Password ou passoire, protège ton compte

Un atelier autour des mots de passe et de la gestion des clés d'accès à vos différents comptes.
#password
#cybersécurité

visuel généré par et pour le festival ***Nothing2Hide Decentralized***

Public : Tout public intéressé par le sujet de la cybersécurité et des solutions pour protéger l'accès à ses données

Durée : 2h30 à 3h

Objectifs : En fonction du niveau de compétences numériques des différents usagers les objectifs suivants pourront être abordés

- ☐ Comprendre pourquoi les mots de passe sont vulnérables
- ☐ Expliquer comment les pirates cassent les mots de passe (force brute, dictionnaire, réutilisation)
- ☐ Créer un mot de passe solide et mémorisable
- ☐ Identifier les bonnes pratiques de gestion des mots de passe
- ☐ Activer la double authentification (2FA)
- ☐ Utiliser un logiciel/gestionnaire de mots de passe (selon le public)

Matériel : Pour le médiateur ordinateur et vidéoprojecteur et un accès à Internet, jeu "Devine mon mot de passe", feuilles et stylos, fiche participant.

Déroulé : Pour permettre un engagement maximal du public d'un atelier collectif il convient de bien maîtriser les phases d'engagements du public (par des mises en situations, des questionnements implicatifs ou encore de la mise en pratique) et les phases plus descendantes de partage d'information.

| Introduction

- Questionner : “Quand utilise-t-on un mot de passe ? A quoi sert un mot de passe ? Combien de mot de passe différent avez-vous ? Est-ce que vous utilisez parfois le même mot de passe pour des comptes différents ?
- Faire émerger les représentations : Faire une comparaison avec les clés de la maison
- Expliquer l’importance des mots de passes dits “forts” : 81 % des piratages sont liés mots de passe faibles selon l’étude de Verizon de 2018
- Proposer au public de tester si l'un de leur mot de passe fait partie d'une fuite de données via https://haveibeenpwned.com/Passwords

| Jeu : Devine mon mot de passe (voir fiche jeu)

Objectif du jeu : voir que plus il y a d’éléments différents dans un mot de passe plus il est difficile de le trouver.

· Étape 1 : deviner une couleur
· Étape 2 : couleur + symbole
· Étape 3 : couleur + symbole + chiffre

| Comment les pirates cassent les mots de passe

· ***Attaque par Force brute :*** par le biais d’un programme lancé sur une machine un test de toutes les combinaisons de caractères possibles est lancé. Cette méthode est la plus simple pour déchiffrer les mots de passe courts ou ceux composés d'un seul ensemble de caractères comme des chiffres uniquement.

· ***Attaque par Dictionnaire :*** via un programme spécialisé, tout comme pour l’attaque par force brute, l’attaque par dictionnaire va se baser sur une liste prédéfinie de mots de passe récupérée dans les fuites de données plutôt que sur une suite logique.

· ***Attaque par Credential stuffing*** : cette attaque consiste à réaliser, à l'aide de logiciels, des tentatives d'authentification massive sur des sites et services web à partir d'un même couples identifiants/mots de passe (généralement, une adresse électronique et un mot de passe) trop souvent utilisés sur différents comptes.

Toutes ces attaques sont automatisées avec des machines de plus en plus puissantes leur permettant de faire un nombre de calculs monstrueux en quelques secondes - jusqu'à 200 milliards de tests par seconde avec les derniers processeurs graphiques comme la RTX 5090.

Video Konbini - https://www.youtube.com/watch?v=YI-6nZFxwNg - jusqu'à 2'35

Une étude de Kaspersky publiée le 7 mai 2026 indique que d'après leurs test qui se base sur +231 millions de mots de passe qu'on peut trouver sur le dark web et tirés de fuites ayant eu lieu entre 2023 et 2026, 48% des mots de passe sont craqués en moins d'une minute et 60% en moins d'une heure.

L'étude indique aussi que les suites de chiffres et les dates de naissance sont trop souvent présentes dans les mots de passe. Du côté des caractères spéciaux, le symbole @ arrive largement en tête : il figure dans un mot de passe sur dix. Le point arrive en deuxième position, suivi du point d'exclamation.

Vérification de la robustesse d'un mot de passe
https://nothing2hide.org/fr/verifier-la-robustesse-de-votre-mot-de-passe/

Psyomjesus, CC BY-SA 4.0 via Wikimedia Commons

| Créer un mot de passe solide

Un mot de passe solide doit être suffisamment long et complexe en intégrant des lettres (majuscules et minuscules), des chiffres, de la ponctuation, des caractères spéciaux et n'avoir aucun rapport avec votre vie personnelle.

Quelques méthodes de création

1. Méthode des premières lettres : méthode qui consiste à retenir les premières lettres d'une phrase comme une citation, un proverbe, ou encore les paroles d'une chanson. Par exemple : « Qui voit Ouessant voit son sang, qui voit Sein voit sa fin » donne QvOss,QvSvsf ou « Horizon pas net, reste à la buvette » qui donnerait HpN,r@Lb, des mots de passe qui pourraient être amélioré et plus sécurisés avec l'ajout de chiffres.

2. **Méthode phonétique :** méthode qui consiste à utiliser la phonétique, c'est-à-dire à retenir les sons de chaque syllabe (comme dans les SMS) pour fabriquer une phrase facile à retenir. « J'ai eu deux cadeaux à Noël » devient « Gu2KdO@nowel ».

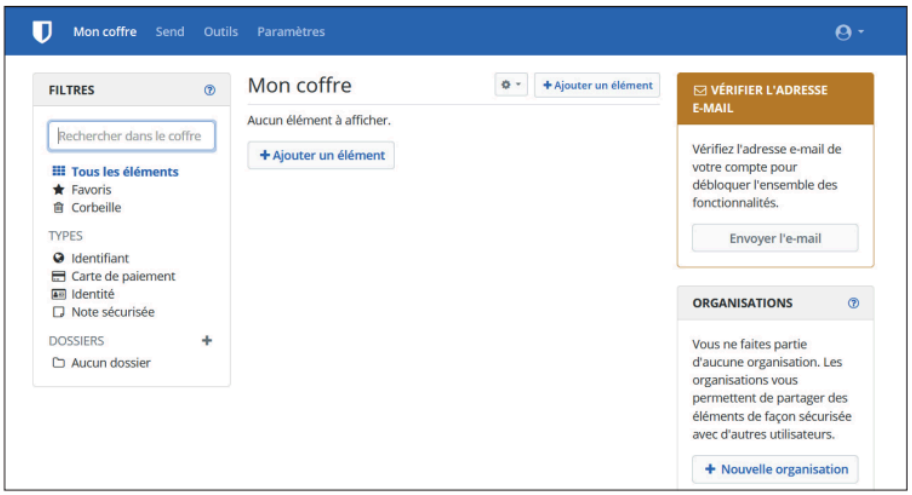
3. **Méthode du site modifié :** méthode qui utilise le nom du site sur lequel vous créez le compte avec votre mot secret, votre date d'inscription sur ce site et quelques caractères spéciaux bien placés. Par exemple avec une inscription sur le site de la FNAC le 15 mai dernier « !15Fnac05GwenHaDu26? »

4. **Méthode de phrase de passe :** méthode où l'on utilise une succession de mots simples sans lien entre eux, en ajoutant quelques signes spéciaux, majuscules et chiffres. Par exemple « LesPoulesDansentÀMinuit! »

Outils : le générateur de mots de passe de Proton Pass ou celui de motdepasse.xyz

| Gestionnaires de mots de passe
Bitwarden, KeepassXC sur Les Bases ou sur le site du cnam ou encore Proton Pass, qui sont des outils numériques à prendre en main.

B



Avantages : un seul mot de passe maître, stockage chiffré, auto-remplissage … un outil intéressant mais qu'il faut apprendre à l'utiliser !

Recommandation : éviter les gestionnaires intégrés aux navigateurs car ils peuvent avoir des failles (dernièrement le gestionnaire de mots de passe du navigateur Edge a été critiqué car il donnait accès en clair aux données stockées dans ce gestionnaire (voir la vidéo sur le site de Korben.info) …

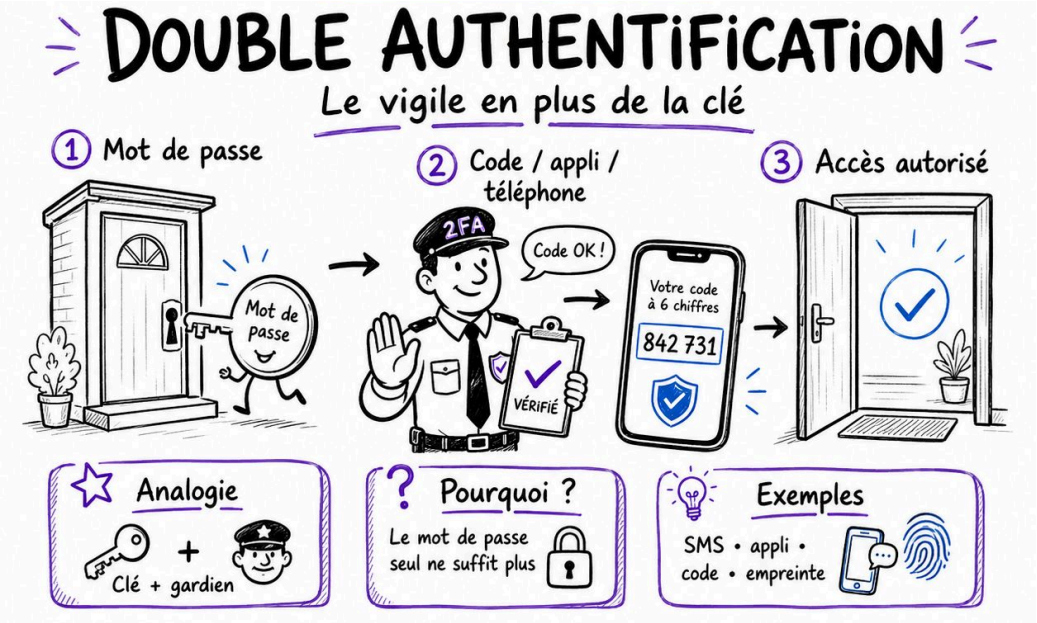
Solution : désactiver dans les paramètres de votre navigateur la possibilité d'enregistrer automatiquement les mots de passe !

Et les noter dans un calepin ? Si cela peut paraître dangereux (car on peut le voler) il est certain qu'il ne pourra pas être piraté à distance, ni par intrusion dans l'appareil. Le carnet, s'il est bien utilisé, permet d'adopter une méthodologie sécurisée en encourageant à utiliser un mot de passe différent par service, puisqu'on ne dépend plus de sa mémoire seule, à proposer des mots de passe plus longs, plus robustes, parce qu'ils sont notés.

Hack du calepin : ces mots de passe notés dans le calepin peuvent être une version tronquée du véritable mot de passe, car chaque mot de passe noté peut disposer d'un élément complémentaire qui lui reste mémorisé comme un mot court mais personnel qui sera

à rajouter à chaque fois. Cela renforce la sécurité tout en stimulant les capacités de mémorisation.

| La solution de la Double authentification 2FA
L'authentification à deux facteurs est une méthode de sécurité qui ajoute une seconde couche de vérification d'identité. Au lieu de se fier uniquement à un mot de passe, la 2FA (*two-factor authentication*) exige que vous confirmiez votre identité en utilisant un deuxième facteur d'identification distincts.



Source : Aide en Informatique

| Changer souvent de mot de passe ?
Une mauvaise "bonne" idée ! C'est ce que rappelle la CNIL dans sa nouvelle recommandation sur les mots de passe du 17 octobre 2022 en s'appuyant sur les « recommandations relatives à l'authentification multifacteur et aux mots de passe » publiées par l'ANSSI en 2021.

En effet, plusieurs études ont démontré que « forcer l'utilisateur à changer son mot de passe à une fréquence régulière n'est pas une mesure réellement efficace ».

En pratique, lors du renouvellement contraint du mot de passe, la majorité des utilisateurs utilise un nouveau mot de passe très proche du précédent, en ajoutant un caractère. La CNIL précise que « les bénéfices en termes de sécurité sont ainsi mineurs et largement contrebalancés par l'expérience utilisateur négative ».

| Conclusion
On refait un point sur les éléments importants à retenir et on répond aux questions éventuelles qui peuvent être posées par les participants à l'atelier.

1. Un mot de passe doit être long, complexe et unique, on utilise un mot de passe par compte !
2. Quand cela est proposé on active la double authentification.
3. Si vous apprenez qu'un site où vous avez un compte a été piraté, pensez à changer votre mot de passe (si cela ne vous a pas déjà été proposé par le site).

Outils : Des outils à utiliser pendant l'atelier

1. Générateur de mot de passe solide en ligne (CNIL)
2. Vérifier la robustesse de votre mot de passe (Nothing To Hide)
3. Mon mot de passe est-il compromis ? (HaveIbeenPwned)

Ressources : Quelques liens vers des sites ressources pour en savoir plus, pour approfondir le sujet, pour s'informer mais aussi pour s'inspirer ...

- ☐ Les conseils de la CNIL pour un bon mot de passe
- ☐ Les mots de passe, 2 kits pédagogiques proposés par Emmaüs Connect
- ☐ Fiches pédagogiques - Wiki Nothing To Hide