febelfin

Si ça ressemble à du phishing, c'est probablement du phishing !

SI ÇA RESSEMBLE À DU PHISHING, C'EST PROBABLEMENT DU PHISHING

La fraude en ligne reste un problème persistant. Dans le prolongement des années précédentes, les cybercriminels ont continué l'an dernier à envoyer en masse des messages de phishing dans lesquels ils se faisaient passer pour une personne ou une organisation de confiance (par ex. une banque ou une autorité publique). Heureusement, le secteur bancaire a pu détecter, bloquer ou récupérer 75 % des virements frauduleux liés au phishing. Les fraudeurs ont néanmoins réussi à s'emparer de 49 millions d'euros grâce à cette fraude.

€ 49 millions
butin en 2024

La fraude en ligne ne cesse d'évoluer - et les méthodes sont de plus en plus sournoises. Alors qu'elle reposait au départ sur un phishing via de simples courriels, nous constatons aujourd'hui un nombre croissant de cas où les fraudeurs réussissent à convaincre leurs victimes d'effectuer elles-mêmes l'opération de transfert d'argent. Cela débute souvent par un appel téléphonique qui parait plausible, un site web d'apparence professionnelle ou une demande urgente via une application de confiance comme itsme®. D'emblée, vous avez l'impression de parler à votre banque ou à une autorité publique, ou de recevoir une proposition d'investissement formidable.

Fraude à l'investissement, fraude au faux support technique bancaire et demandes trompeuses via des applications numériques, etc. : les formes d'escroquerie sont de plus en plus sophistiquées. Et même si bien des efforts ont déjà été déployés pour mettre les clients en garde, la prise de conscience reste faible dans une grande partie de la population. Comme au cours des dernières années, il apparaît que de nombreux Belges demeurent insuffisamment armés contre ces formes modernes d'escroquerie.

Heureusement, de plus en plus de personnes sont sur leurs gardes aussitôt qu'elles soupçonnent une escroquerie : elles s'empressent alors de contacter leur banque ou de vérifier le solde et les transactions sur leur compte. Dans le même temps, la population est de mieux en mieux informée à propos du phishing et des passeurs d'argent, les mules financières. Le nombre de personnes qui communiquent leur code PIN ou envoient leur carte bancaire à une adresse donnée continue également de diminuer.

Ces constats soulignent l'importance d'une sensibilisation constante. En effet, tout le monde peut devenir la cible d'une fraude en ligne. Les jeunes sont particulièrement vulnérables, en partie à cause de leur attitude souvent nonchalante à l'égard de la sécurité en ligne.

C'est pourquoi le secteur s'investit pleinement dans des initiatives innovantes et des collaborations solides pour lutter efficacement contre la fraude en ligne. En joignant nos forces à celles de partenaires de différents horizons - des sociétés technologiques aux institutions financières en passant par les pouvoirs publics et l'enseignement - nous bâtissons un rempart solide contre la cybercriminalité. Au travers de campagnes ciblées, d'outils intelligents et d'une sensibilisation permanente, nous entendons non seulement répondre à la fraude, mais aussi la prévenir encore plus souvent. Car ce n'est qu'ensemble que nous pourrons renforcer la sécurité numérique de chacun.

Découvrez tous les détails dans notre dossier qui présente les tout derniers chiffres et une vue d'ensemble de certaines des nouvelles initiatives du secteur.

LES FRAUDEURS CONTINUENT DE RAFLER UN SOLIDE BUTIN

Ils débarquent avec un message aux apparences innocentes. Une notification de votre banque, un avertissement de la police, une mise à jour de votre mutuelle ou de votre compagnie des eaux. Tout semble habituel - jusqu'à ce que vous y regardiez à deux fois. Car derrière ces noms familiers comme Mutualité chrétienne, Inami, SWDE ou Police fédérale, se cache souvent un escroc qui a un plan.

Le phishing est aujourd'hui devenu l'une des formes les plus courantes de fraude en ligne. Safeonweb, le point de contact du Centre pour la Cybersécurité Belgique, reçoit chaque jour presque 26 000 signalements de messages suspects.

Cela représente donc près de 9,5 millions de signalements par an, un chiffre hallucinant qui souligne la profondeur de l'enracinement de cette forme de fraude.

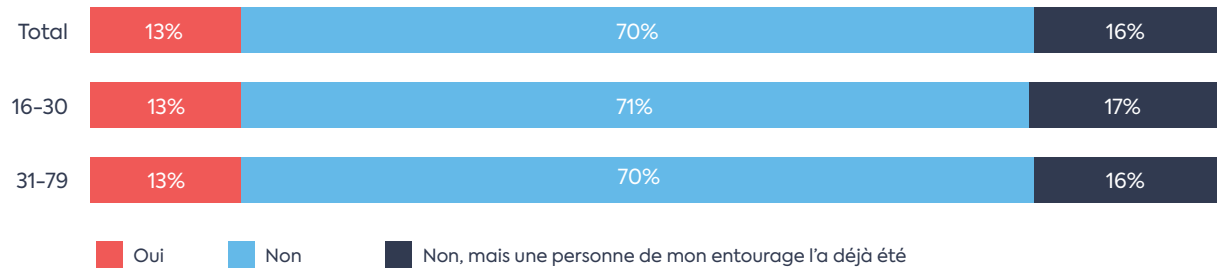
Et même si les banques parviennent à détecter, bloquer ou récupérer 75 % des virements frauduleux, le phishing reste une pratique lucrative. Rien qu'en 2024, quelque 49 millions d'euros ont été détournés par ce biais. Cela montre combien ces attaques sont devenues convaincantes et combien il est essentiel de demeurer vigilant.

Une étude réalisée par Febelfin en collaboration avec le bureau d'études Indiville confirme l'ampleur de cette forme de fraude.

Un danger actuel

L'enquête révèle que 13 % des Belges ont déjà été victimes de phishing à un moment ou à un autre de leur vie.

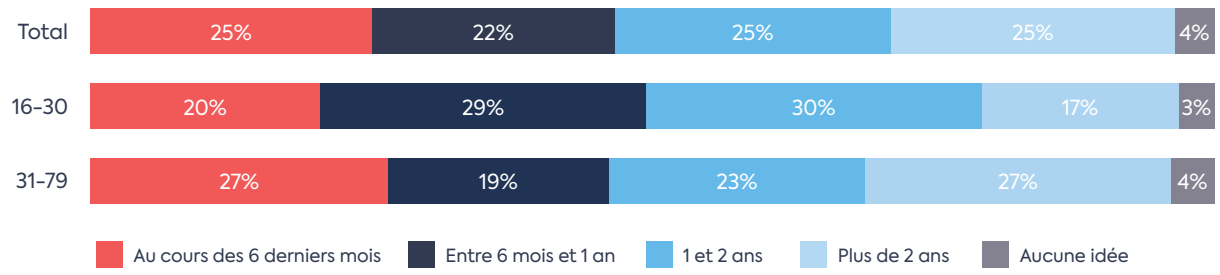
Avez-vous déjà été victime de phishing ?



Source: Indiville

Si l'on considère la date à laquelle les personnes interrogées ont été victimes de phishing, il est clair que le problème reste pleinement d'actualité.

C'était il y a combien de temps ?



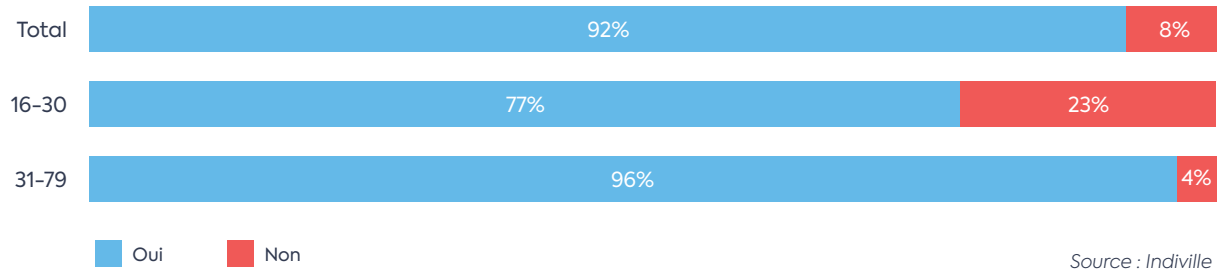
Source : Indiville

[1] Source : Safeonweb juillet 2025
[2] Enquête IndiVille, 20 janvier - 9 février 2025, sur un échantillon représentatif de la population belge n : 2149 sondés NL/FR, âge 16-79. Marge d'erreur maximale : 2,1%

Connaissance de cette forme de fraude

Même si de nombreuses personnes sont conscientes du danger, il convient d'encore améliorer la connaissance du phishing. Saviez-vous que 8 % de la population belge n'a jamais entendu parler de cette forme de fraude ? Chez les jeunes de 16 à 30 ans, ce pourcentage est encore plus élevé : 23 % ne savent pas de quoi il s'agit. Les personnes plus âgées, en revanche, sont généralement mieux informées : 4 % d'entre elles seulement n'ont jamais entendu parler de phishing. Cela suggère que les initiatives de sensibilisation destinées aux personnes âgées en collaboration avec des partenaires locaux, telles que nos sessions d'information sur la sécurité des services bancaires et des paiements en ligne (voir p. 12), portent leurs fruits.

Avez-vous déjà entendu parler du phishing ?



Source : Indiville

Des pièges importants, surtout pour les jeunes

Partager des codes bancaires et communiquer des données financières

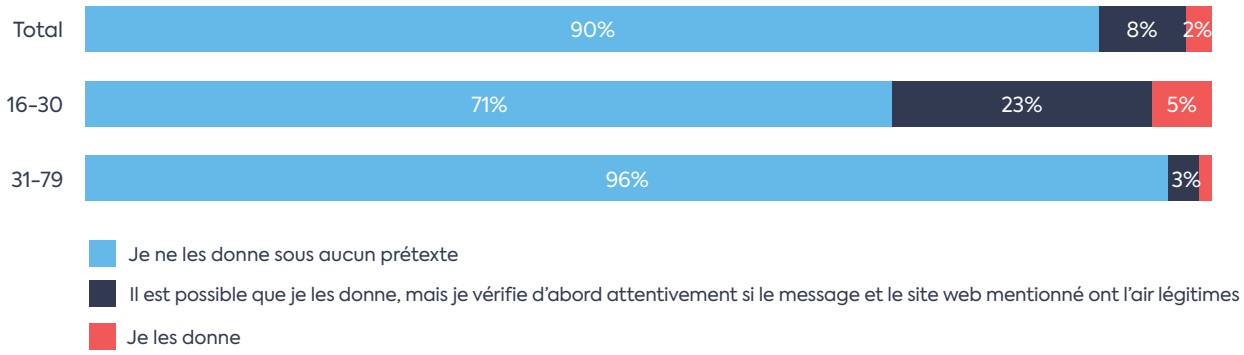
La plupart des Belges le savent désormais : il ne faut jamais transmettre ses codes bancaires. Quel que soit leur âge, 9 personnes interrogées sur 10 déclarent qu'elles ne communiqueraient en aucun cas leur code. Mais une petite minorité - 2 % - le ferait sans hésiter.

Cependant, si l'on considère en particulier les jeunes, le tableau est moins rose. Ainsi, 23 % d'entre eux indiquent qu'ils communiqueraient éventuellement leurs codes bancaires si on le leur demandait par e-mail, SMS ou tout autre moyen numérique - après avoir soigneusement examiné le message et le site web vers lequel il renvoie. Et 5 % des jeunes transmettraient même leurs codes sans aucune vérification.

Mais il y a aussi de bonnes nouvelles. En effet, alors qu'en 2022, 13 % des jeunes avouaient être prêts à communiquer sans souci leur code bancaire, ils ne sont plus que 5 % aujourd'hui.

Une nette amélioration qui montre que la sensibilisation fonctionne - même si ce pourcentage est toujours beaucoup trop élevé et que la vigilance reste de mise.

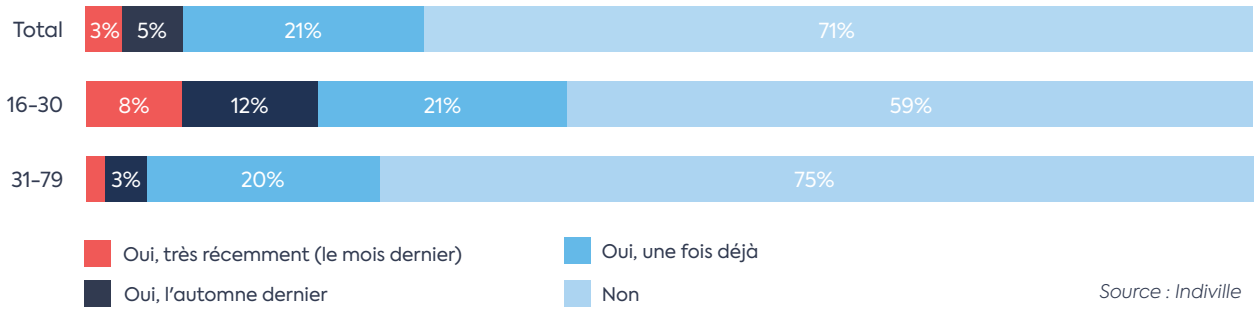
Si votre banque vous demande vos codes bancaires par e-mail, SMS, WhatsApp, téléphone...



Source : Indiville

En outre, l'enquête révèle que d'une manière générale, les jeunes sont plus nombreux à partager des informations financières qu'ils regrettent par la suite d'avoir mises en ligne. Ainsi, 8 % de l'ensemble des répondants ont déclaré avoir été dans ce cas au cours des derniers mois, alors que ce pourcentage est nettement plus élevé chez les jeunes : 20 %.

Avez-vous déjà transmis en ligne des données financières qui vous mettent mal à l'aise par la suite ?



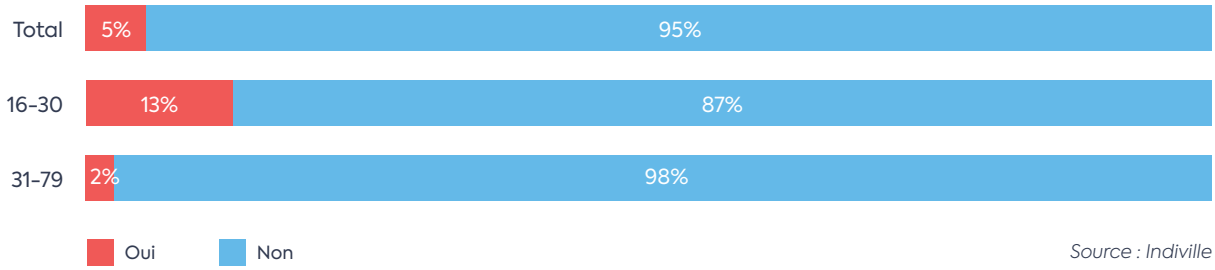
Source : Indiville

Renvoyer une carte bancaire

Imaginez : vous recevez un appel ou un message de votre « banque ». Votre carte bancaire est sur le point d'expirer. Pour éviter tout souci lors du passage d'une carte à l'autre, on vous recommande de renvoyer votre ancienne carte et le code PIN correspondant sans perdre de temps. Pour la plupart des Belges, la réponse est claire : c'est non, bien sûr. L'enquête montre ainsi que 95 % des personnes interrogées ne renverraient jamais leur carte bancaire, même sur demande insistante de « la banque ».

Mais chez les jeunes, la réaction est différente : ils sont 13 % à indiquer qu'ils seraient enclins à renvoyer leur carte. Ce chiffre est alarmant, d'autant qu'il ne traduit aucune amélioration par rapport à l'année précédente. Il souligne en revanche à quel point il est important d'informer les jeunes et de leur faire prendre conscience des risques. En effet, les escrocs sont de plus en plus malins et profitent de la moindre inexpérience de leurs victimes.

Renverriez-vous votre carte bancaire si votre banque vous le demandait par e-mail, SMS, WhatsApp, téléphone, courrier ?



Source : Indiville

QUE FAIRE SI VOUS ÊTES TOMBÉ DANS LE PIÈGE DU PHISHING ?

Savoir quelles dispositions prendre

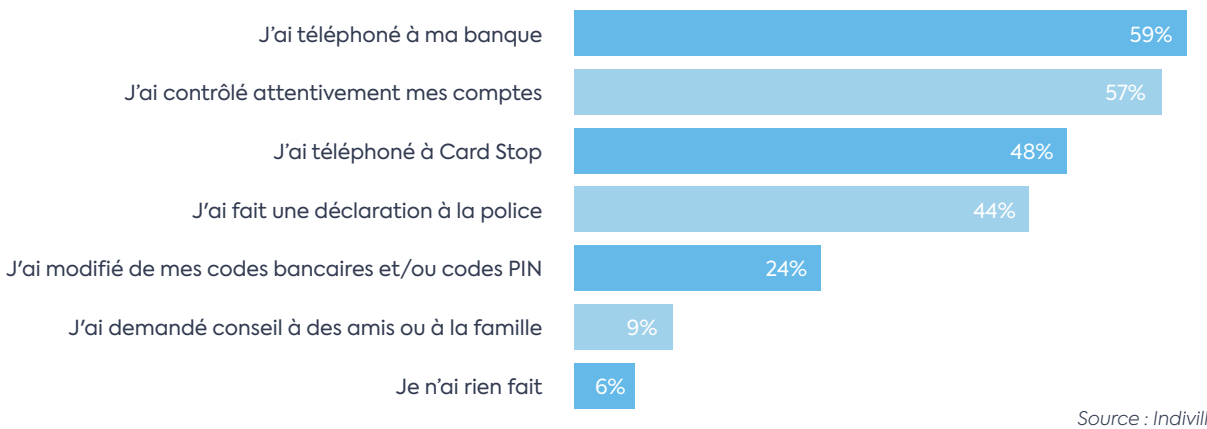
C'est une question que personne n'aime se poser, mais à laquelle il est préférable de savoir répondre. Car malgré toutes les campagnes d'avertissement et les conseils de prévention, cela peut toujours arriver : un clic malencontreux, un moment d'inattention, et vous voilà victime.

Heureusement, nous constatons que les gens sont de plus en plus nombreux à savoir comment réagir en cas de problème. L'enquête montre que 64 % des victimes savaient d'emblée quelles dispositions prendre ou à quel endroit chercher de l'aide. 6 % des victimes ne savaient pas elles-mêmes quelles démarches entreprendre, mais des proches ont heureusement pu leur donner de bons conseils.

Il nous reste cependant du travail, en particulier auprès des jeunes. Dans la tranche d'âge des 16-30 ans, pas moins de 39 % ont déclaré ne pas savoir quoi faire après une tentative de phishing réussie. À titre de comparaison, ce chiffre est de 27 % chez les personnes âgées de 31 à 79 ans. Cela montre qu'il est au moins aussi important de savoir quoi faire après un cas de phishing que de le prévenir.

En effet, ceux qui savent quoi faire peuvent agir rapidement. Et la rapidité de réaction fait souvent la différence entre des pertes limitées et des dommages importants.

Parmi les étapes suivantes, lesquelles avez-vous franchies ?



Source : Indiville

Pour mieux armer les gens contre la fraude en ligne, Febelfin a élaboré un nouveau dépliant en collaboration avec la police locale et des partenaires tels que SAAMO et d'autres parties prenantes. Ce guide pratique rassemble toutes les informations essentielles en un seul endroit : que faire en cas d'arnaque, où trouver de l'aide et comment mieux se protéger. Il s'agit d'un outil pratique qui guide les gens de manière claire dans une situation souvent confuse.

TÉLÉCHARGER LE DÉPLIANT →

L'importance d'une sensibilisation permanente

Les chiffres parlent d'eux-mêmes : de plus en plus de personnes reconnaissent les signes de phishing. De nets progrès ont été réalisés en matière de sensibilisation à la fraude en ligne. Mais en même temps, il reste essentiel de continuer à renforcer les connaissances et la résilience numérique, en particulier chez les jeunes, qui évoluent souvent dans un monde en ligne où les risques ne sont pas toujours visibles.

C'est pourquoi le secteur financier s'engage pleinement dans des actions ciblées. Non seulement en apprenant aux jeunes à reconnaître et éviter le phishing, mais aussi en soutenant les victimes par des mesures claires et une aide accessible. En effet, plus vite une personne sait quoi faire, moins les dommages sont importants.

Dans cette perspective, Febelfin a lancé une **campagne** choc sur la fraude dans les jeux en ligne, un thème qui touche directement les jeunes. Elle a également initié la plateforme éducative **Banque en Classe**, sur laquelle les enseignants peuvent trouver des conférences et du matériel pédagogique sur des sujets financiers, y compris la fraude en ligne. L'objectif ? Responsabiliser les jeunes dans leurs choix numériques et leur apporter les connaissances nécessaires pour naviguer en toute sécurité dans un monde en ligne de plus en plus complexe.

banque en classe

VISIONNER LA VIDÉO →

LE PHISHING EST PEUT-ÊTRE LA FORME LA PLUS CONNUE DE FRAUDE EN LIGNE, MAIS ELLE EST LOIN D'ÊTRE LA SEULE

D'autres formes de fraude en ligne sont encore trop peu connues

Les fraudeurs en ligne ne se reposent pas sur leurs lauriers. Outre le phishing, ils recourent de plus en plus à d'autres formes de fraude en ligne pour tromper leurs victimes. Pensez à la fraude à la demande d'aide, où l'escroc se fait passer pour l'un de vos amis dans le besoin, ou à la fraude à l'investissement avec des promesses de gains rapides. La fraude au faux support bancaire et technique gagne également du terrain, tout comme les récentes tentatives commises par des fraudeurs demandant l'approbation d'actions via l'application d'identification itsme®.

Exemples de fraude via itsme® :

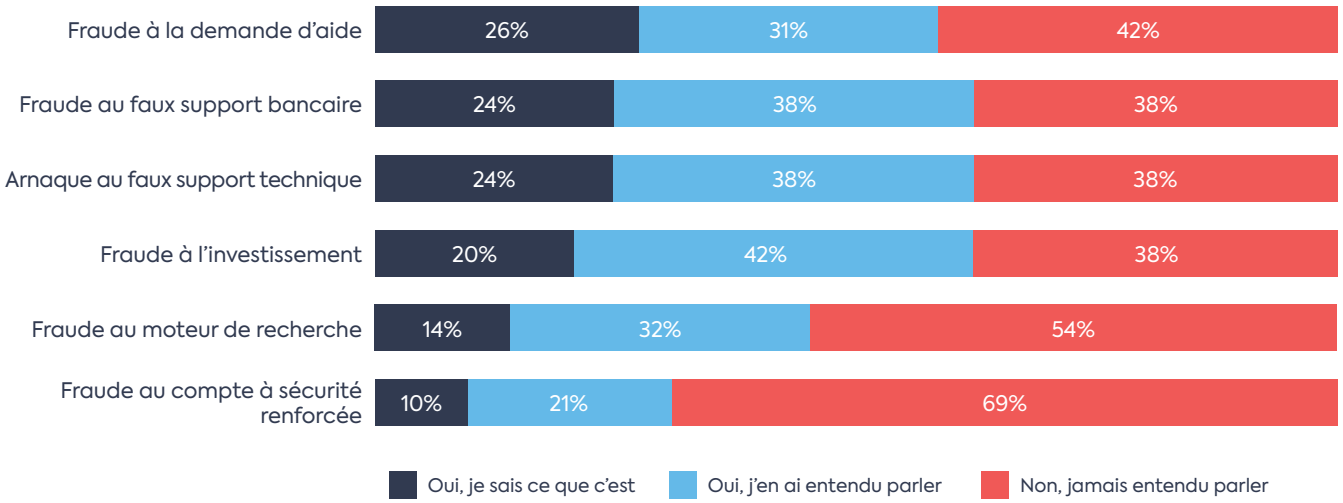
- Les victimes sont informées que des paiements suspects ont été détectés et qu'elles peuvent les annuler via itsme®. En réalité, c'est ainsi qu'elles approuvent les paiements destinés à l'escroc.
- Un faux collaborateur de banque demande à la victime de confirmer son identité via itsme®, mais ce faisant, celle-ci lui donne en réalité accès à son environnement bancaire en ligne.

DÉCOUVREZ QUELQUES CONSEILS POUR ÉVITER CETTE FRAUDE →

Une étude montre que ces formes de fraude sont encore trop peu connues du grand public. Seul un Belge sur cinq sait exactement ce qu'impliquent ces formes de fraude. Un tiers en a bien entendu parler, mais ne sait pas vraiment de quoi il retourne. Et près de la moitié sont dans l'ignorance la plus totale. Il est intéressant de noter que cette méconnaissance n'est pas liée à l'âge : jeunes ou moins jeunes, la plupart des gens ne sont pas suffisamment familiarisés avec ce phénomène.

En fait, certaines formes de fraude sont presque totalement inconnues. Par exemple, 69 % des personnes interrogées n'ont jamais entendu parler de la fraude aux comptes à sécurité renforcée et 54 % ne connaissent pas la fraude au moteur de recherche. Même en ce qui concerne la fraude à l'investissement - une forme de fraude qui fait souvent la une de l'actualité - seuls 20 % des répondants savent exactement ce qu'elle implique.

Connaissez-vous ces formes de fraude ?



Source : Indiville

Cela montre que nous avons encore pas mal de pain sur la planche. Car comment se protéger de quelque chose dont on ignore l'existence ?

Le secteur financier continue donc à communiquer sur le sujet et à développer des initiatives afin de mettre en garde contre ces types de fraude.

Conseil

Le dossier en ligne de Febelfin explique de manière simple les différents types de fraude en ligne et vous donne de précieux conseils sur la manière de vous protéger.

EN SAVOIR PLUS →

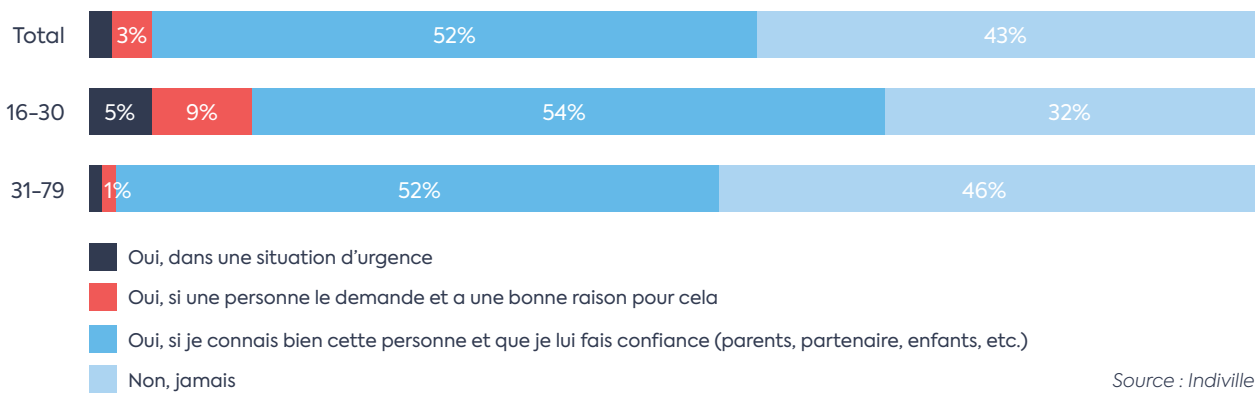
MULES FINANCIÈRES

Gagner de l'argent rapidement ? Un bon plan, non ? Un inconnu vous demande de lui prêter pour un moment votre carte bancaire ou votre compte. De l'argent vite gagné, on dirait. Mais derrière cette proposition innocente se cache souvent une réalité bien plus grave : vous devenez une mule financière - et vous devenez donc complice d'une fraude.

Les gens continuent de tomber dans le piège. Une étude montre que 14 % des jeunes sont prêts à partager leur carte bancaire et leur code PIN pour de l'argent. Ce pourcentage traduit d'ailleurs une légère augmentation par rapport à 2024. Pour l'ensemble de la population, cette part est de 5 %.

Ce qui commence par un banal « ok » imprudent peut se solder par un casier judiciaire. C'est pourquoi Febelfin met en garde inlassablement : ne vous laissez pas avoir.

Donneriez-vous votre carte bancaire et votre code PIN à une autre personne ?



Source : Indiville

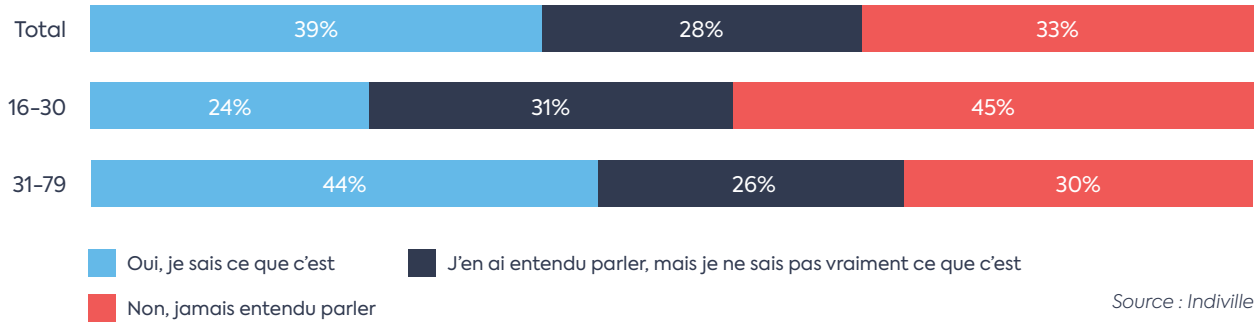
QU'EST-CE QU'UNE MULE FINANCIÈRE ?

Une mule financière est une personne qui laisse des criminels utiliser son compte bancaire et/ou sa carte bancaire et son code PIN pour blanchir de l'argent sale. Cela permet au criminel de déposer de l'argent sale sur le compte bancaire de la mule financière afin de pouvoir ensuite le retirer (à l'aide de la carte bancaire et du code PIN de la mule) ou de le transférer vers d'autres comptes. Les escrocs sont ainsi intouchables. Pour en savoir plus, consultez notre **dossier en ligne**.

Qu'est-ce qu'une mule financière ? De nombreux jeunes n'en ont aucune idée.

Si près de 40 % des Belges connaissent la signification de ce terme, ce chiffre tombe à 24 % chez les jeunes. Et pas moins de 45 % d'entre eux n'en ont même jamais entendu parler.

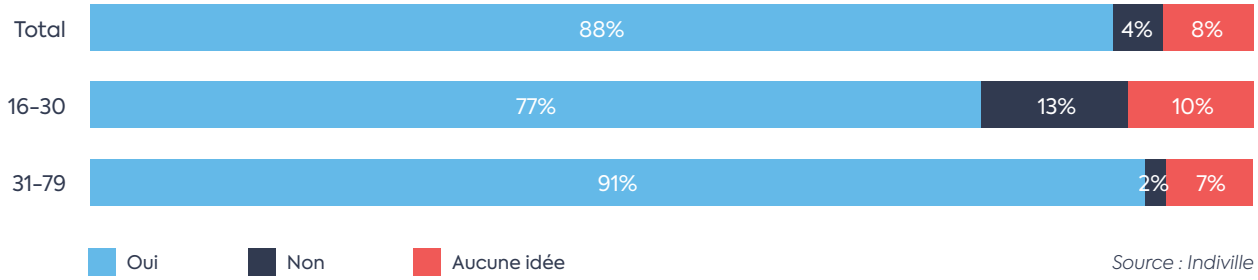
Savez-vous ce qu'est une mule financière ?



Source : Indiville

Et ce que beaucoup ne comprennent pas, c'est que toute personne qui prête son compte ou sa carte bancaire à des fins criminelles commet un délit pénal - avec des conséquences graves telles que des amendes, des peines d'emprisonnement et l'obligation de dédommager la victime.

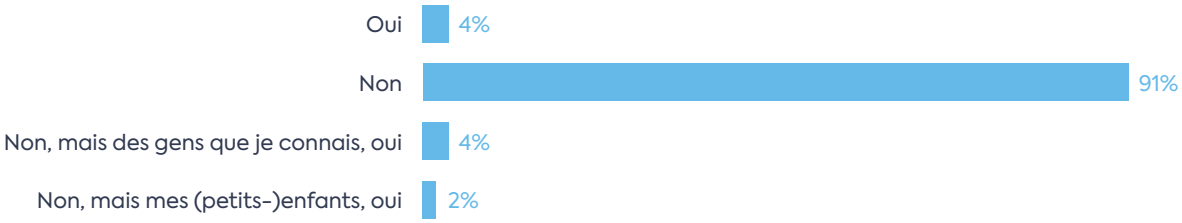
Pensez-vous que servir de mule financière constitue une infraction pénale ?



Source : Indiville

Pourtant, le phénomène reste méconnu. L'enquête montre que 4 % des Belges se sont déjà vu proposer de devenir une mule financière, et que 4 % connaissent quelqu'un qui a tenté l'expérience. Chez les jeunes, ces chiffres sont encore plus élevés : 7% ont déjà été approchés eux-mêmes, et 12% connaissent quelqu'un à qui une telle proposition a été faite.

Avez-vous déjà été approchés pour devenir une mule financière ?



Les chiffres restent stables depuis des années, ce qui est inquiétant. Les jeunes restent une cible privilégiée pour cette forme de fraude. Il est donc essentiel de continuer à les informer sur ce qu'est une mule financière et, surtout, sur les risques encourus.

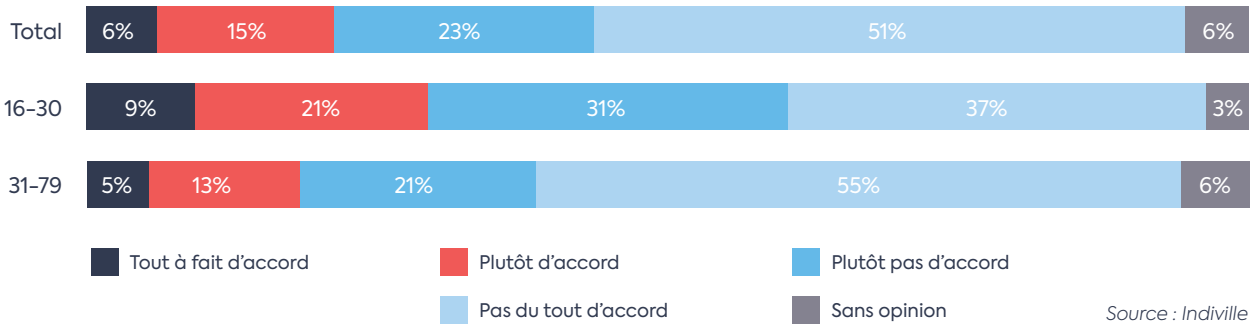
ACHATS EN LIGNE : RAPIDES, FACILES... ET SÛRS ?

Pour de nombreux Belges, les mesures de sécurité supplémentaires prises lors d'achats en ligne - comme l'introduction d'un code supplémentaire, d'une empreinte digitale ou l'utilisation d'un lecteur de carte - sont désormais considérées comme allant de soi. Ils le savent : ces quelques secondes supplémentaires les protègent de la fraude.

Pourtant, tout le monde n'est pas de cet avis. L'enquête montre qu'un Belge sur cinq considère ces étapes comme fastidieuses plutôt que comme une protection. Les jeunes, en particulier, les vivent plus souvent comme un obstacle : 30 % d'entre eux les trouvent contraignantes, contre 18 % parmi les générations plus âgées.

Et cela n'est pas sans risque. En effet, ceux qui considèrent la sécurité comme superflue sont souvent moins vigilants face aux escroqueries en ligne. Il est donc important de continuer à expliquer pourquoi ce clic ou ce code supplémentaire est nécessaire. Surtout auprès des jeunes, dont trois sur dix ne sont pas encore suffisamment conscients de l'importance des serrures numériques.

Je trouve superflu de devoir parcourir plusieurs étapes de vérification lorsque je fais des achats en ligne

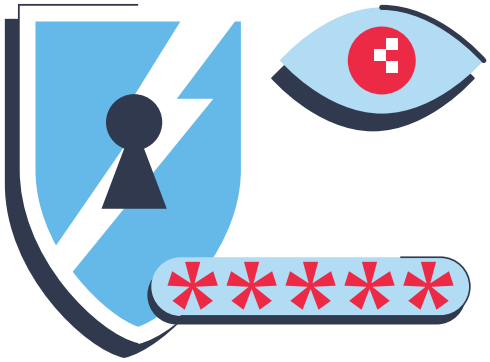


Source : Indiville

LA LUTTE CONTRE LA FRAUDE EN LIGNE NE RELÈVE PAS DE LA RESPONSABILITÉ D'UN SEUL MAIS DE TOUS

Les fraudeurs en ligne sont de plus en plus malins - et nous devons l'être, nous aussi. Pour limiter la fraude en ligne, il est important de continuer à sensibiliser autant que possible la population avec tous les acteurs sur le terrain. Un consommateur vigilant et informé est moins susceptible de se retrouver victime du phishing. En outre, la lutte contre la criminalité financière est une **responsabilité partagée**, qui doit également être assumée par différentes parties, comme les consommateurs, le secteur des télécommunications et les plateformes de médias sociaux. Seule une **collaboration étroite** avec tous les acteurs sur le terrain, soutenue par la législation (européenne), nous permettra d'inverser la tendance.

Mais cela ne s'arrête pas là. Le respect de la législation en matière de protection des données et de cybersécurité par tous les acteurs de la chaîne (commerçants en ligne, plateformes de médias (sociaux) en ligne, télécoms, etc.) est aussi extrêmement important pour lutter contre la fraude par internet et protéger les consommateurs. **Ces acteurs ont également une responsabilité vis-à-vis de la société**. La Commission européenne, le Conseil européen et le Parlement européen le reconnaissent également. Dans le cadre de la révision de la DSP2, la Commission européenne a présenté une proposition de Règlement sur les services de paiement (RSP) visant à préserver le régime de responsabilité et à relever les défis susmentionnés. Ainsi, ils fournissent des outils supplémentaires pour lutter contre la fraude et



escomptent que tous les acteurs de la chaîne (commerçants en ligne, plateformes de médias (sociaux) en ligne, télécoms...) fassent leur part dans la lutte contre la fraude.

En résumé, la lutte contre la fraude n'est pas seulement l'affaire des banques. **Les banques ont besoin du soutien de tous les acteurs de l'écosystème pour lutter contre les fraudeurs**. Les consommateurs, le secteur des télécommunications, les commerçants en ligne, les plateformes de médias sociaux... et les banques doivent travailler ensemble pour protéger les citoyens des méthodes de plus en plus sournoises des fraudeurs en ligne.

Febelfin a formulé quelques recommandations dans son mémorandum politique sur la cybersécurité.

CONSULTEZ LE MÉMORANDUM →

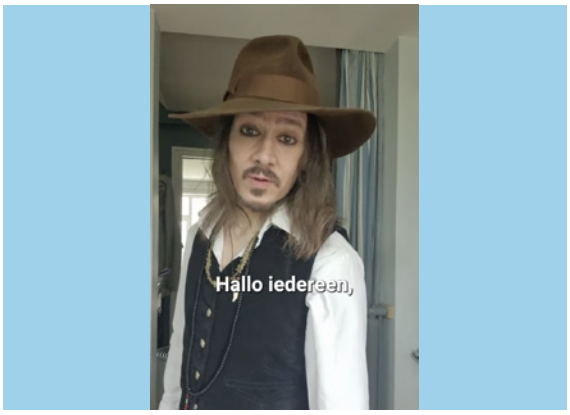
Febelfin n'est pas restée inactive l'année dernière

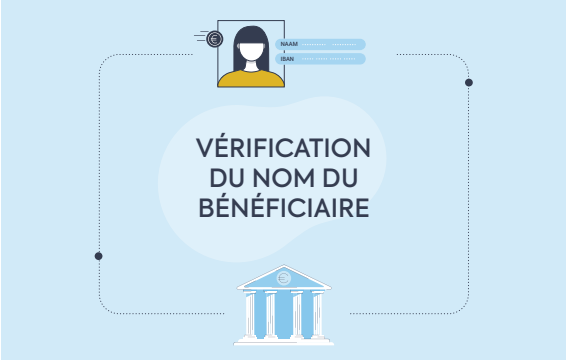
Nous avons **à nouveau lancé de nombreuses initiatives**, chaque fois en collaboration avec des partenaires solides - car c'est là que réside notre force. En collaboration, entre autres, avec la police locale et SAAMO, nous avons élaboré un **dépliant** clair contenant toutes les informations essentielles pour les victimes d'escroquerie en ligne. Grâce à un panel de test composé par SAAMO, nous sommes sûrs que les groupes cibles vulnérables comprennent et peuvent eux aussi utiliser ces informations.

Nous avons **également** organisé durant toute l'année des **séances d'information sur la sécurité des services bancaires en ligne**. Notre formation en ligne a été suivie par plus de 450 coaches numériques, qui possèdent désormais un grand nombre de connaissances sur les dernières formes de fraude et sur le matériel éducatif disponible.

Nous avons aussi tiré parti de l'actualité

En octobre, nous avons collaboré avec Safeonweb sur l'authentification à 2 facteurs. Nous avons sensibilisé le public à l'**ingénierie sociale via itsme®** et lancé la campagne marquante « **Johnny Depp** » sur la fraude aux rencontres, qui a généré de nombreux témoignages. Notre **campagne pour les jeunes** avec Patrick Ridremont a connu un véritable succès : plus de 2 millions de jeunes ont vu la vidéo dans laquelle il met en garde contre le partage de données personnelles en échange de gamecoins gratuits.





Nous évoluons sur le plan technique

Nous avons commencé à introduire progressivement la vérification du nom du bénéficiaire, c'est-à-dire la **vérification du nom IBAN** - un outil malin qui alerte les clients si le nom du bénéficiaire et le numéro de compte ne correspondent pas. Ce service gratuit renforce la confiance dans les virements et aide à prévenir la fraude.

Et nous allons continuer !

Le secteur financier reste déterminé à développer de nouvelles initiatives ciblées. Car ce n'est qu'ensemble que nous ferons la différence dans la lutte contre la fraude en ligne.

Fédération belge du secteur financier
Boulevard du Roi Albert II 19, 1210 Bruxelles
www.febelfin.be