Ne mordez pas à l'hameçon

Le point sur la fraude et l'escroquerie

febelfin

Aujourd'hui, nous sommes tous en ligne, plus que jamais. La pandémie de coronavirus de 2020 a encore accéléré la vie numérique. Elle a entraîné toute une série de changements, mais aussi provoqué une augmentation du nombre de messages frauduleux, qui circulent constamment.

La fraude sur Internet est omniprésente aujourd'hui. Tout Belge a déjà au moins une fois été victime d'une tentative de fraude en ligne. Mais tout n'est pas sombre : malgré les nombreuses tentatives de fraude, il ressort des chiffres de 2021[1] que les cas de phishing réussis ont diminué d'un quart. Nous assistons toutefois à une transition vers d'autres formes de fraude.

Où en sommes-nous aujourd'hui ? Comment évolue la fraude en ligne et quelles en sont les formes actuelles ? Nous vous dévoilons ici les résultats de l'enquête annuelle[2] réalisée par Febelfin en collaboration avec le bureau d'études IndiVille.

PHISHING : LA PÊCHE AUX CODES SECRETS

Les fraudeurs mettent la main sur les codes les codes bancaires personnels de leurs victimes potentielles en se faisant passer pour une organisation connue ou de confiance. Pour parvenir à leurs fins, ils envoient un courrier électronique, un SMS, un message sur WhatsApp, Facebook Messenger ou d'autres médias sociaux... Celui-ci contient un lien vers un site web, souvent presque parfaitement imité, via lequel la victime introduit ses codes bancaires personnels. Lorsqu'ils arrivent à s'approprier ces données, les fraudeurs effectuent des transactions au nom de la victime et vident son compte.

LE SAVIEZ-VOUS ?

Le terme « phishing », ou hameçonnage en français, a été utilisé pour la première fois en 1996, lorsque des pirates informatiques ont tenté de voler les mots de passe d'utilisateurs d'America Online (désormais AOL). Une opération qu'ils comparaient au « fishing », la pêche sportive. Ces « pêcheurs » jetaient en effet des lignes dans la « mer » des internautes, avec leurs faux courriers électroniques. C'est comme lorsque l'on pêche à la ligne : il suffit que quelques personnes mordent à l'hameçon pour que le phishing soit un succès.

Le nombre de tentatives de phishing reste élevé aujourd'hui, et aucun secteur n'est épargné. Heureusement, tout n'est pas sombre : le nombre de tentatives de phishing réussies diminue. En 2020, 34 millions d'euros avaient été dérobés en recourant à cette forme de fraude. En 2021, on a observé une nette diminution de 9 millions d'euros, soit plus de 26 %. Grâce à la coopération entre les différentes parties prenantes, aux efforts des banques et aux différentes campagnes de sensibilisation, moins de hameçonneurs ont pu passer à l'action. La surveillance accrue exercée par les banques a aussi permis de limiter considérablement les dégâts : en 2021, pas moins de 75 % de tous les virements frauduleux effectués dans le cadre de tentatives de phishing ont été bloqués ou récupérés.

Malheureusement, nous avons également constaté une importante transition vers d'autres formes de fraude en 2021, comme la fraude à l'investissement, la fraude à la facture, la fraude à la demande d'aide ou la fraude aux comptes à sécurité renforcée, dans le cadre desquelles la victime est poussée à transférer elle-même de l'argent. Les fraudeurs utilisent différents canaux, comme le courrier électronique, la lettre, le téléphone, les SMS, les médias sociaux et WhatsApp. Ils fraudent en se faisant passer pour les représentants de diverses organisations et institutions, comme des banques, des administrations, des opérateurs de télécommunications, des services publics, etc. La coopération est donc essentielle dans la lutte contre les fraudeurs en ligne, en 2022 et les années à venir.

[1] Les chiffres sur le phishing en 2021 | Febelfin

[2] *Enquête IndiVille réalisée en février-mars 2022, sur un échantillon représentatif de la population belge n : 2 164 enquêtes NL/FR, dans la tranche d'âge 16-79 ans.*

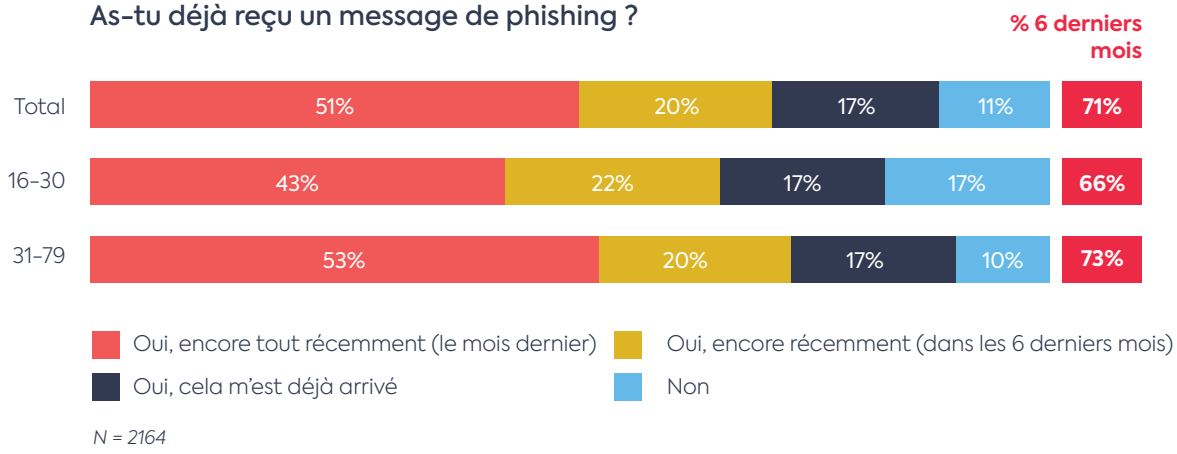
LES TENTATIVES DE PHISHING CONTINUENT D'AUGMENTER

71%

des personnes interrogées ont ainsi reçu un message de phishing au cours des 6 derniers mois.

Même s'il y a eu moins de tentatives **fructueuses** en 2021, le problème du phishing ne cesse de croître. Le **nombre de tentatives de phishing augmente** en effet encore en 2022. 71 % des personnes interrogées ont ainsi reçu un message de phishing au cours des 6 derniers mois. Il s'agit d'une nette augmentation par rapport à 2021, année au cours de laquelle 34 % des répondants ont reçu un message de phishing.

As-tu déjà reçu un message de phishing ?



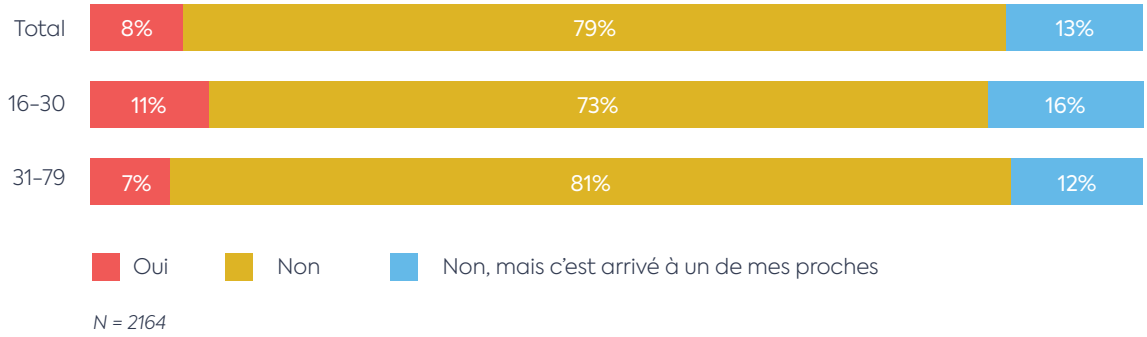
N = 2164

8%

des personnes interrogées ont déjà répondu à une message frauduleux

Parmi les personnes ayant reçu ce genre de message frauduleux, 8 % y ont donné suite. Cela montre l'importance de continuer à sensibiliser la population à la fraude en ligne et d'aider les gens à reconnaître les messages frauduleux.

As-tu déjà été victime de phishing ?



N = 2164

QUELLES MESURES DEVEZ-VOUS PRENDRE SI VOUS ÊTES VICTIME DE PHISHING ?

- **Contactez immédiatement votre banque.**
- **Appelez Card Stop au 078 170 170 pour bloquer vos cartes bancaires.**
- **Portez plainte auprès de la police.**

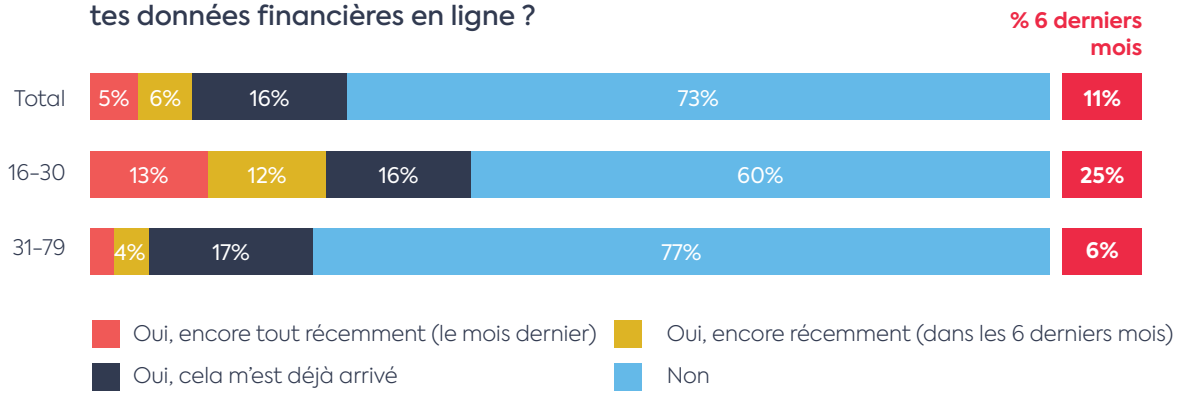
Communiquez-vous sans hésiter des données financières à des inconnus ?

11%

des interrogés ont communiqué, au cours des 6 derniers mois, des données financières qu'ils ne se sentaient pas à l'aise de transmettre

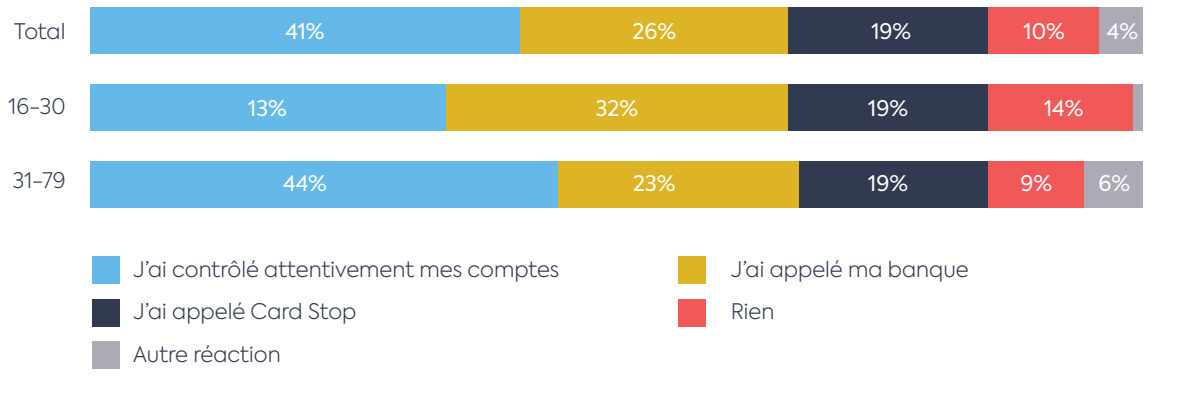
En général, 11 % des Belges interrogés ont communiqué, au cours des 6 derniers mois, des données financières qu'ils ne se sentaient pas à l'aise de transmettre.
Cela représente une augmentation par rapport à 2021, où ils n'étaient que **7 %** dans ce cas.
Une note positive à cet égard : **90 %** de ces personnes ont agi et **contrôlé** leur compte, ou **contacté la banque ou Card Stop** après avoir communiqué des données financières.

T'es-tu déjà senti mal à l'aise après avoir transmis tes données financières en ligne ?



N = 2164

Et qu'as-tu fait alors ?



N = 607

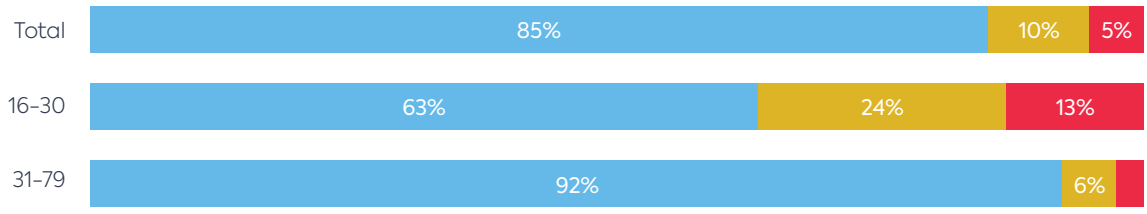
Vos codes bancaires svp

5%

de la population transmet sans hésitation ses codes bancaires

Et pourtant, certains transmettraient leurs codes bancaires sans hésiter si leur banque les leur demandait. Il s'agit de 5 % de la population. Parmi les jeunes de 16 à 30 ans, ce chiffre s'élève même à 13 %, ce qui est particulièrement alarmant. **Votre banque ne vous demandera jamais vos codes secrets**. Attention : lorsqu'un prétendu employé de votre banque le fait, vous avez un fraudeur en ligne !

Si ma banque demande mes codes bancaires via e-mail, sms, whatsapp, téléphone...



- Je ne les transmets en aucun cas
- Il y a une possibilité que je les donne, mais je vérifierai d'abord très attentivement si l'e-mail et le site web de référence ont l'air légitimes
- Je les communiquerai

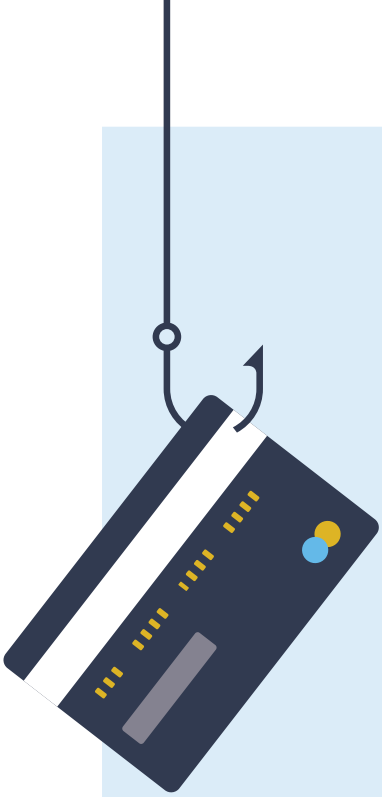
N = 2164

On constate également une recrudescence du phishing à la carte bancaire et du phishing à la carte bancaire à domicile. **6 %** des Belges (contre 3 % en 2021) **donneraient leur carte bancaire avec code PIN à quelqu'un qu'ils ne connaissent pas. Ici aussi, le pourcentage parmi les jeunes s'élève à 16 %.**

Donnerais-tu ta carte bancaire et ton code pin à quelqu'un d'autre ?

- Oui, si quelqu'un est vraiment dans le besoin
- Oui, si quelqu'un me le demande et qu'il a une bonne raison pour cela
- Oui, si je connais bien cette personne et que je lui fais confiance (par ex. parents, partenaire, enfants...)
- Non, jamais

N = 2164



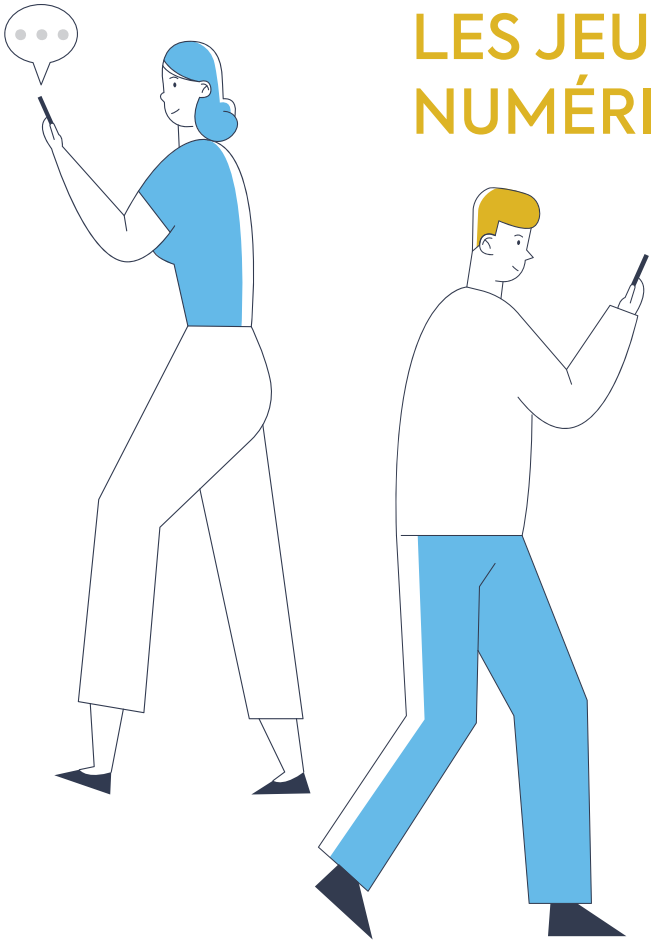
QU'EST-CE QUE LE PHISHING À LA CARTE BANCAIRE ?

Les fraudeurs essaient d'obtenir directement de vous **votre carte bancaire et ses codes**. Comment procèdent-ils ?

- Vous recevez un courrier électronique ou un SMS de votre « banque » indiquant que votre carte de débit doit être remplacée. Vous devez soi-disant restituer votre ancienne carte de débit, en vue de son recyclage, avant que la nouvelle carte ne vous soit envoyée.
- Le lien contenu dans le courrier électronique ou le SMS vous conduit au faux site web. Les fraudeurs vous demandent alors ce qui suit :
  - Introduire vos données personnelles et votre numéro de carte ;
  - Introduire votre code PIN actuel et choisir un nouveau code PIN ;
  - Envoyer votre carte de débit actuelle par la poste.

Dans le cas du phishing à la carte bancaire à domicile, les escrocs viennent chez vous, en se faisant passer pour votre banquier, et vous aident à vous connecter à votre environnement bancaire en ligne. Cela leur permet bien sûr de regarder par-dessus votre épaule et de voir vos codes. Les escrocs demanderont aussi à récupérer votre carte bancaire et et se volatiliseront avec.

SOUVENEZ-VOUS : Votre banque ne viendra jamais à votre domicile pour récupérer votre carte. Elle ne vous demandera jamais non plus de renvoyer votre carte bancaire ou de communiquer votre code PIN. Refusez toujours de le faire !



LES JEUNES : DES ENFANTS DU NUMÉRIQUE MULTITÂCHES ?

Malheureusement, les jeunes obtiennent les plus mauvais résultats dans cette enquête. On suppose trop souvent qu'ayant grandi à l'ère numérique, ils sont également bien informés sur les services bancaires et la sécurité en ligne. S'il est vrai qu'ils maîtrisent toutes sortes de gadgets numériques et sont au courant des dernières tendances en ligne, il ressort pourtant de l'enquête qu'ils sont beaucoup moins au fait de la sécurité en ligne.

Si l'on se fie au Baromètre de l'Inclusion numérique de la Fondation Roi Baudouin (FRB)[3] , près d'un jeune âgé de 16 à 24 ans sur trois (33 %) a de faibles compétences numériques générales. Des enfants du numérique multitâches ? Pas tout à fait...

Il ressort aussi de l'enquête de la FRB que 97 % des jeunes disposent d'un smartphone. Cela les rend encore plus vulnérables, car nous nous faisons souvent plus facilement piéger lorsque nous sommes « très occupés » sur notre portable.

[3] Baromètre de l'Inclusion numérique 2022

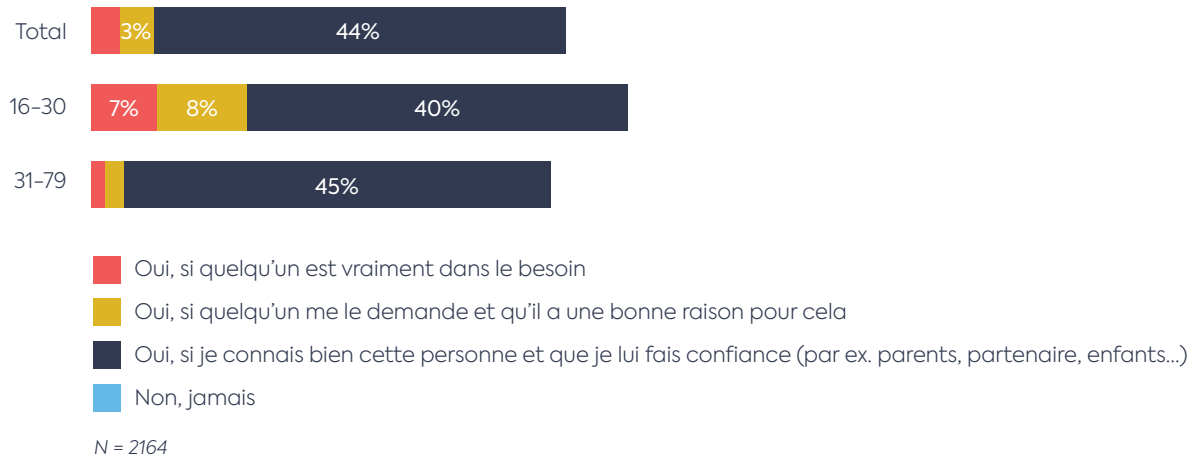
Pas assez attentifs à la sécurité en ligne des données bancaires

25%

des jeunes ont communiqué des données financières qu'ils ne se sentaient pas à l'aise de transmettre

Une grande partie des jeunes ne sont pas assez attentifs à la sécurité en ligne. Relevons quelques chiffres inquiétants de l'enquête : parmi les jeunes de 16 à 30 ans interrogés, pas moins de 25 % ont communiqué, au cours des 6 derniers mois, des données financières qu'ils ne se sentaient pas à l'aise de transmettre. Il ne s'agit pas seulement d'une augmentation importante par rapport à 2021, où ce pourcentage était d'environ 17 %. C'est aussi **beaucoup plus élevé que parmi les adultes** (11 %).
De même, **16 %** des jeunes interrogés **transmettraient sans hésiter leurs codes bancaires si leur « banque » les leur demandait**. C'est une évolution très négative : en 2021, seuls 8 % des jeunes interrogés l'auraient fait.

Donnerais-tu ta carte bancaire et ton code pin à quelqu'un d'autre ?



N = 2164

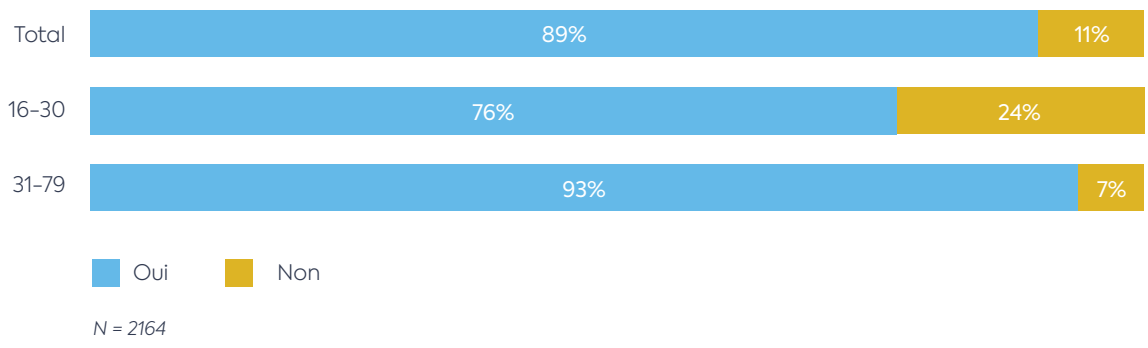
1 jeune sur 4 ne connaît pas le mot « phishing »

24%

des jeunes n'ont jamais entendu le mot « phishing »

C'est clairement un gros problème. En raison de leurs faibles compétences numériques générales, les jeunes sont également plus vulnérables lorsqu'ils sont confrontés au phishing. 24 % des jeunes n'ont jamais entendu ce mot. C'est une légère amélioration, car 30 % n'avaient jamais entendu parler de phishing en 2021.

As-tu déjà entendu parler de phishing ?



N = 2164

LES JEUNES COMME MULES FINANCIÈRES

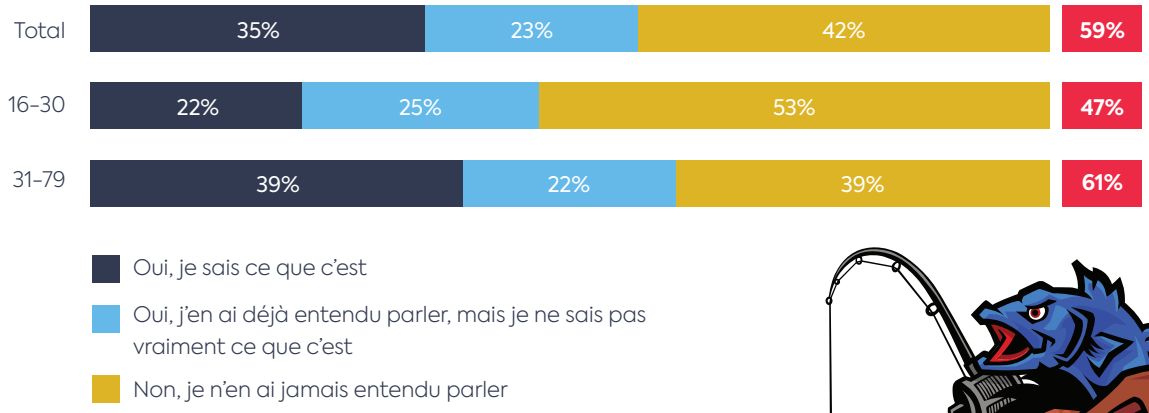
78%

des jeunes ne savent pas ce qu'est une mule financière.

Ce manque de sensibilisation des jeunes à l'importance de la sécurité en ligne les rend également plus susceptibles de devenir des mules financières. **16 %** des jeunes **prêteraient leur carte bancaire** à quelqu'un qu'ils ne connaissent pas, en échange d'argent. La situation a empiré par rapport à l'année passée, où ils n'étaient que 9 %. Une personne qui fait ça devient une mule financière et peut **faire l'objet de sanctions**.

Le problème est que très peu de jeunes savent ce qu'est une mule financière. Presque **8 sur 10** d'entre eux n'en ont aucune idée. À peine **22 %** savent ce qu'est une mule financière et, même dans ce cas, ils sont peu conscients des dangers encourus.

Sais-tu ce qu'est une mule financière ?



Pourtant, le phénomène n'est plus marginal : les criminels recrutent les jeunes à la sortie des écoles, dans les lieux festifs ou à proximité des gares, mais aussi en ligne. Et ce n'est plus une exclusivité des grandes villes : **10 %** des jeunes interrogés ont **déjà été approchés** pour devenir une mule financière. En 2021, ils n'étaient encore que 6 %. Et **13 % des jeunes connaissent quelqu'un** qui a été **approché** pour devenir une mule financière.

Les escrocs deviennent par ailleurs de plus en plus créatifs en matière de blanchiment d'argent et d'utilisation des mules financières. Ils ne se limitent plus à demander la carte bancaire et le code PIN, mais aussi, de plus en plus fréquemment, la carte d'identité (ou une copie de celle-ci), le numéro de portable et les coordonnées. Autant d'informations qui peuvent également faciliter la fraude que projettent les criminels.

QU'EST-CE QU'UNE MULE FINANCIÈRE ?

Une mule financière met son compte bancaire et/ou sa carte bancaire et ses codes à la disposition de criminels. Ces derniers utilisent les mules financières pour **faire circuler de l'argent obtenu illégalement** (par ex. dans le cadre du phishing) et le faire parvenir **entre leurs mains**. Les criminels promettent aux mules financières qu'elles gagneront rapidement et facilement de l'argent, en contrepartie du prêt de leur compte bancaire et/ou de leur carte bancaire et de leur code PIN.

Servir de mule financière est-il punissable ?

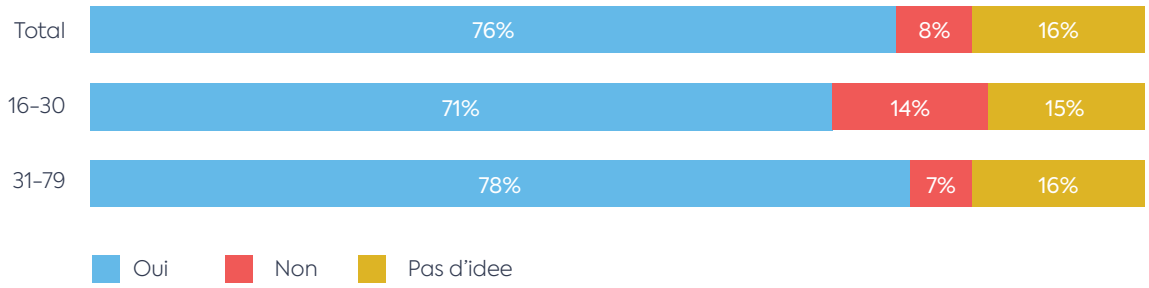
14%

des jeunes interrogés pensent que servir de mule financière ne constitue pas une infraction.

14 % des jeunes interrogés pensent que servir de mule financière n'est pas punissable. Ils se trompent : prêter sa carte bancaire et ses codes revient à participer à un blanchiment d'argent, et c'est bien un acte punissable. Les conséquences sont souvent graves :

- Une mule financière peut être tenue responsable et poursuivie. Elle risque dans ce cas de lourdes amendes juridiques et fiscales, voire une peine de prison.
- Une condamnation aura également une incidence sur la relation future avec les banques.
- Qui plus est, la mule financière risque que le hameçonneur vide son compte.

A ton avis, la mule financière court-elle, elle-même, un risque ?



LES BANQUES ET LA LUTTE CONTRE LA FRAUDE

QUELQUES FAITS SUR LA FRAUDE

- L'année dernière, **47 917** cas de fraude ou d'escroquerie ont été signalés au Point de contact du SPF Économie.
- Cela représente une moyenne de **131** signalements par jour.
- Plus de la moitié étaient liés au **phishing ou à de faux sites web**.
- Il s'agit du deuxième plus grand nombre jamais enregistré, après 2020, année exceptionnelle marquée par la pandémie de coronavirus, au cours de laquelle plus de 55 000 signalements ont eu lieu. Depuis le lancement du Point de contact, en 2016, ce nombre a doublé.

Les services bancaires en ligne sont extrêmement populaires : la majorité des gens (**91 %**) privilégient **les paiements en ligne** et ce pourcentage continuera d'augmenter. La sécurité en ligne est donc une priorité absolue pour les banques belges.

Celles-ci se démènent pour assurer la sécurité des systèmes bancaires et permettre aux clients d'effectuer leurs transactions en toute sécurité :

- Les services bancaires en ligne passent toujours par une **connexion sécurisée**.
- Pour y accéder, vous devez toujours vous **identifier** et confirmer votre identité.
- Les ordres de paiement doivent toujours **être signés numériquement**. Vous acceptez ainsi l'exécution de l'ordre de paiement.
- Vous êtes **automatiquement déconnecté** de la banque en ligne si aucune activité n'a lieu durant un certain laps de temps.
- Au sein des banques, des **experts en matière de sécurité** surveillent et analysent en permanence les techniques utilisées par les cybercriminels afin d'adapter les mesures de sécurité.

- Les banques surveillent les transactions pour détecter les comportements suspects. Si une banque constate **un ordre de paiement suspect**, elle ne le traite pas immédiatement. Elle procède d'abord à un certain nombre de vérifications complémentaires. Dans ce cadre, elle peut contacter directement le client pour confirmer l'ordre de paiement. C'est ainsi que 75 % de tous les transferts frauduleux, dans le cadre d'une tentative de phishing, sont détectés ou récupérés.

Plusieurs mécanismes de sécurité sont donc mis en œuvre. Mais nous savons aussi qu'un quart (26 %) des Belges trouvent ces mesures, comme l'authentification en deux étapes, plutôt inutiles. Cette proportion est encore plus élevée parmi les jeunes (38 %). Une grande partie de la population considère donc que ces mesures constituent plutôt un obstacle. C'est à la fois intéressant et inquiétant, car elles servent avant toute chose à garantir la sécurité des consommateurs. Les banques doivent faire constamment un numéro d'équilibriste à cet égard :

- Les banques veulent garantir des paiements fluides et maximiser la facilité d'utilisation pour le consommateur.
- Parallèlement, elles veulent bien sûr garantir une sécurité suffisante et essayer de bloquer et de récupérer les transactions frauduleuses qui sont, malgré tout, souvent correctement signées, parce que des codes ont été transmis. Cela requiert des investissements continus et le déploiement permanent de personnel et d'infrastructures de la part du secteur bancaire.

QU'EST-CE QUE LA VÉRIFICATION OU VALIDATION EN DEUX ÉTAPES, AUSSI APPELÉE « AUTHENTIFICATION À DEUX FACTEURS » ?

Pour accéder à votre compte, vous devez prouver que vous êtes bien la personne que vous prétendez être. Vous pouvez le faire de 3 manières ou avec 3 facteurs :

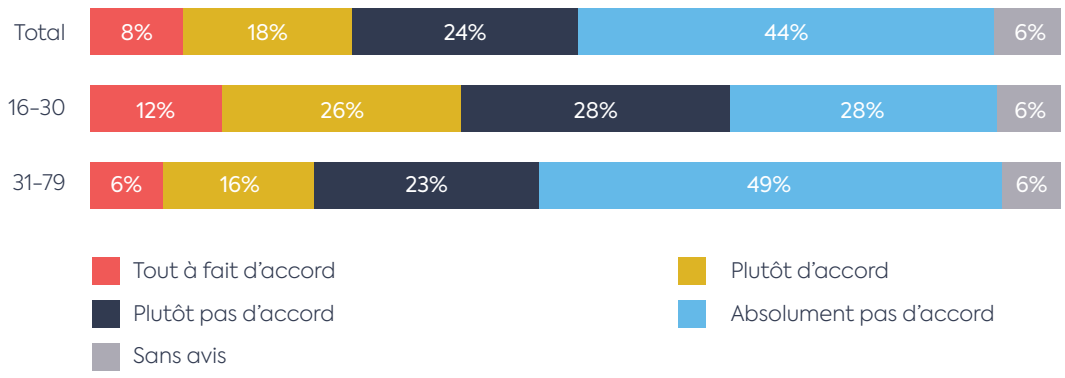
*avec quelque chose que vous seul **connaissez** (votre mot de passe ou code PIN)*

*avec quelque chose dont vous seul **disposez** (votre téléphone ou un dispositif de confiance, aussi appelé token)*

*avec quelque chose de votre **personne** (votre empreinte digitale, votre visage, votre iris...)*

Vous utilisez généralement l'un de ces facteurs, souvent un mot de passe, pour prouver qui vous êtes, mais il est préférable d'en utiliser deux ou plus : c'est l'authentification à deux ou plusieurs facteurs (2FA ou MFA). À titre d'exemple, vous utilisez un mot de passe et, en complément, un code est envoyé sur votre téléphone portable. Ou vous utilisez votre empreinte digitale et une application pour obtenir un accès.

Je trouve superflu de devoir parcourir les différentes étapes lorsque je fais des achats en ligne



N = 2164

LA SENSIBILISATION RESTE INDISPENSABLE

Le Baromètre de l'Inclusion numérique de la FRB montre que le niveau des compétences numériques générales des Belges ne progresse quasiment pas. **La sensibilisation à la sécurité en ligne et aux compétences numériques est et reste donc un impératif.** De nombreuses personnes indiquent également qu'elles aimeraient en savoir plus sur la façon d'effectuer des transactions bancaires en ligne en toute sécurité. 50 % des répondants à l'étude IndiVille se disent intéressés par une telle formation.

Entretenir les compétences numériques

Les compétences numériques ne sont bien sûr pas acquises une fois pour toutes. Il faut constamment les rafraîchir. La nature des compétences numériques évolue au gré des changements et des innovations au sein de la société, ainsi qu'avec l'introduction de nouvelles applications en ligne. Il est donc important de toujours se tenir à jour et d'être vigilant.

Quand peut-on considérer qu'on a de bonnes compétences numériques en matière de cybersécurité ?

- Êtes-vous capable de vous assurer qu'un site web est sécurisé (en vérifiant l'URL, les certificats de sécurité, etc.) ?
- Êtes-vous capable de lire et comprendre des documents, mais aussi d'effectuer des actions sur une page web, visant à limiter la collecte de vos données à caractère personnel ? Il peut s'agir de la politique de respect de la vie privée, de la divulgation restreinte de votre emplacement, de l'accès limité au contenu d'un profil personnel, du refus de collecter des données à des fins publicitaires, etc.
- Êtes-vous capable d'ajuster les paramètres d'un navigateur afin de limiter les cookies générés ?
- Pouvez-vous reconnaître certaines formes de fraude et avez-vous la puce à l'oreille lorsqu'on vous demande de transmettre des codes personnels ?

Ces compétences numériques constituent un élément important pour pouvoir se protéger en permanence contre le phishing et d'autres formes de fraude.

Protégez-vous contre la fraude en ligne

Vous pouvez vous protéger contre le phishing de nombreuses manières. La règle d'or est la suivante : ne cliquez jamais sans réfléchir sur un lien. Lorsque l'on est accaparé par les tâches sur son smartphone, on a vite fait de cliquer à la hâte sur un lien dans un message ou lors de l'installation d'une application, et ce n'est pas toujours très malin !

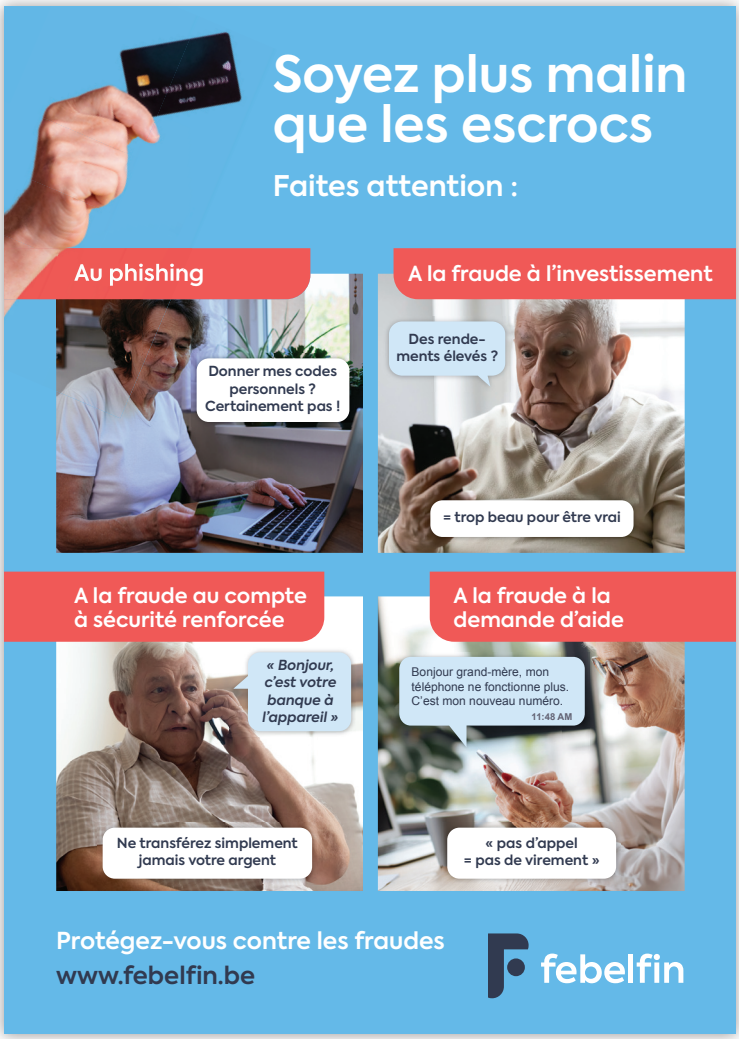
Le secteur bancaire contribue à soutenir la campagne du CCB : découvrez « OK n'est pas toujours OK » ici. Vous souhaitez être au courant des dernières cybermenaces ? Nous vous conseillons alors d'installer l'application Safeonweb. Elle a déjà été téléchargée plus de 180 000 fois et vous informe parfaitement des messages frauduleux en circulation.

CONSEIL! Si vous recevez une notification de votre PC ou smartphone indiquant qu'une mise à jour est disponible, **installez-la**. Une mise à jour remédie souvent aux vulnérabilités de votre appareil. **Comment mettre à jour votre appareil ?** Lisez-en plus sur Safeonweb : **Procédez régulièrement à des mises à jour** (safeonweb.be)

Téléchargez uniquement depuis des stores d'applis reconnus

Plus de conseils sur safeonweb.be

Febelfin sensibilise



Le secteur bancaire a indubitablement un rôle important à jouer dans la sensibilisation à la sécurité en ligne. Febelfin s'engage donc résolument dans ce domaine : outre des campagnes annuelles et des collaborations avec un large réseau de partenaires, des employés enthousiastes de Febelfin ont donné cette année **plus de 50 séances d'information et webinaires sur les opérations bancaires et les paiements numériques sécurisés à travers la Flandre et la Wallonie.**

Vu la forte demande de séances d'information sur ce thème, Febelfin est en train de mettre au point un **apprentissage en ligne gratuit** qui repose sur le principe « former le formateur », et qui peut servir de **référence** pour les professionnels et bénévoles œuvrant en faveur de la sécurité en ligne. Une fois l'apprentissage en ligne terminé, vous obtenez le certificat correspondant. En voici les grandes lignes :

- Les formes de fraude les plus pertinentes et les plus actuelles
- Un aperçu de tous les outils et matériels de sensibilisation existants
- Des recommandations sur la manière de procéder avec les débutants numériques
- Des trucs et astuces pour effectuer des opérations bancaires sécurisées
- La possibilité de poser des questions aux experts de Febelfin

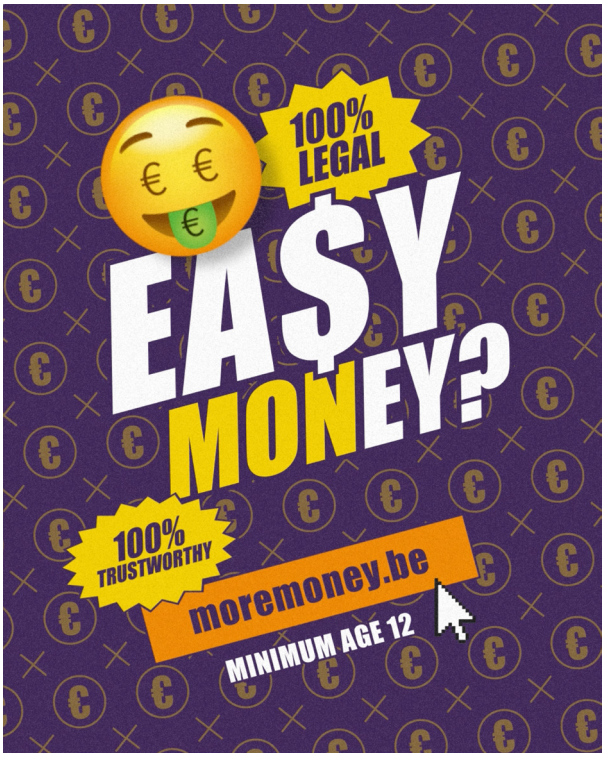
Si vous désirez de plus amples informations à ce sujet, vous pouvez toujours contacter **info@febelfin.be**. Outre les séances d'information, Febelfin propose beaucoup de **matériel de campagne et de sensibilisation gratuit** sur les différentes formes de fraude : des **posters aux autocollants, en passant par les brochures d'information**, chacun trouvera chaussure à son pied. Febelfin peut procurer les fichiers sources afin que le logo de votre organisation puisse également être mentionné.

La fraude est partout, même là où se trouve votre enfant

Le phishing, la fraude en ligne et la recherche de mules financières ont souvent lieu en coulisses. Derrière les écrans, devrions-nous dire... Sur TikTok ou Instagram, par exemple. Des canaux où ne se trouvent que des jeunes et où ils sont précisément les plus vulnérables. Car les parents n'utilisent généralement pas ces applications et ignorent donc parfois ce que voient les jeunes. Sur les réseaux sociaux, les enfants reçoivent constamment des propositions alléchantes et leurs compétences en matière de sécurité électronique sont constamment mises à l'épreuve. Nous devons en être conscients. Et si nous traitions hors ligne un problème en ligne ? Et rendions visible ce qui est souvent invisible aux parents. C'est dans ce contexte que Febelfin a développé une nouvelle campagne destinée aux jeunes, mais aussi (et surtout) aux parents. Pour qu'ils soient au courant de la fraude en ligne, qu'ils la reconnaissent et qu'ils en informent leur fils ou leur fille.

Avec une campagne à l'air libre, qui débute par un gigantesque panneau d'affichage sur la Place de la Bourse à Bruxelles, avec une publicité louche. Nous comptons sur les PR et la saine indignation de tous ceux qui la voient. Si vous vous rendez sur le lien, le message suivant s'affiche : « C'est ce que votre enfant verra en ligne. Aidez-le à reconnaître la fraude en ligne. Surfez sur protegezvousenligne.be ». Parallèlement, nous lançons une campagne sur les réseaux sociaux avec une série de témoignages.

Si vous souhaitez en savoir plus ou utiliser le matériel de campagne, veuillez contacter info@febelfin.be



LA COLLABORATION EST DÉCISIVE

Le secteur bancaire n'est toutefois pas le seul à être chargé de cette sensibilisation. La lutte contre la fraude est une responsabilité partagée. On ne peut véritablement changer les choses que si différents secteurs collaborent. Les plus grands catalyseurs de la fraude ne se trouvent en effet plus seulement dans le secteur bancaire. Ils se sont propagés à d'autres secteurs.

La fraude est un phénomène social. Tous les secteurs de la société doivent donc prendre part à la lutte, à commencer par les télécoms et les plateformes de commerce en ligne. Ce n'est qu'ensemble que nous pouvons réduire la fraude au strict minimum. La coopération peut encore grandement s'améliorer, à différents niveaux.

La sécurité des paiements est une responsabilité partagée : le secteur bancaire fournit une infrastructure numérique sécurisée, le client est informé et vigilant, la police et le parquet poursuivent les infractions, et les autorités publiques fournissent le cadre juridique adéquat. Si nous parvenons à maintenir cet équilibre, il est possible de limiter les dégâts. C'est ensemble que nous gagnerons la lutte contre la fraude, car chaque arnaque est une arnaque de trop.

febelfin

Fédération belge du secteur financier

www.febelfin.be