



RECONNAÎTRE ET ÉVITER LES ARNAQUES EN LIGNE

La Brigade
des
arnaques

Atelier numérique ligue de l'enseignement 05

CAS N°1 : MADAME AZUR



Madame Azur a découvert qu'on avait fait des achats à sa place et en son nom sur internet. Elle ne comprend pas d'où vient sa fuite de données. Jetons un coup d'oeil à son ordinateur et surtout à ses mails.



madameazur@mail.com - Boîte de réception

caporalpoivre@mail.com -
Voici les photos que tu
m'as demandées !  

mademoisellelila@mail.com
Lien pour le manteau 

cabinetemeraudeetparme@mail.com
Vous êtes en retard dans
votre paiement !!! 

Bonjour Chère Azur,

Voici les photos du chien car tu m'as demandé de
ses nouvelles.
J'espère que tu te portes bien, je pense que tu lui
manques.

A bientôt peut-être,

Amicalement,

Poivre

Photochien.jpg



Téléchargez la pièce jointe

Aperçu

madameazur@mail.com - Boîte de réception

caporalpoivre@mail.com -

Voici les photos que tu
m'as demandées !  

mademoisellelila@mail.com

Lien pour le manteau 

cabinetemeraudeetparme@mail.com

Vous êtes en retard dans
votre paiement !!! 

Salut ma belle !

Tu m'as dit que tu as adoré mon manteau de l'autre
jour, du coup voici le lien pour l'acheter :

[https://www.almeparis.com/products/manteau-
dorian-noir](https://www.almeparis.com/products/manteau-dorian-noir)

Gros bisou !

Lila

madameazur@mail.com - Boîte de réception

caporalpoivre@mail.com -

Voici les photos que tu
m'as demandées !  

mademoisellelila@mail.com

Lien pour le manteau 

cabinetemeraudeetparme@mail.com

Vous êtes en retard dans
votre paiement !!! 

Bonjour,

Nous avons constater un retard de paiement suite à
votre dernier examen médicale.

Merci de nous renvoyer vos coordonnées sur ce lien
LE PLUS RAPIDEMENT POSSIBLE !!!, sous peine
d'amende.

<http://cripplezone.ru/payement/>

Sincèrement vôtre,

Docteur Emeraude

QUI A ARNAQUÉ MME AZUR ?

Bureau

Phishing

Docteur
Emeraude

Qu'est-ce que le phishing ?

L'art de se faire passer pour quelqu'un d'autre

Qu'est-ce que le phishing ?

L'hameçonnage est une technique qui consiste à se faire passer pour un tiers de confiance (votre banque, une administration, un commerçant, un proche) pour vous pousser à communiquer des informations personnelles ou bancaires, ou à installer un programme malveillant. Il peut arriver par mail, mais aussi par SMS (on parle de « smishing »), par QR code frauduleux (« quishing ») ou par téléphone.

Comment le reconnaître ?

Un message frauduleux joue presque toujours sur l'urgence (« sous 48h », « sous peine d'amende »). L'adresse de l'expéditeur ou le lien sont souvent fantaisistes, le message contient parfois des fautes, et surtout on vous demande de cliquer sur un lien ou d'ouvrir une pièce jointe pour livrer des informations confidentielles.

Le bon réflexe

Ne cliquez **jamais** sur le lien reçu. Rendez-vous directement sur le site officiel en tapant vous-même son adresse, ou passez par votre application habituelle.

Et ça n'arrive pas que par mail...

Tous les chemins mènent à Rome

Les mêmes pièges peuvent arriver par SMS et QR Code. De manière générale tout ce qui peut vous amener sur internet.

Chronopost : votre colis est en attente de livraison. Des frais de 2,99 € restent à régler : <http://chronopost-suivi.xyz/pay>

AMELI : votre carte Vitale arrive à expiration. Confirmez vos informations avant le 05/09 : <http://ameli-maj.info>

ANTAI : une amende de 35 € reste impayée. Régularisez votre situation sous 48h : <http://amendes-gouv.net>

CAS N°2 : DOCTEUR EMERAUDE



L'adresse mail qui a contacté Mme Azur est bien celle du Docteur Emeraude ! Il nie avoir envoyé ce mail donc on peut suspecter une nouvelle arnaque, cette fois-ci envers le docteur ! Il dit être très prudent mais on va quand même fouiller sa boîte mail.

CONFIDENTIAL

docteuemeraude@mail.com - Boîte de réception

france-travail.fr
Fuite de données



professeurparme@mail.com
J'ai une question pour le boulot ?



Bonjour,

Suite à un piratage massif de nos serveurs, nous pensons que les données que vous nous aviez confiées ne sont plus en sécurité.

Nous vous invitons à rapidement changer de mot de passe en vous identifiant sur www.france-travail.fr



docteu^{re}meraude@mail.com - Boîte de réception

france-travail.fr
Fuite de données



professeurparme@mail.com
J'ai une question pour le boulot ?



Salut Emeraude,

J'ai une question, toi qui t'y connais en sécurité informatique. Ma femme me dit qu'il faut un mot de passe différent pour chaque site... On est d'accord que c'est trop compliqué et que personne ne fait ça ?! Moi par exemple j'ai le même mot de passe pour la boîte mail du cabinet médical et mon compte France Travail.

Tu me diras ça !

A bientôt,

Parme

QUI A ARNAQUÉ DOCTEUR EMERAUDE ?

Infirmierie

Fuite de
données/
piratage de
compte

Professeur
Parme

Qu'est-ce qu'une fuite de données ?

Elles s'échappent !

Qu'est-ce que c'est ?

Une fuite de données, c'est quand des informations personnelles que vous aviez confiées à un site (mot de passe, adresse, numéro) sont dérobées ou rendues publiques à la suite d'un piratage de ce site. Le piratage de compte, c'est la conséquence : quelqu'un prend le contrôle d'un de vos comptes, souvent parce que le mot de passe qui a fuité était aussi utilisé ailleurs.

Comment les reconnaître ?

Le site concerné est censé vous prévenir qu'il a subi une fuite. Côté piratage, les signes sont concrets : vous n'arrivez plus à vous connecter, vos proches reçoivent des messages que vous n'avez pas envoyés, ou vous recevez des alertes de connexion et des demandes de réinitialisation que vous n'avez pas demandées.

Le bon réflexe

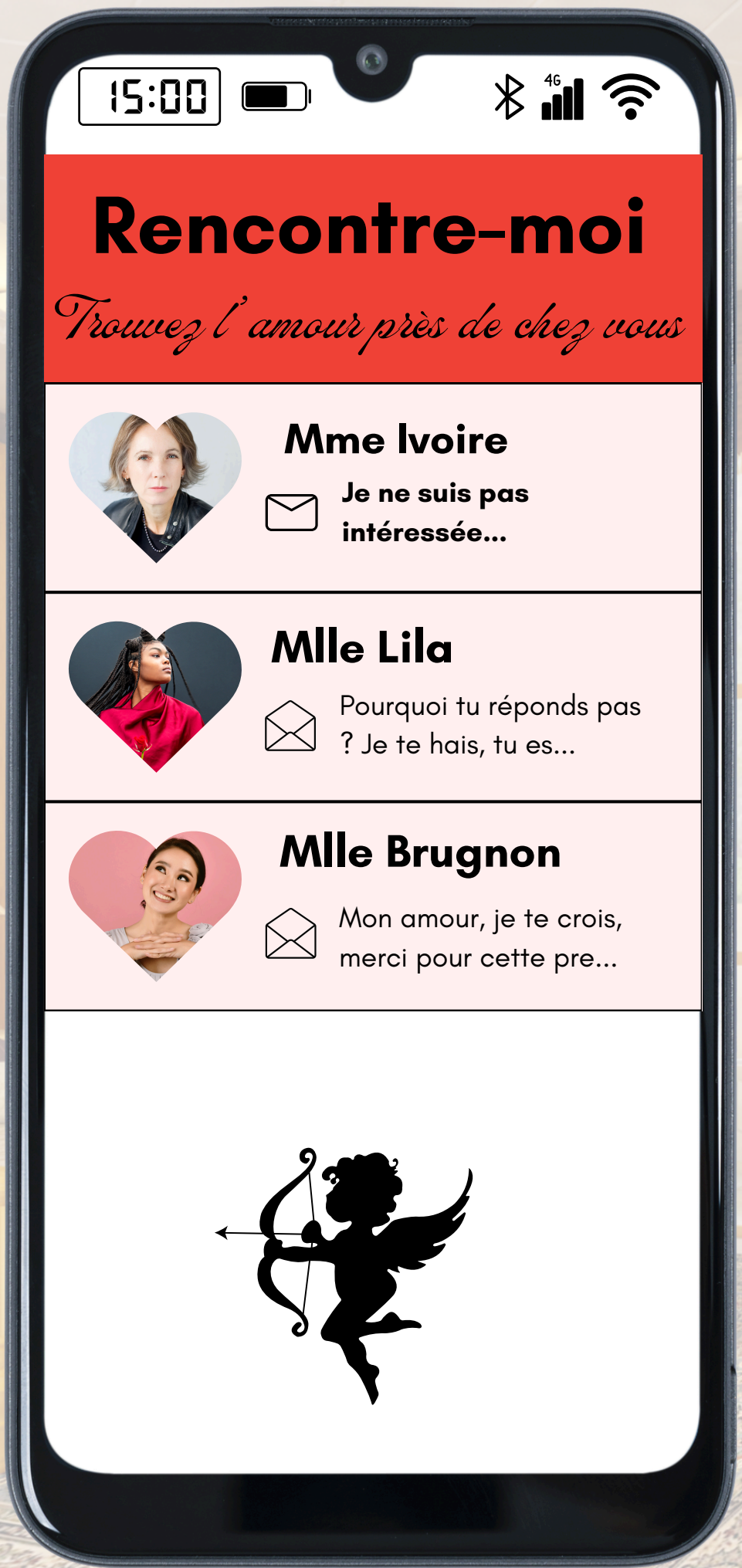
Un mot de passe différent pour chaque compte important, pour qu'une seule fuite ne fasse pas tomber tous les autres. Et quand c'est possible, activez la double authentification.

CAS N°3 : PROFESSEUR PARME



Nous allons voir le professeur Parme et on lui demande d'où vient le piratage de sa boîte mail.
Il pense qu'il s'est fait avoir sur une application de rencontre.
Il nous tend son téléphone.

CONFIDENTIAL



15:00



Rencontre-moi

Trouvez l'amour près de chez vous



Mme Ivoire



Je ne suis pas intéressée...



Mlle Lila



Pourquoi tu réponds pas ? Je te hais, tu es...



Mlle Brugnion



Mon amour, je te crois, merci pour cette pre...





15:00



Rencontre-moi

Trouvez l'amour près de chez vous



Mlle Lila

Comment oses-tu me quitter avec un message ? Quelle honte !

Pourquoi tu réponds pas ? Je te hais ! Je vais tout faire pour te pourrir la vie !

Arrête ! J'ai rencontré quelqu'un d'autre. Laisse-moi tranquille maintenant !





15:00



Rencontre-moi

Trouvez l'amour près de chez vous



Mlle Brugnion

Je ne te crois pas quand tu me dis que tu ne la vois plus. Prouve le moi !
Donne moi ton mot de passe de messagerie !

Je te jure que c'est vrai ! Vérifie toi-même, voici mon mot de passe :
Azerty12345

Oh merci mon doudou ! Je te fais confiance maintenant, je vais bientôt venir te voir, cette fois c'est sûr que je vais y arriver, je dois juste avoir encore un rdv avec le médecin...



QUI A ARNAQUÉ PROFESSEUR PARME ?

Chambre

Arnaque aux
sentiments

Mlle Brugnon

Qu'est-ce que l'arnaque aux sentiments ?

Coeur brisé, portefeuille vide

Qu'est-ce que c'est ?

L'escroc crée une relation amoureuse fictive en ligne pour gagner votre confiance, puis vous soutirer de l'argent ou des informations personnelles. Les prétextes ne manquent jamais : une urgence médicale, un voyage pour venir vous voir qui échoue, un placement à ne pas rater.

Comment la reconnaître ?

La personne trouve toujours une bonne excuse pour ne jamais vous rencontrer ni faire d'appel vidéo. Elle déclare des sentiments très vite, cherche à vous éloigner de vos proches, et finit toujours par demander de l'argent ou un service important. Nouveauté : elle utilise parfois des photos, et même des vidéos ou une voix, fabriquées par intelligence artificielle pour paraître crédible. Aujourd'hui, l'IA permet même d'imiter une voix au téléphone : un proche qui vous appelle en urgence pour de l'argent n'est pas toujours celui que vous croyez.

Le bon réflexe

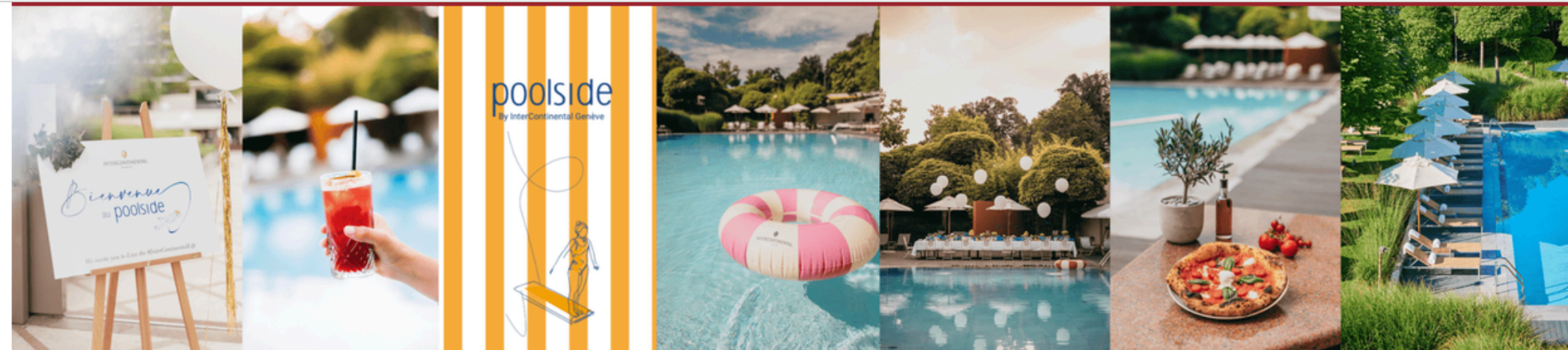
N'envoyez jamais d'argent à une personne que vous n'avez jamais rencontrée en vrai. Exigez un appel vidéo, et parlez-en à un proche : le regard extérieur est souvent la meilleure protection.

CAS N°4 : MLLE BRUGNON



Mademoiselle Brugnon nie les faits, pourtant ce sont bien ses photos qui ont été envoyées sur l'application de rencontre. Quelqu'un les lui a donc volées. C'est là qu'elle nous avoue s'être fait piéger, quelques jours plus tôt, par un placement financier trop beau pour être vrai. Elle nous montre comment tout a commencé.

CONFIDENTIAL



Newsletter

Podcasts

Vidéos

MONDE
ECONOMIQUE

Contact

Login

FR | EN



Décryptage

Croissance

Strategic Case

Culture Business

Interview

Parcours

Editio



**Elle investit 300 € et en gagne 4 200
en un mois : découvrez sa
méthode !**

Grâce à une [nouvelle plateforme](#) soutenue par de grands noms français, des milliers d'épargnants obtiennent des rendements exceptionnels, sans risque et sans connaissances particulières. Les places sont limitées.

- ✓ Rendement garanti
- ✓ Retrait à tout moment
- ✓ Accompagnement personnalisé



**« Rome is transforming » :
Interview exclusive avec Roberto
Gualtieri, emblématique Maire de
Rome**

Photo: Roberto Gualtieri © Roma Capitale
Entre crise économique et crise de confiance, Roberto Gualtieri...

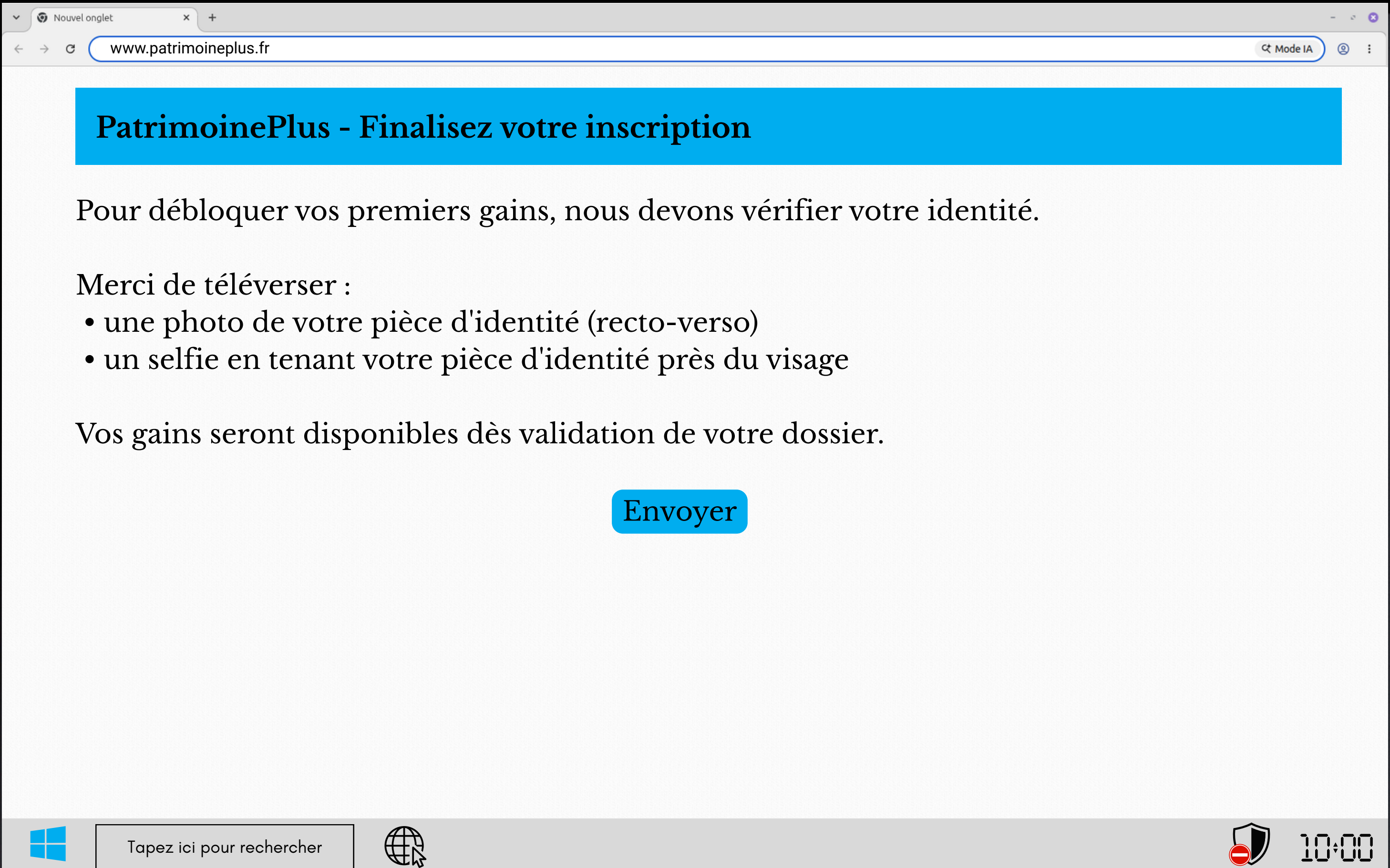


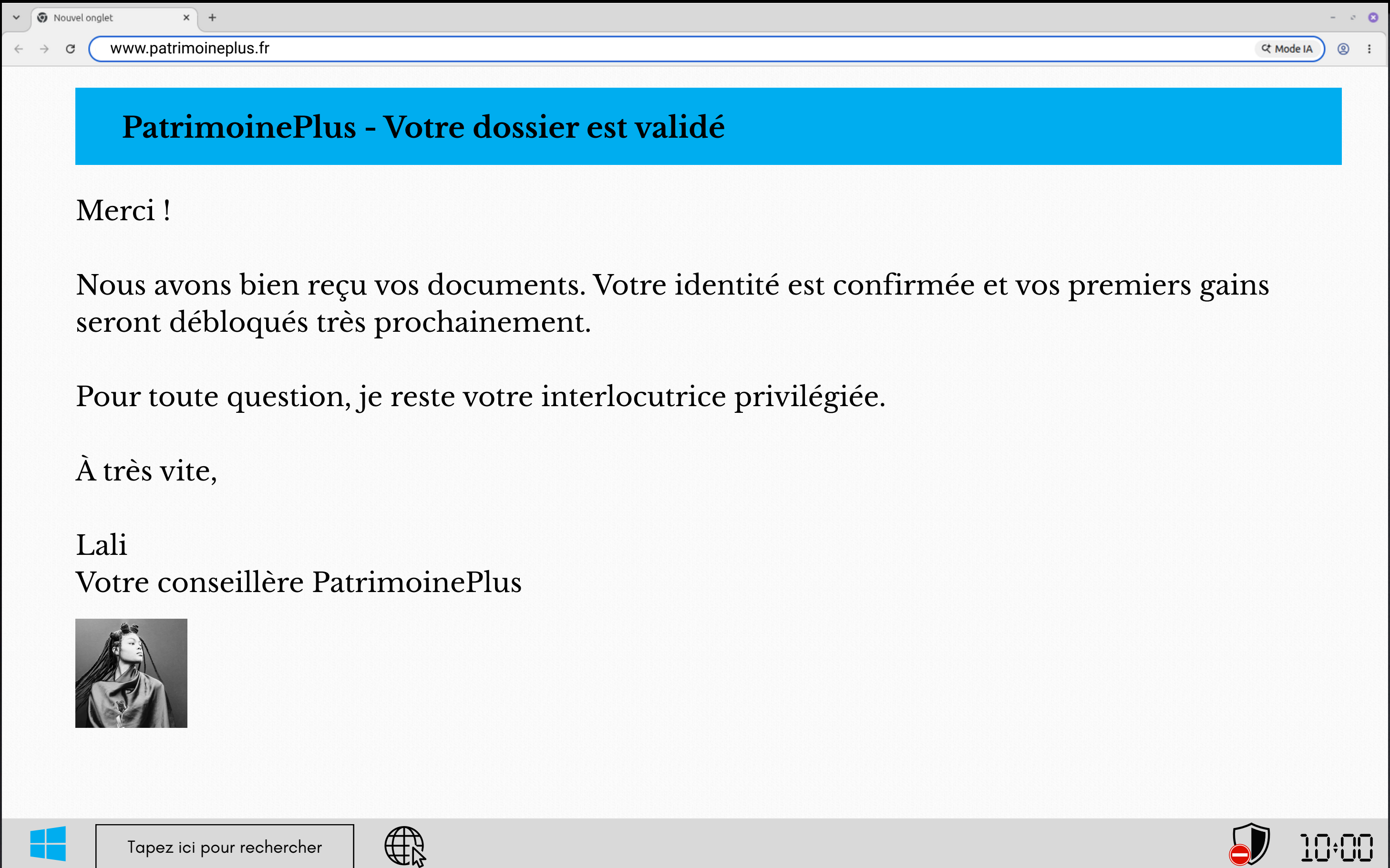
Moins de bruit, plus de sens : comment l'IA de LinkedIn révolutionne votre fil d'actualité

Par Marjorie Hayoz Pour un dirigeant, le



10:00





PatrimoinePlus - Votre dossier est validé

Merci !

Nous avons bien reçu vos documents. Votre identité est confirmée et vos premiers gains seront débloqués très prochainement.

Pour toute question, je reste votre interlocutrice privilégiée.

À très vite,

Lali

Votre conseillère PatrimoinePlus



QUI A ARNAQUÉ Mlle BRUGNON ?

Terrasse

Faux
placement/
Fausse info

Mlle Lila

Qu'est-ce que l'arnaque au faux placement ?

Si c'est trop beau pour être vrai, c'est que c'est faux !

Qu'est-ce que c'est ?

Un faux placement, c'est une arnaque qui vous promet de gagner beaucoup d'argent, vite et sans risque. Pour vous convaincre, les escrocs s'appuient souvent sur de fausses informations : une publicité qui ressemble à un vrai article de presse, une fausse déclaration d'une personnalité connue, de faux témoignages de gens enrichis. Une fois votre argent versé, ou vos papiers transmis, tout disparaît.

Comment la reconnaître ?

La promesse est trop belle : rendement « garanti », « sans risque », gains rapides. On vous met la pression avec des places limitées ou un temps compté. L'article ou la publicité imite un vrai média, mais l'adresse du site est douteuse. Et on finit par vous demander de l'argent, ou une pièce d'identité et un selfie.

Le bon réflexe

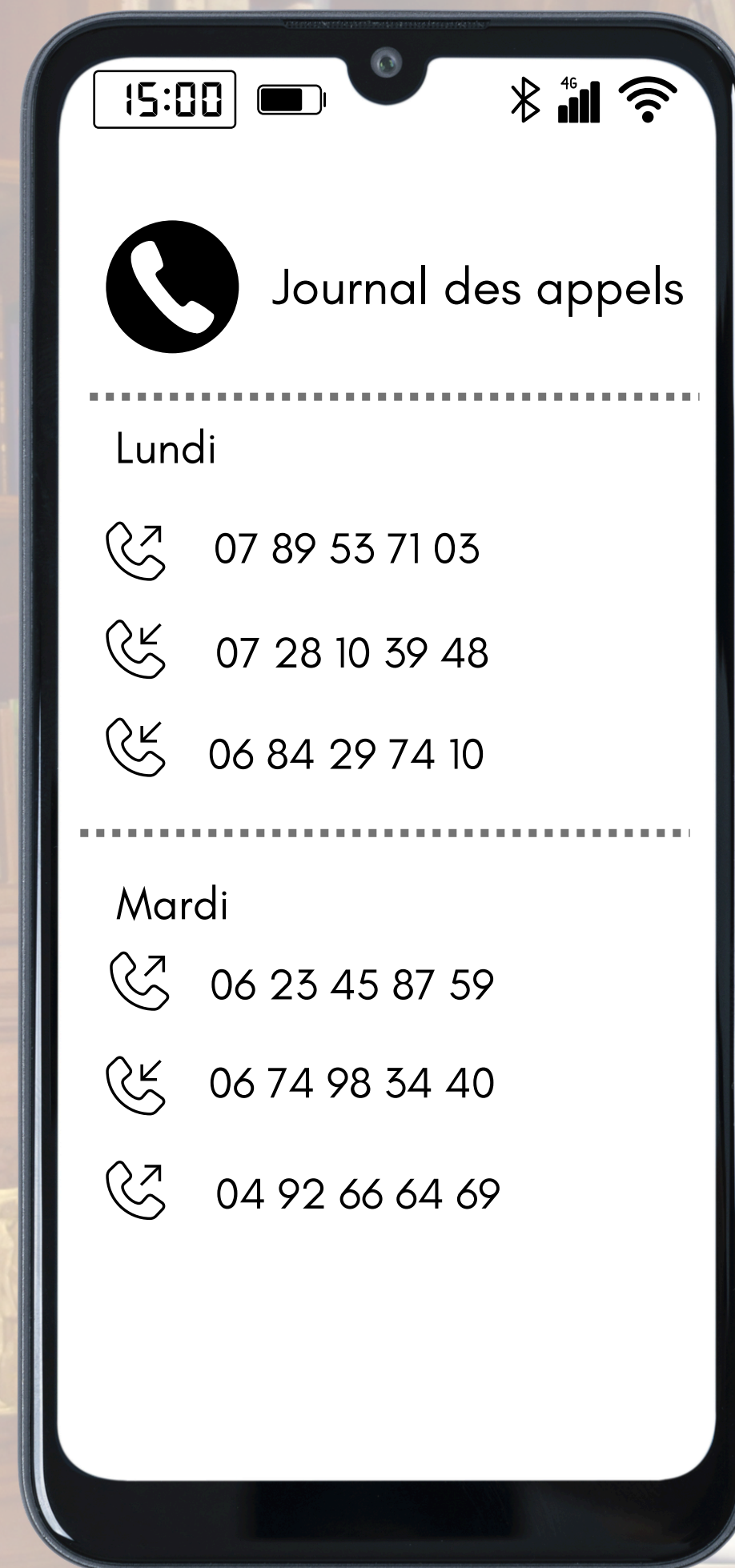
Méfiez-vous de toute promesse d'argent facile : un placement sans risque et à fort rendement, ça n'existe pas. Recoupez toujours l'information ailleurs, sur un site officiel, et ne transmettez jamais vos papiers d'identité pour débloquer des gains.

CAS N°5 : MLLE LILA



Mlle Lila a volé les photos de Mlle Brugnon parce qu'elle avait besoin d'argent. Sa banque l'a appelée le mardi précédent, sa conseillère au téléphone qui lui a expliqué qu'il y avait des virements suspects sur son compte. Mlle Lila a suivi toutes les indications de la banquière mais elle s'est rendue compte après que son compte avait entièrement été vidé !

CONFIDENTIAL



Journal des appels

Lundi

 07 89 53 71 03

 07 28 10 39 48

 06 84 29 74 10

Mardi

 06 23 45 87 59

 06 74 98 34 40

 04 92 66 64 69

QUI A ARNAQUÉ M^{lle} LILA ?

Bibliothèque

Arnaque à la
fausse
conseillère
bancaire

Mme Ivoire

Qu'est-ce que l'arnaque au faux conseiller bancaire ?

Je connais bien mon banquier...

Qu'est-ce que c'est ?

Un escroc vous appelle en se faisant passer pour votre conseiller ou pour le service anti-fraude de votre banque. Il prétend qu'une opération suspecte est en cours sur votre compte et vous met en confiance pour vous faire valider, sans le savoir, de vraies opérations frauduleuses ou pour vous soutirer vos codes.

Comment la reconnaître ?

L'appel joue sur l'urgence et la peur : « une fraude est en cours, il faut agir tout de suite ». On vous demande vos codes de validation, un virement « de sécurisation », ou d'installer une application. Nouveauté à connaître : les escrocs savent aujourd'hui faire afficher le vrai numéro et le vrai nom de votre banque sur votre téléphone. Ce n'est donc pas parce que le nom de la banque s'affiche que l'appel est vrai.

Le bon réflexe

Jamais une vraie banque ne vous demandera vos codes, ni un virement pour « sécuriser » votre compte. Au moindre doute, raccrochez, et rappelez vous-même le numéro figurant au dos de votre carte bancaire.

CAS N°6 : MADAME IVOIRE



Mme Ivoire avoue : elle a été recrutée via internet par un anonyme qui lui a expliqué comment faire. Elle n'a pas eu le choix, cette personne avait la main sur toutes ses données même les plus compromettantes.

On regarde son ordinateur.





Votre ordinateur a été verrouillé

Votre ordinateur nous a averti qu'il était infecté par un virus et un logiciel espion. Les données suivantes sont à risque:

- Identifiant Facebook, identifiants de messagerie
- Information de carte de crédit, accès bancaires
- Fichiers sur cet ordinateur



Ne redémarrez pas votre ordinateur et contactez Windows, sinon nous ne pourrions garantir la sécurité de vos données.

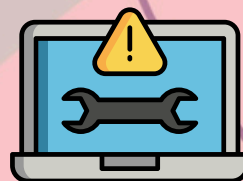


Pour plus d'informations sur ce problème et sur les solutions possibles, consultez le site <https://www.windows.com/stopcode>

Si vous contactez l'assistance, transmettez-leur ces informations:

Code d'arrêt: SPYWARE

Appelez le support technique Windows: 09 77 19 94 56
(Appel gratuit)



Connexions à votre ordinateur



IP : 91.204.78.203



Tapez ici pour rechercher



16:00

Qu'est-ce que l'arnaque au faux support technique ?

Faux informaticien, vrai arnaqueur

Qu'est-ce que c'est ?

On vous fait croire que votre ordinateur a un grave problème pour vous pousser à payer un faux dépannage ou à donner accès à votre appareil. Ça passe par une fenêtre d'alerte qui bloque l'écran, un appel, ou un mail. La même technique sert aussi de faux service après-vente : un prétendu conseiller d'un site connu vous propose un remboursement ou une réparation qui n'existent pas.

Comment la reconnaître ?

Une vraie alerte de Windows ou d'Apple ne vous donne jamais un numéro à appeler. Méfiez-vous d'un écran qui se bloque avec un message alarmant, d'une pression pour payer vite, ou d'une demande d'installer un logiciel qui donne la main à distance sur votre ordinateur à quelqu'un que vous ne connaissez pas.

Le bon réflexe

Ne rappelez jamais le numéro affiché et n'installez aucun logiciel à la demande d'un inconnu. Si l'écran est bloqué, éteignez l'appareil et rouvrez-le, ou faites-le vérifier par une personne de confiance.

Récapitulons...

Les 5 idées à retenir

●
Ne communiquez jamais vos mots de passe ni vos codes bancaires, par mail, par téléphone ou par message. Aucune banque, aucune administration ne vous les demandera.

●
Ne cliquez pas dans l'urgence. Un message qui vous presse d'agir « sous 48h » est presque toujours suspect. Rendez-vous vous-même sur le site officiel plutôt que de cliquer sur le lien reçu.

●
Un mot de passe différent pour chaque compte important, pour qu'une seule fuite ne fasse pas tomber tous les autres.

●
Une promesse trop belle cache une arnaque : un placement sans risque et à fort rendement, un grand amour qui réclame de l'argent, un gain inattendu. Recoupez toujours l'information.

●
Ce qui s'affiche peut être faux : le nom d'un expéditeur, le numéro d'un appel, une alerte sur votre écran, une pièce jointe. Dans le doute, vérifiez par un autre moyen.

Les ressources

On contacte qui ?

17Cyber — le réflexe en cas de problème : on décrit sa situation, on est orienté vers la bonne aide. *17cyber.gouv.fr*

Cybermalveillance.gouv.fr — conseils et fiches pratiques sur toutes les arnaques.

Info Escroqueries — pour être conseillé par téléphone : 0 805 805 817 (gratuit).

signal.conso.gouv.fr — pour signaler une arnaque à la consommation ou un site douteux.

Avez-vous des questions ?



Sources : Cybermalveillance.gouv.fr — définitions et fiches réflexes de l'ensemble des arnaques présentées (hameçonnage, piratage de compte, arnaque aux sentiments, faux conseiller bancaire, faux support technique).

CNIL — protection des données personnelles et fuites de données. [cnil.fr](https://www.cnil.fr)

ANSSI — Agence nationale de la sécurité des systèmes d'information. [cyber.gouv.fr](https://www.cyber.gouv.fr)