Les formations aux usages du numérique

Les mots de passe…

… sans les maux de tête

2024

Rodrigue Galani

Centre de **culture numérique**
Université de Strasbourg

Objectifs de la séance

Les usages du numérique se multiplient mais également **le nombre et la diversité des menaces pour les individus comme pour les organismes privés et publics.**

Ces menaces peuvent concerner votre ordinateur, le réseau, les bases de données et autres serveurs.

Elles peuvent se manifester par un piratage (intrusion) mais également sous d'autres formes (dégradation du fonctionnement, du matériel…).

Le plus souvent c'est un manque d'information et de formation qui sont l'origine des pratiques à risque.

- Nous allons voir ensemble quelque unes des menaces qui peuvent se présenter à vous, qu'elles concernent votre poste de travail à l'université ou votre ordinateur personnel.
- Nous verrons également les pratiques qui présentent un risque important et malheureusement souvent répandues.
- Bien entendu, je soulignerai les pratiques que vous pouvez adopter pour réduire les risques.

Les faits

Pour le grand public et les entreprises on observe que les déclarations de cybermalveillance sont en constante augmentation (et tout n'est pas déclaré) : **Depuis 2017, plus de 950 000 demandes d'assistances arrivent sur la plateforme cybermalveillance.gouv.fr qui a comptabilisé plus de 280 000 demandes d'assistance en 2023.**

Les effets peuvent concerner uniquement la sphère privée ou la sphère professionnelle. Parfois ils s'étendent de l'un à l'autre.

- Fuite de données personnelles > rançons, usurpation d'identité, fraudes
- Fuite de données sensibles > vol de données bancaires , de propriété intellectuelle
- Dégâts matériels et immatériels > matériel à remplacer, perte ou corruption de données…

D'après une étude (Asterès, 2023), les cyberattaques réussies en France durant l'année 2021 ont coûté 2 milliards d'euros dans les organisations

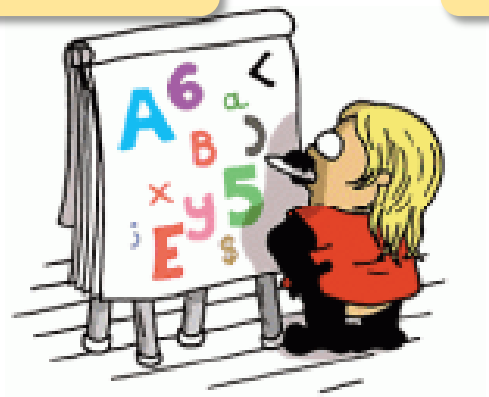
Les étapes à risque

Identifier : Qui êtes-vous ? Réponse: Pseudo, Login, Nom d'utilisateur, Identifiant

Authentifier : Etes-vous bien qui vous dites ? Réponse : Mot de passe, code chiffré, données biométriques…

Dans le langage courant on dira identification pour les deux phases.

Création



Conservation

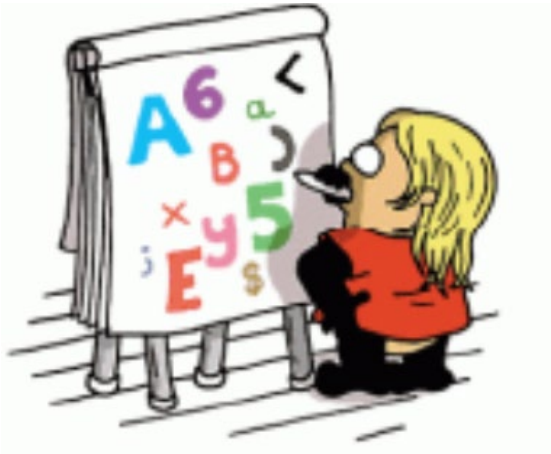
Authentification

Et autres causes "techniques d'intrusion

Le point faible de la sécurité : **NOUS** (85% des problèmes de sécurité sont liés à l'utilisateur).

Création du mot de passe

La grande majorité des mots de passes sont trop **faibles. Le renforcer consiste à allonger le temps que l'on peut prendre pour le découvrir.**



Dans un article de Francenum (2023) on nous rappelle qu'un mot de passe robuste en 2020 l'est beaucoup moins en 2023. **En conséquence, il faut changer nos mots de passe régulièrement en les renforçant à chaque fois d'avantage.**

COMBIEN DE TEMPS FAUT-IL À UN PIRATE POUR TROUVER VOTRE MOT DE PASSE EN 2023 ?

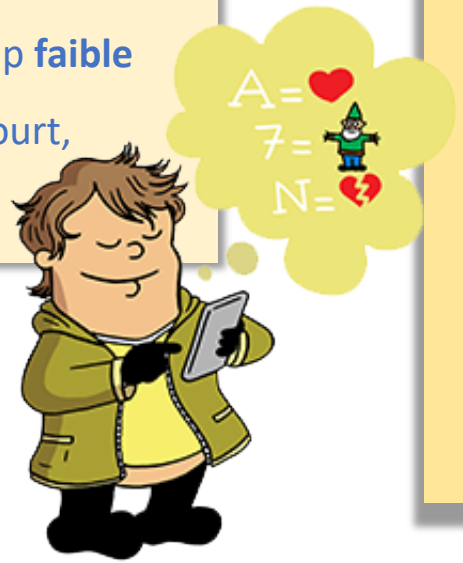
Nombre de caractères	Nombres seulement	Lettres minuscules	Lettres majuscules et minuscules	Nombres, lettres majuscules et minuscules	Nombres, lettres majuscules et minuscules, symboles
4	Immédiat	Immédiat	Immédiat	Immédiat	Immédiat
5	Immédiat	Immédiat	Immédiat	Immédiat	Immédiat
6	Immédiat	Immédiat	Immédiat	Immédiat	Immédiat
7	Immédiat	Immédiat	1 seconde	2 secondes	4 secondes
8	Immédiat	Immédiat	28 secondes	2 minutes	5 minutes
9	Immédiat	3 secondes	24 minutes	2 heures	6 heures
10	Immédiat	1 minute	21 heures	5 jours	2 semaines
11	Immédiat	32 minutes	1 mois	10 mois	3 ans
12	1 seconde	14 heures	6 ans	53 ans	226 ans
13	5 secondes	2 semaines	332 années	3 000 années	15 000 ans
14	52 secondes	1 an	17 000 ans	202 000 ans	1 million d'années
15	9 minutes	27 ans	898 000 ans	12 millions d'années	77 millions d'années
16	1 heure	713 ans	46 millions d'années	779 millions d'années	5 milliards d'années
17	14 heures	18 000 ans	2 milliards d'années	48 milliards d'années	380 milliards d'années
18	6 jours	481 000 ans	126 milliards d'années	1 trillion d'années	26 trillions d'années

Infographie FRANCENUM.GOUV.FR Source : Hive Systems

Les mots de passe faibles

Vol de mdp par attaque brute

Le pirate tente d'entrer sur un compte simplement en essayant **les identifiants les plus probables**, c'est-à-dire votre adresse de courriel ou votre nom et un mdp **faible** (mdp créé avec des éléments accessibles, trop court, fréquent…)

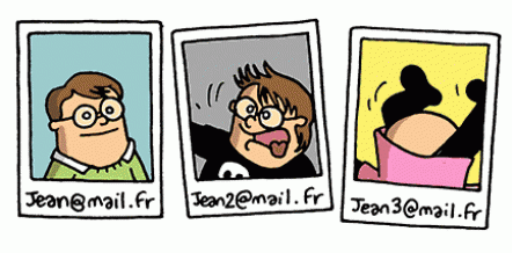


Pensez à utiliser des adresses de courriel (ou l'identifiant) différentes

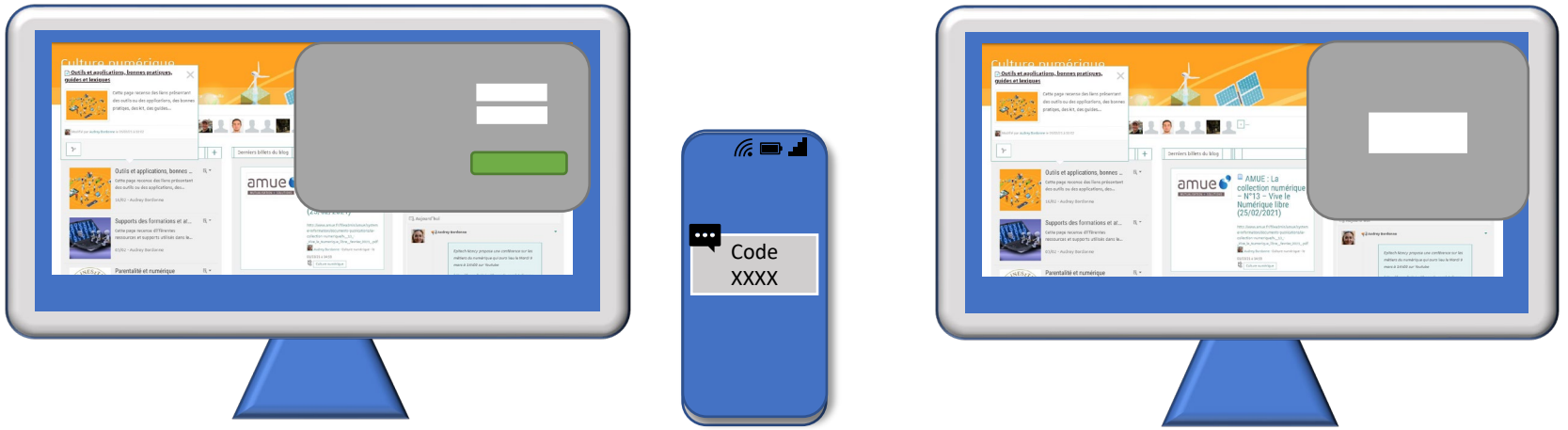
La réponse : renforcer

Pensez à créer des mdp forts

- ❑ Qui ne contiennent pas des éléments de votre vie privée (que l'on peut trouver facilement)
- ❑ Qui ne sont pas issus du dictionnaire
- ❑ De taille supérieure à 12 caractères
- ❑ Différents pour chaque compte en ligne
- ❑ Essayez le "cryptage" d'une phrase
  https://motdepasse.unistra.fr/



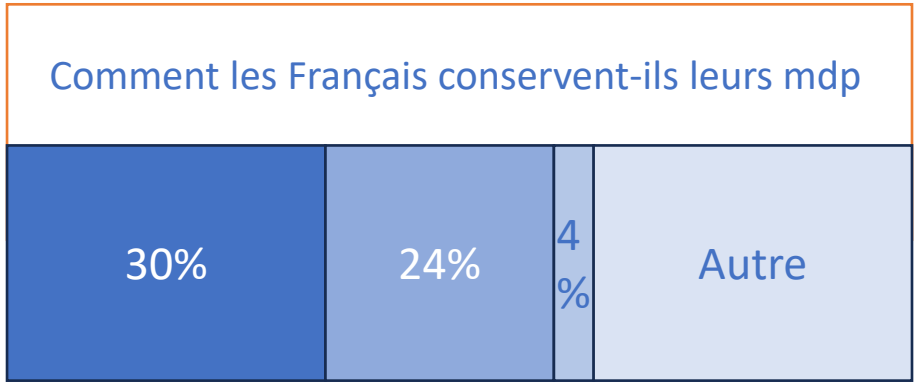
Renforcer la méthode d'authentification : la double authentification



Après l'authentification par mdp, le site web vous envoie un texto (sms) OU un courriel avec **un code unique** que vous devez reproduire à l'invite de la page. **Des applications pour smartphones peuvent également servir d'intermédiaire pour générer ce code.** L'utilisation de votre téléphone ou de votre messagerie devient ainsi une preuve (supplémentaire) de votre identité.

Cette **méthode d'authentification est dite "forte"**. Elle est recommandée par la CNIL dans ses derniers guides

Stockage des mots de passe



Pratiques à risque

Les mots de passe notés sur un carnet ou sur un post-it sont monnaie courante, rien de plus simple alors pour une personne malintentionnée de les récupérer.

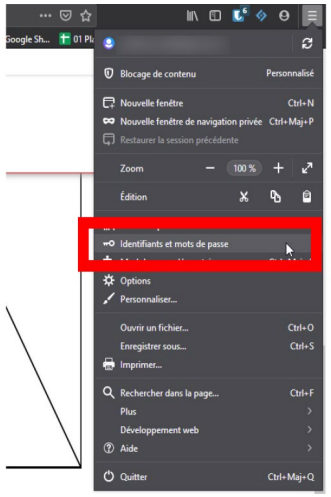
Les mots de passe conservés dans le navigateur. Si vous n'avez pas mis en place une sécurité supplémentaire, toute personne ayant accès à votre ordinateur peut les lire. De manière générale les navigateurs sont mal protégés.

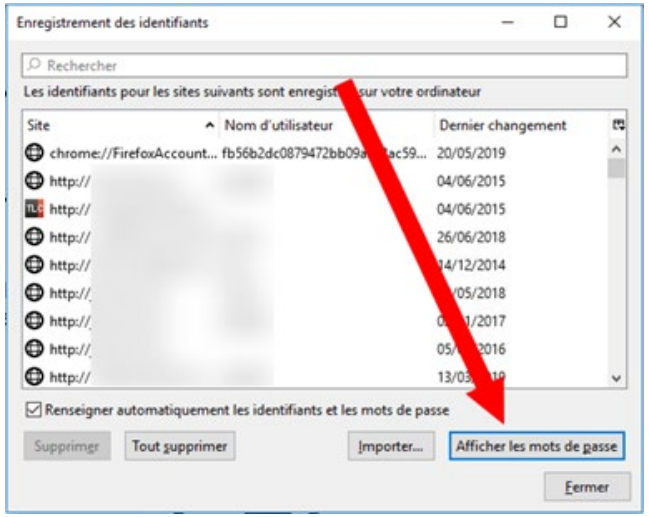
Les mots de passe stockés dans un fichier en ligne n'offrent pas beaucoup plus de sécurité car ils ne sont que rarement protégés par un mot de passe ou un chiffrement du contenu. En accédant au lien qui a pu être envoyé par messagerie on retrouve facilement le fichier et son contenu.

Pourquoi le stockage dans un navigateur est-il dangereux ?

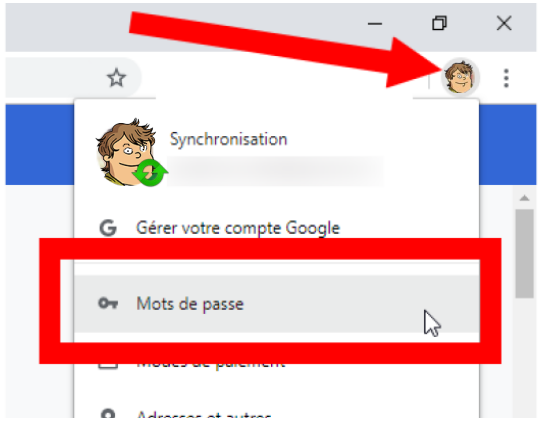
Facile à trouver et menacé par des virus de type "stealer" .

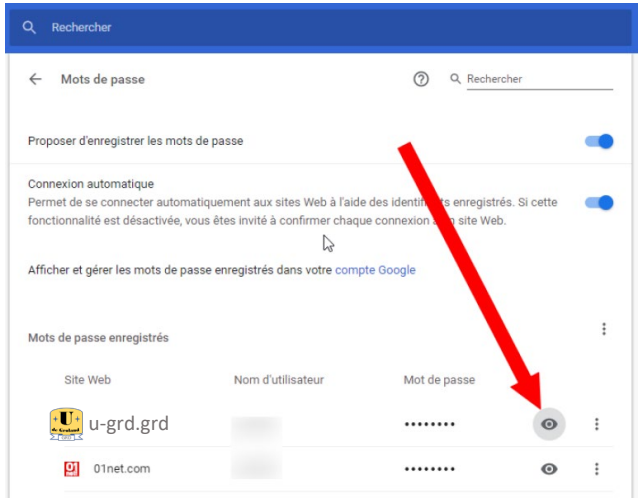
Firefox





Chrome





La réponse

Un mot de passe est personnel et doit rester invisible :

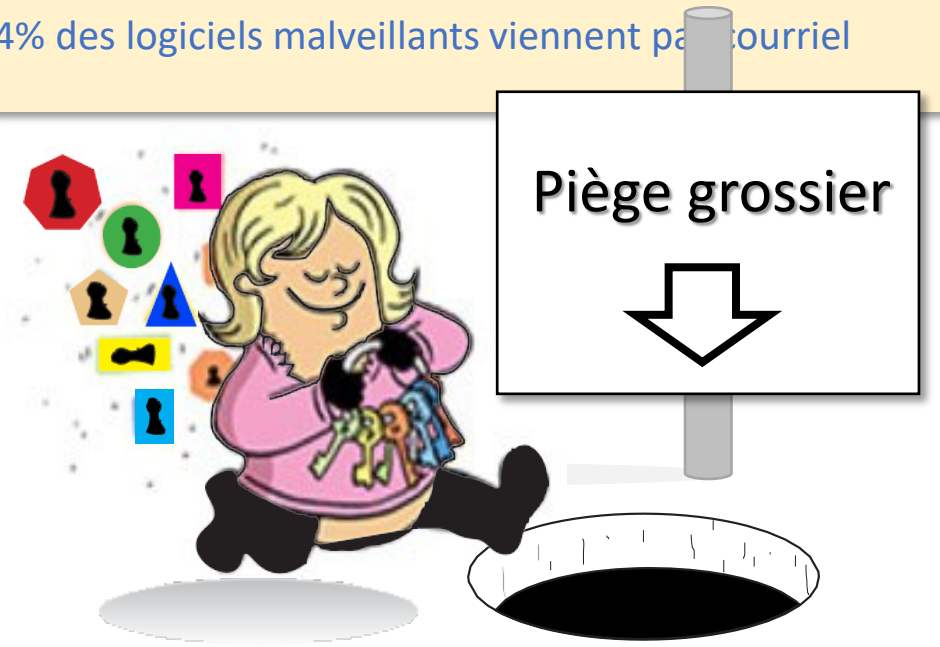
- ❑ Ne le notez nulle part,
- ❑ Ne laissez pas votre navigateur l'enregistrer,
- ❑ Ne le transmettez jamais, même oralement à qui que ce soit
- ❑ Ne répondez pas si on vous le demande
- ❑ Renouvelez-le au moindre doute

Identification et authentification

L'hameçonnage (phishing)

Lors de l'envoi d'un courriel, le cybercriminel se fait passer pour un tiers de confiance (université, banque, site de vente en ligne) afin d'obtenir vos identifiants, ou vous diriger vers un site web frauduleux.

94% des logiciels malveillants viennent par courriel



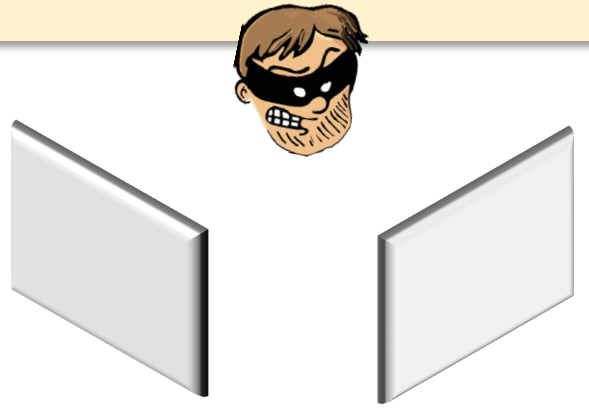
Les bonnes pratiques

- ❑ **Ne cliquez pas sur un lien dans un message**, tapez l'adresse que vous connaissez ou utilisez vos favoris pour vous rendre sur le site officiel
- ❑ **Ne répondez jamais** et si vous avez un doute : vérifiez le courriel (glissez la souris sur l'adresse sans cliquer, si l'adresse est inconnue ou étrange…).
- ❑ **Ne répondez pas aux demandes d'identifiants**

Aucun organisme ne vous demandera vos mots de passe, jamais.

Virus dérobeurs ("stealers")

Depuis 2022 on constate une augmentation des usurpations de comptes. Souvent c'est sur ordinateur privé qui en est la source : installation de logiciels depuis un sites peu protégé, support de stockage qui passe d'un ordinateur à un autre, peu ou pas de protection de l'ordinateur…Un virus de type "stealer" s'installe et laisse fuiter les données comme les mots de passe dans le navigateur. Les identifiants ont été volés vont être revendus ou utilisés.



Vol de mdp par espionnage

Dans ce cas le programme malveillant est un "keylogger". Le programme enregistre les sites visités et les touches que vous utilisez lors de votre authentification sur un site.

La réponse

- ❑ **Ne téléchargez que des logiciels originaux sur le site de l'éditeur.**
- ❑ **Protégez votre ordinateur avec un logiciel de qualité et mettez-le à jour régulièrement (l'antivirus comme l'ordinateur)**
- ❑ **Vérifiez le support mobile (clé USB, disque dur externe) avec un antivirus avant d'ouvrir un fichier qu'il contient**
- ❑ **Évitez les usages mixtes (comptes pro sur PC privé et inversement)**
- ❑ **Désinstallez les logiciels inutiles vous réduisez la "surface d'attaques" possibles**
- ❑ **Faites de sauvegardes**

Conseils pour les antivirus

Attention aux classements commerciaux, aucun antivirus n'est parfait, tous ont des faiblesses et des point forts.

Liste non exhaustive* : Bitdefender (30€), Norton (35€), Eset Nod32 (55€), McAfee (38€/an), Gdata (50€/an)

* Prix 2024 (hors promo) de la protection de base proposée qui peut être différente d'un éditeur à l'autre

Oublier les mdp et les maux de tête avec les gestionnaires de mots de passe

Également appelé coffre-fort (en angl. *Vault*) ou trousseau d'accès chiffré, le gestionnaire de mdp est un logiciel installé sur votre ordinateur, un support externe (clé USB par exemple) ou encore sur un serveur distant.

Il stocke les triplets identifiants + mdp + adresse associée. Les données sont chiffrées.

Il ne s'ouvre qu'avec un **mot de passe maître que vous êtes seul à détenir**.

La CNIL (Commission nationale de l'informatique et des libertés) comme l' ANSSI (Agence nationale de la sécurité des systèmes d'information) conseillent l'utilisation d'un gestionnaire de mot passe.

Une fois le logiciel installé et le mot de passe maître choisi, vous enregistrer vos mots de passe un à un ou les importer (si vous les avez stockés sur votre navigateur par exemple).

Ensuite il suffira d'ouvrir le gestionnaire avec le mot de passe maître pour accéder à tous les mdp de vos comptes.
En un clic les champs sont remplis sans même devoir les taper.
Le mot de passe maître doit être fort.

- ❑ Vous ne devez retenir qu'un seul mot de passe
- ❑ Vous pouvez rendre tous vos mdp très complexes
- ❑ Vous bénéficiez souvent de bonus pratiques : générateur de mdp complexes, enregistrement automatique des nouveaux mdp, stockage de documents importants et des données bancaires, remplissage automatique des formulaires en ligne, version pour mobiles…etc.

Attention : le mot de passe maître n'est pas récupérable et ne bénéficie pas de l'option "mot de passe oublié"

Choisir son gestionnaire de mot de passe

Parmi les logiciels la CNIL conseille :

- **KeepassXC** (conseillé et certifié par l'ANSSI également)
- ZenyPass
- Passwordsafe

KeePass,
RoboForm, LastPass,
Keeper, Dashlane, Password,
Sticky Password, BitWarden, 1Password,
Enovacom, Avira, Kapersky,
Password Boss,
Cyclonis, Zenyway, Passwordsafe

Sinon en 2023 les plus reconnus sont :

KeepassXC , gratuit > français et opensource

Passwordsafe, gratuit > allemand et opensource

Bitwarden, gratuit en illimité. Payant pour des fonctions supplémentaires (10 €/an) > Etats-Unis

ZenyPass, gratuit jusqu'à 15 identifiants. Payant pour plus (49€ sans abonnement) > français et opensource

Dashlane, gratuit pour un appareil. Payant pour tous vos appareils (33€/an) > Etats-Unis

NordPass, Payant (18€/an avec un abonnement de deux ans) > Panama

1Password, Payant (36€/an) > Canada

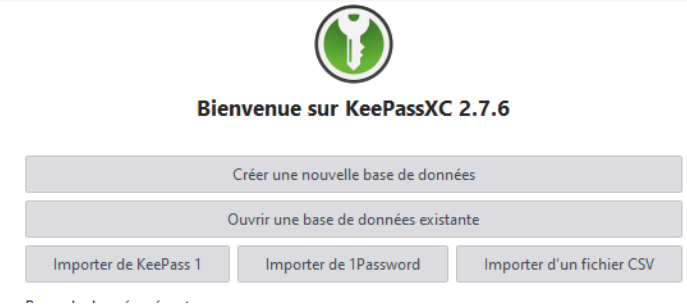
Seul Keepass permet de choisir le support de stockage de vos mots de passe (disque, clé usb, cloud…)

L'exemple de KeePassXC

L'application peut être installée sur tout appareil fonctionnant avec Windows, MacOS ou Linux. Elle peut également être installée sur un support externe. Le site de l'éditeur.

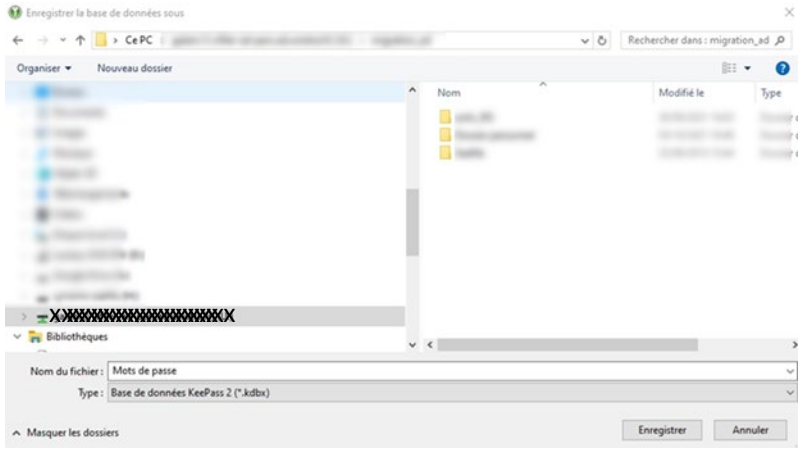
Elle est gratuite (mais vous pouvez les soutenir : Donate)

Une fois l'installation réalisée et l'application lancée, on crée la base de données (le coffre) en deux étapes.

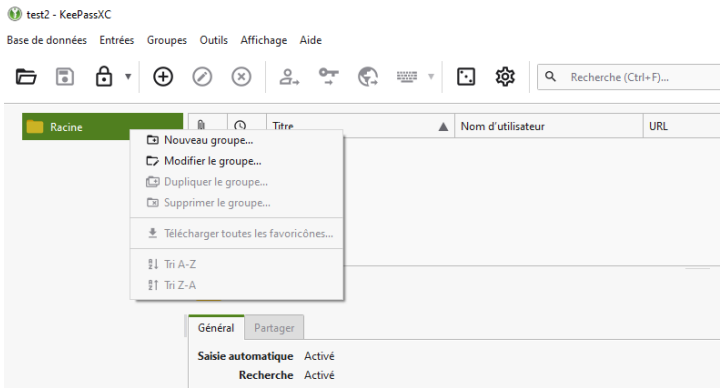


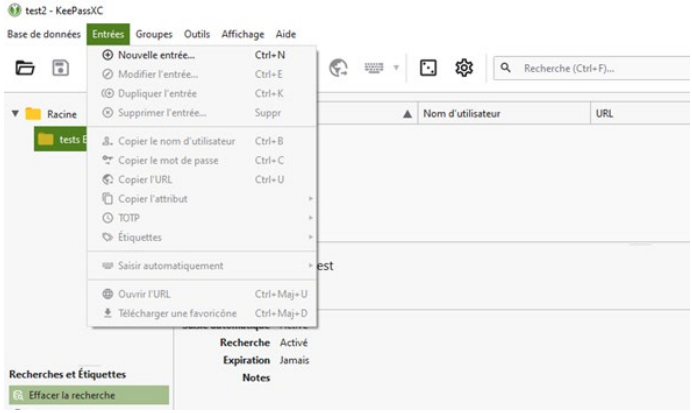
L'exemple de KeePassXC

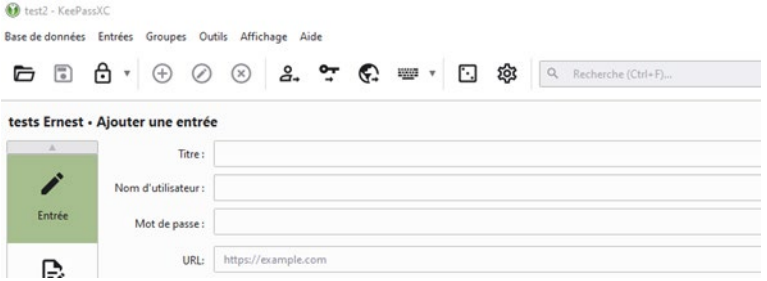
Dans la phase suivante on définit le mot de passe maître puis la localisation de la base de données (coffre)



Il ne reste plus qu'à y déposer vos mots de passe dans des dossiers comme dans un explorateur de fichiers





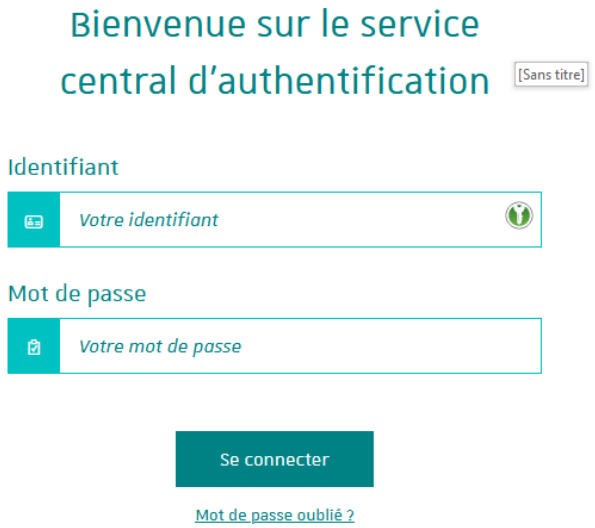


Les groupes sont les dossiers où on peut ranger ces entrées (les triplets) selon votre propre méthode

L'exemple de KeePassXC

Pour l'utiliser il est recommandé d'ajouter une extension au navigateur: " KeePass-browser".

Une fois cette extension intégrée pas l'application (3-4 étapes) vous n'aurez plus besoin de passer par cette dernière pour compléter les champs d'identification d'un site enregistré.



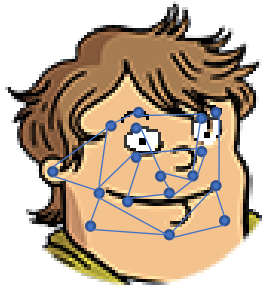
Ici l'icône de KeepassXC est verte indiquant que le coffre-fort est déverrouillé.

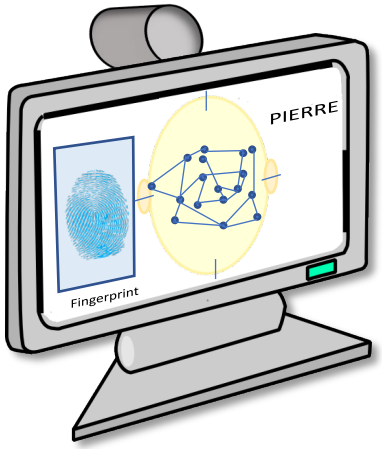
Si elle est grise, coffre verrouillé, vous pouvez le déverrouiller en cliquant sur cette icône (le mot de passe maître vous sera demandé)

Vous pouvez utiliser paramètres pour définir les conditions d'utilisation du coffre et sa fermeture en vous rendant dans les paramètres de l'application à l'onglet sécurité

Tendances actuelles : changement de méthode

L'utilisation des **données biométriques** (voix, visage, empreinte digitale, pupille…) ou d'un support de **stockage physique** (clé d'authentification) se développent.





Les clés peuvent remplacer les mots de passe et /ou l'authentification à deux facteurs (normes U2F, FIDO2)

Problèmes :

Peu généralisés

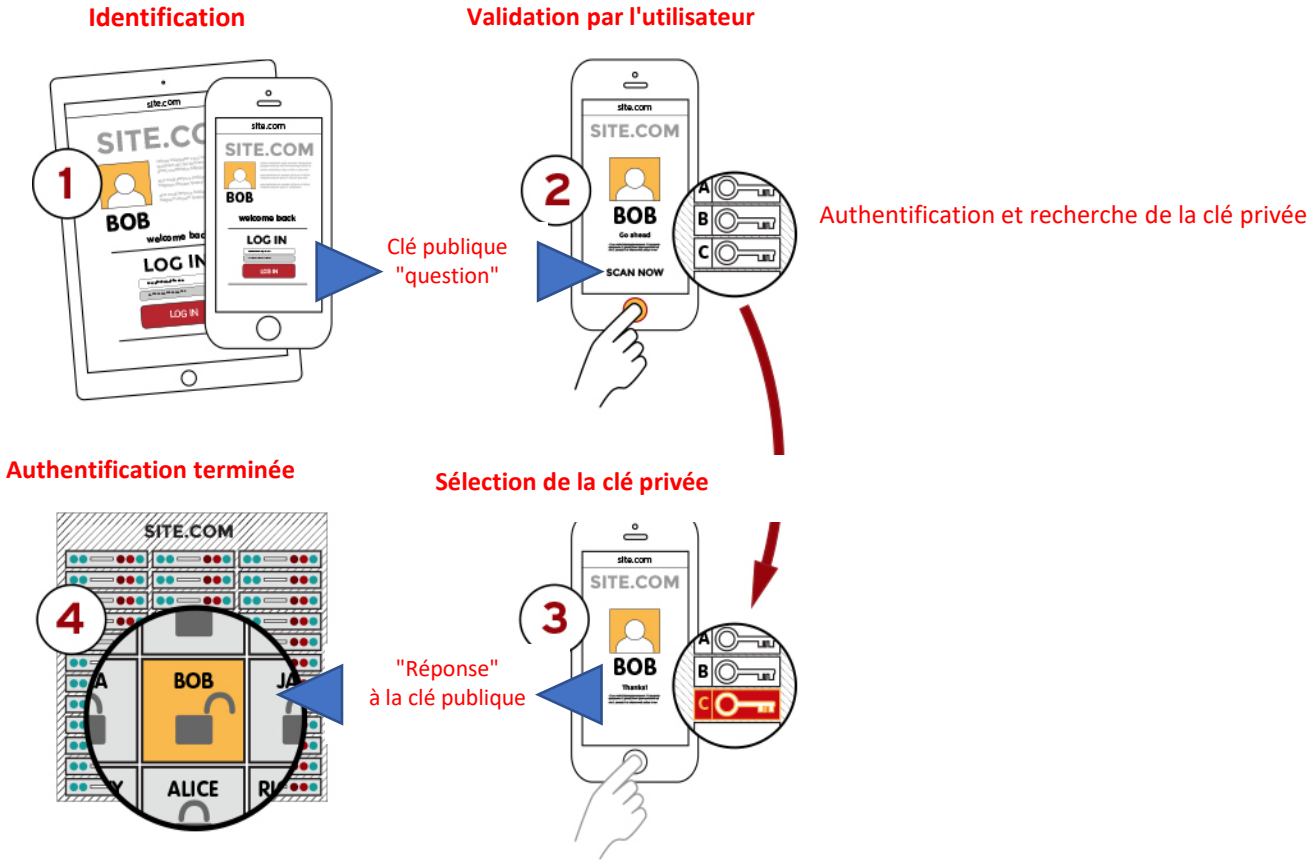
Coût

En cours de développement

Passkey (ou clé d'accès) est un standard soutenu par la FIDO Alliance (Fast Identity Online) et tous les géants du numérique afin de supprimer l'utilisation de mots de passe tout en augmentant la sécurité.

Comment ça marche?

A la création d'un compte en ligne **deux clés** (cryptées) sont produites : une publique et une privée. **Elles sont uniques pour ce compte.**
La clé publique est accessible au fournisseur mais celle-ci ne peut fonctionner sans la clé privée qui n'est utilisable que depuis votre téléphone ou tout autre appareil connecté que vous aurez approuvé et qui sera physiquement proche.
Cette clé privé (cryptée) ne peut être activée sans une donnée biométrique ou éventuellement un code depuis votre téléphone.



Et si jamais….

Informez les administrateurs du site !

Alertez vos amis !

Effacez vos données bancaires sur le site !

Changez le mot de passe !

Prévenez la banque

Portez plainte

Depuis 2020 il existe une plateforme d'assistance : https://www.cybermalveillance.gouv.fr

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

- ❑ Qualification du problème (diagnostic)
- ❑ Conseils et solutions
- ❑ Mise en relation avec un professionnel spécialisé

Mais aussi des conseils de protection, des sites officiels pour signaler et des guides pour porter plainte

Merci pour
votre attention

Centre
de **culture numérique**
Université de Strasbourg