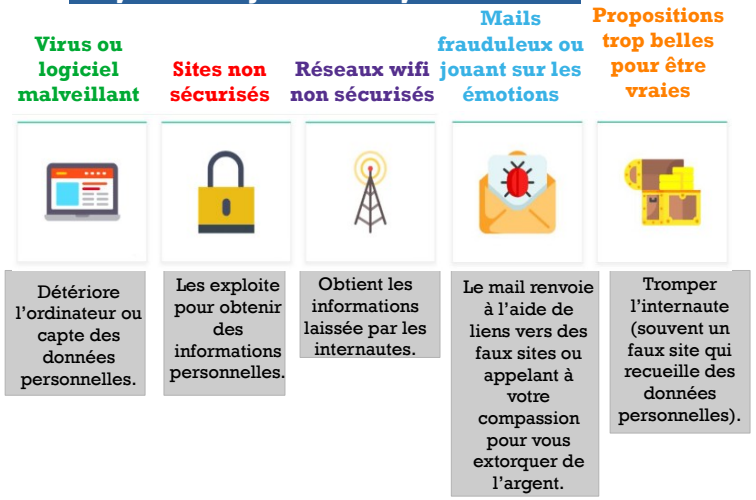
Fiche résumé
La sécurité sur Internet

Moyens et objectifs du cybercriminel



Identifier un site fiable

Comment protéger ses équipements de cyberattaques ?

- **Avoir un antivirus :** Vous **protège contre les logiciels malveillants**. Aujourd'hui, la **plupart** des équipements sont vendus avec **un système de sécurité**. Par exemple, « Windows Defender » sur les équipements Windows.
- **Effectuer les mises à jour :** Permet de **corriger les failles de sécurité éventuelles** de votre ordinateur ou de vos logiciels, applications.
- **Privilégier vos réseaux Wifi privés :** votre réseau privé est **protégé par une clé de sécurité.** Les **Wifi publics ne sont pas sécurisés** ! Un cybercriminel peut facilement prendre le contrôle des réseaux. Quand vous n'êtes pas chez vous, privilégiez vos données mobile de votre smartphone pour aller sur Internet.
- **Faire preuve de vigilance :** Ne dites **pas tout de vous sur Internet**, n'envoyez jamais de documents permettant de vous identifier clairement à des personnes non légitimes. De la même manière, vous pouvez tout à fait choisir un autre nom, prénom, adresse que les vôtres quand vous voulez vous créer un compte de divertissement. **Ne cliquez jamais sur des liens dans des mails suspicieux** et ne télécharger des pièces jointes que si vous connaissez bien l'expéditeur du mail.
- **Effectuer des sauvegardes régulières de vos données :** Pour éviter que vos données disparaissent pendant un piratage ou une panne informatique, il est conseillé d'effectuer des **sauvegardes régulières de ses données, de préférence sur plusieurs supports.** Pour ce faire, vous pouvez utiliser des disques durs externes ou bien sauvegarder vos données dans le Cloud.
- **Savoir identifier un site Web fiable :** vérifier l'adresse URL, son protocole de sécurité, le contenu du site (fautes d'orthographes, syntaxe…).
- **Utiliser des mots forts :** Utilisez des **mots de passe complexes** pour accéder à vos espaces personnels en ligne surtout quand il s'agit de **sites « sensibles »** (Ameli, impôts, Caf, France Travail, messageries). Ils doivent être **uniques pour chaque site et changés régulièrement** pour éviter un piratage de vos comptes massif.
- **Utiliser la double-authentification :** Certains sites vous proposent d'activer la **double-authentification**. Activez-la et lors de chaque **connexion** à ce site, on vous demandera un **code unique temporaire** que vous recevrez par **SMS** ou par votre **boîte de messagerie électronique.**
- **Pensez à supprimer vos données de navigation lors de la fermeture de votre navigateur :** votre historique et les cookies des sites que vous avez visité seront alors effacés.

Créer un mot de passe complexe

Doit contenir :

- Majuscules
- Minuscules
- Chiffres
- Au moins 8 caractères (12 recommandé)
- Signes de ponctuation (. , ; : ! ? …)
- Symboles (€ $ % # @ …)
- Ne pas contenir de données à caractères personnelles (Nom, date de naissance…)

La méthode des premières lettres :

« **J**e **c**rée **u**n **m**ot **d**e **p**asse **s**uper **s**écurisé **!**
Plus **d**e **12** **c**aractères **e**t **6** **t**ypes **d**ifférents **!** »

Jcumdpss!Pd12ce6td!

La méthode phonétique :

« J'ai acheté huit CD pour cent euros cet après-midi »

Ght8CD%E7am

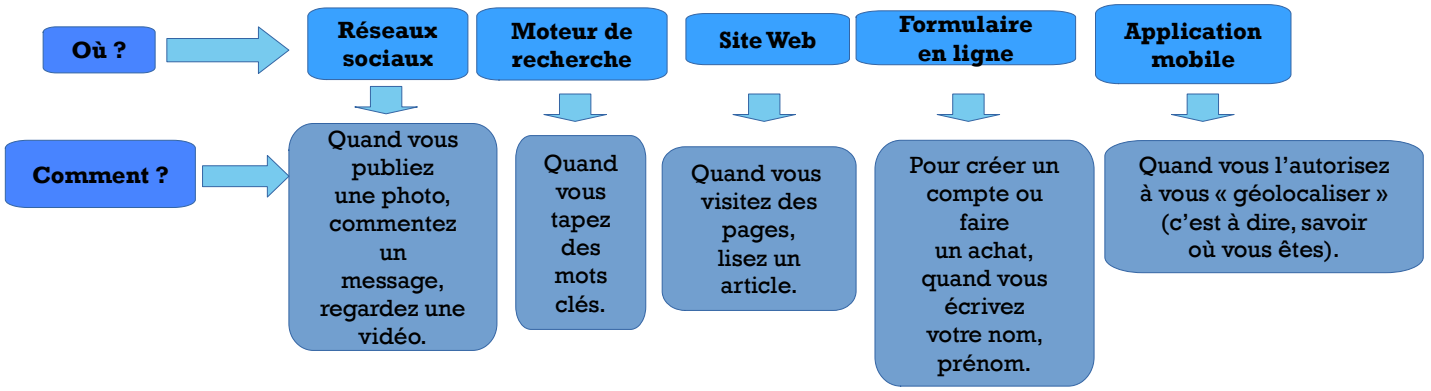
La fenêtre de navigation privée

En utilisant une **fenêtre de navigation privée** pour aller sur Internet, les **cookies** enregistrés sur votre ordinateur seront **automatiquement effacés** à la fermeture de votre navigateur.

⚠ Attention : Naviguer dans une fenêtre de navigation privée ne vous rend pas anonyme pour autant !

Les données personnelles

Chaque fois que vous **cherchez une information** sur internet ou que vous **visitez** un site, vous laissez des **informations sur vous**. On les appelle des **« données personnelles »** : elles permettent de **vous identifier**.



Le phishing (hameçonnage par mail)

Si vous recevez un mail d'un organisme public ou privé sur lequel vous avez **déjà créé un compte, ne cliquez pas sur les liens proposés.**
Connectez vous directement sur votre compte pour vérifier l'information.
Gardez à l'esprit qu'un organisme quel qu'il soit ne vous **demandera jamais** votre mot de passe ou vos coordonnées bancaires. Même votre conseiller bancaire ne connaît pas votre code d'accès à votre compte.

Pour vérifier l'**émetteur** du message, **vérifiez son adresse mail**.

L'objet du mail frauduleux évoque souvent un **sujet peu ordinaire** :

Quelques exemples :

- Un prétendu pirate aurait trouvé des vulnérabilités sur un site Internet et demande une rançon pour ne pas utiliser vos données personnelles.
- Un ami aurait grand besoin d'aide, mais refuse d'être appelé par téléphone.
- Un organisme important (votre banque, EDF, etc.) aurait perdu votre identifiant et votre mot de passe à la suite d'un incident technique.
- Une entreprise vous annonce qu'elle vous accorde un trop perçu pour une facture.
- Des félicitations pour avoir gagné un lot important lors d'un tirage au sort dont vous n'avez jamais entendu parler.

⚠ Si vous avez un doute sur un mail, contactez si possible directement l'organisme concerné pour confirmer ou non le message que vous avez reçu.

Bassens - Damien Courty - 2024