Bienvenue

Le webinaire commence à 14h

22 novembre 2021
«La sécurité des données bancaires: phishing et mûle financière»
Invitées : C. Gorez, Febelfin et M-A Dembour, Parquet de Bruxelles

Autre webinaire proposé :

9/12/21
14h-15h

Fraudes aux sentiments, **M-A. Borgers, NENIU ASBL, L. Decort, AB-Reoc et R. Kalfa, VSZ**

Informations et inscription : www.observatoire-credit.be

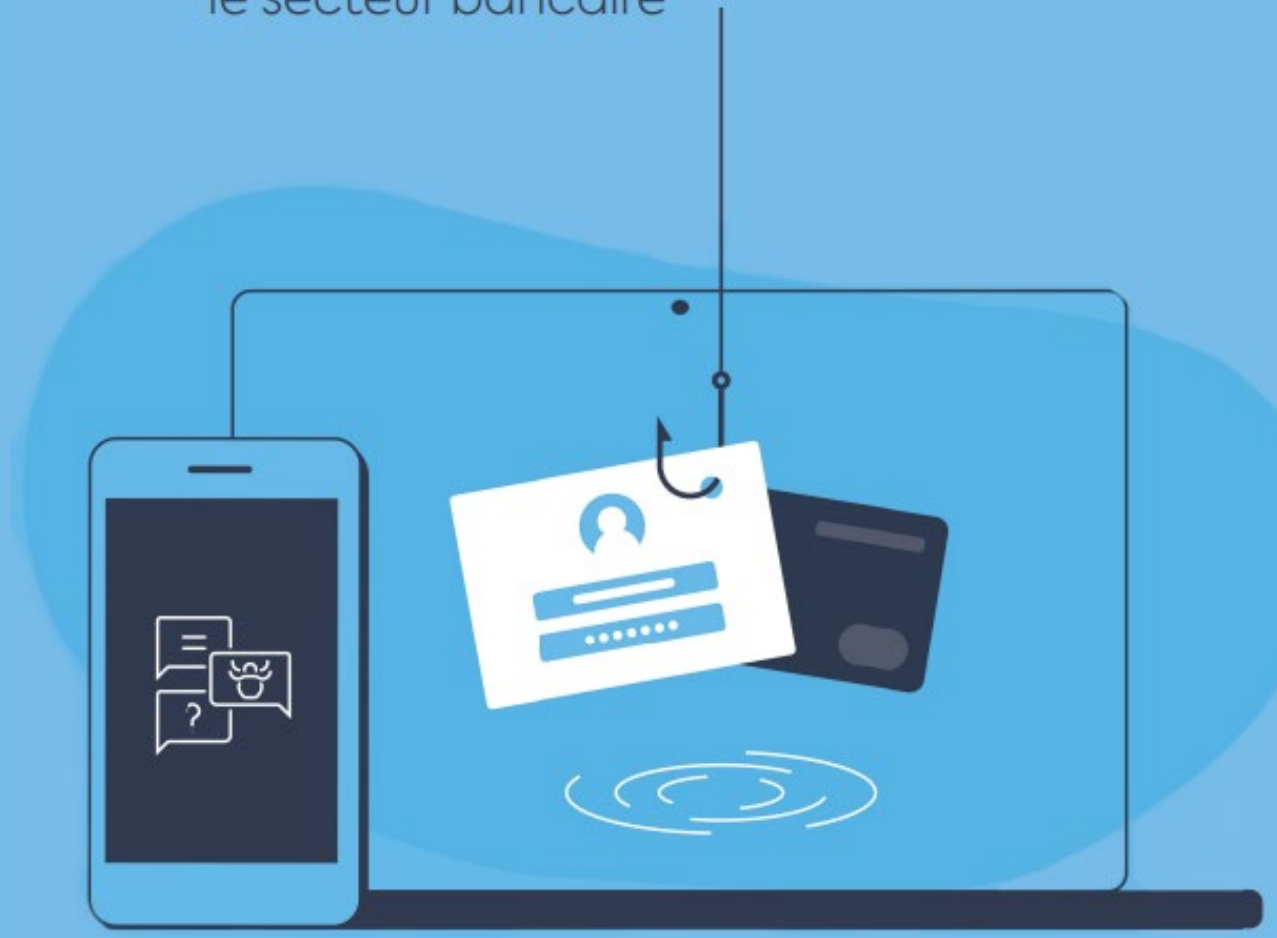
A réécouter sur notre site internet :

14/10/21	Ventes frauduleuses et autres publicités trompeuses, **W. Matgen, CEC Belgium**
28/10/21	Arnaques à la consommation liées aux bureaux de recouvrement frauduleux, **L.Hilson, SPF Economie**
09/11/21	Offres d'investissement et de crédit: méfiez-vous des escrocs !, **A-L. Oumouadène et C. Vanheuverswyn, FSMA**

Observatoire du Crédit et de l'Endettement

There is plenty of 'phish' in the sea

Fraude et escroquerie dans le secteur bancaire

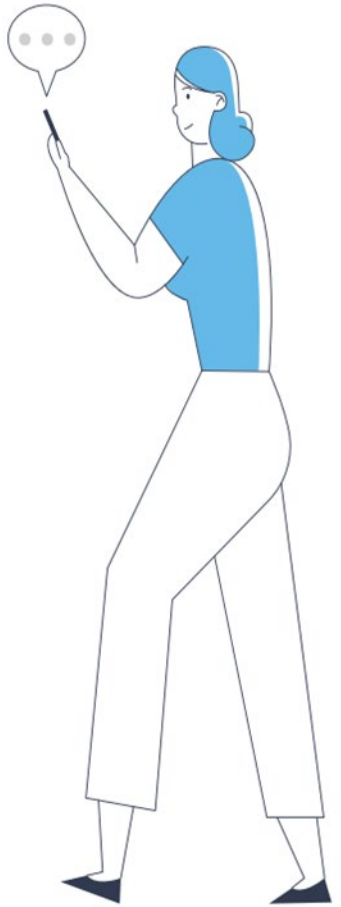


febelfin

Charline Gorez
Marketing & Communication Specialist

Agenda

- Définitions et chiffres clés
- Tendances dans le phishing et autres fraudes
- Mules financières
- Parties prenantes
- Actions du secteur financier
- A retenir!



Chiffres clés

febelfin

Définitions

- Le **phishing** est une forme d'escroquerie où les fraudeurs vous envoient un message contenant un lien vers un faux site web. Si vous y introduisez vos codes bancaires personnels, ils auront libre accès à votre compte.
- Le **smishing** = phishing mais le message est spécifiquement envoyé par sms.

Chiffres clés

2020 :

- 67.000 transactions frauduleuses
- Montant net total ± € 34 mio
- Augmentation de 204 % du nombre de victimes de phishing par rapport à 2019, avec un total de 7502 signalements (Police Fédérale)

2021 :

- Tous les signaux indiquent une poursuite de cette tendance.

34% **de la population a reçu un message d'hameçonnage au cours du dernier mois.** Au total, 56 % ont reçu un tel message au cours des six derniers mois. Cela montre l'ampleur du phénomène. Il faut être constamment sur ses gardes face à ces fraudes.

30% des jeunes n'ont **jamais entendu parler du phishing**.

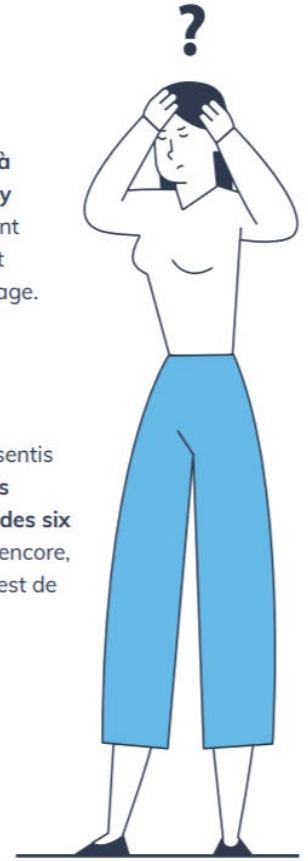
26% **a déjà partagé des informations financières** pour ensuite se sentir coupable de les avoir communiquées. L'an dernier, ce groupe représentait 23%.

3% **des Belges donneraient leur code bancaire si leur banque le leur demandait.** Le fait que 8% des jeunes soient aussi prêts à le faire n'est pas non plus un bon signe.

Les Belges ne sont pas encore suffisamment sensibilisés à l'hameçonnage. 12 % de la population n'a encore jamais entendu parler du phishing.

3% **de ceux qui ont déjà reçu un message de phishing y ont donné suite.** Les jeunes sont plus vulnérables puisqu'ils sont 5% à avoir répondu à ce message.

7% des Belges se sont sentis mal à l'aise d'avoir **partagé des données financières au cours des six derniers mois**. Plus inquiétant encore, chez les 16-30 ans, cette part est de 17%.



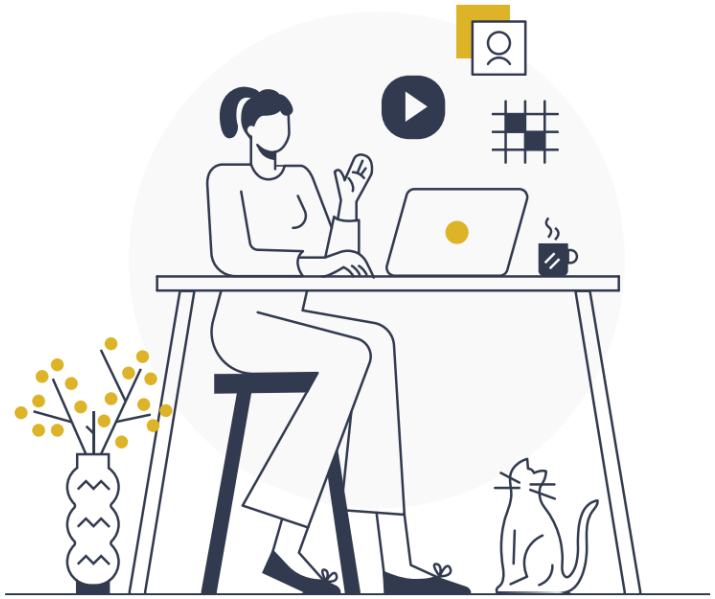
[1] *Enquête de Febelfin menée en collaboration avec IndiVille et réalisée du 3 au 5 mars 2021 auprès de 2.045 personnes entre 16 et 79 ans.*

Tendances dans le phishing et autres fraudes

febelfin

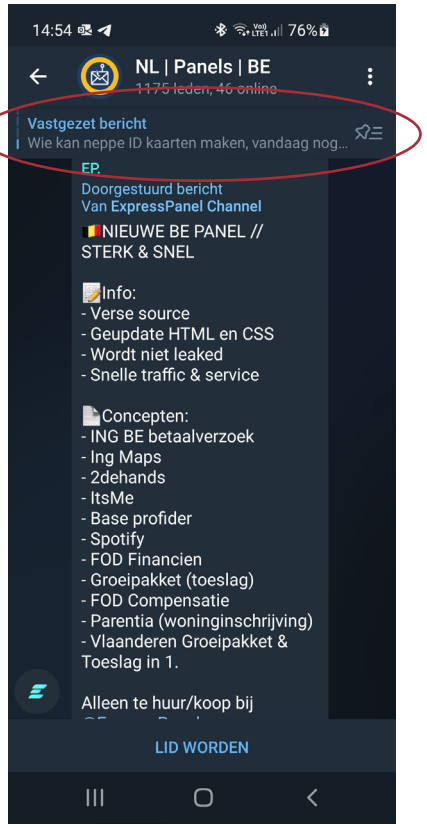
Tendances dans le phishing

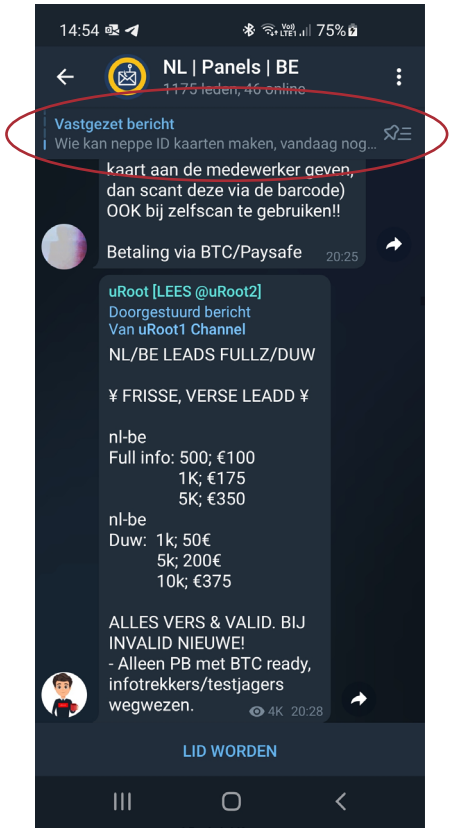
- 2020 : crise sanitaire & économique → aussi une **“crise du phishing”.**
- **Augmentation** significative du **(des tentatives de) phishing** depuis novembre 2020.
- Le **seuil d’entrée** dans la fraude numérique est toujours plus bas :
  - des kits de phishing sont disponibles à des prix très bas.
  - Beaucoup de phishers recrutés.
  - via divers canaux : e-mail/sms/médias sociaux/téléphone/moteurs de recherche.
- Les pratiques de fraude s’adaptent au **nouveau style de vie** :
  - jouer sur les émotions, la peur et l’ignorance.
  - se faire passer pour des organisation fiables (cf. organismes de santé, services publics, banques, …).
  - augmentation des achats en ligne et télétravail → les fraudeurs se font passer pour des livreurs, des plates-formes d’e-commerce ou des prestataires de réseaux.



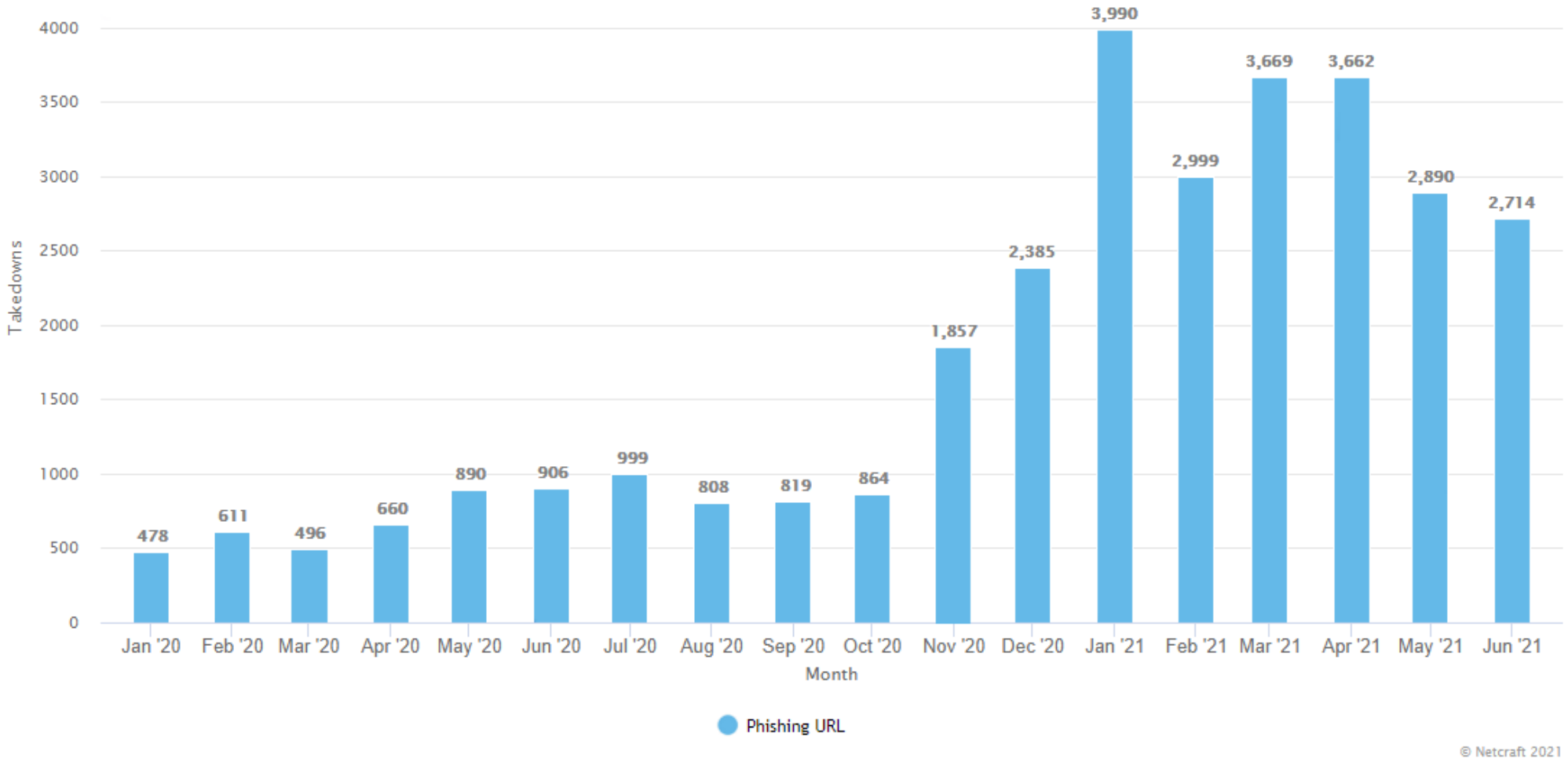
Tendances dans le phishing

- Les messages **concernant le corona** (par ex. masques, primes promises, …) ont augmenté le “risque de clic”.
- Dans la plupart des cas, une pression est exercée sur les victimes pour qu’elles donnent leurs codes personnels (codes pin, codes du lecteur de carte) ou les fraudeurs s’efforcent de mettre la main sur la carte bancaire matérielle.
- Cash-out via virements, paiements par carte (shopping en ligne), mules, etc.



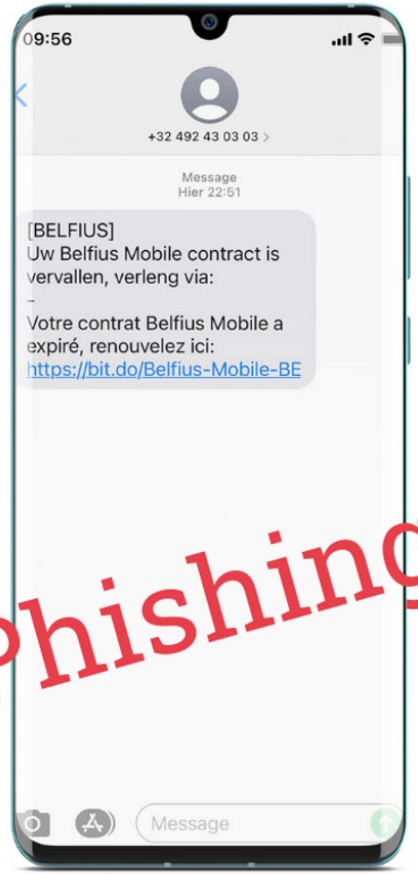


Recrutement de phishers ! Des fraudeurs occupés à discuter sur internet…

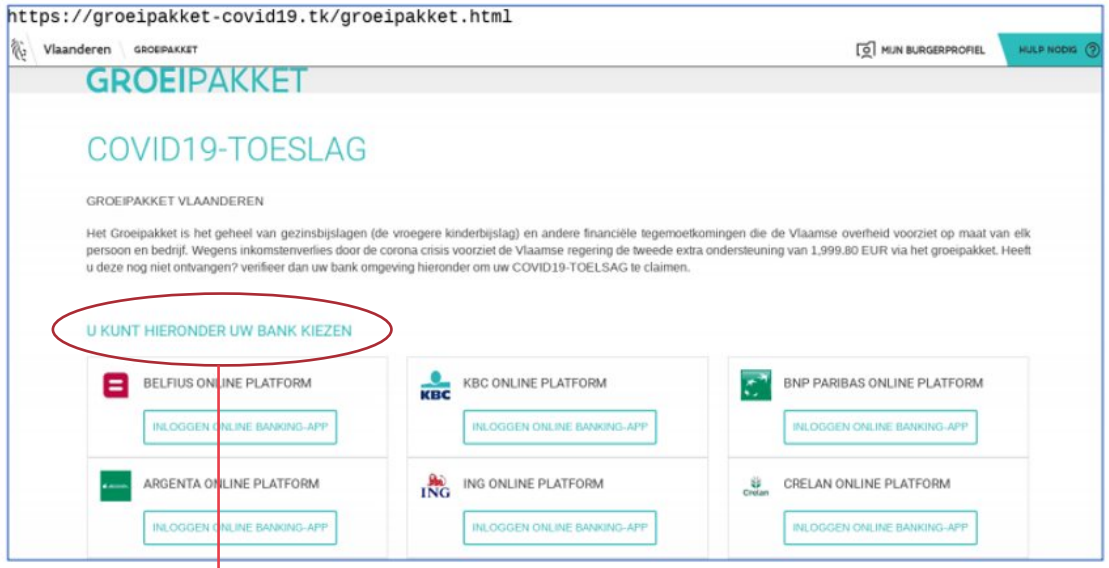


Croissance significative du (des tentatives de) phishing depuis novembre 2020

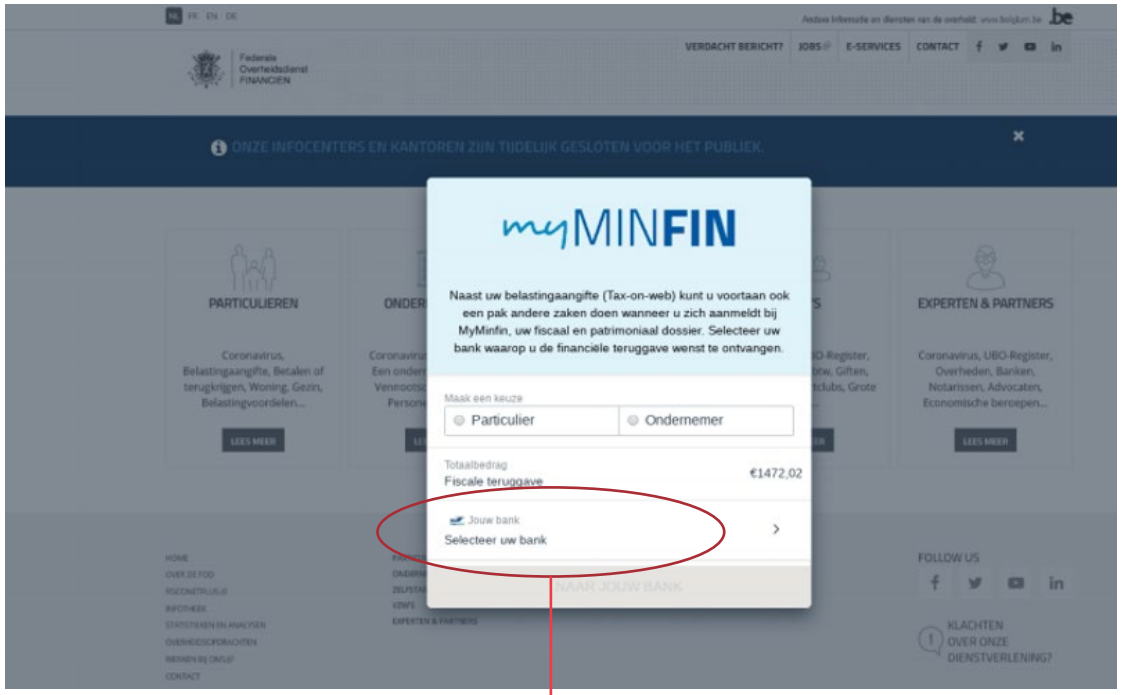
Exemples de sms de phishing (smishing)



Exemples de fausses pages web quand on clique sur le lien

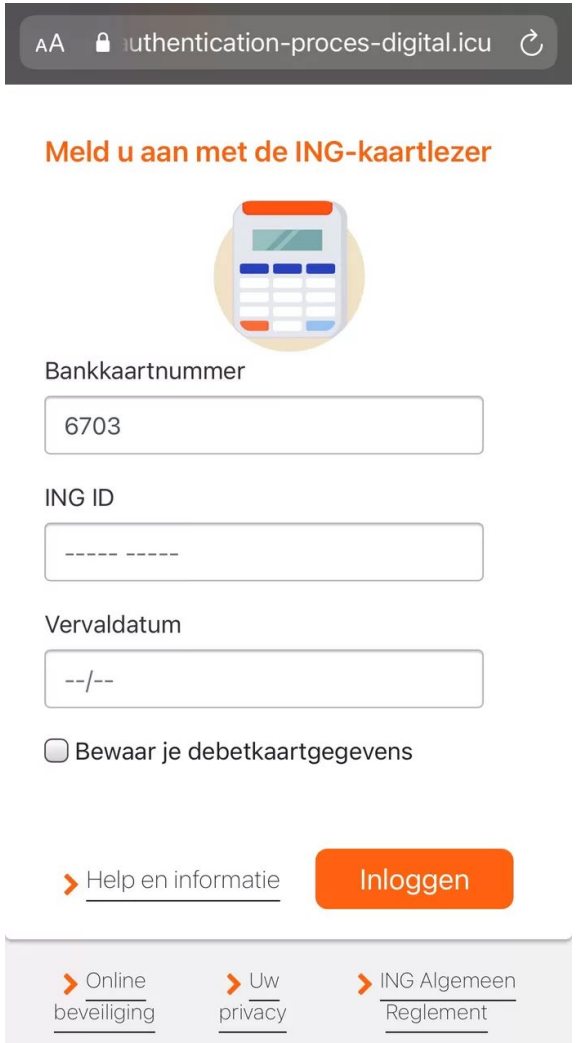


“Vous pouvez choisir ci-dessous votre banque”

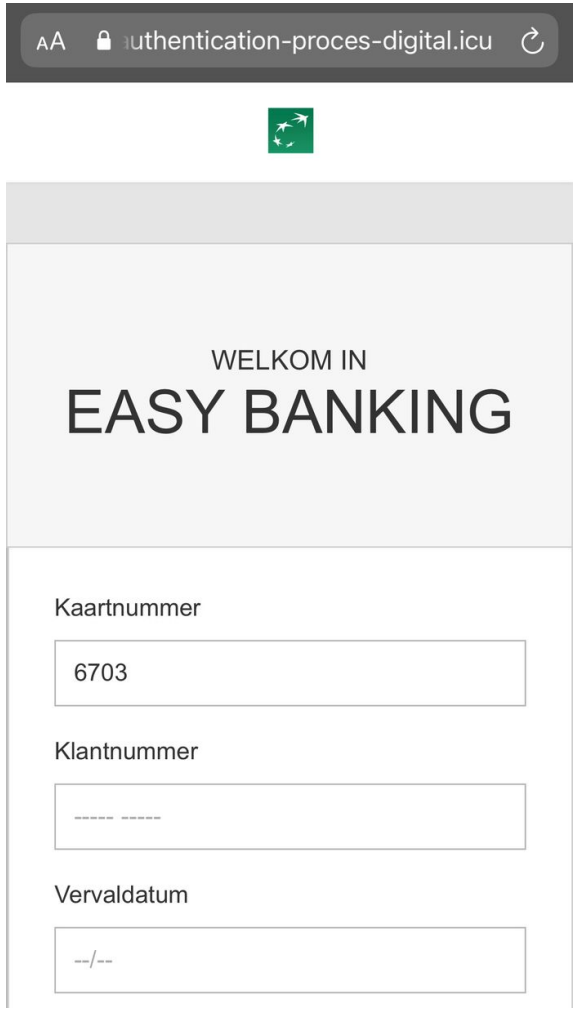


“Sélectionnez votre banque”

Choisir sa banque



Fausse page se faisant passer pour ING



Fausse page se faisant passer pour BNP Paribas Fortis

"Vous avez encore reçu une prime de 317,53€. Cliquez ici pour recevoir le montant"

Fausse page internet où l'on vous demande de choisir votre banque pour "s'inscrire" pour recevoir la prime.

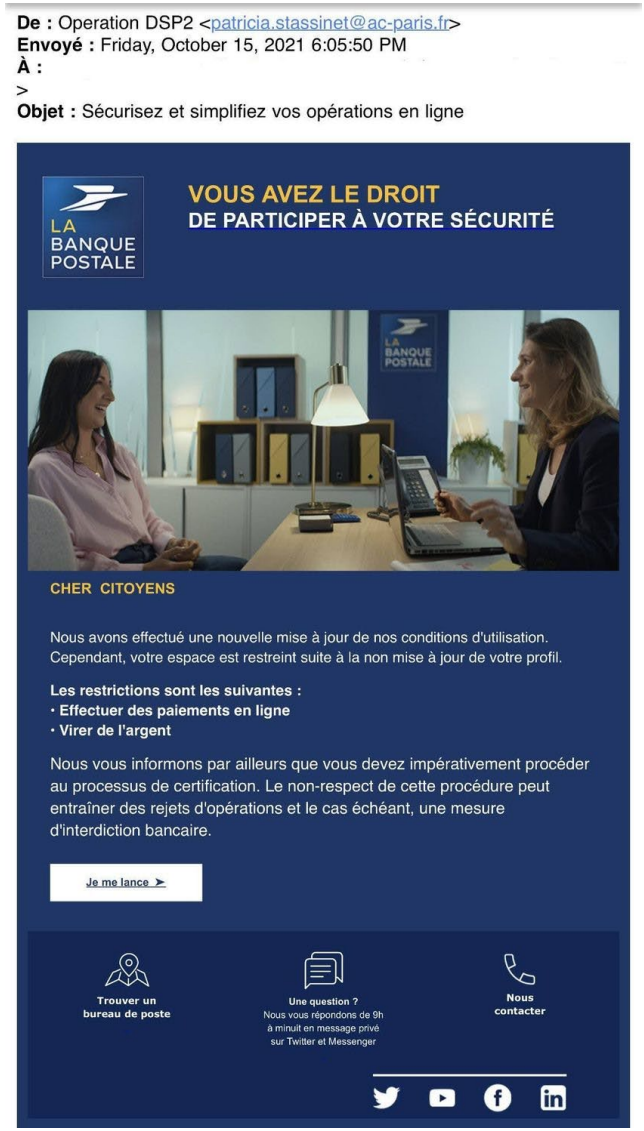
Comment reconnaitre un mail de phishing ?

Adresse mail bizarre ou ne correspondant pas à l'organisation

Adressage non personnalisé

Pression/contrainte/ menace
Ou élément qui attire la curiosité ou on parle d'argent, etc.

Lien pour compléter vos données personnelles/bancaires sur un site ou téléchargement



De : Operation DSP2 <patricia.stassinet@ac-paris.fr>
Envoyé : Friday, October 15, 2021 6:05:50 PM
À :
>
Objet : Sécurisez et simplifiez vos opérations en ligne

LA BANQUE POSTALE

VOUS AVEZ LE DROIT
DE PARTICIPER À VOTRE SÉCURITÉ

CHER CITOYENS

Nous avons effectué une nouvelle mise à jour de nos conditions d'utilisation. Cependant, votre espace est restreint suite à la non mise à jour de votre profil.

Les restrictions sont les suivantes :
- **Effectuer des paiements en ligne**
- **Virer de l'argent**

Nous vous informons par ailleurs que vous devez impérativement procéder au processus de certification. Le non-respect de cette procédure peut entraîner des rejets d'opérations et le cas échéant, une mesure d'interdiction bancaire.

Je me lance ➤

Trouver un bureau de poste

Une question ? Nous vous répondons de 9h à minuit en message privé sur Twitter et Messenger

Nous contacter

Comment reconnaitre un mail de phishing ?

Placez toujours le curseur de votre souris sur le lien sans cliquer dessus afin de vérifier le nom de domaine exact qui se cache sous le lien.

Van: "Febelfin" <info@terbergspecials.be>
Aan: "johan vansteenwegen" <johan.vansteenwegen@telenet.be>
Verzonden: Zondag 29 oktober 2017 13:23:27
Onderwerp: Bericht

Geachte klant,

Uit onze administratie is naar voren gekomen dat u nog geen gebruik maakt van onze nieuwe kaart. De nieuwe kaart is beter beveiligd tegen fraude-activiteiten en voldoet zich aan de Europese veiligheidsvoorschriften betreft bankierzaken.

Belangrijkste aanpassing: Banken moeten klanten verzekeren tegen financiële schade bij eventuele fraude-activiteiten. Als gevolg hiervan introduceren wij de nieuwe beter beveiligde kaart.

Vanwege de veiligheid van onze klanten verplicht ING het gebruik van de nieuwe kaart. Het gebruik van uw huidige product vervalt per 10 november 2017 voor gebruik.

Uit vei http://www.ing.be.fcnnbfn.info/aanvragen ail uit naam van Febelfin
Click or tap to follow link.

Vraag hier kosteloos uw nieuwe kaart aan.

Wij vertrouwen erop u hiermee voldoende te hebben geïnformeerd en van dienst te zijn geweest.

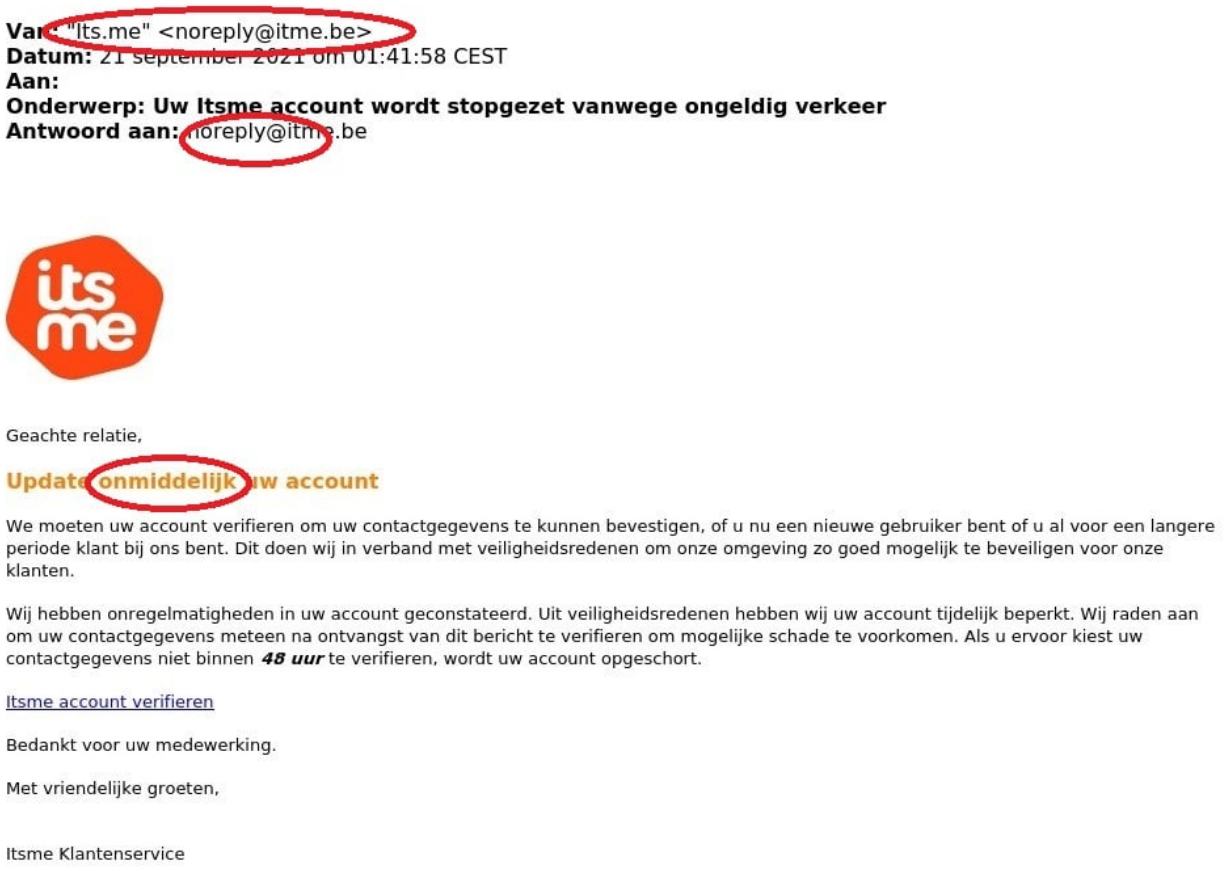
Alvast hartelijk dank voor uw medewerking.

Met vriendelijke groeten,

Pascale Jacobs
ING
Afdeling personeelszaken

febelfin

Autres exemples récents



Van: "Its.me" <noreply@itme.be>
Datum: 21 september 2021 om 01:41:58 CEST
Aan:
Onderwerp: Uw Itsme account wordt stopgezet vanwege ongeldig verkeer
Antwoord aan: noreply@itme.be

Geachte relatie,

Update onmiddelijk uw account

We moeten uw account verifieren om uw contactgegevens te kunnen bevestigen, of u nu een nieuwe gebruiker bent of u al voor een langere periode klant bij ons bent. Dit doen wij in verband met veiligheidsredenen om onze omgeving zo goed mogelijk te beveiligen voor onze klanten.

Wij hebben onregelmatigheden in uw account geconstateerd. Uit veiligheidsredenen hebben wij uw account tijdelijk beperkt. Wij raden aan om uw contactgegevens meteen na ontvangst van dit bericht te verifieren om mogelijke schade te voorkomen. Als u ervoor kiest uw contactgegevens niet binnen ***48 uur*** te verifieren, wordt uw account opgeschort.

Itsme account verifieren

Bedankt voor uw medewerking.

Met vriendelijke groeten,

Itsme Klantenservice

Van: "Belfius" <belfius6@lezennu.com>
Aan:
Verzonden:
Onderwerp: Kennisgeving

Beste klant,

U heeft een nieuw bericht in uw persoonlijke postvak.
Postvak openen

Met vriendelijke groet,

Toon Sneyers
Afdeling personeelszaken

Dit is een automatisch gegenereerde e-mail

febelfin

Les fraudeurs s’attaquent au maillon “le plus faible”

- Les fraudeurs s’en prennent au **maillon le plus faible** (= client/e) via l’**“ingénierie sociale” :**
  - Phishing : demandes de codes pin et/ou de codes de réponse
  - Scam : fausses factures, demandes d’aide, investissements, cryptomonnaies, compte sûr, fraude CEO
  - Malware : installation de “logiciels malveillants” sur des pc ou un smartphone

2020 : une année sous le signe de la fraude et des escroqueries

JANVIER-FÉVRIER

Phishing à la carte bancaire par courrier (renvoyez votre carte bancaire découpée et donnez votre code pin)

A PARTIR DE MARS

(début de la compensation corona par courriel, sms)

- Fraude à la demande d'aide WhatsApp
- Fraude aux comptes à sécurité renforcée
- Fraude par SMS CardStop, ITSME
- Courriels de phishing du SPF Finances (demandez votre remboursement d'impôts ici) et du SPF Economie (demandez votre prime corona ici)

SEPTEMBRE

Fraude aux comptes à sécurité renforcée

OCTOBRE

- Phishing paquet Bpost
- Smishing Card Stop

NOVEMBRE

- Fraude WhatsApp
- Phishing mise à jour du lecteur de cartes
- Black Friday et Cyber Monday : la fête annuelle du phishing devient incontrôlable

DÉCEMBRE

- Phishing paquet Bpost
- Smishing Card Stop
- Phishing à la carte bancaire par courrier (envoyez votre carte bancaire découpée et donnez votre code PIN)

Vous trouverez de plus amples informations sur les types de fraude évoqués ci-avant en vous rendant sur **www.febelfin.be**

Phishing à la carte bancaire

- Les fraudeurs tentent d'obtenir **directement votre carte bancaire et les codes** allant de pair :
    - Vous recevez un e-mail ou un SMS de votre « banque » dans lequel il est indiqué que vous devez remplacer votre carte de débit. Vous êtes invité/e à renvoyer l'ancienne carte de débit afin de la recycler et l'on vous dit que la nouvelle carte sera envoyée.
    - Le lien dans l'e-mail ou le SMS vous amène sur un site web factice. Les fraudeurs vous demandent alors :
        - de compléter vos données personnelles et votre numéro de carte;
        - d'introduire votre code pin actuel et d'en choisir un nouveau;
        - et de renvoyer votre carte de débit actuelle par la poste.

À retenir

Votre banque ne vous demandera **jamais le code pin** de votre carte de débit. Votre banque ne vous demandera j**amais non plus de lui renvoyer votre carte de débit**.

Phishing à la carte bancaire à domicile

- Les **fraudeurs se font passer pour des employés de votre banque et vous appellent** pour vous avertir, par exemple, que des transactions suspectes ont été effectuées avec votre carte bancaire. Mais, de façon soudaine, ils vous disent que la liaison téléphonique est mauvaise et vous proposent de se rendre directement chez vous afin de résoudre le problème. Ils se comportent généralement de manière professionnelle et font tout pour gagner votre confiance.

- Ils **viennent à votre domicile** et s'assoient à vos côtés lorsque vous vous connectez à la banque en ligne. De cette façon, ils vont voir votre code personnel ou noter le code de réponse du lecteur de carte. Ils vont par la suite couper votre carte bancaire devant vous, après l'avoir évidemment rapidement échangée avec une autre, ou alors ils vont veiller à ne pas couper la puce de la carte.

A retenir

Les employés de banque ne vous demanderont jamais vos codes personnels (codes pin ou codes de réponse). Ils ne viendront également jamais chez vous pour couper ou récupérer votre carte bancaire ou encore pour résoudre des problèmes de paiement.

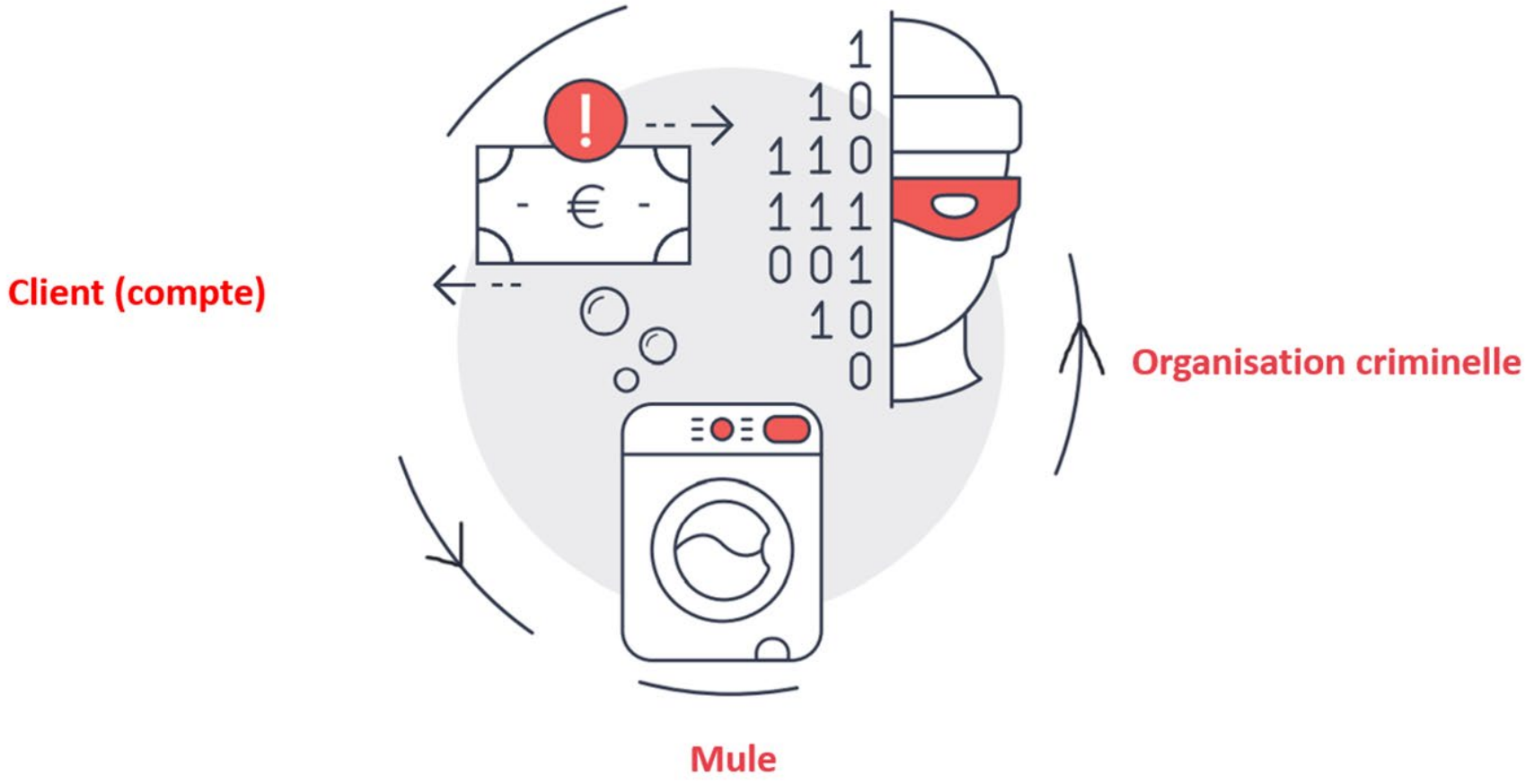
Urgent = suspect

En cas de doute, coupez la conversation et contactez votre banque afin de vérifier les dires de la personne qui vous a contacté. Ne vous laissez pas avoir si cette personne vous mentionne que c'est très urgent. C'est un prétexte courant utilisé par les fraudeurs pour créer de la panique auprès de leurs potentielles victimes. Ils essaient ainsi de les amener à agir plus rapidement.

Mules financières

febelfin

L’argent n’aboutit pas directement sur le compte du fraudeur…



Le rôle de la mule financière

Qu’est-ce qu’une mule ?

- Mules (=money mules) : **personnes qui font/laissent transiter illégalement de l'argent via leur compte**. Il s'agit souvent de personnes qui ont des difficultés financières et/ou qui veulent se procurer de l'argent de manière simple.

Qui ?

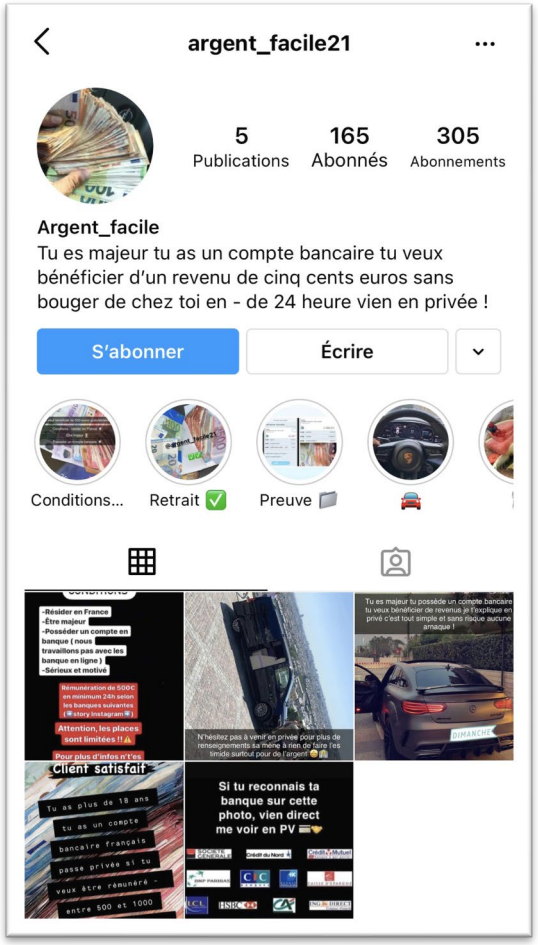
- Le groupe cible par excellence : les jeunes. 1 jeune sur 10 serait ainsi d’accord pour prêter son compte et/ou sa carte bancaire en échange d'argent !

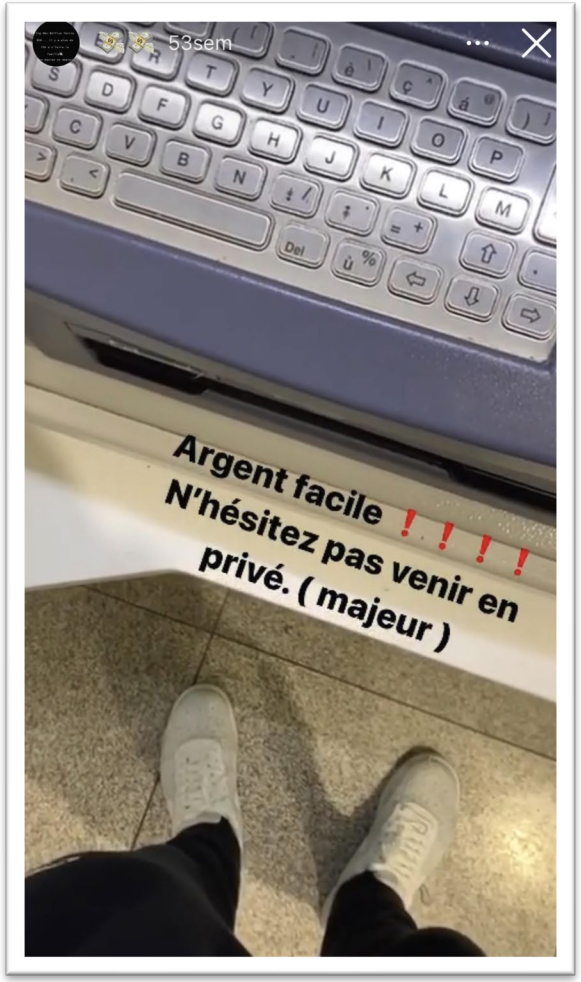
Le rôle de la mule financière

Comment ?

- La cible potentielle est approchée en ligne ou dans la vie réelle par un recruteur qui lui demande de lui **prêter son compte et/ou sa carte bancaire et son code PIN** en échange d'une **rémunération**.
- En ligne, ce sont les **médias sociaux** (Instagram…) qui sont populaires, dans la vraie vie, le recrutement a lieu dans **les gares, les lieux de sortie** ou à proximité des **écoles**.
- La pratique est décrite comme **« parfaitement sûre », « légale »** ou présentée comme un **« service d'ami »**.
- Quiconque donne suite à cette « proposition d'échange » devient une mule.
- Les criminels ont besoin des mules, de leur compte et/ou de leur carte bancaire pour **faire transiter de l'argent illégalement ou pour retirer cet argent en cash**. De l'argent qui a généralement été volé par le biais du **phishing**.
- En utilisant le compte bancaire et/ou la carte de la mule, les criminels effacent toute trace d'eux-mêmes. Ils se rendent anonymes mais la mule, elle, ne l'est pas!
- Dans la pratique, la rémunération est faible et la mule se retrouve souvent avec un compte vidé.


remuneration_immediat
7
Publications
155
Abonnés
718
Abonnements
Argent facile bb
Entrepreneur
Bonjour vous cherchez à arrondir vos fin de mois?
C'est simple il vous suffit de vous inscrire et vous recevrez un paiement chaque mois pour + info pv
secure.jaalifestyle.com/ref/pryss
S'abonner
Écrire
job srx
500€ en une semaine tu veux savoir comment je fais ? Tape info
Votre Solde : € 1,137.00


argent_facile21
5
Publications
165
Abonnés
305
Abonnements
Argent_facile
Tu es majeur tu as un compte bancaire tu veux bénéficier d'un revenu de cinq cents euros sans bouger de chez toi en - de 24 heure vien en privée !
S'abonner
Écrire
Conditions...
Retrait ✅
Preuve
Client satisfait
Tu as plus de 18 ans
tu as un compte bancaire français
passe privée si tu veux être rémunéré
entre 500 et 1000
Si tu reconnais ta banque sur cette photo, vien direct me voir en PV


53sem
Argent facile ! ! ! !
N'hésitez pas venir en privé. (majeur)


Merci pour votre confiance la famille
maestro

openbaar ministerie
ministère public

Mules bancaires
infractions pénales

Marie-Astrid DEMBOUR
Substitut du Procureur du Roi de Bruxelles
22/11/2021

Plan

- **Introduction**
- **Niveau d’implication**
- **Infractions les plus courantes**
- **Conséquences concrètes**
- **« PIEGE » de la mule bancaire**
- **Conclusion**

Introduction

Niveau d'implication

- **Qui sont-elles dans le dossier pénal ?**

- **Corréité (être auteur ou co-auteur → même peine)**

Art. 66. Seront punis comme auteurs d'un crime ou d'un délit :
Ceux qui l'auront exécuté ou qui auront coopéré directement à son exécution;
Ceux qui, par un fait quelconque, auront prêté pour l'exécution une aide telle que, sans leur assistance, le crime ou le délit n'eût pu être commis;
Ceux qui, par dons, promesses, menaces, abus d'autorité ou de pouvoir, machinations ou artifices coupables, auront directement provoqué à ce crime ou à ce délit;

- **Complicité (peine immédiatement inférieure)**

Art. 67. Seront punis comme complices d'un crime ou d'un délit :
Ceux qui auront donné des instructions pour le commettre;
Ceux qui auront procuré des armes, des instruments, **ou tout autre moyen qui a servi au crime ou au délit, sachant qu'ils devaient y servir;**
Ceux qui, hors le cas prévu par le § 3 de l'article 66, auront, avec connaissance, aidé ou assisté l'auteur ou les auteurs du crime ou du délit dans les faits qui l'ont préparé ou facilité, ou dans ceux qui l'ont consommé.

→ L'implication dépend de chaque dossier

Infractions les plus courantes

1. CODE PENAL :

Blanchiment (505§1 CP) - infraction principalement retenue pour les mules

2° Avoir acheté, reçu en échange ou à titre gratuit, possédé, gardé ou géré des choses visées à l'article 42, 3° *[=avantage patrimonial tiré d'une infraction]* alors qu'ils connaissaient ou devaient connaître l'origine de ces choses au début de ces opérations;

3° avoir converti ou transféré des choses visées à l'article 42, 3°, dans le but de dissimuler ou de déguiser leur origine illicite ou d'aider toute personne qui est impliquée...

4° avoir dissimulé ou déguisé la nature, l'origine, l'emplacement, la disposition...

→ 15 j à 5 a et/ou 26 à 100.000 € + **confiscation obligatoire (cfr. infra)**

Escroquerie (496 CP)

« ...dans le but de s'approprier une chose appartenant à autrui, se sera fait remettre ou délivrer des fonds, meubles, obligations, quittances, décharges, soit en faisant usage de faux noms ou de fausses qualités, soit en employant des **manoeuvres frauduleuses** pour persuader l'existence de fausses entreprises, d'un pouvoir ou d'un crédit imaginaire, pour faire naître l'espérance ou la crainte d'un succès, d'un accident ou de tout autre événement chimérique, ou pour abuser autrement de la confiance ou de la crédulité, ... »

→ Emprisonnement 1m à 5a + amende 26 à 3000 €

Infractions les plus courantes

1. CODE PENAL (suite):

Faux et usage de faux (art. 193, 196, 197, 213 et 214 CP)

fausse facture ou facture falsifiée, tout contrat avec une identité usurpée, ...
→ Réclusion 5 à 10 ans + amende de 26 à 2000 € (+ interd. art 32 CP)
(mais correctionnalisation donc emprisonnement de 1m à 5a)

Faux informatiques (210 CP)

« un faux, en introduisant dans un système informatique, en modifiant ou effaçant des données, qui sont stockées, traitées ou transmises par un système informatique, ou en modifiant par tout moyen technologique l'utilisation possible des données dans un système informatique, et par là modifie la portée juridique de telles données, ... »
→ 6m-5a et/ou amende de 26 à 2000 €

Infractions les plus courantes

1. CODE PENAL (suite):

association de malfaiteurs (322 CP et s.)

« Toute association formée dans le but d'attenter aux personnes ou aux propriétés est un crime ou un délit, qui existe par le seul fait de l'organisation de la bande. »

→ Membres : 6 mois à 5 ans (+ interd fac art.33)

Ou

organisation criminelle (324bis et ter CP)

« Constitue une organisation criminelle l'association structurée de plus de deux personnes, établie dans le temps, en vue de commettre de façon concertée, des crimes et délits punissables d'un emprisonnement de trois ans ou d'une peine plus grave, pour obtenir, directement ou indirectement, des avantages patrimoniaux »

→ Membres : 1 a à 3 ans et/ou 100 à 5.000 €

Infractions les plus courantes

2. Loi du 18 mars 2018...

…relative au statut et au contrôle des établissements de paiement et des établissements de monnaie électronique, à l'accès à l'**activité de prestataire de services de paiement**, et à l'activité d'émission de monnaie électronique, et à l'accès aux systèmes de paiement (entrée en vigueur le 26/3/2018)

Article 149 interdit de fournir des services de paiement en Belgique sans respecter certaines dispositions strictes (articles 5 et 9 de la loi), et notamment sans être un établissement ou une autorité reconnu(e) expressément par la loi.

→ 1 mois à 1 an et/ou une amende de 50 à 10 000 euros.

En résumé, prêter son compte est interdit !

Conséquences concrètes

Directions pénales possibles (de la plus sévère à la moins sévère)

- mise à l'instruction avec mandat d'arrêt (détention préventive durant l'enquête) puis renvoi devant le Tribunal correctionnel
- citation devant le Tribunal correctionnel
- alternatives aux poursuites : MP ou TR ou PRÊT (dossier reste auprès du M.P.)

Devant le Tribunal correctionnel

- Article 65 du code pénal (absorption : peine la plus forte)
- Emprisonnement/amende - sursis - PTA - probation
- Confiscations (art.42 CP) prévues par le code comme étant
  - obligatoires (notamment pour le blanchiment !)
  - ou facultatives

« PIEGE » de la mule bancaire

→ Croit à l'argent facile sans conséquences (encouragé par les recruteurs)
mais enquêtes affinées,
crédibilité des explications balayée par éléments concrets

→ Ne veut pas « balancer » et se retrouve seule au procès
donc seule à assumer le dommage réclamé par les victimes et/ou
les confiscations requises par le Ministère Public

→ Autres conséquences hors justice

Conclusion

prévention & éducation

indispensables

- Mule: danger personnel de prêter son compte

- Société : participation à un phénomène criminel important, nombreuses victimes, argent détourné n'est pas spécialement investi dans l'économie belge et peut financer d'autres infractions

Merci pour votre attention

Marie-Astrid DEMBOUR
Substitut du Procureur du Roi de Bruxelles
22/11/2021

Le rôle de la mule financière

Conséquences ?

- Menaces et violences physiques
- Punissable – poursuites pénales (amende/travail d'intérêt général/prison)
- Mule mineure : les parents peuvent être tenus pour responsables
- Votre banque peut refuser d'encore vous accorder un compte ou une carte bancaire, voire un prêt.

➔ La mule est **complice de fraude**. Elle fait du **blanchiment d'argent**.
➔ Conséquences graves.

Vous servez de mule?

- Cessez tout transfert d'argent et/ou ne retirez pas en cash l'argent qui a été versé sur ton compte.
- Contactez au plus vite votre banque.
- Faites bloquer votre carte bancaire via Card Stop.
- Déposez plainte auprès de la police.

Le rôle de la mule financière

Que faire en tant que parent/accompagnateur…?

- Expliquez ce que sont les mules afin que les jeunes puissent apprendre à reconnaître ces pratiques.
- Apprenez aux jeunes comment réagir face à des comptes de médias sociaux qui promettent de l'argent facile et rapide.
- **Faites comprendre aux jeunes qu'ils ne doivent jamais prêter leur carte, leur compte ou leurs codes bancaires, même à un soi-disant "ami".**

Prêter mon compte et ma carte de banque? Jamais ! Ça n’en vaut pas la peine…

Témoignage d'une mule

« J'étais dans un bar avec des amis lorsque trois hommes que nous ne connaissions pas se sont assis à notre table. L'un d'entre eux nous a dit « Les gars, il y a de l'argent à se faire sans risque, vous êtes intéressés ? ». J'ai voulu savoir ce qu'il voulait dire par « sans risque ». C'est là qu'il m'a dit « Ne t'inquiète pas, ce que je vais te proposer est légal, tu n'auras pas de problèmes avec la police ». Il m'explique alors que je dois juste lui donner ma carte bancaire et mon code. Il ajoute que de l'argent sera versé sur mon compte et que je pourrais avoir 40% de la somme. Il m'a ensuite ajouté à Snapchat pour pouvoir communiquer avec moi.

Le lendemain, j'ai reçu un message où il m'a dit que 9000€ seront versés sur mon compte. Lorsque l'argent a été versé, il m'a donné rendez-vous à la Gare Centrale à Bruxelles pour me rendre ma carte et m'expliquer la suite des choses : je devais retirer environ 2500€ par jour. Il m'a précisé à ce moment-là de dire à la banque que c'était pour l'achat d'une voiture, si jamais elle me posait des questions. Il m'a aussi menacé en me disant que si je gardais l'argent pour moi, son chef ne serait pas content et qu'il savait où j'habitais.

Quand la somme a été réunie, on s'est à nouveau vus et il a pris tout le cash. Il m'a dit que l'on se recontacterait le soir-même pour qu'il puisse me donner les 40%. Mais le soir arrivé, j'ai remarqué qu'il m'avait supprimé de Snapchat. Je ne pouvais donc plus le contacter. Après quelques mois, j'ai reçu un courrier de la police me convoquant au commissariat. Le jour de la convocation, les policiers m'ont expliqué que j'étais complice de fraude. Aujourd'hui, cela a des lourdes conséquences pour moi car je dois rembourser l'argent volé aux victimes. Mon dossier est traité par le Procureur du Roi. Les criminels n'ont, quant à eux, jamais été retrouvés.

Le pire dans tout cela est que je connais beaucoup de jeunes, des amis ou des connaissances, qui ont été abordés comme moi dans des lieux publics avec la promesse de se faire de l'argent rapidement. »

Parties prenantes

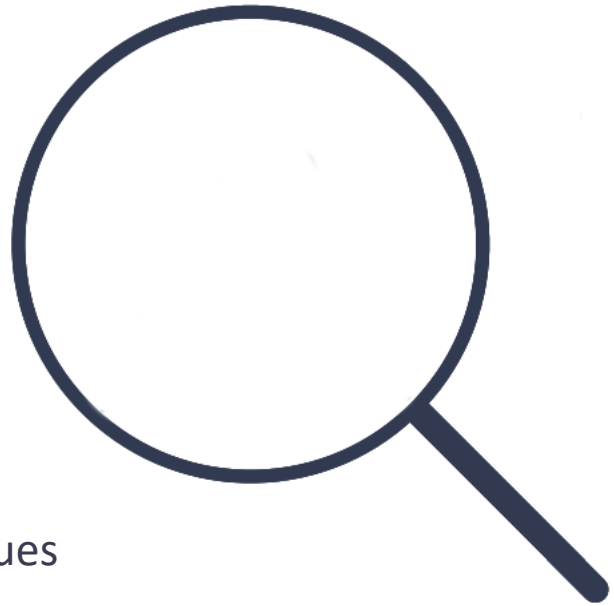
La collaboration, clé du succès !

- 2020 : **67.000 transactions frauduleuses** via phishing & montant net total **± € 34 mio.**
- **Escalade** via les médias, le monde politique et les organisations de consommateurs.
- **La priorité** pour les banques et Febelfin.
- Une **approche multidisciplinaire** est nécessaire car le phishing est un phénomène sociétal → impact sur l'ensemble de la société.

→Besoin d'une **collaboration** plus **efficace** avec toutes les parties prenantes !

Febelfin collabore avec les banques, la police, les médias…

Banques



- Systèmes de sécurité
- Surveillance des risques “plus élevés”
- Communication pour sensibiliser

Febelfin

- Groupes de travail
- Procédure en cas de crise
- Partage de connaissances
- Le secteur sensibilise
- Dialogue avec parties prenantes externes

Febelfin collabore avec les banques, la police, les médias…

Banques-Febelfin

Autres parties prenantes :

- Ombudsfin
- Médias/Presse
- Organisations de consommateurs
- Client/es

Politique :

- Ministre Télécoms
- Secrétaire d'Etat à la Protection des Consommateurs
- Ministre de la Justice
- Ministre de l'Intérieur
- Ministre des Finances

Autorités de contrôle/ réglemementaires :

- BNB
- IBPT (télécoms)

Parties prenantes/collaboration active :

- Télécoms
- CCB (Centre for Cybersecurity Belgium)
- Cyber Security Coalition
- Police et Parquet
- Celllule de Traitement des Informations financières (CTIF)

Actions du secteur

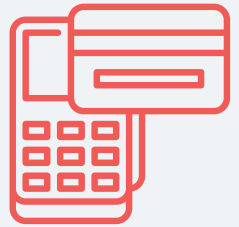
febelfin

Des systèmes bancaires sûrs

Messages ATM
“ne vous laissez pas distraire”

Connexion sûre banque en ligne

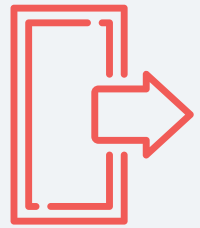
Enregistrement obligatoire



Lecteur de carte :
code pin et code de réponse

Signer des ordres de paiement en ligne

Limites de paiement



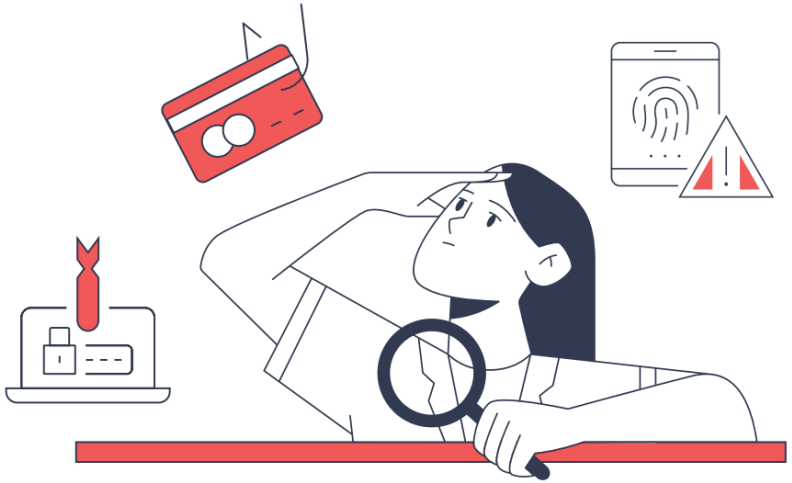
Déconnexion automatique

Experts qui suivent le comportement des criminels en ligne

febelfin

Systèmes de sécurité forts = recherche d'équilibre

- Les banques consentent des efforts considérables pour prévenir le phishing :
  - "**authentification en deux phases**" = le client s'identifie lui-même à l'aide de 2 éléments (carte/téléphone & code pin/empreinte digitale/scan du visage) pour initier des e-paiements.
  - Contrôle intensif des transactions : 75% de l'ensemble des virements frauduleux sont détectés ou récupérés.
  - Collaboration étroite avec les télécoms (pour le smishing & spoofing), parquet, justice, police,…
- L'équilibre est crucial : le ou la client-e souhaite des **paiements sans soucis et rapides (paiements instantanés)** et **une détection efficace de la fraude (il faut du temps)**.
- MAIS : **33% des Belges** jugent ces **étapes de sécurisation supplémentaires superflues → = les assimilent à un frein.**



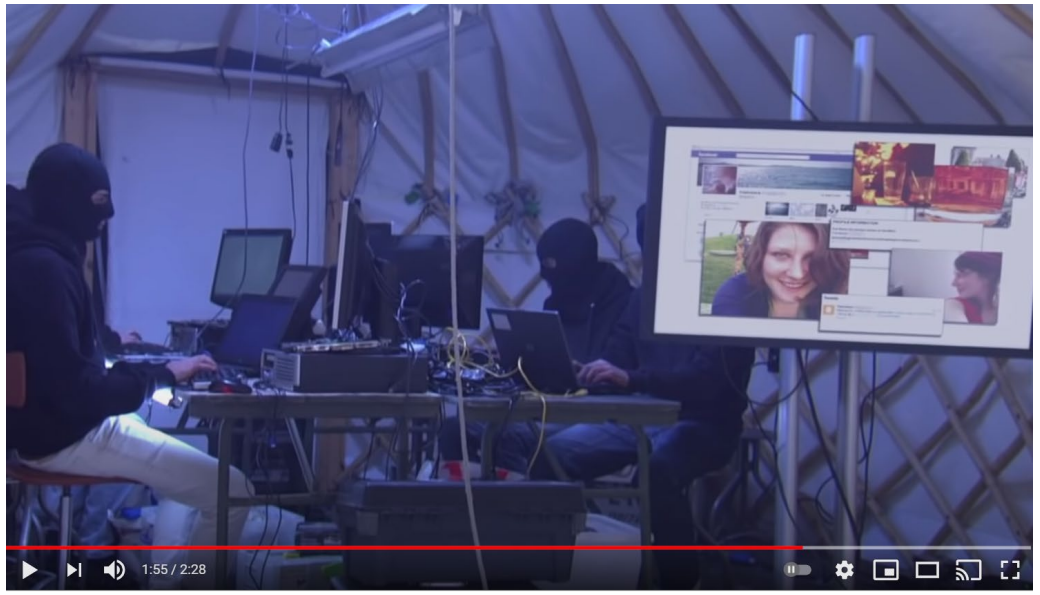
La sensibilisation est nécessaire !

- 12% de la population n’ont encore jamais entendu parler du phishing.
- 30% des jeunes (16-30 ans) n’ont encore jamais entendu parler du phishing.
- 78% des Belges ne signalent pas de faux sms.

→Sensibiliser la clientèle en permanence est primordial car chaque victime est une victime de trop !

Le secteur soutient la prise de conscience

Comme les banques, Febelfin sensibilise elle aussi depuis 2012 à la fraude…
Point de départ : les gens partagent trop d'informations sur internet, les médias sociaux, …



Nouvelle campagne contre le phishing

Affiche

Banner

Messages sur les distributeurs

https://www.safeonweb.be/index.php/fr/materiel-de-campagne

Initiatives en 2021

- **Campagne de sensibilisation** le 16/11 en collaboration avec le Centre pour la Cybersécurité Belgique & la Cyber Security Coalition
- Evocation dans le **soap "Familie"** sur le phishing + **capsules de prévention sur la Une et Tipik du 22 au 26 novembre**.
- **Brochure plurilingue** présentant des informations sur les **mules** diffusée au niveau des CLB/PMS, écoles d'enseignement secondaire, ateliers, CPAS, services de police locaux, …
- Développement **matériel éducatif mules** en collaboration avec **ED TV**

Capsules sur la Une et Tipik dans l'esprit Unité 42

Initiatives en 2021

- Collaboration **Enseignons.be**
- Partage et organisation webinaires phishing & mules avec ≠ partenaires
- **Brochure** “There is plenty of phish in the sea”
- ”Phishing week” Radio 2 (VRT)
- Participation reportage (VRT)

A retenir!

febelfin

Ne communiquez jamais vos codes personnels !

Ne donnez jamais vos codes personnels (code pin et code de réponse) en réponse à un courriel, un appel téléphonique, un sms, un message WhatsApp ou sur un média social.

Ne cliquez jamais non plus sur un lien reçu, mais tapez toujours vous-même l'adresse du site web de votre banque dans votre navigateur ou encore, utilisez votre propre application bancaire mobile. Ce n'est qu'alors que vous pourrez avoir la certitude que tout va bien.

Le paiement et la banque numériques sont et restent sûrs tant que vous gardez vos codes personnels pour vous et restez vigilant/e.

Vous ne donneriez quand même pas votre portefeuille à un inconnu ?

Vous avez reçu un message suspect?

Transférez-le à suspect@safeonweb.be

Si c'est un message au nom d'une banque : envoyez-le à la banque mentionnée. Chaque banque a une adresse spéciale dédiée au phishing.

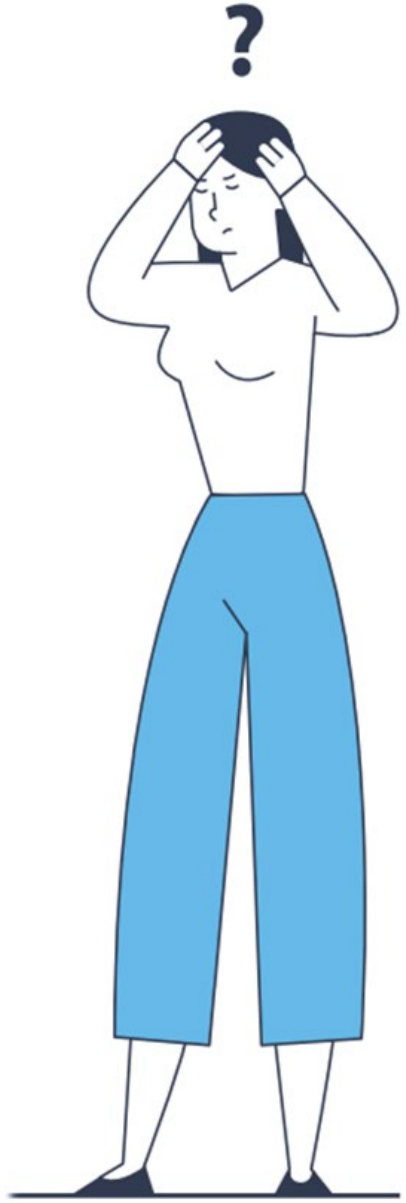
En signalant ces messages, vous pouvez faire **bloquer** les sites de phishing et **éviter** que d'autres ne tombent dans le piège

2021 :

- 3,7 millions de messages suspects envoyés à suspect@safeonweb.be, en moyenne 12.000 par jour (CCB)
- 1,3 million de liens suspects bloqués (CCB)
- Moyenne quotidienne de 25 000 avertissements directs sur les clics sur des liens suspects (CCB)

Vous avez transmis vos codes ?

- Prenez contact **au plus vite** avec votre **banque**
- Avertissez immédiatement **Card Stop** si vous avez également transmis vos données de carte.
- **Modifiez au plus vite vos codes**. Si vous avez communiqué un mot de passe que vous utilisez aussi à d'autres endroits, changez-le immédiatement.
- Déposez plainte auprès de la **police** et transmettez une copie du PV à la banque.



Pour rester au courant

Gardez une longueur d'avance sur les cybercriminels

Avec la nouvelle application Safeonweb, vous recevrez des mises à jour et des notifications sur les messages de phishing et les nouvelles formes d'escroquerie en ligne.

DISPONIBLE SUR Google Play

Télécharger dans App Store

Safeonweb.be

Belgian Financial Sector Federation
www.febelfin.be

22 novembre 2021

«La sécurité des données bancaires: phishing et mûle financière»

Invitées : C. Gorez, Febelfin et M-A Dembour, Parquet de Bruxelles

Questions - Réponses

Observatoire du Crédit et de l'Endettement