Qui sommes nous ?

- Enquêteur et technicien en nouvelles technologies (OPJ et personne qualifiée) ;

- Deux volets :
  - Enquêtes judiciaires (Internet) ;
  - Criminalistique numérique.

Principales motivations des délinquants

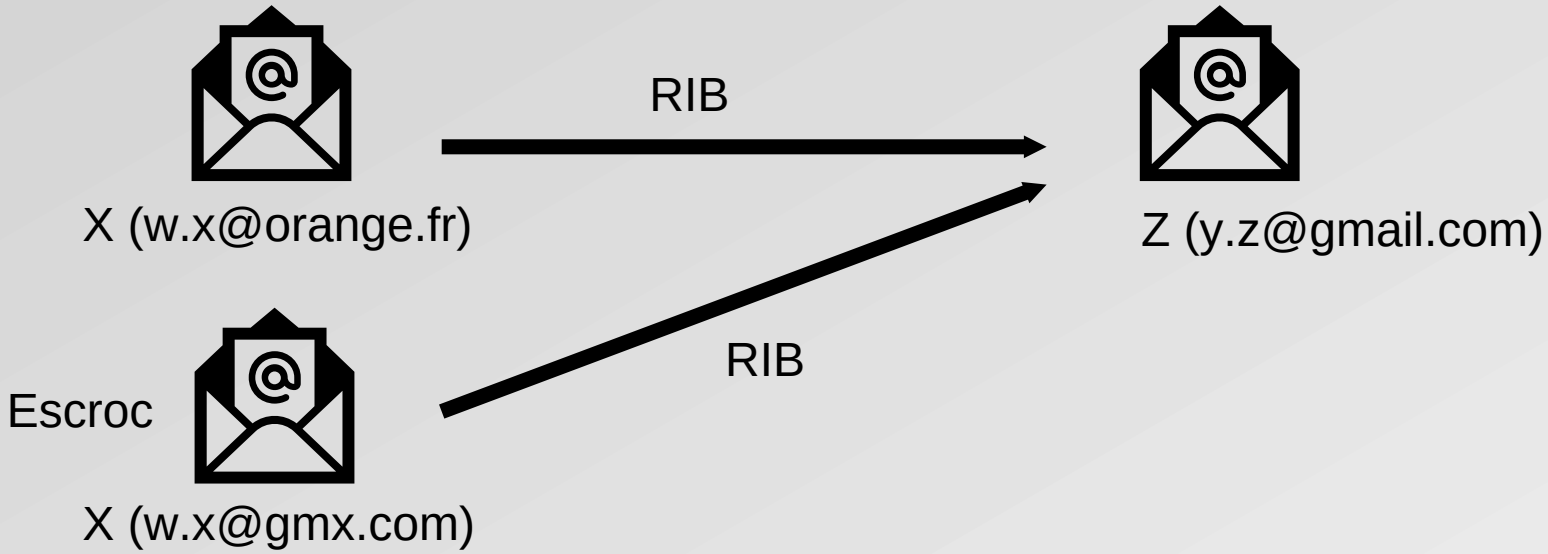
- Différentes motivations de la part des auteurs
  - Recherche de profit : escroquerie, vol de données ;
  - Diffamation (réseaux sociaux) ;
  - Espionnage ;
  - Défi, amusement ;
  - Déstabilisation (fake news).

Ransomware

- Chiffrement des données des serveurs d’une entreprise ou d’un organisme par introduction d’un logiciel malveillant
  - Pièce jointe d’un courriel, changement de mot de passe ;
- Demande de rançon pour obtenir la clé de déchiffrement ;
- Nécessite une intrusion préalable et une analyse du système d’information ;
- S’accompagne d’un vol de données ;
- Peut toucher des particuliers.

FOVI

- FOVI (faux ordres de virement) :
  - Intrusion dans la boîte mail de l’émetteur ou du destinataire ;
  - Substitution du RIB/IBAN par l’escroc.

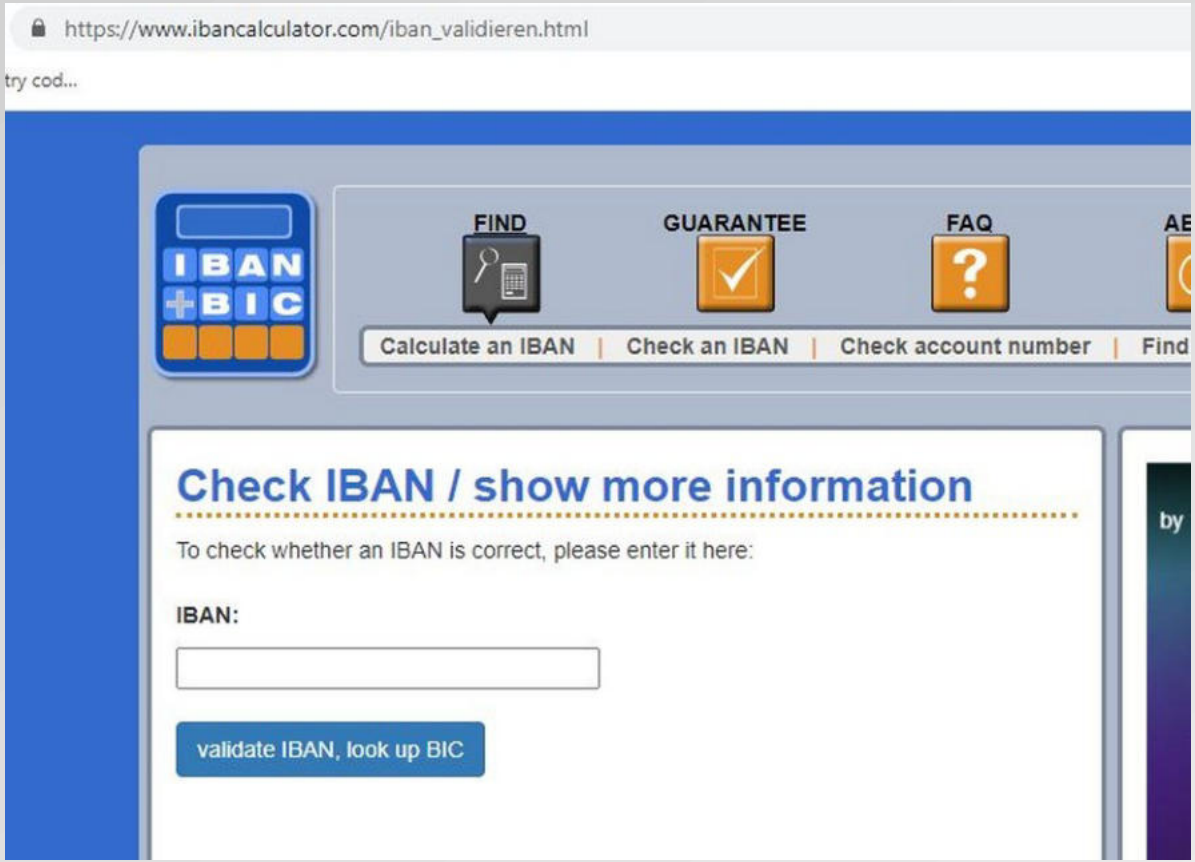


FOVI

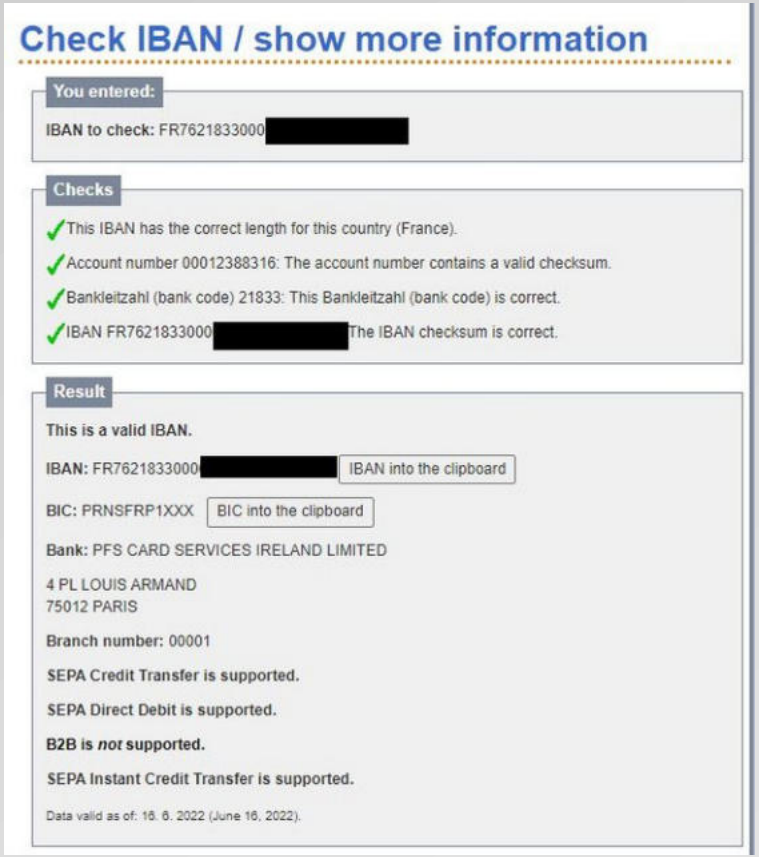
- Utilisation d’une adresse email approchante :
  - Même nom d’expéditeur mais adresse email différente
  - Exemple : RIB attendu de M. X (w.x@orange.fr) et RIB reçu de M. X mais depuis adresse w.x@gmx.com

- Utilisation de banques en ligne par les escrocs :
  - Nickel (FR76 1659 0000)
  - Revolut (FR76 2823 0000)
  - PFD Card Service Ireland (FR76 2183 0000)

FOVI


https://www.ibancalculator.com/iban_validieren.html
try cod...
IBAN +BIC
FIND
GUARANTEE
FAQ
Calculate an IBAN | Check an IBAN | Check account number | Find
Check IBAN / show more information
To check whether an IBAN is correct, please enter it here:
IBAN:
validate IBAN, look up BIC
by

FOVI



Check IBAN / show more information

You entered:

IBAN to check: FR7621833000[redacted]

Checks

- ✓ This IBAN has the correct length for this country (France).
- ✓ Account number 00012388316: The account number contains a valid checksum.
- ✓ Bankleitzahl (bank code) 21833: This Bankleitzahl (bank code) is correct.
- ✓ IBAN FR7621833000[redacted] The IBAN checksum is correct.

Result

This is a valid IBAN.

IBAN: FR7621833000[redacted] IBAN into the clipboard

BIC: PRNSFRP1XXX BIC into the clipboard

Bank: PFS CARD SERVICES IRELAND LIMITED

4 PL LOUIS ARMAND
75012 PARIS

Branch number: 00001

SEPA Credit Transfer is supported.

SEPA Direct Debit is supported.

B2B is *not* supported.

SEPA Instant Credit Transfer is supported.

Data valid as of: 16. 6. 2022 (June 16, 2022).

https://www.ibancalculator.com/

https://www.iban.com

Méthode du faux conseiller

- Appel/SMS d’un conseiller bancaire (service anti-fraude)
  - Le numéro affiché est parfois celui de l’agence de la personne contactée ;
  - Le conseiller signale des opérations frauduleuses sur le compte :
    - Demande du numéro de carte bancaire et du cryptogramme
    - Demande de virements pour mettre les fonds en sécurité
    - Envoi d’un coursier pour récupérer la carte bancaire
  - Ce type d’opérations n’est jamais effectué par les banques

Consulter les mises en garde sur les sites des banques

Méthode du faux conseiller

- Appel d’un conseiller bancaire signalant des opérations frauduleuses
  - Le numéro affiché est celui de la banque
  - Réception de codes par SMS
  - Le conseiller demande les codes
- Le conseiller est en fait un escroc ; les codes lui servent pour :
  - Accéder au compte et valider des virements (double authentification) ;
  - Valider des paiements en ligne.

Certains escrocs parviennent à obtenir une carte SIM

Méthode du faux conseiller

- Demande d’achats de coupons Transcash pour obtenir le remboursement.
- Variante avec conseiller meilleurtaux.com proposant un rachat de crédit.
- Un véritable conseiller a une adresse email @site_banque
  - dugenoux@meilleurtaux.com, dugenoux@credit-mutuel.fr...
  - Jamais dugenoux@gmail.com, dugenoux@proton.me…
  - Attention aux imitations : dugenoux@credit-mut.com

Investissement miraculeux

- Publicité sur Internet / faux article (accompagné d’un lien)
  - Personnalité / célébrité incitant à investir dans les cryptomonnaies ou des actions
- La victime est contacté par un escroc (email / téléphone)
  - Se fait passer pour un représentant d’une grande banque ou d’une société de trading ;
  - Propose un contrat ;
  - Mise en confiance, la victime investit, parfois de grosses sommes ;
  - Elle n’a ensuite plus de nouvelle du trader (ne répond plus au téléphone ou aux emails) ;

Investissement miraculeux

- Deux manières d’opérer :
  - Création d’un véritable compte bancaire ou portefeuille de cryptomonnaie sur une plateforme officielle (binance, coinbase…)
    - Le trader propose à la victime de gérer son portefeuille (identifiants, prise de main à distance avec AnyDesk)
  - Utilisation d’un faux site de gestion de cryptomonnaie
    - La victime pense y détenir un portefeuille qui n’existe pas
    - L’argent de la victime est viré sur un compte appartenant à l’escroc et n’est jamais converti en cryptomonnaie

Hameçonnage / phishing

- Email / SMS
  - Semble légitime (logo d’organismes et d’entreprises connus)
    - Sécurité sociale
    - Compte formation
    - Chronopost
    - …
  - Signale une anomalie et la nécessité de se connecter à son compte utilisateur ou de fournir des renseignements pour la résoudre
    - Renouvellement carte Vitale, colis bloqué, ...

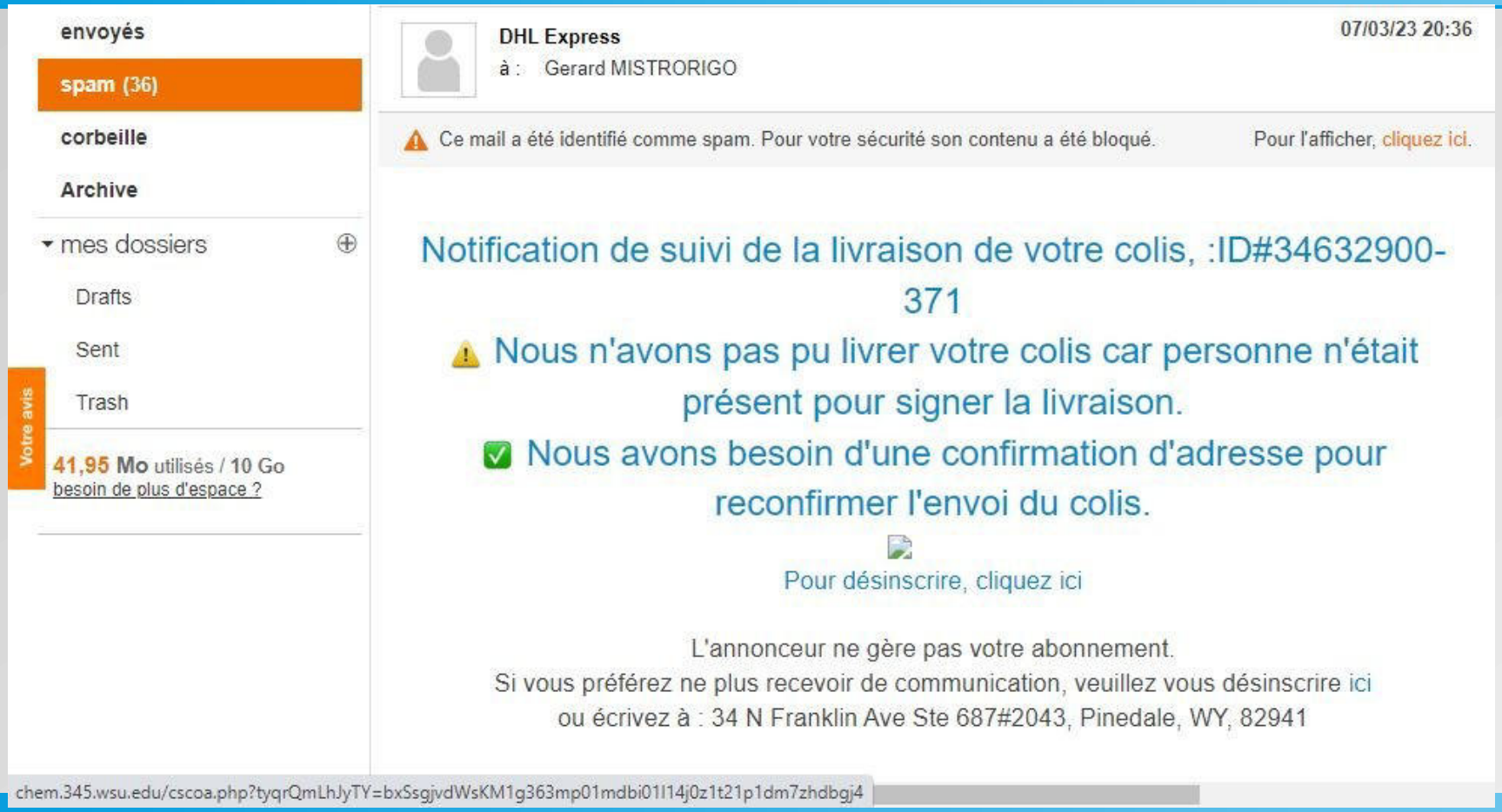
Hameçonnage / phishing

- Contiennent des liens vers des sites frauduleux qui ressemblent aux sites officiels
  - Les victimes pensent se connecter sur le site officiel ;
  - Données saisies et identifiants/mots de passe récupérés par les escrocs :
    - Usurpation d’identité ;
    - Connexions frauduleuses aux comptes utilisateurs (banque, boîte mail)
  - Récupération du numéro de carte bancaire
    - Frais pour débloquer un colis / amende impayée

Hameçonnage / phishing

- Se connecter à son compte utilisateur uniquement depuis les sites officiels
  - Exemple : impots.gouv.fr, ameli.fr
- Ne jamais cliquer sur les liens (exemple : gouv-fr.com) ;
- En cas de doute contacter l’organisme ou le service client
  - Utiliser les coordonnées et les moyens de contact indiqués sur le site officiel
- Ne rien payer.

Exemple d’un hameçonnage



Exemple d’un hameçonnage

chem.345.wsu.edu/cscoa.php?tyqrQmLhJyTY=bx5sgjvdWsKM1g363mp01mdbi01l14j0z1t21p1dm7zhdbgj4

Vente en ligne

- Fausse annonce
  - La victime paie un acompte voire l'intégralité et ne reçoit jamais le produit
  - Demande de documents à la victime pour une location (copie pièce d'identité, etc.) → usurpation d'identité

- Faux site de vente en ligne
  - La victime passe commande et paie ; elle ne reçoit jamais le produit ;
  - + usurpation d'identité

Vente en ligne

- Faux site de vente en ligne qui imite un site légitime :
  - Exemple : cdscount.com au lieu de cdiscount.com

Arnaque au chèque

- Arnaque au chèque :
  - M. X vend un objet à M. Z pour 2000 € ;
  - M. Z explique ne pouvoir fournir qu'un chèque de 4000 € et demande à M. X un remboursement de 2000 € en échange ;
  - M. X reçoit le chèque et le RIB de M. Z et procède au remboursement de 2000 € ;
  - M. X découvre plus tard que le chèque est un faux ou sans provision.

- Différents variantes
  - Exemple : avance de salaire dans le cadre d'une fausse offre d'emploi

Faux SAV informatique

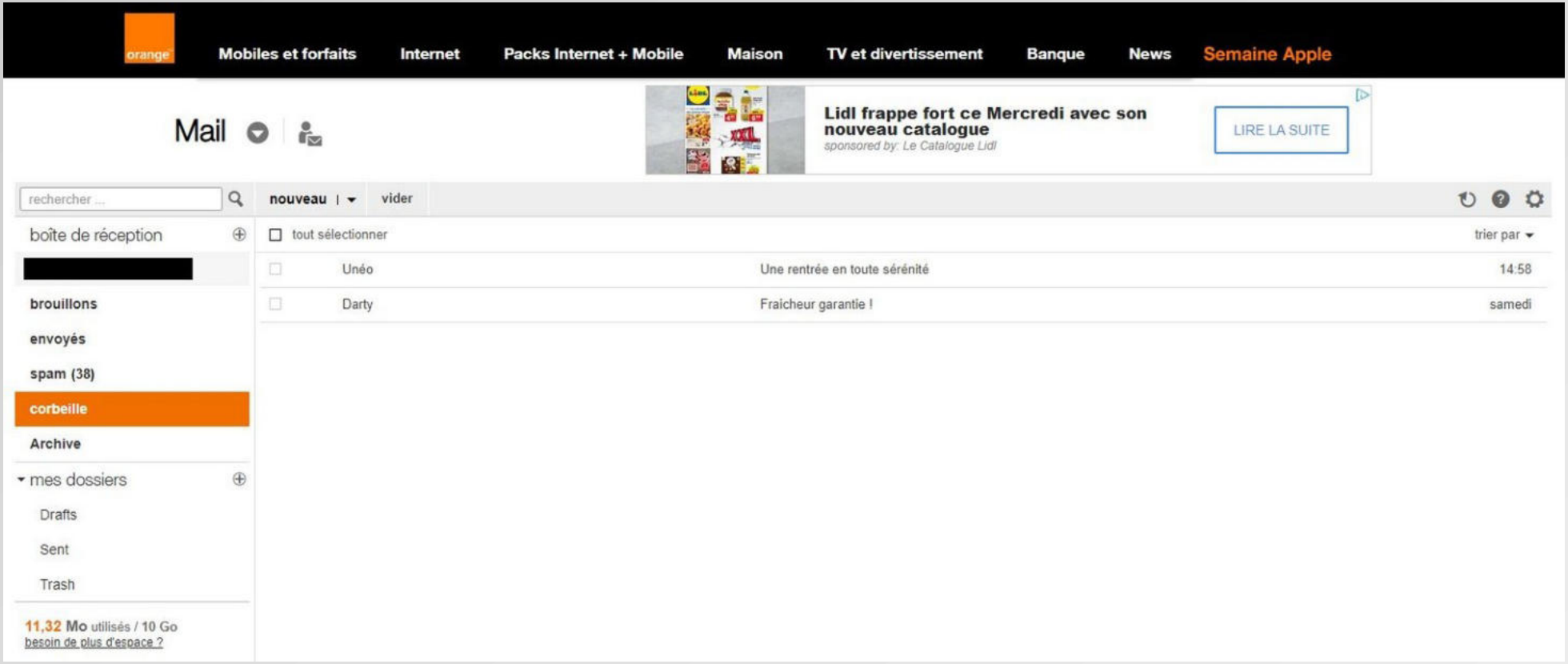
- Un message d’erreur indiquant une panne grave et imminente s’affiche sur l’écran
  - Il précise un numéro de téléphone à contacter d’urgence ;
  - Ce numéro est celui d’un escroc qui se fait passer pour un technicien
    - Il prend la main à distance sur l’ordinateur
    - A l’issue du pseudo-dépannage il demande le paiement de la prestation par carte bancaire (montant souvent très élevé : 400€)
    - A pu en profiter pour voler des données sur l’ordinateur et le numéro de carte bancaire

Un redémarrage de l’ordinateur suffit généralement à éliminer le message

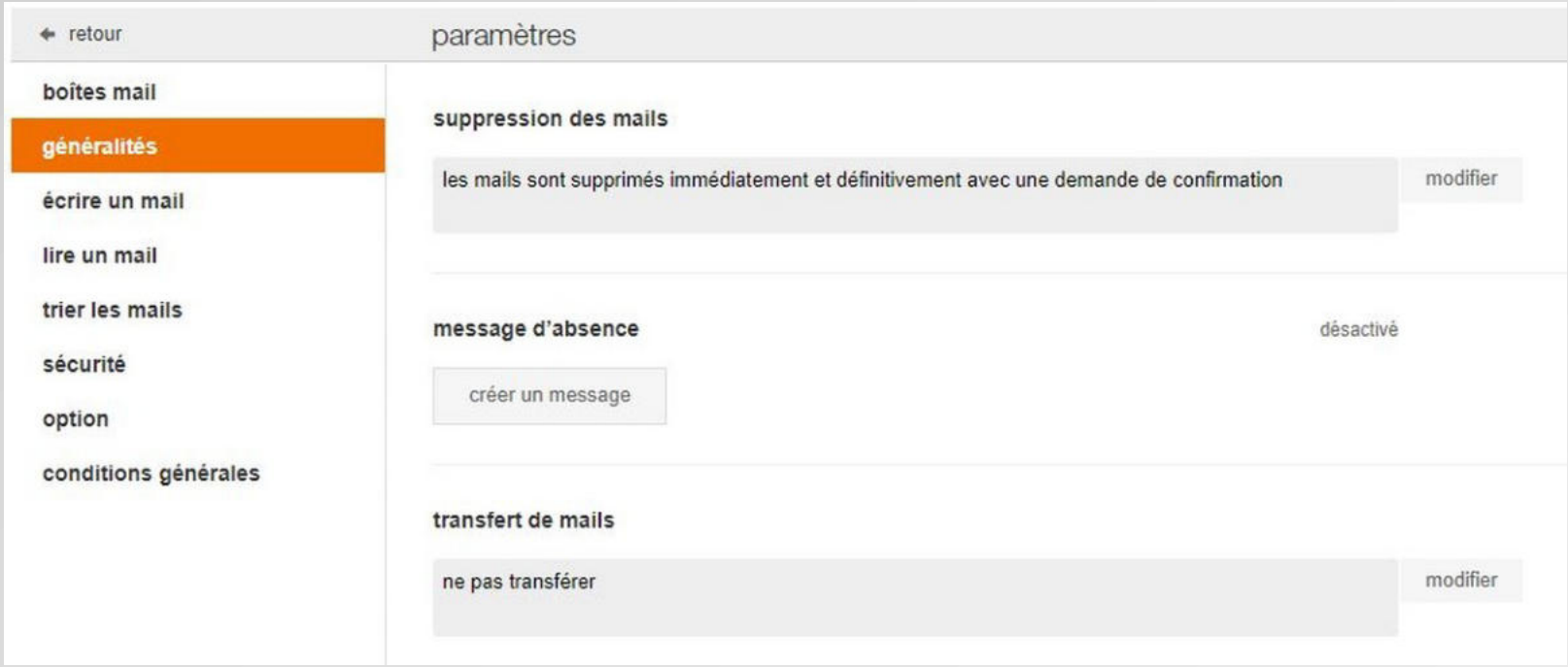
Autres escroqueries

- SMS d’un numéro inconnu
  - La personne se présente comme quelqu’un que vous connaissez
  - Explique que son téléphone est en panne ou perdu/volé d’où le n° inconnu
  - Explique être en difficulté et avoir besoin d’argent
- Arnaque aux sentiments :
  - Réseaux sociaux ou sites de rencontre ;
  - Demande d’argent
  - Généralement les mêmes stratagèmes :
    - La personne est à l’étranger a perdu sa carte bancaire ou se l’est fait voler ;
    - Elle a un proche atteint d’une maladie grave (père, fils…) ;
    - Elle a un proche décédé à l’étranger.

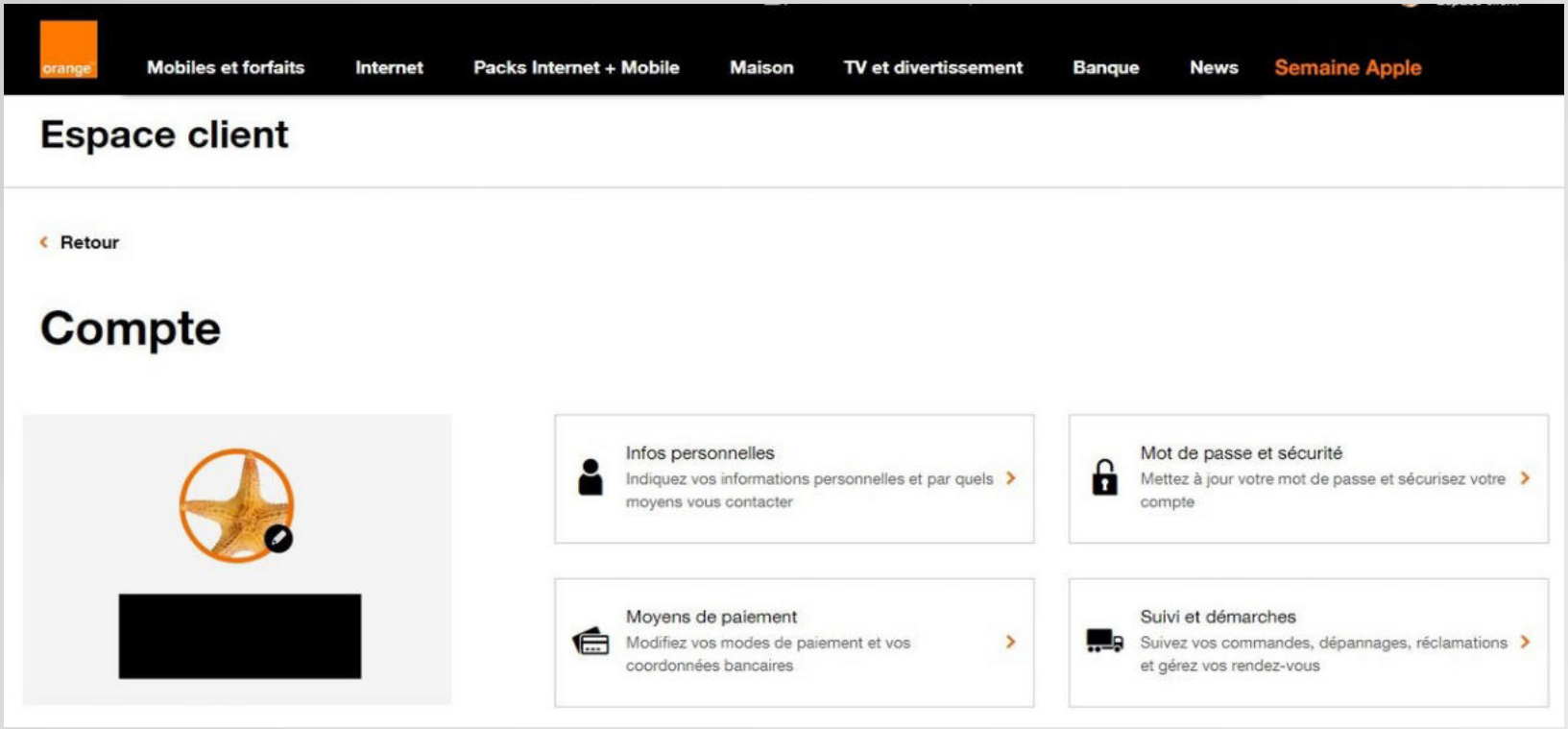
Sécurité des boîtes mail



Orange


retour
paramètres
boîtes mail
généralités
écrire un mail
lire un mail
trier les mails
sécurité
option
conditions générales
suppression des mails
les mails sont supprimés immédiatement et définitivement avec une demande de confirmation
modifier
message d'absence
désactivé
créer un message
transfert de mails
ne pas transférer
modifier

Orange


orange
Mobiles et forfaits
Internet
Packs Internet + Mobile
Maison
TV et divertissement
Banque
News
Semaine Apple
Espace client
Retour
Compte
[redacted]
Infos personnelles
Indiquez vos informations personnelles et par quels moyens vous contacter
Mot de passe et sécurité
Mettez à jour votre mot de passe et sécurisez votre compte
Moyens de paiement
Modifiez vos modes de paiement et vos coordonnées bancaires
Suivi et démarches
Suivez vos commandes, dépannages, réclamations et gérez vos rendez-vous

Orange

Sécurité de votre compte

Avec Orange, la sécurité de votre compte est bien assurée. Sur cette page, vous pouvez consulter et gérer tous les paramètres de sécurité de votre compte.

Votre identifiant de compte

Votre identifiant de compte peut être votre numéro de mobile ou votre adresse e-mail Orange. Il est indispensable pour vous connecter à l'Espace client et accéder aux services Orange.

[redacted]

Modifier

Votre mot de passe

[redacted]

Modifier

Protégez votre compte

Pour être averti de modifications sur votre compte ou en cas d'oubli de votre mot de passe, renseignez vos coordonnées.

[redacted]

Modifier vos coordonnées

Votre service Mobile Connect

Paramétrez gratuitement Mobile Connect pour vous identifier en toute sécurité à l'aide de votre mobile Orange ou Sosh.

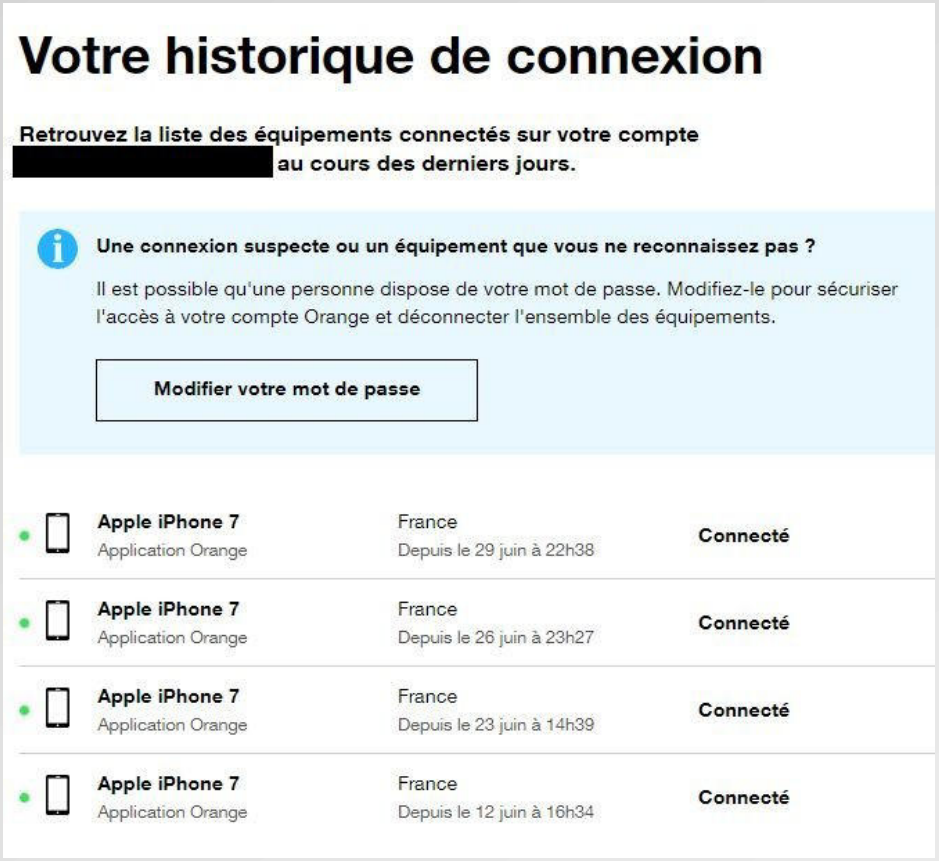
[redacted]

Désactiver

Votre historique de connexion

Consultez la liste des équipements utilisés pour se connecter à votre compte au cours des 30 derniers jours.

Consulter



Votre historique de connexion

Retrouvez la liste des équipements connectés sur votre compte [redacted] au cours des derniers jours.

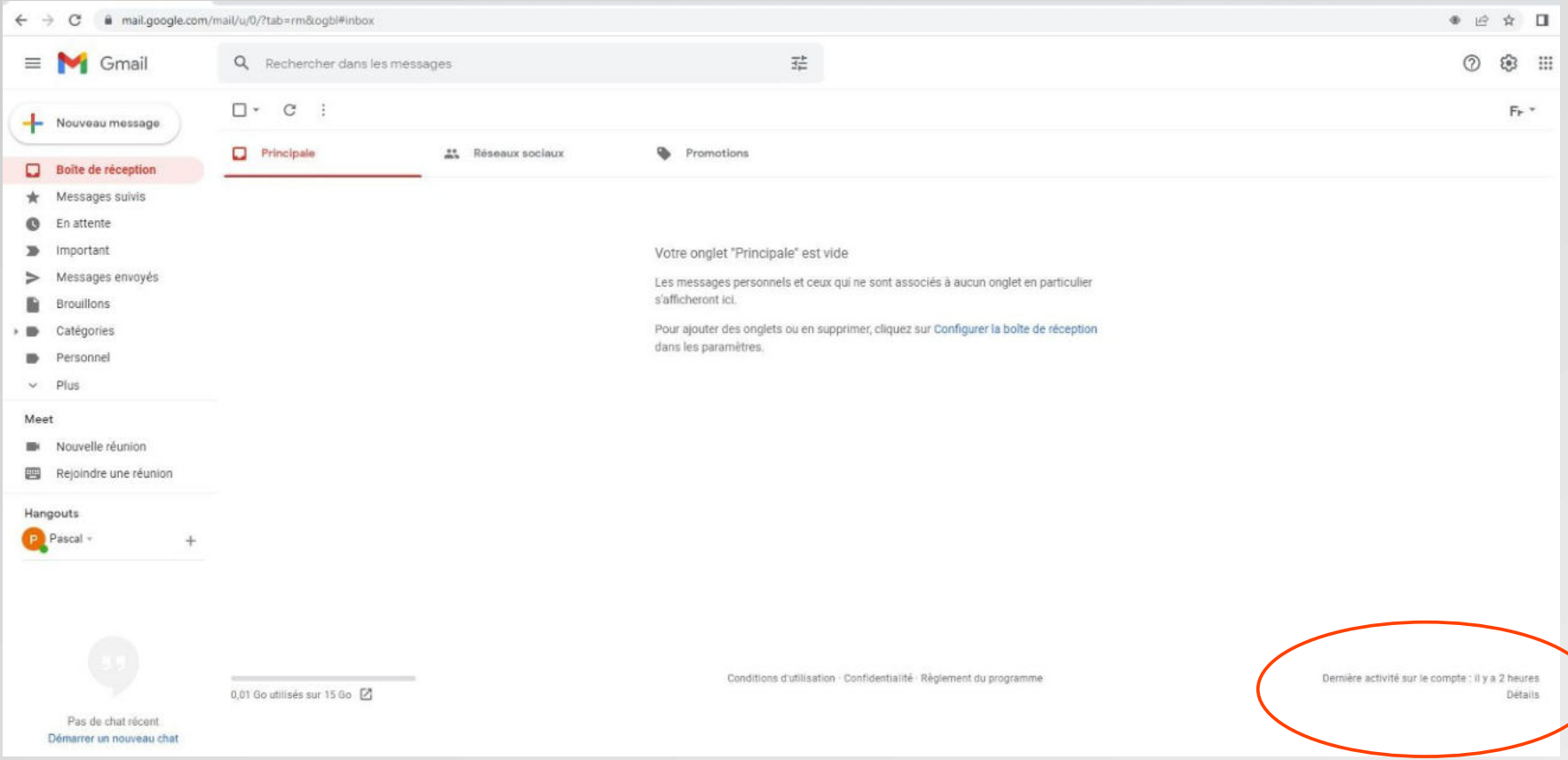
Une connexion suspecte ou un équipement que vous ne reconnaissez pas ?

Il est possible qu'une personne dispose de votre mot de passe. Modifiez-le pour sécuriser l'accès à votre compte Orange et déconnecter l'ensemble des équipements.

Modifier votre mot de passe

Apple iPhone 7	Application Orange	France	Depuis le 29 juin à 22h38	**Connecté**
Apple iPhone 7	Application Orange	France	Depuis le 26 juin à 23h27	**Connecté**
Apple iPhone 7	Application Orange	France	Depuis le 23 juin à 14h39	**Connecté**
Apple iPhone 7	Application Orange	France	Depuis le 12 juin à 16h34	**Connecté**

Google


mail.google.com/mail/u/0/?tab=rm&ogbl#inbox
Gmail
Rechercher dans les messages
Nouveau message
Boîte de réception
Messages suivis
En attente
Important
Messages envoyés
Brouillons
Catégories
Personnel
Plus
Meet
Nouvelle réunion
Rejoindre une réunion
Hangouts
Pascal
Principale
Réseaux sociaux
Promotions
Votre onglet "Principale" est vide
Les messages personnels et ceux qui ne sont associés à aucun onglet en particulier s'afficheront ici.
Pour ajouter des onglets ou en supprimer, cliquez sur Configurer la boîte de réception dans les paramètres.
Pas de chat récent
Démarrer un nouveau chat
0,01 Go utilisés sur 15 Go
Conditions d'utilisation · Confidentialité · Règlement du programme
Dernière activité sur le compte : il y a 2 heures
Détails

Google

Dernière activité sur le compte : il y a 2 heures
Détails

Informations sur l'activité - Google Chrome

mail.google.com/mail/u/0/?ui=2&ik=4a72460c16&jsver=guaGlxde0bA.fr..es5&cbl=gmail.pinto-server_20220627.04_p2&view=ac

Activité concernant ce compte

Cette fonction fournit des informations sur l'activité récemment enregistrée sur ce compte de messagerie et sur les autres activités simultanées. En savoir plus

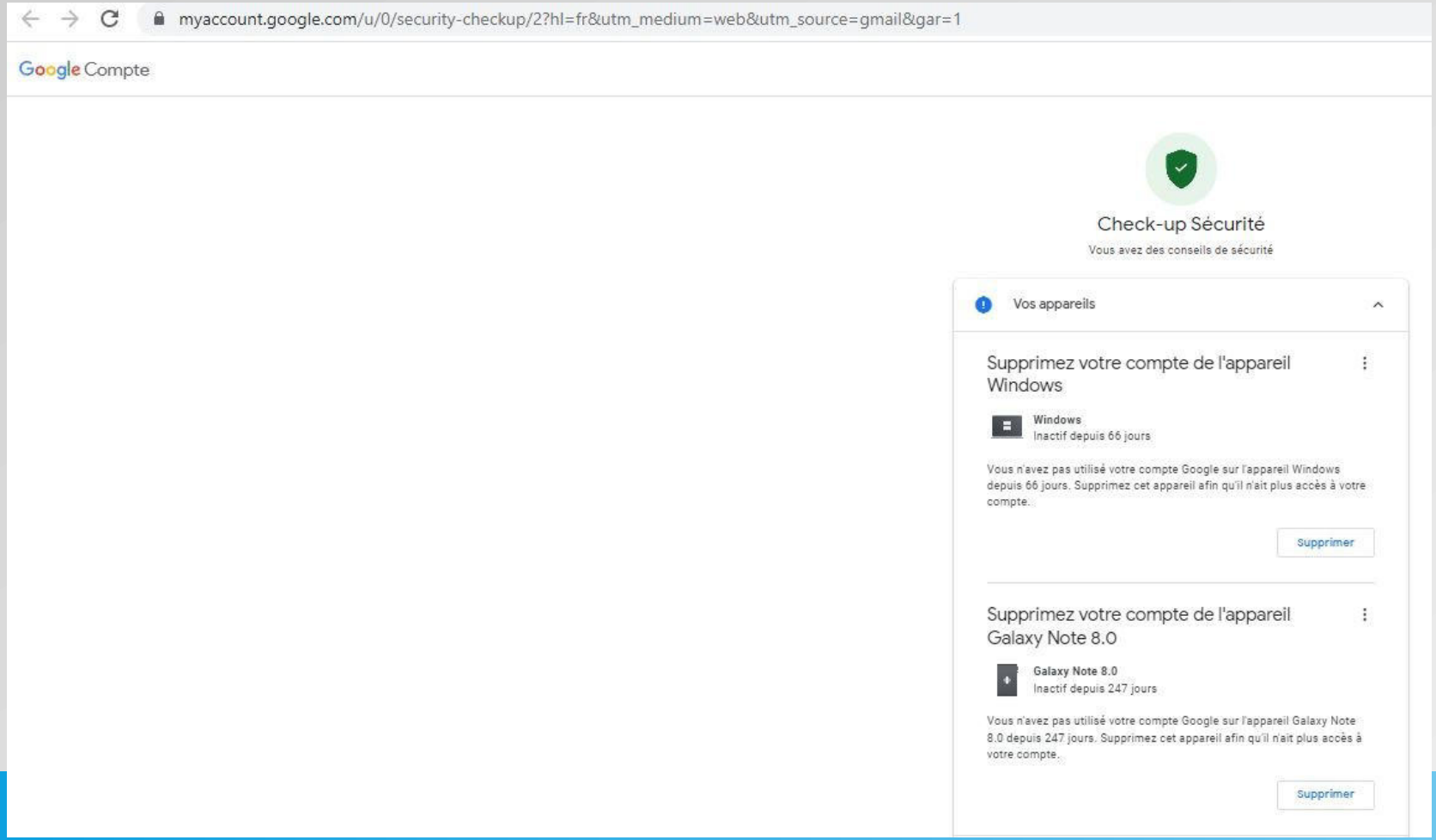
Ce compte ne semble pas être ouvert dans un autre emplacement. Cependant, certaines sessions sont peut-être toujours ouvertes.

Consultez la page Check-up Sécurité pour en savoir plus

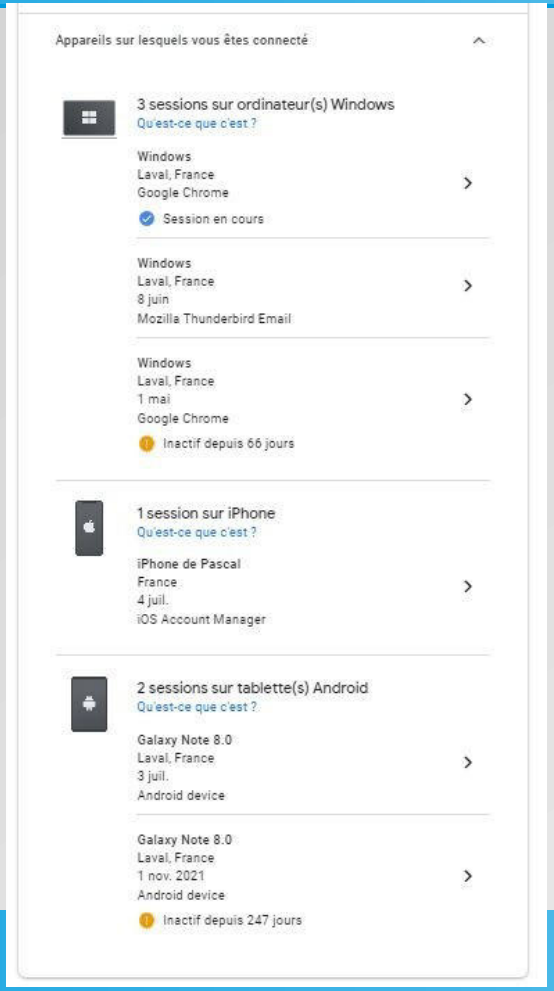
Activité récente :

Type d'accès [?] (Navigateur, mobile, POP3, etc.)	**Emplacement (adresse IP)** [?]	**Date/heure** (Affiché dans votre fuseau horaire)
Navigateur (Chrome) Masquer les détails *"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.0.0 Safari/537.36,gzip(gfe),gzip(gfe)"*	* France (2a01:cb05:9008:d400:6452:7c69:4c42:d592)	20:44 (il y a 1 minute)
Application autorisée (946018238758-bi6ni53dfoddlgn97pk3b8i7nphige40.apps.googleusercontent.com) Masquer les détails *"name: Mac OS X Mail"* *"os: Mac OS X"* *"os-version: 12.4 (21F79)"* *"vendor: Apple Inc."* *"version: 16.0 (3696.100.31)"* Nom de domaine OAuth : *946018238758-bi6ni53dfoddlgn97pk3b8i7nphige40.apps.googleusercontent.com* Gérer l'accès au compte	France (2a01:cb05:9008:d400:9079:a356:3049:1d4f)	18:28 (il y a 2 heures)
Application autorisée (406964657835-aq8lmia8j95dhl1a2bvharmfk3t1hgqj.apps.googleusercontent.com) Masquer les détails *"name: Thunderbird"* *"version: 102.0"* Nom de domaine OAuth : *406964657835-aq8lmia8j95dhl1a2bvharmfk3t1hgqj.apps.googleusercontent.com* Gérer l'accès au compte	France (2a01:cb05:9008:d400:35dd:c39f:30b0:3812)	07:22 (il y a 13 heures)
Application autorisée (406964657835-aq8lmia8j95dhl1a2bvharmfk3t1hgqj.apps.googleusercontent.com) Afficher les détails	France (2a01:cb05:9008:d400:f8b6:3be5:7ba1:867c)	5 juil. (il y a 1 jour)

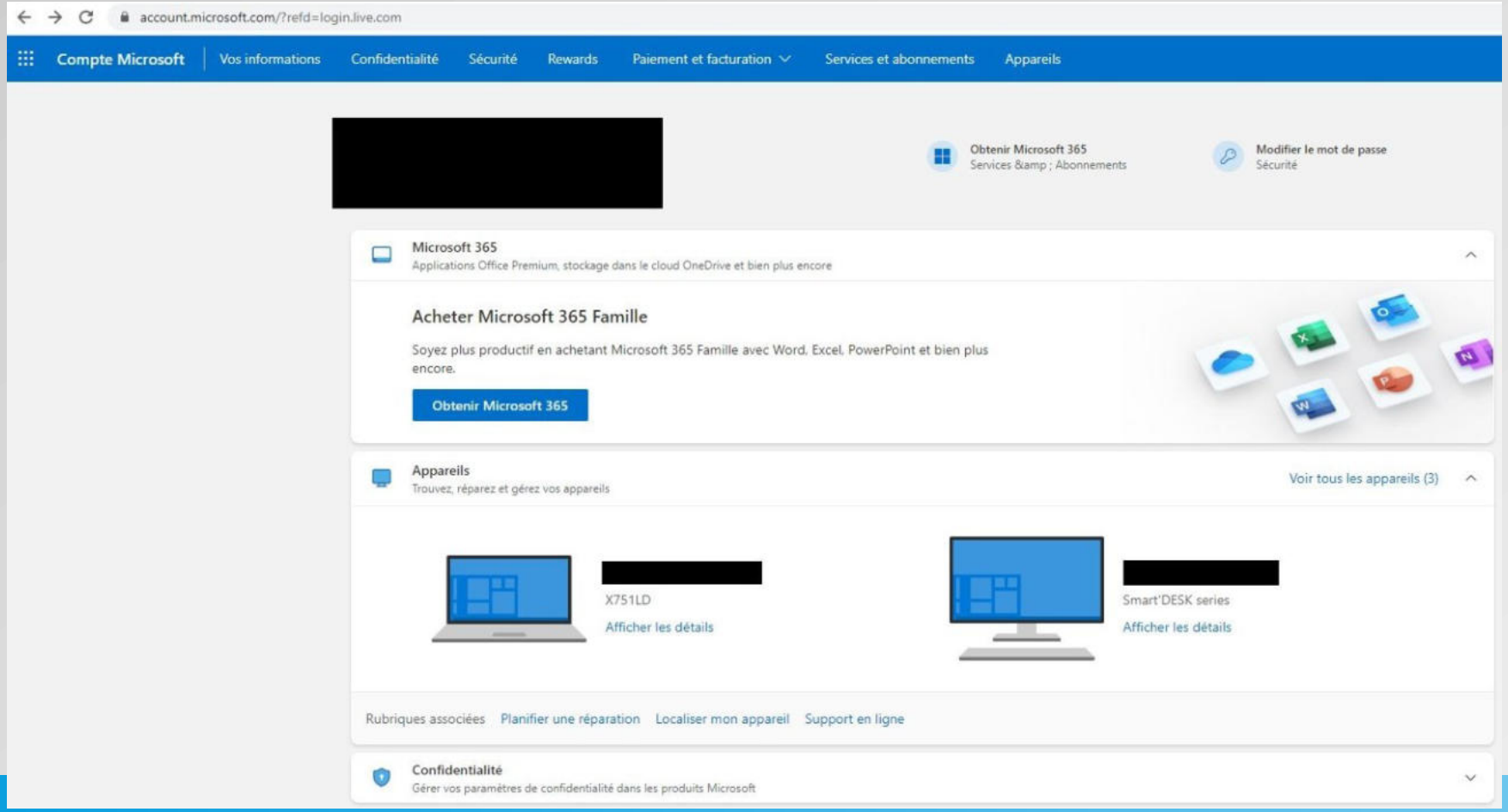
Google


myaccount.google.com/u/0/security-checkup/2?hl=fr&utm_medium=web&utm_source=gmail&gar=1
Google Compte
Check-up Sécurité
Vous avez des conseils de sécurité
Vos appareils
Supprimez votre compte de l'appareil Windows
Windows
Inactif depuis 66 jours
Vous n'avez pas utilisé votre compte Google sur l'appareil Windows depuis 66 jours. Supprimez cet appareil afin qu'il n'ait plus accès à votre compte.
Supprimer
Supprimez votre compte de l'appareil Galaxy Note 8.0
Galaxy Note 8.0
Inactif depuis 247 jours
Vous n'avez pas utilisé votre compte Google sur l'appareil Galaxy Note 8.0 depuis 247 jours. Supprimez cet appareil afin qu'il n'ait plus accès à votre compte.
Supprimer

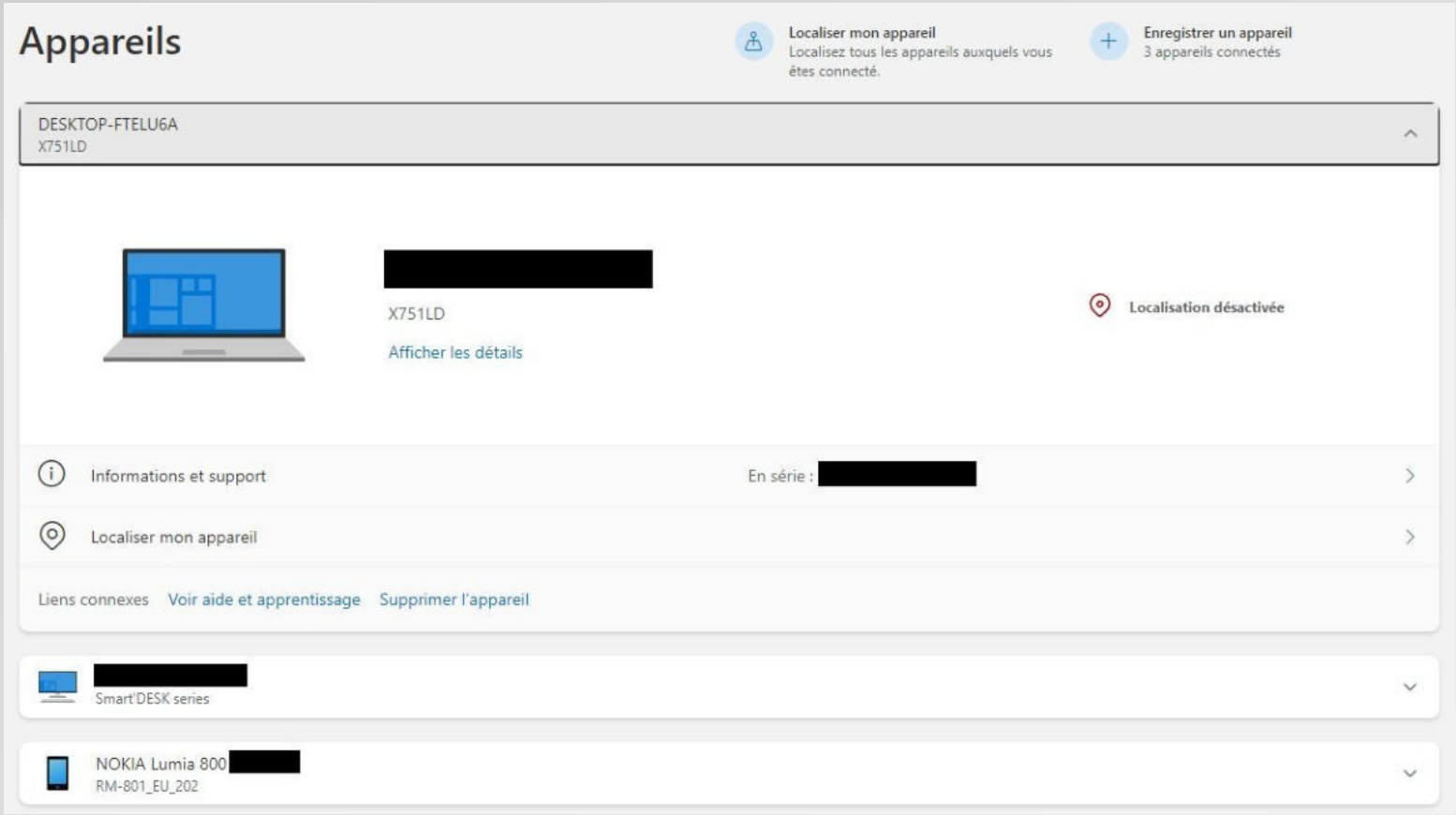
Google


Appareils sur lesquels vous êtes connecté
3 sessions sur ordinateur(s) Windows
Qu'est-ce que c'est ?
Windows
Laval, France
Google Chrome
Session en cours
Windows
Laval, France
8 juin
Mozilla Thunderbird Email
Windows
Laval, France
1 mai
Google Chrome
Inactif depuis 66 jours
1 session sur iPhone
Qu'est-ce que c'est ?
iPhone de Pascal
France
4 juil.
iOS Account Manager
2 sessions sur tablette(s) Android
Qu'est-ce que c'est ?
Galaxy Note 8.0
Laval, France
3 juil.
Android device
Galaxy Note 8.0
Laval, France
1 nov. 2021
Android device
Inactif depuis 247 jours

Microsoft


account.microsoft.com/?refd=login.live.com
Compte Microsoft
Vos informations
Confidentialité
Sécurité
Rewards
Paiement et facturation
Services et abonnements
Appareils
[redacted]
Obtenir Microsoft 365
Services &amp ; Abonnements
Modifier le mot de passe
Sécurité
Microsoft 365
Applications Office Premium, stockage dans le cloud OneDrive et bien plus encore
Acheter Microsoft 365 Famille
Soyez plus productif en achetant Microsoft 365 Famille avec Word, Excel, PowerPoint et bien plus encore.
Obtenir Microsoft 365
Appareils
Trouvez, réparez et gérez vos appareils
Voir tous les appareils (3)
[redacted]
X751LD
Afficher les détails
[redacted]
Smart'DESK series
Afficher les détails
Rubriques associées
Planifier une réparation
Localiser mon appareil
Support en ligne
Confidentialité
Gérer vos paramètres de confidentialité dans les produits Microsoft

Microsoft


Appareils
Localiser mon appareil
Localisez tous les appareils auxquels vous êtes connecté.
Enregistrer un appareil
3 appareils connectés
DESKTOP-FTELU6A
X751LD
[redacted]
X751LD
Afficher les détails
Localisation désactivée
Informations et support
En série : [redacted]
Localiser mon appareil
Liens connexes
Voir aide et apprentissage
Supprimer l'appareil
[redacted]
Smart'DESK series
NOKIA Lumia 800[redacted]
RM-801_EU_202

Microsoft

Sécurité

[redacted]

Notion de base sur la sécurité

Gérez votre mot de passe, protégez votre compte et consultez des ressources de sécurité supplémentaires.

Activité de connexion

Vérifiez où et quand vous vous êtes connecté et dites-nous si quelque chose vous semble inhabituel.

Consulter mon activité

Sécurité du mot de passe

Aidez à sécuriser votre compte en utilisant un mot de passe plus fort.

Changer mon mot de passe

Options de sécurité avancées

Essayez les dernières options de sécurité pour sécuriser votre compte.

Prise en main

Microsoft

Afficher quand et où vous avez utilisé votre compte

Vous devez reconnaître toutes ces activités récentes. Si vous ne reconnaissez pas l'une d'entre elles, cliquez dessus pour nous le faire savoir.

En savoir plus sur la page des activités récentes

Découvrir comment renforcer la sécurité de votre compte

Activité récente

	Heure (CET)	Type de session	Emplacement approximatif
	Il y a 3 heures	Synchronisation automatique	Non disponible
	Protocole :IMAP Adresse IP :2a01:[redacted] Alias de compte :[redacted]	Heure :Il y a 3 heures Emplacement approximatif :Non disponible Type : Synchronisation réussie	C'est inhabituel ? Protéger votre compte
	Protocole :IMAP Adresse IP :2a01:[redacted] Alias de compte :[redacted]	Heure :Il y a 14 heures Emplacement approximatif :Non disponible Type : Synchronisation réussie	C'est inhabituel ? Protéger votre compte

Liens utiles

- ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information)
  - https://www.ssi.gouv.fr
- Assistance aux victimes de cybermalveillance
  - https://www.cybermalveillance.gouv.fr
- Signalement de contenus illicites
  - https://www.internet-signalement.gouv.fr
- THESEE (plainte en ligne pour les arnaques sur Internet)
  - https://www.masecurite.interieur.gouv.fr/fr/demarches-en-ligne/plainte-en-ligne-arnaques-internet-thesee

Liens utiles

- https://www.pre-plainte-en-ligne.gouv.fr
- https://filigrane.beta.gouv.fr