CYBERSÉCURITÉ - CYBERTRANQUILITÉ

Pour une utilisation sereine des outils numériques

Stéphanie DUMAS
Formation informatique

lundi 8 juillet 2024

PLAN

1. SE CONNAÎTRE, C’EST SE PROTÉGER
2. COMPRENDRE, C’EST NOUS PROTÉGER
3. AGIR ET PROMOUVOIR LA CYBERSÉCURITÉ

PARTIE 1

SE CONNAÎTRE, C’EST SE PROTÉGER

DÉFINITION

- Ensemble des moyens utilisés pour assurer la **sécurité** des **systèmes** et des **données informatiques** d'un État, d'une entreprise, etc.
- Elle concerne aussi bien les **supports physiques** (papier, serveurs, ordinateurs) que **numériques** (sites internet, réseaux, accès)

- (dictionnaire le Robert)

SE CONNAÎTRE

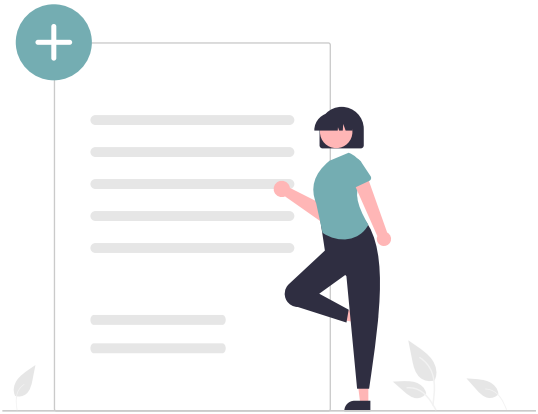
Au quotidien, comment protégez-vous :

- Vos informations personnelles ?
- Les données de vos clients ?
- Vos fichiers ?
- Vos équipements ?

BINGO DES MAUVAISES PRATIQUES PERSONNELLES

Comptez 1 point pour chaque affirmation :

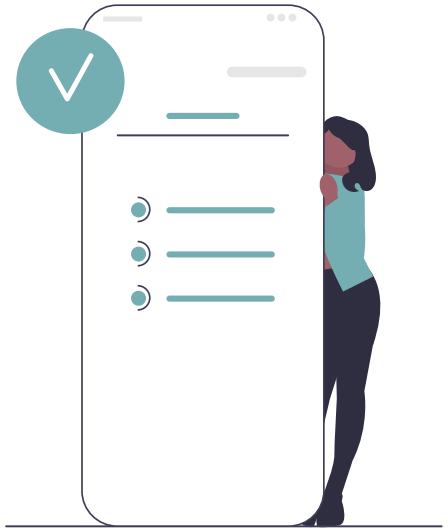
1. Je réutilise parfois/souvent le **même mot de passe**
2. Plusieurs personnes peuvent utiliser ma **session d'ordinateur**
3. Je **prête** parfois mon smartphone à mes proches
4. Certains de mes proches ont **accès** à mes mots de passe
5. J'ai ma **CNI/passeport/carte vitale** dans ma boîte mail
6. Je ne fais pas souvent les **mises à jour**
7. Je n'ai pas de mot de passe pour **déverrouiller** mon ordinateur
8. L'accès à mon smartphone est un **code à chiffres ou un schéma** à dessiner
9. Je n'enclenche jamais la **double authentification**
10. Je me connecte parfois au **Wi-Fi publics** (hôtels, gares, fast foods, entreprises, etc.)
11. Je n'enregistre jamais mes mots de passe dans **un gestionnaire**
12. Je poste des photos de mes proches et enfants sur **les réseaux sociaux**
13. Je n'ai pas d'**antivirus** et ne fais jamais de scan
14. Je ne fais jamais **de sauvegardes** de mes données



BINGO DES MAUVAISES PRATIQUES PROFESSIONNELLES

Comptez 1 point pour chaque affirmation :

1. Je n'éteins jamais ni ne mets en **veille** mon PC
2. Mes collègues peuvent se connecter à **ma session** en mon absence
3. Je consulte ma **boîte mail pro** sur mon ordinateur personnel
4. Quand je change de mot de passe je ne change **qu'un ou deux caractères**
5. Mon bureau n'est jamais **fermé à clé**
6. J'indique parfois quand je suis en vacances sur les **réseaux sociaux**
7. Je ne suis pas formé(e) au **RGPD**
8. Je **conserve** tous mes dossiers clients depuis des années
9. Mes équipes ont **accès** à tous les dossiers de l'entreprise
10. Je n'ai pas de **filtre anti espionnage** sur mon écran de PC ou de smartphone
11. Je ne vérifie pas **l'identité d'une organisation** qui me semble légitime au téléphone
12. Vos appareils ne sont pas **chiffrés** en cas de vol de matériel



QUELLE EST VOTRE PROFIL D'UTILISATEUR ?

- de 5 points

C'est pas mal du tout ! Le risque 0 n'existe pas en cyber sécurité mais vous avez compris comment limiter les risques. **Bravo.**

Entre 5 et 15 points

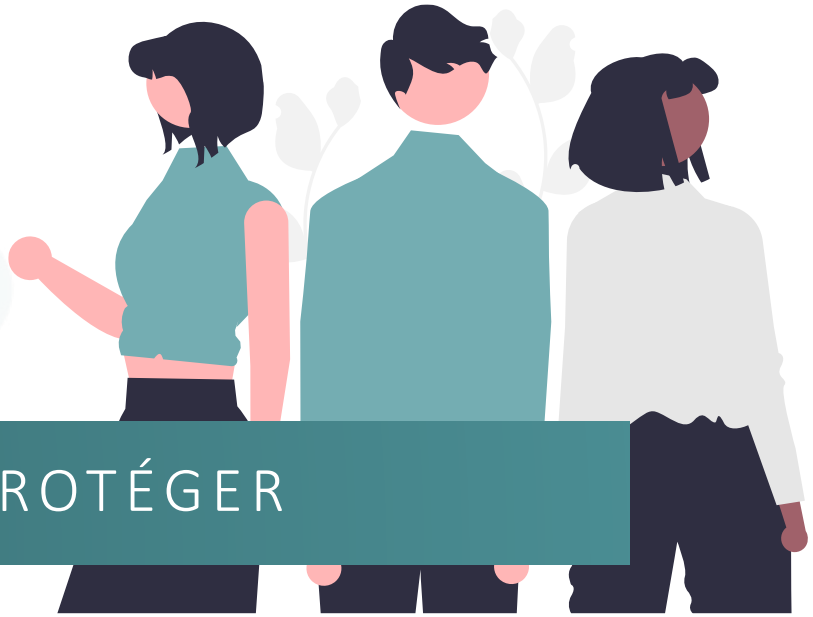
Il y a **quelques bonnes pratiques** mais il faut aller plus loin pour s'assurer davantage de protection.

+ de 15 points

Oupsi ! Il est urgent de faire quelque chose pour se protéger : le risque d'avoir des soucis importants est grand !

PARTIE 2

COMPRENDRE, C'EST NOUS PROTÉGER



SE PROTÉGER

Sécuriser son environnement informatique

COMMENCER

Stéphanie DUMAS
Formation informatique

LES PRINCIPALES SOURCES DE CYBER-INSÉCURITÉS

Personnelles

- Les mots de passe
- Les équipements partagés
- Le manque de confidentialité
- La boîte mail
- Les virus
- Le manque de MàJ

Professionnelles

- Les mots de passe
- La boîte mail
- Les accès mal protégés (Win + L)
- L'ingénierie sociale
- L'accumulation documentaire

FOCUS SUR LES INSÉCURITÉS PROFESSIONNELLES

Les mots de passe

- Ce sont les **accès principaux** à tous nos comptes utilisateurs. Un mot de passe trop léger ou réutilisé est une porte ouverte vers toutes nos autres données. Ils sont **la cible principale des pirates** car faciles à trouver la plupart du temps.

Les accès mal protégés

- Qu'ils soient **physiques** (un bureau par exemple) ou **numériques** (un compte utilisateur), il est important de savoir **QUI** a accès à **QUOI**. Ainsi, les risques de fuites, de vol ou de destruction sont limités.

L'ingénierie sociale

- Gare aux personnes naïves qui ont la **langue trop pendue**. L'ingénierie sociale consiste à **endormir votre vigilance** en vous faisant croire que vous avez à faire à quelqu'un de confiance pour lui **donner les informations** dont il a besoin.

FOCUS SUR LES INSÉCURITÉS PROFESSIONNELLES

Le phishing

- Pratique consistant à vous envoyer **un mail réaliste** afin de vous soutirer des informations ou de l'argent. L'auteur du mail sème le doute et **joue sur votre confiance** pour arriver à ses fins.
- https://safeonweb.be/fr/apprenez-reconnaitre-les-e-mails-frauduleux

L'accumulation

- **Le RGPD** vous oblige à faire fréquemment le ménage dans vos fichiers et papiers afin **d'éviter de conserver des informations** dont vous n'avez plus besoin mais qui pourraient permettre à des personnes mal intentionnées de **profiter de vous ou de vos clients**.

Les mises à jour

- Les mises à jour garantissent à vos appareils **les dernières options de sécurité** du concepteur. Ne pas les faire laisse la porte ouverte aux pirates pour utiliser des failles connues.

PARTIE 3

AGIR ET PROMOUVOIR LA CYBER SÉCURITÉ

BILAN ET TOUR DE TABLE FINAL

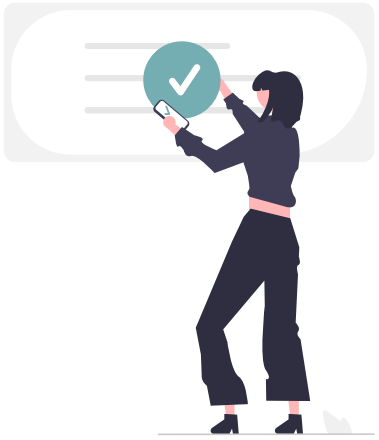
LES BONNES PRATIQUES À ADOPTER

À la maison

1. Je ne réutilise JAMAIS le **même mot de passe**
2. Personne ne doit avoir accès à ma **session d'ordinateur**
3. Je ne **prête pas** mon smartphone sans surveillance
4. Je ne communique mes **mots de passe** à PERSONNE
5. Je **supprime** mes documents personnels de la boîte mail
6. Je fais systématiquement mes **mises à jour** d'appareils/logiciels
7. Je mets un mot de passe à ma **session admin** et je **chiffre** mon ordinateur
8. Si possible je verrouille mes appareils par **mon empreinte digitale** ou mon visage
9. Dès que je peux, j'enclenche la **double authentification**
10. Je ne me connecte jamais aux **wi-fi publics,** j'utilise plutôt la 4G
11. J'utilise correctement mon **gestionnaire de mots de passe**
12. Je ne donne **aucune information personnelle** sur les réseaux sociaux ou internet
13. Je mets un **antivirus** sur mon ordinateur et fais mes scans régulièrement
14. Je fais des **sauvegardes régulières** de mes données, sur un disque dur ou un coffre fort numérique par exemple

LES BONNES PRATIQUES À ADOPTER

Au travail



1. J'**éteints** toujours mon PC en fin de journée et le **mets en veille** quand je quitte la pièce (même 10 minutes)
2. **Personne** à part mon directeur et le service informatique ne doivent avoir accès à **mes identifiants**
3. Je ne **consulte pas** mes mails sur mes appareils personnels
4. Je change **intégralement** de mot de passe quand demandé
5. Je **sécurise les espaces physiques** où sont stockées mes données et appareils
6. Je ne donne pas **d'information sur mon activité** en dehors de mon réseau professionnel
7. Je me forme, moi et mes équipes, au **RGPD**
8. Je fais **régulièrement le ménage** dans mes données
9. Je **configure les accès** selon les salariés
10. Je mets un **film de confidentialité** sur tous mes écrans
11. Je **vérifie l'identité** des organisations qui me demandent des informations
12. Je **chiffre** mes ordinateurs pour protéger les données en cas de vol

ET QUAND C'EST TROP TARD, QUE FAIRE ?

AGIR :

1. **Déconnecter** ses appareils du réseau internet (Wi-fi et drive)
2. NE **PAS éteindre** son PC
3. Ne **pas payer** de rançon
4. Appeler le **service informatique**
5. Ne **plus toucher** à l'appareil
6. **Prévenir** les équipes

ALERTER :

- Le service ou l'entreprise **informatique**
- Les **sous-traitants** et **partenaires**
- La **CNIL** sous 72 h
- Les **clients**
- La **police/gendarmerie**
- Les **assurances**

SE RELEVER :

- **Former** ses équipes
- **Protéger** ses locaux
- Initier des **sauvegardes régulières**
- Verrouiller **les accès**
- Changer tous **les mots de passe**
- **Chiffrer** les données et appareils
- Tenir des **registres de sécurité** informatique à jour

AVEZ-VOUS BIEN RETENU ?

https://forms.gle/VsezC5bWD9ukM8mq9

LES RESSOURCES UTILES

- Conseil et assistance en cas de cyberattaque : https://www.cybermalveillance.gouv.fr/
- Notification de vol de données auprès de la CNIL : https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles
- Les bonnes pratiques de cybermalveillance.gouv : https://www.cybermalveillance.gouv.fr/bonnes-pratiques
- Dénoncer :
  - Les spams vocaux et sms : https://www.33700.fr/
  - Les mails de phishing : https://www.signal-spam.fr/
  - Du contenu illicite sur internet : https://www.internet-signalement.gouv.fr/PharosS1/
  - Une arnaque sur internet : https://www.service-public.fr/particuliers/vosdroits/N31138

Stéphanie DUMAS
Formation informatique

MERCI