SENSIBILISATION AUX RISQUES CYBER

POLICE NATIONALE

POLICE NATIONALE · DIRECTION CENTRALE DE LA POLICE JUDICIAIRE ·

RECYM

RÉSEAU DES EXPERTS CYBER-MENACES
DE LA DIRECTION NATIONALE
DE LA POLICE JUDICIAIRE

Mise à jour : 15 Avril 2024

Présentation des animateurs

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

Réseau des Experts Cybermenaces - RECyM

- 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 :

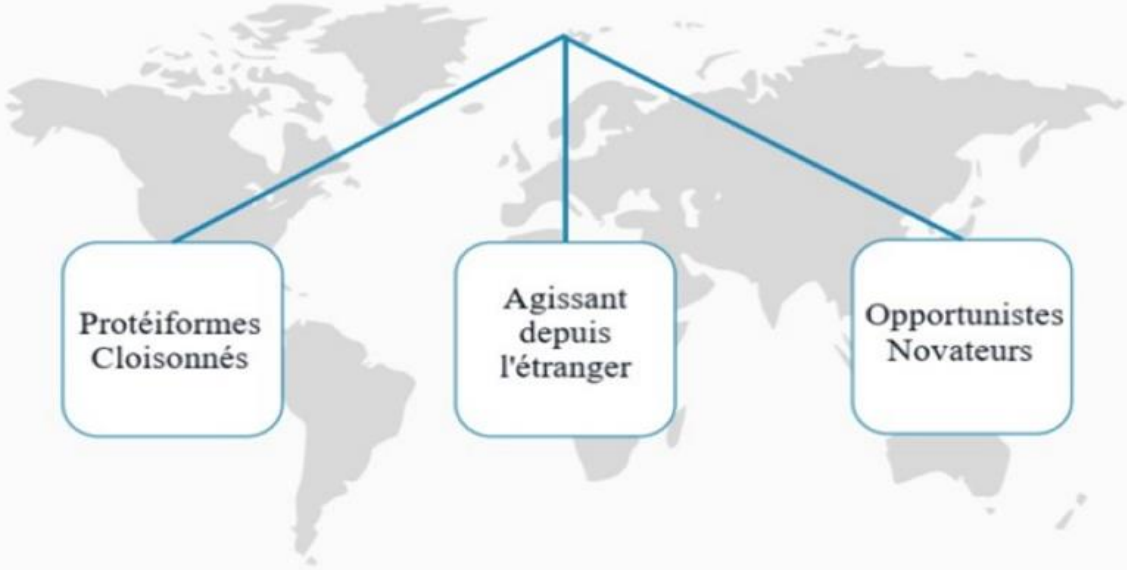
RECYM
RÉSEAU DES EXPERTS CYBER-MENACES
DE LA DIRECTION NATIONALE
DE LA POLICE JUDICIAIRE

cybermenaces-bordeaux@interieur.gouv.fr

Évolution de la criminalité organisée depuis 20 ans

Evolution d'une délinquance en bande organisée au niveau national…

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



Les intentions criminelles

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

Les escroqueries

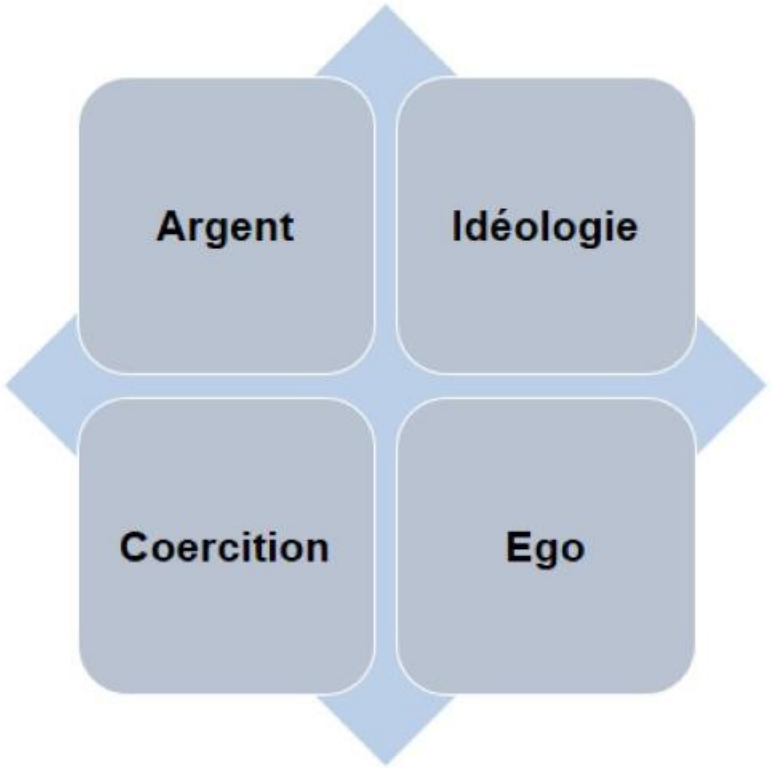
Art 313-1 CP:

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

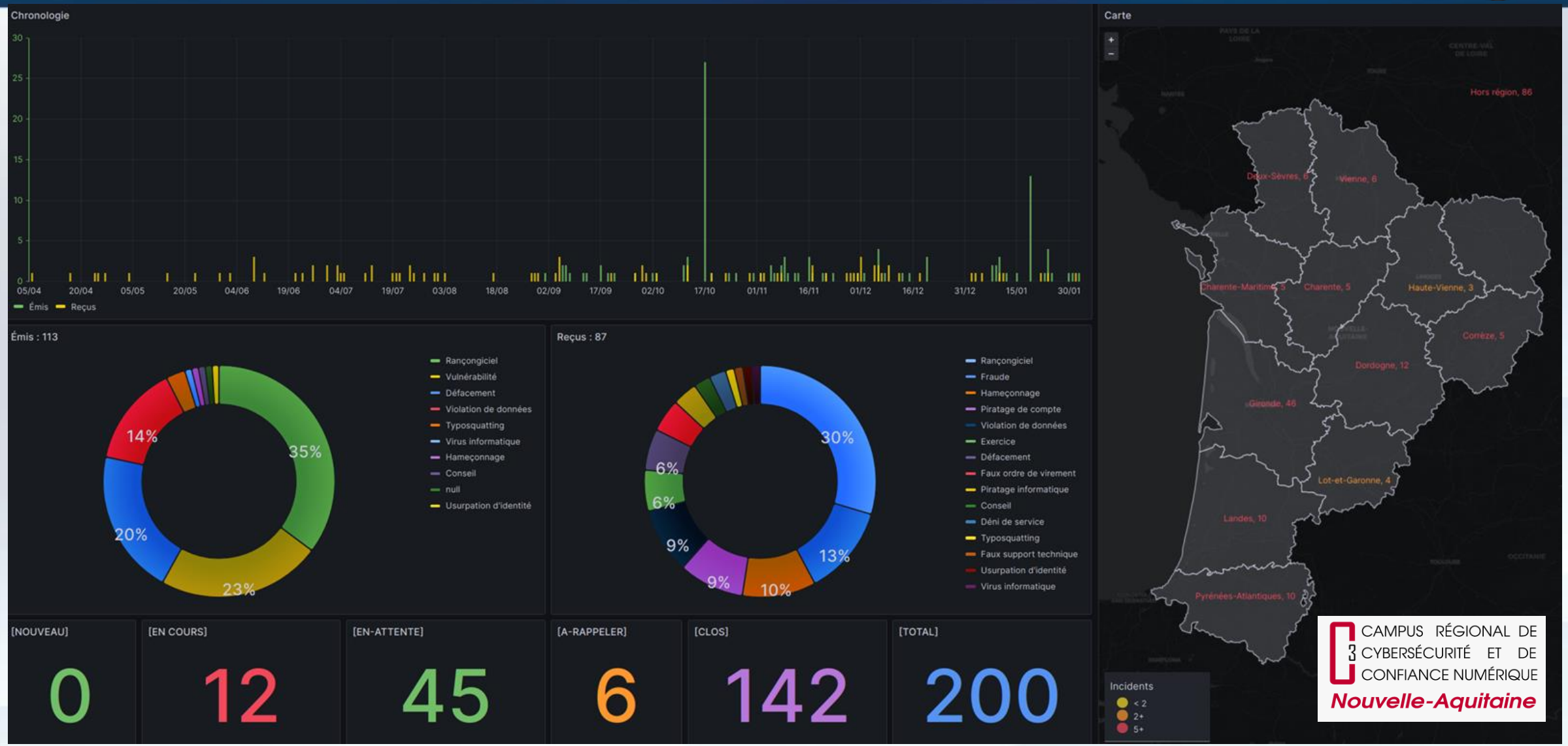
Matrice d'influence en escroquerie et ingénierie sociale sur les réseaux sociaux

Matrice MICE + Réseaux sociaux



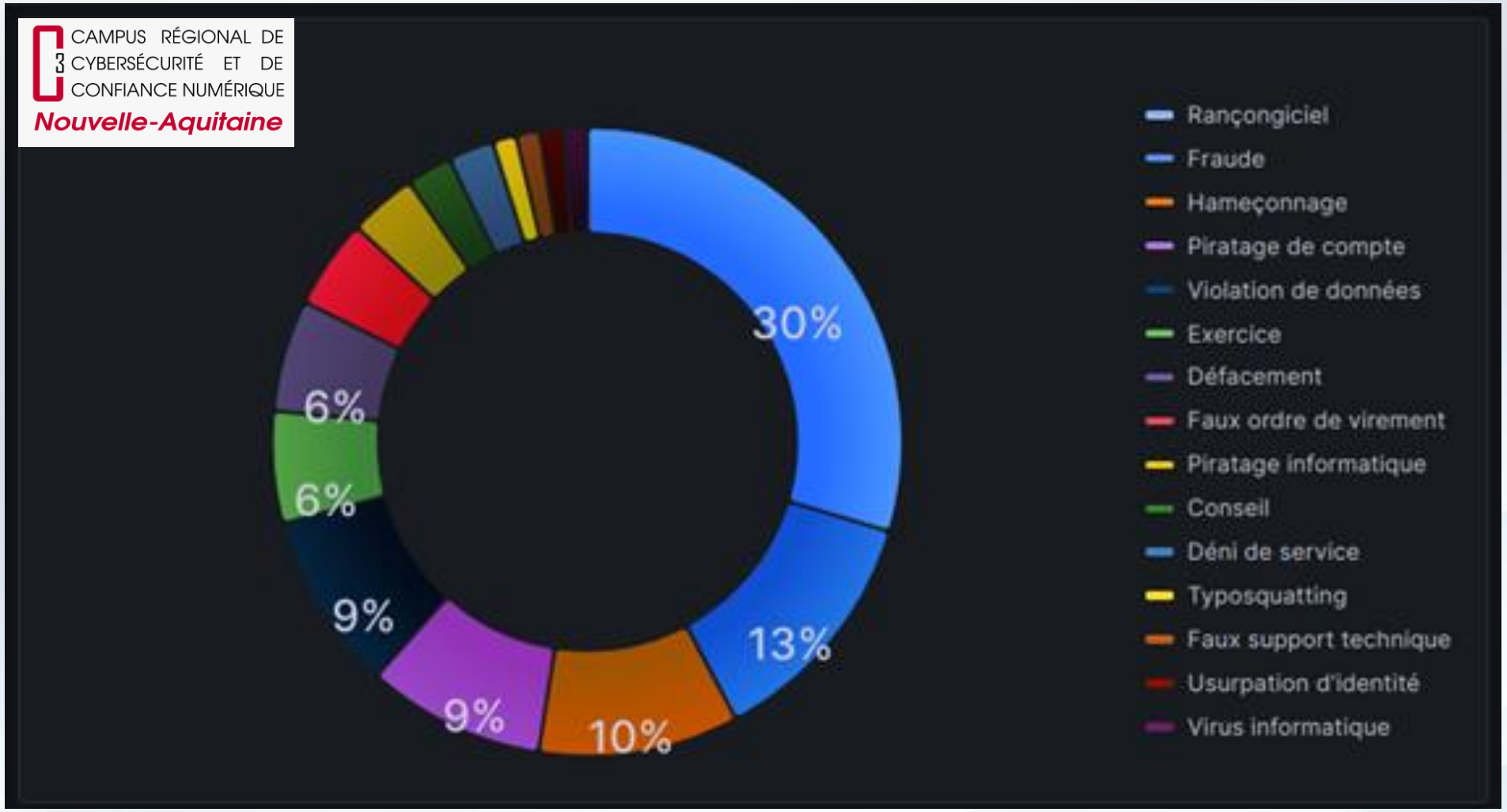
Facebook
Twitter
Instagram
Pinterest
viadeo
LinkedIn

Quelques chiffres sur les modes opératoires



Source : https://www.campuscyber-na.fr/

Quelques chiffres sur les modes opératoires



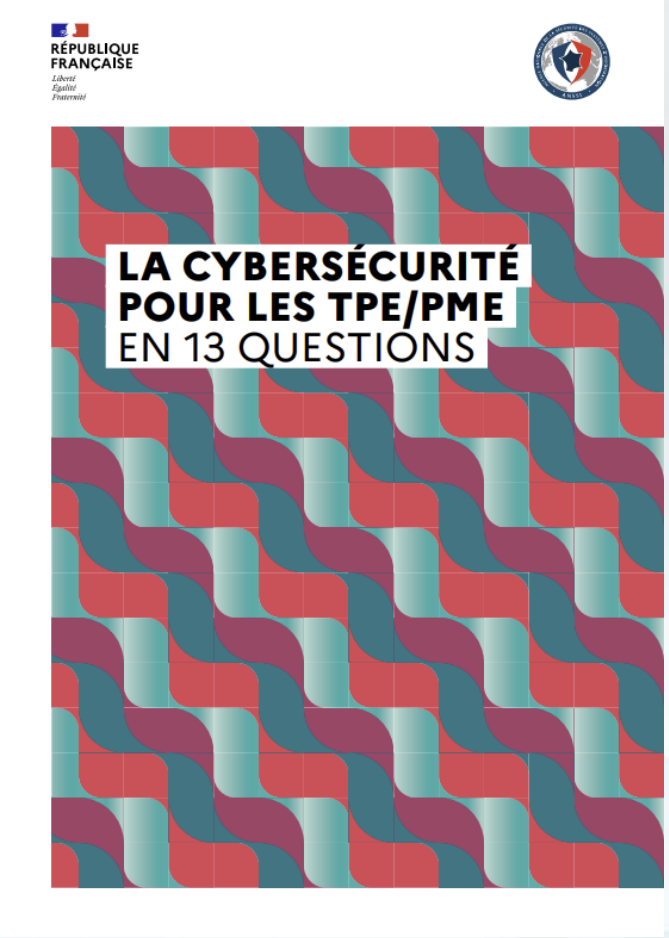
Source : https://www.campuscyber-na.fr/

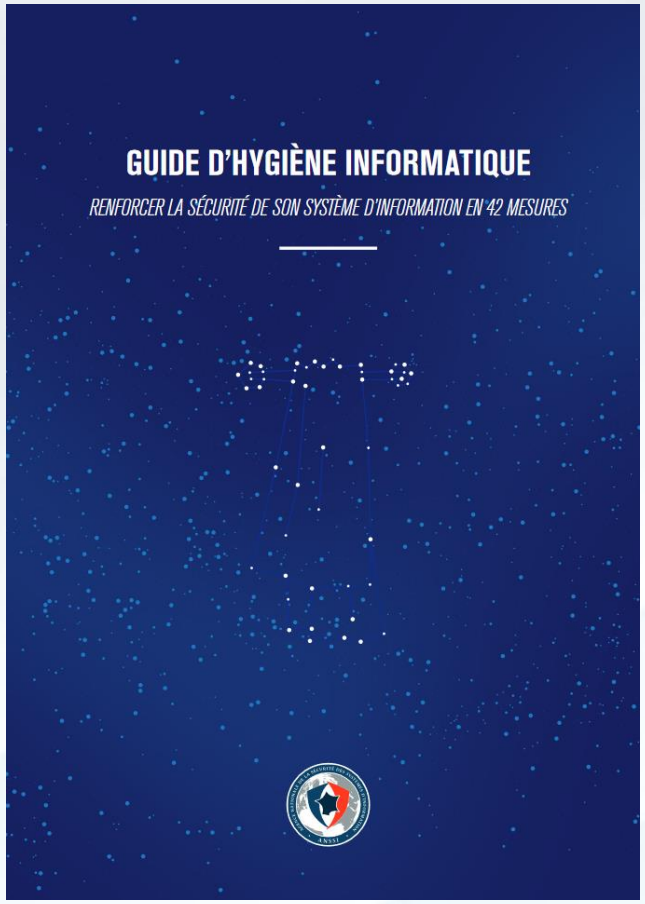
Guides de l'ANSSI

Pour la sécurité de votre entreprise

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

Authentification

Bonnes pratiques – Gestionnaire de mot de passe

Authentification – Choix du mot de passe

- Pourquoi faut il éviter les mot 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

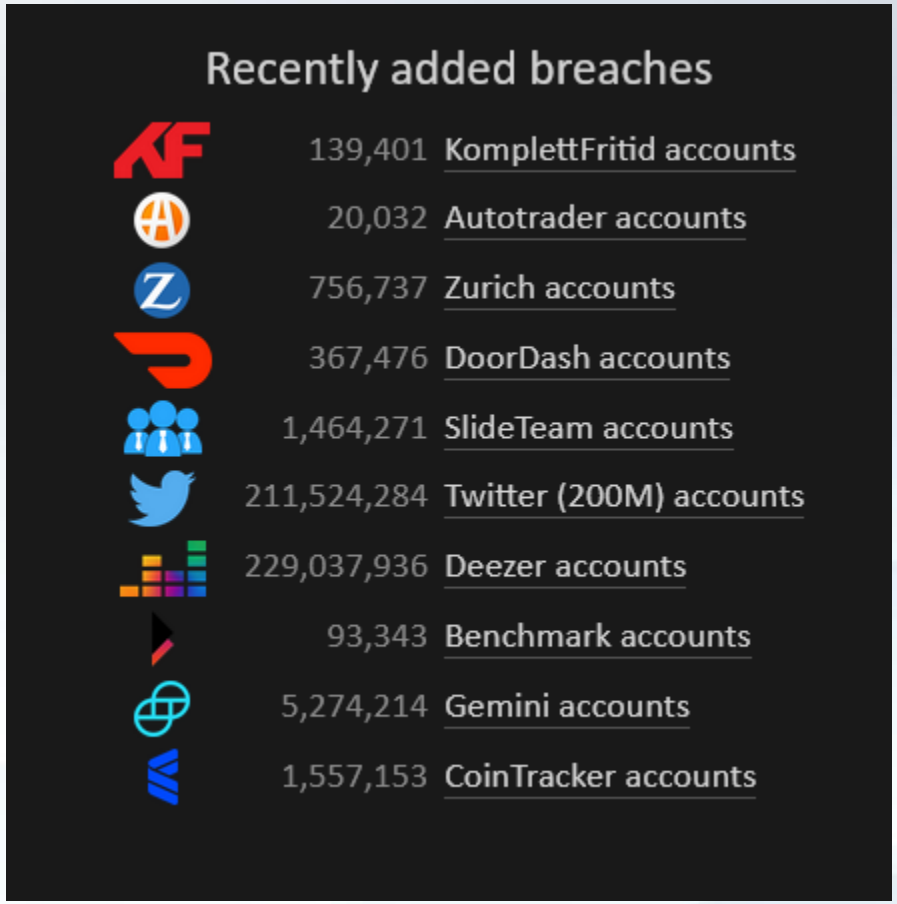
Les pires mots de passe utilisés en France

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

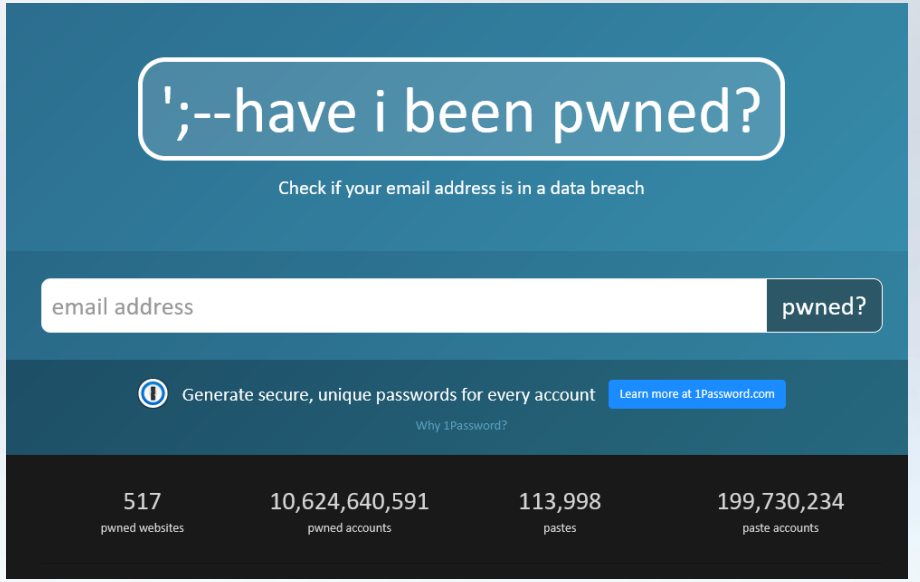
- Mot de passe unique : facile à retenir mais très risqué à cause des fuites de données.
- Compte réseaux sociaux -> Email -> Banque
- Utiliser un mot de passe différent pour chaque service

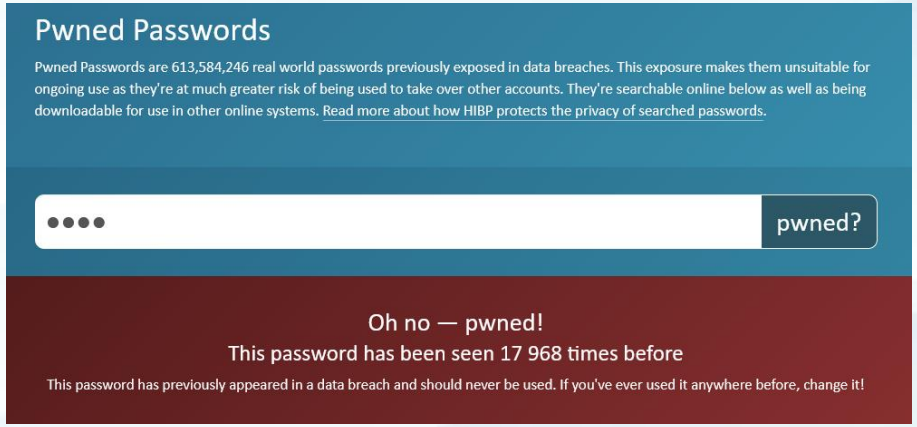


https://haveibeenpwned.com/

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





https://haveibeenpwned.com/

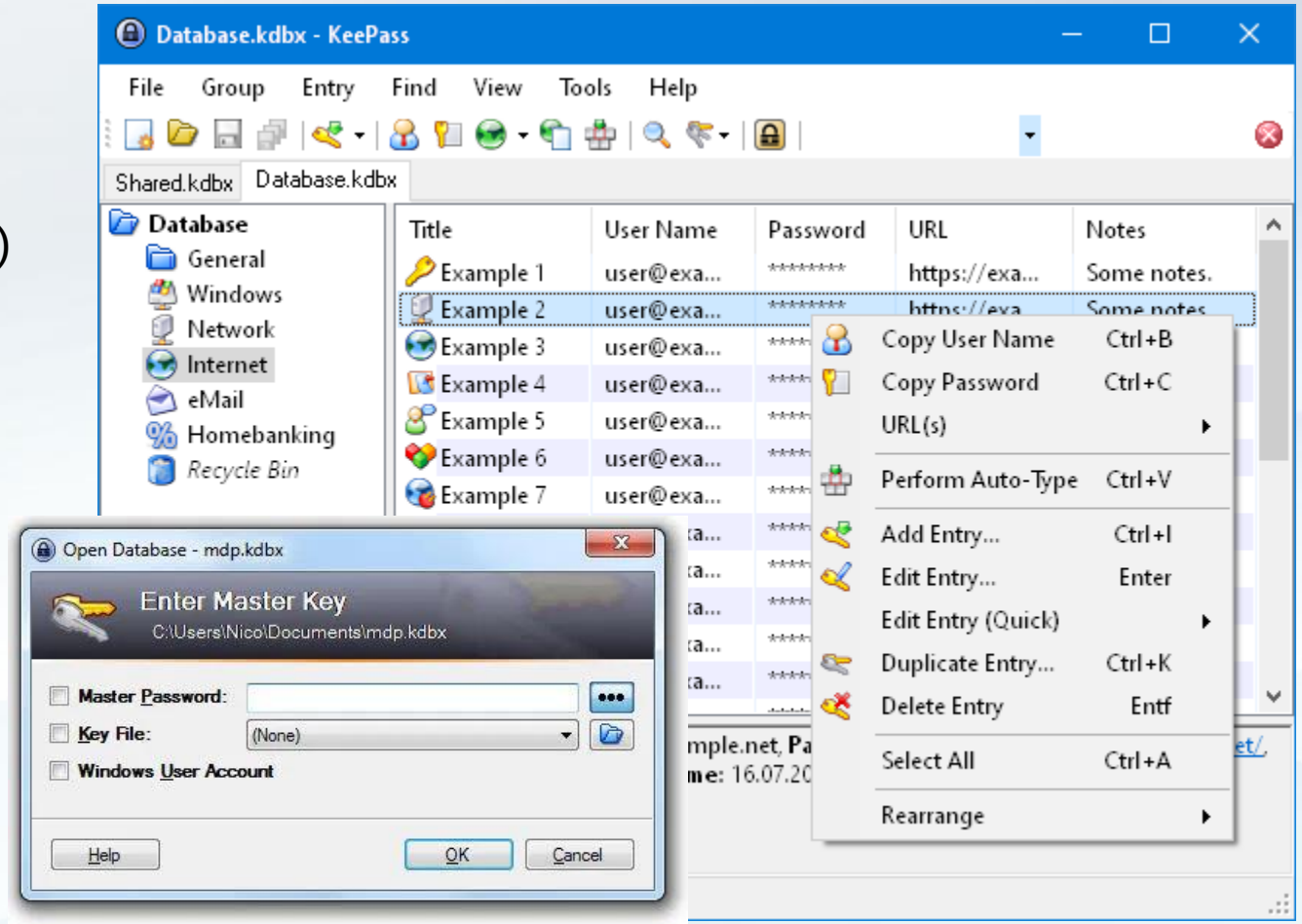
Comment gérer ses mots de passe ?

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

Coffre fort de mot de passe

Coffre fort pour mots de passe

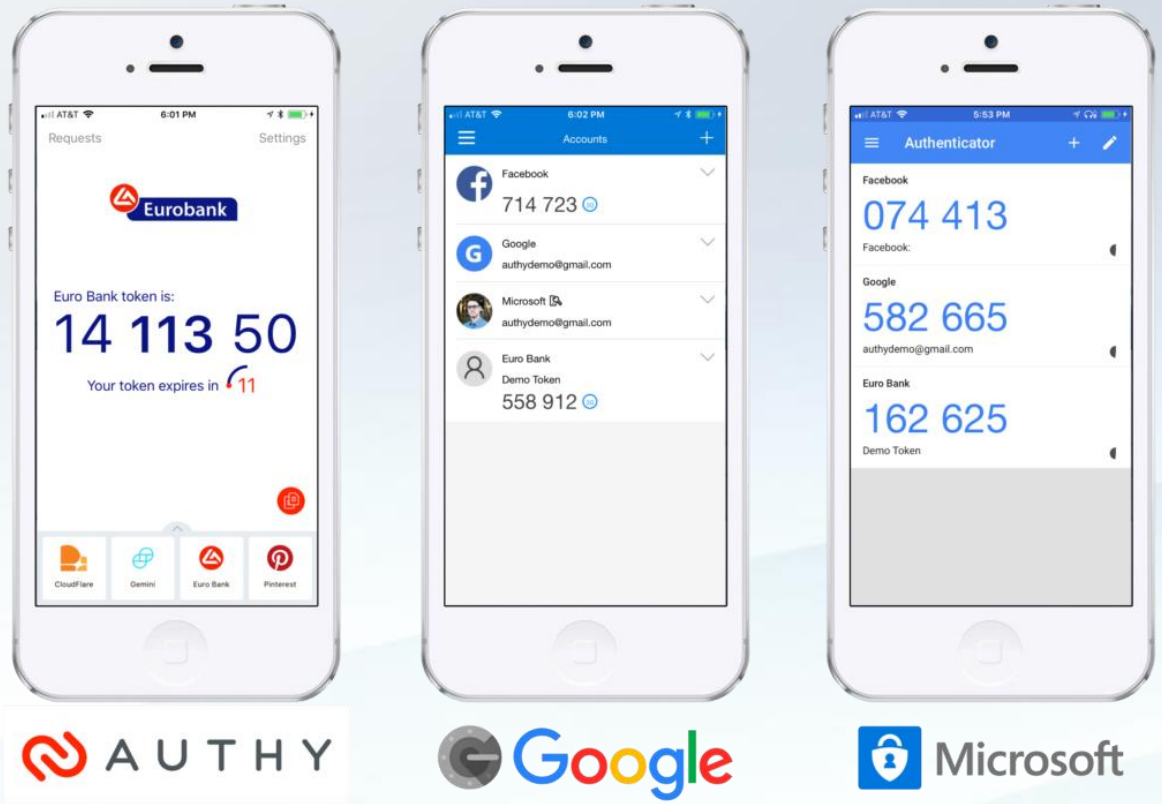
- Utilisation d'un gestionnaire de mot de passe
- Stockage de vos mots de passe dans un fichier chiffré (protégé par mot de passe : 1 seul à retenir)
- Génère les mots de passe pour vous (robustes et uniques)
- Saisit les mots de passe pour vous (directement ou via un plugin de navigateur)
- Le fichier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



https://www.ssi.gouv.fr/entreprise/certification_cspn/keepass-version-2-10-portable/

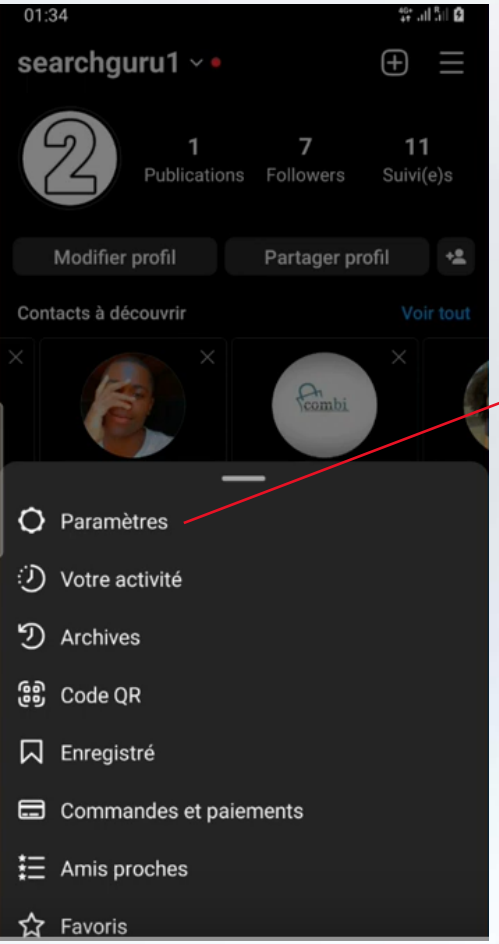
Authentification à 2 facteurs (2FA)

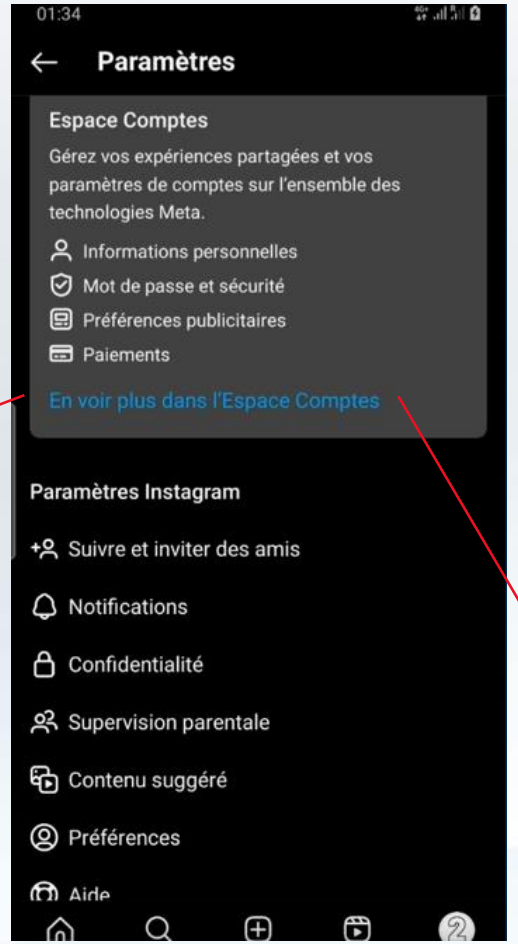
- Principe : compléter votre mot de passe (élément connu) avec un 2ème élément détenu (ex: votre smartphone via une app ou un SMS).
- **Bloque les accès** frauduleux en cas de mot de passe faible ou compromis.
- A activer systématiquement quand c'est disponible.

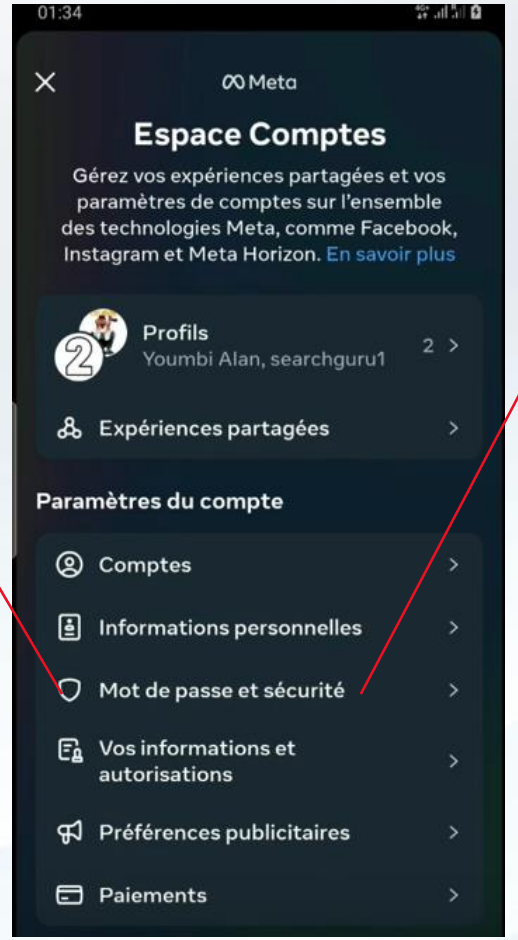


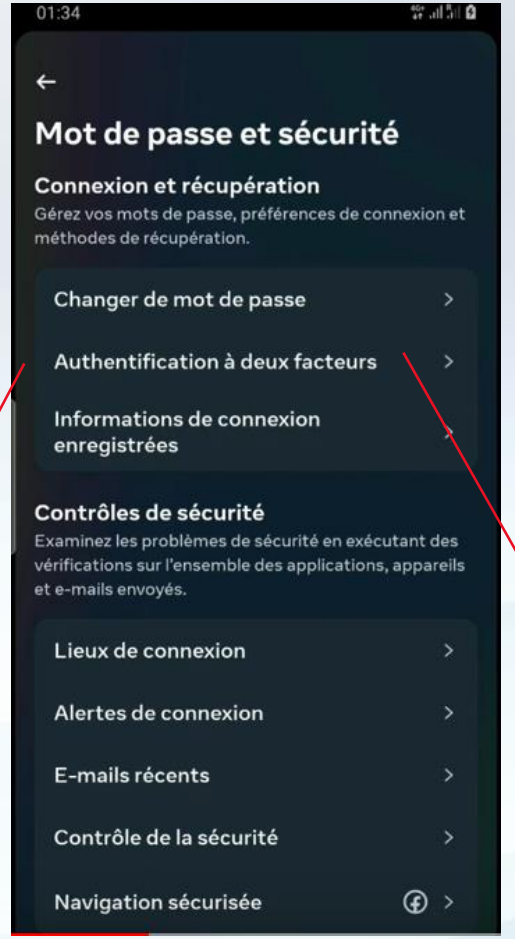
Exemples d'app TOTP (Time-based One Time Password)

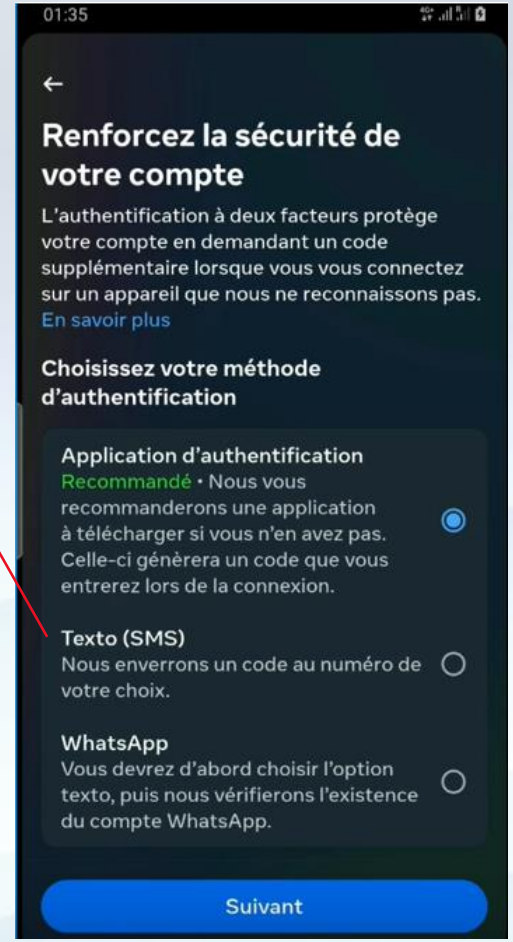
2FA sur appli mobile : Instagram



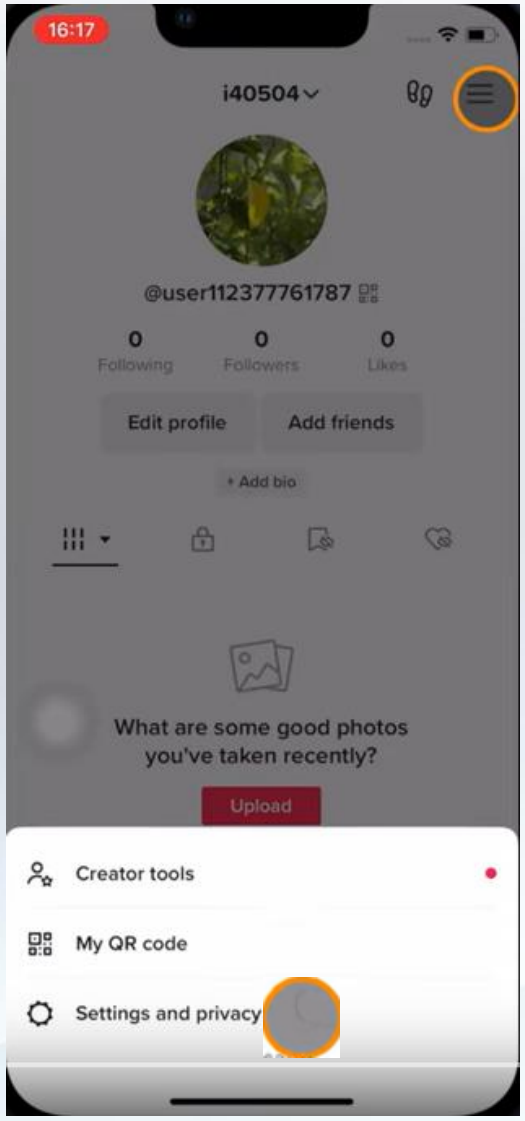


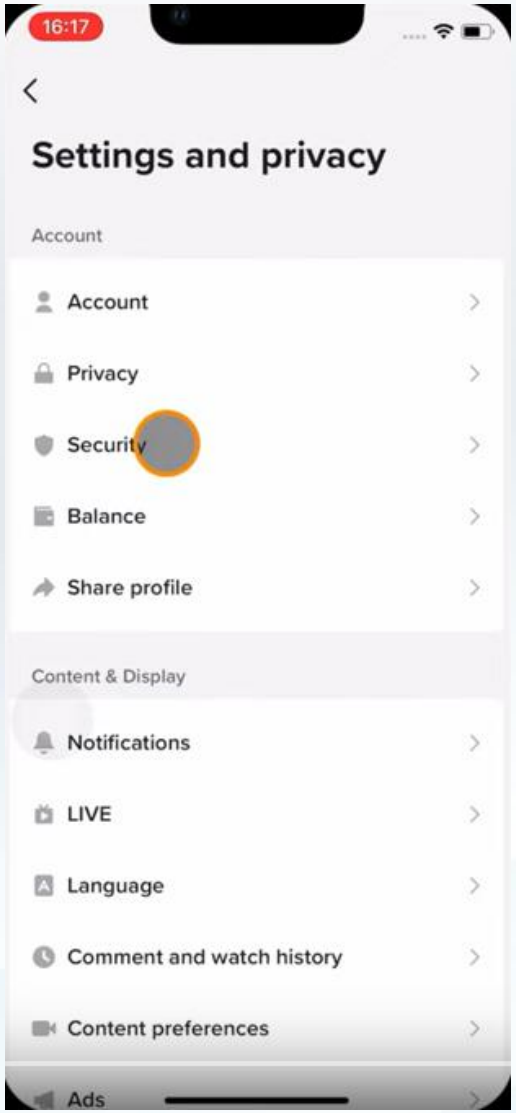


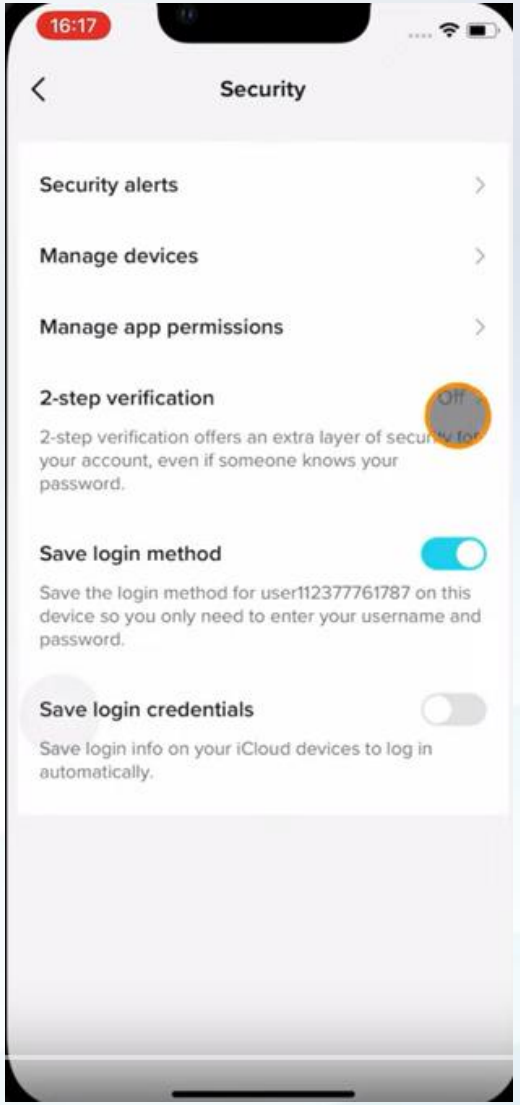


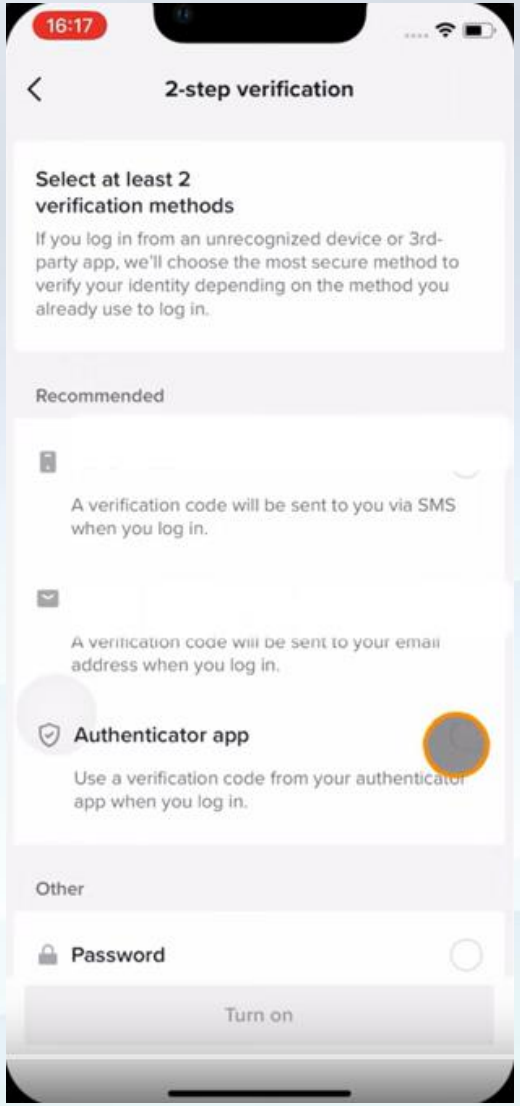


2FA sur appli mobile : Tiktok

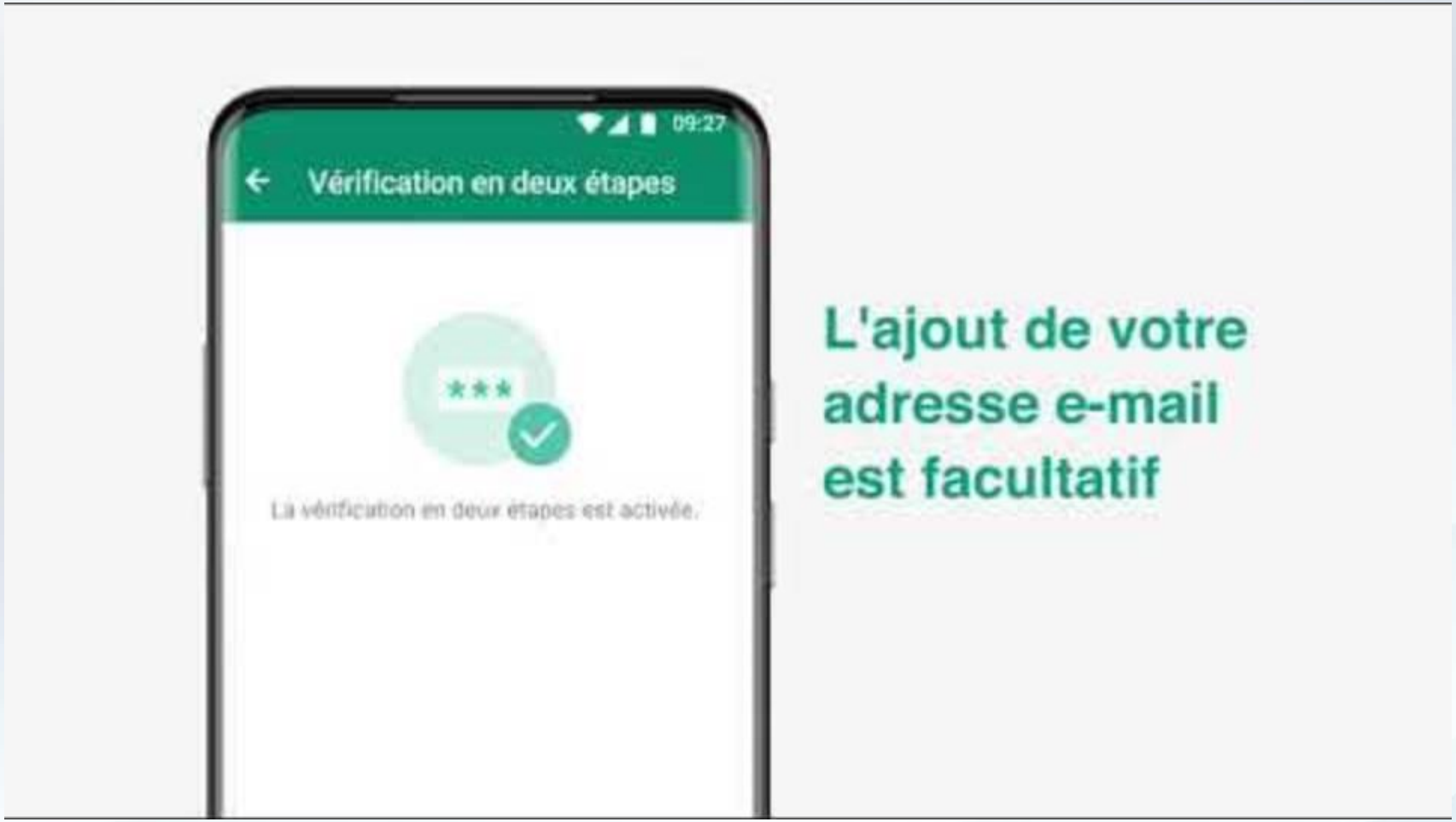




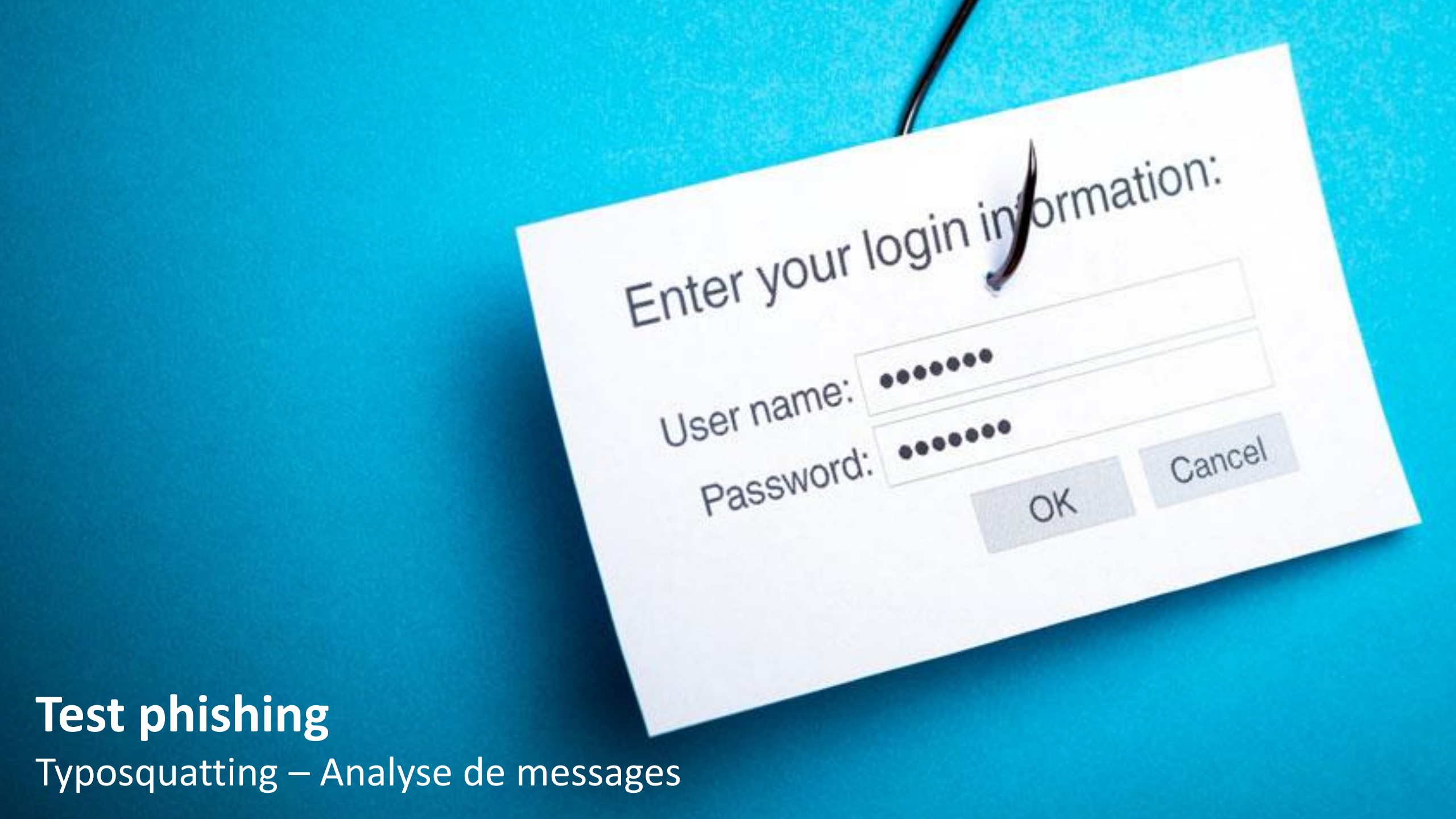




Mot de passe dans WhatsApp



https://www.youtube.com/watch?v=ywyqXvjShv4

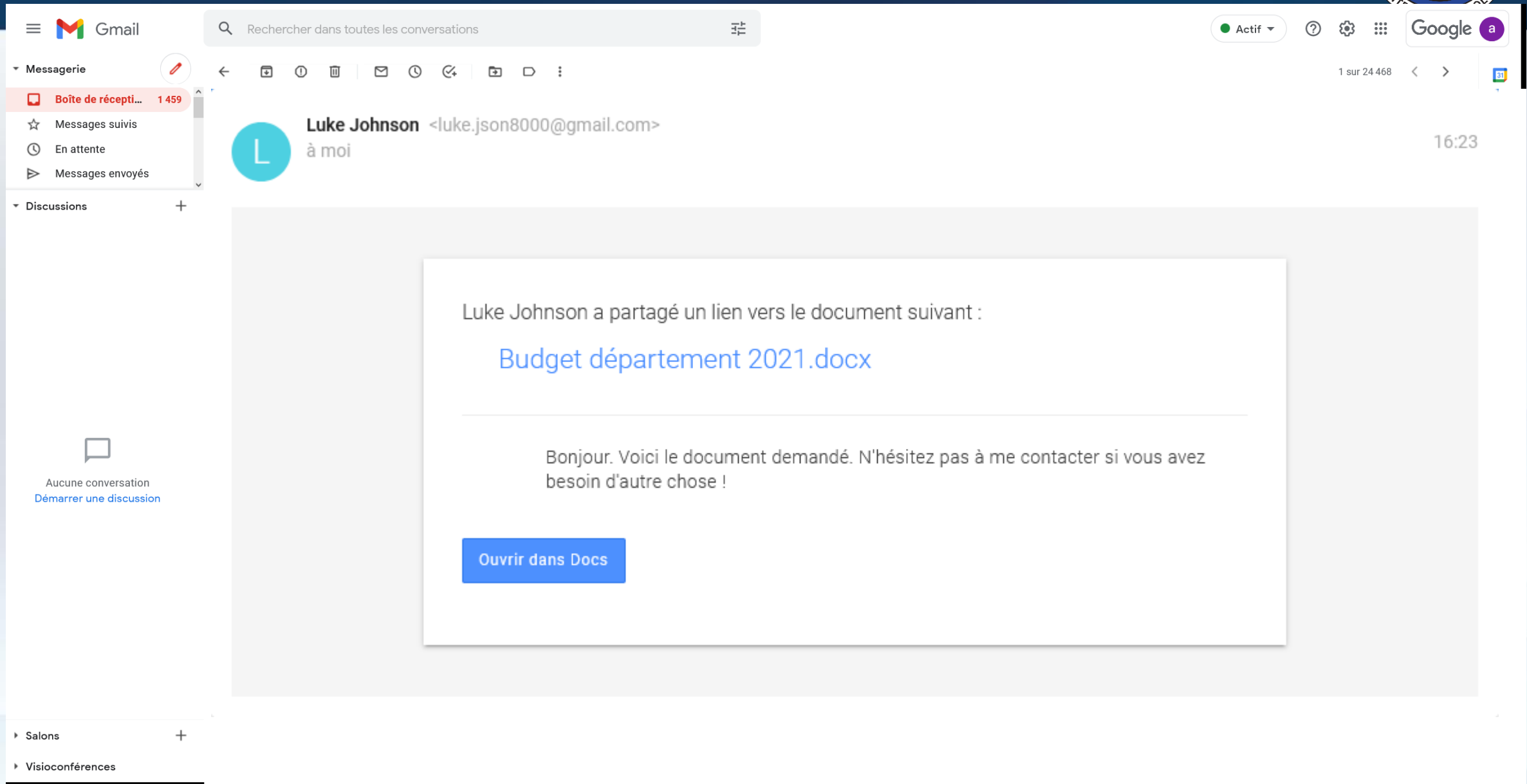


Test phishing

Typosquatting – Analyse de messages

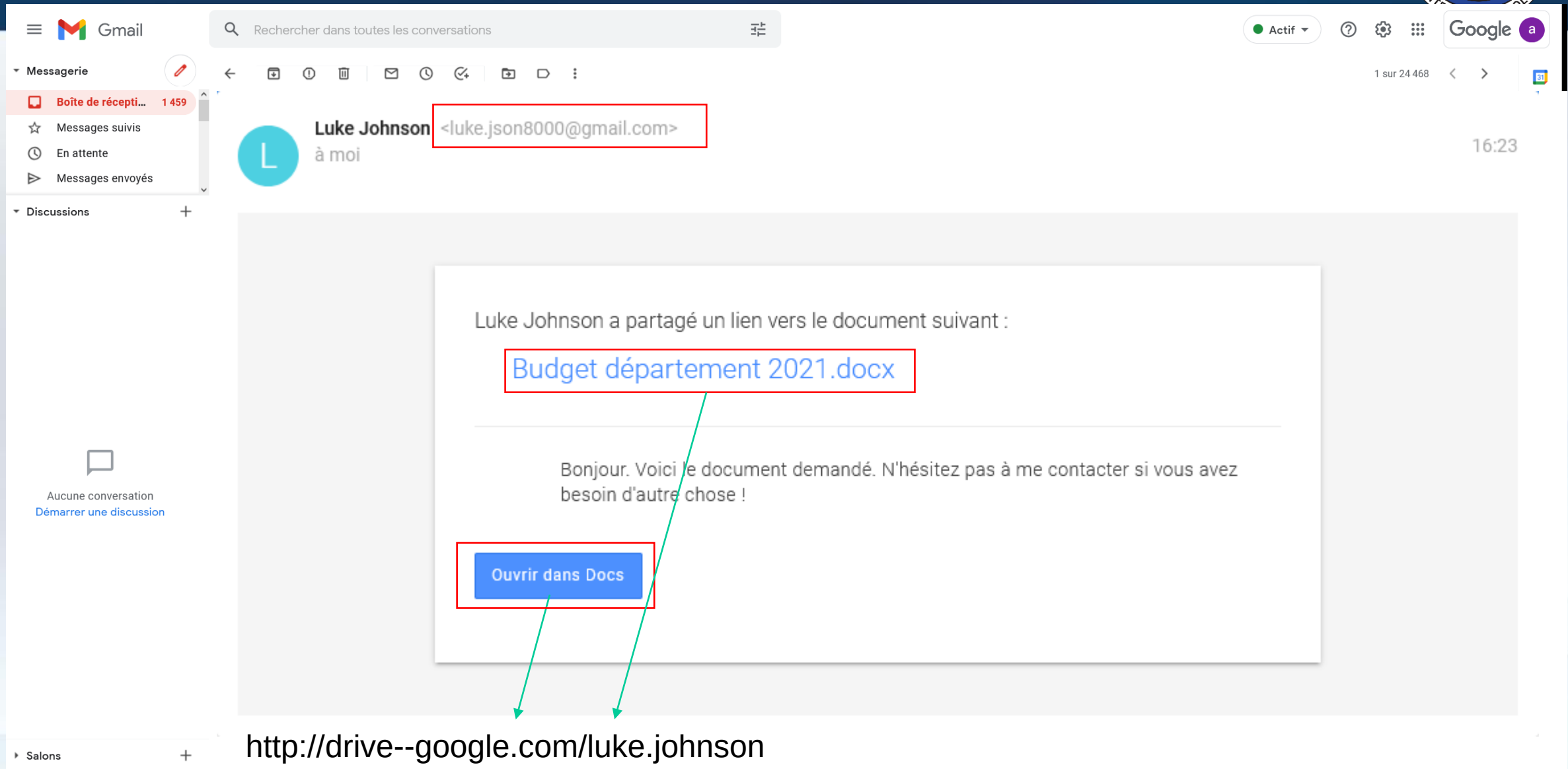
Test phishing – Google Docs

Quizz



Test phishing – Google Docs

Quizz



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

Test phishing – Structure des adresses

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

Test phishing – Structure des adresses

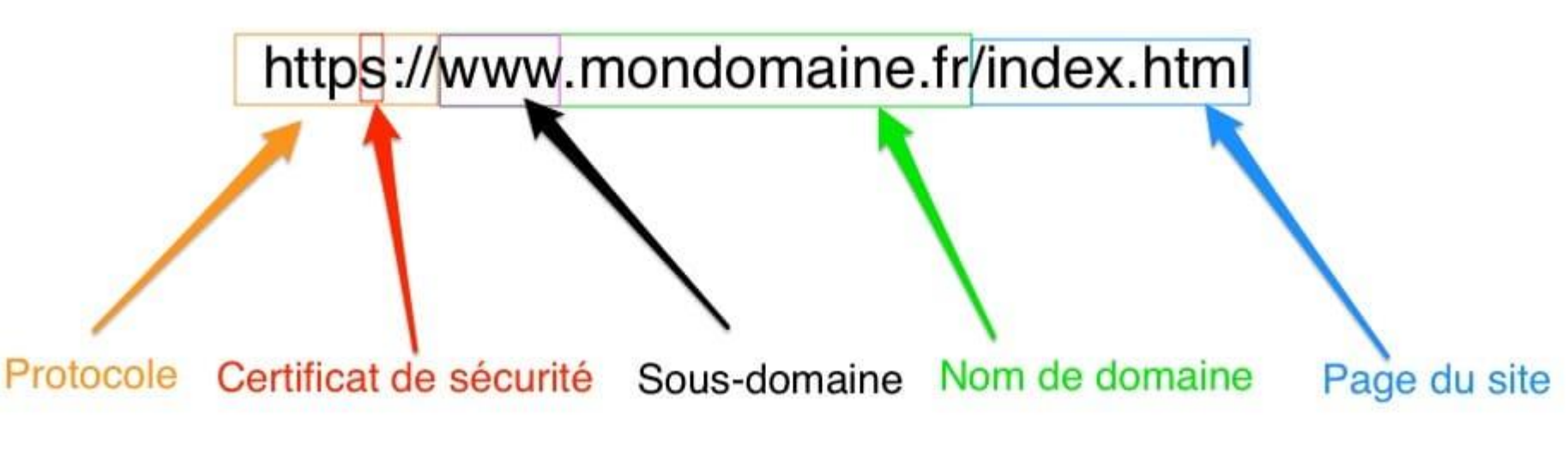
Adresse email

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)

Test phishing – Structure des adresses

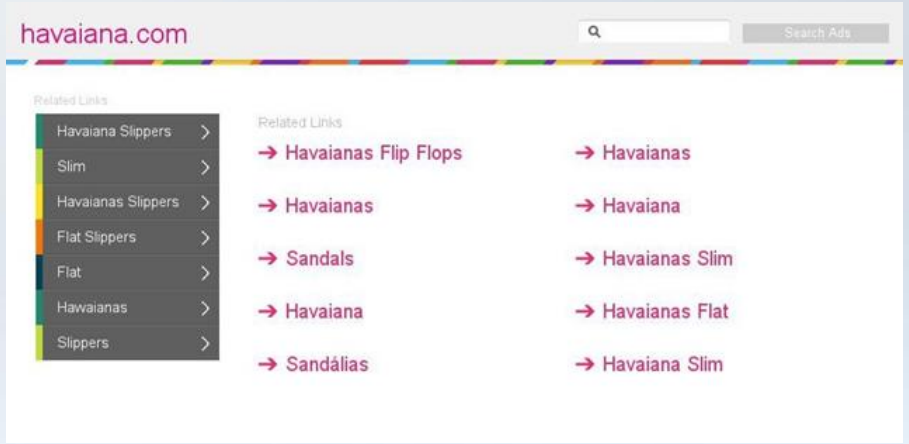
Adresse web (URL)



Typosquatting : oubli d'une lettre dans la marque cybersquattée

<affelou.com> D2020-2074

<bazachic.com> D2019-1404



<havaiana.com> D2019-0777

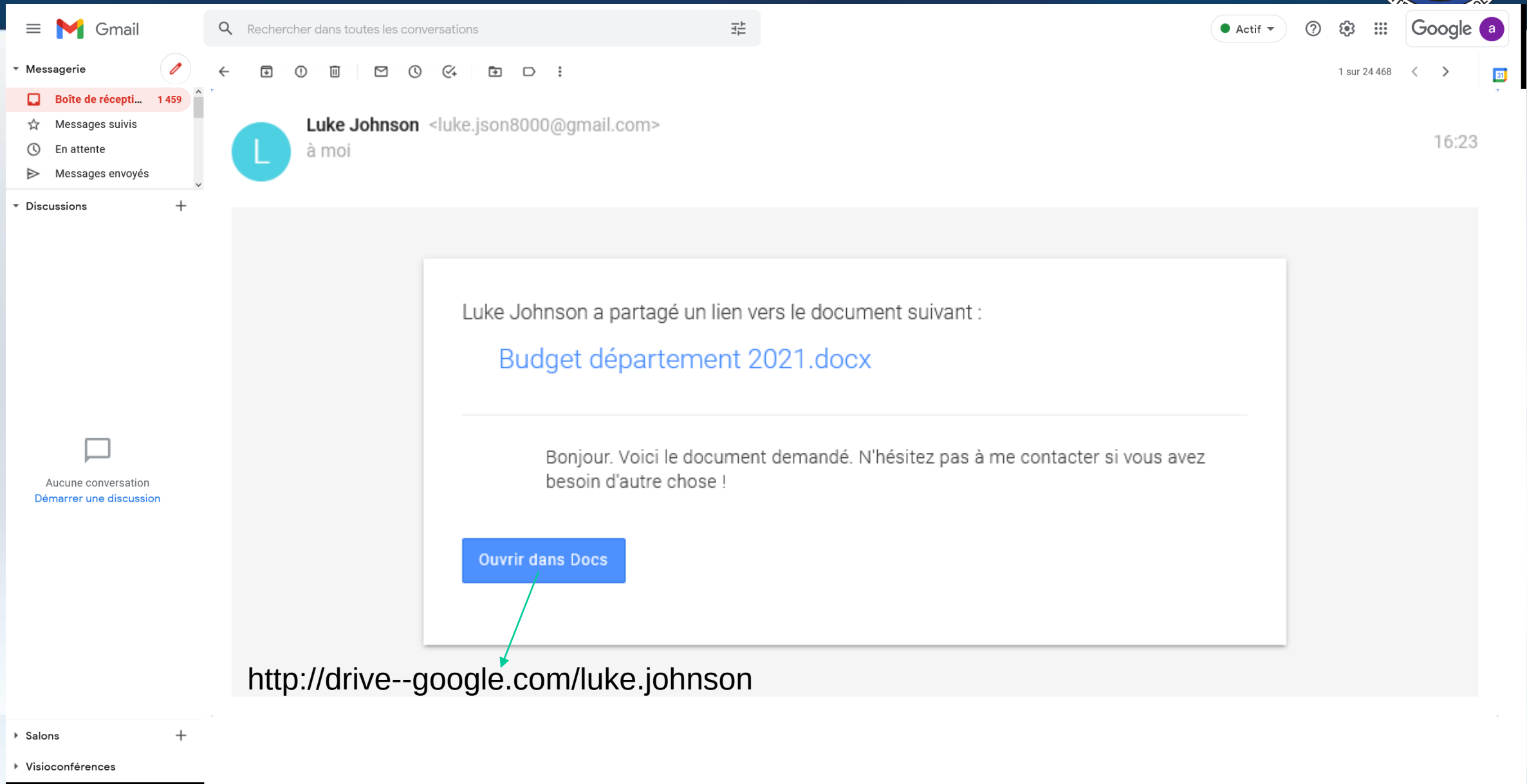
<jackdaniel.com> FA1712001762300

<leroymerli.es> DES2021-0021

<meileurtaux.com> D2019-0326

Test phishing – Google Docs

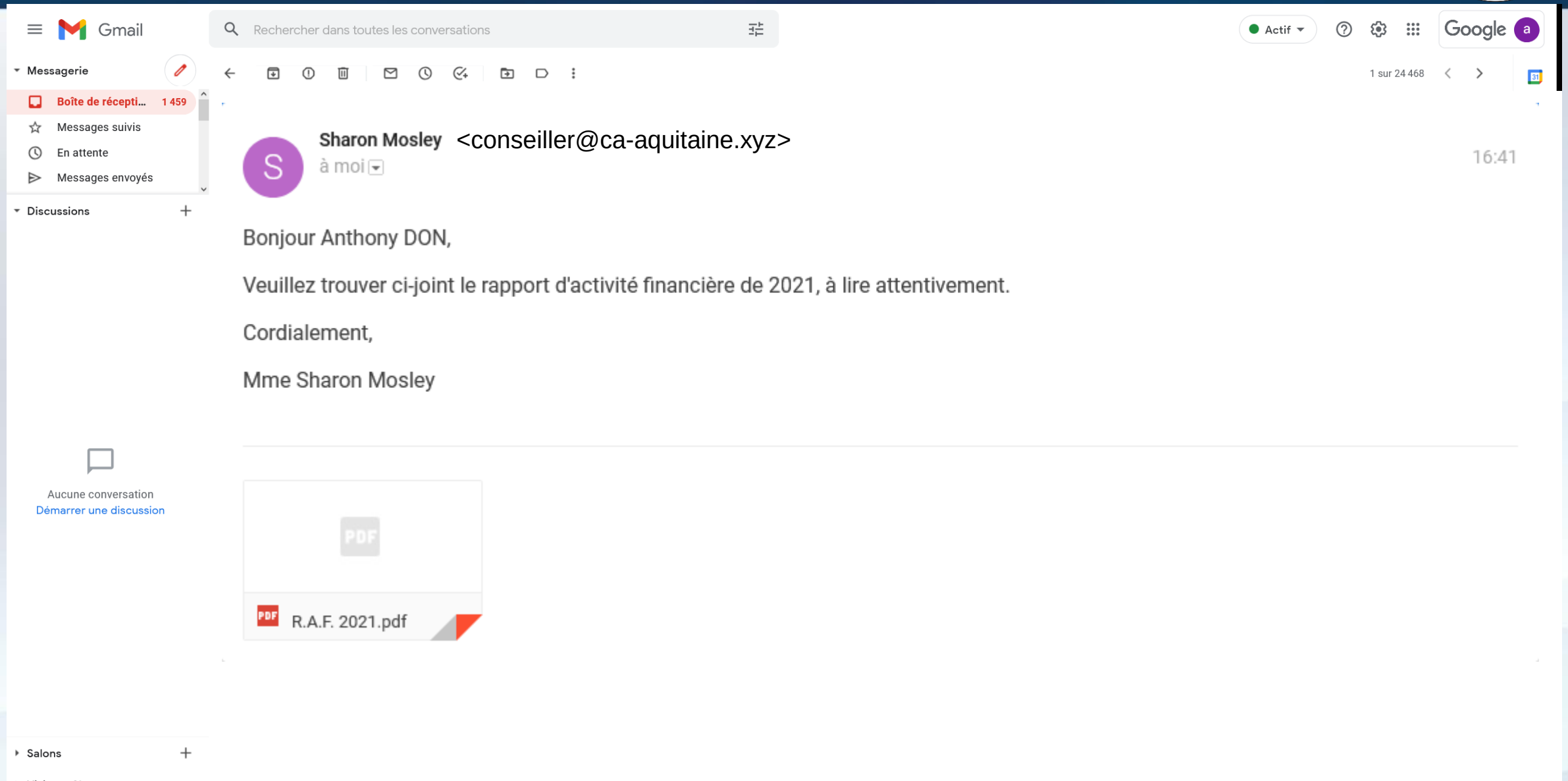
Quizz



POLICE NATIONALE

Test phishing – Google Docs

Quizz



Savoir réagir face à une attaque informatique

Reconnaître les signes d’un système compromis

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

Réflexes en cas d'intrusion

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

Déposer plainte ?

Pour la sécurité de votre entreprise

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

POLICE NATIONALE

Déposer plainte ?

Pour la sécurité de votre entreprise

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

CYBER MALVEILLANCE .GOUV.FR

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

POLICE NATIONALE

QUIZZ

https://etc.ch/BZFB

Merci de votre attention

cybermenaces-bordeaux@interieur.gouv.fr