FRAUDE EN LIGNE LE GUIDE ANTI-ARNAQUES

À l'affût de données confidentielles et d'argent, les escrocs exploitent souvent la naïveté, le bon cœur ou l'appât du gain pour tromper les internautes. Voici nos pistes pour détecter les fraudes, ou s'en défendre quand le mal est fait.

Déjà affaibli par un problème de santé, Christian a paniqué lorsque l'écran de son ordinateur s'est mis à clignoter, en affichant un inquiétant message signé Microsoft. « *L'accès à ce PC a été bloqué pour des raisons de sécurité. Contactez l'assistance Windows à ce numéro.* » Devant son ordi paralysé, Christian appelle et apprend que des achats suspects ont été effectués en ligne avec sa carte bancaire et qu'il est possible de les annuler. « *Ils étaient soi-disant en liaison avec ma banque. En fait, c'étaient eux qui créaient les opérations, et je les ai confirmées en leur donnant mes coordonnées bancaires,* nous confie-t-il. *Je me suis fait avoir de 750 euros, que la banque n'a pas remboursés car j'avais validé le débit.* »

Microsoft n'est pour rien dans cette arnaque rondement menée. Comme des milliers d'autres internautes, Christian a été victime d'une variante du *phishing* (hameçonnage en français), une technique utilisée par les escrocs pour soutirer de l'argent ou des informations en usurpant l'identité d'une entreprise, d'un service public ou d'une banque. Mise en confiance par un message comportant un en-tête ou un logo familier, la victime est incitée à communiquer son numéro de carte bancaire ou de sécurité sociale en urgence, sous divers prétextes. Ces derniers mois ont vu l'explosion des arnaques.

Un Français sur deux

Ces affaires-là tournent bien. D'après une étude de la Fédération bancaire française menée avec Harris Interactive*, 51 % des Français ont déjà été confrontés à une tentative d'arnaque aux données bancaires et 7 % déclarent avoir été réellement escroqués. Le montant exact de la fraude est difficile à chiffrer, de nombreuses victimes ne portant pas plainte. Mais pour l'année 2021, l'Observatoire de la sécurité des moyens de paiement de la Banque de France l'évalue à 1,2 milliard d'euros, dont 465 millions pour les chèques, 464 millions pour les cartes bancaires et 287 millions pour les virements.

La bonne nouvelle, c'est que la lutte contre les escroqueries se renforce. Mise en place en 2021, l'obligation de l'authentification forte – la confirmation d'un paiement par un code reçu par SMS – s'est traduite par une baisse de 1,9 % de la fraude en ligne. La France s'est aussi dotée de nouveaux services d'assistance aux victimes, coordonnés par Cybermalveillance.gouv.fr. Mais bien sûr, rien ne remplace l'adoption de bonnes pratiques, que nous rappelons dans ce dossier. ● **Patrick Bertholet**

* « *Perceptions et comportements des Français en matière de cybersécurité* », étude réalisée en ligne du 14 au 15 septembre auprès d'un échantillon représentatif de 1 014 personnes âgées de 18 ans et plus.

LES BONS CONSEILS POUR ÉVITER DE SE FAIRE PIÉGER

01.
CRÉEZ DES MOTS DE PASSE SOLIDES

Un mot de passe doit être long **– de huit à douze chiffres, lettres et signes –** et changé régulièrement. Utilisez la double authentification, qui valide le mot de passe par un code envoyé par SMS. Un gestionnaire de mots de passe est utile pour éviter les trous de mémoire.

02.
METTEZ À JOUR VOTRE SYSTÈME D'EXPLOITATION ET VOS LOGICIELS

Tous les systèmes comportent des failles de sécurité. Il est donc **fortement conseillé d'installer les mises à jour dès qu'elles sont disponibles,** sous Windows, mais aussi sous macOS, Linux, Android ou iOS. On procédera de même pour les principaux logiciels.

03.
INSTALLEZ UN ANTIVIRUS

Sur PC, le module Defender intégré à Windows 11 assure une protection convenable, mais il n'est pas aussi complet que **les suites payantes qui intègrent des fonctions avancées de sécurisation des transactions ou de détection du phishing**. Rappelons que les virus touchent également les Mac.

04.
AVANT L'ACHAT, LISEZ BIEN LES PETITES LIGNES

Avant de sortir la carte bancaire sur internet, **vérifiez les conditions générales de l'enseigne** et les avis des clients pour éviter les fraudes. Autant que possible, privilégiez les boutiques situées en Europe.

05.
SAUVEGARDEZ VOS DONNÉES HORS LIGNE

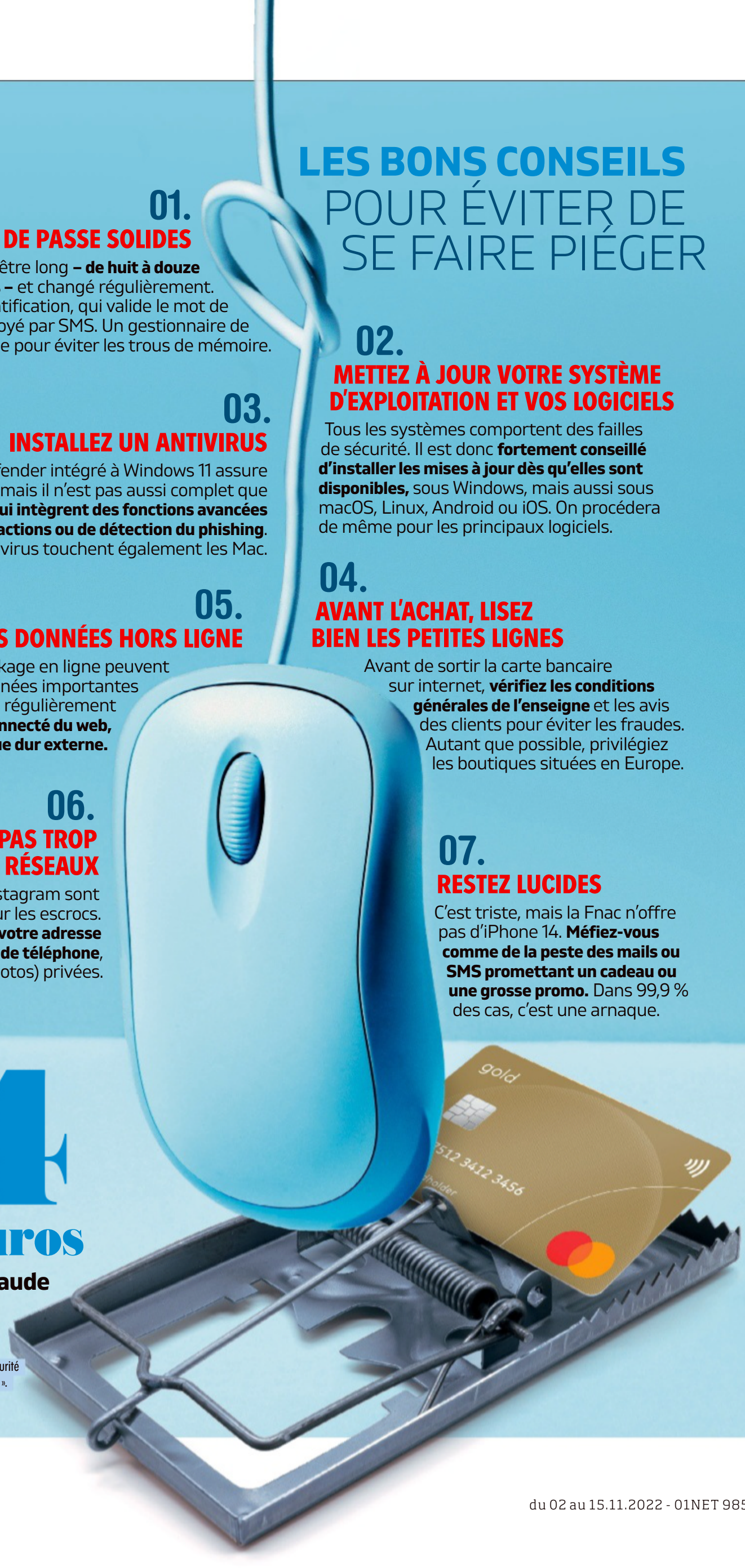
Les services de stockage en ligne peuvent être attaqués. Les données importantes doivent être copiées régulièrement **sur un support déconnecté du web, comme un disque dur externe.**

06.
N'EN DÎTES PAS TROP SUR LES RÉSEAUX

LinkedIn, Facebook ou Instagram sont de vraies mines d'or pour les escrocs. **Ne laissez pas apparaître votre adresse mail ou votre numéro de téléphone**, ni d'informations (ou de photos) privées.

07.
RESTEZ LUCIDES

C'est triste, mais la Fnac n'offre pas d'iPhone 14. **Méfiez-vous comme de la peste des mails ou SMS promettant un cadeau ou une grosse promo.** Dans 99,9 % des cas, c'est une arnaque.



464 millions d'euros

c'est le montant de **la fraude à la carte bancaire** pour l'année 2021.

Source : Banque de France, « Observatoire de la sécurité des moyens de paiement – Rapport annuel 2021 ».

MARTIN BARRAUD.PANUPONG PIEWKLENG/ISTOCKPHOTO

LES 7 FAMILLES D'ESCROQUERIE ET COMMENT S'EN SORTIR

Les particuliers sont surtout visés par le hameçonnage, des ruses incitant les internautes à révéler leurs données confidentielles. Mais il existe d'autres techniques d'extorsion encore plus redoutables.

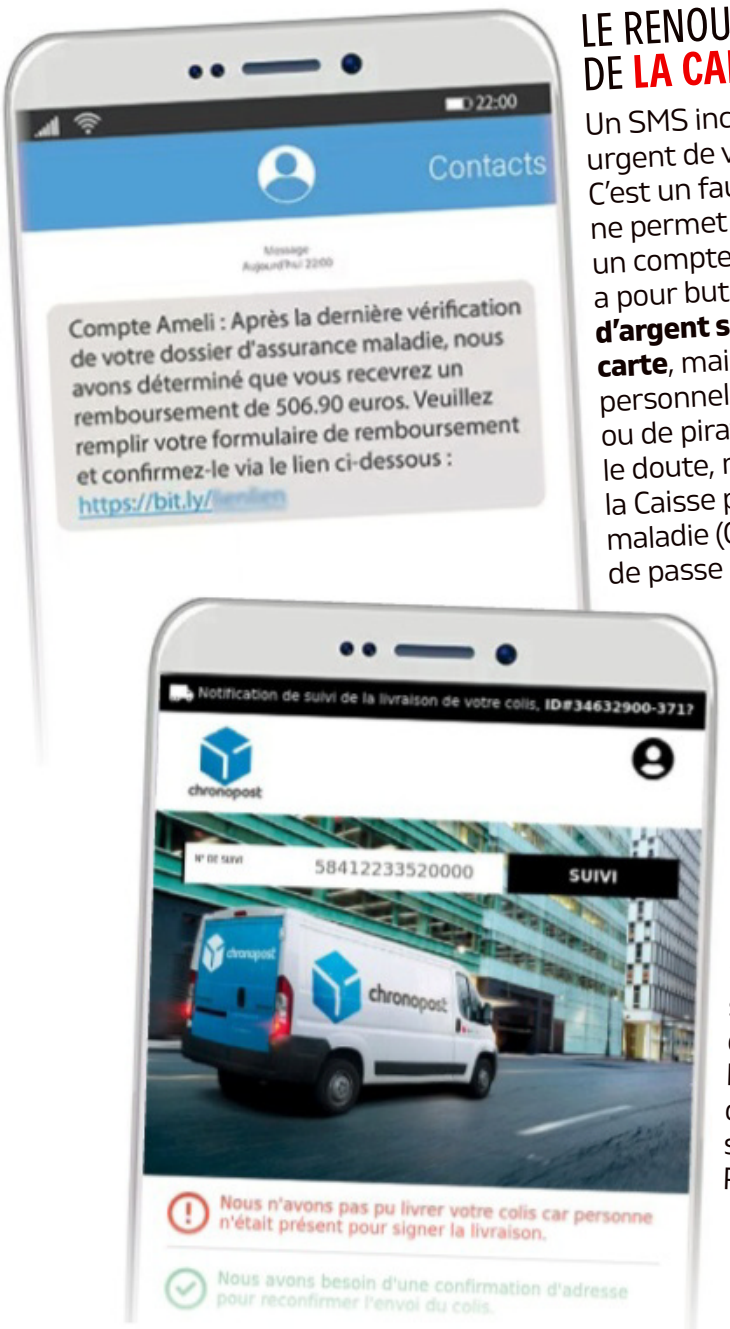
1 LE HAMEÇONNAGE ET SES VARIANTES

Grâce à des techniques bien rodées, des escrocs volent les internautes avec leur aide.

Le hameçonnage *(phishing)* représente la forme d'arnaque la plus courante sur internet. En 2021, elle représentait près de 80 % des recherches sur la plateforme Cybermalveillance.gouv.fr. Cette technique consiste à usurper l'identité d'une banque, d'un service public ou même de la police pour obtenir des informations confidentielles ou de l'argent. La ruse peut aussi avoir pour but d'infecter l'ordinateur par un virus logé dans une pièce jointe, ou de valider un paiement en ligne par un code à saisir sur un smartphone. Ces arnaques exploitent les failles des utilisateurs plutôt que celles de leur équipement, ce qui les rend assez simples à mettre en œuvre et très rentables.

JE SUIS VICTIME, QUE FAIRE ?

Si vous avez communiqué vos codes de carte, contactez immédiatement votre banque pour tenter de faire annuler les paiements effectués, puis portez plainte. Changez enfin les mots de passe d'accès aux différents services concernés (impôts, banque, assurance maladie…).



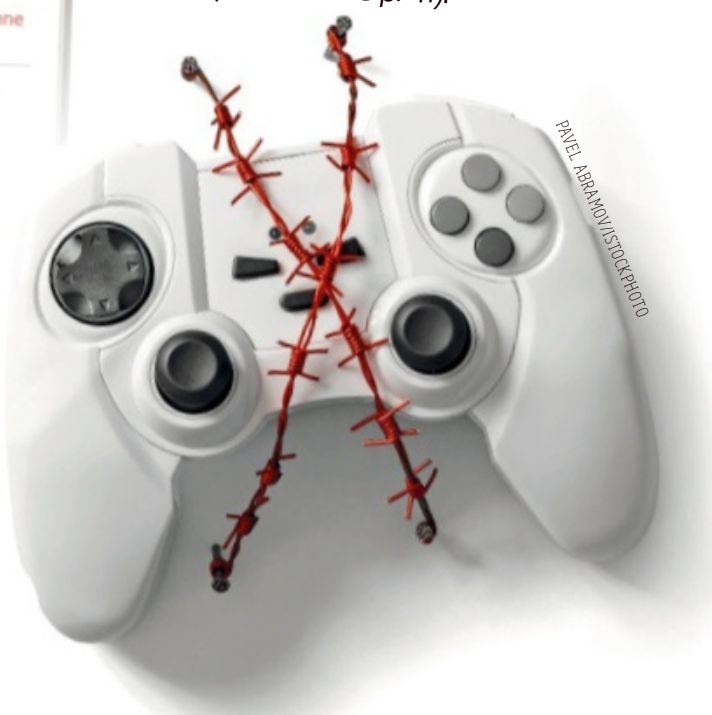
LE RENOUVELLEMENT DE LA CARTE VITALE

Un SMS incite au renouvellement urgent de votre carte Vitale ? C'est un faux, l'Assurance Maladie ne permet l'opération que depuis un compte Ameli. Cette arnaque a pour but de **récupérer un peu d'argent sur la fausse nouvelle carte**, mais surtout les données personnelles, afin de les revendre ou de pirater le compte. Dans le doute, mieux vaut contacter la Caisse primaire d'assurance maladie (CPAM) et changer le mot de passe de votre compte Ameli.

GRAPHITE/ISTOCKPHOTO

LE FAUX COLIS EN ATTENTE DE LIVRAISON

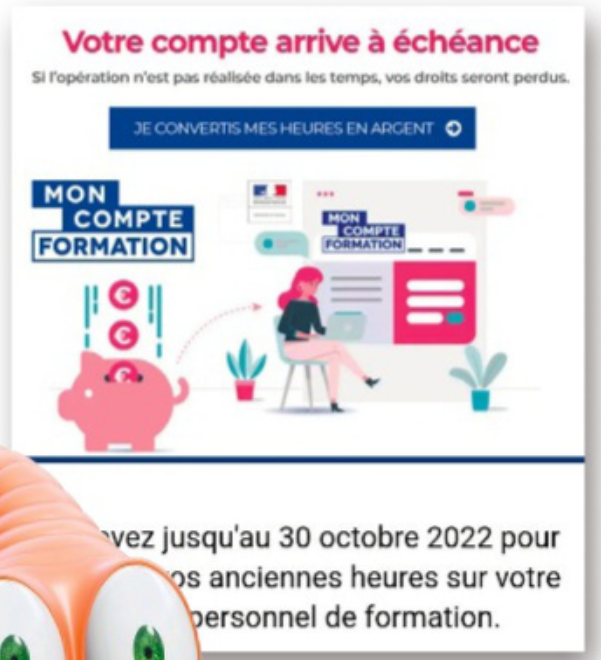
Un SMS ou un mail indique qu'un colis n'a pu être livré. Pour le recevoir, **il faut payer des frais d'expédition ou communiquer ses coordonnées bancaires**. Il ne faut ni payer ni cliquer sur le lien souvent intégré au message, qui peut installer un virus sur le téléphone. Trop tard ? Faîtes opposition, portez plainte et signalez l'arnaque sur la plateforme Perceval *(lire encadré p. 41)*.



PAVEL ABRAMOV/ISTOCKPHOTO

LE GROS LOT QUI PEUT COÛTER CHER

Félicitations, vous avez remporté une grosse somme au jeu Euromillions, un iPhone 14 flambant neuf à la Fnac… ou pas. Ce type de SMS ou de mail vise à vous **extorquer toutes vos coordonnées,** votre numéro de téléphone portable et parfois une copie de votre pièce d'identité. Plus le paiement d'une petite somme pour « *frais de dossier* ». Poubelle.

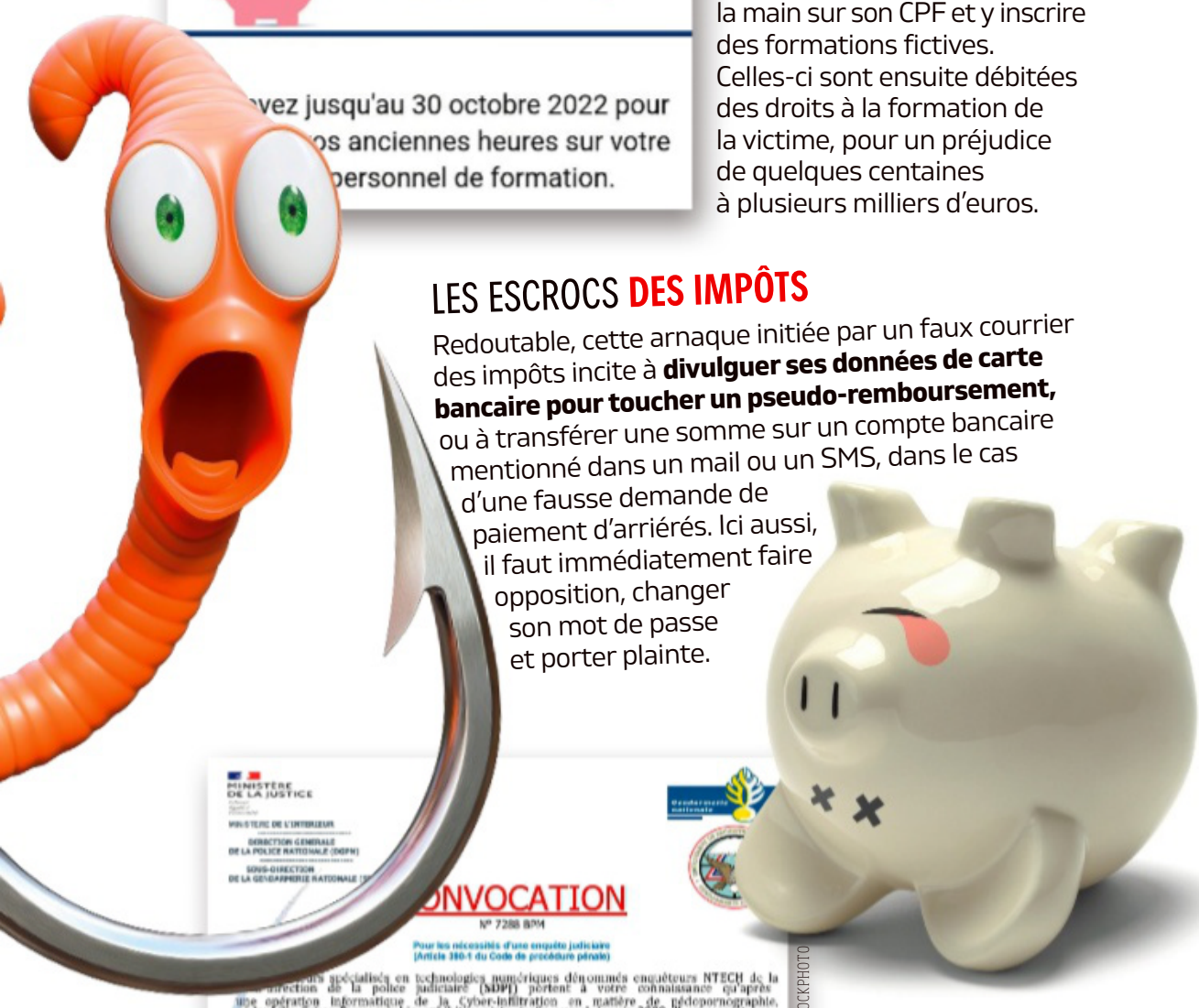


LES RAPPELS AU COMPTE PERSONNEL DE FORMATION

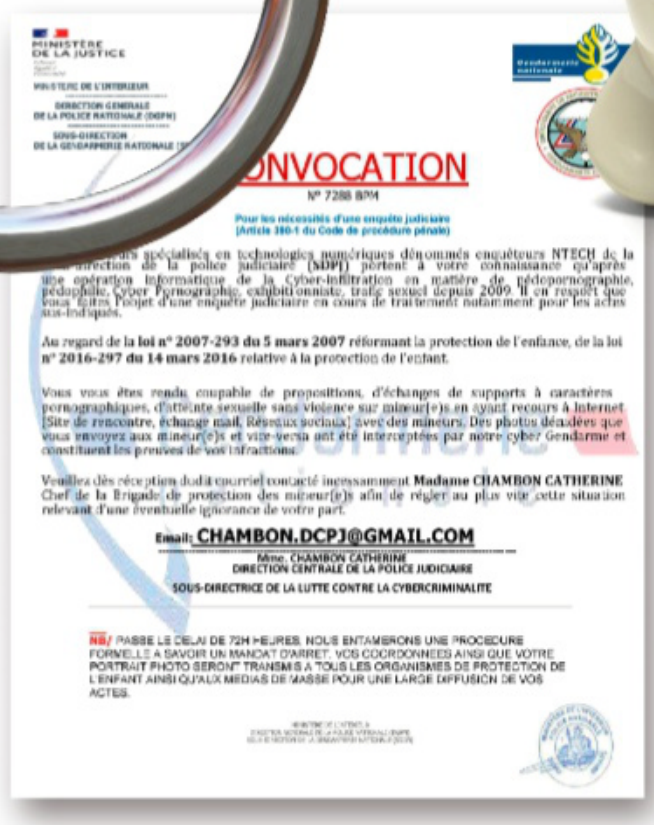
Menée au téléphone ou par SMS, l'arnaque consiste à **soutirer les codes d'accès et le numéro de sécurité sociale** d'une personne pour prendre la main sur son CPF et y inscrire des formations fictives. Celles-ci sont ensuite débitées des droits à la formation de la victime, pour un préjudice de quelques centaines à plusieurs milliers d'euros.

LES ESCROCS DES IMPÔTS

Redoutable, cette arnaque initiée par un faux courrier des impôts incite à **divulguer ses données de carte bancaire pour toucher un pseudo-remboursement,** ou à transférer une somme sur un compte bancaire mentionné dans un mail ou un SMS, dans le cas d'une fausse demande de paiement d'arriérés. Ici aussi, il faut immédiatement faire opposition, changer son mot de passe et porter plainte.



MICHAEL BURRELL/ISTOCKPHOTO



L'ACCUSATION DE PÉDOPORNOGRAPHIE

Un courrier électronique à en-tête de la police ou de la gendarmerie vous menace de poursuites et de dénonciation publique pour avoir consulté des contenus pédophiles. **L'objectif est d'obtenir de l'argent en échange de l'annulation des poursuites**. Ceux qui tombent dans le panneau doivent conserver les preuves (capture, détails du paiement) et porter plainte.

ADAM SMIGIELSKI/ISTOCKPHOTO

LES PIÈGES DE L'E-COMMERCE

Produit non conforme, absence de livraison, fausse boutique… Les achats en ligne peuvent réserver des surprises.

Ou plutôt de bien mauvaises surprises. Quelques méthodes simples permettent néanmoins de réduire les risques, à commencer par la vérification de l'identité du vendeur et sa localisation. Mieux vaut privilégier les sites situés en Europe pour simplifier les éventuels recours. Dans tous les cas, il faut bien parcourir les avis de clients et les conditions générales de vente et s'assurer qu'un contact est disponible en cas de pépin. Les adresses non sécurisées pour le paiement en ligne (sans le « s » de « https:// ») ou ne gérant pas la double authentification sont à bannir.

JE SUIS VICTIME, QUE FAIRE ?

Les pratiques frauduleuses sur internet peuvent être déclarées à la Direction générale de la répression des fraudes (DGCCRF) et signalées sur la plateforme Pharos du ministère de l'Intérieur. Pour un litige de livraison ou de facturation, il faut d'abord tenter de joindre le marchant en ligne. En cas d'échec, il est conseillé de se rapprocher d'une association de consommateurs avant de porter plainte.

POLICE, GENDARMERIE, THÉSÉE…

OÙ ET QUAND PORTER PLAINTE ?

En France, le dépôt de plainte pour une escroquerie peut s'effectuer dans tout commissariat de police ou gendarmerie de son choix, ou par écrit auprès du procureur de la République. Depuis mars 2021, la plainte peut également être déposée en ligne, sur la plateforme officielle Thésée, opérée par le ministère de l'Intérieur. Ce site *(lire p. 41)* reçoit les signalements de certains délits, comme le piratage de messagerie, le chantage et les rançongiciels, les fraudes liées aux petites annonces et à la vente en ligne. Les fraudes spécifiques à la carte bancaire, elles, doivent toujours faire l'objet d'une plainte en commissariat ou en gendarmerie. Dans tous les cas, il faut réunir un maximum de preuves de l'infraction (captures d'écran, mails, SMS, relevés de compte…) et agir le plus rapidement possible.

CAGKANSAYINISTOCKPHOTO

3 LA FRAUDE À LA CARTE BANCAIRE

Bonne nouvelle, le risque de se faire pirater sa carte en ligne est en baisse.

Vive l'authentification forte ! Entrée en vigueur en 2021, la deuxième directive européenne sur les services de paiement (DSP2) impose que les transactions par carte bancaire soient soumises à un code envoyé par SMS ou à un contrôle biométrique, en plus des habituels numéros inscrits sur celle-ci. Le système n'est toutefois pas infaillible, car non applicable pour les paiements de moins de 30 euros. La double authentification peut aussi être contournée par le hameçonnage.
Il faut donc rester prudent et éplucher régulièrement ses comptes bancaires pour repérer les anomalies.

JE SUIS VICTIME, QUE FAIRE ?
En cas de transaction suspecte, il faut immédiatement prendre contact avec sa banque pour annuler les paiements, ce qui est en principe possible tant que vous n'avez pas communiqué les paramètres du compte au fraudeur. Il est aussi conseillé de signaler la fraude sur le service Perceval *(lire p. 41)* du ministère de l'Intérieur, puis de porter plainte.

4 LA SEXTORSION, LE CHANTAGE AUX PHOTOS ET VIDÉOS PRIVÉES

Attention aux images échangées avec des inconnus.

Extorsion, cyberharcèlement, suicide d'adolescents… Les conséquences du chantage aux photos ou vidéos privées peuvent être dramatiques. Tout commence souvent sur les réseaux sociaux et les sites de rencontre, par d'innocents messages échangés avec un(e) séduisant(e) internaute en quête de l'âme sœur. La confiance s'installant, la victime est incitée à envoyer des vidéos ou des photos suggestives. L'escroc referme alors son piège en menaçant de diffuser ces images, sauf à payer une rançon. Celle-ci sera bien souvent renouvelée, pour des montants de plus en plus importants.

JE SUIS VICTIME, QUE FAIRE ?
Dès qu'une personne est victime de chantage, il faut conserver les preuves et déposer plainte, même s'il n'y a pas encore eu d'argent versé. Dans le cas d'enfants de moins de 18 ans, les enregistrements peuvent être qualifiés de pédopornographie, ce qui aggrave les sanctions pour les escrocs.

ILYA RUMYANTSEV/ISTOCKPHOTO

5 LE CHANTAGE À LA WEBCAM

Le piratage bidon qui fonctionne.

L'arnaque à la webcam fonctionne au bluff. L'attaque se matérialise sous la forme d'un mail prétendant que des images enregistrées par la webcam vont être diffusées. Afin d'effrayer la victime, le courrier est parfois envoyé de sa propre boîte mail. Pour éviter la honte, il faut payer une rançon, souvent en bitcoins. Il s'agit d'une extorsion, un délit passible de sept ans de prison et de 100000 euros d'amende. Dans la plupart des cas, l'escroc n'a rien, le détournement de webcam étant difficile à réaliser, et l'adresse mail a été déguisée.

JE SUIS VICTIME, QUE FAIRE ?
Ne jamais payer, ne jamais répondre. Si vous avez craqué, il faut porter plainte immédiatement avec les preuves de l'infraction (captures d'écran, messages…) et tenter d'annuler le paiement. Si votre propre adresse mail a réellement été utilisée, vérifiez vos comptes et changez les mots de passe.

COMMENT SE PROTÉGER DES ARNAQUES PAR TÉLÉPHONE ?

Les escrocs du web ciblent massivement les smartphones, utilisés par de nombreux Français pour leurs achats en ligne et la gestion de leurs réseaux sociaux.

Gare aux courriers indésirables et surtout aux faux SMS, souvent très bien imités, qui annoncent l'arrivée d'un (faux) colis ou incitent au (faux) remplacement de la carte Vitale. Lus trop vite sur un petit écran, ces messages peuvent facilement être pris pour des infos légitimes.
Les SMS suspects, mais aussi les appels indésirables, peuvent être signalés sur une plateforme officielle, en les renvoyant au numéro 33700. Pour se protéger, mieux vaut disposer d'un smartphone récent, équipé des dernières mises à jour. Dans leur dernière mouture, le système Android de Google et l'appli Gmail repèrent assez bien les SMS et mails indésirables. Pour une protection optimale, il peut néanmoins être sage d'installer un bon antivirus sur le smartphone. La plupart des suites pour PC (Avast, BitDefender, Kaspersky…) prennent en charge le système Android. En revanche, ils ne sont pas exploitables sur les iPhone d'Apple.

HEMUL75/ISTOCKPHOTO

6 LE FAUX SUPPORT TECHNIQUE

Quand l'ordi se fige, ne pas paniquer.

Comme pour Christian, l'arnaque au dépannage informatique démarre souvent avec le blocage de l'ordinateur lors d'une navigation sur internet. Il ne s'agit pas d'un virus, mais d'un simple script malveillant logé sur certaines pages web. Un message à l'écran, encadré par des logos de Microsoft, Apple ou Google, invite à appeler un numéro d'urgence pour dépanner la machine – qui fonctionne en réalité toujours très bien. Au téléphone, un « opérateur » propose alors diverses solutions, comme l'installation d'un antivirus à un prix exorbitant ou la prise de contrôle à distance de la machine pour la réparer. L'escroc peut alors piller les données et récupérer les mots de passe enregistrés sur le navigateur. L'utilisateur peut aussi être incité à valider des achats en ligne présentés comme suspects, au lieu de les annuler.

JE SUIS VICTIME, QUE FAIRE ?

Coupez la connexion internet pour redémarrer la machine ou forcez la fermeture dans le gestionnaire des tâches (Control+Alt+Suppr sous Windows). Lancez un scan antivirus, désinstallez l'éventuel logiciel de prise de contrôle à distance et changez tous vos mots de passe. Enfin, contactez votre banque.

TALAJ/ISTOCKPHOTO

7 LE PIRATAGE DE MESSAGERIE

Gare aux mots de passe trop faciles à deviner.

Vos amis reçoivent des mails de votre part que vous n'avez jamais envoyés ? Vous ne parvenez plus à vous connecter à Facebook ou Instagram ? Ces symptômes sont typiques d'un piratage de compte. Il peut avoir des conséquences catastrophiques quand la messagerie contient de nombreuses informations confidentielles. Précisons toutefois qu'il est facile de modifier une partie de l'adresse d'expédition d'un mail. La supercherie se détecte en examinant son en-tête.

JE SUIS VICTIME, QUE FAIRE ?

Tentez de modifier votre mot de passe. Si l'accès au compte est impossible, contactez le service concerné pour signaler le piratage et demandez la réinitialisation du code. Si les coordonnées bancaires étaient enregistrées sur le compte compromis, prévenez immédiatement la banque pour faire opposition aux transferts suspects.

MARTHE LEMELLE

Les banques remboursent la fraude

TROIS QUESTIONS À MAYA ATIG

DIRECTRICE GÉNÉRALE DE LA FÉDÉRATION BANCAIRE FRANÇAISE

Quelle est la procédure à suivre, pour un particulier, lorsqu'il constate un prélèvement suspect sur son compte ?

Le premier réflexe en cas de mouvement suspect doit être de faire opposition à votre carte *(en appelant immédiatement votre banque ou le serveur interbancaire d'opposition au 0 892 705 705, NDLR)*. Il convient ensuite de prendre contact avec son conseiller, qui déterminera les circonstances et orientera sur les formalités à suivre.

Peut-on obtenir la restitution des sommes détournées à la suite d'une arnaque sur le Net ?

La banque rembourse le client lorsque celui-ci n'a pas fait preuve de négligence grave. Il est par exemple victime d'un vol et voit ses comptes débités sans avoir initié d'opération. Si vos codes d'accès ont été utilisés et si un paiement a pu être réalisé, la banque appréciera au cas par cas s'il y a eu négligence grave ou agissement intentionnel. Dans ces hypothèses, la banque pourra refuser le remboursement.

Quels sont les recours possibles ?

Il faut d'abord voir avec son banquier ce qu'il est possible de faire. Il est par ailleurs recommandé de porter plainte auprès de la police ou de la gendarmerie. Enfin, en cas de désaccord avec sa banque, le médiateur bancaire peut être saisi. Il faut savoir que les banques remboursent la fraude. Selon l'Observatoire de la sécurité des moyens de paiement, qui dépend de la Banque de France, plus de 85 % des clients qui adressent une demande en cas de paiements par carte contestés sont remboursés.

LES SITES OFFICIELS POUR OBTENIR DE L'AIDE

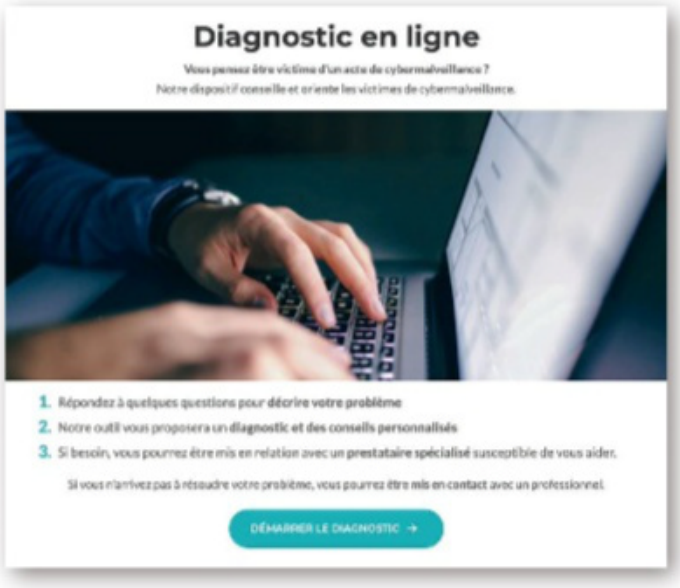
Sous la férule du gouvernement, plusieurs plateformes proposent de l'information et de l'assistance contre les cybermenaces. Phishing, piratage de compte, sextorsion… toutes les formes d'arnaques sont expliquées et prises en charge.

CYBERMALVEILLANCE.GOUV.FR

Le centre d'accueil et d'assistance contre les menaces

Depuis 2017, cette plateforme constitue le point d'accueil pour toutes les victimes d'actes de malveillance sur internet. Il s'agit d'un dispositif national de sensibilisation, de prévention et d'assistance accessible aux particuliers, aux entreprises et aux collectivités locales. La structure Cybermalveillance.gouv.fr a été créée, sous l'égide du gouvernement français, par un groupement d'intérêt économique qui rassemble aujourd'hui une cinquantaine de membres publics (Agence nationale de la sécurité des systèmes d'information, La Poste, Caisse des dépôts, etc.) ou privés (Google, Microsoft, Kaspersky, etc.). L'objectif est de cumuler les ressources et l'expertise de ces acteurs pour lutter contre les cybermenaces, mais aussi de détecter les nouvelles attaques grâce aux signalements effectués.

UN AUTODIAGNOSTIC. « *Nous échangeons des informations avec les services d'ordre et le ministère de l'Intérieur lorsque nous constatons un pic d'affluence,* explique Jean-Jacques Latour, l'un des responsables de la plateforme. *L'année dernière, notre article sur les infractions pédopornographiques, en tête de toutes les visites, a été consulté 450 000 fois.* » Pour ce type d'arnaque, et toutes les autres, le site Cybermalveillance propose des fiches d'informations et des conseils précis pour détecter les pièges et donner des moyens de s'en défendre. En quelques questions, le site réalise un diagnostic de l'attaque et aiguille l'internaute vers les autres plateformes officielles comme Service Public.fr, Perceval, Pharos ou Thésée. Le site propose aussi des supports pédagogiques comme le « Cyber Guide Famille ». Ce mémo destiné aux parents et aux ados a été lancé à l'occasion du Cybermois, la campagne de sensibilisation à la cybersécurité qui a lieu chaque année en octobre. Au menu, la création de bons mots de passe, la sauvegarde de données et de bons conseils pour éviter ou contrer les margoulins du web. ●



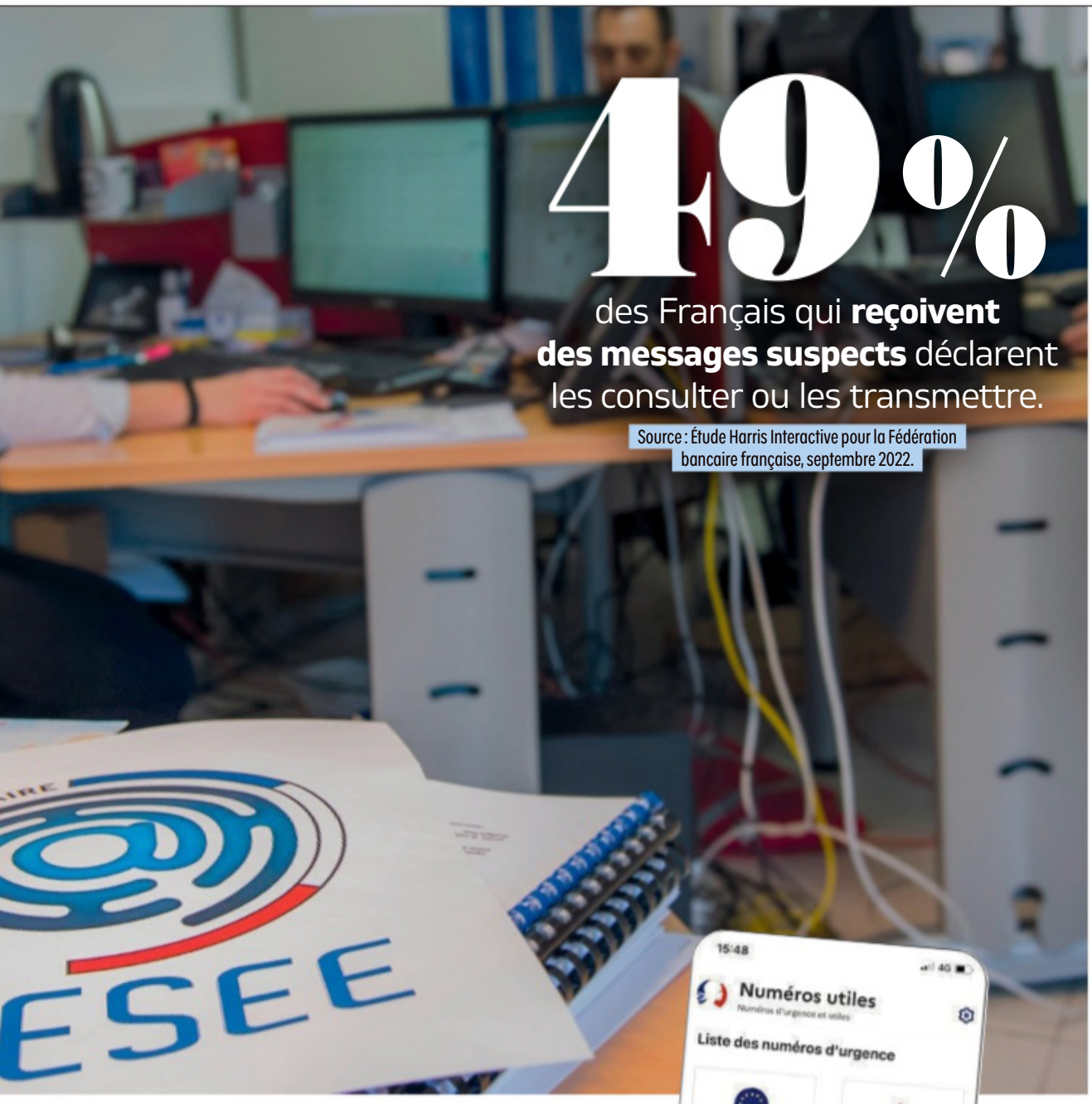
MI/DICOM/PIERRE CHABAUD

17 POLICIERS ET GENDARMES sont affectés à Thésée via l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication.

SERVICE-PUBLIC.FR

LE SITE OFFICIEL DE L'ADMINISTRATION

Créé en 2000 et refondé à plusieurs reprises, Service-public.fr est le site officiel de l'Administration française, le portail d'accès pour de nombreuses informations et démarches. **C'est l'adresse web de référence pour tout connaître des droits et devoirs citoyens,** pour récupérer des formulaires officiels ou obtenir les coordonnées des services d'aide sociale ou des forces de l'ordre. S'il ne gère pas directement les affaires d'arnaque en ligne, il facilite l'accès au service adéquat, comme la plateforme Thésée pour porter plainte.



THÉSÉE

Pour porter plainte en ligne

Depuis mars 2021, les victimes d'infractions sur internet peuvent porter plainte sur la plateforme Thésée (acronyme de « traitement harmonisé des enquêtes et signalements pour les e-escroqueries »), mise en place par le ministère de l'Intérieur.

HUIT JOURS DE DÉLAI. Pour limiter l'engorgement des commissariats et gendarmeries – où le dépôt de plainte reste possible –, ce service enregistre les signalements de huit types d'arnaques : l'utilisation frauduleuse des données de carte bancaire, le piratage de compte mail, les faux sites de vente, petites annonces ou locations, le chantage en ligne, l'extorsion par logiciel et les escroqueries aux sentiments. Pour déposer plainte en ligne, il faut se rendre sur le site Service-public.fr, rubrique « Arnaque sur Internet », puis se laisser guider par l'interface. La connexion requiert un compte FranceConnect ou un identifiant à un service public (Impôts.gouv.fr, Laposte.fr, Ameli.fr…). Les dossiers sont envoyés par mail et traités par une équipe de 17 policiers et gendarmes chargés de déterminer leur recevabilité. Le délai de réponse est estimé à huit jours, pour un volume de plaintes évalué à 500 par jour.●

PHAROS

Lumière sur les pires méfaits du web

Racisme, pédophilie, atteinte aux mineurs, incitation à la haine, apologie du terrorisme… Le site Pharos (pour « plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements ») recueille les signalements des comportements les plus choquants constatés sur internet. En quelques clics, l'interface s'assure que ceux-ci figurent dans son domaine de compétence et renvoie, si ce n'est pas le cas, vers les autres services publics d'assistance comme Thésée. Le site prodigue aussi de bonnes infos sur les dangers encourus par les enfants et ados sur la Toile ainsi que pour protéger son ordinateur.●

PERCEVAL

CONTRE LA FRAUDE À LA CARTE

Elle porte un nom longuet, mais sa mission est claire, lutter contre l'arnaque à la carte bancaire. La Plateforme électronique de recueil de coordonnées bancaires et de leurs conditions d'emploi rapportées par les victimes d'achats frauduleux en ligne, ou Perceval, collecte et analyse les usages frauduleux des cartes pour des achats effectués en ligne. Ce site de la gendarmerie nationale est accessible en ligne par l'intermédiaire d'un compte du service public FranceConnect. Il signale directement la fraude aux forces de l'ordre, sans toutefois permettre le dépôt de plainte, et accélère la demande d'opposition auprès des banques. Attention, la demande ne peut être effectuée que si vous disposez de la carte et si vous n'êtes pas à l'origine de l'achat.