FÉDÉRATION HAUTES-ALPES
la ligue de l'enseignement
un avenir par l'éducation populaire

SE PROTÉGER AVEC UN BON MOT DE PASSE

Hacke-moi si tu peux !

Atelier numérique ligue de l'enseignement 05

Aujourd'hui c'est vous les pirates

Trouvez le plus grand nombre de mots de passe.

Pour bien se protéger, le mieux est de comprendre comment s'y prennent ceux qui veulent nous pirater.

Le temps de l'atelier, vous allez donc changer de camp : à chaque étape, vous jouez le rôle du pirate qui essaie de deviner un mot de passe.

À chaque fois, on verra ensemble comment se protéger.

Attaque par devinette

Cherchez l'info qu'il faut !

Le principe

Le ou la pirate cherche des informations sur vous dans ce que vous laissez visible en ligne (réseaux sociaux, blog, forum). Prénom d'un proche, date de naissance, lieu de vacances, nom de l'animal… tout ce qui traîne peut servir à deviner un mot de passe.

A vous de jouer !

Regardez ce profil Instagram public. Une des informations est sûrement le mot de passe...

MOT DE PASSE : _ _ _ _ _ _

Jacqueline M.

🎂 Pâtissière à ses heures

🏠 Angoulême

😎 Mamie Rock’n Roll

Jacqueline M. Mon dessert préféré ! La Forêt noire !

Jacqueline M. Le nouvel amour de ma vie ! Il s’appelle Souris !

Jacqueline M. Babysitting chez mon fils Louis, en Bretagne !

Attaque par devinette

Vous avez la réponse ?

La réponse :

SOURIS

Le conseil

On ne met jamais une information personnelle dans un mot de passe : date de naissance, ville actuelle ou ancienne, nom de l'animal, prénom des petits-enfants…
Tout ce qui est visible sur internet est public, et un pirate peut le retrouver.

Attaque par force brute

Taper, taper, taper

Le principe

La ou le pirate essaie toutes les combinaisons possibles, l'une après l'autre, jusqu'à trouver la bonne.

A vous de jouer !

Trouvez le code qui déverrouille le téléphone.

MOT DE PASSE : _ _ _

Attaque par force brute

Vous avez la réponse ?

La réponse :

009

Le conseil

Avec 3 chiffres, il y a 1000 combinaisons possibles. À la main, on peut toutes les essayer, mais c'est très long.
Un ordinateur, lui, teste des milliers de combinaisons par seconde. Plus le mot de passe est court, plus il tombe vite.

Le temps qu'il faut à un pirate pour craquer votre mot de passe par force brute en 2026

16 x RTX 5090 | bcrypt (10)

Nombre de caractères	Nombres seulement	Lettres minuscules	Lettres majuscules et minuscules	Nombres, lettres majuscules et minuscules	Nombres, lettres majuscules et minuscules, symboles
4	Instantané	Instantané	Instantané	Instantané	Instantané
5	Instantané	Instantané	46 minutes	2 heures	3 heures
6	Instantané	37 minutes	2 jours	5 jours	1 semaine
7	Instantané	16 heures	3 mois	10 mois	2 ans
8	Instantané	2 semaines	12 ans	50 ans	132 ans
9	2 heures	1 an	636 ans	3k ans	9k ans
10	20 heures	32 ans	33k ans	191k ans	645k ans
11	1 semaine	839 ans	1M ans	11M ans	45M ans
12	3 mois	21k ans	89M ans	737M ans	3Md ans
13	2 ans	567k ans	4Md ans	45Md ans	221Md ans
14	23 ans	14M ans	241Md ans	2Bn ans	15Bn ans
15	229 ans	383M ans	12Bn ans	175Bn ans	1Bd ans
16	2k ans	9Md ans	653Bn ans	10Bd ans	75Bd ans
17	22k ans	259Md ans	33Bd ans	675Bd ans	5Tn ans
18	228k ans	6Bn ans	1Tn ans	41Tn ans	372Tn ans

Hive Systems

› hivesystems.com/password

Attaque par dictionnaire

Non pas le Larousse...

Le principe

Plutôt que d'essayer toutes les combinaisons, le pirate commence par une liste toute prête des mots de passe les plus courants. Et il en existe des vraies.

A vous de jouer !

Voici la liste des mots de passe les plus utilisés. Le mot de passe recherché s'y trouve.

MOT DE PASSE : _ _ _ _ _ (que des lettres)

Mots de passe les plus utilisés en France en 2025

1. admin
2. 123456
3. password
4. azerty
5. 123456789
6. 12345678
7. azertyuiop
8. azerty123
9. final9999
10. 12345

Attaque par dictionnaire

Vous avez la réponse ?

La réponse :

admin

Le conseil

Cette liste n'est pas inventée : ce sont vraiment les mots de passe les plus utilisés. Plus un mot de passe est simple et évident, plus il est facile à casser.
Pour en créer un solide, pensez à la phrase de passe : plusieurs mots collés, faciles à retenir pour vous, impossibles à deviner pour un pirate.

Attaque par réutilisation

On prend les mêmes et on recommence !

Le principe

Beaucoup de gens utilisent le même mot de passe partout. Si la ou le pirate en découvre un seul, il l'essaie sur tous vos autres comptes.

A vous de jouer !

Vous avez déjà trouvé un mot de passe tout à l'heure. Essayez-le pour vous connecter à un autre compte.

MOT DE PASSE : _ _ _ _ _ _

Attaque par réutilisation

Vous avez la réponse ?

La réponse :

SOURIS

Le conseil

Un seul mot de passe découvert, et c'est plusieurs comptes qui tombent.
Chaque compte important devrait avoir son propre mot de passe !

Comment retenir tous ses mots de passe ?

Mémoire de poisson rouge...

Avoir un mot de passe différent partout, c'est le bon réflexe. Mais impossible de tous les retenir. Trois solutions, de la plus simple à la plus complète.

LE CARNET PAPIER

Un petit carnet, rangé chez vous en lieu sûr. Simple, et hors de portée des pirates puisqu'il n'est pas sur internet.

LE NAVIGATEUR (CHROME, FIREFOX...)

Il propose de retenir vos mots de passe. C'est pratique et déjà mieux que d'utiliser le même partout. Sa limite : tout est ouvert dès que quelqu'un accède à votre ordinateur.

LE GESTIONNAIRE DE MOTS DE PASSE

Une application spécialisée qui range tous vos mots de passe derrière un seul mot de passe principal. C'est la solution la plus complète, à envisager une fois qu'on est à l'aise.

Attaque par hameçonnage (phishing)

On vous appâte !

Le principe

La ou le pirate se fait passer pour un organisme de confiance (votre banque, les impôts, la Sécurité sociale, un livreur) pour vous pousser à donner vous-même vos informations.
Il vous envoie un message qui fait peur ou qui presse : « votre compte va être fermé », « un problème de paiement », « votre colis est bloqué ».
Un lien vous emmène vers un faux site qui ressemble au vrai.

A vous de jouer !

Vous avez envoyé un faux mail à votre victime avec un lien vers un faux site. Elle s'y connecte…

Banque des Hautes-Alpes

De : service-securite@banquedeshautesalpes-verification.com

Objet : Suspension imminente de votre compte

Cher client, chère cliente,

Nous avons détecté une connexion inhabituelle à votre espace client. Pour votre sécurité, votre compte bancaire sera bloqué sous 24 heures si vous ne confirmez pas vos informations.

Merci de vous authentifier immédiatement en cliquant sur le bouton ci-dessous.

Vérifier mon compte

Cordialement,
Le service de sécurité de la Banque des Hautes-Alpes

Attaque par hameçonnage

Vous avez trouvé le piège ?

La réponse :

- L'adresse de l'expéditeur bizarre (banquedeshautes-alpes-verification.com), qui n'est pas l'adresse normale de la banque. C'est le premier réflexe : toujours regarder qui envoie.
- L'urgence et la menace (« bloqué sous 24 heures »), pour vous faire agir vite sans réfléchir. Une vraie banque ne vous menace pas de fermeture par mail.
- Le « Cher client » impersonnel : votre vraie banque vous appelle par votre nom.
- Le bouton qui presse (« Vérifier mon compte »), qui mène au faux site. C'est LE lien sur lequel il ne faut jamais cliquer.
- Et le fond du message : une banque ne demande jamais de « confirmer vos informations » par mail.

Le conseil :

Ne cliquez jamais sur le lien d'un mail. Allez sur le site vous-même, par votre favori ou en tapant l'adresse habituelle.

Attaque par hameçonnage

Le piège n’arrive pas que par mail.

Par SMS

« Votre colis est en attente, cliquez ici », « Votre compte CPF va expirer ». Mêmes ficelles, même faux lien.

Par téléphone

Quelqu'un vous appelle en se faisant passer pour votre banque ou un conseiller, et vous demande un code reçu par SMS, ou de confirmer vos identifiants.

La règle d’or

Une banque, un service public ou une vraie entreprise ne vous demandera JAMAIS votre mot de passe ni vos codes, ni par mail, ni par SMS, ni par téléphone.

La double authentification (2FA)

Votre deuxième verrou

Même le meilleur mot de passe peut être volé. La double authentification ajoute une deuxième vérification, pour que votre mot de passe ne suffise plus à lui seul.

En plus de votre mot de passe, le site demande une deuxième preuve que c'est bien vous. Le plus souvent : un code envoyé par SMS sur votre téléphone, parfois un mail.

Résultat : même si un pirate a votre mot de passe, il ne peut rien faire sans votre téléphone ou votre mail.

Les ressources

Si vous voulez aller plus loin...

Pour vérifier si mon adresse mail a fuité : Have I Been Pwned (haveibeenpwned.com). Le site est en anglais mais il suffit d'y taper son adresse mail.

Pour créer un mot de passe solide : le générateur de mots de passe de la CNIL (https://www.cnil.fr/fr/generer-un-mot-de-passe-solide).

En cas d'arnaque ou de piratage : Cybermalveillance.gouv.fr. C'est LE bon réflexe, le service public d'aide aux victimes. Le site propose aussi des fiches et vidéos grand public.

Récapitulons...

Les 5 idées à retenir

Jamais d'information personnelle dans un mot de passe.
Date de naissance, ville, nom de l'animal, prénom des petits-enfants… tout ça se retrouve facilement sur internet.

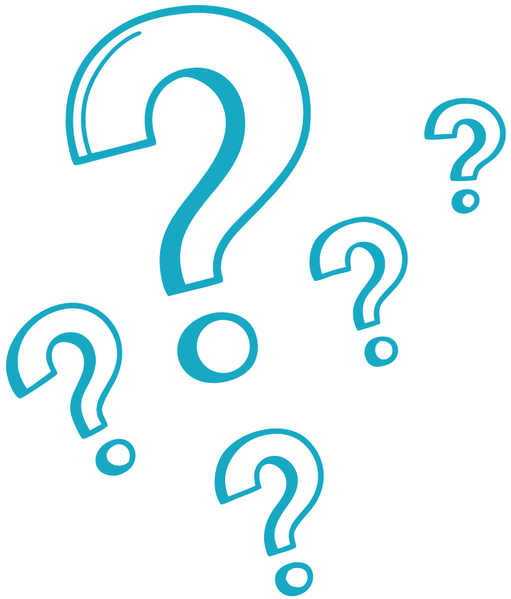
Un mot de passe long et complexe.
Une phrase de passe (plusieurs mots avec symboles) est plus solide qu'un mot court.

Un mot de passe différent pour chaque compte.
Si un seul est découvert, les autres restent protégés. Un carnet en lieu sûr ou un gestionnaire vous aide à les retenir.

On ne donne jamais son mot de passe.
Aucune banque, aucun service public ne le demandera, ni par mail, ni par SMS, ni par téléphone. En cas de doute, allez sur le site vous-même.

Activez la double authentification.
C'est votre deuxième verrou. Activez-la dès qu’on vous la propose.

Avez-vous des questions ?



Sources : Liste des mots de passe les plus utilisés : NordPass (nordpass.com) 2025.
Temps nécessaire pour casser un mot de passe : Hive Systems Password Table 2026.
Recommandations sur les mots de passe et l'authentification : CNIL (cnil.fr) et ANSSI (cyber.gouv.fr, le site de l'ANSSI).
Aide aux victimes et définitions (hameçonnage, etc.) : Cybermalveillance.gouv.fr.