febelfin

Don’t be fooled by a ‘phish’

Effectuer des opérations bancaires, faire des courses, réserver des vacances… tout se passe de plus en plus en ligne. Malheureusement, cela signifie aussi que la criminalité se déplace vers le monde numérique. Celui-ci est devenu, pour les fraudeurs, l'espace idéal pour escroquer les gens financièrement.

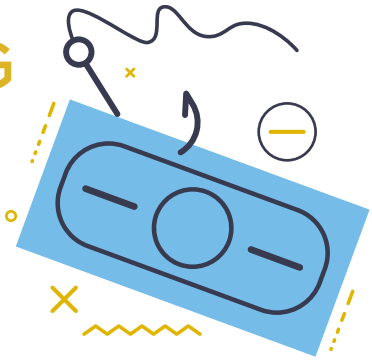
En 2022, les cybercriminels ont envoyé un très grand nombre de messages de phishing, en se faisant passer pour des organisations de confiance, telles que des banques, des entreprises d'utilité publique et des services publics. Quels que soient l'âge, le niveau de formation, la langue… tout le monde est dans le collimateur des cybercriminels, et, malheureusement aussi, les jeunes. Une vigilance constante reste donc de mise.

Comment la fraude en ligne évolue-t-elle et quelles en sont les formes les plus actuelles ? Le public est-il suffisamment informé sur le « phishing » et les « mules financières » ? Sur quels aspects le secteur met-il l'accent ? Découvrez toutes les réponses à ces questions dans ce dossier d'information qui reprend les chiffres d'une enquête récente[1].

QU'EST-CE QUE LE PHISHING ?

Il s'agit d'une forme de fraude dans le cadre de laquelle les criminels « pêchent » les codes bancaires personnels de leurs victimes potentielles en se faisant passer pour une organisation connue ou de confiance.

PLUS DE MESSAGES DE PHISHING EN 2022 = PLUS DE BUTIN



39,8 € millions
en 2022

En 2022, un total de **39,8 millions d'euros** a été dérobé par le biais du phishing, soit une hausse par rapport à l'année précédente (2021 : 25 millions d'euros). Cette évolution tient principalement à l'**augmentation considérable** du nombre de messages de **phishing** envoyés.

L'ampleur de toutes ces tentatives de phishing est confirmée par les résultats de l'enquête menée par Febelfin, en collaboration avec le bureau d'études Indiville. Selon cette étude, 69 % des Belges ont reçu au moins un message de phishing au cours des 6 derniers mois[2].

Cette augmentation est confirmée par les chiffres du Centre pour la Cybersécurité Belgique : en 2022, les internautes belges ont transféré pas moins de 6 millions de messages suspects à l'adresse e-mail suspect@safeonweb.be, soit 1,5 million de messages de plus qu'en 2021.

[1] Enquête Indiville, 3-20 mars 2023, sur un échantillon représentatif de la population belge n : 2.117 enquêtes NL/FR, 16-79 ans. Marge d'erreur maximale : 2,1 %.

[2] Plus précisément, les 3 derniers mois de 2022 et les 3 premiers de 2023.

Les escrocs vont à la « pêche » aux données, mais ils le font de différentes manières

Ce n'est pas un phénomène nouveau. Il y a une **constante dans le phishing** : les fraudeurs pêchent des données (bancaires) par divers canaux : e-mail, téléphone, lettres, SMS, médias sociaux ou WhatsApp. Ils essaient d'escroquer financièrement les gens en se faisant passer pour des organisations ou des institutions fiables (banques, services publics, entreprises d'utilité publique...). Le message envoyé contient un lien vers un faux site web, où la victime est invitée à introduire ses codes bancaires personnels. Une fois que les fraudeurs ont mis la main sur ceux-ci, ils peuvent effectuer des transactions au nom de la victime.

PHISHING À LA CARTE BANCAIRE

Dans le cadre du **phishing à la carte bancaire**, les fraudeurs vous demandent par e-mail, téléphone ou SMS d'envoyer votre carte bancaire par la poste à une certaine adresse. Ils vous fournissent simultanément un lien vers un faux site web, où vous devez introduire vos codes personnels. Les fraudeurs disposent ainsi d'un seul coup de votre carte bancaire et de vos codes personnels.

PHISHING À LA CARTE BANCAIRE À DOMICILE

Dans le cadre du **phishing à la carte bancaire** à domicile, le fraudeur vous téléphone en se faisant passer pour un employé de la banque et vous dit que des transactions suspectes ont été détectées sur votre compte. Il vous propose de passer chez vous pour résoudre le problème. Le fraudeur fait alors en sorte que vous vous connectiez à votre banque en ligne. Il peut ainsi facilement noter votre code personnel.

Désormais, il existe également des **variantes** de cette méthode, à savoir le **phishing à la carte bancaire** ou le **phishing à la carte bancaire à domicile**.

Les cybercriminels jouent aussi sur l'actualité. Durant la **crise énergétique** de 2022, la population belge a été inondée de messages frauduleux promettant des primes ou d'autres formes d'aides publiques, dans un contexte de flambée des prix de l'énergie. Les cybercriminels ont développé mille et un stratagèmes pour inciter leurs victimes potentielles à cliquer sur des liens frauduleux, en particulier à un moment où les conséquences de la crise énergétique et de l'inflation croissante généraient de profondes incertitudes.

AUTRES FORMES COURANTES DE FRAUDE

En 2021, nous avons clairement constaté une évolution vers d'autres formes de fraude, telles que la fraude à l'investissement, la fraude à la facture, la fraude aux comptes à sécurité renforcée, la fraude à la demande d'aide... Des formes de fraude dans le cadre desquelles la **victime** est **manipulée et persuadée de transférer** de **l'argent elle-même**. En 2022, la part de ces formes de fraude est restée **stable**.

FRAUDE À LA DEMANDE D'AIDE

Dans le cadre de la **fraude à la demande** d'aide, les fraudeurs se font passer, dans un e-mail, SMS ou message sur les médias sociaux, pour l'un ou l'une de vos proches. Ou inversement : ils écrivent à vos proches en votre nom et demandent une aide financière de toute urgence.

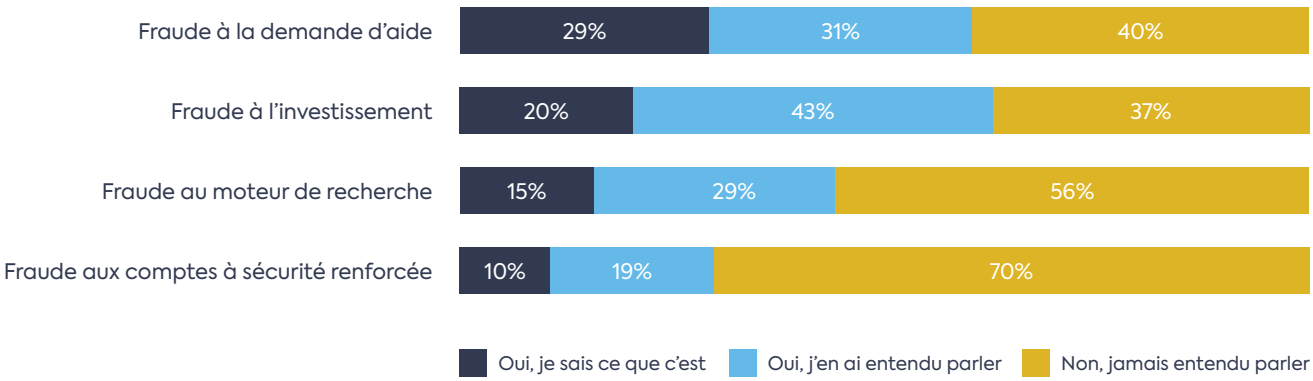
Les Belges ne sont pas toujours informé-e-s des formes actuelles de fraude

FRAUDE À L'INVESTISSEMENT

Dans le cadre de la **fraude à l'investissement**, les fraudeurs vous proposent « l'affaire du siècle », un investissement qui promet un rendement élevé. À ceci près qu'il apparaît ensuite que cet investissement n'existe pas.

Il ressort des résultats de l'étude Indiville[3] que les Belges devraient encore améliorer leurs connaissances sur les (nouvelles) formes de fraude.

Connaissez-vous ces formes de fraude ?



Source : Étude Indiville

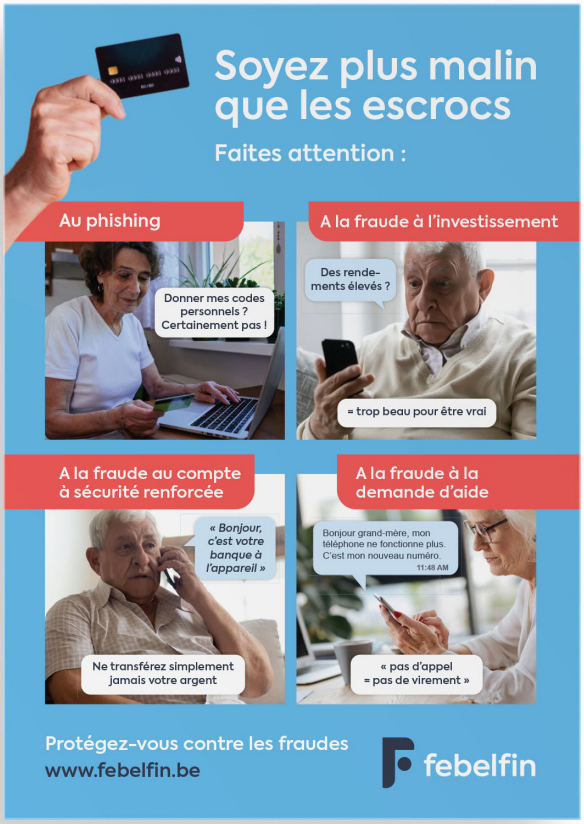
[3] Enquête Indiville, 3-20 mars 2023, sur un échantillon représentatif de la population belge n : 2.117 enquêtes NL/FR, 16-79 ans. Marge d'erreur maximale : 2,1 %.

La fraude à la demande d'aide et la fraude à l'investissement sont un peu mieux connues de la population : 60 % des Belges ont déjà entendu parler de la première et 63 % de la seconde. En revanche, moins de la moitié des Belges connaissent la **fraude au moteur de recherche** et la **fraude aux comptes à sécurité renforcée**.

Ces dernières années, Febelfin s'est efforcée de sensibiliser (encore davantage) la population aux différentes formes de fraude et de l'informer sur les risques et les mesures préventives qui peuvent être prises, au moyen de divers communiqués de presse et d'un matériel visuel (poster, stickers, livret-jeux...). L'objectif était d'aider la population à mieux reconnaître la fraude et à se protéger contre toutes sortes d'escroqueries en ligne. Il est très important de faire preuve d'une vigilance constante et de partager régulièrement des informations et des mises à jour sur la question, pour pouvoir lutter conjointement contre ces formes de fraude et réduire leurs conséquences néfastes.

FRAUDE AUX COMPTES À SÉCURITÉ RENFORCÉE

Dans le cadre de la **fraude aux comptes à sécurité renforcée**, les escrocs vous envoient d'abord (mais pas toujours) un message de phishing pour vous soutirer vos codes bancaires personnels. Ils tentent ainsi d'avoir accès à votre compte. Ensuite, ils vous passent un coup de téléphone. Ils se font passer pour un employé de votre banque et vous demandent de transférer de l'argent sur un nouveau compte, prétendument sécurisé. Ce type de fraude vise principalement les personnes âgées.



Poster et stickers pour sensibiliser les seniors aux formes actuelles de fraude

LES BELGES ONT-ILS APPRIS QUELQUE CHOSE SUR LE PHISHING ET LES MULES FINANCIÈRES CES DERNIÈRES ANNÉES ?

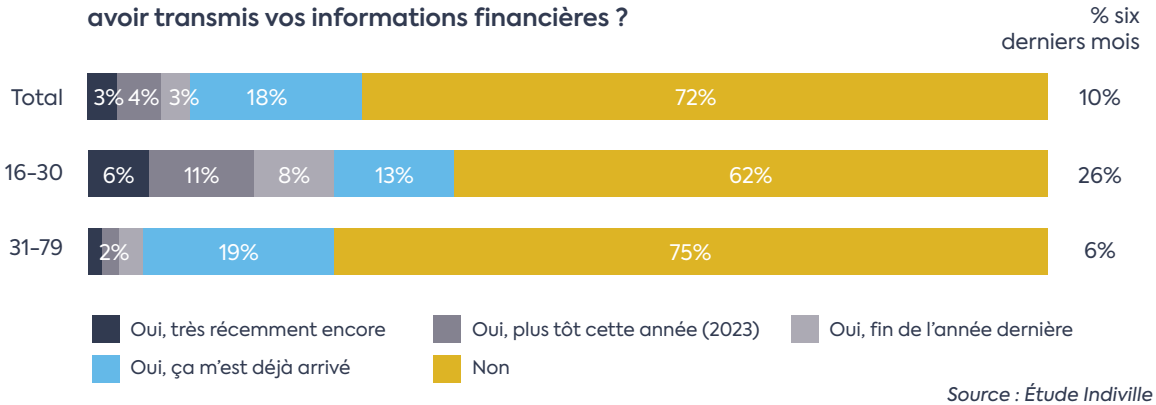
Le problème du phishing, des mules financières et, en général, de la fraude en ligne demeure trop important. Il ressort néanmoins de l'enquête Indiville que la façon dont les Belges font face à la fraude en ligne s'est améliorée. Les actions du secteur et de ses partenaires commencent à porter leurs fruits, mais il reste nécessaire d'informer de manière continue le public, en particulier les jeunes, surtout compte tenu de l'augmentation des tentatives de phishing. En raison du nombre croissant de messages de phishing envoyés, les dommages n'ont malheureusement pas encore diminué, malgré le comportement plus avisé des Belges.

PHISHING

Nous partageons moins d'informations financières et agissons plus

En 2023, 10 % des répondant-e-s ont partagé des informations financières qu'ils et elles ne se sentaient pas à l'aise de communiquer (11 % en 2022). Ce pourcentage est légèrement plus élevé chez les 16-30 ans (18 %), mais on observe une **amélioration** par rapport à 2022 (25 %).

Vous êtes-vous déjà senti-e mal à l'aise après avoir transmis vos informations financières ?

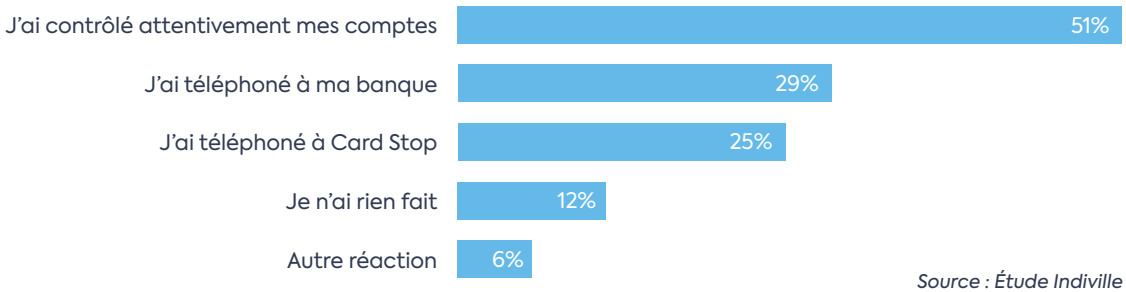


Source : Étude Indiville

Autre note positive : **88 %** des répondant-e-s ont **entrepris l'une ou l'autre démarche** après avoir partagé cette information. Comme il ressort du tableau suivant, 51 % des répondant-e-s ont vérifié leurs comptes bancaires après avoir partagé des informations financières. Les plus âgé-e-s vérifient leurs comptes un peu plus souvent que les jeunes (55 % contre 44 %).

29 % des répondant-e-s ont contacté leur banque et 25 % ont appelé Card Stop.

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

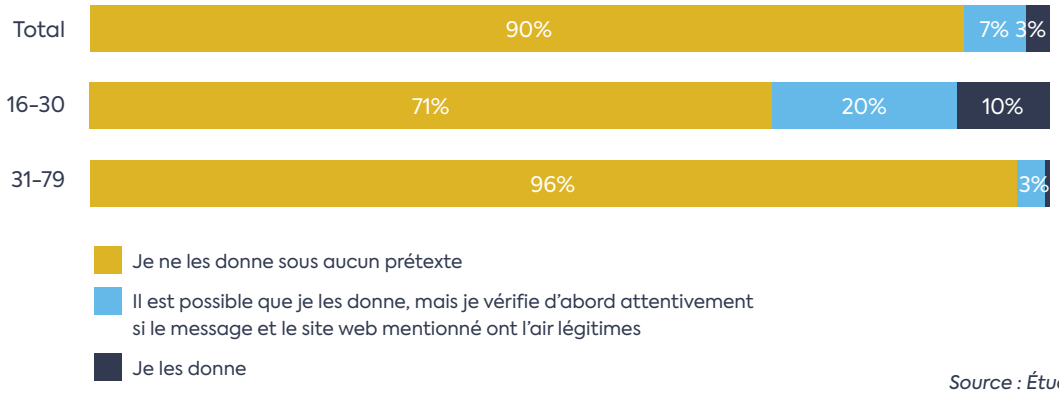


Source : Étude Indiville

9 Belges sur 10 ne donneraient en aucun cas leurs codes à la banque

Pourtant, 3 % des répondant-e-s partageraient encore leurs codes bancaires sans hésiter si leur banque le leur demandait (en 2022, on en était à 5 %). **Les jeunes,** en particulier, demeurent **plus vulnérables**. En effet, 10 % des 16-30 ans partagent leurs codes bancaires plus facilement que les autres groupes d'âge. Bien que ce pourcentage soit toujours beaucoup trop élevé, on note une **amélioration par rapport à 2022**, où il était de 13 %. Il est positif de constater une amélioration par rapport à l'année précédente en ce qui concerne le partage de codes bancaires. Cela signifie que la population est **plus consciente des risques liés au partage d'informations bancaires personnelles**, même si les chiffres démontrent également que la sensibilisation demeure nécessaire.

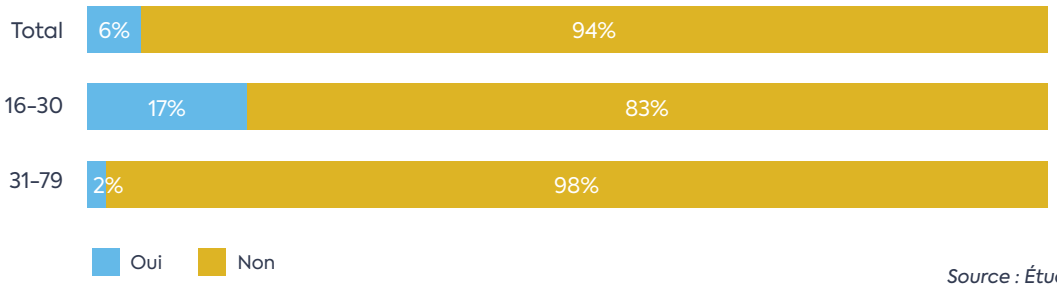
Si votre banque vous demande vos codes bancaires par e-mail, SMS, WhatsApp, téléphone…



Source : Étude Indiville

Nous constatons aussi que **6 %** de la population serait prête **à renvoyer sa carte bancaire si la banque le lui demandait**. Chez les 16 à 30 ans, cette part grimpe toutefois à 17 %. La vulnérabilité marquée des jeunes à la fraude en ligne demeure particulièrement préoccupante.

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



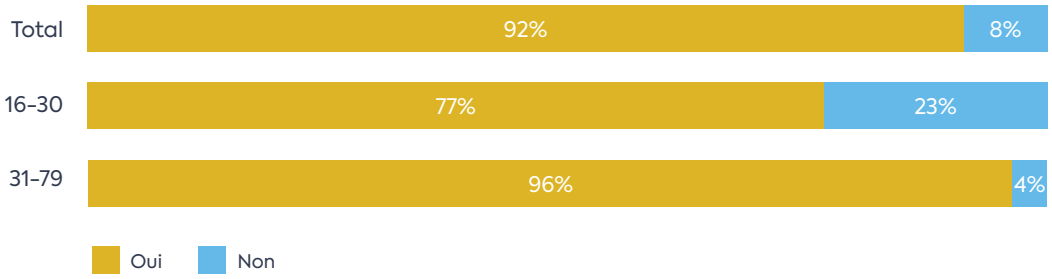
Source : Étude Indiville

Ce sont surtout les jeunes qui ignorent ce qu'est le phishing

8 % des Belges **n'ont jamais entendu parler de phishing**. Les personnes âgées obtiennent de meilleurs résultats à cet égard : 4 % n'ont jamais entendu parler de phishing, ce qui est mieux qu'en 2022 (7 %).

Malgré une légère amélioration par rapport à 2021 (24 %) et 2022 (30 %), le nombre de jeunes qui ne savent pas ce qu'est le phishing demeure trop élevé (**23 %**).

Avez-vous déjà entendu parler du phishing ?

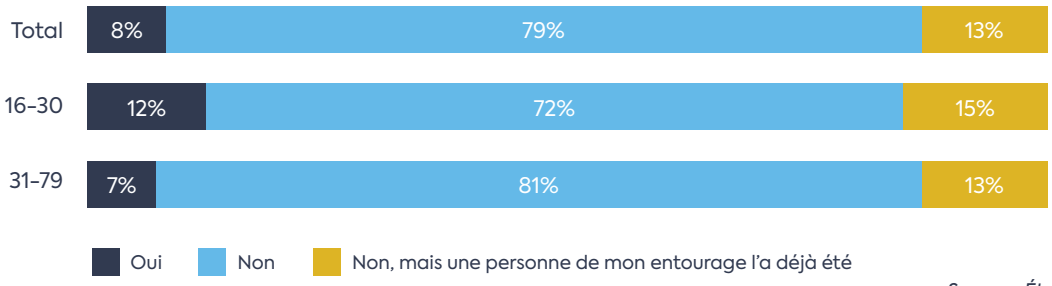


Source : Étude Indiville

Près d'un-e Belge sur dix a déjà été victime de phishing

8 % précisément des Belges déclarent avoir déjà été **victimes** de phishing. Ce pourcentage est plus élevé chez les jeunes, à savoir 12 %. Bien que les jeunes baignent depuis leur naissance dans la technologie numérique et qu'ils et elles passent pour des « digital natives », cela ne signifie malheureusement pas que les uns et les autres disposent de toutes les compétences numériques et soient tout à fait au courant de la manière d'effectuer des opérations bancaires en ligne en toute sécurité. Les jeunes font par ailleurs partie du groupe de population qui indique le plus souvent connaître une personne qui a déjà été victime de phishing (15 %).

Avez-vous déjà été victime de phishing ?



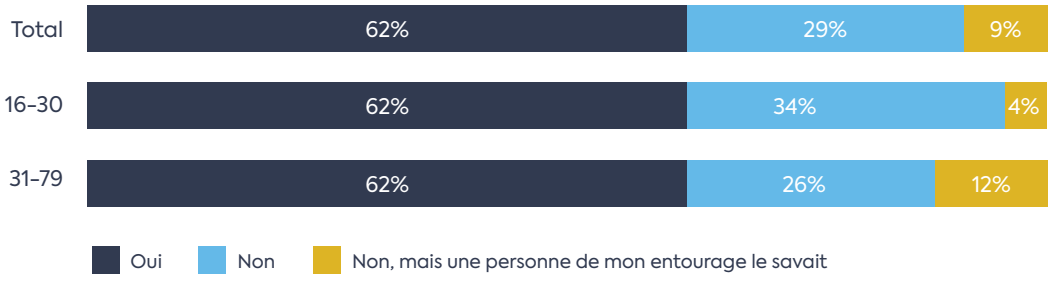
Source : Étude Indiville

Ces résultats soulignent l'importance d'une éducation et d'une sensibilisation ciblées à la sécurité en ligne, spécifiquement destinées aux jeunes. Il est crucial d'inculquer à ceux et celles-ci les connaissances et compétences nécessaires pour se protéger contre les attaques de phishing et d'autres formes de fraude en ligne.

Nous ne savons pas quoi faire lorsque nous tombons dans le piège

62 % seulement des Belges victimes de phishing savaient **quelles démarches entreprendre**.

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

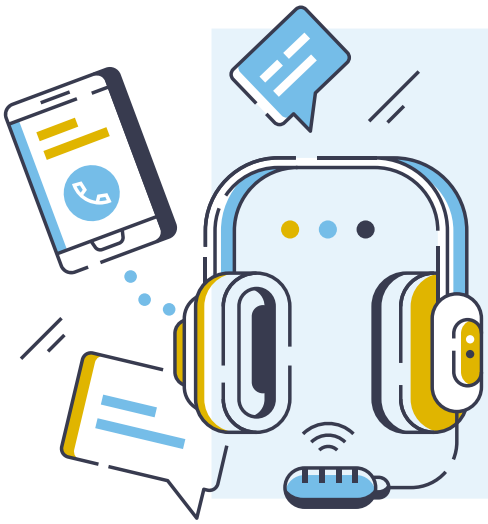


Source : Étude Indiville

CARD STOP 078 170 170 24/24

VICTIME DE PHISHING ? SUIVEZ CES ÉTAPES :

- Appelez Card Stop au 078 170 170 pour bloquer votre carte bancaire.
- Contactez le plus rapidement possible votre banque pour faire bloquer également votre application bancaire. Toutes les coordonnées des banques en cas de fraude sont répertoriées sur le site web de Card Stop.
- Portez plainte à la police.



SAVIEZ-VOUS QUE...

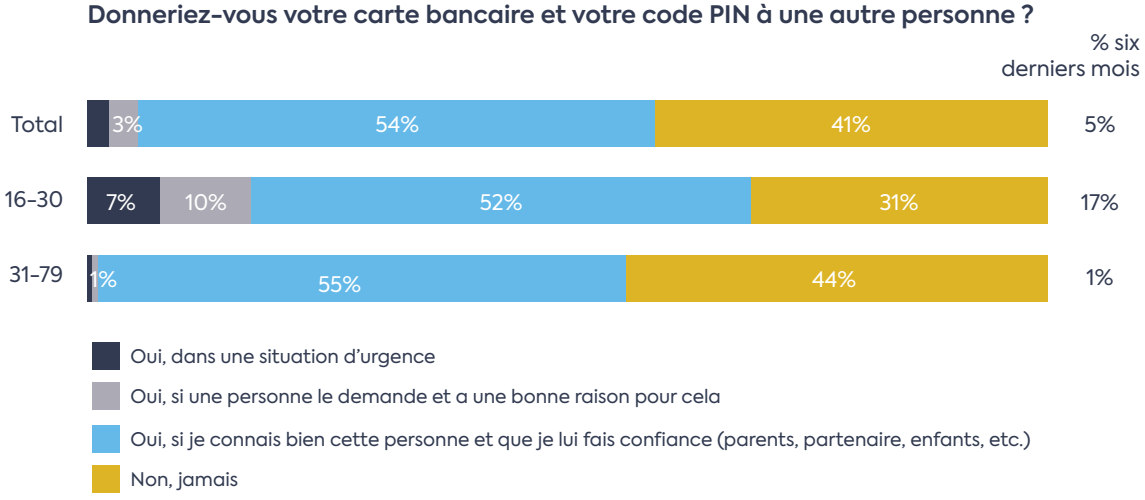
Les banques sont disponibles en permanence en cas de fraude en ligne ?
Les cybercriminels peuvent commettre des infractions à tout moment, même après les heures de bureau ou le week-end. C'est pour cette raison qu'en cas de fraude en ligne, il est important que les banques offrent un service continu à la clientèle. Ainsi, les banques sont joignables 24 heures sur 24 et 7 jours sur 7 via des numéros spéciaux de lutte contre la fraude.

MULES FINANCIÈRES

Ce n'est pas une bonne idée de prêter votre carte bancaire et votre code PIN

Votre carte bancaire et votre code PIN sont strictement personnels. Le but n'est surtout pas de les partager avec des inconnu-e-s. Selon l'étude, **5 %** des Belges donneraient malgré tout leur carte bancaire et leur code PIN à une personne qu'ils ou elles ne connaissent pas, en échange d'argent. Et les 16-30 ans s'avèrent à nouveau plus vulnérables que les plus âgé-e-s : **17 % des jeunes le feraient**, ce qui confirme les chiffres de 2022.

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



Source : Étude Indiville

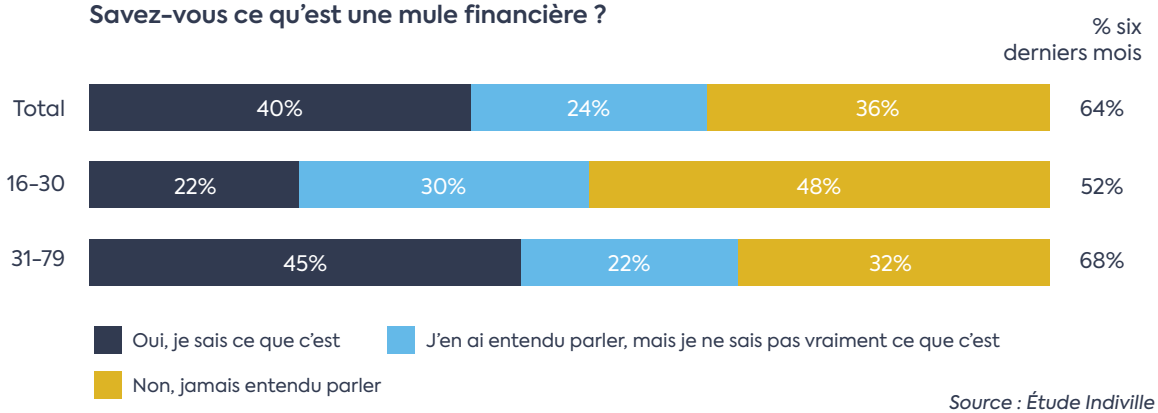
Ne gâchez pas votre vie en devenant une mule financière

Prêter votre carte bancaire à une tierce personne en échange d'argent, autrement dit devenir une mule financière, peut avoir de **sérieuses conséquences** sur votre vie. Bien que 40 % de la population sache ce qu'est une mule financière, ce pourcentage est nettement inférieur chez les jeunes. Seuls 22 % d'entre eux et elles sont capables d'expliquer clairement ce qu'est une mule financière. Ce manque de connaissances a aussi pour conséquence que les jeunes ne sont pas suffisamment conscient-e-s des dangers encourus et du fait qu'il s'agit d'une infraction pénale.

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. Les criminels peuvent ainsi déposer cet argent obtenu illégalement sur le compte bancaire de la mule financière pour ensuite le retirer (avec la carte bancaire et le code PIN de celle-ci) ou le transférer vers d'autres comptes. Les escrocs restent ainsi hors d'atteinte.

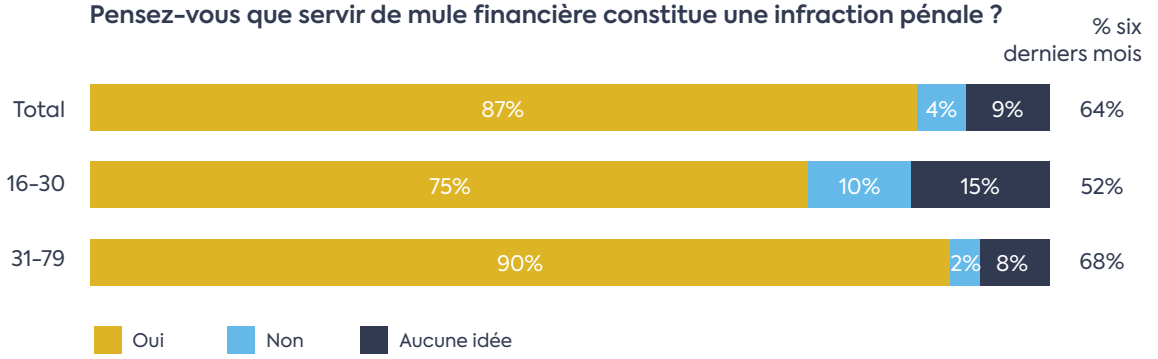
Savez-vous ce qu'est une mule financière ?



Source : Étude Indiville

Il est étonnant de constater que 10 % des jeunes sont même convaincus que faire la mule financière ne constitue pas une **infraction pénale**. Cela les rend vulnérables à la tromperie et les expose à d'éventuelles poursuites. Sur les 7 % de jeunes à qui l'on a déjà demandé de devenir une mule financière, 3 sur 4 auraient répondu positivement à cette demande.

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



Source : Étude Indiville

Il est donc très important de tenir les jeunes informé-e-s du phénomène des mules financières, des risques que celles-ci courent et des sanctions auxquelles elles s'exposent.

LA SÉCURITÉ EN LIGNE DEMEURE LA PRIORITÉ ABSOLUE POUR LES BANQUES

Il est essentiel pour le secteur bancaire d'assurer la sécurité des opérations bancaires en ligne et de prévenir les pratiques frauduleuses. Grâce à **des partenariats, des projets innovants, un suivi intensif, des programmes éducatifs et la sensibilisation**, le secteur bancaire s'efforce de prévenir autant que possible les tentatives de fraude, d'accroître les connaissances sur la sécurité bancaire et diverses formes de fraude en ligne, et ce afin de mieux protéger la population contre les dangers de la cybercriminalité.

UN SUIVI INTENSIF ET DES PROJETS INNOVANTS SONT UTILES

La grande majorité des virements frauduleux effectués dans le cadre du phishing sont détectés, bloqués ou récupérés

Les banques prennent de multiples mesures pour assurer la sécurité des systèmes bancaires et permettre aux client-e-s d'effectuer leurs transactions en toute sécurité. Les banques **assurent constamment le suivi des transactions** pour déceler les comportements suspects. Lorsque la banque détecte un ordre de paiement suspect, celui-ci n'est pas immédiatement traité. Des contrôles supplémentaires sont d'abord effectués. Dans certains cas, la banque peut contacter directement le ou la client-e pour vérifier l'ordre de paiement. Un suivi intensif peut également prévenir de nombreux préjudices :

Environ 75 % de tous les virements frauduleux effectués dans le cadre du phishing sont détectés et bloqués ou récupérés.

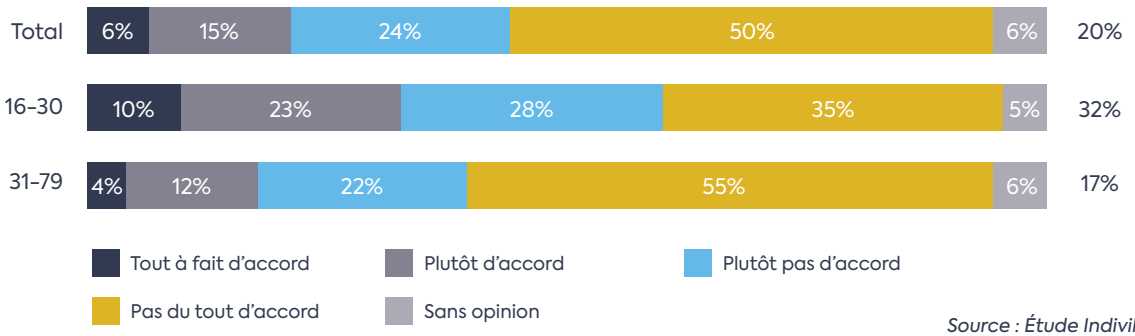
Authentification dans le cadre d'achats en ligne

Depuis une dizaine d'années, les banques mettent en œuvre divers systèmes, comme l'**authentification forte du ou de la client-e (« Strong Customer Authentication » ou SCA)**, qui visent à sécuriser les transactions effectuées dans le cadre des services bancaires en ligne et mobiles. La SCA accroît la protection des consommateur-rice-s en leur demandant de prendre des mesures supplémentaires pour confirmer leur identité lors de leurs achats en ligne ou de la signature de paiements. Cette mesure vise à prévenir la fraude et à protéger les client-e-s contre les transactions frauduleuses.

Le principe de cette forme d'authentification est que le ou la client-e s'identifie au moyen de deux facteurs ou plus. Ceux-ci ont trait à la connaissance (quelque chose que seul-e l'utilisateur-rice sait), à la possession (quelque chose que seul-e l'utilisateur-rice détient) et à l'identité (quelque chose que l'utilisateur-rice est). Vous n'utilisez habituellement qu'un de ces facteurs, souvent un mot de passe, pour prouver qui vous êtes, mais il est obligatoire d'en utiliser deux ou plus pour effectuer des opérations bancaires mobiles et sur internet.

Note positive : **de moins en moins de Belges (20 %) considèrent que ces mesures de sécurité sont superflues**. C'est mieux que les dernières années : en 2022, 26 % des Belges estimaient que les mesures de sécurité dans le cadre des achats en ligne étaient superflues, alors que ce pourcentage était encore de 33 % en 2021.

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



Source : Étude Indiville

Ce sont surtout les **jeunes** qui semblent encore faire preuve d'une certaine **nonchalance** à cet égard. En effet, 32 % des 16-30 ans considèrent les mesures de sécurité comme un obstacle (contre 38 % en 2021). Heureusement, l'**évolution est aussi positive** chez les jeunes, ce qui prouve que le secteur doit continuer à expliquer pourquoi cette sécurité intégrée va dans l'intérêt des client-e-s.

Procédure « Mule Stop »

Une autre initiative dans la lutte contre la fraude en ligne est la procédure **« Mule Stop »**, introduite en 2020. Cette procédure permet à **la banque de la victime de demander à la banque de la mule financière de bloquer le montant frauduleusement transféré**. Les banques peuvent ainsi agir rapidement et limiter le préjudice financier lorsque des mules financières sont impliquées dans des transactions frauduleuses.

Vérification du nom de l'IBAN

Le secteur bancaire travaille aussi à la mise en œuvre d'une **vérification du nom de l'IBAN** pour les virements numériques. Ce contrôle vise à lutter contre des formes spécifiques de fraude, en particulier la fraude à la facture. Lors de la saisie d'un ordre de virement, la banque vérifie si le numéro de compte (IBAN) correspond au nom du ou de la bénéficiaire. Si ce n'est pas le cas, elle en informe le ou la consommateur-rice avant que le virement ne soit effectué. Ce dernier ou cette dernière peut alors décider de confirmer ou non l'ordre de virement. Cette vérification du nom de l'IBAN constitue donc une mesure de sécurité supplémentaire.

PARTENARIATS AVEC LES PARTIES PRENANTES DE TOUS LES SECTEURS

Le secteur financier reconnaît l'importance d'une coopération étroite et continue avec le **secteur des télécommunications** et les **autres parties prenantes concernées** pour assurer la sécurité de leurs client-e-s.
Un exemple impressionnant de cette collaboration est le blocage efficace du « **spoofing** ». Grâce à ces efforts, environ 100.000 numéros de téléphone de banques ont déjà été bloqués, ce qui signifie qu'ils ne peuvent plus être utilisés par les fraudeurs qui recourent au spoofing.

La collaboration entre les fournisseurs belges d'accès à internet, le Centre pour la Cybersécurité Belgique et Febelfin constitue un autre excellent exemple de partenariat. Nous avons développé ensemble une procédure et un système, le Belgium Anti-Phishing Shield, qui met les internautes en garde contre des sites web dangereux. En 2022, la collaboration avec la population a permis d'éviter pas moins de 14 millions de clics vers des sites suspects, soit environ 25 avertissements aux internautes par minute[4].

Ces partenariats stratégiques permettent d'ériger une **ligne de défense** solide contre les numéros de téléphone frauduleux et les sites web dangereux. La police et la justice ont pour responsabilité de détecter, d'arrêter et de poursuivre les criminels, une tâche particulièrement complexe et de grande ampleur dans le cadre de la fraude en ligne. Il semble opportun d'optimiser la coopération et l'organisation avec **la police et la justice**. En intervenant ensemble, nous construisons un environnement numérique plus sûr pour la population et contribuons à la lutte globale contre la cybercriminalité.

Dans le cadre du **spoofing**, un escroc peut faire apparaître sur l'écran de votre téléphone non pas son propre numéro de téléphone, mais un numéro de téléphone différent.

Smishing : phishing par SMS.

[4] 14 millions de clics vers des sites suspects évités en 2022 grâce au système unique « anti-phishing shield » | Centre pour la Cybersécurité Belgique (belgium.be)

SENSIBILISATION

Modules pour apprendre à faire face au phishing

Febelfin soutient les initiatives de partenaires tels que la Belgian Cyber Security Coalition et le Centre pour la Cybersécurité Belgique, qui ont lancé une série de formations en ligne « Surfer sans soucis ». L'un des modules, intitulé « Regarde où tu vas », est maintenant disponible sur le site web de Safeonweb. Ce module contient des vidéos informatives qui donnent des conseils pour détecter les liens frauduleux.

À la fin du module, un questionnaire vous permet de tester vos (nouvelles) connaissances.

Febelfin coopérera en outre de nouveau avec le Centre pour la Cybersécurité Belgique et la Cyber Security Coalition en 2023, dans le cadre d'une vaste campagne de lutte contre le phishing.

Une information adaptée aux jeunes

La protection des jeunes contre la cybercriminalité constitue l'une des priorités du secteur bancaire. Febelfin sait l'importance d'être présente sur tous les canaux utilisés par la jeune génération pour s'informer : les médias sociaux (YouTube, TikTok...) et un site web spécifique : « financesetmoi.be ». Il est de notre responsabilité commune de veiller à ce que les jeunes aient accès à des informations correctes et objectives pour les sensibiliser aux pièges et aux risques de la fraude en ligne, comme les « finfluenceur-se-s ».

finances &moi

Nouveau : formation en ligne « effectuer en toute sécurité des opérations bancaires en ligne » pour les accompagnateur-rice-s numériques

Febelfin a récemment développé une nouvelle formation en ligne pour les coachs numériques, c'est-à-dire des **bénévoles ou professionnel-le-s** qui **aident les gens** à développer leurs compétences numériques. La formation en ligne comprend un chapitre distinct sur la manière d'effectuer en toute sécurité des opérations bancaires en ligne et les différentes formes de fraude. Febelfin souhaite partager ainsi ses connaissances et permettre au plus grand nombre d'effectuer des opérations bancaires et des paiements en ligne en toute sécurité. La formation numérique est gratuite et proposée en français et en néerlandais.

Séances d'information et webinaires

Febelfin organise par ailleurs de nombreuses **séances d'information** présentielles et en ligne, ainsi que des **webinaires**, sur la manière d'effectuer en toute sécurité des opérations bancaires et des paiements en ligne, éventuellement complétés par une explication des différentes formes de fraude. Nous parcourons toute la Belgique pour organiser de telles sessions et sensibiliser la population.

Efforts conjoints et sensibilisation, la clé de la lutte contre la cybercriminalité

Ce n'est qu'en **unissant nos forces pour lutter contre la cybercriminalité et en sensibilisant continuellement** la population que nous pourrons réduire la cybercriminalité. Le secteur financier s'engage activement dans la lutte contre la fraude.

Il est essentiel que **les banques, les autorités (police, justice), les entreprises, le monde universitaire et la société dans son ensemble** collaborent pour prendre des mesures efficaces afin d'améliorer les connaissances sur la sécurité et la fraude en ligne. Nous pouvons résolument faire face aux défis du monde numérique en apprenant, en innovant et en échangeant des informations, tous et toutes ensemble. Il y va de notre responsabilité conjointe de veiller à ce que tout le monde, jeunes et moins jeunes, puisse naviguer en toute sécurité dans le monde numérique. Si nous continuons à collaborer et à accroître la sensibilité à cette problématique, nous pouvons **créer un environnement numérique résilient et sécurisé pour les générations présentes et à venir**.

Fédération belge du secteur financier

www.febelfin.be