Presse écrite FRA

LA CROIX

Edition : **20 aout 2026 P.4-5,5**

Famille du média : **PQN (Quotidiens nationaux)**

Périodicité : **Quotidienne**

Audience : **629000**

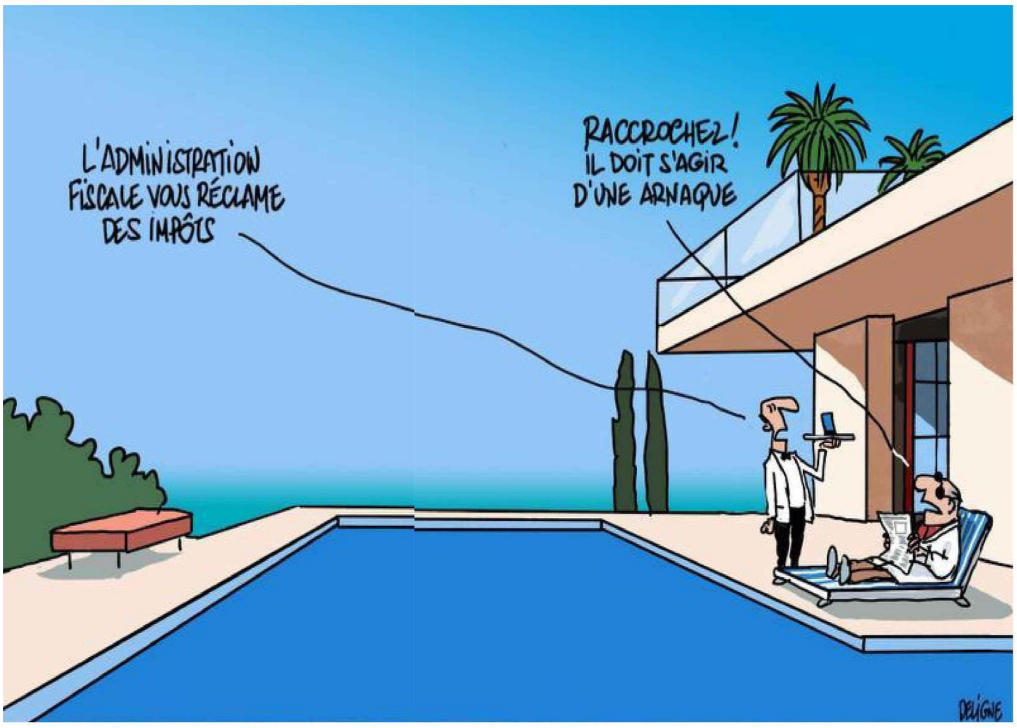
Journaliste : **Gaïa Herbelin**

Nombre de mots : **1202**

ÉVÉNEMENT

Avec les données fiscales de 350 000 particuliers dans la nature, les tentatives d'escroquerie risquent de se multiplier dans les semaines à venir. Hameçonnage, usurpation d'identité voire cambriolage ou agression : comment se protéger face à ces menaces ?

Après la fuite de données fiscales, gare aux arnaques !



350 000 particuliers et 250 000 professionnels. Au total, ce sont les données de 600 000 contribuables qui ont été consultées ou extraites du système d'information en ligne de la Direction générale des finances publiques (DGFIP), entre juin et juillet. Parmi les données volées, on retrouve l'identifiant fiscal, l'état civil, les coordonnées postales, téléphoniques et électroniques et la situation fiscale (situation de famille, nombre de personnes à charge, nombre de parts, revenu fiscal de référence, taux de prélèvement à la source). Côté entreprises, le Siren et la raison sociale sont concernés.

L'attaque a été revendiquée par un groupe de hackeurs surnommés ZeroBytes, supposément français *(lire ci-contre)*. Ils affirment avoir déjà vendu les données récupérées pour quelques milliers d'euros et soulignent la facilité avec laquelle ils se sont attaqués aux organisations françaises.

Si les informations volées ont bien été vendues, les personnes concernées par la fuite de données sont désormais exposées à un certain nombre de menaces dont il n'est pas toujours facile de se protéger. Première arnaque à laquelle il faudra faire attention dans les semaines à venir : le hameçonnage, ou *« phishing »*. Cette technique revient à envoyer un mail ou un SMS à la victime, dans lequel on introduit un lien sur lequel on peut cliquer. Le but, pour le pirate, est de conduire sa proie à renseigner de nouvelles informations dont il pourra se servir par la suite pour établir des arnaques crédibles et pousser la cible à lui virer des sommes d'argent, à la manière des faux conseillers bancaires.

Première arnaque à laquelle il faudra faire attention dans les semaines à venir : le hameçonnage, ou « phishing », une technique qui revient à envoyer à la victime un lien sur lequel on peut cliquer.

Ce type d'escroquerie reste assez simple à détecter dans de nombreux cas. Mais plus le message d'origine est crédible, plus il devient complexe à identifier et donc dangereux : *« Ces arnaques deviennent très ciblées parce que les pirates disposent de véritables informations. En particulier en pleine période de correction des avis d'imposition, cette fuite de données peut donner lieu à de grosses phases de phishing crédibles »*, anticipe Me Djamel Belhaouci, spécialiste de la cybercriminalité.

Attention aux messages qui poussent à cliquer sur un lien inconnu donc, mais aussi aux correspondances hors numérique : *« Un courrier papier peut être aussi frauduleux qu'un email,* avertit Adrien Manniez, expert en cybersécurité. *Vous pouvez recevoir une lettre qui semble provenir des impôts, indiquant que vous avez un trop perçu de quelques centaines d'euros. Mais pour récupérer l'argent, on vous demande de flasher un QR code sur lequel vous devrez entrer vos informations personnelles. »* Une méthode innovante mais qui aboutit au même résultat : la récupération de données personnelles toujours plus fines convoitées par les pirates.

Pour se protéger de ce type d'arnaque, il suffit d'appliquer rigoureusement quelques règles simples : *« Ne cliquez sur rien et n'ouvrez aucun lien envoyé par mail ou par SMS, même s'il paraît sérieux. Si vous recevez un mail de la part des impôts, plutôt que de cliquer sur le lien, rendez-vous plutôt sur impots.gouv.fr et consultez votre messagerie pour voir si on vous a effectivement contacté »*, recommande Adrien Manniez. Un conseil qu'il faut

Sébastien Lecornu demande une « nouvelle unité cyber »

Le premier ministre a demandé mercredi à l'Agence nationale de la sécurité des systèmes d'information (Anssi) de constituer une *« nouvelle unité cyber »* pour offrir une *« réponse opérationnelle plus réactive »* aux cyberattaques qui visent la France. *« Il y a urgence à concevoir et conduire sans délai une réponse opérationnelle plus réactive et plus forte aux cyberattaques que l'État rencontre actuellement. Il faut reprendre l'initiative sur le terrain »*, écrit Sébastien Lecornu, reconnaissant et déplorant qu'en termes de cybersécurité, *« peu de ministères* (soient) *au niveau requis »* en France.

particulièrement suivre lorsque le message en question paraît *« trop beau pour être vrai »* ou s'il vous place *« dans une situation d'urgence »*, le but étant de focaliser l'attention de la victime sur le fond du message pour dissimuler la fraude. De son côté la DGFIP rappelle qu'elle ne *« demande jamais d'informations confidentielles par courriel, SMS ou téléphone »* et qu'il ne faut pas communiquer ses *« codes, identifiants, mots de passe ou coordonnées bancaires en réponse à une sollicitation »*.

Plus graves que les campagnes de phishing, les experts du secteur cyber anticipent de nouvelles usurpations d'identité : *« Si les pirates détiennent vos coordonnées bancaires et d'imposition, il devient facile d'ouvrir un crédit en ligne ou un compte*

bancaire à votre nom », s'inquiète Adrien Manniez. Une crainte partagée par Me Belhaouci : *« Il faut disposer de tous les éléments, mais si la pièce d'identité de la victime a également fuité, des tiers peuvent contracter des prêts. »* Pour repérer ce type d'escroquerie, le plus sûr reste de consulter régulièrement ses comptes et de s'assurer qu'aucun paiement n'a été effectué par un tiers.

Pire encore que l'usurpation d'identité, certains craignent que la fuite des données fiscales, couplée à l'adresse postale, provoque des agressions physiques : *« Plusieurs affaires d'enlèvement et de séquestration ont débuté par des fuites de données dans le secteur de la cryptomonnaie,* rappelle Me Belhaouci. *Certains agresseurs ont obtenu des virements de plusieurs millions d'euros de cette manière. Ce sont des menaces qui peuvent concerner les personnes à hauts revenus dont les données ont été exposées. »* Et dans ce cas précis, à moins de déménager et donc de changer d'adresse postale, peu de mesures de protection pourront prévenir les risques.

Les entreprises pourraient, elles aussi, être soumises à de plus grands risques d'arnaques dans les semaines à venir, mais de manière détournée, notamment les arnaques « au faux président ».

Les entreprises pourraient, elles aussi, être soumises à de plus grands risques d'arnaques dans les semaines à venir, mais de manière détournée. En effet, ce n'est pas la divulgation des Siren et des raisons sociales des structures qui pose problème, mais plutôt les informations personnelles des chefs d'entreprise. Les arnaques *« au faux président »* pourraient donc se multiplier prochainement. Pour les pirates cela consiste à se faire passer pour le PDG d'une structure pour exiger des virements importants, parfois aidé par des deepfakes, c'est-à-dire des contenus multimédias créés par intelligence artificielle et qui imitent l'apparence ou la voix de personnes réelles.

La DGFIP a annoncé contacter les particuliers victimes par mail ou par courrier afin d'appeler à la vigilance des utilisateurs, une opération qui devrait s'achever en fin de semaine (un mail qui invite à consulter la messagerie cryptée consultable sur le site impôts.gouv.fr). Quant aux entreprises, l'administration devrait les joindre dès la semaine prochaine.

Cette attaque visant les données fiscales s'inscrit dans un contexte de multiplication des piratages des systèmes d'information publics. En 2025, le fisc à lui seul a dû repousser 6 972 cyberattaques.

Gaïa Herbelin