There is plenty of ‘phish’ in the sea

Fraude et escroquerie dans le secteur bancaire

febelfin

2020 : quand l'hameçonnage a la pêche

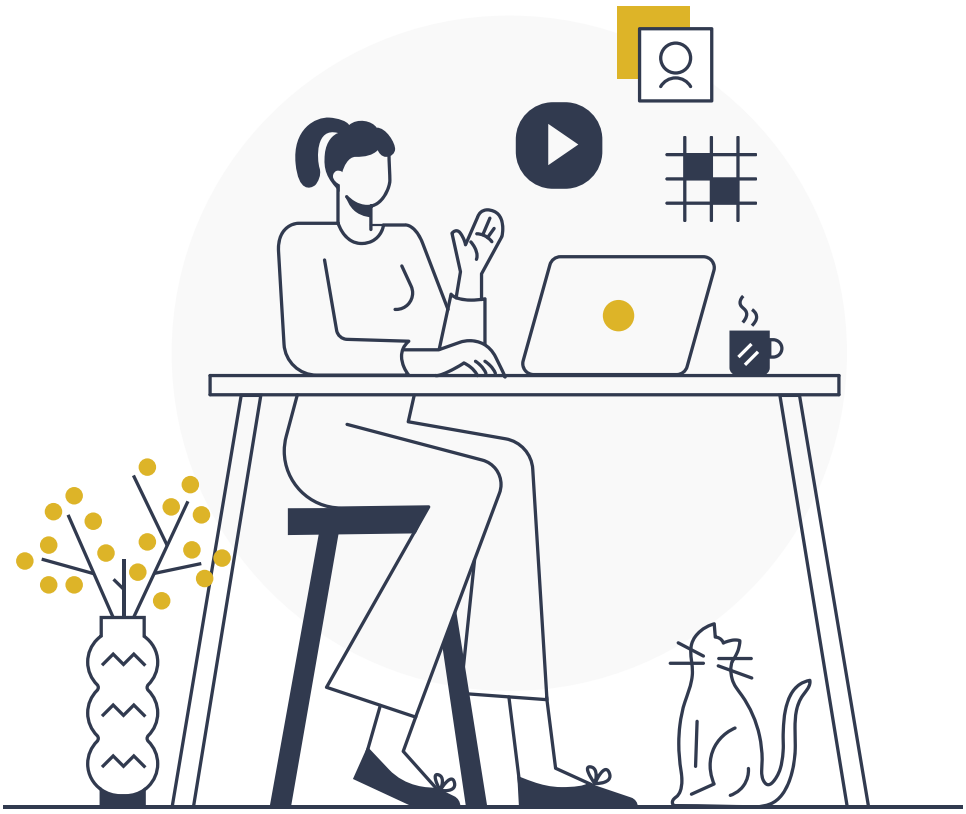
L'année 2020 a été marquée par des défis sans précédent : la pandémie de coronavirus a profondément modifié notre quotidien et les mesures de confinement ont eu un impact majeur sur l'économie. Pendant que les familles et les entreprises se débattaient avec les difficultés, les bandes criminelles en ont profité pour adapter rapidement leurs techniques de fraude à l'évolution de nos modes de vie. On a ainsi vu éclore bon nombre d'arnaques jouant sur l'émotion et la peur des gens face à la pandémie, orchestrées par des fraudeurs se faisant passer pour des employés d'organisations de confiance, comme des organismes de santé, des services gouvernementaux ou des banques. Les messages relatifs au coronavirus (par ex. concernant les masques buccaux, les primes promises...) ont attiré l'attention, ce qui a renforcé la «tentation du clic».

En 2020, les internautes belges ont transféré exactement 3.225.234 messages à l'adresse électronique suspect@safeonweb.be. Soit chaque jour plus de 8.800 messages, ce qui représente presque le double de l'année précédente (1,7 million de messages).
Source: CCB

Les criminels profitent également de l'augmentation des achats en ligne et du travail à domicile en se faisant passer pour des sociétés de livraison de colis, des plates-formes de e-commerce ou des fournisseurs de réseaux. En outre, les criminels recrutent des «mules» pour blanchir l'argent volé en plaçant de fausses annonces sur les sites d'emploi et les médias sociaux, ciblant les personnes à la recherche d'un emploi ou désireuses de gagner facilement de l'argent pendant la pandémie.

Safeonweb a détecté 667.356 liens frauduleux en 2020
Source: CCB

Les pratiques frauduleuses sont de plus en plus sophistiquées et les fraudeurs utilisent les technologies et internet pour rendre leur approche encore plus convaincante. Cela a conduit à une multiplication des scénarios de fraudes, au cours desquels les consommateurs sont amenés par les criminels à leur transférer eux-mêmes de l'argent. Il suffit de songer à cet égard aux fraudes aux comptes à sécurité renforcée ou à la fraude à la demande d'aide, deux techniques de fraude qui ont percé l'an dernier.



QUELQUES FAITS INTÉRESSANTS

Les fraudeurs préfèrent s'en prendre aux **personnes** plutôt qu'aux systèmes. Un examen des attaques frauduleuses fructueuses de ces dernières années met cette constante en évidence. C'est aussi la stratégie la plus simple pour les cybercriminels. Pourquoi s'attaqueraient-ils à des pare-feux et des systèmes antivirus complexes alors qu'il existe une voie tellement plus facile ? Neuf violations de données réussies sur dix résultent d'une erreur humaine. L'expression «Les gens ne pensent pas, ils cliquent» était toujours d'actualité en 2020.

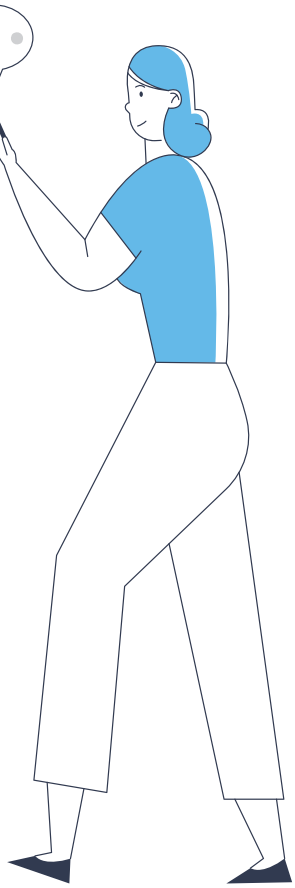
Les pêcheurs d'informations n'ont pas besoin de rechercher des profils «faibles» : peu importe l'âge, la langue, le sexe, l'éducation... tout le monde peut être victime de phishing (ou hameçonnage).

Plus le contenu du courriel sera **court et précis**, plus le destinataire sera tenté d'ouvrir l'URL ou la pièce jointe malveillante. Surtout si une demande d'aide lui est adressée. Pour les cybercriminels, les courriers d'hameçonnage ne sont pas de la grande science ni de la haute littérature : il s'agit simplement de poser la bonne question au bon moment. Et d'office... les gens ne sont que trop heureux d'aider et de compléter les détails.

Lorsqu'un faux message provient d'une personne que le destinataire **connaît** (ou croit connaître), pas moins de 30 % des gens cliqueront sur le lien qu'il contient. Plus les fraudeurs auront effectué de recherches préliminaires et plus le contenu du message sera personnalisé, plus les chances que les destinataires mordent à l'hameçon seront grandes.

Les fraudeurs aiment aussi jouer sur l'**actualité** : même si le fait divers est inventé ou exagéré, les gens veulent connaître tout de suite la nouvelle et réagissent trop vite. Et il n'y a pas que les infos qui retiennent l'attention, les messages des autorités ou les communications d'entreprise font tout aussi bien l'affaire.

On est fragile sur un **mobile** : c'est lorsqu'ils ouvrent leur smartphone que les destinataires sont les plus susceptibles d'être hameçonnés. Sur un smartphone, on survole plus qu'on ne lit un courriel et on clique plus vite sur un lien. Généralement, on est occupé à autre chose en même temps, comme à regarder une émission de télé.



Les escrocs ne prennent pas de **vacances**, malheureusement : alors que la plupart des gens ont tendance à ralentir pendant les mois de vacances, les fraudeurs, eux, passent à la vitesse supérieure.

A noter que le **jeudi** est le jour de l'hameçonnage par excellence : c'est le moment où vous avez le plus de chances de vous faire avoir.

Source: Whitepaper Phished

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

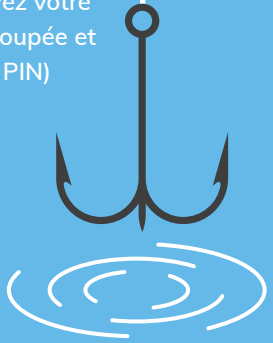
- Phishing paquet Bpost
- Smishing Card Stop

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**

LUTTE CONTRE LA FRAUDE ET L'ESCROQUERIE : PRIORITÉ ABSOLUE POUR LE SECTEUR BANCAIRE EN 2021

En 2020, nous avons constaté une augmentation considérable de toutes les formes de fraude en ligne, y compris le phishing. Dans le cas du phishing, les victimes donnent sans le vouloir - généralement en cliquant sur un lien qui les mène vers un site web frauduleux - leurs codes bancaires personnels aux fraudeurs qui vont alors s'en servir pour effectuer des transactions en leur nom. Nos statistiques montrent qu'**en 2020, environ 67.000 transactions frauduleuses ont été réalisées via phishing, pour un montant total net de quelque 34 millions d'euros. Malheureusement, la fraude ne s'arrête pas avec le passage à une nouvelle année. Tout indique que cette tendance à la hausse se poursuivra en 2021.**

Les conclusions d'une récente étude de Febelfin (mars 2021) menée en collaboration avec le bureau d'études IndiVille sont également préoccupantes :

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.

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

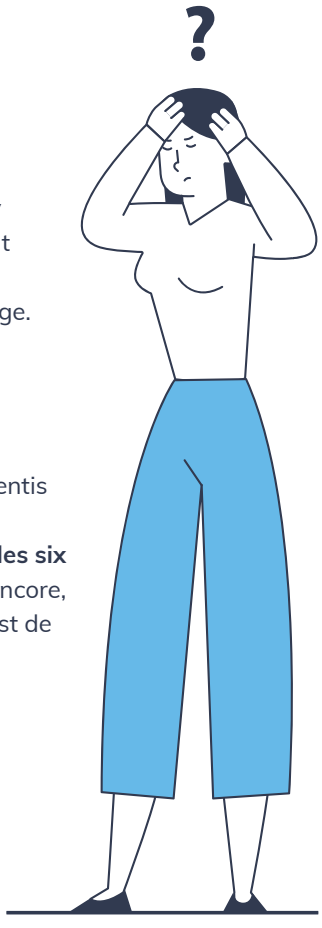
30% des jeunes n'ont **jamais entendu parler du phishing**.

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.

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.*

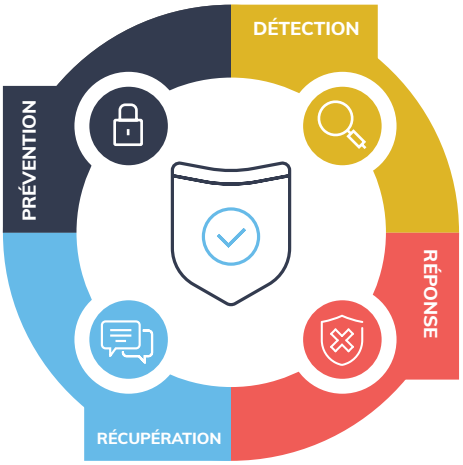
Dans le même temps, les chiffres du dernier Unisys Security Index™ montrent que l'inquiétude des Belges face à la cybercriminalité a diminué. Et c'est inquiétant ! Au niveau mondial, les préoccupations concernant la sécurité sur internet ont diminué de 7 points (de 179 à 172 points) par rapport à l'an dernier. La Belgique suit la tendance générale, mais la diminution de cette inquiétude est beaucoup plus forte chez nous (de 160 à 141 points). Les Belges sont également moins préoccupés par le piratage et les virus informatiques, avec seulement 44% contre 54% l'an dernier.

Ce sont là autant de bonnes raisons de penser que des actions et une sensibilisation permanentes dans ce domaine sont absolument nécessaires auprès de différents groupes cibles, en particulier les jeunes. L'hypothèse selon laquelle les jeunes ont une meilleure maîtrise du numérique ne semble pas se vérifier lorsqu'il s'agit de faire face aux dangers de la fraude en ligne. C'est pourquoi le secteur bancaire considère la lutte contre la fraude et les escroqueries comme une priorité absolue pour 2021. Il continuera dès lors à investir dans des campagnes de sensibilisation axées sur des groupes cibles spécifiques, en collaboration avec les autorités et diverses parties prenantes.

COMMENT LES BANQUES LUTTENT-ELLES CONTRE LE PHISHING ?

Prévention
- Authentifier
- Sensibiliser le client

Récupération
- Contacter les banques concernées
- Contacter les fournisseurs et commerçants



Détection
- Surveiller de manière proactive
- Détecter de manière précoce via la "Fraud Hotline"

Réponse
- Bloquer les sites Web
- Enquêter sur la fraude
- Ajuster les procédures de détection des fraudes
- Garder le taux de faux positifs sous contrôle

Authentification et détection

Les banques ont intégré divers systèmes pour garantir la sécurité des transactions et prévenir et/ou contenir autant que possible la fraude par hameçonnage. Par exemple, l'authentification en deux étapes est requise pour les services bancaires en ligne et mobiles depuis une dizaine d'années. Le client s'identifie au moyen de deux éléments - une carte ou un téléphone, un code PIN, une empreinte digitale ou un scan du visage - pour initier des paiements électroniques. Le secteur bancaire belge a été un précurseur en la matière. L'utilisation de nouvelles techniques biométriques est une perspective à envisager dans un avenir proche. L'intelligence artificielle est elle aussi déjà utilisée par certaines banques pour détecter les fraudes.

Par ailleurs, en investissant dans un suivi intensif, les banques parviennent aussi à réparer une grande partie des dégâts. Ces efforts donnent des résultats remarquables : **plus de 75 % de tous les virements frauduleux** (utilisant un code de réponse « pêché » par les fraudeurs) **sont détectés par les banques et bloqués ou récupérés**.

Equilibre délicat entre convivialité et sécurité

Garantir des **paiements fluides et rapides et une détection efficace des fraudes est un exercice d'équilibre difficile et délicat**. Cela requiert du secteur bancaire des **investissements permanents dans le personnel et les infrastructures**. Mais le **client attend** également **une facilité d'utilisation et des paiements rapides** (il suffit de penser aux paiements instantanés qui permettent à l'argent de se retrouver sur le compte bancaire du destinataire en quelques secondes). Une banque a besoin de temps pour mener une enquête approfondie si une anomalie est détectée. Chaque équipe de lutte contre la fraude a ses propres règles et procédures en la matière. Concilier sécurité et facilité d'utilisation constitue donc un défi pour le secteur. Il s'agit bien d'un véritable exercice d'équilibre.

> **33% des Belges jugent superflues les étapes de sécurité (par ex. la saisie du numéro de carte, le recours à un lecteur de carte) pour les achats en ligne. Ils perçoivent ces démarches plutôt comme un obstacle. Cette attitude est inquiétante, car ces mesures ont été intégrées précisément pour la sécurité du consommateur, déclare Karel Baert, CEO de Febelfin.**

Répéter, encore et encore

Les campagnes de sensibilisation battent également leur plein, le secteur appelant chacun à se montrer vigilant face au phishing et à la fraude en ligne. Les campagnes de conseils, tant sur les médias sociaux qu'à la télévision et à la radio, ont touché un large public cible. Mais il y a encore du travail, comme le montre le nombre de cas de fraudes. Les campagnes de sensibilisation restent nécessaires. Répercutons donc ensemble au maximum le message essentiel : ne partagez jamais vos codes personnels (code PIN et code de réponse).

1 MESSAGE : NE DONNEZ JAMAIS VOS CODES ET NE CLIQUEZ PAS SUR UN LIEN

La crise du coronavirus et les nombreux contacts numériques sont l'occasion pour les fraudeurs d'escroquer les gens. Les différentes formes de phishing sont nombreuses et complexes. Les fraudeurs utilisent non seulement différents canaux - tels que le courrier électronique, la lettre, le téléphone, le SMS, les médias sociaux et WhatsApp - mais ils commettent également des fraudes au nom de différentes organisations et institutions telles que des banques, des administrations publiques, des opérateurs de télécommunications, des entreprises d'utilité publique, etc. La liste est longue. Compte tenu de la grande variété de canaux, **tout le monde est une victime potentielle**.

L'ingéniosité des fraudeurs peut être impressionnante, mais le phishing reste **facile à prévenir** :

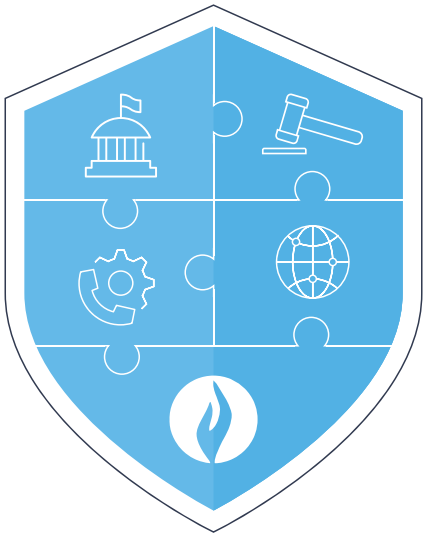
Ne donnez jamais vos codes personnels (code pin et code de réponse) en réponse à un courriel, un appel téléphonique, un sms, un message WhatsApp ou sur un média social.

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.

En résumé, le paiement et la banque numériques sont et restent sûrs, pour autant que vous gardiez vos codes personnels pour vous et fassiez preuve de vigilance. Après tout, on ne donne jamais son portefeuille au premier-venu non plus, n'est-ce pas ?

Nouvelles initiatives

Il est extrêmement important de pouvoir intervenir rapidement, car l'argent passe souvent d'un compte bancaire à un autre en très peu de temps, par l'intermédiaire de mules. C'est pourquoi le «mule stop proces» a été introduit à la mi-2020, afin que la banque de la victime puisse demander efficacement à la banque de la mule de bloquer le montant de la fraude qui a été transféré.



Compte tenu de la nature du problème, il existe non seulement des groupes de travail techniques composés d'experts financiers qui échangent des informations afin de détecter autant que possible les fraudes, mais le secteur travaille également sur des partenariats avec d'autres parties prenantes. Il existe ainsi des initiatives en collaboration avec les opérateurs de télécommunications, les fournisseurs d'accès à internet, le Parquet, la police, les instances publiques et le système judiciaire pour lutter contre le phishing dans toutes ses dimensions et manifestations et pour diffuser le message d'approche et de sensibilisation le plus largement possible. À l'avenir, ces collaborations devraient être encore plus structurées et automatisées. Cela contribuera dans une large mesure à accélérer la vitesse à laquelle des mesures peuvent être prises pour détecter et contrer la fraude.

Ce qui est certain, c'est que la volonté du secteur bancaire en la matière est considérable.

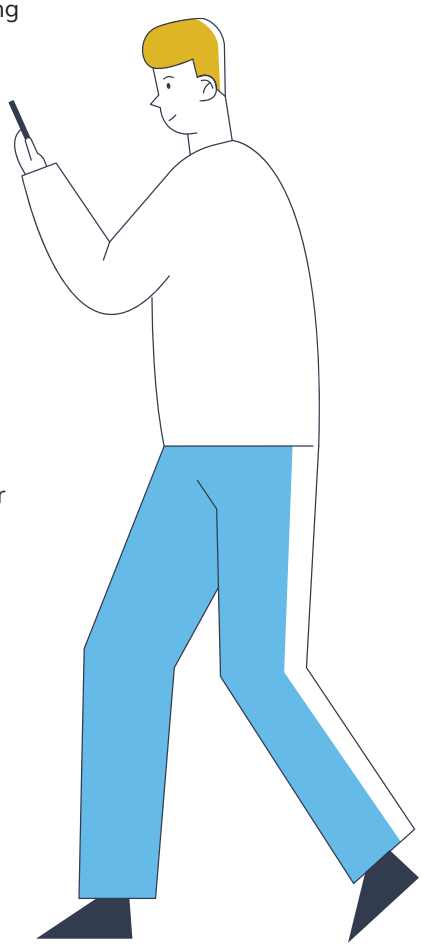
Actuellement, il n'est pas encore possible d'échanger des données personnelles relatives à la fraude en raison de la législation (sur la vie privée). Les banques restent très prudentes dans ce domaine car elles sont liées par la législation et les autorités de contrôle à des réglementations très strictes.

Febelfin examine la possibilité de mettre en place entre institutions financières un système d'échange de données d'identité de mules sur une base légale.

La science peut-elle offrir une solution ?

Pourquoi les gens continuent-ils de cliquer sur des liens ou de se laisser piéger par d'autres formes de fraude ? La science du comportement nous dit que cela peut tenir au fait qu'à ce moment précis, notre cerveau passe en mode «pensée rapide» et que nous ne réfléchissons plus rationnellement. Les fraudeurs exploitent habilement un certain nombre de mécanismes qui interviennent à ce moment-là :

- **Loss aversion :** la peur d'enregistrer des pertes
- **Social influence :** changement d'attitude ou de comportement causé par une pression extérieure, réelle ou imaginaire.
- **Unrealistic optimism :** nous pensons toujours que le phishing ne passera pas par nous.
- **Discounting :** les gens sont toujours très réceptifs aux grands rabais ou aux éditions limitées.
- **Availability heuristic :** sorte de raccourcis vers des exemples directs qui parlent à notre mémoire.



Toutefois, ces mêmes mécanismes peuvent être utilisés pour développer des techniques comportementales qui incitent subtilement les gens à se comporter d'une certaine manière ou, pour le dire autrement, qui les «poussent» (nudging). Pour l'instant, il n'a pas encore été réalisé beaucoup d'expériences scientifiques recourant au nudging pour limiter le phishing. Quelques premiers pas ont été accomplis dans ce sens au Royaume-Uni et aux Pays-Bas. Febelfin suit de près ce dossier et entend poursuivre l'examen de ces expériences.

Toujours rester au fait

Notre «académie interne», Febelfin Academy, a développé un large éventail de formations pour tous les «groupes cibles» au sein de l'institution financière - des collaborateurs commerciaux aux experts produits et aux dirigeants. Cela permet à tous les acteurs du secteur de rester au courant. Febelfin Academy travaille en étroite collaboration avec les milieux business (experts des institutions financières) ainsi qu'avec des formateurs et des organisations de niveau international (par exemple, le FMI).

Vous trouverez ci-dessous une sélection de leur offre :

- Sensibilisation générale de tous les collaborateurs des institutions financières : e-learning basé sur des situations concrètes avec des exercices et des simulations, à visée tant privée que professionnelle.

  Cyber security: Do's & Don'ts (eng) - e-learning

- Formation pour les experts en fraude/cyber : formations avancées avec certification

  Business and digital transformation skills (The Master Channel) - online courses

  Traject Certified Fraud Examiner (CFE) - en collaboration avec le FMI

- Formations pour les gestionnaires de produits dans le contexte des paiements : PSD2 et SCA

  PSD2 & Open banking: impact on the financial ecosystem and new challenges

- Gestion des risques : la cybersécurité est clairement l'un des principaux nouveaux domaines de risque pour nos membres et une attention toute particulière lui est consacrée dans les cours de gestion des risques – surtout maintenant, dans le contexte du coronavirus – le groupe cible étant les gestionnaires de risques et les managers compliance.

  CoVID 19: New challenges in Risk Management - Live Webinar

  Masterclass in Risk Management

- Efficacité du Conseil d'Administration : programme exécutif pour les membres du Conseil d'Administration axé sur les cyberrisques et la manière de gérer ceux-ci en tant que responsable - quelles questions poser pour s'armer contre les cyberrisques.

  Executive program - The Board of Directors in the Financial Sector

UN GRAND FILET DE PÊCHE EST NÉCESSAIRE

Cependant, le secteur se heurte aux **limites** de ce qu'il peut faire seul. Ces dernières années, nous avons vu les plus grands catalyseurs de la fraude se déplacer hors du secteur bancaire vers d'autres secteurs, une tendance qui n'a fait que se renforcer avec la pandémie. Les criminels contournent de plus en plus souvent les systèmes de sécurité sophistiqués des banques.
Néanmoins, nous devons également veiller à ce que cette fraude cesse.

Le phishing n'est pas le problème du seul secteur bancaire, c'est un **phénomène de société**. Nous sommes à un point de basculement. Tous les **secteurs** doivent assumer conjointement leur **responsabilité** dans cette lutte, il suffit de penser aux télécoms et aux plates-formes de commerce en ligne. Et ce n'est qu'ensemble que nous pourrons tenter d'enrayer autant que possible la fraude. Il y a encore une marge importante pour une coopération étroite, non seulement sur une base sectorielle mais aussi par-delà le secteur.

Les liens entre la fraude, le crime organisé et le terrorisme constituent une menace importante et croissante pour la sécurité nationale. Les bandes criminelles impliquées utilisent le produit de la fraude pour financer d'autres activités nuisibles et illégales, causant des souffrances et des dommages indicibles à notre société. Il est donc crucial que le gouvernement assume sa responsabilité en la matière et examine comment créer un cadre législatif approprié. Des capacités et des moyens suffisants doivent également être alloués pour que les services de police puissent faire leur travail et lutter contre les bandes criminelles.

Tout le monde est impliqué dans la lutte contre la cyberfraude. Les paiements sécurisés sont une responsabilité partagée : le secteur bancaire garantit une infrastructure numérique sécurisée, le client est informé et vigilant, la police et le Parquet poursuivent le crime et les pouvoirs publics fournissent le cadre juridique adéquat. Si nous pouvons maintenir cet équilibre, les dommages peuvent être limités. **Ce n'est qu'ensemble que nous pourrons gagner cette bataille, en gardant à l'esprit que chaque cas de phishing est un cas de trop.**

febelfin

Fédération belge du secteur financier

www.febelfin.be