febelfin

Phishing & autres arnaques en vue

La fraude en ligne demeure omniprésente. En 2023, les cybercriminels ont continué à envoyer massivement des messages de phishing en se faisant passer pour des proches de leurs victimes ou une organisation de confiance, telle qu'une banque ou un service public. En 2023, 75 % de tous les virements frauduleux effectués à la suite d'un phishing (hameçonnage) ont été bloqués ou récupérés par le secteur bancaire. Malgré ces efforts, ce sont cependant encore 40 millions d'euros[1] qui ont pu être dérobés par le biais du phishing.

En outre, nous constatons que d'autres formes de fraude en ligne, dans le cadre desquelles le/la client-e est manipulé-e et incité-e à effectuer lui/elle-même un paiement frauduleux, continuent de se déployer largement, comme la fraude à l'investissement ou l'arnaque au faux support technique[2]. Il est alarmant de constater que le grand public n'est pas encore suffisamment sensibilisé à ces nouvelles formes de fraude.

Heureusement, il y a aussi de bonnes nouvelles. Malgré les nombreuses tentatives de fraude en ligne et les cas d'arnaques réussies, nous constatons une évolution positive en termes d'actions entreprises lorsqu'il y a soupçon de fraude. En 2023, 91 % des personnes qui ont ainsi à un moment pensé avoir été victimes de fraude en ligne ont entrepris des démarches.

On observe également une diminution du nombre de personnes prêtes à partager leur code PIN et à envoyer leur carte bancaire à une adresse donnée. La population est également plus consciente du phénomène des mules financières.

Toutes ces observations indiquent que nous devons continuer à mettre l'accent sur une sensibilisation permanente. Tout le monde peut être la cible d'une fraude en ligne. Nous constatons que les jeunes, en particulier, sont de plus en plus dans le collimateur des fraudeurs en raison de leur attitude souvent désinvolte en matière de sécurité en ligne.

C'est pourquoi, en tant que secteur, nous restons engagés dans de nouvelles initiatives et de nouveaux partenariats pour lutter ensemble contre la fraude en ligne.

Quel est l'état des connaissances du public en matière de fraude en ligne ? Quelles sont les formes de fraude actuelles, quel est notre niveau de précautions lorsque nous achetons en ligne et communiquons-nous toujours nos codes aussi facilement ? Quels efforts le secteur a-t-il déployés et quelles sont nos priorités pour l'avenir ? Découvrez tous les détails dans ce dossier d'information qui présente les chiffres disponibles les plus récents.

[1] Source : chiffres Febelfin sur la base de l'enquête auprès des membres du Comité Fraudsys.

[2] La fraude à l'investissement est une forme d'escroquerie dans le cadre de laquelle les fraudeurs vous proposent des actions ou des produits financiers fictifs ou sans valeur. Dans l'arnaque au faux support technique, les escrocs se font passer pour des collaborateur-rice-s de votre banque et vous contactent par téléphone.

LE PHISHING NE S'ESSOUFFLE PAS

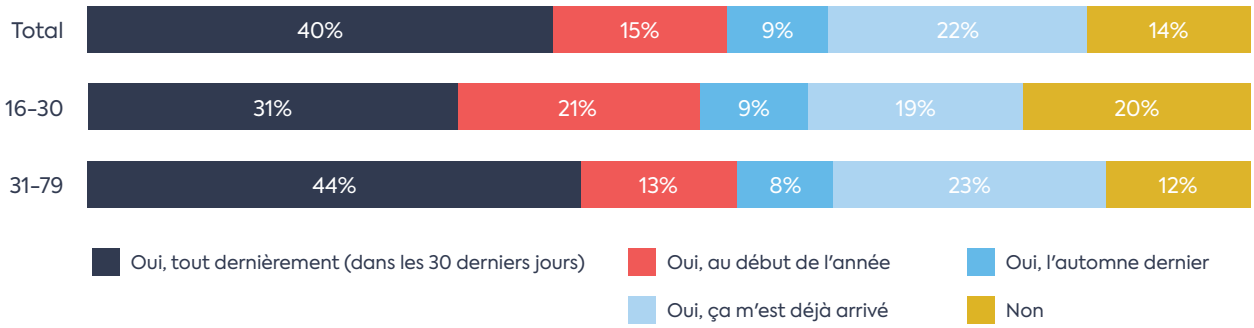
40 millions €
Butin en 2023

Malgré toutes les initiatives de sensibilisation, le phishing reste une technique de fraude populaire pour les cybercriminels.

Bien que 75 % des virements frauduleux effectués à la suite d'un phishing aient été bloqués ou récupérés par les banques, le phishing a malgré tout permis aux fraudeurs de détourner quelque 40 millions d'euros en 2023 (comme l'année précédente)[3].

Une récente étude réalisée par Febelfin, en collaboration avec le cabinet d'études Indiville[4] confirme l'ampleur des tentatives de phishing. Plus précisément, 55 % de la population a déjà reçu au moins un message de phishing cette année, et dans 40 % des cas, cela s'est produit très récemment. Ces chiffres sont comparables à ceux de l'année dernière.

Avez-vous déjà reçu un message de phishing ? Et, si oui, quand pour la dernière fois ?



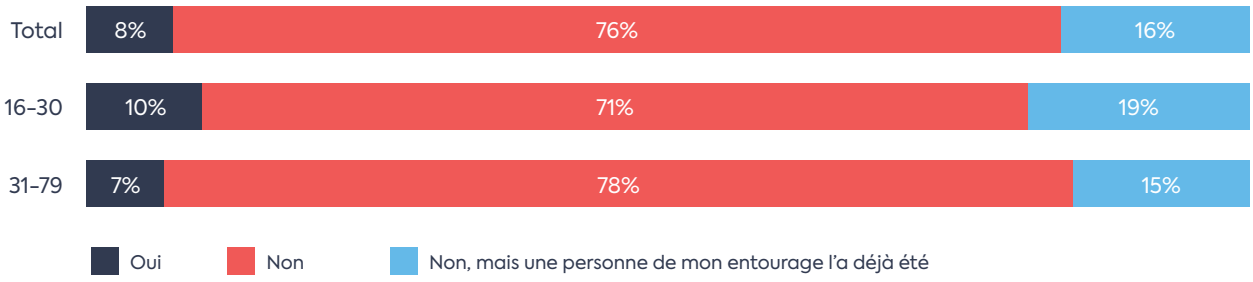
Source : Indiville

Les cybercriminels continuent donc d'envoyer massivement des messages de phishing. En 2023, près de 10 millions de messages ont été retransférés par des particuliers au point de contact suspect@safeonweb.be. En 2022, on en dénombrait 6 millions. En moyenne, 27.000 messages sont transmis chaque jour.

L'enquête montre que 8 % des personnes interrogées ont déjà été victimes de phishing. Les jeunes sont plus vulnérables (10 %). Ils sont également plus susceptibles de connaître quelqu'un qui a déjà été victime de phishing (19 %, 2022 : 15 %).

[3] Source : chiffres Febelfin sur la base de l'enquête auprès des membres du Comité Fraudsys.
[4] Enquête Indiville, 1 – 18 mars 2024, sur un échantillon représentatif de la population belge n: 2109 sondés NL/FR, âge 16-79. Marge d'erreur maximale : 2,1%

Avez-vous déjà été victime de phishing ?

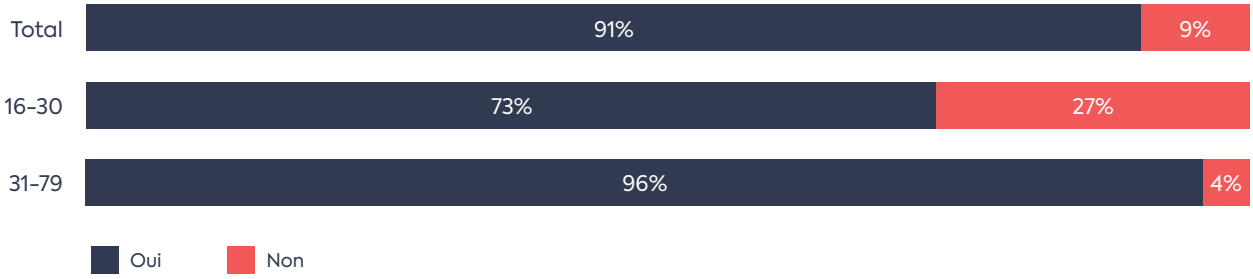


Source : Indiville

La connaissance du phishing doit être renforcée dans le public

Globalement, 9 % de la population belge n'a jamais entendu parler du phishing. Les personnes plus âgées sont légèrement mieux informées sur cette forme de fraude, puisque seulement 4 % d'entre elles n'en ont jamais entendu parler, tandis que chez les jeunes, près d'un tiers ne connaissent pas le terme « phishing ». Ce résultat est moins bon qu'il y a un an et est particulièrement inquiétant.

Avez-vous déjà entendu parler du phishing ?



Source : Indiville

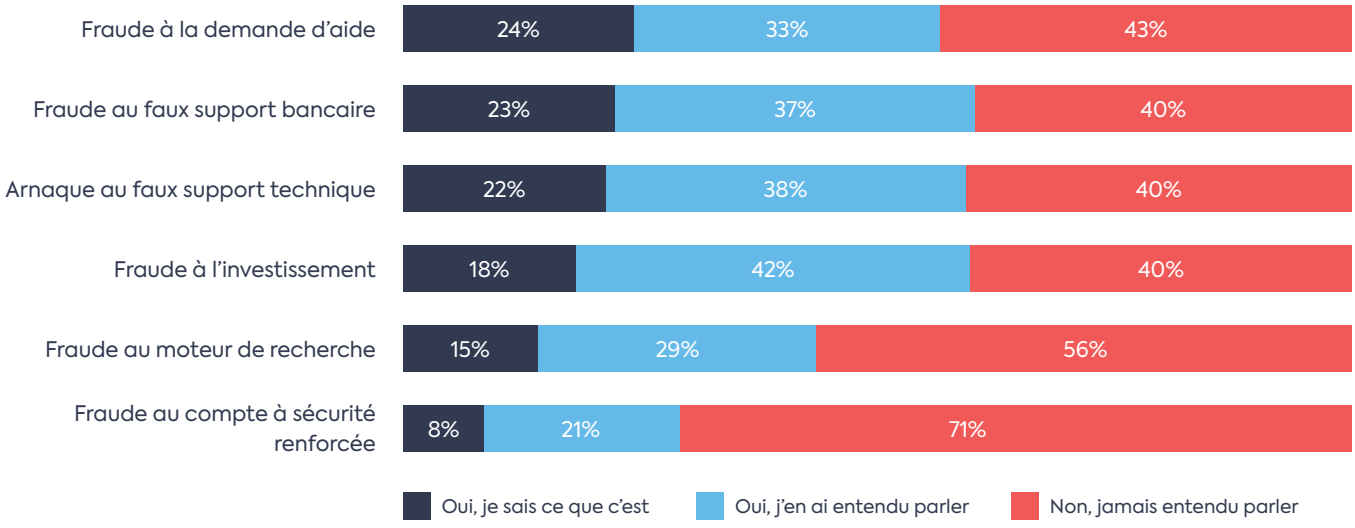
Ce chiffre montre qu'il est essentiel de continuer à informer les jeunes et d'éveiller leur vigilance face au phishing. En effet, ils restent une cible de choix pour les cybercriminels. Febelfin met dès lors tout en œuvre pour adapter sa communication à ce groupe cible. En novembre 2023, par exemple, nous avons lancé la campagne « Le phishing, ça se joue dans dans les détails ! » en collaboration avec Safeonweb et la Cyber Security Coalition. Nous avons aussi lancé l'escape game mobile, The Hacker Hotline, avec lequel Febelfin sillonne chaque semaine le pays pour informer les jeunes. Ce jeu les sensibilise de manière ludique aux dangers de la fraude en ligne et leur apprend à se protéger contre cette forme de fraude.

UNE FORME DE PHISHING EN CHASSE UNE AUTRE

De nouvelles formes de fraude en ligne se développent

Les formes de fraude en ligne dans le cadre desquelles la victime effectue elle-même un virement à la demande du cybercriminel continuent de progresser. Il s'agit notamment de la fraude à la facture, de la fraude au CEO, de la fraude sentimentale, de la fraude à la demande d'aide, de l'arnaque au faux support technique et bancaire, de la fraude à l'investissement et de la fraude au compte à sécurité renforcée. Ces pratiques ne sont généralement que peu voire pas connues des Belges. Ainsi, en moyenne, un peu moins d'un Belge sur cinq sait ce qu'impliquent ces formes de fraude, 33% en ont entendu parler, mais près de la moitié de la population est dans le flou le plus total. En moyenne, les jeunes semblent un peu plus au courant de ces formes de fraude que l'autre groupe d'âge (17% contre 21%). Mais la connaissance reste faible dans les deux groupes.

Connaissez-vous ces formes de fraude ?



Source : Indiville

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

CONSEIL

Si vous avez du mal à vous y retrouver, consultez le **dossier en ligne** sur le site web de Febelfin et découvrez les différents types de fraude en ligne.

Davantage de signalements de fraudes au faux support technique (bancaire)

Au cours de l'année écoulée, davantage de cas de fraude au faux support technique bancaire et au faux support technique ont été signalés.

QU'EST-CE QUE L'ARNAQUE AU FAUX SUPPORT TECHNIQUE ?

Dans le cas de l'arnaque au faux support technique, les escrocs se font passer pour des collaborateur-rice-s du service d'assistance d'une société informatique et vous appellent. Ils vous demandent d'allumer votre ordinateur et de suivre leurs instructions car il y aurait un problème avec votre ordinateur. Rien n'est plus faux : en réalité, ils vous piratent et prennent le contrôle de votre ordinateur, puis pillent vos comptes.

QU'EST-CE QUE LA FRAUDE AU FAUX SUPPORT TECHNIQUE BANCAIRE ?

La fraude au faux support technique bancaire est comparable à l'arnaque au faux support technique, mais les escrocs se font passer pour des collaborateur-rice-s de votre banque et vous appellent pour vous demander de partager votre écran d'ordinateur et vos codes personnels avec eux parce que des transactions prétendument suspectes ont été découvertes sur votre compte bancaire. C'est ainsi qu'ils parviennent à effectuer des virements au départ de votre compte et à vous subtiliser beaucoup d'argent.

Dans ce contexte, Febelfin a publié plusieurs communiqués de presse invitant les consommateur-rice-s à être vigilant-e-s lorsqu'ils/elles sont contacté-e-s et invité-e-s à partager leur écran d'ordinateur, à transmettre des codes personnels et à effectuer des transactions en ligne.

Un-e collaborateur-rice de banque ou un-e employé-e du support technique d'une société informatique ne vous demandera jamais vos codes personnels et, de surcroît, ne vous invitera pas à installer un logiciel lui permettant de prendre le contrôle de votre ordinateur à distance.

Attention à la fraude Card Stop par téléphone

La fraude Card Stop est un autre type de fraude contre lequel nous avons mis en garde à plusieurs reprises en 2023, et récemment encore. Comment cela fonctionne-t-il ? Les futures victimes sont appelées par un numéro de téléphone mobile. La personne à l'autre bout du fil prétend être un-e collaborateur-rice de Card Stop et informe le/la client-e que des transactions suspectes ont été détectées sur son compte bancaire. En réalité, il s'agit d'un appel frauduleux qui n'émane pas de Card Stop, mais d'escrocs. En collaboration avec Worldline, Febelfin rappelle aux consommateur-rice-s qu'ils/elles ne doivent jamais communiquer leurs codes bancaires par SMS, e-mail, médias sociaux ou téléphone.

LE SAVIEZ-VOUS ?

Dans le secteur, ce type d'action est souvent appelé « robotic phonescamming » : une voix robotisée appelle de nombreux numéros en masse et demande à la personne en ligne d'appuyer sur une touche si elle souhaite obtenir de l'aide. Un opérateur humain prend ensuite le relais, sachant que la victime potentielle a déjà été trompée par la manipulation robotique et qu'elle a donc plus de chances de tomber dans le piège, après la manipulation humaine.

L'aide à domicile pour les opérations bancaires, généralement une méthode d'escroquerie

Un nouveau type d'escroquerie est apparu ces derniers mois : des personnes qui se prétendent collaborateur-rice-s du service fraudes d'une banque, employé-e-s de Card Stop ou policier-ère-s contactent des personnes âgées par téléphone pour les prévenir qu'une fraude a été détectée sur leur compte. Ces fraudeurs proposent ensuite de se rendre au domicile de la victime, prétendument pour régler la situation. Malheureusement, ils n'ont qu'un seul objectif en tête : leur dérober tout ce qui leur tombe sous la main (carte bancaire, argent liquide, bijoux, etc.).

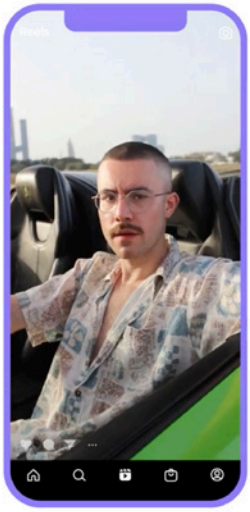
Comme les seniors sont évidemment une cible vulnérable et que nous voulons éviter autant que possible de tels cas, nous avons communiqué à ce sujet avec la Police fédérale et le SPF Intérieur.

La fraude à l'investissement atteint des sommets

La fraude à l'investissement est en plein essor. En 2023, les fraudeurs ont réussi à soutirer pas moins de 15,48 millions à leurs victimes (source : FSMA) par le biais de la fraude à l'investissement. Bien que les investisseurs soient un peu plus sensibilisés à la fraude à l'investissement, celle-ci reste d'une manière générale une forme de fraude peu connue des Belges.

En mars 2024, Febelfin a donc lancé, en collaboration avec le célèbre influenceur Sami Farhat, une campagne visant la fraude à l'investissement, intitulée « Rejoins leur communauté sans dépenser ton blé ! ».

Depuis une voiture de luxe, Sami appelait ses followers à suivre ses conseils financiers et à rejoindre son groupe Telegram privé pour, selon ses propres termes, « devenir riche rapidement ». Au terme de l'histoire, les followers ont finalement découvert que tout cela n'était qu'une énorme supercherie. Sami a aussitôt insisté sur la nécessité de rester vigilant-e face aux fraudes à l'investissement commises par de faux « finfluencers » sur les médias sociaux. Febelfin a ainsi touché un grand nombre de jeunes avec un message essentiel : « Rejoins leur communauté sans dépenser ton blé ! »



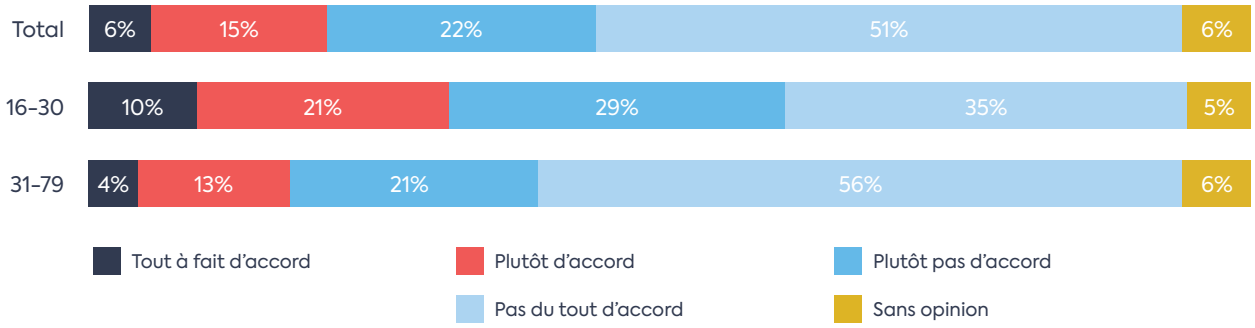
Quelques conseils pour éviter la fraude à l'investissement :

- **Vérifiez toujours l'identité du prestataire :** nom, siège social, pays d'établissement, coordonnées, etc.
- **Ne faites jamais confiance à un prestataire que vous ne pouvez pas identifier clairement.** Si l'entreprise est basée en dehors de l'UE, sachez que des problèmes risquent de survenir si vous vous retrouvez dans une situation conflictuelle et que vous voulez intenter une action en justice.
- **Méfiez-vous du démarchage (téléphonique) :** quelqu'un vous contacte en ligne ou par téléphone pour vous faire une offre financière non sollicitée ? Il s'agit souvent d'une arnaque.
- **Méfiez-vous si votre interlocuteur vous demande de transférer de l'argent** sur un compte bancaire situé dans un pays différent de celui où le prestataire est établi.
- **Le prestataire vous demande un paiement supplémentaire ?** C'est souvent un indice de fraude.
- Bref, si c'est trop beau pour être vrai, c'est souvent parce que ce n'est pas vrai.

Quelle est notre position sur la sécurité des achats en ligne ?

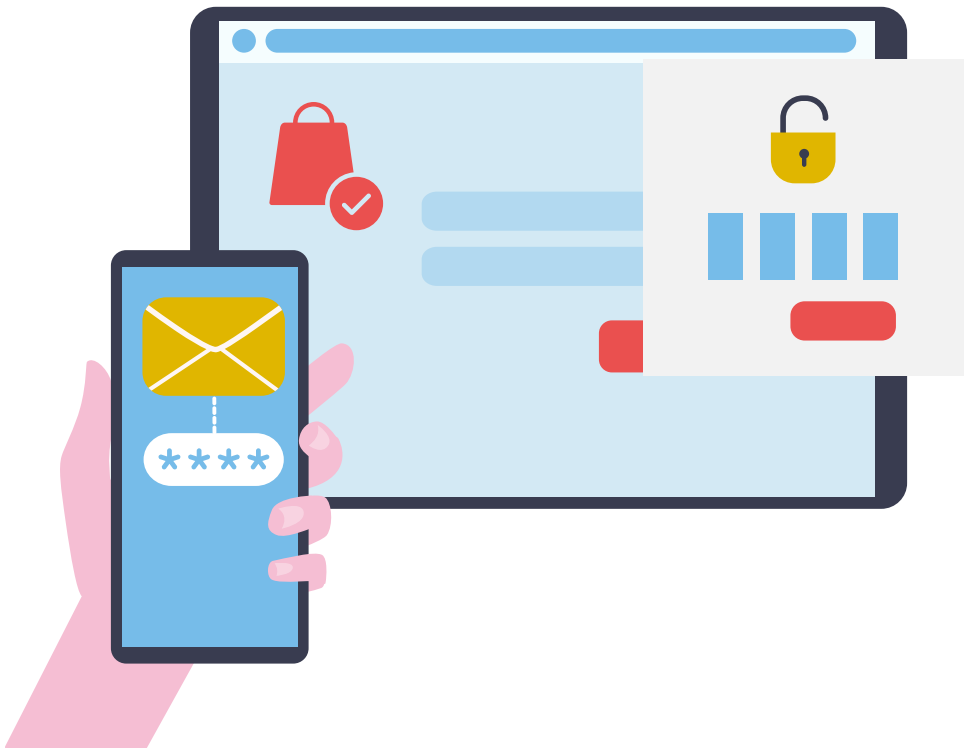
Heureusement, la majorité des Belges ne considère pas comme superflues les différentes étapes de sécurité (vérification en 2 étapes ou confirmation de l'identité en plusieurs étapes) pour les achats en ligne, par ex. l'introduction des codes de réponse du lecteur de carte ou de votre code itsme. C'est là une nouvelle amélioration des chiffres, comme l'année dernière d'ailleurs, et c'est une bonne chose.

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



Source : Indiville

Cependant, pour 1 Belge sur 5, ces mesures de sécurité restent un obstacle plus qu'une protection. Chez les jeunes, le groupe qui considère ces mesures comme un obstacle est légèrement plus important (31 %). C'est pourquoi il est et reste important de mieux les informer à ce sujet et de changer le regard que ces jeunes portent sur les mesures de sécurité en ligne : nous devons veiller à ce que ces mesures soient perçues comme une protection nécessaire contre les risques en ligne, plutôt que comme un obstacle.

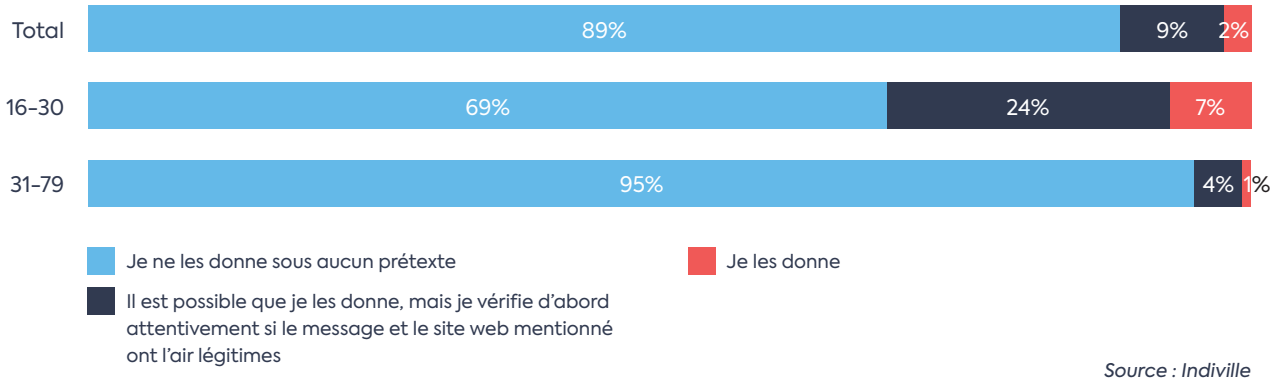


Moins de gens transmettent leurs codes ou envoient des cartes bancaires !

Mais il y a aussi de bonnes nouvelles : l'enquête montre que nous nous améliorons par rapport à l'année dernière lorsqu'il s'agit de ne pas transmettre nos codes bancaires et de ne pas renvoyer nos cartes bancaires.

89% des Belges ne communiqueraient en aucun cas leur code à la banque. Mais 2% de la population, et 7% des jeunes, donneraient leur **code bancaire** sans hésiter si la **banque** le leur demandait. Cela reste trop, mais c'est malgré tout une amélioration pour la deuxième année consécutive (2023 : 10%, 2022 : 13%).

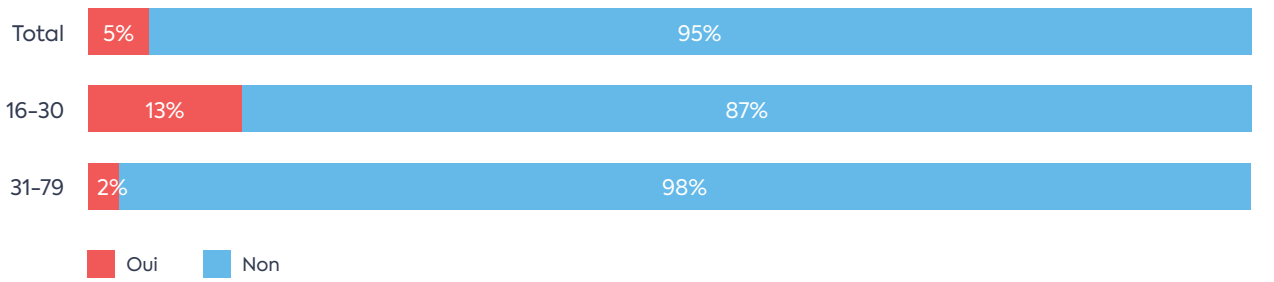
Si votre banque vous demande vos codes bancaires par e-mail, SMS, WhatsApp, téléphone...



Source : Indiville

95 % des Belges ne restitueraient en aucun cas leur carte bancaire à la banque. Une fois de plus, les jeunes font un peu moins bien que le reste de la population. 13 % d'entre eux rendraient leur carte si la banque le leur demandait, mais c'est malgré tout mieux que l'année précédente (2023 : 17 %).

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

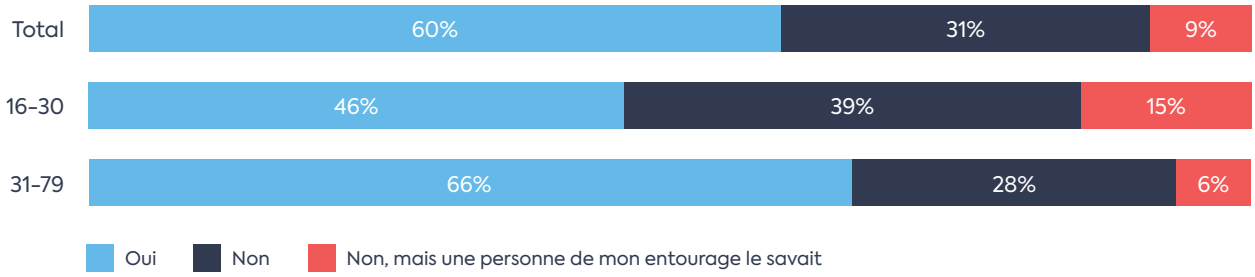


Source : Indiville

En cas de suspicion de fraude en ligne, les consommateur-rice-s entreprennent aussi davantage de démarches

Nous constatons une évolution positive en ce qui concerne les démarches entreprises en cas de suspicion de fraude. 6 victimes de phishing sur 10 savaient ce qu'il fallait faire et 91 % ont entrepris des démarches aussitôt qu'elles ont soupçonné une (tentative de) fraude en ligne, par exemple en vérifiant leur compte ou en contactant Card Stop.

Saviez-vous quelles démarches entreprendre ou à qui demander de l'aide ?



Source : Indiville

53% ont vérifié attentivement leurs comptes, 30% ont appelé la banque et 26% ont appelé Card Stop. Bien que les jeunes soient en moyenne moins bien informé-e-s sur les mesures à prendre en cas de soupçon de fraude, ils/elles ont désormais le réflexe de vérifier leurs comptes plus souvent que les années précédentes (2024 : 51%, 2023 : 44%, 2022 : 34%). Il s'agit donc d'un pas dans la bonne direction.

CONNAISSEZ-VOUS LE NUMÉRO DE CARD STOP ?

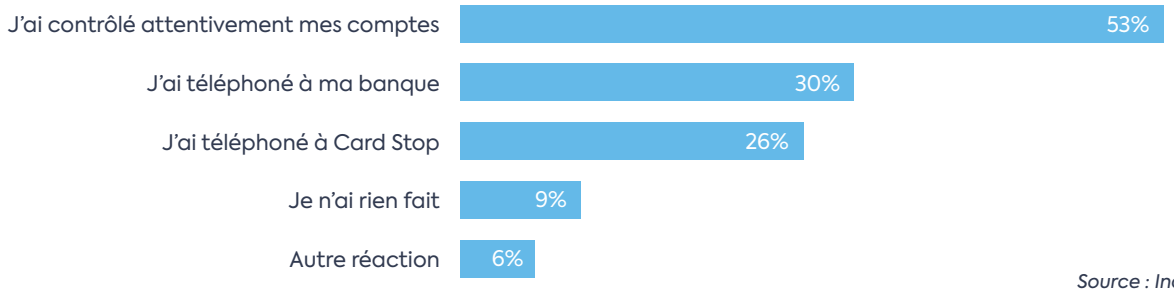
CARD 078 170 170 STOP 24/24

Vous pouvez joindre Card Stop via le numéro **078 170 170** si vous voulez faire bloquer votre carte de paiement après un vol, une perte ou une tentative de fraude.

VICTIME DE FRAUDES EN LIGNE ?

Contactez aussi votre banque. Les banques disposent de services dédiés à la fraude qui sont joignables 24/24, 7/7. Vous retrouverez toutes les coordonnées sur **le site web de Card Stop**.

Vous vous êtes senti-e mal à l'aise... Qu'avez-vous fait ensuite ?



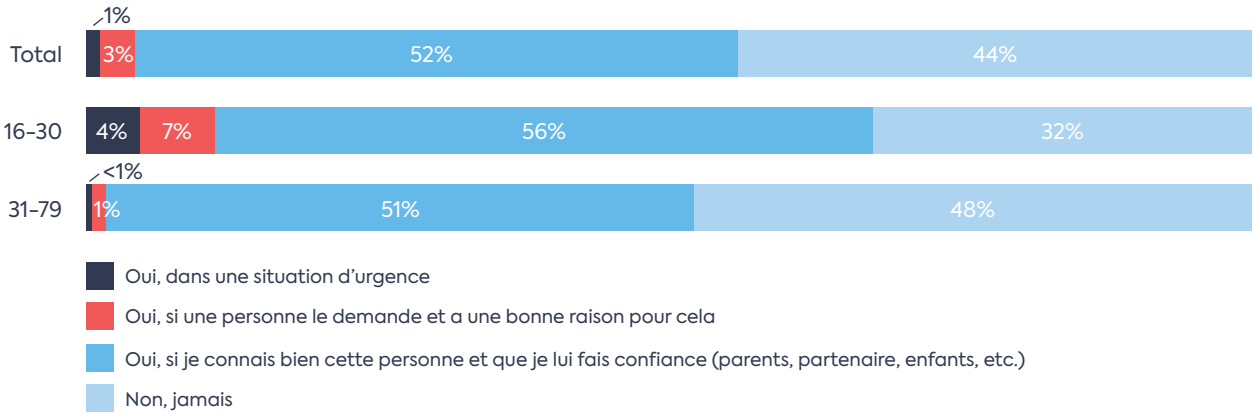
Source : Indiville

La problématique des mules financières est encore trop peu connue

Un individu vous aborde et vous demande si vous voulez gagner de l'argent rapidement et facilement en prêtant votre compte bancaire et/ou votre carte bancaire pendant quelque temps... Pour les jeunes, la tentation reste particulièrement grande.

4 % de la population belge donnerait sa carte bancaire et son code PIN à un inconnu en échange d'argent. Chez les jeunes, 11 % seraient prêt-e-s à le faire, ce qui représente une amélioration par rapport à l'année dernière, mais reste évidemment trop élevé.

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



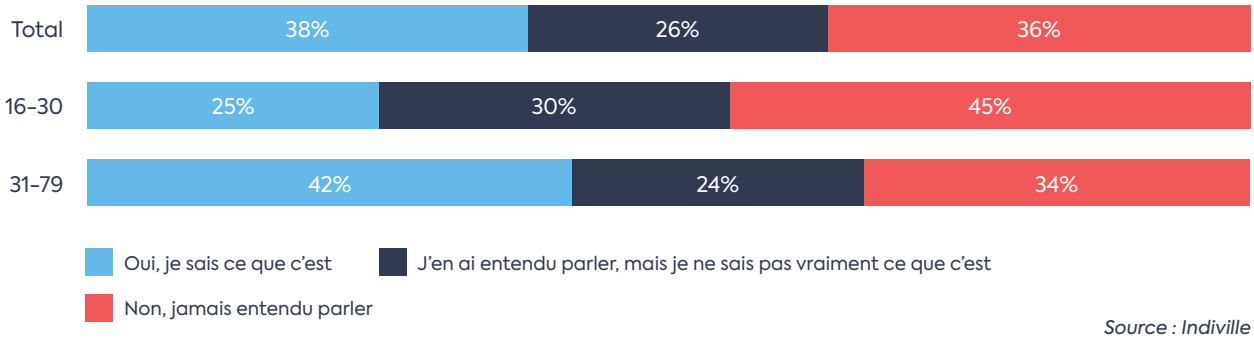
Source : Indiville

QU'EST-CE QU'UNE MULE FINANCÈRE ?

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**.

Près de 40 % des Belges savent ce qu'est une mule financière, mais chez les jeunes, cette proportion n'est que de 25 %. 45% des jeunes n'ont même jamais entendu parler de ce phénomène.

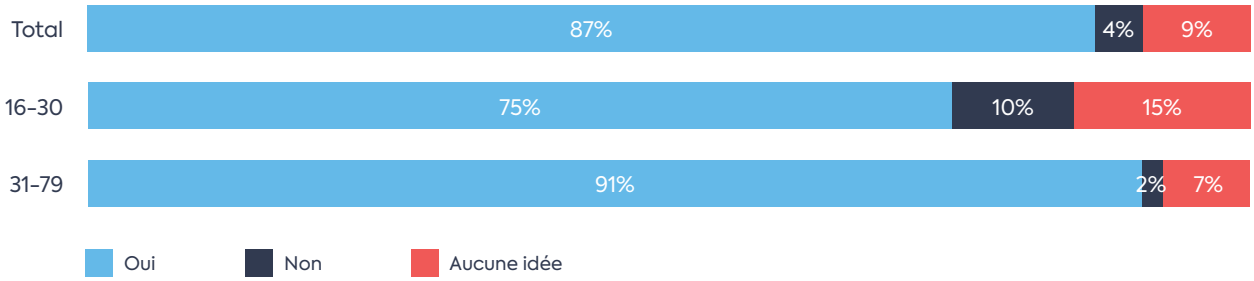
Savez-vous ce qu'est une mule financière ?



Source : Indiville

Dans de nombreux cas, les jeunes ne savent pas non plus que servir de mule financière est punissable. Les conséquences sont pourtant lourdes : peines de prison, amendes, dédommagement des victimes, etc.

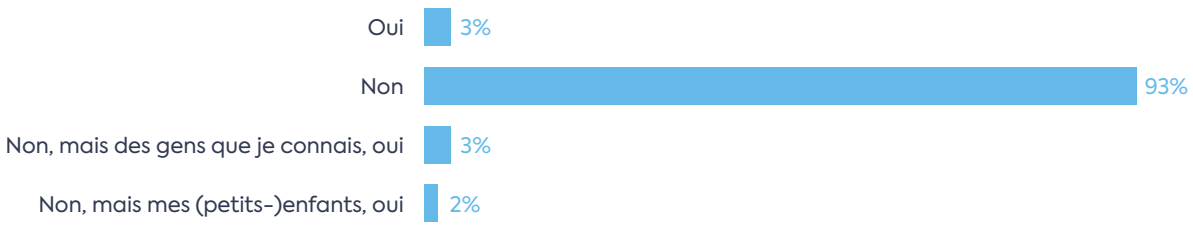
Pensez-vous que servir de mule financière constitue une infraction pénale ?



Source : Indiville

En outre, 3 % déclarent avoir déjà été approchés par un fraudeur qui leur a demandé de devenir une mule financière et 5 % connaissent des personnes à qui cette demande a été faite. Ce pourcentage est également plus élevé chez les jeunes : 6 % ont déjà été approchés eux-mêmes et 12 % connaissent quelqu'un à qui cela est arrivé.

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



Il reste donc essentiel d'expliquer le phénomène des mules financières, en particulier aux jeunes, et de les sensibiliser aux risques auxquels ils/elles s'exposent et aux sanctions encourues. Car les jeunes sont une cible privilégiée pour ce type de fraude.

LE SECTEUR FINANCIER DÉVELOPPE EN PERMANENCE DE NOUVELLES INITIATIVES POUR LUTTER CONTRE LA FRAUDE EN LIGNE

Apprentissage en ligne pour les coachs numériques

En 2023, Febelfin a lancé une nouvelle formation en ligne pour les coachs numériques qui aident les personnes à renforcer leurs compétences numériques. Cette formation en ligne fournit aux coachs numériques les conseils et outils nécessaires pour aider les consommateur-rice-s moins averti-e-s sur le plan numérique. Une attention spécifique est accordée à la sécurité en ligne et à l'explication des différentes formes de fraude en ligne.

La formation en ligne connaît un beau succès : jusqu'à présent, près de 400 bénévoles et professionnel-le-s l'ont suivie. Ce succès souligne une fois de plus l'importance de la sensibilisation et de la formation des différents groupes cibles et parties prenantes.

Contrôle du nom-IBAN

En outre, le secteur met tout en œuvre pour permettre l'introduction du **contrôle du nom-IBAN**. Il s'agit d'un outil permettant de lutter contre certains types de fraude au virement, comme la fraude à la facture. Lors de l'introduction d'un ordre de virement, la banque du/de la donneur-se d'ordre vérifie auprès de la banque du/de la bénéficiaire si le numéro de compte (IBAN) et le nom du bénéficiaire correspondent. Si ce n'est pas le cas, la banque avertit le/la client-e, grâce à cette vérification du nom-IBAN, qu'il y a peut-être fraude ou escroquerie. Les banques s'appliquent donc à permettre l'introduction de ce contrôle.

Le système d'alerte d'incidents

Le **système d'alerte d'incidents** est un projet qui devrait permettre aux banques de partager des informations sur des incidents dans le cadre de paiements afin de mieux protéger encore les clients contre des incidents suspects.
L'identification à partir de mouvements suspects pourrait être partagée entre les banques afin qu'elles puissent prendre en compte les risques identifiés.
Le partage de ces informations se fera conformément à la loi sur la protection des données personnelles.

Le secteur financier plaide pour la mise en œuvre de ce projet qui contribuera à une lutte encore plus efficace contre les incidents en ligne et la problématique des mules financières.

Ateliers et sessions d'information sur mesure pour différents groupes cibles

Afin de sensibiliser davantage les jeunes au fait qu'ils/elles constituent une cible importante et vulnérable pour les cybercriminels, nous avons également continué à collaborer avec les écoles, les organisations de jeunesse et les partenaires locaux au cours de l'année écoulée.

Notre escape game mobile, la Hacker Hotline, qui se déplace chaque semaine, sillonne tout le pays pour prévenir les jeunes, de manière ludique et accessible, des risques de fraude en ligne et leur donner des conseils sur la manière d'éviter de tomber dans le piège.

Nos sessions d'information sur les formes de fraude en ligne, qui mettent notamment l'accent sur les mules financières, seront également poursuivies. Febelfin a ainsi participé à la « Journée de la sécurité » organisée par la police et les pompiers à Knokke-Heist. Nous y avons proposé des ateliers sur la fraude en ligne et les mules financières aux différentes écoles secondaires locales et avons, à cette occasion, touché plus de 1.000 élèves.

Comme nous voulons atteindre et informer autant que possible les différents groupes de population vulnérables, nous continuons également à proposer des sessions d'information sur les services bancaires numériques sécurisés à d'autres groupes cibles, tels que les personnes âgées. En collaboration avec les représentants des différentes banques, nous répondons à toutes leurs questions sur les services bancaires numériques et leur sécurité au cours de ces sessions.

Febelfin a également collaboré à un E-learning « Cybersécurité » du VDAB (service public de l'emploi de la Flandre) qui sera proposé à tous les titulaires d'un compte auprès du VDAB.

Événement « Cybersécurité » pour les parties prenantes

En collaboration avec le BIN Kenniscentrum (Centre d'expertise - Partenariat local de Prévention) et les Services fédéraux des Gouverneurs du Brabant flamand et d'Anvers, Febelfin a organisé un événement pour les parties prenantes sur la cybersécurité. Ensemble, ils ont cherché à répondre à des questions importantes telles que « Comment pouvons-nous collaborer plus étroitement en tant qu'acteurs concernés ? » et « Comment pouvons-nous diffuser encore mieux des informations cruciales sur la cybersécurité au sein de nos groupes cibles locaux ? ». Cet événement a permis des échanges d'idées inspirantes et la cybersécurité a une fois de plus été placée en tête des priorités.

Campagne de sensibilisation annuelle à la problématique des mules financières

Febelfin est consciente des dangers du phénomène des mules financières et mise sur une sensibilisation supplémentaire par le biais d'un communiqué de presse annuel pour attirer l'attention sur ce point, mais aussi en proposant des roadshows pour les jeunes et du matériel didactique gratuit. Vous trouverez plus d'informations à ce sujet à la page 12 de ce dossier.

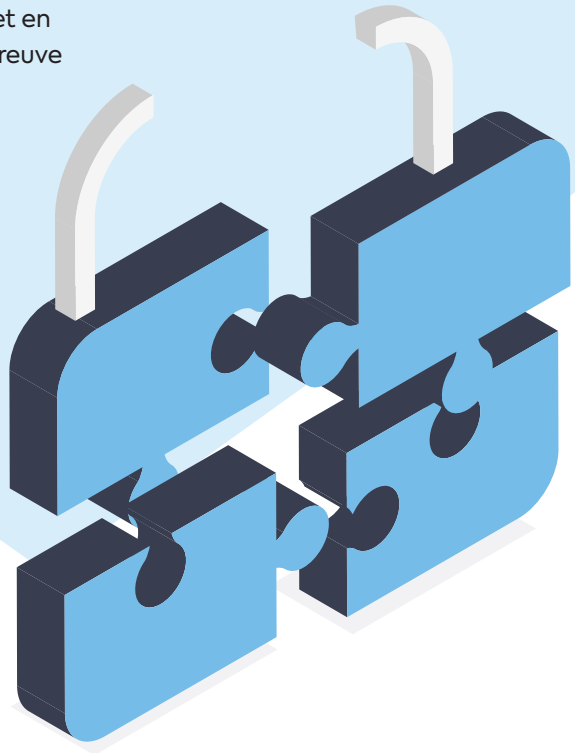
LA COLLABORATION ENTRE LES DIFFÉRENTES PARTIES PRENANTES RESTE CRUCIALE

Le secteur est pleinement conscient que nous ne pourrons réussir dans la lutte contre le phishing et la fraude en ligne qu'en unissant nos forces. Une coopération permanente avec les différentes parties prenantes, les pouvoirs publics et les organisations de terrain est et reste nécessaire dans cette optique. Febelfin proposera donc aux autres parties prenantes de mettre en commun leur expertise et leurs ressources afin d'organiser des campagnes conjointes à l'avenir.

Les techniques des escrocs en ligne progressent sans cesse, grâce à des évolutions technologiques telles que l'IA et les deep fakes, et nous devrons encore relever de nombreux défis. Il est essentiel de suivre ensemble et en permanence ces évolutions et de faire preuve de la capacité d'adaptation nécessaire.

Ce n'est qu'en développant une vision et une stratégie communes à toutes les parties concernées sur la manière de poursuivre la lutte contre la cybercriminalité et de faire tourner l'économie en toute sécurité que nous pourrons garantir ensemble que chacun-e se sente protégé-e dans le monde numérique d'aujourd'hui et de demain.

Febelfin a formulé quelques recommandations dans son mémorandum politique sur la cybersécurité. Celles-ci peuvent être consultées ici.



Fédération belge du Secteur Financier

www.febelfin.be