# PROJET :
# SENSIBILISATION AUX RISQUES NUMÉRIQUES

Daphné ATTOUMANI
Emilie CHELONE



***sources :***
https://www.cybermalveillance.gouv.fr/bonnes-pratiques
https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/
MOOC de l'ANSSI

# SOMMAIRE

- Les différentes cibles au sein d'une entreprise
  - Les Politiques au sein de l'entreprise
    - L'identification
      - Les mails, spams dangereux à ne pas négliger
        - Séparer le professionnel du personnel
          - Les mises à jour régulières
            - Les antivirus & VPNs

# Les différentes cibles que l'on rencontre dans une entreprise

Les principales cibles :


*De quoi pourraient-elles être victimes :*

- **Phishing** (hameçonnage) : obtenir des renseignements personnels à travers un formulaire via un site malveillant, dans le but de perpétrer une usurpation d'identité.
- **Shoulder surfing** : observer l'écran de sa cible par-dessus son épaule.
- **Keylogger** : logiciel malveillant qui enregistre l'ordre des touches tapées.
- **Ingénierie sociale** : récolte d'informations personnelles, le plus souvent frauduleusement et à l'insu de l'utilisateur, afin de déduire les mots de passe, d'accéder aux systèmes informatiques, voire d'usurper l'identité ou de conduire des activités d'espionnage industriel.

# Les politiques de l'entreprise (gestion de l'accès aux données) (1/2)



Il est important que l'accès aux données sensibles de l'entreprise soit restreintes.

Pour cela il est conseillé d'appliquer une **charte informatique** en entreprise (le but est d'informer les salariés de ce qu'ils peuvent faire et de ce qu'il doivent faire) :

-Tout employé qui quitte l'entreprise se voit **retirer de tous ses droits et accès aux données** de l'entreprise.

-La gestion des documents et informations sensibles devront être **accessibles par mot de passe**.

-**Changer les mots de passe** régulièrement.

-**Verrouiller systématiquement** son poste de travail en quittant son bureau durant les pauses et à la fin de la journée de travail.

# Les politiques de l'entreprise (gestion de l'accès aux données) (2/2)

En cas de constat d'un comportement inhabituel venant du poste de travail ou d'un serveur :

- déconnecter la machine du réseau;
- maintenir sous tension mais pas redémarrer la machine;
- prévenir la hiérarchie et le référent en sécurité des systèmes d'information.

Les appareils conseillés pour la gestion de données sensibles :

- ordinateur
- disque dur
- clé USB

Ces derniers doivent rester dans un lieu sûr, exemple : un local accessible par clé ou badge.

# Il est préférable de séparer le professionnel et le personnel

- Ne pas faire suivre les messages électroniques professionnels sur des services de messagerie personnelles.
- Ne pas héberger de données professionnelles sur les équipements personnels (clé USB, téléphone, etc.) ou sur des moyens personnels de stockage en ligne.
- Ne pas connecter de supports amovibles personnels (clés USB, disques durs externes, etc.) aux ordinateurs de l'entreprise.
- Utiliser plusieurs adresses électroniques dédiées aux différentes activités sur internet :
  - activités "sérieuses" (banques, professionnelle, etc.)
  - activités en ligne (forums, jeux concours, etc.)

Si vous voulez travailler hors bureau, **ne pas privilégier** l'utilisation d'un ordinateur/smartphone qui ne soit pas de confiance et potentiellement infecté (ordinateur libre d'accès dans un hôtel, cybercafé...).

# L’identification (1/3)

Tous sites ou applications demandent un identifiant et un mot de passe c’est pourquoi le mot passe doit être:

- suffisamment long et complexe et impossible à deviner : **12 caractères mélangeant majuscules, minuscules, chiffres et caractères spéciaux**.

Les principales attaques contre les mots de passe sont

- le **piratage par force brute** (logiciel qui essaie tous les mots de passe possible)
- le **piratage par dictionnaire** (Les mots de passe qui ont fuité forment une liste de possibilité qui permet de trouver le mot de passe de la cible)
- l’**usurpation d’identité** (l’attaquant usurpe votre identité afin de voler des données)

exemple :

mot de passe : LouLou ✗

mot de passe : H8jdf!_bsdYYU? ✓

**NE PAS TRANSMETTRE SON MOT DE PASSE A UN COLLEGUE**

**/!**

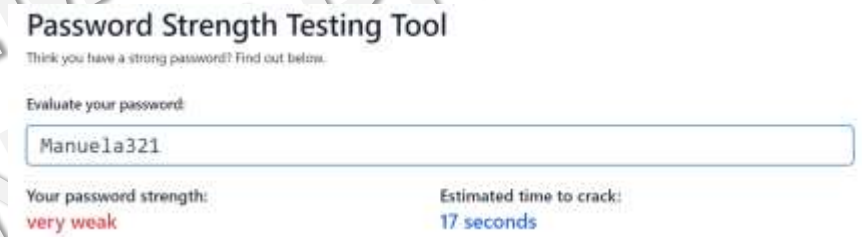
**NE PAS ÉCRIRE SON MOT DE PASSE SUR UN POST-IT COLLÉ À CÔTÉ DE SON POSTE DE TRAVAILLE**

# L’identification (2/3)

Des sites permettent d’estimer au bout de combien de temps votre mot de passe peut se faire pirater.

(/!\Ne pas utiliser son vrai mot de passe pour vérifier !)

- https://bitwarden.com/password-strength/
- https://www.csa.gov.sg/gosafeonline/resources/password-checker



# Contre-mesure possible (2/2)

- La **double identification** : recevoir un sms ou un mail avec un code provisoire pour confirmer votre identité lors de la connexion.

Possibilité de double identification pour les mails (gmail, outlook...), réseaux sociaux (snapchat, facebook...), les clouds.


- Le **gestionnaire de mot de passe** : permet de stocker ses mots de passe, qui sont protégés par un mot de passe (qui sera le seul à retenir).

- La **reconnaissance biométrique** : reconnaissance par empreinte ou faciale.

# Les mails, spams, messages indésirables(1/2)

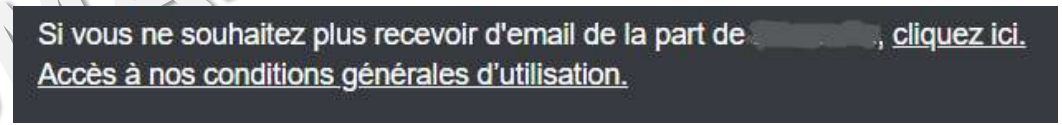
Ces messages malveillants visent à **voler vos données personnelles** ou à **transmettre un virus** via un lien.

Comment les reconnaître :

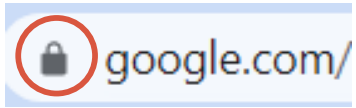
- présences de fautes d'orthographes (dans le mail et dans le nom d'utilisateur)
- message suspect

Pour **éviter de recevoir des spams**:

- À la fin de certains mails il y a la rubrique "se désabonner" qui permet de ne plus recevoir d'annonces de cet émetteur :



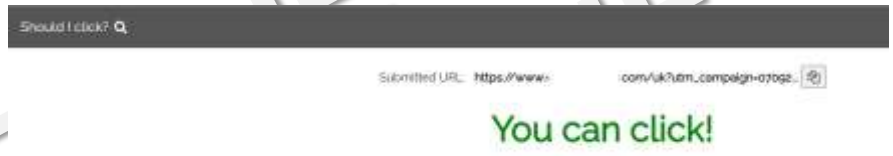

- Vider sa corbeille assez souvent
- Vérifier le cadenas dans la barre de l'URL pour être sûr de la sécurité du site



# Les mails, spams, messages indésirables(2/2)

Il existe des sites qui permettent de **vérifier la fiabilité d'un lien**.

https://www.shouldiclick.org/home.html




Ce qu'il **faut faire** dans le cas où vous avez ouvert un lien malveillant :

- **NE PAS** transmettre des données sensibles (adresse physique ou virtuelle, mot de passe, nom, prénom etc...);
- **Signaler** l'émetteur

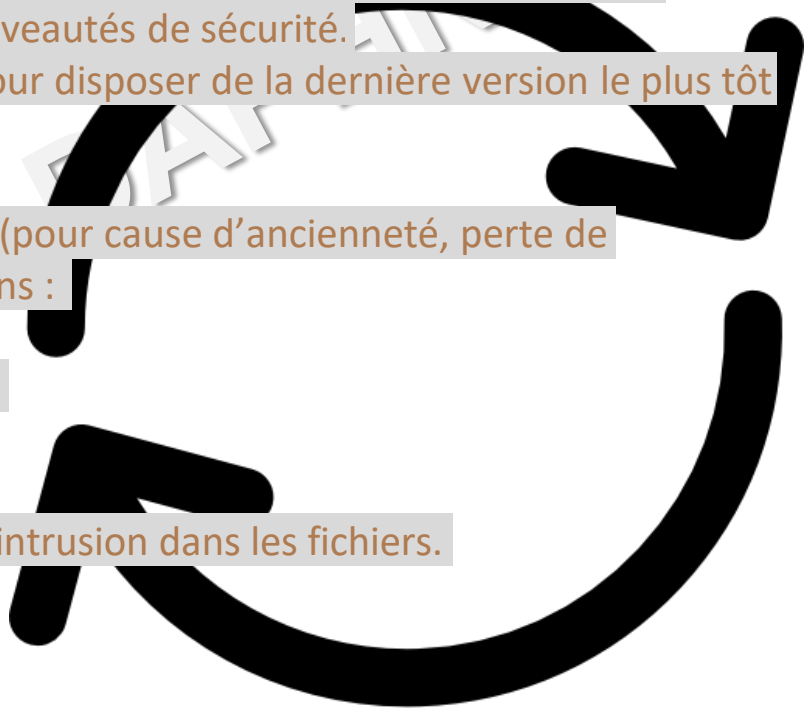
# Faire des mises à jours régulières

Il faut savoir que les mises à jour sont annoncées après avoir corrigé une défaillance dans le système, c'est pourquoi afin d'avoir les dernières nouveautés de sécurité.
Il est conseillé d'activer la mise à jour automatique pour disposer de la dernière version le plus tôt possible.

Pour les appareils qui **ne peuvent pas être mis à jour** (pour cause d'ancienneté, perte de garantie…) il est nécessaire de trouver d'autres moyens :

- en ne le **connectant pas à internet**
- en le **séparant du reste du réseau informatique**
- en **désactivant les services vulnérables**.

**Activer le pare-feu** local des postes permet d'éviter l'intrusion dans les fichiers.



# Antivirus et VPN(1/2)

Une alternative pour se protéger des attaques est d'utiliser le service de navigateur privé. Veillez à bien fermer vos sessions après utilisation et n'enregistrez jamais vos mots de passe dans le navigateur.
Vous pouvez aussi investir dans des antivirus et VPNs pour protéger l'ordinateur en local et en déplacement.

**Antivirus** : programme qui a pour but principal de détecter, neutraliser ou éradiquer les logiciels malveillants des ordinateurs et autres appareils informatiques qui sont infectés.

Il est important de le garder à jour pour qu'il soit au top de sa fonctionnalité.

ex : antivirus du logiciel, Kaspersky, Bitdefender...

# Antivirus et VPN(2/2)

**VPN** (Réseau Privé Virtuel) : service qui établit une connexion chiffrée et sécurisée entre votre ordinateur et internet.

Utile lorsque vous êtes en déplacement et que vous n'avez accès qu'à des réseaux WiFi publique et mal sécurisés. De nos jours, de plus en plus de personnes pratiquent le nomadisme, c'est-à-dire le fait de travailler depuis des endroits différents voire des pays différents. Dans ce cas, le VPN est un sécurisant fiable.

ex : NordVPN, CyberGhost...