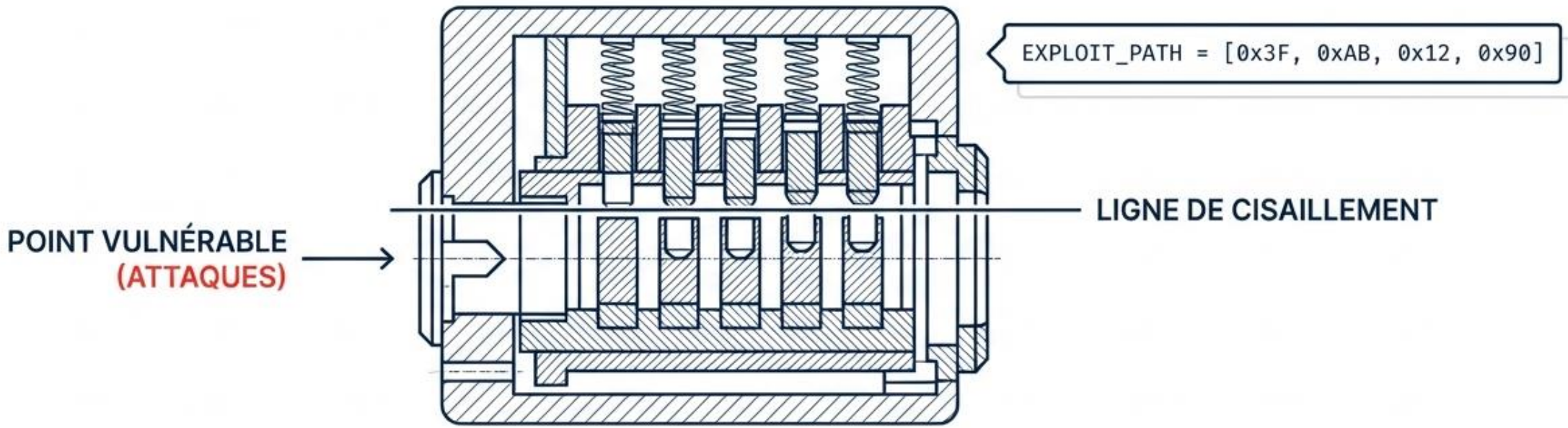
La Science des Mots de Passe : Attaques, Entropie et Réalité

Comprendre la mécanique du piratage pour mieux se défendre.



ENTROPIE FAIBLE (VULNÉRABLE)

PASSWORD = "123456"

ENTROPIE ÉLEVÉE (SECURE)

PASS90RD = "c8$JKL9@p!2q2#"

La Vitesse de la Rupture : La menace en 2025

Analyse basée sur une puissance de calcul de 12 × RTX 5090 (Benchmark Hive Systems).

Nombre de caractères	Nombres seulement	Lettres minuscules	Lettres majuscules et minuscules	Lettres majuscules et minuscules, symboles	
4 chars	Instantané	Instantané	Instantané	Instantané	Instantané	Instantané
5 chars	Instantané	Instantané	Instantané	57 minutes	2 heures	4 heures
6 chars	Instantané	46 minutes	2 jours	6 jours	2 semaines	2 semaines
7 chars	Instantané	20 heures	4 mois	1 an	2 ans	2 ans
8 chars	Instantané	3 semaines	15 ans	62 ans	164 ans	164 ans
9 chars	2 heures	2 ans	791 ans	3k ans	11k ans	11k ans
10 chars	1 jour	40 ans	41k ans	238k ans	803k ans	803k ans
11 chars	1 semaine	1k ans	2M ans	14M ans	56M ans	56M ans
12 chars	3 mois	27k ans	111M ans	917M ans	3Md ans	3Md ans
13 chars	3 ans	705k ans	5Md ans	56Md ans	275Md ans	275Md ans
14 chars	28 ans	18M ans	300Md ans	3Bn ans	19Bn ans	19Bn ans
15 chars	284 ans	477M ans	15Bn ans	218Bn ans	1Bd ans	1Bd ans
16 chars	2k ans	12Md ans	812Bn ans	13Bd ans	94Bd ans	94Bd ans
17 chars	28k ans	322Md ans	42Bd ans	840Bd ans	6Tn ans	6Tn ans
18 chars	284k ans	8Bn ans	2Tn ans	52Tn ans	463Tn ans	463Tn ans

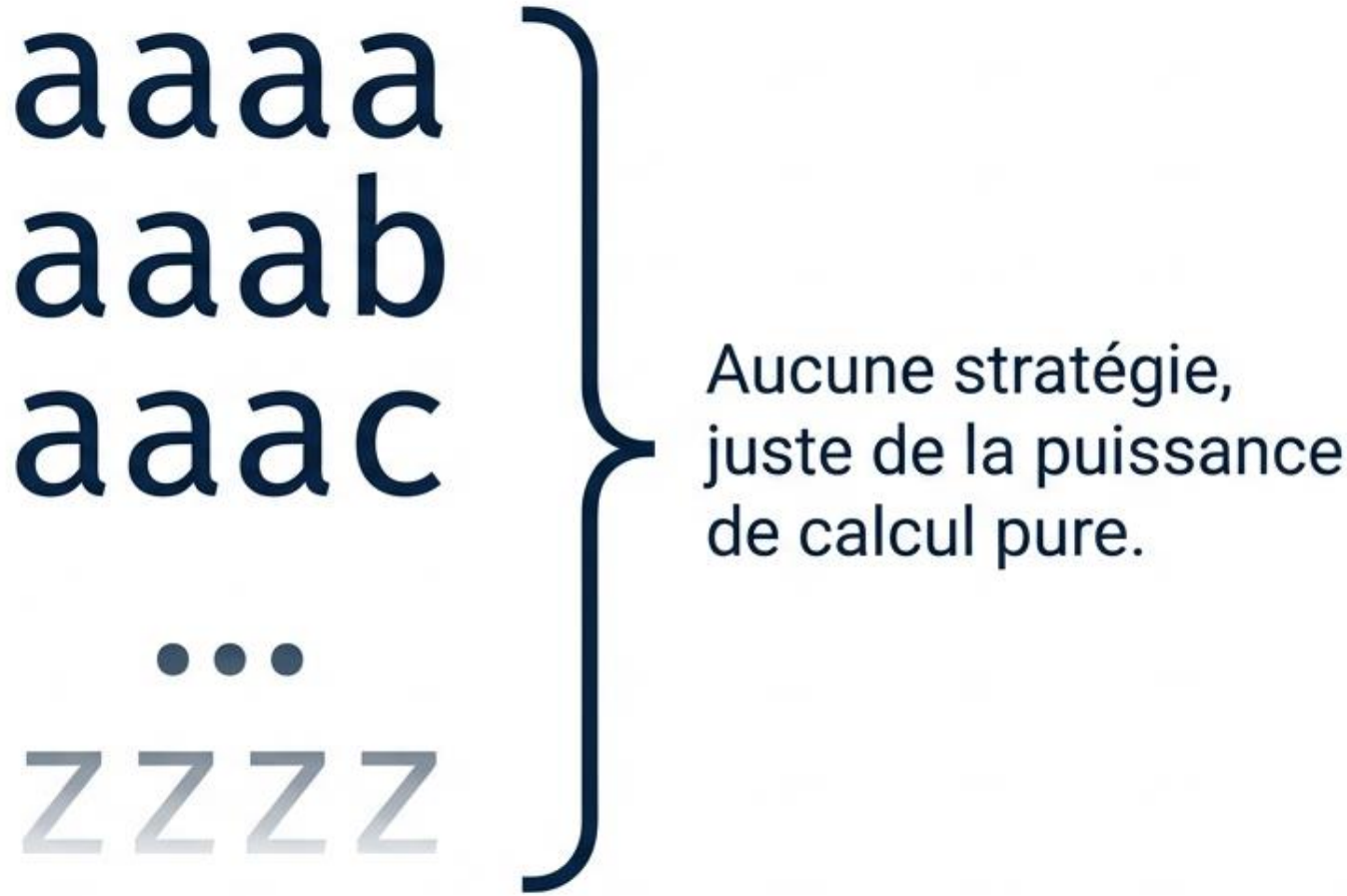
Zone de Danger : Tout mot de passe de moins de 11 caractères est vulnérable aux fermes de GPU modernes.
La sécurité commence véritablement à 12 caractères.

Le Concept Fondamental : L'Attaque par Force Brute

Le brute force est une méthode d'attaque qui consiste à tester toutes les combinaisons possibles d'un mot de passe jusqu'à trouver la bonne.

C'est un jeu de probabilité : puissance de calcul vs espace de recherche.

Attaque 1 : Force Brute Simple (Le "Bourrin")



Limite : Exponentiellement impossible au-delà de 10-12 caractères.

Attaque 2 : Attaque par Dictionnaire (L'Approche Humaine)

Le Mécanisme

La Réalité

85% des humains utilisent des mots du dictionnaire ou des schémas prévisibles.

Exemples Échoués

Bonjour2025!
Chocolat75!
Soleil123

"Si votre mot de passe est basé sur un mot réel, cette attaque le trouvera en quelques secondes."

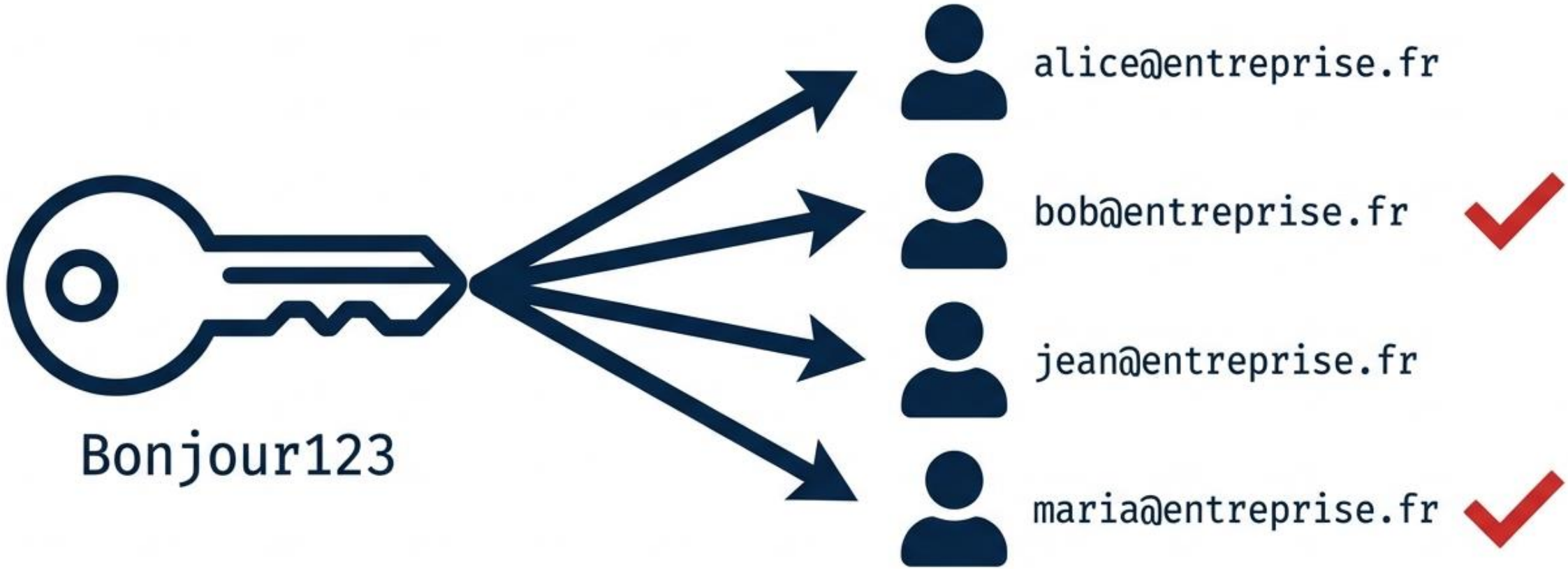
Attaque 3 : Force Brute Hybride (La Combinaison)

Mot du Dictionnaire	+	Règle de Force Brute	=	Mot de Passe Cassé

```
Bonjour + 0000-9999 → Bonjour9999
Chien + Voiture → ChienVoiture
Paris + ! → Paris!
```

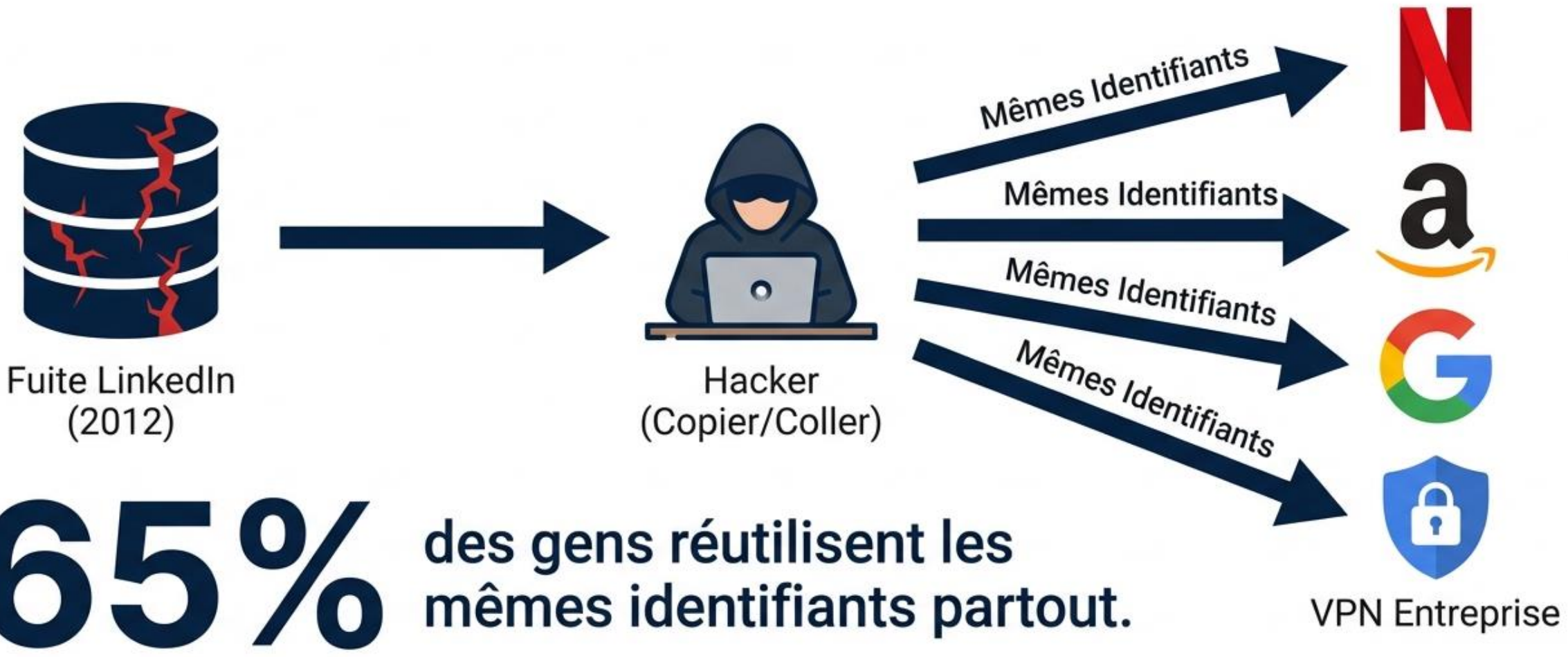
Cette attaque casse **99%** des **mots de passe humains**, car la **structure** est prévisible.

Attaque 4 : Force Brute Inversée (Le Filet)



Au lieu de tester 1000 mots de passe sur 1 utilisateur,
on teste 1 mot de passe courant sur 1000 utilisateurs.

Attaque 5 : Credential Stuffing (Le Recyclage)



65% des gens réutilisent les mêmes identifiants partout.

Il n’y a aucun brute-force ici. C’est du recyclage de données volées.

La Théorie de la Défense : Comprendre l'Entropie

L'entropie mesure l'imprévisibilité d'un mot de passe.

Prévisible
(Faible Entropie)

Imprévisible
(Forte Entropie)

Entropie Mathématique

$$\lim_{x \to 0} \sum_{n=1}^{\infty} x(x) \longrightarrow (n-i) \quad x^n \to \frac{y}{n}$$

Basée sur la combinatoire théorique.
Analyse brute des possibilités.

Entropie Réelle

Basée sur la psychologie et la prévisibilité humaine.
Prend en compte les biais et les habitudes.

L'Illusion de l'Entropie Mathématique

Entropie = Longueur x log2(Taille_Alphabet)

Mot de passe : `abcd1234`

Longueur : 8

Alphabet : 36 (lettres + chiffres)

Résultat : ≈ 41 bits

Problème : Les mathématiques supposent que ce mot de passe est totalement aléatoire. En réalité, ‘abcd1234’ est une suite logique prévisible.

Clinical
Cyber-Editorial

Le Facteur Humain : Pourquoi les Maths se Trompent

Les humains ne sont pas des générateurs de **nombres aléatoires**.

Mots du dictionnaire

Années (1980-2025)

Villes / Prénoms

Substitutions (Leet)

Suites Clavier

Structure Universelle

Un mot de passe de 80 bits théoriques peut n'avoir que 20 bits réels à cause de ces patterns.

Étude de Cas : Autopsie de "B0nj0ur2025!"

10 + 6 + 6 + 3 ≈ 25 bits d'entropie réelle

Entropie Mathématique Théorique : 78 bits

Entropie Réelle (Attaquant) : 25 bits

Conclusion : Des millions de fois plus faible que prévu.

Clinical Cyber-Editorial

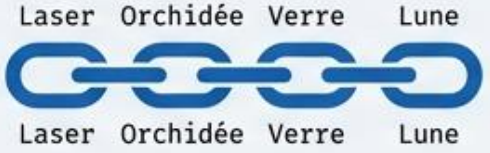
Comparatif de Résistance : Théorie vs Réalité

Mot de passe	Entropie Math	Entropie Réelle	Résistance
Tf8!R9eL#yP2	~78 bits	~78 bits	Très Forte
B0nj0ur2025!	~78 bits	~25 bits	Très Faible
Chocolat75!	~65 bits	~15-20 bits	Très Faible
Laser-Orchidée-Verre-Lune	~55 bits	~55 bits	Forte

La Stratégie Gagnante : Comment battre les attaquants

Stop aux Patterns

Évitez la structure "Mot + Année + Symbole".



Phrase de Passe

Utilisez 4 mots aléatoires (ex: Laser-Orchidée-Verre-Lune).

Activer le MFA

La double authentification bloque le Credential Stuffing.

Gestionnaire de Mots de Passe

Pour des mots de passe uniques et aléatoires partout.

Un bon mot de passe est un mot de passe ayant une forte entropie réelle.

L'Essentiel à Retenir

- **La vitesse compte :** Les GPU modernes cassent les mots de passe de 8 caractères instantanément.
- **L'humain est prévisible :** Les attaques par dictionnaire et hybrides exploitent nos habitudes (dates, prénoms).
- **L'entropie réelle est la clé :** Ne confondez pas complexité apparente (B0nj0ur2025!) et aléatoire réel.
- **La solution :** Adoptez des phrases de passe longues (4 mots aléatoires) ou utilisez un gestionnaire de mots de passe.