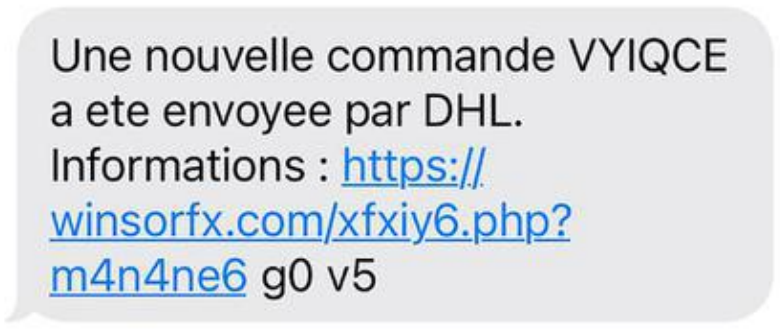
**7.424**
2020

**+ 201,79 %**

**2.460**
2019

**+ 87 %**

**1.314**
2018




## 34.000.000

**En euros, le butin total des « phishers » en 2020 ; 67.000 transactions frauduleuses leur ont permis d'atteindre ce montant.**

## 3.225.234

**Le nombre de messages transférés à l'adresse suspect@safeonweb.be en 2020. En moyenne, cela fait plus de 8.800 messages par jour. C'est une augmentation de 90 % par rapport à 2019.**

## 506

**Le nombre de plaintes pour phishing déposées auprès de l'Ombudsfin (médiation des services financiers) en 2021 (chiffres arrêtés au 1er septembre 2021), ce qui constitue déjà une augmentation de 28 % par rapport à l'ensemble de 2020. C'est un tiers de l'ensemble des plaintes.**

## Récupérer l'argent dérobé : du cas par cas

**Sur les 34 millions disparus l'année passée via du phishing, combien les victimes ont-elles pu retoucher ? Febelfin n'a pas la réponse. Pas plus que les banques, plutôt discrètes sur le sujet. Une seule chose à retenir : un remboursement n'est jamais garanti. « C'est vraiment du cas par cas », glisse l'une d'elles. « Chaque fraude fait l'objet d'une enquête approfondie », confie une autre.**

**En réalité, la question est délicate. « Les règles ne disent pas dans quel cas on a un remboursement ou pas », pose d'emblée Rodolphe de Pierpont, le porte-parole de Febelfin. « Mais une directive européenne donne les grands principes. En substance, elle dit qu'en cas de fraude au système bancaire, la banque doit rembourser, sauf si le client a fait preuve de négligence grave. »**

**Une notion qui est évidemment sujette à interprétation. « Dans l'enquête menée par la banque, toute la question est de savoir si le client a été négligent, a transmis ses codes sans faire attention, etc. » Dans les faits, Febelfin assure que les remboursements sont nombreux. Mais dans les services de l'Ombudsfin (le médiateur du service financier), les plaintes concernant le phishing augmentent. « C'est la problématique qui nous est le plus soumise, et de loin. Elle concerne toutes les banques », souligne Jean Cattaruzza, l'ombudsman. Durant les neufs premiers mois de cette année, un tiers des 1.450 plaintes reçues (et recevables) par ses services concernaient le phishing. Pour l'ensemble de 2020, ce n'était encore qu'un quart.**

**Ici, c'est l'éventuelle intervention humaine qui sert de ligne de démarcation. « On considère que, lorsque la victime a fait ses manipulations devant un écran, elle n'est pas consentante à ce qui va se passer après. Par contre, lorsqu'elle est sollicitée pour donner oralement son code, là, on estime que l'on est aux confins de la négligence grave. Les banques ne font pas forcément cette distinction. Elles estiment qu'il y a négligence dans les deux cas. » Bref, la prudence est donc plus que jamais recommandée. Reste une piste pour ceux qui souhaitent se protéger. Certaines assurances commencent à proposer des cyberpolices aux particuliers.** C.DA.

suites pénales plus difficile, la capacité policière, le mauvais outillage pour lutter contre les organisations criminelles à l'étranger, etc. », détaille Martin François, porte-parole du parquet de Bruxelles.

### Prévention : une collaboration indispensable

Finalement, une des solutions les plus efficaces contre le phishing reste d'éviter que la personne ne clique sur le lien. D'où l'importance de la prévention. En première ligne : le CCB et son outil, évoqué plus haut. « On traite les mails que l'on reçoit de façon automatisée. Si les liens sont frauduleux, on les fait bloquer via les moteurs de recherche et on diffuse sur la fausse page un message prévenant l'utilisateur », commente Katrien Eggers, la porte-parole de la structure qui a bloqué l'année passée plus de 670.000 liens frauduleux.

Autres institutions capables de faire barrage : les banques. D'après Febelfin, plus de 75 % de tous les virements frauduleux ont été détectés, bloqués ou récupérés par les établissements bancaires l'année passée. Là encore, c'est automatique. Des outils sophistiqués effectuent un screening des ordres de paiement et des transactions. « Nous détectons des comportements qui pourraient être frauduleux. Nous bloquons ensuite la transaction suspecte et on prend contact avec le client », explique Alexandre Pluvinage, responsable de la sensibilisation à la fraude chez ING.

Blocage également de mise chez les opérateurs télécoms. A la manœuvre : l'Institut belge des services postaux et des télécommunications (IBPT). « Dès qu'il y a un SMS manifestement frauduleux, il est transmis aux opérateurs mobiles avec la demande de blocage du numéro. Ces SMS sont souvent signalés via l'un des opérateurs, via leurs clients », explique Jimmy Smedt, le porte-parole de l'IBPT. Aujourd'hui, une coopération entre les différents acteurs se développe de plus en plus. Mais d'après plusieurs de nos interlocuteurs, elle doit encore être approfondie et même automatisée pour contrer un phénomène qui, lui, ne présente aucun signe d'essoufflement.

## Un mystérieux virus nommé Flubot

**Rarement un virus avait infecté autant de smartphones dans le Royaume. La première vague de Flubot a eu lieu en mai dernier ; 5.000 clients ont alors été bloqués et 12.000 appareils probablement infectés. La deuxième s'est déroulée du 6 au 13 septembre, avec deux millions de SMS frauduleux circulant par jour. Vous l'aurez compris, Flubot se propage par SMS. La personne ouvre un message lui demandant de télécharger une application. Si elle s'exécute, le virus peut prendre le contrôle total du GSM et, surtout, envoie des SMS au nom de la victime vers tous les contacts de son répertoire. Reste qu'à l'heure actuelle, aucune somme d'argent n'aurait été dérobée grâce à ce virus. A quoi sert-il, alors ? Personne ne sait, mais tout le monde s'accorde sur sa dangerosité : il peut capturer des données, même bancaires, avoir accès aux mots de passe, etc.** C.DA.

DUMPING SOCIAL

# Huit personnes déférées au juge d'instruction, une sous mandat d'arrêt et d'importantes saisies

Quatre-vingts enquêteurs de la Police judiciaire fédérale de Bruxelles et 26 inspecteurs sociaux de l'ONSS : les effectifs belges déployés dans le cadre d'une vaste opération policière qui s'est tenue ce mardi sous la coordination d'Europol sont loin d'être légers. Dans le viseur ? « Un réseau de sociétés belges et étrangères et de leurs gérants organisant une vaste fraude au dumping social », fait savoir l'Auditorat du travail de Bruxelles, en charge de l'enquête (pour laquelle une instruction a été ouverte). « Cette organisation criminelle faisait venir des ouvriers roumains en Belgique via des sociétés implantées dans divers pays européens et ce, sans respecter les règles européennes et nationales en matière de détachement, d'assujettissement des travailleurs à la sécurité sociale et de conditions de travail, dont la rémunération. » Visiblement, ce sont des observations effectuées sur un chantier par le Contrôle des lois sociales (CLS, le service d'inspection sociale spécialisé du SPF Emploi) qui ont mis la puce à l'oreille des enquêteurs. Pour l'heure, le chantier concerné par ces constats ainsi que les noms des sociétés belges visées par l'enquête sont gardés secrets par le magistrat en charge de l'enquête.

A l'issue d'une trentaine de perquisitions organisées de manière simultanée en Belgique, au Luxembourg et en Italie – avec le concours des polices des pays concernés –, on sait néanmoins que 32 véhicules de luxe ou professionnels, d'importantes sommes d'argent en cash (300.000 euros) ainsi que « de nombreux objets de valeur et des biens immobiliers » ont été saisis. Toujours d'après l'Auditorat du travail de Bruxelles, huit personnes ont été déférées à la juge d'instruction en charge de l'affaire et une personne a été placée sous mandat d'arrêt européen en Italie. A.SE.