Les Gardiens du Cyberespace
Démystifier la Cybersécurité

Objectifs :

- comprendre, se rassurer, agir
- sécuriser vos appareils et données personnelles facilement

par Cyrille Allet

📚 Pourquoi parler de Cybersécurité ?

Usage quotidien

Téléphones, ordinateurs, tablettes, télévisions ...

Arnaques fréquentes

Tentatives de vols en hausse constante

Prévention

Mieux vaut anticiper que réparer. Se protéger avec des gestes simples

🔔 Vous n’avez pas besoin d’être expert !

📚 Pourquoi parler de Cybersécurité ?

Trimestre 2025

2,1 millions de comptes français piratés

Cibles

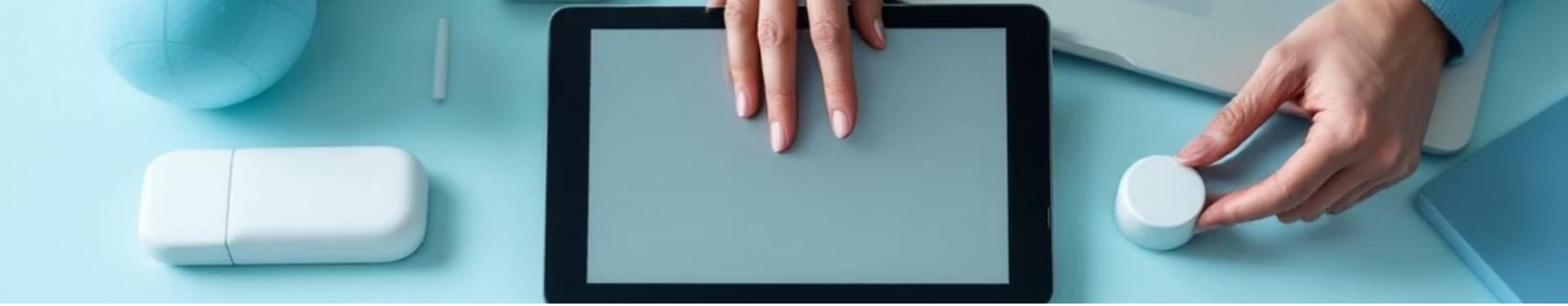
La Poste, FFF (2ème fois), Kiabi Afflelou, Thermoix

Constat

7e pays le plus touché au monde. Retard de sensibilisation à la cyber-sécurité. Mauvais usage des mots de passe. Forte présence en ligne.

🔔 Vous n’avez pas besoin d’être expert !

S’INFORMER
ZATAZ.COM
SE SÉCURISER



Systèmes d'Information

Définition

Ensemble de ressources techniques et humaines pour stocker et traiter l'information.

Diversification

Multiplication des appareils connectés et des points d'accès.

Utilisateurs

Premier maillon de la chaîne de sécurité.

Les Bases de la Cybersécurité

Définition
La cybersécurité comprend l'ensemble des mesures de protection des Systèmes d’Information.

Menaces principales
Les virus, le phishing et les logiciels malveillants sont les dangers les plus courants.

Statistiques alarmantes
Une augmentation de 30% des cyberattaques ciblant les seniors a été constatée en 2023. Ce chiffre continue de croître en 2024 mais...

Les acteurs
Le protecteur : hacker éthique
Le détective : analyste sécurité informatique
L’architecte : ingénieur en sécurité des reseaux
ET VOUS

👉 **Laissez-vous votre porte ouverte en sortant ?**

C'est quoi une cyberattaque ?

Tentative de piratage

Vol, destruction ou altération de données

- **Informations personnelles, données bancaires**
- **Secrets industriels**

Perturbation ou interruption de services

- **Rendre un site web inaccessible**

Extorsion financière

- **Ransomwares chiffrent des données et demandent une rançon**

Prise de contrôle de systèmes informatiques à distance

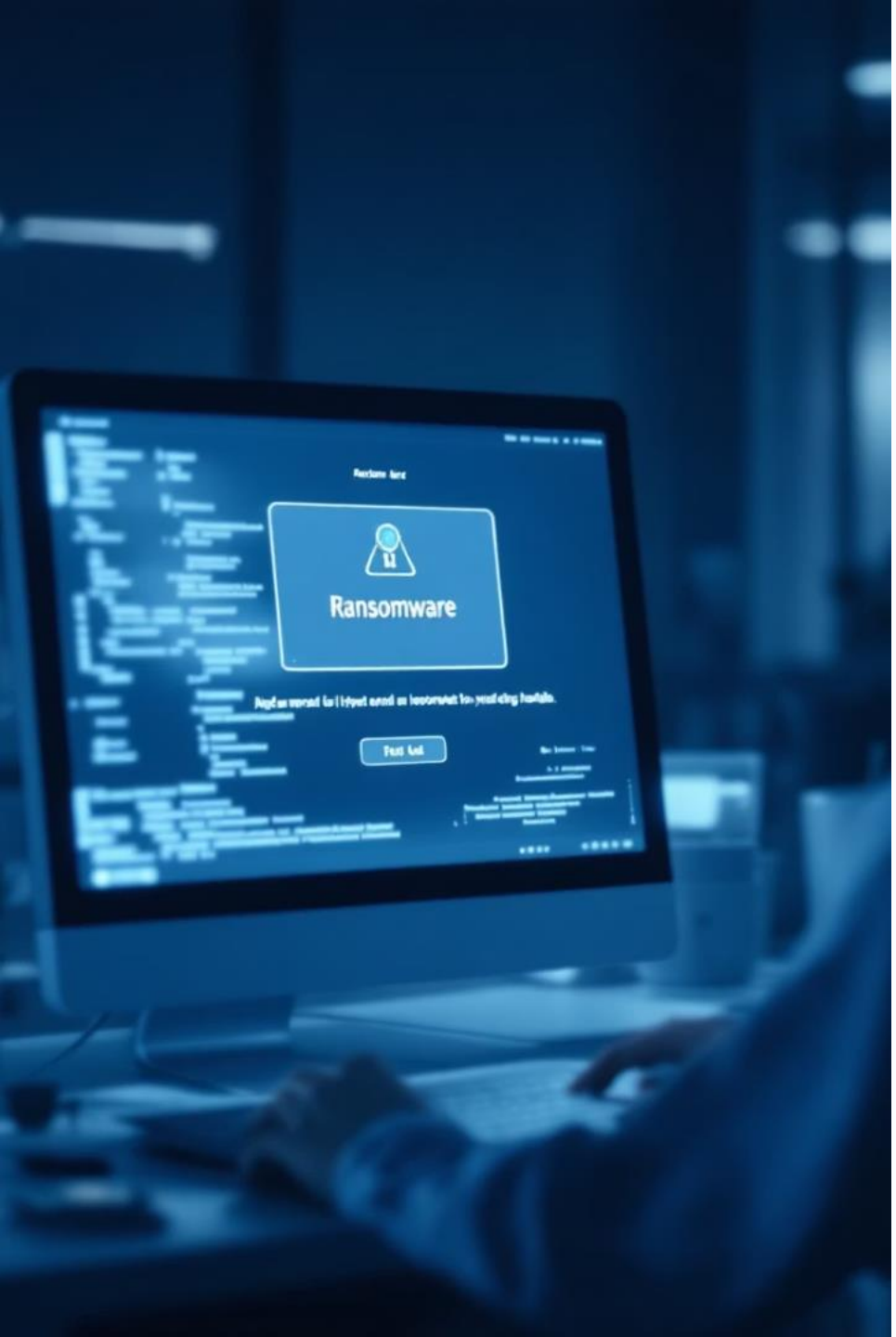
Espionnage industriel ou gouvernemental

C'est quoi une cyberattaque ?

Multiples vecteurs

Hameçonnage. ***Emails, SMS***
Ingénierie sociale. ***Manipulation psychologique par téléphone***
Vulnérabilités logicielles. ***Failles de sécurité Applis ou Systèmes***
Attaques par force brute. ***Deviner mot de passe ou clé chiffrement***
Malwares. ***Virus, ransomwares, keyloggers***
Man-in-the-middle. ***Interception des communications***
...

La défense efficace nécessite une approche multicouche combinant sensibilisation des utilisateurs, mises à jour régulières, authentification forte et surveillance des systèmes.



⚠ Exemples récents en France

2024 : Hôpital d'Armentières - 2023 : CHU Lille

Attaque par rançongiciel

Faux support technique

Arnaques Microsoft et autres

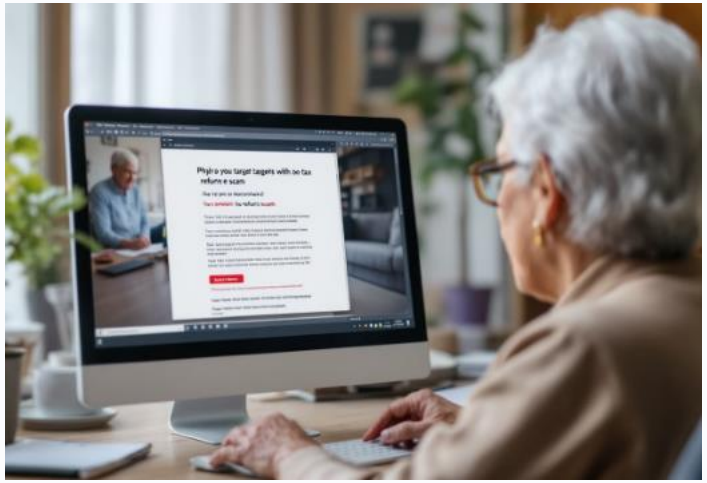
2024 : Académie de Lille - 2023 : Mairie de Lille

Fuite de données

Exemples Concrets de Piratage

Le Phishing

Des e-mails frauduleux imitant les services fiscaux ou annonçant des gains à des loteries.



Faux Support Technique

Des appels de personnes prétendant travailler pour Microsoft. Ils demandent un accès à distance à votre ordinateur.

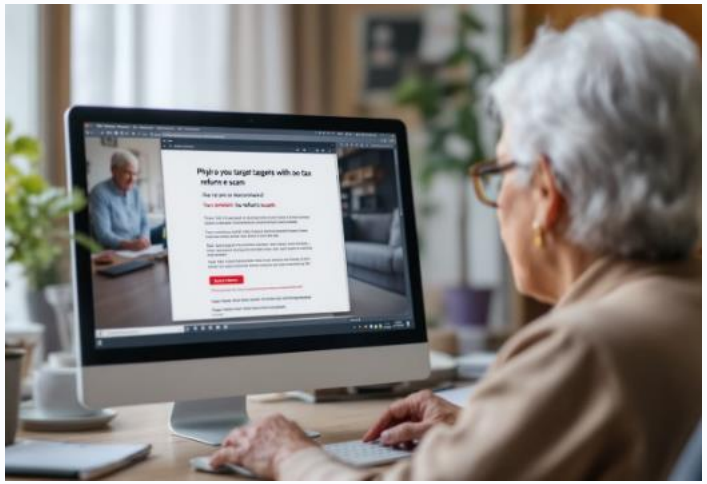
Les Malwares

Des virus et rançongiciels qui bloquent votre ordinateur. Ils exigent un paiement pour libérer vos données personnelles.

Exemples Concrets de Piratage

Le Phishing

Des e-mails frauduleux imitant les services fiscaux ou annonçant des gains à des loteries.

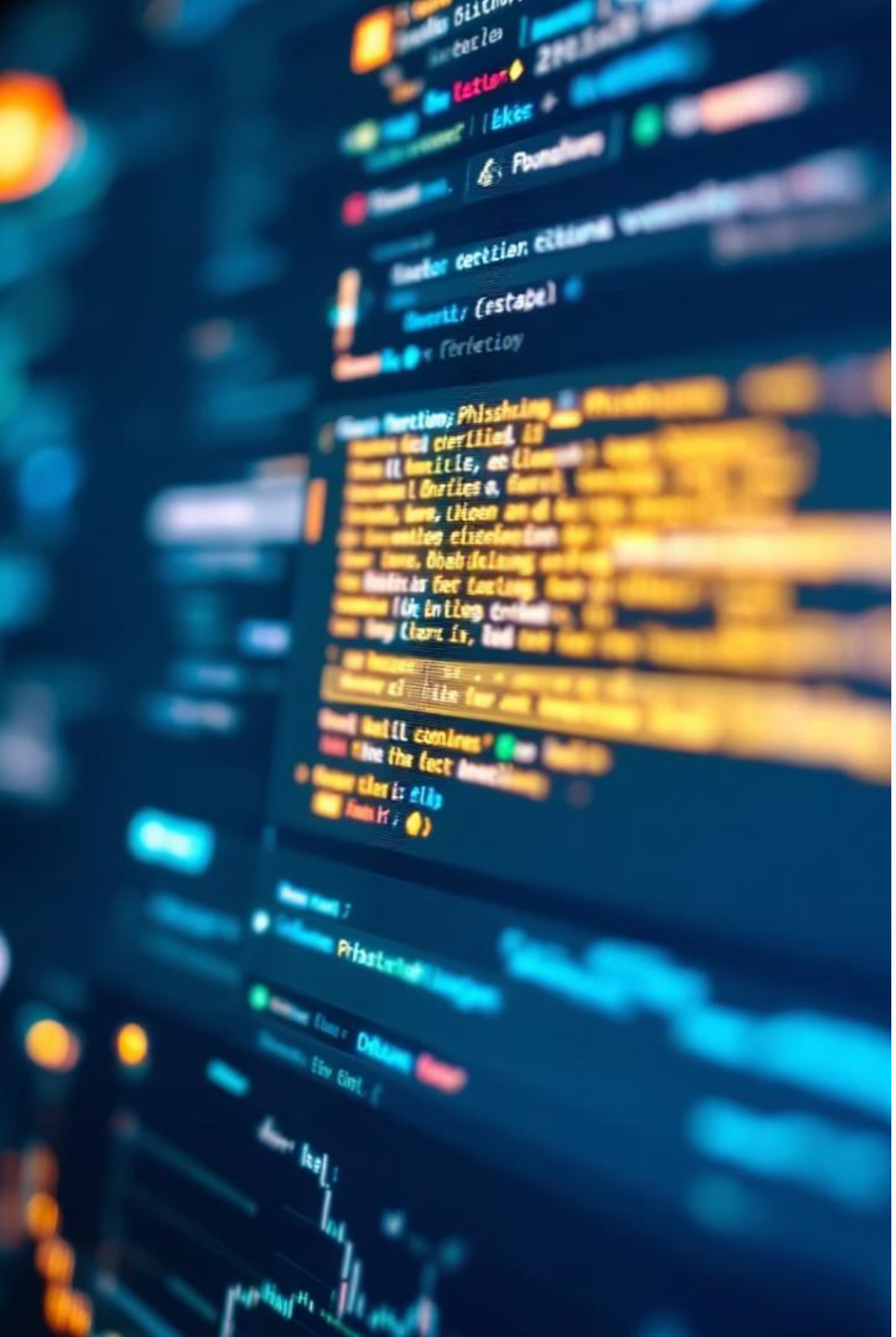


Faux Support Technique

Des appels de personnes prétendant travailler pour Microsoft. Ils demandent un accès à distance à votre ordinateur.

Les Malwares

Des virus et rançongiciels qui bloquent votre ordinateur. Ils exigent un paiement pour libérer vos données personnelles.



🤝 Comment repérer un faux message ?

Trop beau pour être vrai ? Soyez méfiant. Vérifiez l'adresse. Ne cliquez jamais sur un lien étrange.

Émilie a reçu le courrier électronique (mail) ci-dessous et pense qu'il s'agit d'une arnaque.

Quel indice lui fait penser cela ?

Afficher l'alternative textuelle

Sélectionnez une seule réponse.

QUIZZ

S'évaluer
https://app.pix.fr/campagnes/QKSHQS257/presentation

MondialRelay
edu@tazueew.m4.ofir.com.es

Répondre | Transférer | Archiver | Indésirable | Supprimer | Autres

Pour cyrille.allet@gmail.com

08/04/2025, 2

Mise à Jour Expédition : Commande #[54147-2056] Expédiée .

Pour protéger votre vie privée, Thunderbird a bloqué l'affichage du contenu distant dans ce message. Options

Mondial Relay

Mise à Jour sur l'Expédition

Votre colis est en route. Cliquez ci-dessous pour voir plus de détails sur l'expédition.

Voir les Détails de l'Expédition

Numéro de Commande
#ORDR 54147 2056

Statut de l'Expédition
En Transit

Numéro de Suivi:
BR5S4147205
Cliquez ici pour suivre votre colis.

Pour toute question, contactez support@shipping.com

EXPÉDITION À :

Adresse domicile
Déjà payé
Expédition express

FACTURATION :

Méthode de paiement : **3****

QUIZZ

Panneau « Aujourd'hui

MondialRelay
edu@tazueew.m4.ofir.com.es

Répondre | Transférer | Archiver | Indésirable | Supprimer | Autres

Pour cyrille.allet@gmail.com

08/04/2025, 2

Mise à Jour Expédition : Commande #[54147-2056] Expédiée .

Pour protéger votre vie privée, Thunderbird a bloqué l'affichage du contenu distant dans ce message.

Options

Mondial Relay

Mise à Jour sur l'Expédition

Votre colis est en route. Cliquez ci-dessous pour voir plus de détails sur l'expédition.

Voir les Détails de l'Expédition

Numéro de Commande
#ORDR 54147 2056

Statut de l'Expédition
En Transit

Numéro de Suivi:
BR5S4147205

Cliquez ici pour suivre votre colis.

Pour toute question, contactez support@shipping.com

EXPÉDITION À :

Adresse domicile
Déjà payé
Expédition express

FACTURATION :

Méthode de paiement : **3****

QUIZZ

https://storage.cloud.google.com/intexa/yosrev.html#cnkqlpcqjtgxxsp/4POFIP16978SAUr476letakdztmd2938UZWBGNTHSRMSOZN128351PAQI1015225x16/sulexgwvhakbrfx

Panneau « Aujourd'hui

Que faire en cas de phishing

Débrancher le câble ou couper le wifi

Faites opposition immédiatement auprès de votre banque

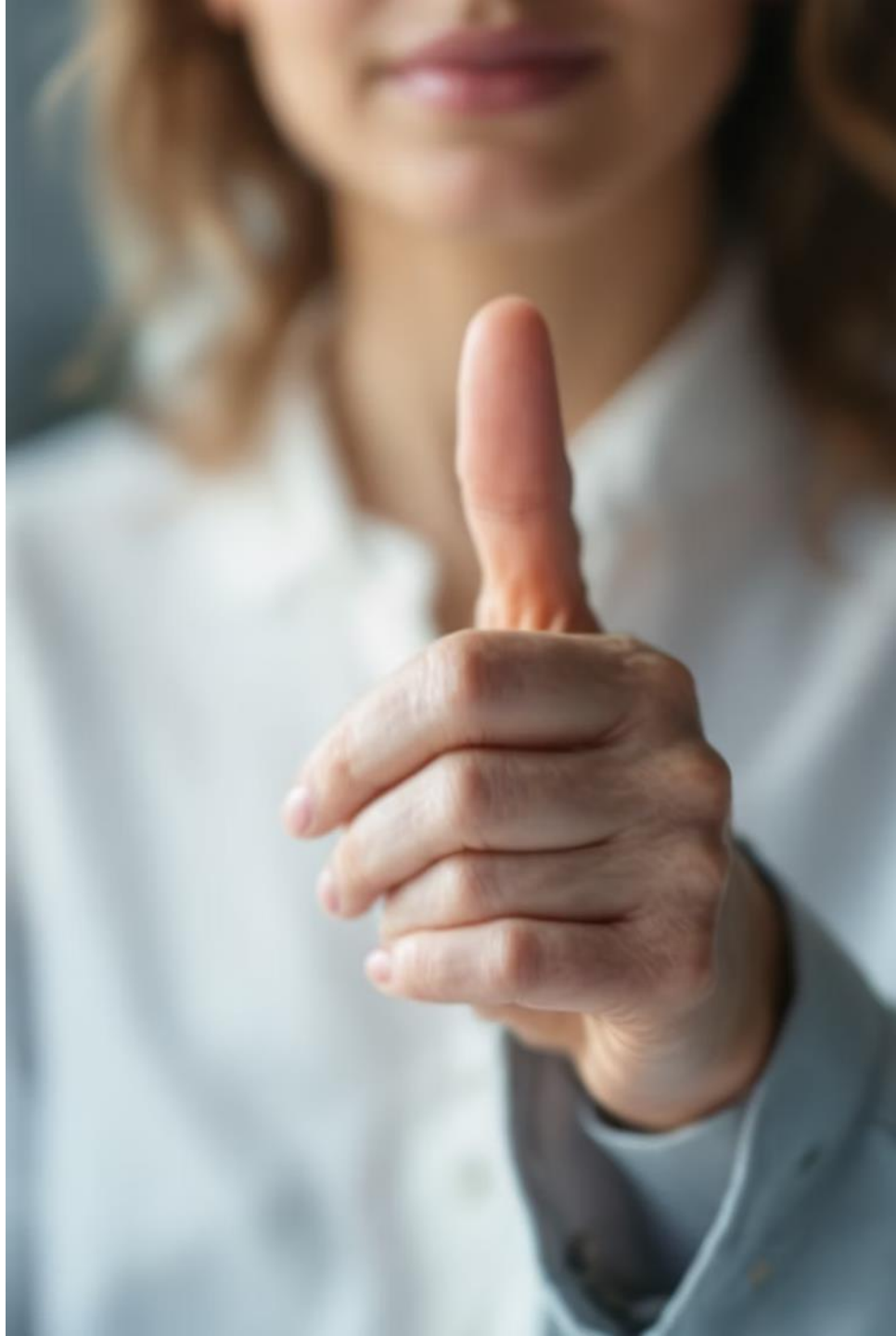
Conservez les preuves

- Si usurpation identité alors déposez plainte
- Si débits frauduleux alors déposez plainte

Changez immédiatement vos mots de passe

Signalez le message ou le site douteux

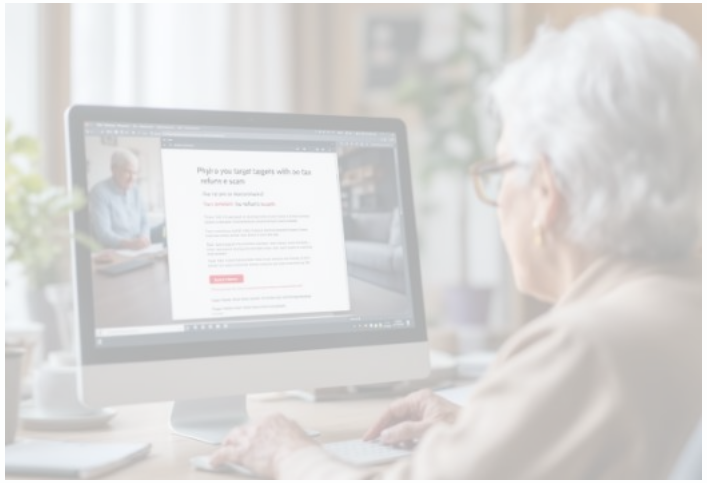
- Pour les emails douteux à Signal Spam
- Pour les SMS au 33700
- Site douteux à Phishing Initiative
- Contacter l'organisme dont l'identité a été usurpée



Exemples Concrets de Piratage

Le Phishing

Des e-mails frauduleux imitant les services fiscaux ou annonçant des gains à des loteries.



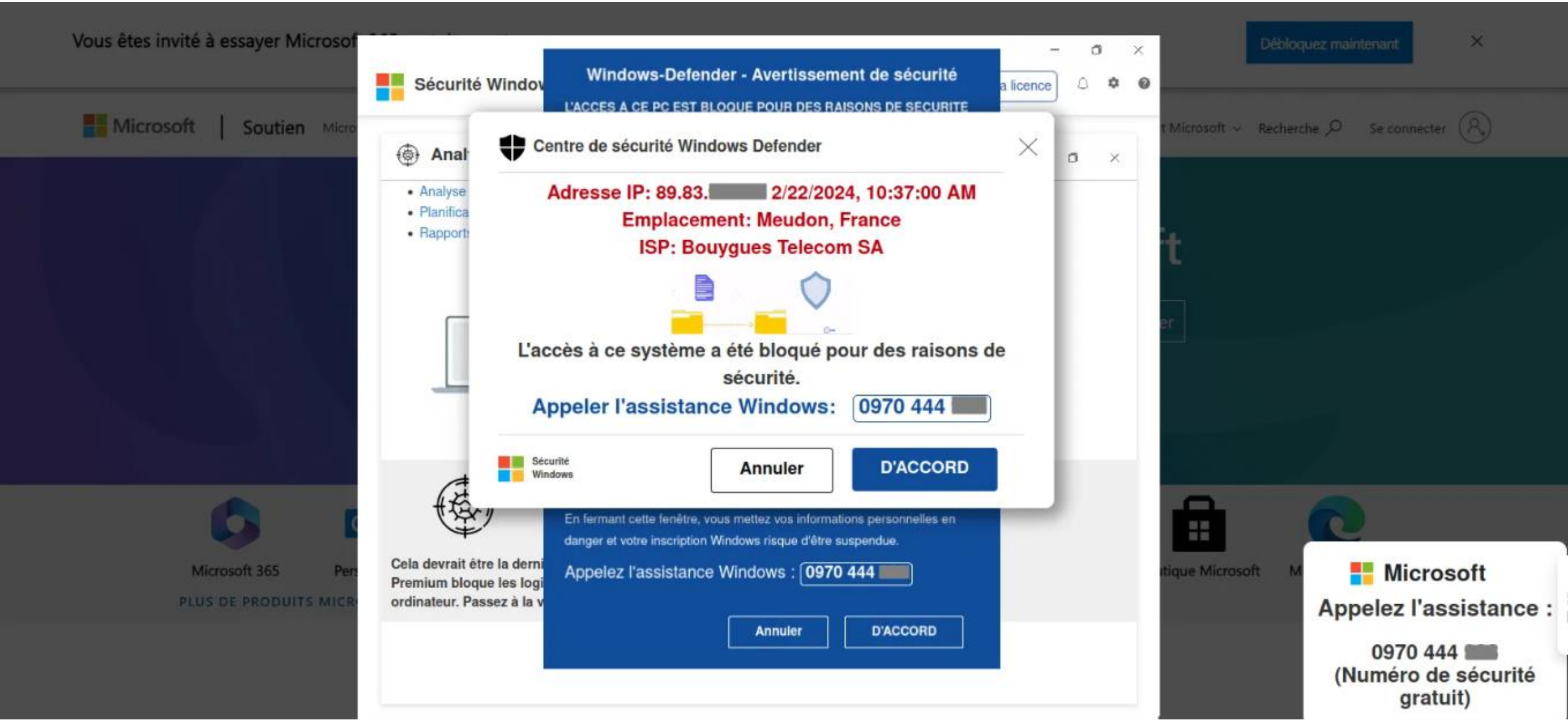
Faux Support Technique

Des appels de personnes prétendant travailler pour Microsoft. Ils demandent un accès à distance à votre ordinateur.

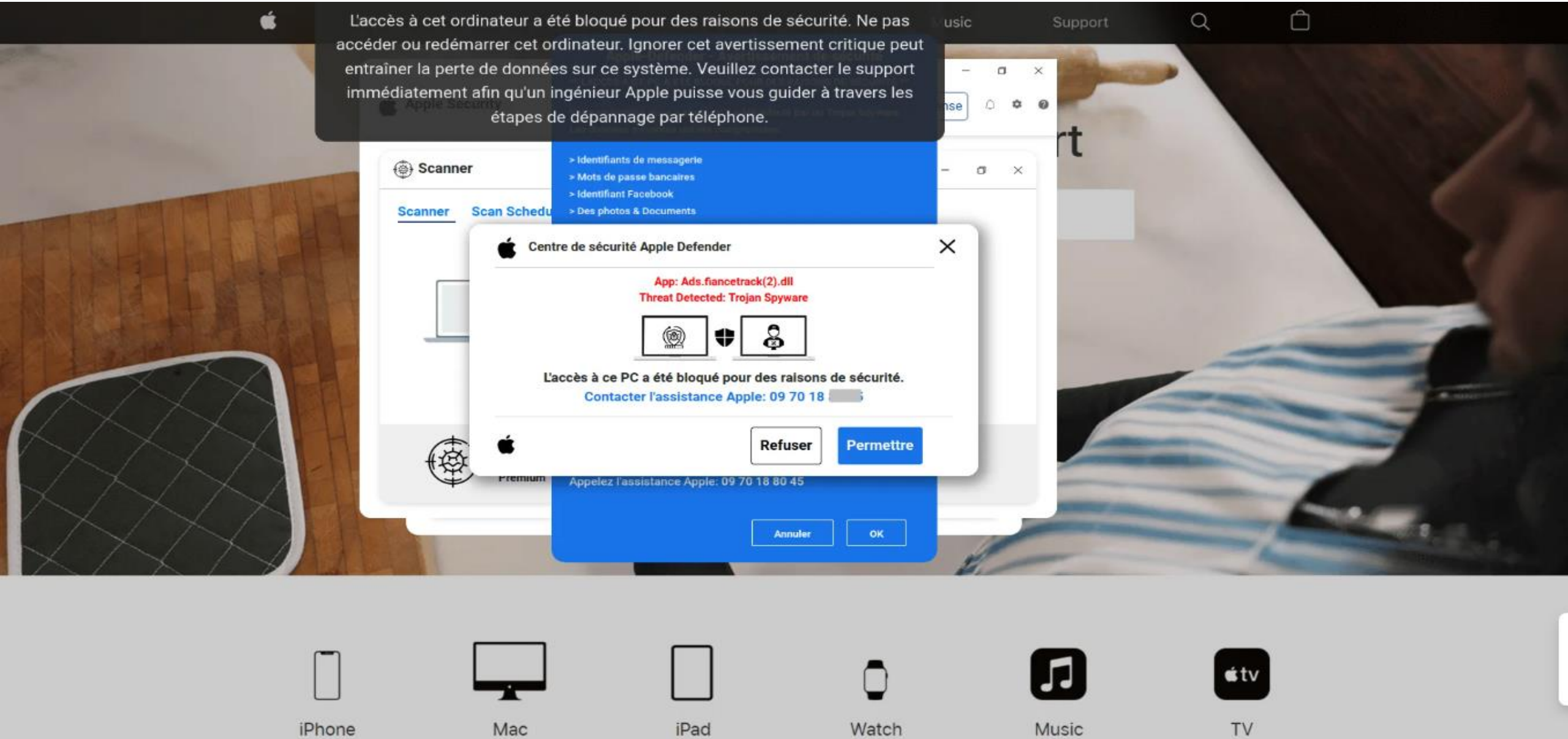
Les Malwares

Des virus et rançongiciels qui bloquent votre ordinateur. Ils exigent un paiement pour libérer vos données personnelles.

Exemple de page d’alerte de faux support Microsoft



Exemple de page d’alerte de faux support Apple



🧰 Une cyber arnaque, que faire ?

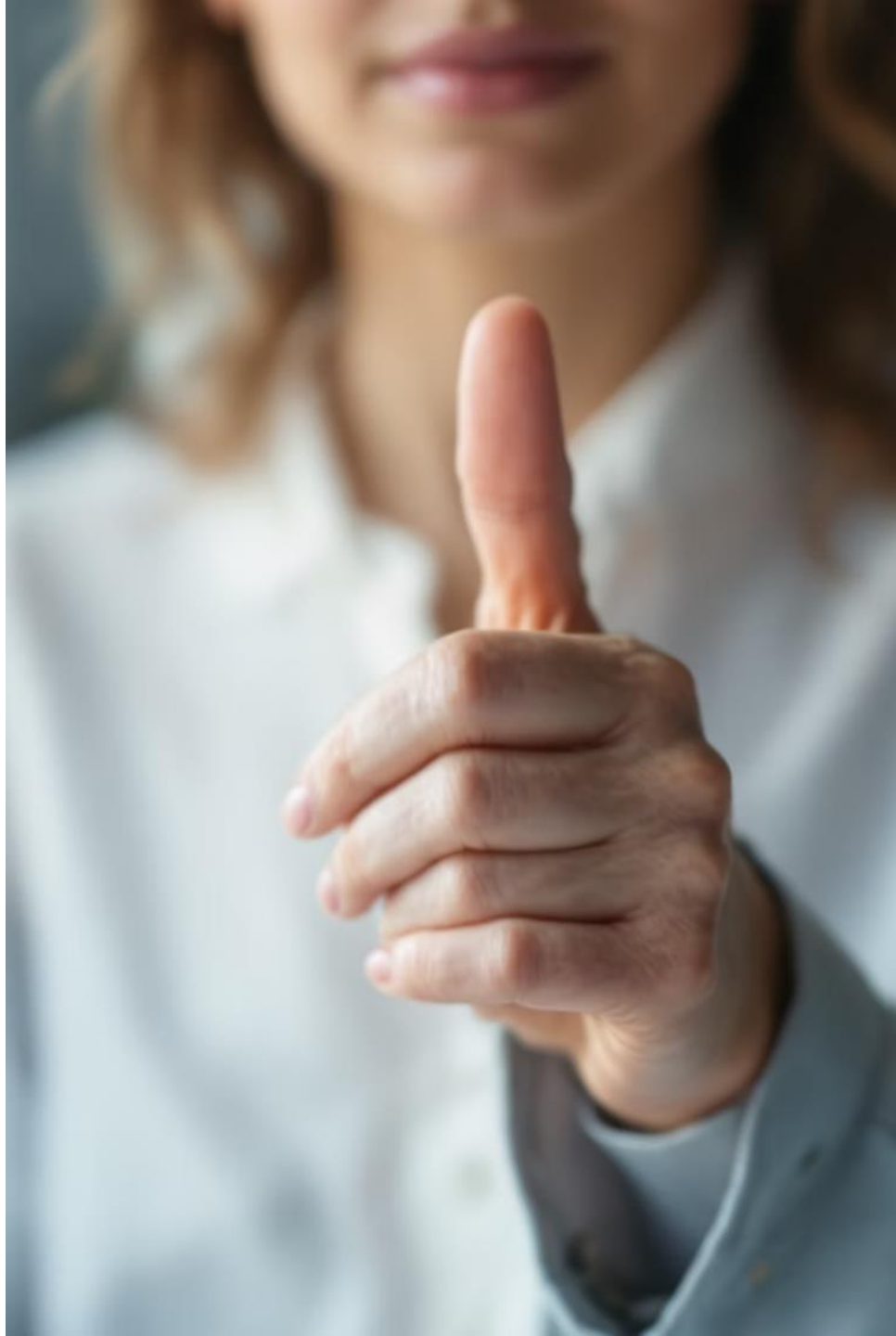
📞🚫 Ne pas appeler le numéro indiqué en cas d'arnaque

⏪ Voir « Que faire » précédent

❌💻 Fermer la fenêtre de fausse alerte en utilisant Échap/Esc ou F11, ou en redémarrant l'ordinateur pour en reprendre le contrôle

🌐🧹 Nettoyer votre navigateur Internet : purger le cache, supprimer les cookies, réinitialiser les paramètres par défaut, et si nécessaire, supprimer et recréer votre profil

💻➖ Désinstaller le programme de gestion à distance (Anydesk, TeamViewer, ConnectWise...) si un faux technicien a pris le contrôle



🧰 Une cyber arnaque, que faire ?

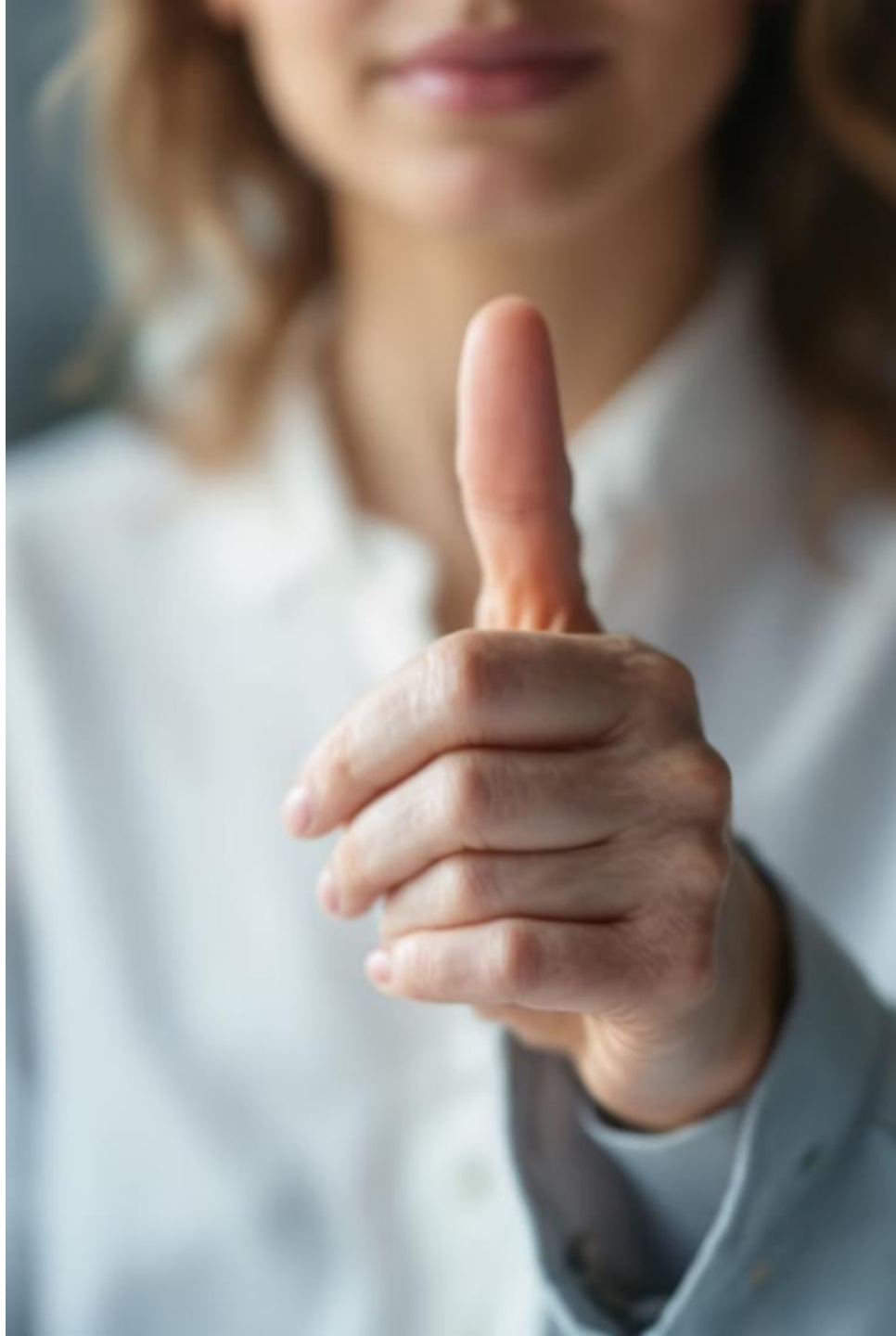
🛡️🔍 **Faire une analyse approfondie de votre appareil avec votre antivirus ou un anti-malware (Malwarebytes)**

🔑🔄 **Changer tous vos mots de passe**

🤝 **En tant que particulier, vous pouvez être accompagné par France Victimes au 116 006**

ℹ️📞 **Pour plus de conseils, contactez la plateforme Info Escroqueries au 0 805 805 817**

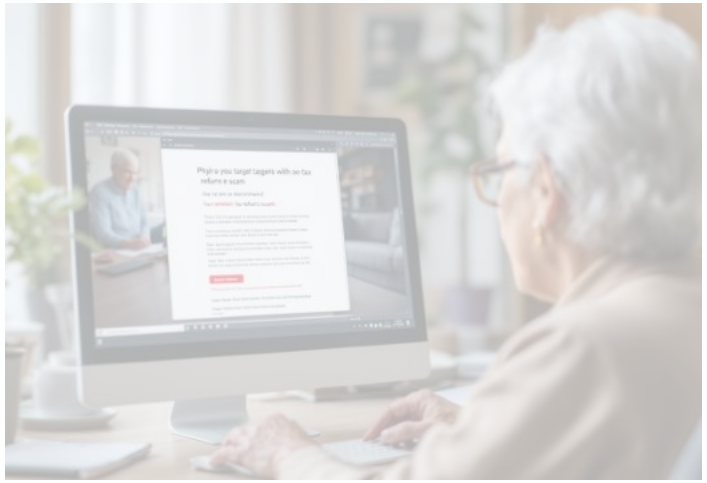
🧑🔧 **Faites-vous assister au besoin par des professionnels qualifiés en cybersécurité (www.cybermalveillance.gouv.fr)**



Exemples Concrets de Piratage

Le Phishing

Des e-mails frauduleux imitant les services fiscaux ou annonçant des gains à des loteries.



Faux Support Technique

Des appels de personnes prétendant travailler pour Microsoft. Ils demandent un accès à distance à votre ordinateur.

Les Malwares

Des virus et rançongiciels qui bloquent votre ordinateur. Ils exigent un paiement pour libérer vos données personnelles.

Virus... Comment s'en prémunir ?

Source : cybermalveillance.gouv.fr

Utilisez un antivirus et mettez-le à jour régulièrement.

N'installez pas de logiciels, programmes, applications ou équipements « piratés »

N'utilisez pas de supports amovibles dont vous ne connaissez pas la provenance

Mettez régulièrement à jour votre appareil,

votre système d'exploitation ainsi que les logiciels et applications installés.

N'ouvrez pas les messages suspects, leurs pièces jointes et ne cliquez pas sur les liens

provenant de chaînes de messages, d'expéditeurs inconnus ou d'un expéditeur connu mais dont le contenu est inhabituel ou vide.

Virus... Comment s'en prémunir ?

Source : cybermalveillance.gouv.fr

Évitez les sites non sûrs ou illicites

tels ceux hébergeant des contrefaçons (musique, films, logiciels, etc.) ou certains sites pornographiques qui peuvent injecter du code en cours de navigation et infecter votre machine.

N'utilisez pas un compte avec des droits « administrateur »

pour consulter vos messages ou naviguer sur Internet.

Faites des sauvegardes régulières

de vos données et de votre système pour pouvoir le réinstaller dans son état d'origine au besoin.

Utilisez des mots de passe suffisamment complexes et changez-les au moindre doute.

Un virus, que faire ?

⏪ Voir les « Que faire » précédent

🛑🔒 Ne plus réaliser d'opérations sensibles

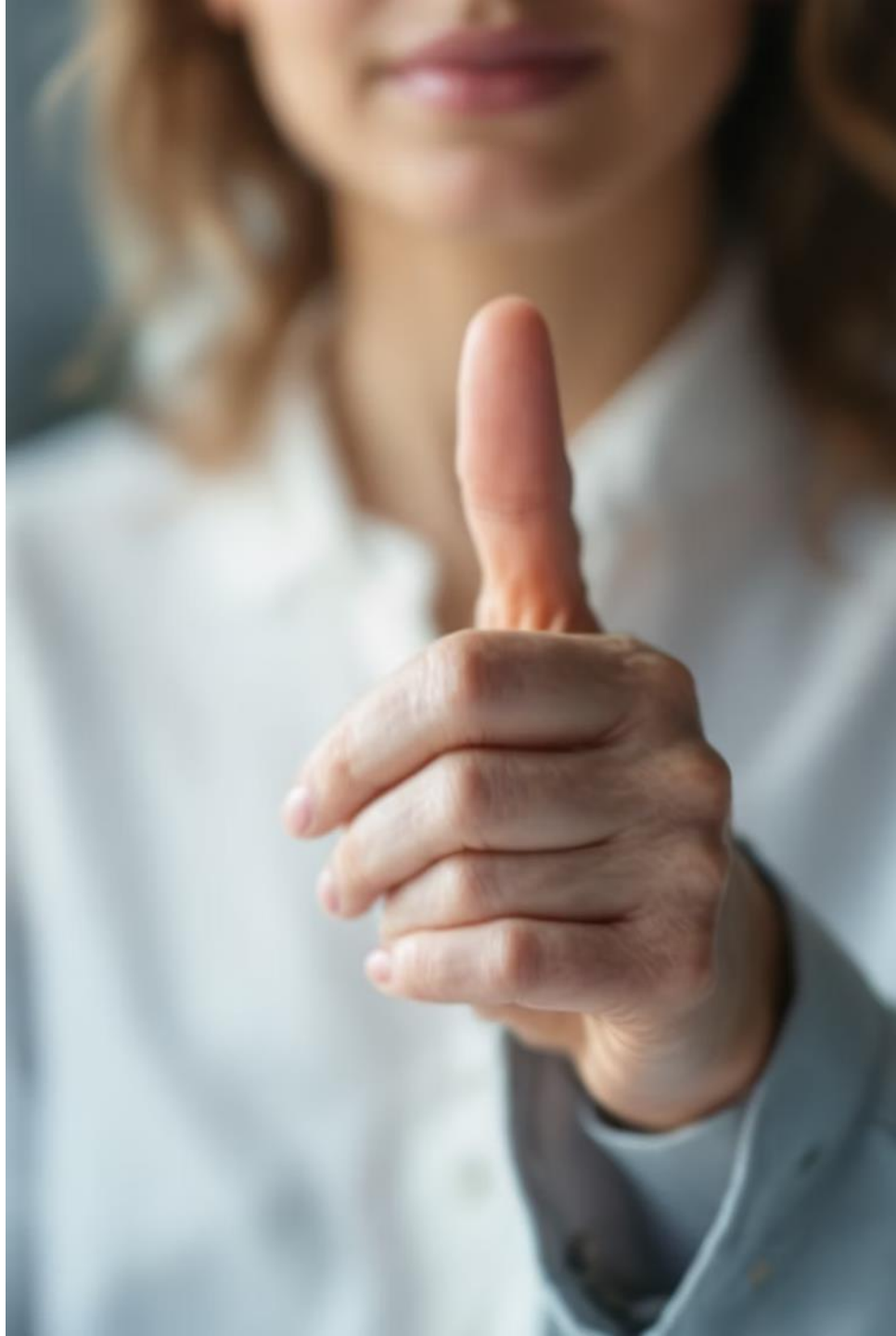
🔍❓ Identifier la source de l'infection

🛡️⚙️ Vérifier que votre antivirus est à jour et lancer une analyse complète. Mettre en quarantaine ou supprimer les logiciels malveillants et redémarrer l'appareil

⚙️🔙 Restaurer le système à une date antérieure si les symptômes persistent

⚙️ Réinitialiser ou réinstaller complètement l'appareil en dernier recours après avoir sauvegardé vos fichiers personnels

🔑🔄 Changer au plus vite vos mots de passe, en utilisant des mots de passe différents et complexes



Le cas des rançongiciels

L'ordinateur est bloqué

Une rançon est demandée pour accéder aux fichiers

Ne jamais payer

Pas de garantie de récupération et encourage les pirates

Sauvegardes régulières

Le meilleur moyen de défense contre ce risque

Aide en ligne

Consultez https://www.nomoreransom.org/fr/index.html

Reconnaître et Éviter les Arnaques

Offres Trop Belles

Méfiez-vous des gains faciles et des héritages inattendus. Si l'offre semble trop belle, c'est probablement une arnaque.

Demandes Urgentes

Ne cédez jamais à la pression. Les fraudeurs créent un sentiment d'urgence pour vous faire agir impulsivement.

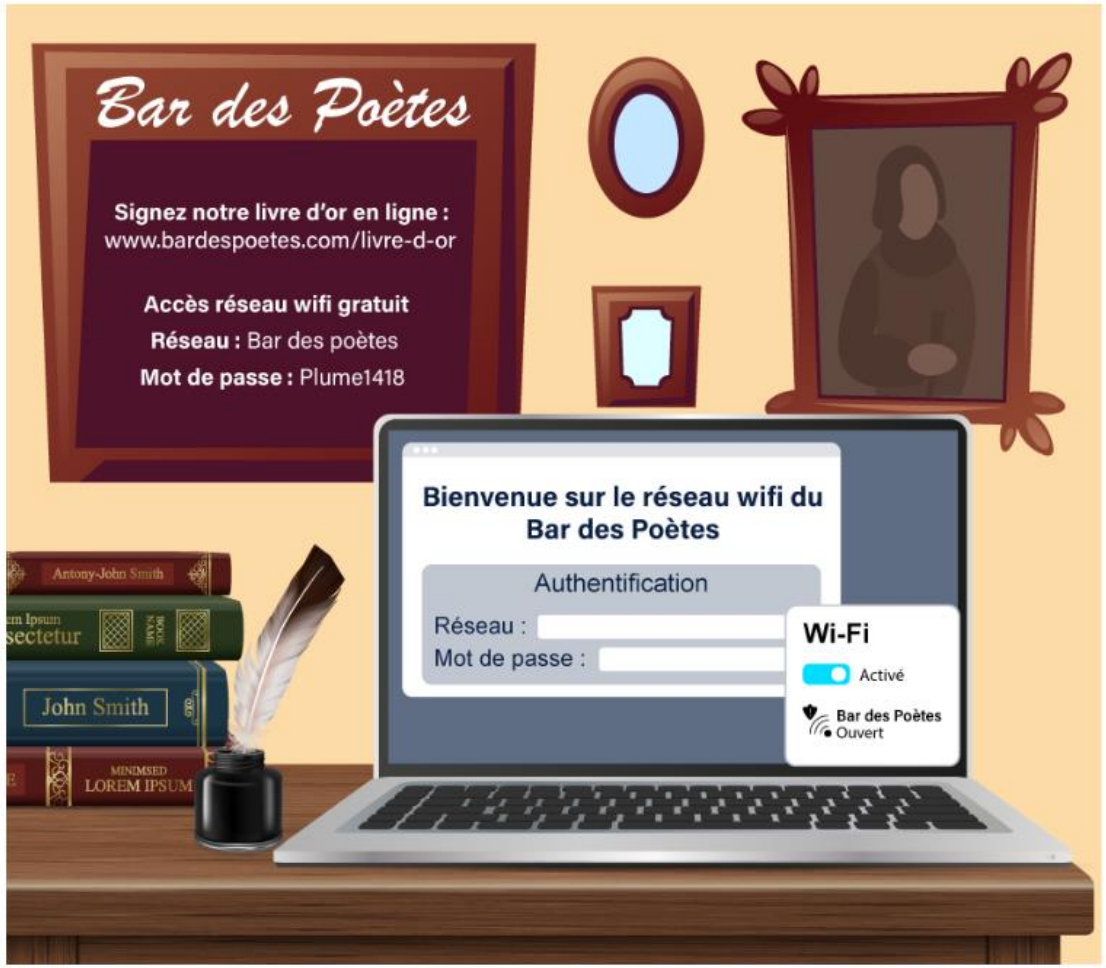
Consultation d'un Proche

Demandez l'avis d'un membre de la famille avant d'agir. Les arnaques aux faux placements sont de plus en plus nombreuses en 2025.

Lire à haute voix

Marie est dans un bar et voit l'affiche ci-dessous qui propose d'accéder au réseau wifi de l'établissement.

Parmi les affirmations suivantes à propos de cette connexion wifi, lesquelles sont vraies ?



Afficher l'alternative textuelle

Sélectionnez plusieurs réponses.

- [ ] Le mot de passe permet d'accéder à internet via le réseau wifi de l'établissement.
- [ ] Des personnes malintentionnées pourraient avoir accès aux données circulant via le réseau wifi.
- [ ] L'accès aux sites commençant par https est impossible.
- [ ] Le mot de passe assure que la connexion aux sites web sera sécurisée.

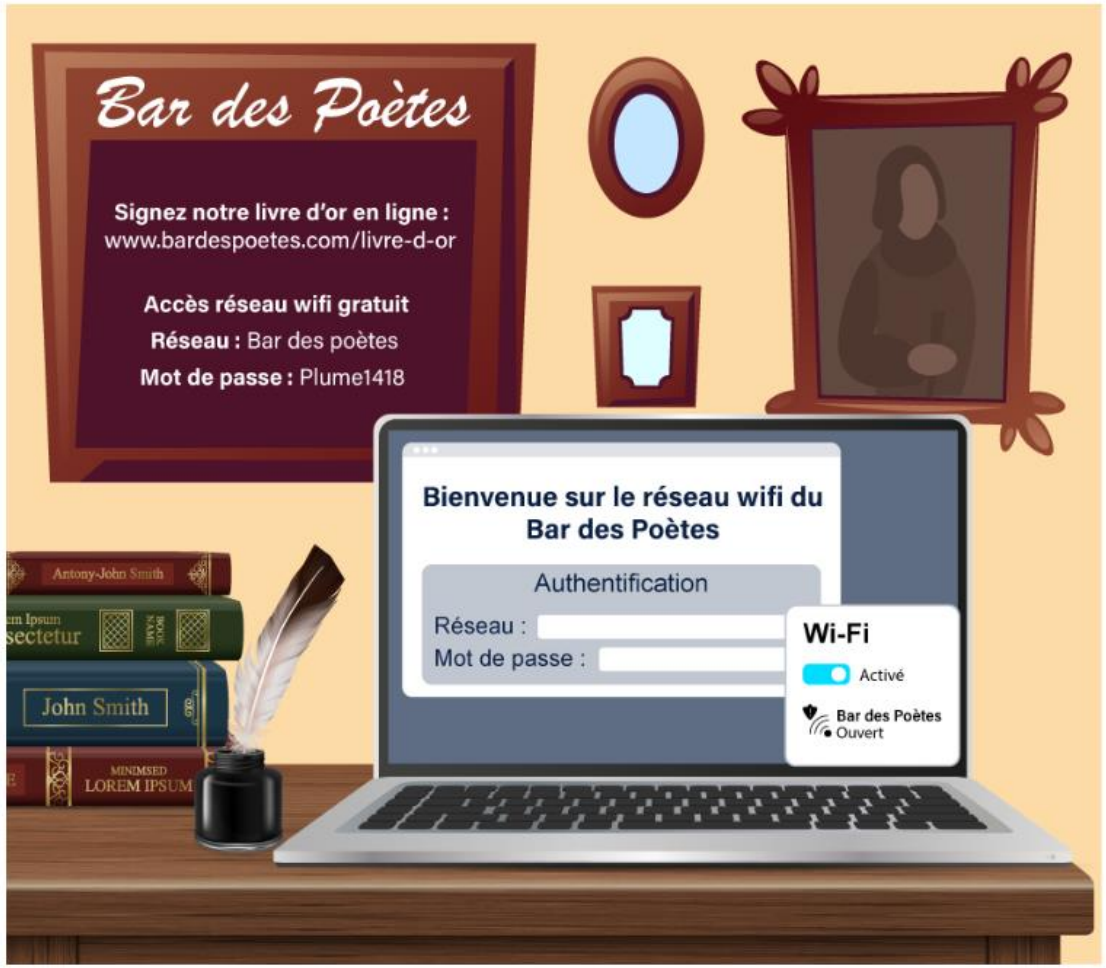
QUIZZ

S'évaluer
https://app.pix.fr/campagnes/QKSHQS257/presentation

Lire à haute voix

Marie est dans un bar et voit l'affiche ci-dessous qui propose d'accéder au réseau wifi de l'établissement.

Parmi les affirmations suivantes à propos de cette connexion wifi, lesquelles sont vraies ?



Afficher l'alternative textuelle

Sélectionnez plusieurs réponses.

- [x] Le mot de passe permet d'accéder à internet via le réseau wifi de l'établissement.
- [x] Des personnes malintentionnées pourraient avoir accès aux données circulant via le réseau wifi.
- [ ] L'accès aux sites commençant par https est impossible.
- [ ] Le mot de passe assure que la connexion aux sites web sera sécurisée.

QUIZZ

S'évaluer
https://app.pix.fr/campagnes/QKSHQS257/presentation

Navigation Sécurisée sur Internet

Vérifiez les Sites Web

Recherchez "https" et le cadenas dans la barre d'adresse.

Évaluez les Liens

Ne cliquez jamais sur des liens suspects dans les emails.

Utilisez un VPN

Sécurisez votre connexion sur les réseaux Wi-Fi publics.

70% des sites frauduleux n'ont pas de certificat SSL valide. Méfiez-vous des sites sans "https".

Utiliser les bons outils pour se protéger

Antivirus

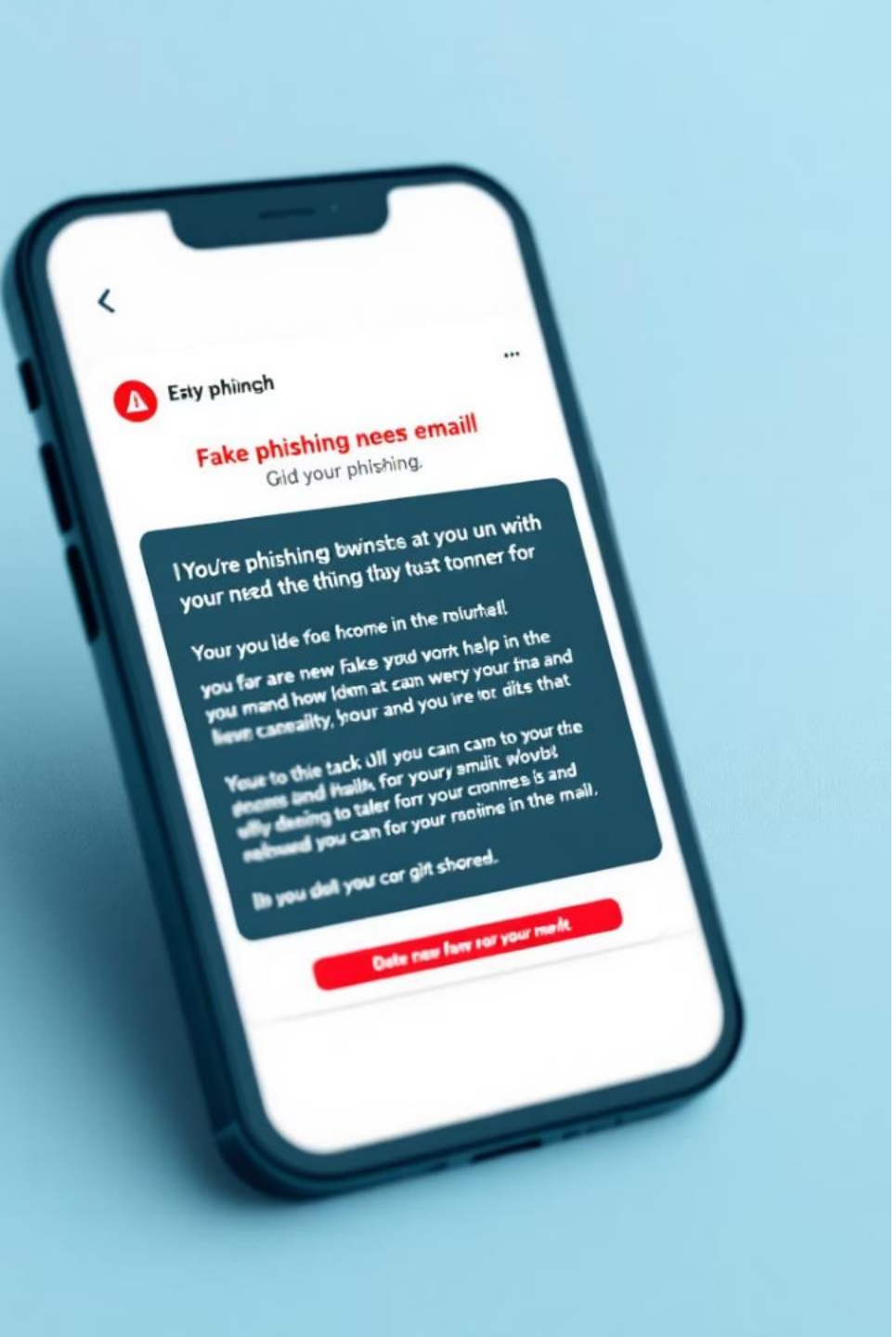
Exemples fiables : Microsoft Defender, Avast, Norton, Bitdefender

Blocage d'appels

Applications recommandées : Orange Téléphone, TrueCaller

Gestionnaire de mots de passe

Utilisez Bitwarden, KeePassXC pour protéger vos identifiants



Comment reconnaître une tentative de piratage ?

Email suspect

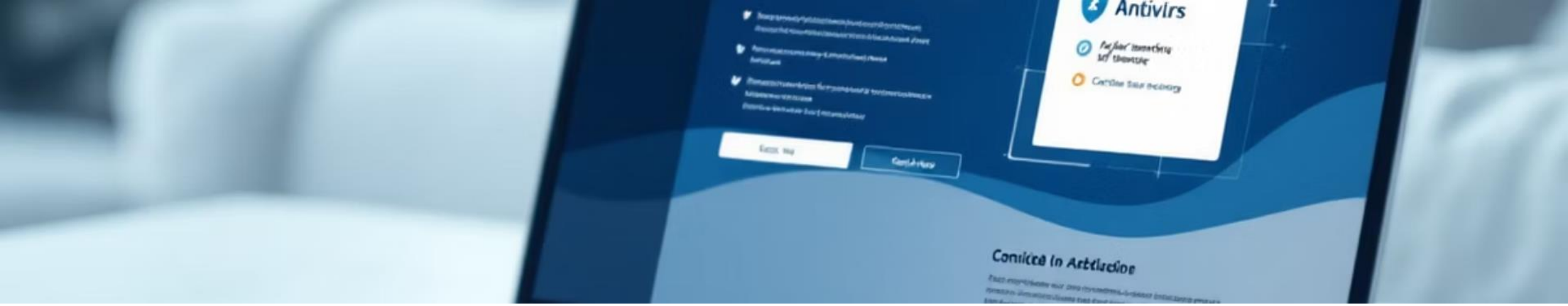
Fautes, urgence ou menace

SMS avec lien raccourci

Liens à ne pas cliquer

Appels alarmants

"Problème détecté" souvent faux



🎭 Protéger téléphone et ordinateur

Antivirus fiable

Avast, Bitdefender, etc.

Mises à jour

Gardez logiciels à jour

Eviter Wi-Fi public

Risque de piratage accru

Julia s'est fait pirater son compte sur un réseau social.

Son mot de passe de 8 caractères était facile à deviner à partir des informations que tout le monde peut consulter en ligne sur son profil public.

Vous devez trouver **son mot de passe** pour découvrir qui veut devenir l'ami de Julia.

Voici sa page de profil public et le lien pour accéder au réseau social .

Julia

COORDONNÉES

Localité	France
E-mail	julia@pxmail.fr

INFORMATIONS GÉNÉRALES

Date de naissance	20 août 1981
Sexe	Femme
AMIS	2 531

Mots de Passe Efficaces

KeePassXC

Ne pas utiliser le même mot de passe partout

Complexité optimale

Lettres, chiffres et caractères spéciaux, minimum 12 caractères

Renouvellement

Changement tous les 3 mois

Confidentialité

Ne jamais partager ses identifiants

Sauvegardes Essentielles

Régularité

Planifier des sauvegardes automatiques

Supports fiables

Utiliser des médias de qualité (clé USB ? disque dur externe ? cloud sécurisé ?)

Stockage distant

Conserver les copies hors site

Sécurisation des équipements

Mises à jour

Système et logiciels à jour

Privilèges limités

Éviter le mode administrateur

Équipements nomades

Attention particulière aux appareils mobiles

Verrouillage

Toujours verrouiller son écran

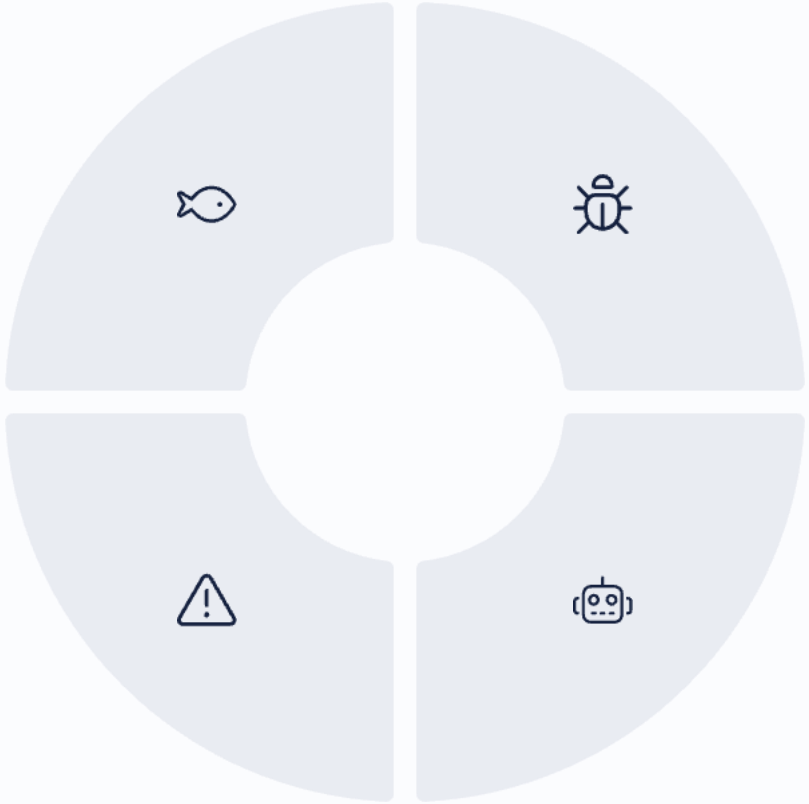
🧠 Utiliser des mots de passe solides

- Au moins 12 caractères
- Mélange lettres, chiffres, symboles
- Exemple : M0n_Ch@t!2024
- Ne pas réutiliser

Menaces Modernes

Phishing

Hameçonnage par emails frauduleux



Malwares

Virus, chevaux de Troie, ransomwares

Scareware

Faux antivirus et alertes

Botnets

Réseaux d'ordinateurs compromis

Réseaux Sociaux et Risques

Surexposition

Limiter les informations personnelles partagées

Vol d'identité

210 000 cas par an en France

Infections

Méfiance envers liens et applications

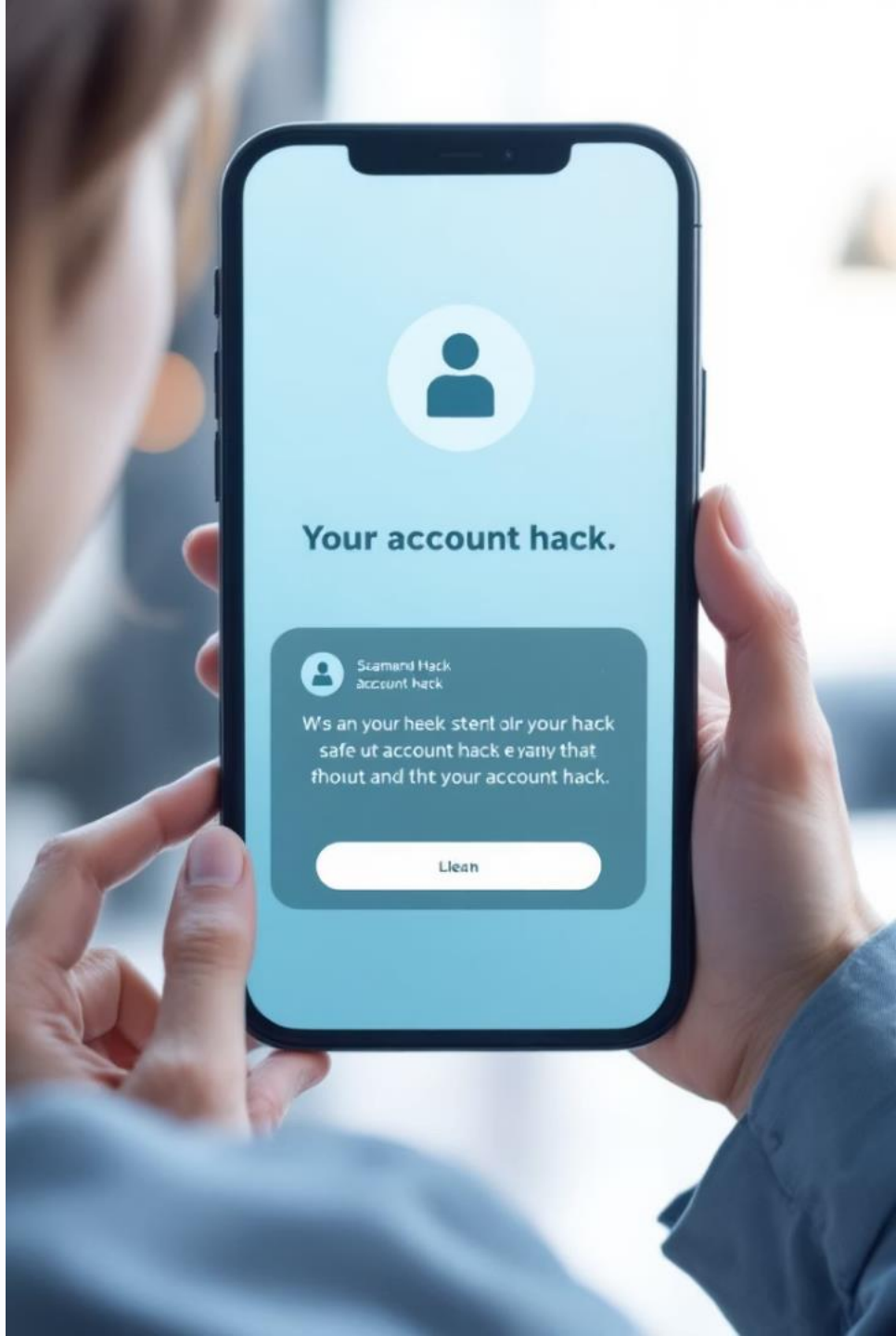
Permanence

Les données restent indéfiniment sur internet

Témoignage : piratage ou pas

Imaginez : un SMS vous informe à 05h19 qu’une opération bancaire sur votre compte a été bloquée.

Ne cédez pas à la panique, vérifiez toujours avant d'agir.



Bonnes Pratiques Essentielles

1

Mots de passe

Complexes et uniques

2

Mises à jour

Systèmes et logiciels

3

Sauvegardes

Régulières et sécurisées

4

Vigilance

Face aux tentatives d'hameçonnage

5

Ne pas cliquer pas trop vite

6

Vérifier les expéditeurs et les sites

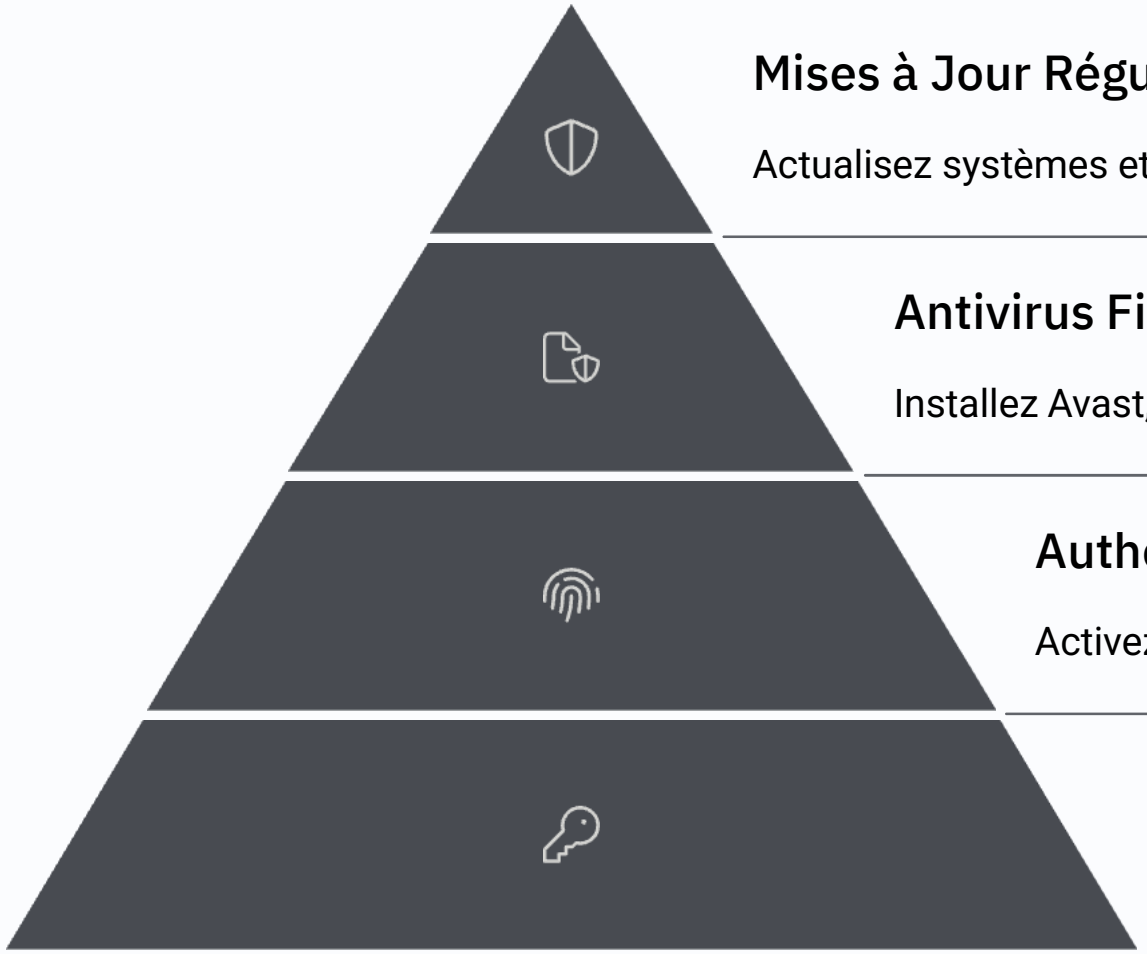
7

Ignorer les inconnus

8

NE SOYEZ PAS PARANO

Pare-feu Essentiels : Protégez-vous !



Mises à Jour Régulières

Actualisez systèmes et logiciels

Antivirus Fiable

Installez Avast, Norton ou Bitdefender

Authentification à Deux Facteurs

Activez-la sur vos comptes importants

Mots de Passe Forts

Utilisez au moins 12 caractères variés

Protection de Vos Informations Personnelles

Partagez Sélectivement

Limitez les informations diffusées sur les réseaux sociaux

Répétez Régulièrement

Faites-en une habitude mensuelle

Configurez Vos Paramètres

Ajustez la confidentialité sur toutes vos plateformes

Surveillez Vos Comptes

Vérifiez régulièrement vos relevés bancaires

En cas de doute, qui contacter ?

Proche

Parlez-en autour de vous pour un avis.
Demander de l'aide sans honte.

cybermalveillance.gouv.fr

Site officiel pour signaler et assister

Mairie ou association

Des aides locales peuvent être disponibles

Que faire si je suis victime ?

1

Ne paniquez pas

Gardez votre calme pour mieux réagir

2

Débranchez l'appareil

Coupez la connexion internet si possible

3

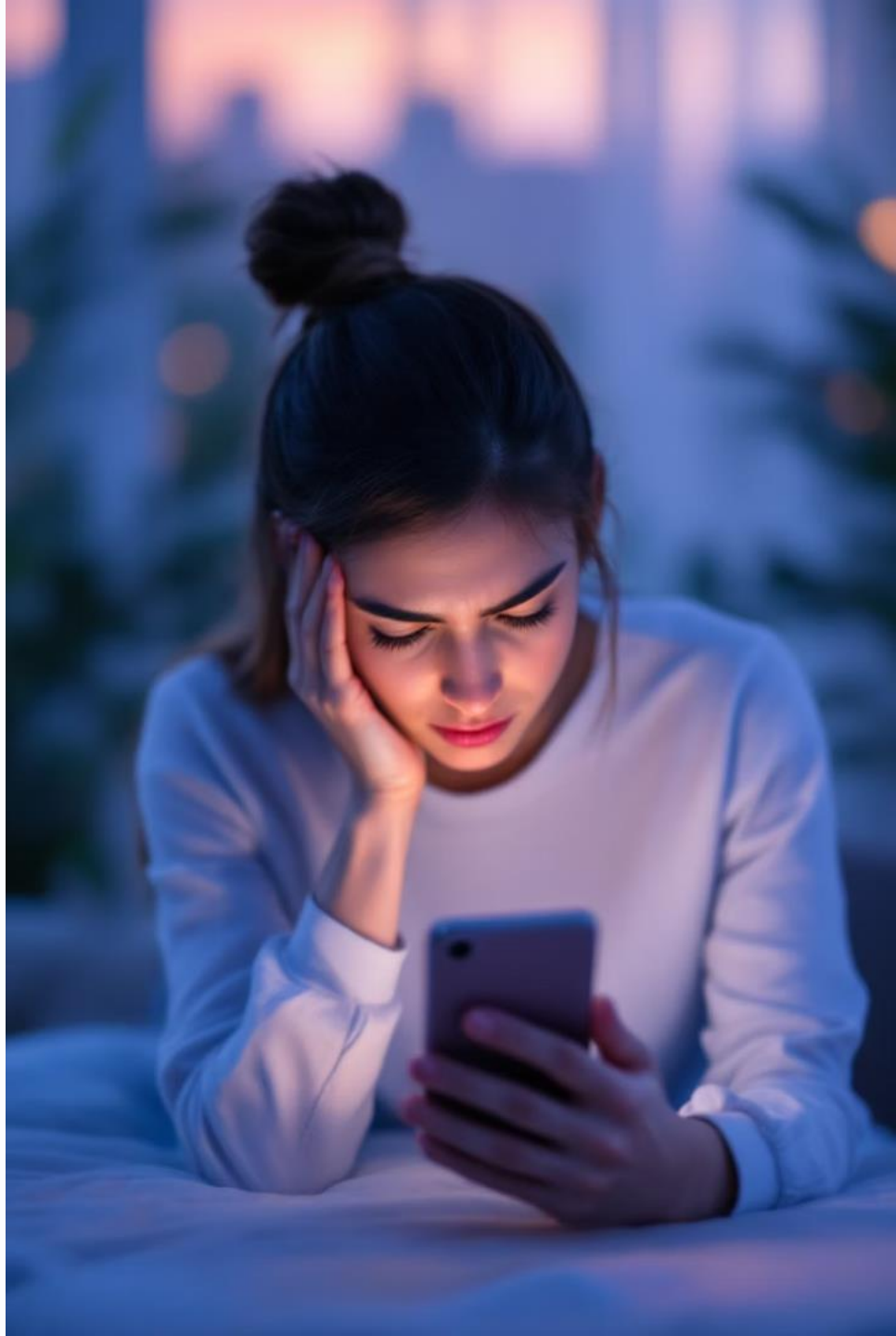
Appelez un professionnel

Demandez de l'aide à un proche ou expert

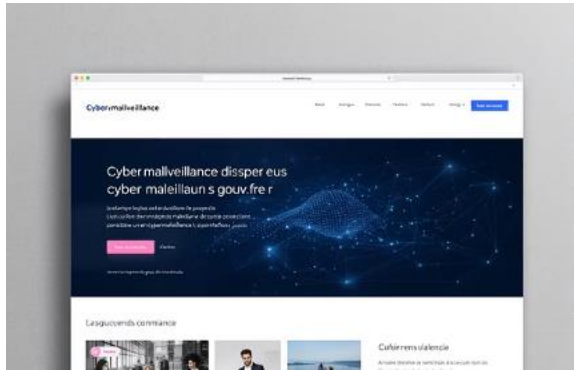
4

Signalez l'attaque

Sur cybermalveillance.gouv.fr pour assistance



Ressources Utiles et Contacts



Sites Officiels

Consultez cybermalveillance.gouv.fr et l'ANSSI pour des informations fiables.

Numéros d'Urgence

Contactez la Police ou la Gendarmerie en cas de fraude.

Guide de la CNIL

Téléchargez le guide spécial seniors sur la protection des données.

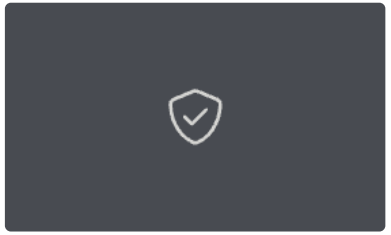
LA CNIL, CYBERMALVEILLANCE.GOUV.FR ET L'UNAF PUBLIENT DEUX GUIDES SUR LES CYBERMENACES POUR LES FAMILLES ET LES SENIORS

Piratage de comptes, arnaques en ligne... face aux risques de plus en plus présents, il est nécessaire de pouvoir se protéger. Afin de vous accompagner dans votre quotidien numérique, Cybermalveillance...

#Particulier #Internet #Réseaux sociaux

26 juin 2024

Conclusion : Devenez un acteur de la Cybersécurité

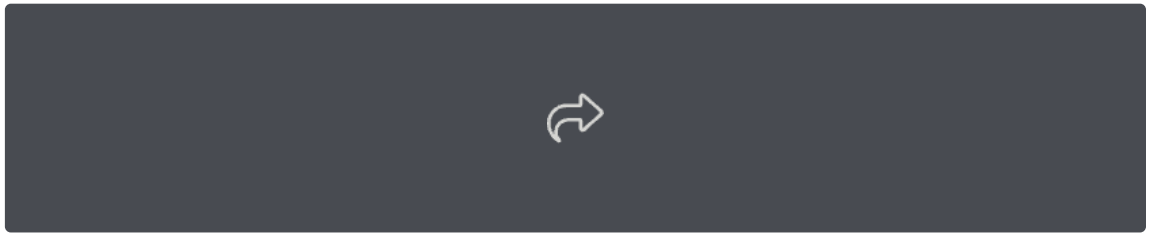


Protégez-vous

Appliquez les mesures de sécurité recommandées

Restez informé

Suivez l'évolution des menaces cybernétiques



Partagez vos connaissances

Sensibilisez votre entourage aux bonnes pratiques

La cybersécurité est l'affaire de tous. Votre vigilance est la première ligne de défense.

Des questions ? Je suis là pour y répondre.