

# SENSIBILISATION AUX RISQUES CYBER



Mise à jour : 15 Avril 2024



**Pierre LABORDE**  
Réserviste Police Nationale



**Anthony DON**  
Dirigeant d'entreprise  
Réserviste civique

Chargés de prévention cybermenaces  
Direction Zonale de la Police Judiciaire de Bordeaux  
DZPJ Sud-Ouest  
Hôtel de Police  
23 rue François de Sourdis  
33062 BORDEAUX

[cybermenaces-bordeaux@interieur.gouv.fr](mailto:cybermenaces-bordeaux@interieur.gouv.fr)

- Dispositif lancé le 09 Mars 2018
- But du RECyM : **sensibiliser le tissu économique local aux risques cyber** et apporter un premier niveau d'assistance aux victimes
- Composé d'enquêteurs de PJ et de réservistes du secteur privé ou public
- Dans le Sud-Ouest : 30 réservistes sous la supervision de la direction zonale de Police Judiciaire de Bordeaux
- Point de contact pour les entreprises et collectivités en Nouvelle-Aquitaine :



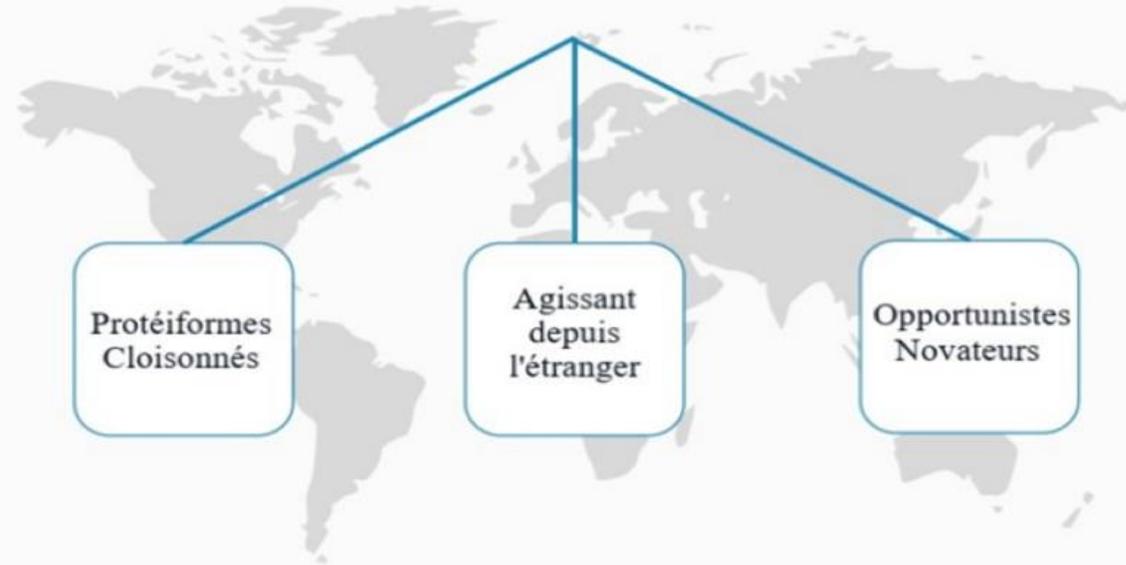
[cybermenaces-bordeaux@interieur.gouv.fr](mailto:cybermenaces-bordeaux@interieur.gouv.fr)



*Evolution d'une délinquance en bande organisée au niveau national...*



*...à une délinquance en Groupe Criminel Organisé (GCO) transnational*



## Le profit :

Phishing, ransomware (rançongiciels), Jackpotting...



## L'atteinte à l'image :

DDos, Défacement



## L'espionnage :

Attaque par point d'eau / Spearphishing

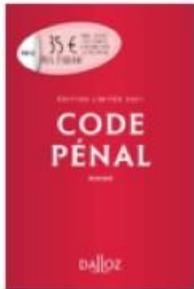


## Le sabotage :

Panne organisée



## Art 313-1 CP:

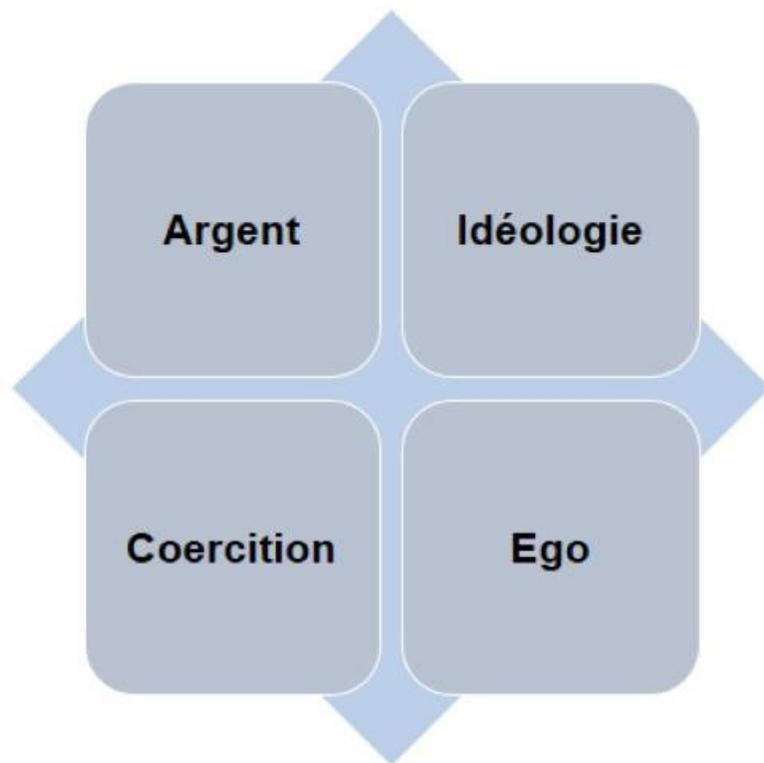


L'escroquerie est le fait, soit par l'usage d'un faux nom ou d'une fausse qualité, soit par l'abus d'une qualité vraie, soit par l'emploi de manœuvres frauduleuses, de tromper une personne physique ou morale et de la déterminer ainsi, à son préjudice ou au préjudice d'un tiers, à remettre des fonds, des valeurs ou un bien quelconque, à fournir un service ou à consentir un acte opérant obligation ou décharge.

- .Escroqueries aux faux virements étrangers
- .Escroqueries aux faux investissements sur le foreign exchange (FOREX)
- .Escroqueries aux placements indexés sur les cryptomonnaies
- .Escroqueries aux faux supports techniques
- .Escroqueries à la fausse amitié (Scam romance)
- .Escroquerie au RGPD
- .Escroquerie au faux RIB d'employé
- .Escroquerie au CV



Matrice MICE



+

Réseaux sociaux



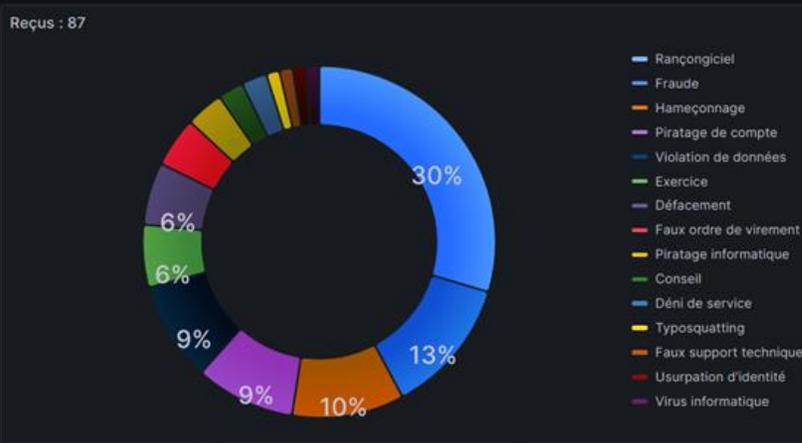
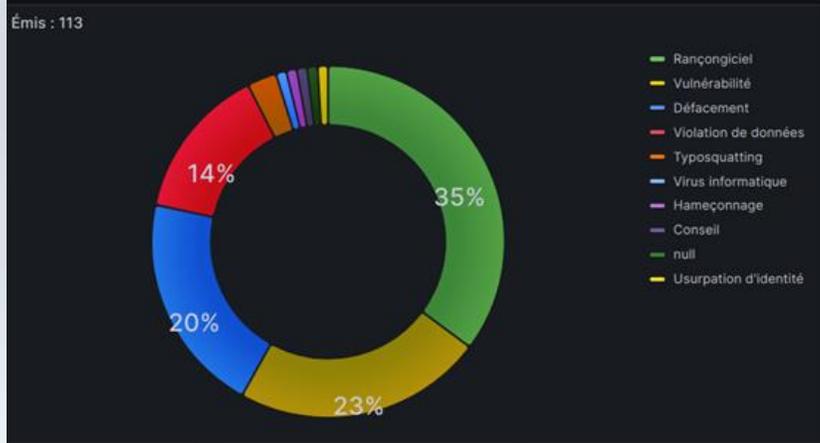
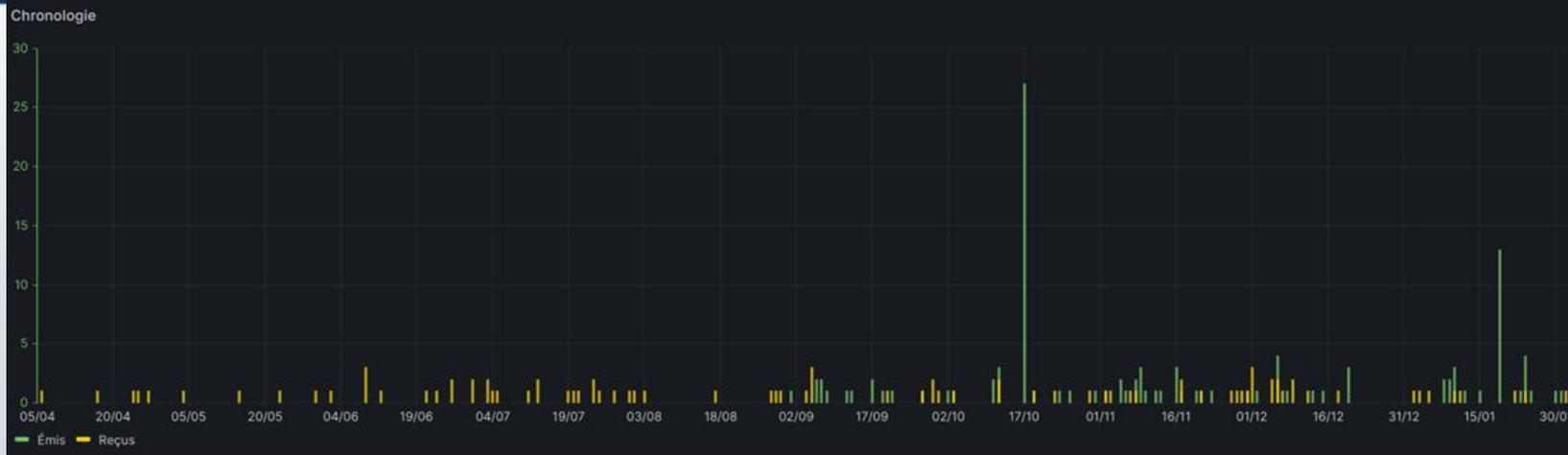
Instagram

Pinterest

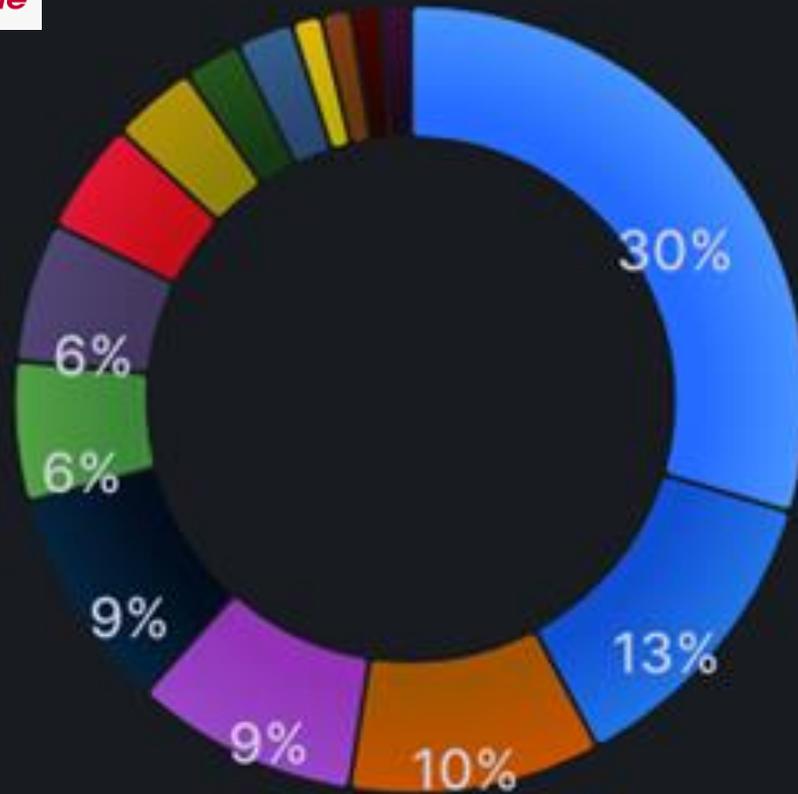


viadeo

LinkedIn



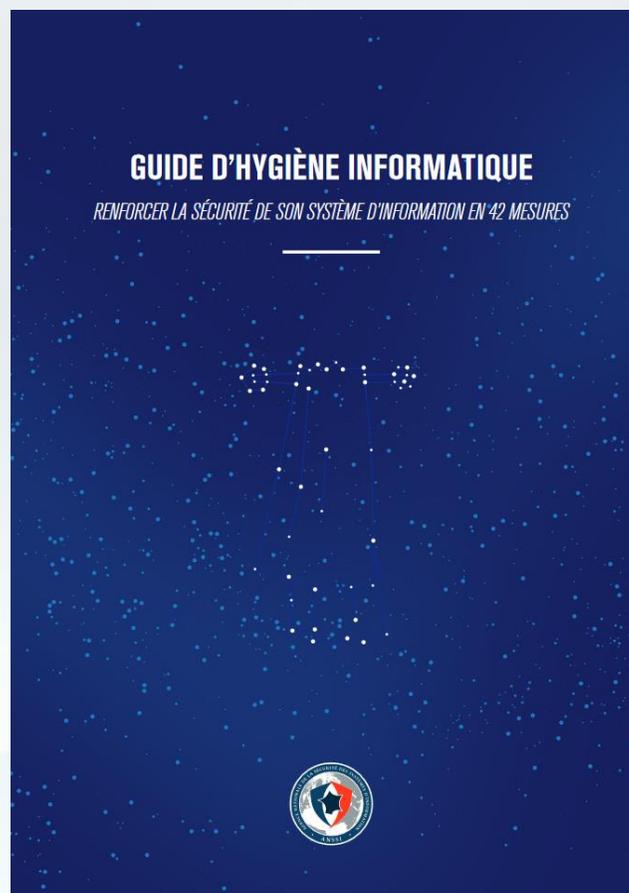
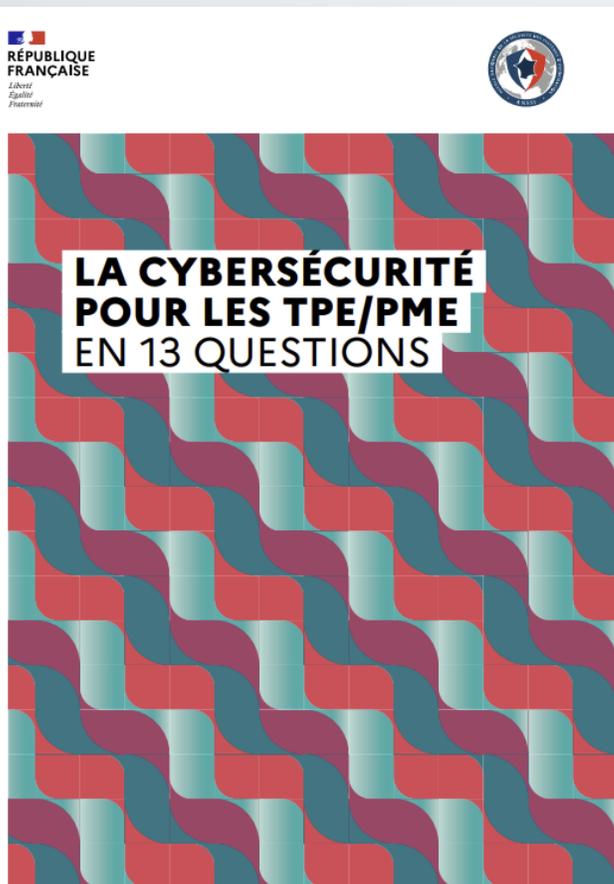
CAMPUS RÉGIONAL DE  
CYBERSÉCURITÉ ET DE  
CONFIANCE NUMÉRIQUE  
*Nouvelle-Aquitaine*



- Rançongiciel
- Fraude
- Hameçonnage
- Piratage de compte
- Violation de données
- Exercice
- Défacement
- Faux ordre de virement
- Piratage informatique
- Conseil
- Déni de service
- Typosquatting
- Faux support technique
- Usurpation d'identité
- Virus informatique

## Pour commencer à sensibiliser son organisation ... les guides de bonnes pratiques de l'ANSSI

<https://www.ssi.gouv.fr/administration/bonnes-pratiques/>



1 – Connaissez-vous bien votre parc informatique et vos actifs métier ?

**2 – Effectuez-vous des sauvegardes régulières ?**

3 – Appliquez-vous régulièrement les mises à jour ?

4 – Utilisez-vous un antivirus ?

**5 – Avez-vous implémenté une politique d'usage de mots de passe robustes ?**

6 – Avez-vous activé un pare-feu ?

7 – Comment sécurisez-vous votre messagerie ?

8 – Comment séparez-vous vos usages informatiques ?

9 – Comment maîtrisez-vous le risque numérique lors des missions et des déplacements professionnels ?

**10 – Comment vous informez-vous ? Comment sensibilisez-vous vos collaborateurs ?**

11 – Avez-vous fait évaluer la couverture de votre police d'assurance au risque cyber ?

**12 – Savez-vous comment réagir en cas de cyberattaque ?**

13 – Envisagez-vous d'utiliser des solutions cloud



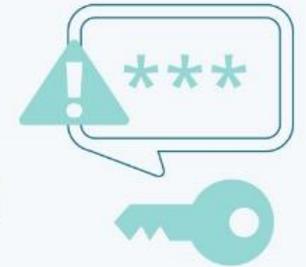
## Authentication

Bonnes pratiques – Gestionnaire de mot de passe

- Pourquoi faut-il éviter les mots de passe **triviaux** / contenant des **informations personnelles** / **courts** ?
- Générer des mots de passe **robustes** : longs et avec le plus grand nombre de symboles différents
- **Modifier les mots de passe par défaut** :  
Routeurs / Caméra IP / Objets connectés / Photocopieurs / Téléphones VOIP

## Les pires mots de passe utilisés en France

Classement des mots de passe français les plus courants en 2019 \*



- |               |                |
|---------------|----------------|
| 1. 123456     | 11. loulou     |
| 2. 123456789  | 12. 123        |
| 3. azerty     | 13. password   |
| 4. 1234561    | 14. azertyuiop |
| 5. qwerty     | 15. 12345678   |
| 6. marseille  | 16. soleil     |
| 7. 000000     | 17. chouchou   |
| 8. 1234567891 | 18. 1234       |
| 9. doudou     | 19. 1234567    |
| 10. 12345     | 20. 123451     |

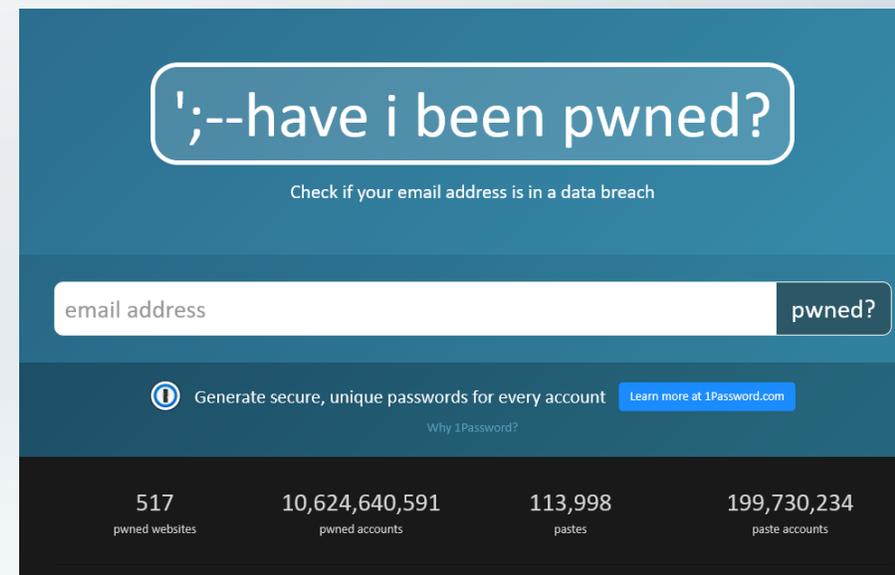
# Authentification – Un mot de passe différent pour chaque service

- Mot de passe unique : facile à retenir mais très risqué à cause des fuites de données.
- Compte réseaux sociaux -> Email -> Banque
- Utiliser un mot de passe différent pour chaque service

Recently added breaches	
	139,401 <u>KomplettFritid accounts</u>
	20,032 <u>Autotrader accounts</u>
	756,737 <u>Zurich accounts</u>
	367,476 <u>DoorDash accounts</u>
	1,464,271 <u>SlideTeam accounts</u>
	211,524,284 <u>Twitter (200M) accounts</u>
	229,037,936 <u>Deezer accounts</u>
	93,343 <u>Benchmark accounts</u>
	5,274,214 <u>Gemini accounts</u>
	1,557,153 <u>CoinTracker accounts</u>

# Authentification – Un mot de passe différent pour chaque service

- Mot de passe unique : facile à retenir mais très risqué à cause des fuites de données.
- Compte réseaux sociaux -> Email -> Banque
- Utiliser un mot de passe différent pour chaque service



';--have i been pwned?

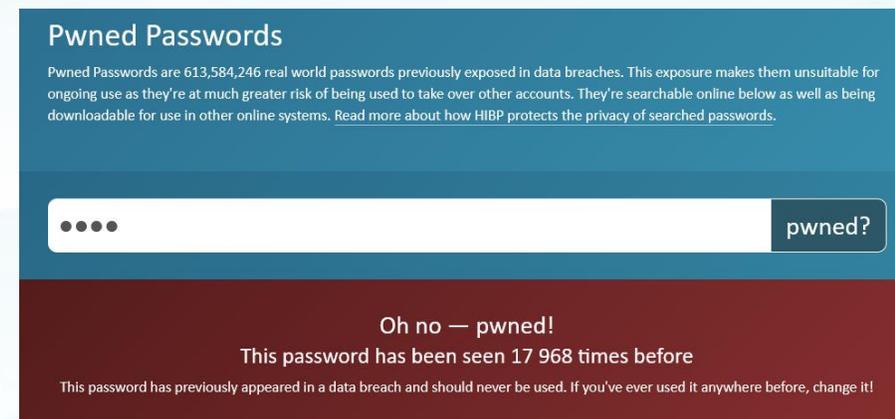
Check if your email address is in a data breach

email address  pwned?

Generate secure, unique passwords for every account [Learn more at 1Password.com](#)

Why 1Password?

517	10,624,640,591	113,998	199,730,234
pwned websites	pwned accounts	pastes	paste accounts



### Pwned Passwords

Pwned Passwords are 613,584,246 real world passwords previously exposed in data breaches. This exposure makes them unsuitable for ongoing use as they're at much greater risk of being used to take over other accounts. They're searchable online below as well as being downloadable for use in other online systems. [Read more about how HIBP protects the privacy of searched passwords.](#)

..... pwned?

Oh no — pwned!  
This password has been seen 17 968 times before

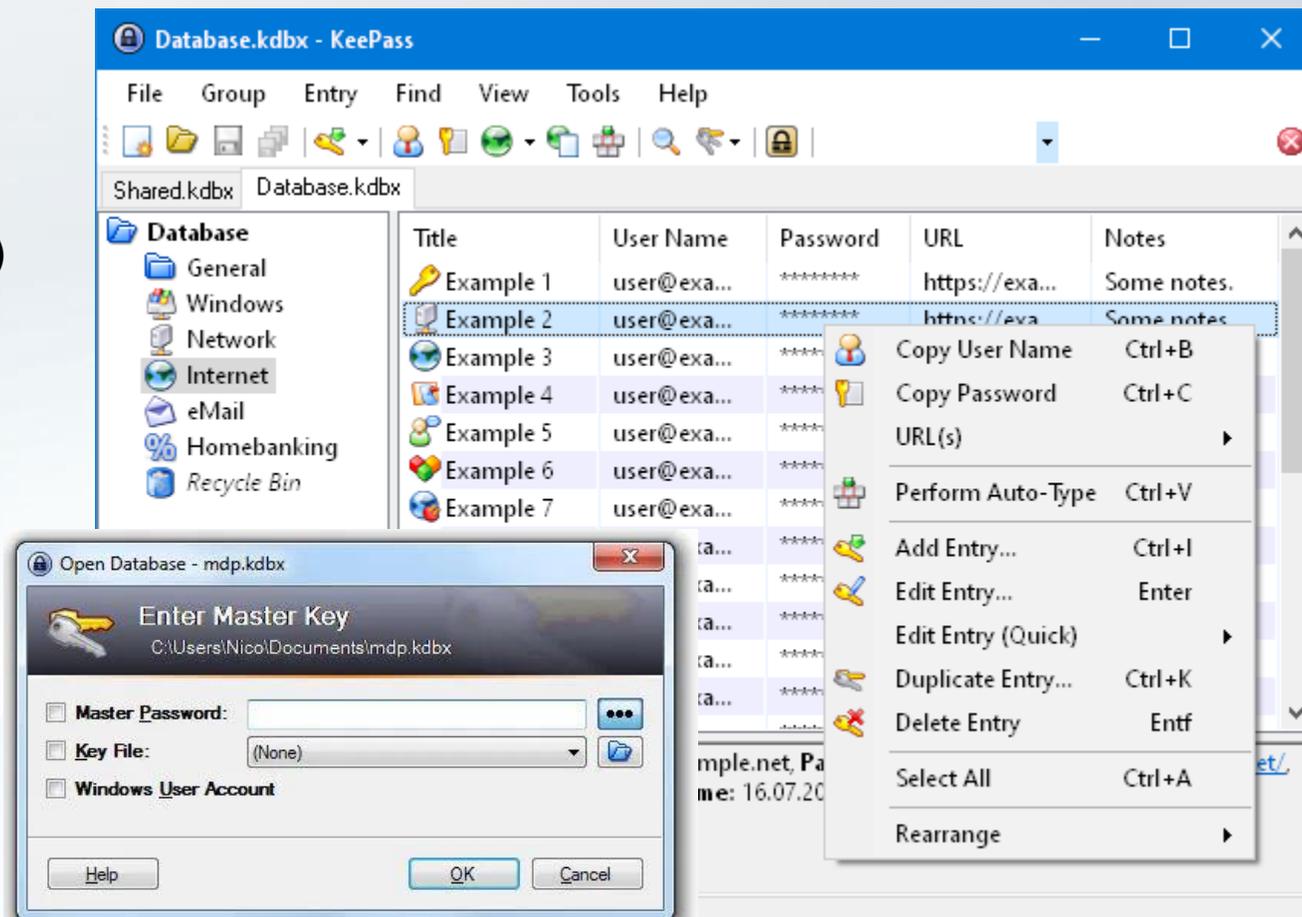
This password has previously appeared in a data breach and should never be used. If you've ever used it anywhere before, change it!

## Comment gérer ses mots de passe ?

- Complexes, uniques -> aléatoires
- Ne pas écrire sur une feuille ou un fichier (Excel, ...)
- Ne pas enregistrer dans le navigateur

## Coffre fort pour mots de passe

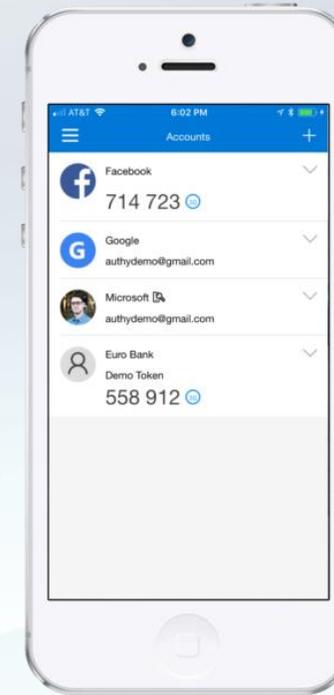
- Utilisation d'un gestionnaire de mot de passe
- Stockage de vos mots de passe dans un fichier chiffré (protégé par mot de passe : 1 seul à retenir)
- Génère les mots de passe pour vous (robustes et uniques)
- Saisit les mots de passe pour vous (directement ou via un plugin de navigateur)
- Le fichier peut être partagé
- KeePass 2.10 Portable est certifié par l'ANSSI



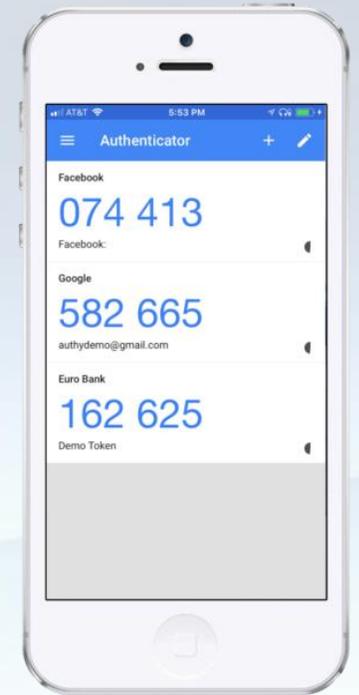
- Principe : compléter votre mot de passe (élément connu) avec un 2ème élément détenu (ex: votre smartphone via une app ou un SMS).
- **Bloque les accès** frauduleux en cas de mot de passe faible ou compromis.
- A activer systématiquement quand c'est disponible.



 AUTHY

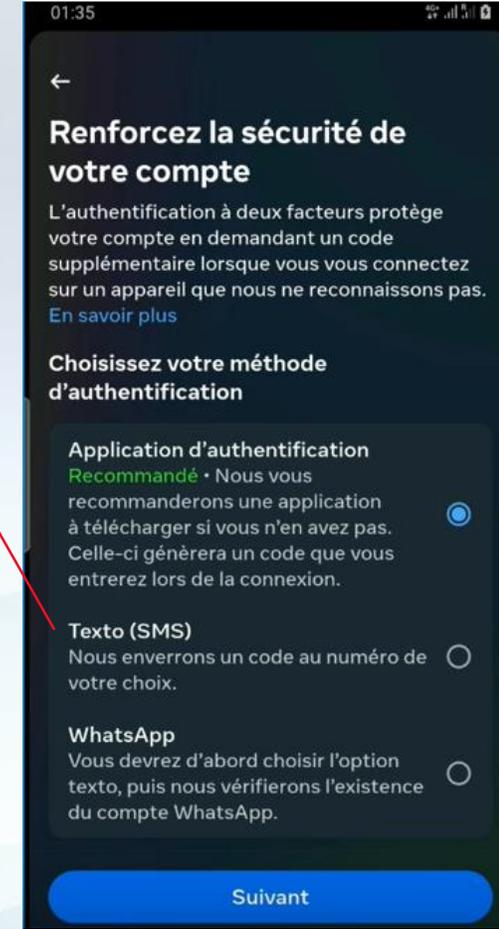
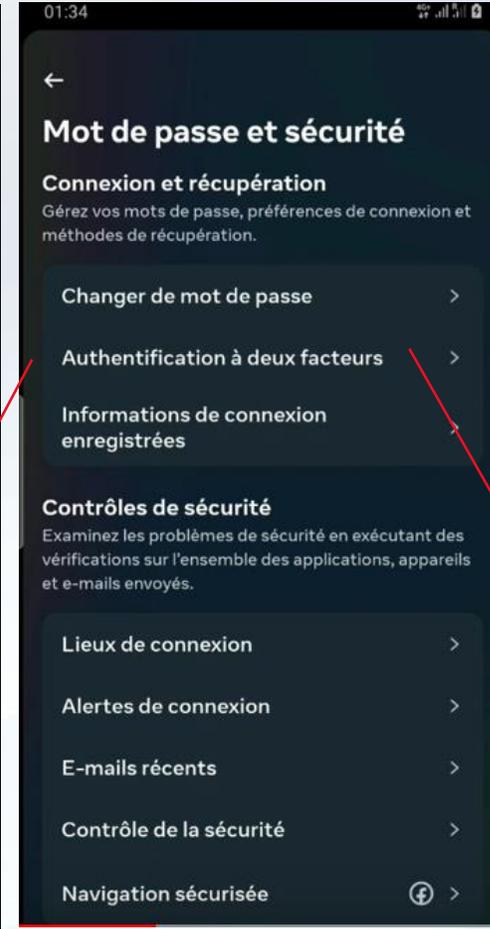
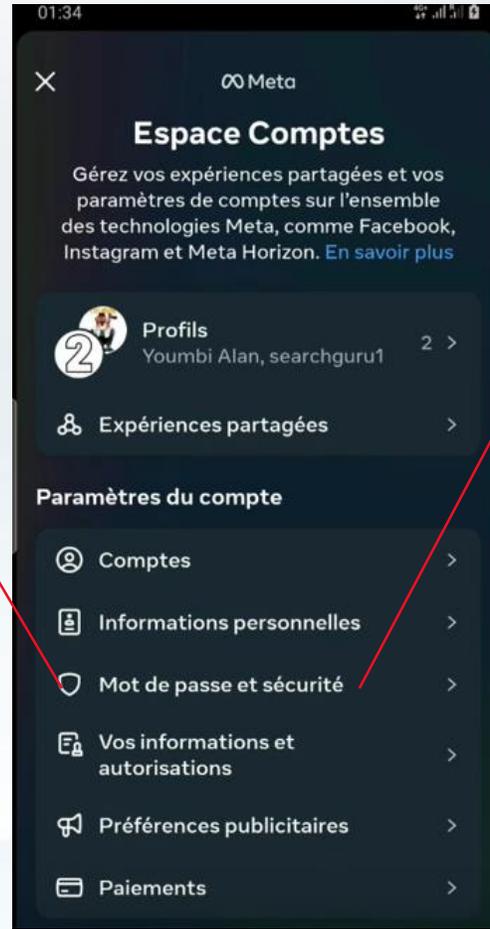
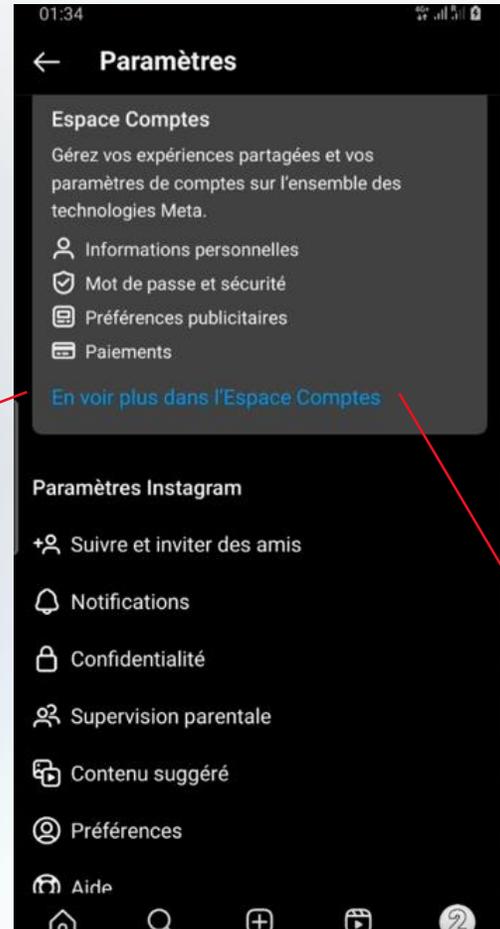
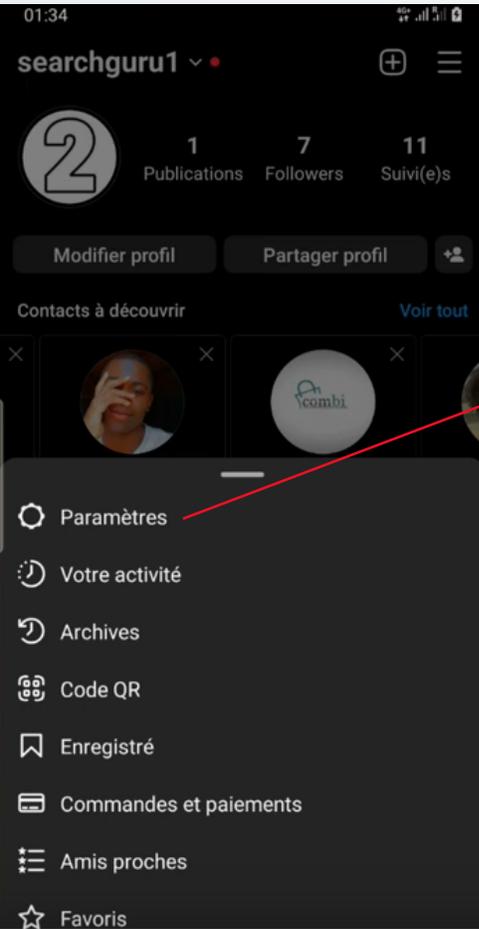


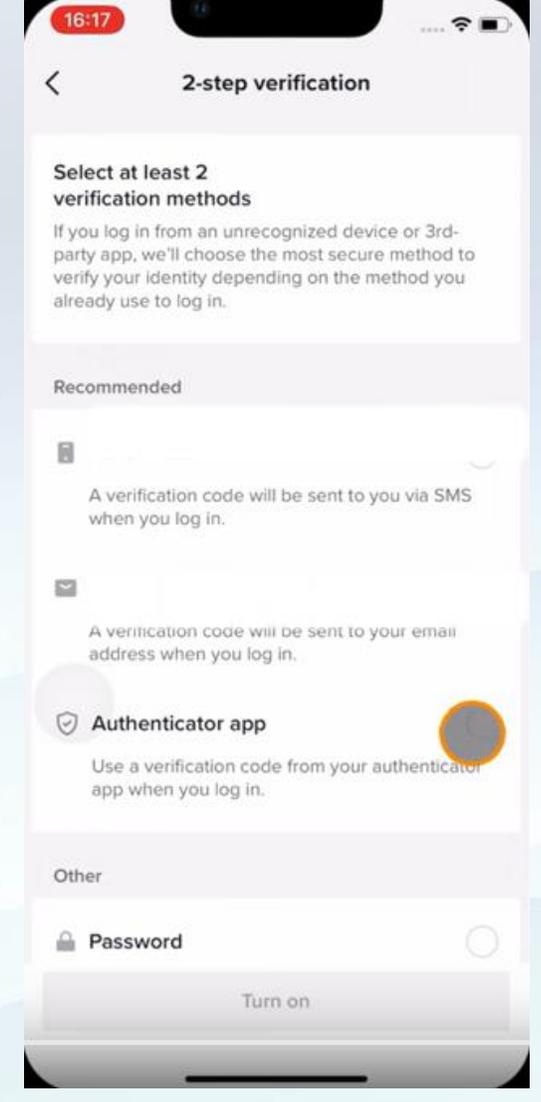
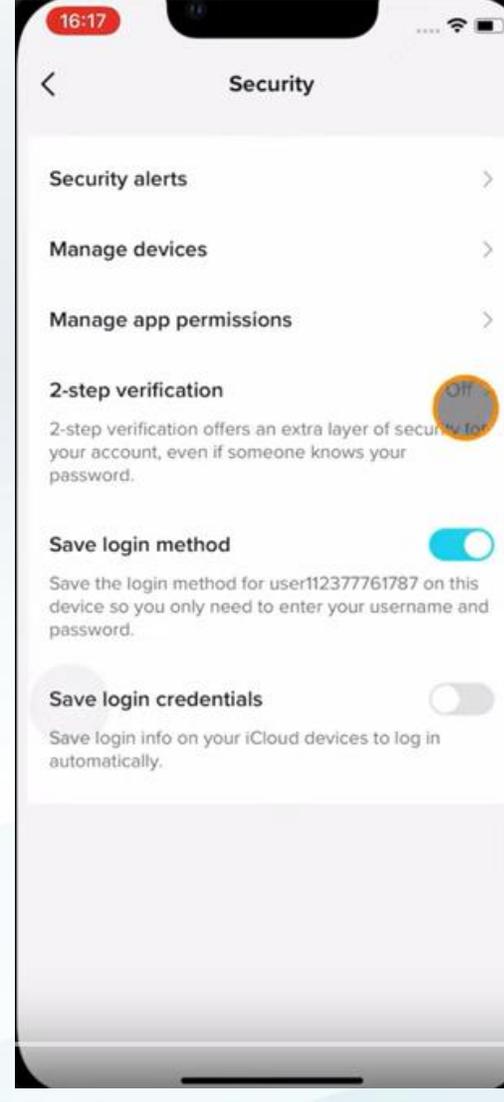
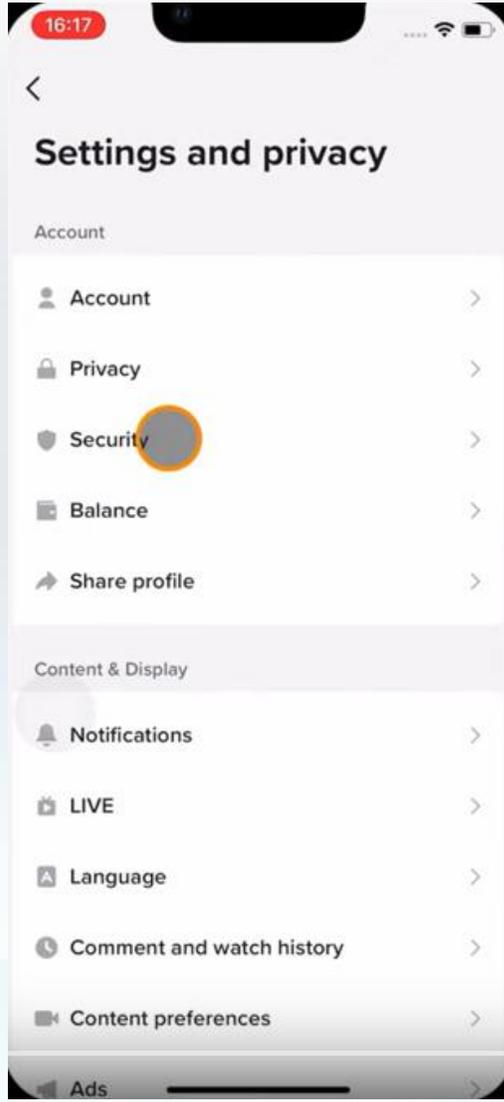
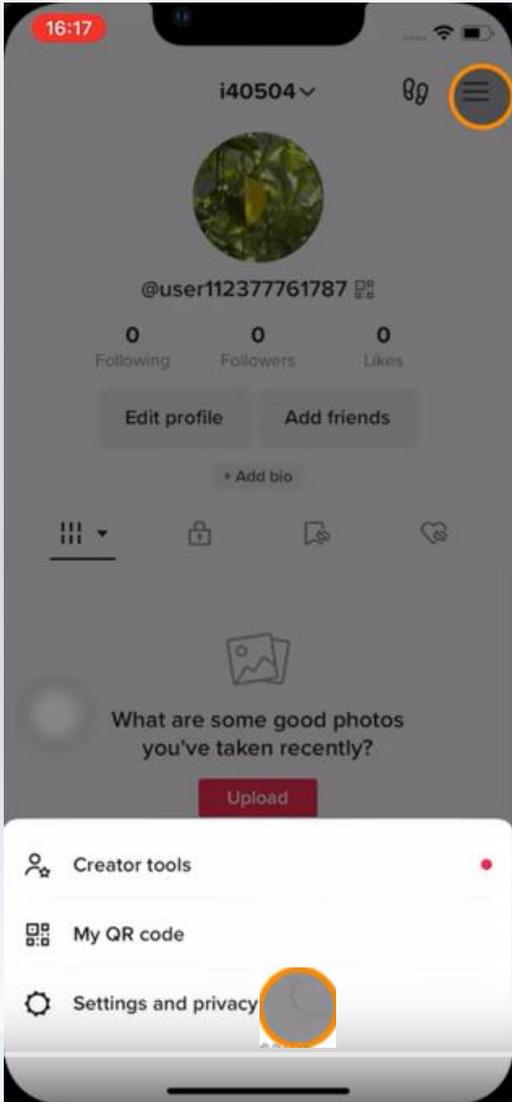
 Google

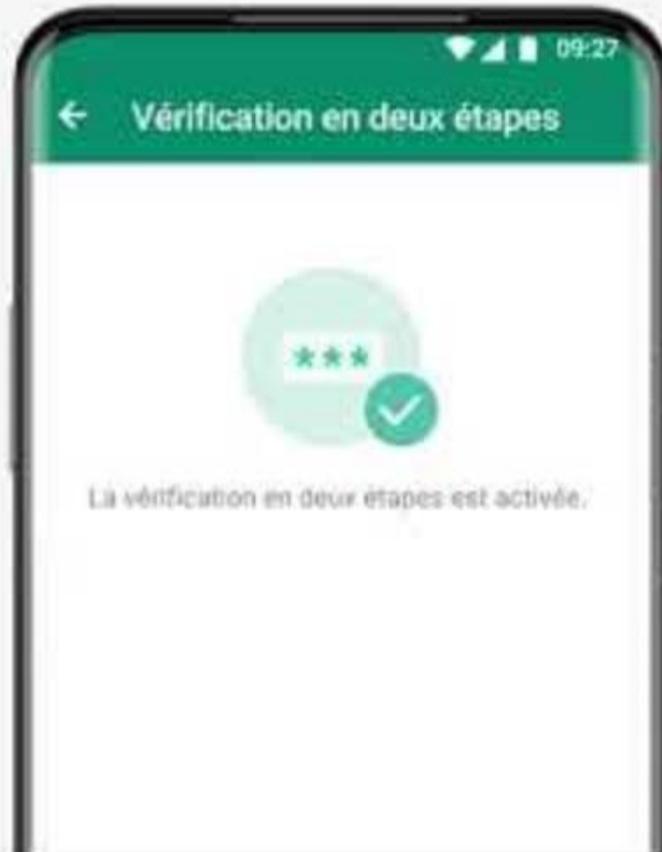


 Microsoft

Exemples d'app TOTP (Time-based One Time Password)







**L'ajout de votre  
adresse e-mail  
est facultatif**



## Test phishing

Typosquatting – Analyse de messages

The screenshot shows a Gmail interface with a phishing email from Luke Johnson. The email content is as follows:

Luke Johnson a partagé un lien vers le document suivant :

[Budget département 2021.docx](#)

---

Bonjour. Voici le document demandé. N'hésitez pas à me contacter si vous avez besoin d'autre chose !

[Ouvrir dans Docs](#)

Rechercher dans toutes les conversations

Actif

1 sur 24 468

Google

16:23

Boîte de récepti... 1 459

Messagerie

Messages suivis

En attente

Messages envoyés

Discussions

Aucune conversation

Démarrer une discussion

Salons

Visioconférences

Luke Johnson <luke.json8000@gmail.com> à moi

Luke Johnson a partagé un lien vers le document suivant :

[Budget département 2021.docx](#)

Bonjour. Voici le document demandé. N'hésitez pas à me contacter si vous avez besoin d'autre chose !

Ouvrir dans Docs

<http://drive--google.com/luke.johnson>

## Adresse email

pierre.martin@orange.fr

**Nom d'utilisateur**

**Extension**

**Nom de domaine**



Le nom de domaine s'analyse de la droite vers la gauche

## Adresse email

pierre.martin@orange.fr

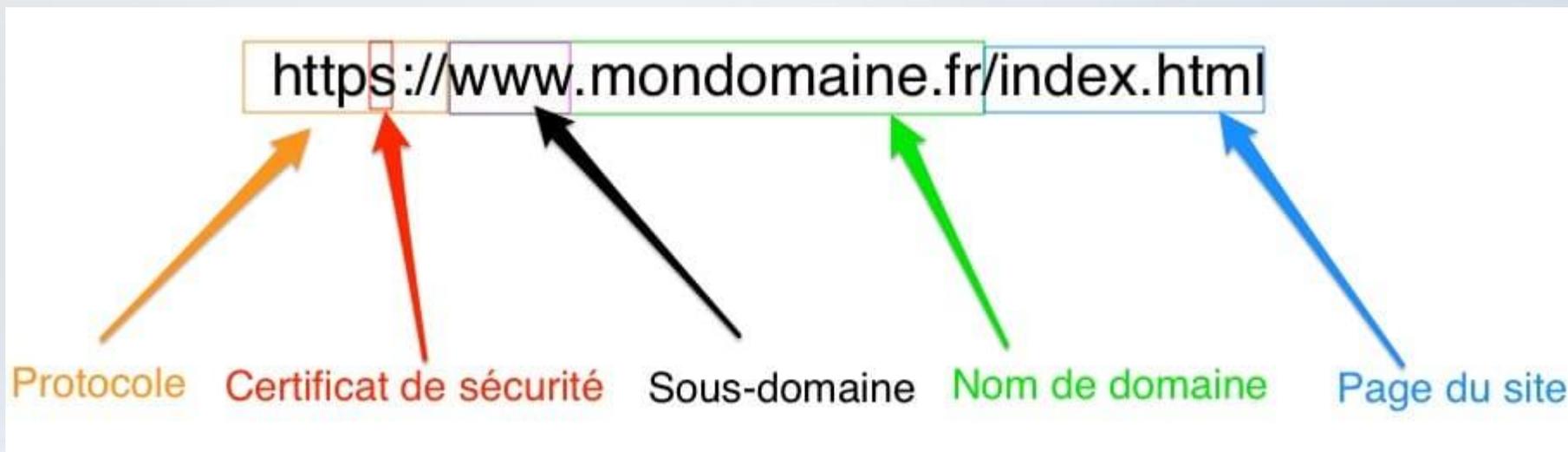
**Nom d'utilisateur**      **Extension**

**Nom de domaine**

### Exemples d'adresses suspectes :

- cartes-grises@yahoo.fr (nom d'utilisateur)
- support@google.xyz (extension)
- direction@impots.gouv.fr.nomdedomainegratuit.fr (nom de domaine + sous-domaine)

## Adresse web (URL)



# Typosquatting : oubli d'une lettre dans la marque cybersquattée

Affelou.com

Liens associés

- Lunettes
- Lunettes Afflelou
- Alain Afflelou
- Afflelou
- Krys Lunettes
- Lunette Afflelou
- Lunettes Afflelou Femme

<affelou.com> D2020-2074

Click here to buy this domain

Bazachic.com

Liens associés

- Mode Femme
- Robe Femme
- Robe Soirée
- Pour
- Robes Pour Mariage
- Robes Soirée
- Robes Femme

<bazachic.com> D2019-1404

havaiana.com

Related Links

- Havaiana Slippers
- Slim
- Havaianas Slippers
- Flat Slippers
- Flat
- Havaianas
- Slippers

Related Links

- Havaianas Flip Flops
- Havaianas
- Sandals
- Havaiana
- Havaianas Slim
- Havaianas Flat
- Sandálias
- Havaiana Slim

<havaiana.com> D2019-0777

jackdaniel.com

Related Links

- Jack Daniels
- Jack Daniel
- Wine and Gift Baskets
- Gift Baskets Gifts
- Get Well Gift Baskets

Related Links

- Wine and Gift Baskets
- Gift Baskets Gifts
- Gourmet Food Gift Baskets
- Send a Gift Basket
- Gifts Flowers Delivery

<jackdaniel.com> FA1712001762300

leroymerli.es

Búsquedas relacionadas

- TIENDAS ONLINE
- CATALOGO BRICODEPOT
- BRICOLAGE
- PALACIO DE HIERRO
- BRICODEPOT

Comprar este dominio.

<leroymerli.es> DES2021-0021

Meilleurtaux.com

Liens associés

- Simulation Crédit Immobilier
- Simulation Pret Credit Immobilier
- Les Taux Credit Immobilier
- Simulateur Taux Credit
- Meilleur Taux Crédit Immobilier
- Credit Rachat
- Taux Credit a la Consommation

<meilleurtaux.com> D2019-0326

Luke Johnson a partagé un lien vers le document suivant :

[Budget département 2021.docx](#)

Bonjour. Voici le document demandé. N'hésitez pas à me contacter si vous avez besoin d'autre chose !

Ouvrir dans Docs

<http://drive--google.com/luke.johnson>

The screenshot shows a Gmail interface. On the left, the navigation pane includes 'Messagerie' with a sub-item 'Boîte de récepti...' containing 1459 messages, and 'Discussions'. The main area displays an email from Sharon Mosley (<conseiller@ca-aquitaine.xyz>) with a purple profile picture and the text 'à moi'. The email body contains the following text: 'Bonjour Anthony DON, Veuillez trouver ci-joint le rapport d'activité financière de 2021, à lire attentivement. Cordialement, Mme Sharon Mosley'. Below the text is a placeholder for a PDF attachment, showing a 'PDF' icon and a thumbnail of a document titled 'R.A.F. 2021.pdf'. The top of the interface shows the Gmail search bar, the 'Actif' status, and the Google logo with a profile picture.

# Savoir réagir face à une attaque informatique





## Signaux faibles

- Ralentissement du système
- Connexions ou activités inhabituelles
- Impossibilité de se connecter à la machine
- Services ouverts non autorisés



## Signaux forts

- Fichier(s) disparu(s) ou chiffré(s), inaccessible(s)
- Modification du coffre-fort de mots de passe
- Messages de rançon
- Création ou destruction de comptes utilisateurs
- Envoi de mails de votre part

Quelles sont les 1ères actions à mettre en place ?

**Isoler** - *Ne pas éteindre les postes infectés mais couper tous les accès réseaux*

**Confiner** - *Mettre en quarantaine les postes infectés et les supports amovibles*

**Sauvegarder** (*journaux d'activité, docs, emails, fichiers, trafic réseau*) + *copie des supports / acquisition mémoire vive*

**Collecter** – *Les renseignements auprès des collaborateurs témoins*

**Communiquer**

Il est primordial de déposer une plainte en cas de menaces, pour les mêmes raisons que nous portons plainte pour tout acte répréhensible dont nous sommes victime.

La création d'un point de contact unique et privilégié sur la Nouvelle-Aquitaine avec une adresse mail dédiée en cas de doute ou d'attaque avérée :

[cybermenaces-bordeaux@interieur.gouv.fr](mailto:cybermenaces-bordeaux@interieur.gouv.fr)





## La police judiciaire de Bordeaux au cœur du démantèlement du réseau cybercriminel international «Hive»

Par Marie-Hélène Hérouart

Publié le 26/01/2023 à 20:36 , mis à jour le 27/01/2023 à 02:29

[Copier le lien](#)



Écouter cet article

00:00/04:42



# Des ressources



<https://www.ssi.gouv.fr/entreprise/bonnes-pratiques/>



<https://secnumacademie.gouv.fr/>

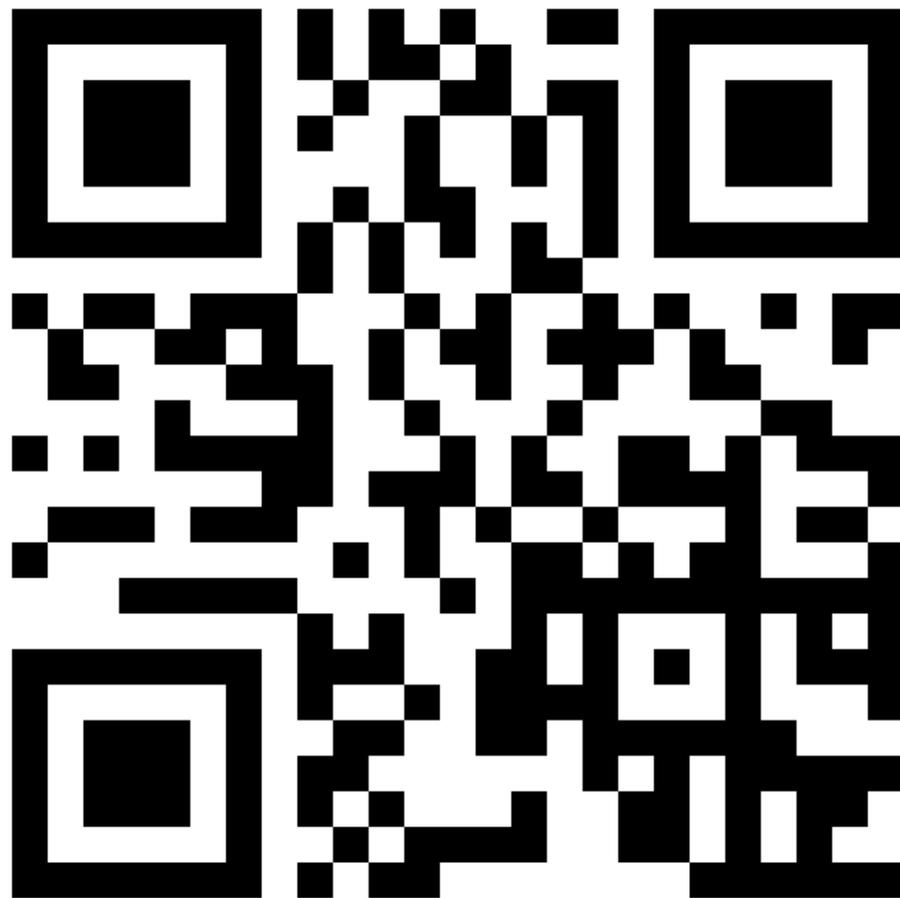
## CNIL.

<https://www.cnil.fr/fr/cybersecurite>



<https://www.cybermalveillance.gouv.fr/cybermenaces>





<https://etc.ch/BZFB>

Merci de votre attention

[cybermenaces-bordeaux@interieur.gouv.fr](mailto:cybermenaces-bordeaux@interieur.gouv.fr)

