Prévention de la fraude individuelle

Boîte à outils

du REPC N° 13

EUCPN
EUROPEAN CRIME PREVENTION NETWORK

eu2018bg.bg
Българско председателство на Съвета на Европейския съюз

Individual fraud is a type of fraud in which individual citizens are being targeted by criminals and are persuaded into a cooperative mindset. The essential tactic to nudge the victim into this compliant relationship is called social engineering. This allows the offender to obtain the confidence from the victim that is crucial to the success of the scam.

REMERCIEMENTS

Cette boîte à outils a été élaborée en étroite collaboration entre le secrétariat du REPC et la présidence bulgare. Nous tenons à les remercier pour les efforts qu'ils ont déployés au cours de leur présidence et pour l'organisation d'un séminaire sur les escroqueries téléphoniques.

De plus, nous souhaiterions remercier tous les représentants nationaux, suppléants et points de contact universitaires du REPC pour leur soutien continu à notre travail, pour avoir partagé leur expertise et pour avoir fourni des informations pour cette boîte à outils.

Nous tenons à remercier tout particulièrement les experts qui ont accepté de participer à l'atelier que nous avons organisé en relation avec cette boîte à outils :

- Mark Button, Université de Portsmouth, Royaume-Uni
- Michael Will, Europol, AP Furtum
- Simeon Dimchev, Section des fraudes de la Direction générale de la police nationale, Bulgarie
- Charlotta Mauritzson, Centre national de la fraude, Suède
- Andries Bomans, Centre pour la cybersécurité, Belgique
- Constantin Lica, Département de lutte contre la fraude, Roumanie
- Aurelian Bocan, Direction générale de la police de Bucarest, Roumanie
- Romana Mazalová, projet « Nedáme se », République tchèque

Citation
REPC (2018). Série Boîte à outils n° 13 du REPC - Prévention de la fraude individuelle. Bruxelles

Mentions légales
Le contenu de cette publication ne reflète pas nécessairement l'opinion officielle d'un État membre de l'UE ou d'une agence ou institution de l'Union européenne ou des Communautés européennes.

Auteurs/éditeurs
Jorne Vanhee, Chargé de recherche, Secrétariat du REPC, Bruxelles, Belgique
Febe Liagre, Chargé de stratégie et de politique, Secrétariat du REPC, Bruxelles, Belgique

Dans le cadre du projet « La poursuite de la mise en œuvre de la MAS du REPC et du réseau informel sur l'approche administrative » - Secrétariat du REPC, novembre 2018, Bruxelles.

Avec le soutien financier du Programme de prévention et de lutte contre la criminalité de l'Union européenne Commission européenne - Direction générale Affaires intérieures

CONTENTS

Remerciements 3

Avant-propos 6

Résumé analytique 8

01 **Introduction** 14

Image du renseignement 18

1. Introduction ... 18
2. L'art de la persuasion ... 22
3. Choisissez votre escroquerie ... 32
4. Calculer les chiffres ... 42
5. Conclusions ... 48

02 **Bonnes pratiques** 50

1. Introduction ... 51
2. Si cela semble trop beau pour être vrai, tel est probablement le cas. ... 56
3. Prévenir les escroqueries téléphoniques : en quoi puis-je vous aider ? ... 63
4. Conclusions ... 68

03

Exemples tirés de la pratique 70

“ Escroquerie de la grand-mère - tu connais ? ” (AT) 70
Bonjour grand-mère, j’ai besoin d’argent (DE) 72
Silver Surfer (LU) 73
N’essayez pas de me berner (SE) 74
Autriche : La liste de surveillance de l’Internet 75
Section des fraudes de la Direction générale de la police nationale bulgare (BG) 76
Mécanisme anti-de la First Investment Bank en Bulgarie (BG) 77
#CyberScams (EC3, Europol) 78
Dans quelle mesure êtes-vous à l’abri du hameçonnage ? (BE) 78
Nedáme se (Nous ne le prendrons pas) (CZ) 79
Le prix de l’amitié (RO) 80
Guide de sécurité pour les aînés (FI) 80
“ Trucs contre les beaux parleurs ” (NL) 81
Action fraud (Royaume-Uni) 81

Endnotes 82

Bibliographie 83

AVANT-PROPOS

La 13e boîte à outils de la série publiée par le secrétariat du REPC se concentre sur le thème principal de la présidence bulgare : la fraude, avec une attention particulière aux escroqueries téléphoniques. Comme la fraude couvre toute une palette de sujets, nous avons décidé de nous focaliser sur la fraude individuelle. Il s'agit de fraudes commises contre des individus par des individus ou des organisations criminelles. Ce type de fraude est devenu, chaque jour davantage, une entreprise rentable et transfrontalière, que certains spécialistes qualifient même « d'escrocs professionnels ». Par conséquent, ce type de criminalité mérite une approche à l'échelle de l'UE. C'est également ce qui ressort du document d'orientation qui est rédigé en tandem avec la présente boîte à outils.

Cette boîte à outils se compose de trois parties. La première tente de brosser un tableau de la situation actuelle en matière de renseignements sur la fraude individuelle. Nous discutons des bonnes pratiques intéressantes dans la deuxième partie et formulons également quelques recommandations sur la manière de prévenir les escroqueries téléphoniques. Ces bonnes pratiques sont énumérées dans la troisième partie. Un résumé analytique est également fourni au lecteur.

RÉSUMÉ ANALYTIQUE

La treizième boîte à outils de la série publiée par le secrétariat du REPC porte sur la prévention de la *fraude individuelle*. La présidence bulgare (premier semestre 2018) a décidé de se concentrer sur :

> " [...] *les questions liées à la fraude, en particulier les escroqueries téléphoniques. Au cours de ces dernières années, ce type de criminalité est devenu une activité criminelle rentable, qui se développe tant au niveau national que transfrontalier. Les groupes criminels spécialisés dans cette activité se développent de façon dynamique et frappent un plus grand nombre de victimes. Compte tenu de la participation active des victimes et de leur implication dans des scénarios criminels et de l'effet traumatisant sur l'esprit des victimes, des efforts sérieux de prévention doivent être déployés, en tenant compte des spécificités aux niveaux local, national et transfrontalier.* "

La fraude individuelle est un type de fraude dans lequel des citoyens sont la cible de criminels. Les victimes sont persuadées d'adopter un esprit de coopération et sont ensuite victimes de fraude. Notre compréhension actuelle de ce type de fraude est principalement liée à ses formes contemporaines, l'hameçonnage en étant l'exemple le plus probable. Toutefois, il est important de reconnaître que la fraude individuelle existe depuis longtemps. Les évolutions technologiques constatées au cours des dernières décennies ont permis d'industrialiser ces escroqueries à une échelle plus grande que jamais imaginée. Qui n'a jamais reçu un e-mail d'hameçonnage de sa vie ?

Comme l'indique clairement le *raisonnement* de la présidence bulgare, les victimes participent activement à leur victimisation. Le délinquant a ciblé l'argent de la victime, mais il ne peut y avoir accès qu'en persuadant la victime de participer. La tactique essentielle pour pousser la victime dans cette relation de bienveillance est appelée **l'ingénierie sociale**. Cela permet au contrevenant de gagner la confiance de la victime, ce qui est essentiel au succès de l'escroquerie. La psychologie sociale nous offre une meilleure compréhension de ce phénomène. En recourant aux principes sociaux quotidiens et en exploitant ces « faiblesses humaines », les délinquants parviennent à activer ce que l'on appelle la deuxième

voie de persuasion. La première voie exige une réflexion et un effort cognitif intenses. Toutefois, la seconde ne nécessite pas une véritable élaboration et réagit presque inconsciemment. Par exemple, en se présentant en la qualité d'une personne d'autorité, telle un policier, les délinquants peuvent facilement obtenir un certain degré d'obéissance de la part de leurs victimes. Ces règles sociales et cognitives empiriques ont leur utilité quotidienne, mais permettent aux délinquants de les exploiter à leur propre avantage.

Ces tactiques trompeuses sont utilisées dans une grande **variété d'escroqueries**. *419 escroqueries, escroqueries de personnes âgées, escroqueries amoureuses, fraudes de PDG, ...* les possibilités sont aussi infinies que la créativité des escrocs. Cette gamme de stratagèmes trompeurs permet aux fraudeurs de cibler un très large public ou d'adopter une approche plus personnalisée. Cette dernière option semble être de plus en plus privilégiée. Les escrocs ont réalisé que, en ciblant intelligemment leurs victimes, ils obtiennent un meilleur « retour sur investissement ». Les courriels d'hameçonnage deviennent de plus en plus sophistiqués et s'adressent à une cible (un groupe) unique. La dernière étape surprenante de cette évolution implique la combinaison d'une nouvelle et d'une ancienne technologie : le téléphone. Le Vishing ou hameçonnage vocal permet de combiner les avantages de l'Internet et du téléphone. Passer un appel téléphonique en ligne n'engendre pratiquement aucun coût, est plus difficile à retracer et peut être automatisé. L'utilisation du téléphone présente d'autres avantages : les gens lui font davantage confiance et, grâce à un cadre plus intime, les victimes sont persuadées plus efficacement. Illustration du niveau de sophistication croissant : les délinquants embauchent même des locuteurs natifs pour que les appels téléphoniques soient aussi authentiques que possible.

Notre compréhension actuelle de la fraude individuelle est toutefois limitée. Un **chiffre gris** entoure ce délit, car nombre de ces escroqueries ne sont pas rapportées. Les victimes ne savent pas qu'elles ont été victimisées, elles ne le perçoivent pas comme suffisamment grave, elles ne pensent pas que le signalement mènera à quoi que ce soit ou elles ne savent tout simplement pas où le signaler en premier lieu. De plus, en raison du rôle actif que la victime joue dans sa propre victimisation, les sentiments de culpabilité et d'embarras l'empêchent de raconter son histoire. Certaines escroqueries ont même des mécanismes d'anti-signalement « intégrés », car les victimes doivent entreprendre des actions illégales dans le cadre de ce stratagème, s'incriminant elles-mêmes dans le processus. Signaler l'arnaque consisterait à avouer sa propre implication.

Ce chiffre gris a également fait naître le **mythe** selon lequel les personnes âgées sont les principales victimes de ce délit, car elles sont des proies faciles. Certaines études ont réfuté ce mythe, bien que nous devions rester prudents en raison du peu de recherches disponibles. Néanmoins, la population plus jeune et le groupe d'âge moyen seraient plus vulnérables aux escroqueries. Un autre mythe implique que les victimes sont généralement dépeintes comme ignorantes ou financièrement illettrées, mais le contraire semble se confirmer. Une des explications possibles est le « fossé du savoir-faire », impliquant que les personnes reconnaissent les signaux d'une escroquerie, mais ne parviennent pas à appliquer ces connaissances à leur propre situation.

Malheureusement, l'existence de ce qu'il est convenu d'appeler des « **listes des dupes** » n'est pas un mythe. Les fraudeurs par téléphone peuvent contacter leurs victimes au hasard ou en consultant les registres publics, mais ils partagent également entre-eux des listes contenant des cibles qui ont déjà été victimes de fraude. L'utilisation de ces listes est révélatrice du niveau élevé de victimisation répétée. Par exemple, certains arnaqueurs tenteront de vous « aider » à récupérer vos actifs perdus...

Étant donné qu'il est extrêmement difficile de contrôler ce délit, le besoin de prévention est élevé. Toutefois, peu de recherches universitaires et évaluatives ont été menées sur la fraude individuelle. Néanmoins, nous pouvons formuler quelques conclusions générales. La tactique de prévention la plus courante consiste à éduquer le public. Cela peut être fait dans le cadre d'une campagne générale de sensibilisation, pouvant générer des effets positifs, surtout lorsqu'elle est menée sous une forme ou l'autre de formation. Essentiellement, ces formations tentent de combler le fossé « savoir-faire » que nous avons cité ci-dessus. Une autre tactique clé consiste à travailler avec les victimes. Vu leur rôle actif et le risque existant d'être abusées à plusieurs reprises, les victimes devraient être soutenues et informées de leur position spécifique.

Au cours de la présidence bulgare, le Secrétariat a collecté plusieurs **bonnes pratiques** en la matière. Elles peuvent être classées en fonction de leur groupe cible. Une première catégorie cible l'ensemble de la population. Il s'agit de campagnes de sensibilisation, telles que celles menées en Bulgarie, Suède, Belgique ou par Europol. Il s'agit de spots radiophoniques, d'affiches, de dépliants, de gadgets,... qui fournissent des informations utiles au public et montrent comment se protéger pour ne pas être abusé. Une deuxième série d'activités

vise les personnes âgées. En l'occurrence, des méthodes plus interactives sont mises en œuvre, comme tel est le cas en République tchèque. Les personnes âgées participent à un jeu de rôles éducatif et interactif dans le cadre duquel elles apprennent à connaître les schémas trompeurs les plus courants et comment y réagir. Cette « expérience vécue » devrait leur permettre de réagir de manière adéquate dans des scénarios réels. L'évaluation de ce projet a prouvé la véracité de cette hypothèse puisque le groupe a refusé deux fois et demie plus de fausses offres qu'un groupe témoin qui n'a pas regardé le jeu de rôles. La dernière catégorie d'activités de prévention était centrée sur les victimes. Des exemples de l'Australie, du Royaume-Uni et du Canada ont démontré la nécessité de ce type de prévention. Il existe cependant - même à l'échelle mondiale - peu de services de soutien aux victimes de fraudes individuelles.

Enfin, le secrétariat du REPC a organisé un atelier avec différents experts pour formuler des **recommandations** sur la manière de prévenir les escroqueries téléphoniques. Elles sont structurées conformément aux cinq stratégies de prévention du crime situationnel. La première stratégie possible consiste à intensifier les efforts qu'un contrevenant doit déployer pour que l'escroquerie réussisse. Restreindre la publication et l'accès aux numéros de téléphone peut déjà y parvenir. Une autre technique pourrait consister à limiter le nombre de numéros de téléphone qu'une personne peut posséder ou, au moins, à limiter leur association à un compte bancaire ou à un numéro d'identification.

Une deuxième stratégie consiste à augmenter les risques. Dans ce cadre, il est essentiel de partager les informations. Ce partage ne doit pas s'arrêter aux frontières du secteur public ou privé, ni au niveau national. Tous les partenaires ont un rôle important à jouer dans la collecte des informations. Connaître ce à quoi vous êtes confronté augmente les chances d'éviter la survenance en premier lieu. Il va sans dire que les rapports devraient être plus faciles et plus accessibles. Les informations doivent être collectées avant de pouvoir être partagées. D'autres recommandations ont été formulées pour réduire l'anonymat de l'appelant, en rendant presque impossible l'usurpation de votre position. Les logiciels de reconnaissance vocale pourraient également présenter un intérêt à cet égard.

La réduction des gains pouvant être dégagés de la commission du délit désigne une troisième stratégie permettant de prévenir les escroqueries téléphoniques. En l'occurrence, la principale recommandation est de saisir les avoirs obtenus illégalement. Pour ce faire, le contrôle des flux d'argent est crucial pour détecter les transactions suspectes. Nos experts ont recommandé une initiative menée à

l'échelle européenne et associant le secteur bancaire pour faciliter ce processus.

Une autre stratégie consiste à réduire les incitations. À cet égard, il est important de ne pas partager un trop grand nombre d'informations sur la manière dont l'escroquerie a été réellement exécutée, car cela permettra d'éviter l'avènement « d'imitateurs ». Cela pourrait également contribuer à prévenir certaines formes de victimisation répétée.

La dernière stratégie consistait à supprimer les excuses. Elle se focalise essentiellement sur la sensibilisation aux escroqueries téléphoniques et sur la manière de se protéger. Dans ce cadre, les bonnes pratiques du passé sont présentées comme des exemples clés. Les campagnes de sensibilisation devraient diffuser un message identique. Par conséquent, des partenariats public-privé et une coopération internationale doivent être noués afin d'être aussi cohérents que possible : *il suffit de dire non.*

INTRODUCTION

Les exemples d'activités frauduleuses de criminels qui tentent d'obtenir de l'argent durement gagné et/ou des renseignements personnels, ne manquent pas, à l'instar du nombre de personnes abusées (Crosman, 2017). Qui n'a pas reçu cette « offre unique » dans sa boîte de réception ou n'a pas entendu parler de l'escroquerie relative au Support Microsoft qui vous appelle pour pouvoir réparer votre ordinateur qui fonctionnait très bien il y a quelques minutes ?

Contrairement à la croyance populaire, ces types d'escroqueries sont loin d'être nouveaux. Les escroqueries et les fraudes existent depuis des siècles (Murphy et Murphy, 2007). La compréhension actuelle de la fraude individuelle est intrinsèquement liée aux nouvelles technologies, telles que l'Internet, mais la fraude existe depuis que l'Homme maîtrise la parole et possède des biens (Button et Cross, 2017). En effet, l'Internet a fourni aux criminels un nouvel espace pour escroquer un nombre de victimes plus élevé qu'ils ne l'avaient jamais imaginé (Whitty, 2013). Des technologies nouvelles et plus anciennes, telles que le téléphone, sont combinées pour adapter les attaques et maximiser les profits. La portée et l'efficacité ont augmenté, les coûts ont diminué, mais les techniques de base sont demeurées les mêmes (Crosman, 2017 ; Button et Cross, 2017 ; Button, McNaughton, Kerr et Owen, 2014). Ces nouveaux développements, combinés à l'impact préjudiciable - financier, émotionnel, relationnel,... - de ces types de criminalité (Button, Lewis, & Tapley, 2009;2014), ont mis en exergue la nécessité de la prévention et la Bulgarie en a fait son cheval de bataille pendant sa présidence du REPC au cours du premier semestre 2018 :

'Dans le cadre de la prévention, la présidence bulgare se concentrera sur les questions liées à la fraude, et en particulier les escroqueries téléphoniques. Au cours de ces dernières années, ce type de criminalité est devenu une activité criminelle rentable, qui se développe tant au niveau national que transfrontalier. Les groupes criminels spécialisés dans cette activité se développent de façon dynamique et frappent un plus grand nombre de victimes. Compte tenu de la participation active des victimes et de leur implication dans des scénarios criminels et de l'effet traumatisant sur l'esprit des victimes, des efforts sérieux de prévention doivent être déployés, en tenant compte des spécificités aux niveaux local, national et transfrontalier.

Cette boîte à outils fournit des renseignements utiles sur ces types de fraude et d'escroquerie et sur leur prévention. La première partie de cet effort s'appuiera sur la littérature existante pour faire la lumière sur ce sujet qui est de plus en plus étudié par les chercheurs. Jusqu'à récemment, les études (criminologiques) ont relativement négligé la fraude au profit d'autres crimes de masse, mais cela a changé (Button & Cross, 2017 ; Button, Lewis, & Tapley, 2009;Button, Lewis, & Tapley, 2014;Titus & Gover, 2001;Levi, 2008 ; Button, Tapley, & Lewis, 2012).

Dans la deuxième partie, nous présenterons quelques bonnes pratiques liées à ce délit et formulerons quelques recommandations et conseils pour des mesures préventives visant les escroqueries téléphoniques en particulier. Ces recommandations se fondent sur un atelier qui a réuni divers experts de toute l'Union européenne. Enfin, une troisième partie dressera la liste de quelques bonnes pratiques qui ont été recueillies lors de la production de cette boîte à outils.

01 PARTIE I:

IMAGE DU RENSEIGNEMENT

1. Introduction

Cette première partie de la boîte à outils explorera la littérature actuelle sur le sujet des escroqueries et des fraudes. Plus précisément, nous nous concentrerons dans cette boîte à outils sur la fraude au niveau individuel, commise principalement (mais pas exclusivement) au moyen des TIC (Button, Tapley, & Lewis, 2012). La fraude est une infraction très diversifiée et englobe un large éventail de comportements (Button, Lewis et Tapley, 2014). Levi et Burrows (2008) la définissent comme telle :

> *" La fraude désigne l'obtention d'un avantage financier ou la cause d'un préjudice par tromperie implicite ou explicite ; c'est le mécanisme par lequel le fraudeur obtient un avantage illicite ou cause un préjudice illicite "* (Levi & Burrows, 2008, p. 7).

En général, nous pouvons affirmer que tous les types de fraude impliquent une forme de tromperie ou de ruse dans l'intention d'en tirer un gain (Button, Lewis, & Tapley, 2009;Murphy & Murphy, 2007;Button et Cross, 2017). En classant les fraudes selon le type de victime, Levi (2008) a établi la typologie suivante :

Secteur des victimes	Sous-secteur des victimes	Exemples de fraude
Privé	Services Financiers	- Fraude par chèque - Contrefaçon de propriété intellectuelle et produits vendus comme authentiques - Monnaie contrefaite - Fraude à l'intégrité des données - Détournement de fonds - Délit d'initié/abus de marché - Fraude à l'assurance - Fraude sur les prêts - Fraude par carte de paiement - Fraude à la passation de marchés
	Fraude non-financière	- Fraude par chèque - Contrefaçon de propriété intellectuelle et produits vendus comme authentiques - Monnaie contrefaite - Fraude à l'intégrité des données - Détournement de fonds - Fraude au jeu - Fraude aux prêts - Fraude à la carte de paiement - Fraude à la passation de marchés
	Individus	- Fraude liées aux organismes de bienfaisance - Fraude à la consommation - Contrefaçon de propriété intellectuelle et produits vendus comme authentiques - Monnaie contrefaite - Fraude en matière d'investissement - Fraude de type pension
Public	Organismes nationaux	- Fraude aux prestations - Détournement de fonds - Fraude à la passation de marchés - Fraude fiscale
	Organismes locaux	- Détournement de fonds - Fraudes en matière de taxes immobilières - Fraude à la passation de marchés
	International (mais affectant le public)	- Fraude à la passation des marchés (par des entreprises nationales face à d'autres entreprises - principalement mais pas toujours étrangères - pour obtenir des contrats à l'étranger) - Fraude aux fonds européens

Lorsque nous nous concentrons sur le secteur des victimes privé, et plus particulièrement sur le sous-secteur des individus considérés en leur qualité de victimes, il existe encore de nombreuses façons différentes d'être abusé, comme l'illustre la même figure. Dans le cadre de cette boîte à outils, toutefois, nous nous concentrerons sur la fraude à la consommation, que Levi et Burrows (2008) définissent comme suit :

> *" une vaste catégorie comprenant les escroqueries à la loterie et aux prix ; les fraudes par appels malhonnêtes et autres fraudes fondées sur les communications ; les descriptions erronées " malhonnêtes " de produits et de services (tels que certains " produits de soins de santé alternatifs " ou aides sexuelles) ; les fraudes liées au jeu (p. ex., les courses et matchs " fixes " sur lesquels des paris ont été placés (dont les paris sur la marge) ; les achats de biens et services non envoyés par le fournisseur "* (Levi et Burrows, 2008, p. 7).

D'autres termes qui circulent dans la littérature sont « fraude individuelle » (Button, Tapley, & Lewis, 2012) et fraude par marketing de masse (Button, Lewis, & Tapley, 2009;Whitty, 2018 ; 2015 ; Wood, Liu, Hanoch, Xi, & Klapatch, 2018), bien que ce dernier se concentre plus strictement sur les techniques de communication de masse qui sont utilisées (Button & Cross, 2017). Dans un souci de cohérence au sein de cette boîte à outils, nous utiliserons ci-après les termes « fraude individuelle », car ils reflètent le mieux notre cible. Les conceptions actuelles de ce type de fraude sont effectivement très liées à ces nouvelles technologies, bien qu'il soit important de reconnaître que la fraude individuelle existe depuis aussi longtemps que nous pouvons parler et posséder une propriété privée. L'évolution de la technologie n'a fait que modifier les moyens d'exécution de ce type de criminalité et lui a permis de s'industrialiser à plus grande échelle (Button & Cross, 2017 ; Leukfeldt & Stol, 2011;Crosman, 2017). Nous pouvons donc classer ces nouvelles formes de « cybercriminalité », c'est-à-dire les délits traditionnels, dont l'ampleur et la portée peuvent être accrues grâce à l'utilisation des TIC. L'hameçonnage est probablement l'exemple le plus connu de cette évolution et prend des proportions énormes (De Kimpe, Walrave, Hardyns, Pauwels, & Ponnet, 2018).

Sans classer tous les types de fraude individuelle dans la catégorie des cyberfraudes, la présente boîte à outils se concentrera sur ces formes contemporaines de fraude et sur leurs caractéristiques mixtes actuelles en ligne et hors ligne. Dans les chapitres suivants, nous nous intéresserons d'abord davantage aux tactiques de persuasion utilisées et plus particulièrement à l'ingénierie sociale, qui sous-tend la plupart de ces types de fraude (Button, McNaughton, Kerr, & Owen, 2014;Europol, 2017). Comme la présidence bulgare a décidé de se concentrer sur les escroqueries auxquelles la victime participe activement, il est impératif d'étudier la manière dont les auteurs convainquent les gens à collaborer (Button & Cross, 2017). Ensuite, un aperçu des différents types de fraudes individuelles sera fourni. Enfin, nous examinerons également les profils des victimes et des auteurs.

https://cyberessentialsdotblog.wordpress.com/2017/02/25/phishing-evolved/

2. L'art de la persuasion

Quel que soit le type d'escroquerie, il est impératif d'établir une relation avec la victime. Le délinquant doit gagner la confiance de ses victimes par la confiance, la sympathie et la persuasion pour que l'arnaque fonctionne (Crosman, 2017). Les moyens utilisés aujourd'hui peuvent différer ; la technique reste fondamentalement la même (Maggi, 2010). **L'ingénierie sociale** désigne la principale tactique permettant de gagner cette confiance et consiste à tromper une personne afin de la convaincre de divulguer involontairement des informations sensibles ou d'accomplir un acte qu'elle ne ferait pas normalement (Europol, 2017 ; Atkins & Huang, 2013;Europol, 2016). Plus précisément, nous nous concentrerons sur la tromperie basée sur l'interaction humaine : l'ingénierie sociale qui profite de l'inclination naturelle de la victime à être aimée. De plus, il existe cependant une deuxième catégorie d'ingénierie sociale qui implique la tromperie informatique, par exemple avec l'utilisation de logiciels malveillants installés dans le courrier électronique, les key loggers ou de fausses fenêtres pop-up (Atkins & Huang, 2013;Singh & Imphal, 2018).

La relation douteuse entre la victime et le délinquant revêt une importance capitale dans la fraude individuelle. Le délinquant dépend essentiellement de sa capacité à développer une relation de confiance avec sa victime pour réussir dans son intention malveillante (Atkins et Huang, 2013). En effet, le délinquant doit pousser la victime à poser des actes qu'elle n'avait pas l'intention de poser et qui peuvent même lui nuire (Yeboah-Boateng & Amanor, 2014;Ollmann, 2007). Une grande partie de la littérature relative à ce sujet peut être trouvée dans des études qui s'inscrivent dans le cadre plus large de la psychologie sociale (Rusch, 1999). Selon le corpus de travail :

> *" Les ingénieurs sociaux tentent souvent de persuader les victimes potentielles en faisant appel à des émotions fortes telles que l'excitation ou la peur, alors que d'autres utilisent des moyens pour établir des relations interpersonnelles ou créer un sentiment de confiance et d'engagement "* (Workman, 2008, p. 1).

De plus, Atkins et Huang (2013) ajoutent que « les ingénieurs sociaux s'appuient sur des biais cognitifs ou des erreurs sociales dans le processus mental pour

lancer et exécuter leurs attaques et produire des réactions émotionnelles automatiques chez leurs victimes » (Atkins et Huang, 2013, p. 24). Ces réponses émotionnelles automatiques font allusion à ce que l'on appelle la voie périphérique dans le Modèle de Vraisemblance de l'Élaboration. Ce modèle semble occuper une position plutôt hégémonique dans la littérature sur les escroqueries et les raisons pour lesquelles les gens tombent dans le piège. Il suppose essentiellement qu'il existe deux voies de persuasion. L'une est la voie centrale, qui exige beaucoup de réflexion et qui, par conséquent, nécessite une élaboration approfondie. La deuxième voie, à savoir la voie périphérique, ne nécessite pas d'être développée, car les individus se concentrent plutôt sur les déclencheurs émotionnels, comme l'attrait ou la crédibilité perçue (Petty & Cacioppo, 2012;Petty & Cacioppo, 1986;Rusch, 1999 ; Bullée, Montoya, Pieters, Junger, & Hartel, 2018;Whitty, 2013). Les escrocs poussent leurs victimes dans cette deuxième voie et suscitent traditionnellement des émotions négatives telles que l'avidité, la solitude ou la peur, et ont récemment commencé à intégrer des demandes de renseignements commerciaux banals et légitimes (p. ex., fraude du PDG) (Workman, 2008 ; Jakobsson, 2016). Afin d'orienter la victime vers cette deuxième voie, la littérature définit certains principes qui sont (mal) utilisés par les auteurs (Jakobsson, 2016). Il est cependant très important de souligner que ces principes - ces « règles empiriques » cognitives - ont, tous, leurs usages et utilités quotidiens. En l'occurrence, la clé réside dans le fait que les auteurs d'escroqueries créent un cadre dans lequel ils peuvent appliquer ces « armes de persuasion », la plupart du temps en les combinant entre-elles, à leur propre avantage. Nous allons désormais discuter des trois auteurs les plus influents identifiés par la littérature à cet égard (Ferreira, Coventry, & Lenzini, 2015).

Parmi ces trois auteurs, Cialdini et ses « six principes d'influence » sont cités le plus souvent (Rusch, 1999 ; Workman, 2008 ; Ferreira, Coventry, & Lenzini, 2015;Bullée, Montoya, Pieters, Junger, & Hartel, 2018;Cialdini, 2001).

1. Autorité :

Ce principe décrit la tendance des gens à se conformer à la demande de personnalités faisant autorité. Dans la bonne situation, les gens sont très susceptibles d'être réceptifs aux affirmations de l'autorité. Cela fonctionne également pour les symboles d'autorité, par exemple, les uniformes, les insignes et les titres ou dans les conversations téléphoniques où l'autorité peut facilement être revendiquée.

Exemple : Ce principe est très fréquent dans les escroqueries impliquant de faux policiers. Nous croyons naturellement les policiers et obtempérons à leurs ordres sur la base de leur uniforme, de leurs titres, ... Imaginez qu'un homme qui prétend être policier vous appelle et vous informe qu'il a besoin de votre code PIN le plus rapidement possible pour fermer votre compte qui a été piraté par des fraudeurs. Toutefois, la seule chose qui disparaîtra sera l'argent placé sur votre compte.

2. Rareté :

Les gens attribuent plus de valeur aux articles qui sont perçus comme étant rares. Cet article ou cette offre spécifique est considéré comme étant en rupture de stock ou n'est disponible que durant une période limitée. Par conséquent, il est perçu comme plus attrayant et désirable.

Exemple : De nombreux courriels d'hameçonnage indiquent dans leur titre que l'offre est « limitée », « il n'en reste que 50 », « unique en son genre »,....

3. Aimer et ressembler :

Les gens ont tendance à aimer les autres qui ont des intérêts, des attitudes et des croyances similaires. C'est une tendance vraiment humaine d'aimer les gens qui sont comme nous. L'identification d'une personne comme ayant des caractéristiques identiques ou similaires aux nôtres nous incite aussi fortement à adopter un raccourci mental dans nos rapports avec cette personne.

Exemple : Ce principe est très fréquent chez les influenceurs des réseaux sociaux. Une partie de leur succès résulte du fait qu'ils sont présentés comme le « garçon ou la fille d'à côté ». Bien sûr, vous souhaiteriez aussi avoir la même tenue. De même, vous voudriez aussi acheter la même chemise que celle que porte votre joueur de football préféré. Les escrocs exploitent facilement cela en se référant à des personnes connues dans leurs combines.

4. Réciprocité :

C'est une règle sociale bien connue qui nous oblige à rendre aux autres ce que nous avons reçu d'eux. Communément, on parle de « tu me rends un service, je

te revaudrai ça ». Même si la faveur que quelqu'un offre n'a pas été demandée par l'autre personne, la personne qui a reçu la faveur peut ressentir une forte obligation de respecter la règle de réciprocité en acceptant la faveur que l'offrant initial demande en retour. Même si cette faveur coûte beaucoup plus cher que l'offre initiale.

Exemple : Si quelque chose de valeur est offert, par exemple un échantillon gratuit, les gens se sentent obligés de retourner cette faveur en achetant le produit ou le service complet. Même si cet échantillon gratuit n'a pas encore été reçu ou n'existe pas du tout.

5. Engagement et cohérence :

Une autre règle sociale réside dans la cohérence dans le comportement et l'engagement à le faire. Si nous promettons quelque chose, nous tiendrons très probablement notre promesse, car, dans le cas contraire, nous donnerions l'impression d'être indigne de la confiance ou indésirables. La cohérence est activée en recherchant et en demandant des engagements initiaux plus modestes, qui peuvent être plus faciles à tenir.

Exemple : L'escroquerie classique impliquant le prince nigérian (cf. infra), également connue sous le nom d'escroquerie 419, qui demande généralement une plus petite faveur à laquelle la victime peut facilement répondre par l'affirmative. Ensuite, une demande plus importante sera formulée, qu'il sera difficile de négliger ou de refuser, car la victime ne serait pas cohérente avec son comportement antérieur...

6. Preuve sociale/conformité :

Ce dernier principe apparaît également dans de nombreuses situations sociales. Afin de décider de l'action la plus appropriée, nous nous synchronisons avec d'autres personnes (groupes de pairs, modèles de rôle,....). Cela peut même induire des actions qui vont à l'encontre de notre propre intérêt, mais qui nous permettent d'être acceptés au sein du groupe.

Exemple : Sur Facebook, on peut voir si une page ou un produit est considéré comme populaire par le nombre de personnes qui l'aiment. Les escrocs peuvent

créer une nouvelle page aussi facilement que n'importe qui, et, en utilisant de faux « likes », ce principe de preuve sociale peut être employé pour convaincre la victime de sa réalité et de sa popularité.

Les principes de Cialdini ont été établis à l'origine à partir de résultats de marketing, mais ils ont démontré toute leur importance dans la littérature relative à l'ingénierie sociale ainsi que dans les escroqueries qui utilisent ces principes de manière malveillante à leur avantage. Toutefois, certains auteurs ont proposé des principes différents, mais similaires, avec une plus grande focalisation sur les escroqueries (40). L'un d'eux est Gragg et ses « sept déclencheurs psychologiques » (40,49) :

1. Forte incidence

Ce déclencheur utilise un état émotionnel exacerbé pour permettre au fraudeur d'obtenir davantage que ce qui serait rationnellement possible dans une situation normale. Par exemple, le fait de surprendre la victime ou de la mettre en colère l'empêchera de réfléchir rationnellement.

Exemple : Promettre à la victime potentielle un prix d'une valeur de plusieurs millions suscitera très probablement de vives émotions et constituera une barrière puissante dans son évaluation logique et rationnelle de l'offre.

2. Surcharge

Si la victime doit traiter un trop grand volume d'informations en une seule fois, l'évaluation des informations en sera affectée de façon négative, ce qui induira des décisions qui n'auraient normalement pas été prises.

La surcharge peut aussi être déclenchée par un litige dans une perspective inattendue. Une nouvelle perspective prend du temps à être intégrée, mais si elle n'est pas disponible, elle pourrait entraîner une réduction de la capacité de traitement de l'information et, par conséquent, de mauvaises décisions.

Exemple : Afin de se conformer à la réglementation RGPD (Règlement général sur

la protection des données), les entreprises du monde entier ont envoyé un grand nombre de courriels pour demander à leurs clients s'ils acceptaient leur nouvelle politique de confidentialité. Il n'a cependant pas fallu longtemps aux fraudeurs pour exploiter cette surcharge et commencer à envoyer des messages similaires, mais avec d'autres intentions que la protection de la vie privée de la population.

3. Réciprocité

À l'instar du principe de Cialdini, il convient de rendre la faveur quand quelque chose est donné ou promis.

Exemple : Dans le cadre de l'escroquerie 419, les victimes se voient promettre d'importantes récompenses. Elles ont naturellement tendance à rendre la pareille en transférant l'argent.

4. Relations trompeuses

En l'occurrence, l'escroc construit une relation sur de fausses prémisses, dans le but d'exploiter l'autre personne.

Exemple : L'escroquerie de la grand-mère utilise intelligemment la relation des personnes âgées avec leurs petits-enfants. Sous de fausses prémisses, ils se fraient un chemin dans cette relation intime et confiante et l'exploitent à leur avantage.

5. Diffusion de la responsabilité et du devoir moral

Suite à ce déclenchement, la cible ne se sent que partiellement responsable des actes qu'elle va commettre. Les actions qui s'ensuivront seront moins difficiles à commettre et c'est particulièrement le cas lorsque la cible estime qu'il en va de son « devoir moral ».

Exemple : Dans le cas de la fraude du PDG, la cible peut être amenée à croire qu'elle portera la responsabilité afférente au refus de signer un gros contrat si elle n'effectue pas un paiement anticipé.

6. Autorité

De nouveau, comme tel est le cas cité par Cialdini, les gens sont, dans la société moderne, conditionnés à répondre à l'autorité, ce qui peut facilement être exploité par les fraudeurs.

Exemple : En utilisant le même exemple que ci-dessus, qui êtes-vous pour dire « non » si l'ordre semble émaner du PDG lui-même ?

Intégrité et cohérence

Ce dernier déclencheur est également similaire à « l'engagement et la cohérence » de Cialdini. Les gens ont tendance à respecter leurs engagements antérieurs, même s'ils sont potentiellement nuisibles pour eux-mêmes.

Exemple : Cela peut être utilisé pour poursuivre une escroquerie, mais cela peut également initier l'escroquerie en faisant appel à des mesures qu'une personne aurait normalement prises ou en reproduisant un scénario dans lequel la victime semble déjà s'être engagée à quelque chose.

Stajano (2011) est un autre auteur influent qui a proposé « sept principes d'escroquerie » que les fraudeurs appliquent :

1. Principe de distraction

Bien que la victime soit distraite par ce qui retient son intérêt, l'escroc peut commettre le véritable « acte » et la victime ne le remarquera probablement pas.

Exemple : Dans les escroqueries de rue, dans le cadre desquelles la cible doit suivre la balle qui est cachée sous un gobelet mélangé avec d'autres gobelets, les fraudeurs parleront souvent du prix que la victime peut gagner et leur montreront un exemple du prix. Tout en mélangeant les gobelets et en détournant l'attention de la victime.

2. Principe de conformité sociale

À l'instar de « l'autorité » de Cialdini et de Gragg, Stajano soutient que les escrocs exploitent cette « suspension de suspicion » pour vous faire obéir à leurs souhaits.

Exemple : Les fraudeurs peuvent également agir comme s'ils étaient des travailleurs légitimes et entrer dans la maison de la victime. Une fois à l'intérieur, ils peuvent facilement explorer la maison.

3. Principe du troupeau

Conformément à la « preuve sociale » de Cialdini, ce principe social permet d'inciter les victimes suspectes à baisser leur garde si elles perçoivent que tel est également le cas pour leurs pairs.

Exemple : Certains courriels d'hameçonnage prétendent qu'ils possèdent le remède contre la calvitie. Souvent, ils utiliseront une citation d'un « client » heureux pour prouver que cela fonctionne. La victime peut être moins méfiante, car d'autres personnes déclarent clairement avoir acheté le produit.

4. Principe de malhonnêteté

En imitant la « diffusion de la responsabilité et du devoir moral » de Gragg, ce principe garantit dans une certaine mesure qu'il vous sera plus difficile de trouver de l'aide. Après avoir réalisé que vous avez été victime d'une escroquerie, vous êtes impliqué dans un stratagème criminel, ce qui incitera à ne pas contacter la police. Cet objectif peut également être atteint en faisant honte à la victime.

Exemple : Dans de nombreuses escroqueries, la victime aura honte de s'être fait piégée. Cela l'incitera à ne pas signaler le délit. Les fraudeurs imaginent spécifiquement de telles escroqueries dans le but de faire honte à la victime (voir également infra).

5. Principe de la tromperie

Les escrocs savent comment manipuler et feront croire à la victime que les choses et les gens sont réels, même s'ils ne le sont pas.

Exemple : En fait, la quasi-totalité des escroqueries suivent ce principe. Les choses et les gens ne sont jamais ce qu'ils semblent être dans le cadre des escroqueries. Si cela semble trop beau pour être vrai, c'est probablement le cas.

6. Principe du besoin et de l'avidité

Également lié à la « rareté » de Cialdini, ce principe signifie que les auteurs manipuleront vos besoins et souhaits afin d'atteindre leur objectif.

Exemple : Si vous vous trouvez dans un pays avec une monnaie différente, vous devrez changer de l'argent. Ce besoin peut facilement être exploité par les escrocs pour abaisser les taux de change.

7. Principe du temps

En conférant à la victime un sentiment d'urgence et de contrainte de temps, elle accélérera très probablement le processus de prise de décision. Cela réduit la capacité de raisonnement, ce qui est à l'avantage du fraudeur car cela permet d'accroître la vulnérabilité de la cible.

Exemple : Dans de nombreuses escroqueries par courriel, la victime sera amenée à croire qu'elle doit réagir rapidement si elle ne veut pas rater cette « occasion unique ».

Ferreira, Coventry et Lenzini (2015, p. 3) ont présenté la figure suivante pour comparer ces trois groupes importants de principes utilisés et manipulés par les fraudeurs :

	C	G	S
1	Autorité	Autorité	Conformité sociale
2	Preuve sociale	Responsabilité de diffusion	Groupe
3	Liens et similarité	Relations trompeuses	Tromperie
4	Engagement et cohérence	Intégrité et cohérence	Malhonnêteté
5	Rareté	Surcharge	Durée
6	Réciprocité	Réciprocité	Besoin et cupidité
7	-	Forte incidence	Distraction

Maintenant que nous comprenons certains principes et techniques clés utilisés et manipulés par les escrocs, nous allons examiner la diversité des escroqueries qui existent.

3. Choisissez votre escroquerie

Comme nous l'avons déjà mentionné ailleurs, même si les tactiques utilisées par les escrocs peuvent être identiques, les moyens utilisés pour ce faire diffèrent de nos jours. Dans cette section, nous fournissons un aperçu non exhaustif de la variété des escroqueries qui existent aujourd'hui. Tout d'abord, quelques exemples d'escroqueries sont fournis et reposent sur leur contenu. Une classification basée sur le mode de livraison est fournie par la suite.

Bien que la recherche criminologique ne se soit intéressée que récemment à ce type de crime, *l'escroquerie 419*, plus connue sous le nom *d'escroquerie du Prince nigérian*, a attiré toute l'attention des chercheurs (Whitty, 2015 ; Whitty, 2018 ; Mba, Onaolapo, Stringhini, et Cavallaro, 2017). Même si le Nigeria ne compte aucun Prince, cette escroquerie trouve son origine au Nigeria, comme son nom l'indique. Il est donc difficile pour les forces de l'ordre d'appréhender ses auteurs (Mba, Onaolapo, Stringhini, & Cavallaro, 2017). Dans le scénario classique, la victime se voit offrir un pourcentage d'une grosse somme d'argent, mais uniquement si la victime participe au transfert d'argent hors du pays. La victime est persuadée de payer les frais supplémentaires afin de transférer l'argent. Inutile de dire que l'argent et le prince n'ont jamais existé (Murphy & Murphy, 2007).

Ce type de fraude individuelle est appelé la « fraude par paiement anticipé ». Un montant inférieur doit être payé pour bénéficier d'un montant encore plus élevé (Mba, Onaolapo, Stringhini, & Cavallaro, 2017). Les *escroqueries amoureuses* peuvent également faire partie de cette catégorie (Whitty, 2018), mais elles ne se limitent pas aux pertes financières. En effet, ce type d'escroquerie a des effets dévastateurs sur le plan émotionnel vu la relation amoureuse qui doit être nouée pour que cette escroquerie fonctionne.

> *" Les criminels prétendent nouer une relation dans l'intention d'escroquer de grosses sommes d'argent à leurs victimes. Les escrocs créent de faux profils sur des sites de rencontres et des sites de réseautage social avec des photographies volées (p. ex., des mannequins attrayants, des officiers de l'armée) et une fausse identité. Ils nouent une relation en ligne avec la victime à l'extérieur du site, " en manipulant " la victime (développement d'une relation hyperpersonnelle avec la victime), jusqu'à ce qu'ils sentent que la victime est disposée*

https://blog.eset.ie/2017/09/18/email-phishing-is-old-but-not-dead/

> *à leur transférer de l'argent. Il a été constaté que cette escroquerie engendrait un " double impact " : une perte financière et la perte d'une relation "* (Whitty, 2018, p. 105).

L'escroquerie de la grand-mère s'appuie également sur une fausse relation, quoique d'une manière différente. Comme expliqué dans des recherches antérieures du REPC (REPC, 2017), les personnes âgées sont amenées à croire qu'elles parlent réellement à un parent. Un petit-enfant absent depuis longtemps est prétendument hospitalisé et nécessiterait un transfert d'argent immédiat pour payer sa chirurgie (Jakobsson, 2016). Elles n'ont pas eu de ses nouvelles depuis longtemps et n'en auront probablement plus jamais...

Une autre escroquerie « célèbre » présentant les mêmes caractéristiques est celle du *soutien technique* (Marzuoli, Kingravi, Dewey, & Pindrop, 2016). Le plus

souvent, ce support technique est proposé par Microsoft et informe la victime par téléphone ou par courriel d'un problème informatique latent. *« Vous ne l'avez peut-être pas encore remarqué, mais votre ordinateur est infecté par un virus »*. Sous réserve d'un transfert d'un montant modique, le membre du personnel sera en mesure de résoudre votre problème à distance (Harley, Grooten, Burn, & Johnston, 2012 ; Bullée J.-W. Montoya, Junger et Hartel, 2016). Comme beaucoup sont informés de cette escroquerie, les auteurs ont récemment créé de fausses pages Internet plus sophistiquées de support qui incitent la victime à appeler le centre de support, qui est très probablement un numéro à tarif majoré (Rauti & Leppänen, 2017).

Sur les 13 États membres qui ont répondu à notre questionnaire, les escroqueries téléphoniques suivantes ont été rapportées comme les plus fréquentes : escroquerie de la grand-mère, usurpation d'identité de policiers, arnaque à la loterie, escroquerie commerciale légale, escroquerie aux accidents (de parents).

D'autres exemples sont les *arnaques aux loteries, aux jeux de hasard, aux opportunités commerciales, aux chaînes de lettres, au télémarketing, etc.* (Button, Lewis, & Tapley, 2014;Button & Cross, 2017 ; Button, Lewis, & Tapley, 2009;Jakobsson, 2016 ; Stajano & Wilson, 2011). Button (2017) nous fournit une classification basée sur huit catégories des fraudes les plus courantes.

1. Fraude aux investissements de consommateurs

En l'occurrence, des actions ou des parts sont vendues à des victimes et sont présentées comme étant très rentables. En réalité, elles sont sans valeur ou inexistantes.

2. Fraude liée aux produits et services de consommation

Cette fraude implique la vente de produits et services inexistants ou la vente de produits et services qui sont sensiblement différents à la livraison.

3. Fraude à l'emploi

La victime se voit proposer un faux service ou un service inadéquat pour obtenir un emploi ou une formation qui est présenté comme menant à un emploi.

4. Fraude en matière de prix et de bourses

Soit la victime est amenée à croire qu'elle participe à une véritable loterie et à payer ses frais de participation, soit elle est informée qu'elle a déjà gagné et qu'elle doit d'abord payer des frais pour pouvoir recevoir ce prix.

5. Fraude au recouvrement imaginaire de créances

En usurpant souvent l'identité d'acteurs ou d'organisations dignes de confiance, la victime se fait piéger ou est contrainte à payer des dettes qu'elle n'a pas contractées.

6. Fraude liée aux organismes de bienfaisance

En l'occurrence, le fraudeur agit comme un organisme de bienfaisance légitime afin d'obtenir des dons de particuliers.

7. Fraude aux relations et abus de confiance

L'escroquerie amoureuse, de la grand-mère, à l'accident,... est un exemple classique de fraudes qui abuse de l'intimité d'une relation personnelle.

8. Fraude à l'identité

Il s'agit de l'utilisation des renseignements personnels d'une victime pour commettre d'autres fraudes ou activités criminelles. Nous n'incluons pas ce type de fraude dans cette boîte à outils, car il ne nécessite pas une participation active de la victime dans la transaction.

La liste est aussi impressionnante que la créativité des fraudeurs et ils peuvent atteindre tous les segments de la population. Toutefois, les escrocs peuvent également privilégier une approche plus ciblée. Tel est le cas des *escroqueries aux compromis commerciaux par courriel (CCC)* (Jakobsson, 2016). Dans ce cas, la victime est sélectionnée parce qu'elle travaille pour une entreprise spécifique ou qu'elle y joue un rôle spécifique. Le plus souvent, l'auteur intervient, après quelques recherches, en qualité de patron de la victime (fraude du PDG) ou d'un autre tiers de confiance (fraude au mandat), et réclame un paiement apparemment normal (Europol, 2017). Par exemple, votre patron vous envoie un courriel pour effectuer un transfert vers l'entreprise X. Ce transfert est urgent ; raison pour laquelle il utilise son adresse électronique « personnelle », et vous êtes la seule personne qu'il peut contacter pour ce faire. Ni l'entreprise, ni l'adresse électronique n'est correcte, mais vous obtempérez (Jakobsson, 2016). Selon la dernière *Évaluation de la menace du crime organisé sur Internet* (Europol, 2018), 65 % de tous les États membres ont signalé des cas de fraude du PDG et plus de la moitié rapportent une augmentation des montants.

Une autre manière de classer ces escroqueries consiste à les distinguer selon la façon dont elles sont présentées à la victime. En toute logique, il peut s'agir d'une interaction en face à face, dans la vie réelle, ou la victime peut être contactée à distance, à l'aide de moyens de communication tels que le courrier électronique ou le téléphone. Il est toutefois impératif de ne pas se laisser aveugler en se concentrant sur un seul mode de prestation pour qu'une escroquerie fonctionne.

https://www.europol.europa.eu/socta/2017/fraud.html

Les auteurs peuvent facilement basculer entre le courrier électronique, le téléphone, le site Internet,... Cela leur permet d'adapter au mieux leur attaque (Button & Cross, 2017).

Les exemples classiques de **l'escroquerie en personne** impliquent l'intervention de faux agents de police afin d'escroquer la victime pour qu'elle paie une prétendue amende ou communique des informations sensibles. Il en va de même pour les escrocs se présentant comme des bricoleurs et qui proposent de vous soulager de certaines tâches ménagères à la maison. Afin de faciliter la vie de la victime, ils lui proposent d'intervenir quand elle est au travail ou en vacances... D'autres exemples courants sont les faux rouleaux d'argent ou les pièges typiques tels que « suivre la balle » ou la vente de faux gadgets (Stajano & Wilson, 2011).

Faux rouleau d'argent : par exemple, échanger des devises étrangères avec de la fausse monnaie.

" Suivre la balle " : le jeu classique où une balle est cachée sous une tasse qui est ensuite mélangée avec deux autres tasses, la victime doit deviner où se trouve la balle, ce qui est impossible car la balle n'est sous aucune d'elles.

Dans la plupart des cas d'ingénierie sociale, toutefois, les escrocs évitent tout contact physique, car cela leur garantit une plus grande protection. De plus, le courrier électronique ou le téléphone est le vecteur idéal pour orienter les victimes vers la voie périphérique (Workman, 2008). Comme Anderson (2016) le décrit d'un point de vue américain :

> *" Pas plus tard que dans les années 1980, le problème des fraudes et des escroqueries était en grande partie un problème local ou organisé par courrier. Les agresseurs localisaient leurs victimes en faisant du porte-à-porte, les mécaniciens proposaient de fausses réparations à l'atelier local de réparation automobile, et les colporteurs vendaient leurs marchandises bidon à la foire du comté ou envoyaient leurs fausses promesses par la poste. Aujourd'hui, les*

> *fraudeurs organisent des fraudes sur le marché de masse au niveau national, voire international, où ils contactent des victimes potentielles par télémarketing, publireportages lors d'émissions télévisées tardives ou sur l'Internet. Les fraudeurs situés en Inde informent les consommateurs qui ont fait appel à l'assistance technique sur l'Internet que 133 problèmes ont été répertoriés dans leur ordinateur qu'ils peuvent les résoudre à distance sous réserve du paiement de leurs frais. Plutôt que de se limiter à faire du porte-à-porte ou à recourir aux services postaux américains, les fraudeurs proposant une foule de faux produits peuvent diffuser des publireportages durant des émissions télévisées tardives, faire de la publicité pour leurs produits sur l'Internet ou faire des appels de télémarketing générés par ordinateur à des millions de consommateurs en quelques minutes.* (Anderson, 2016, p. 4)

La révolution des technologies de communication a permis aux fraudeurs d'industrialiser les anciennes fraudes à faible coût et de créer de nouveaux types d'escroqueries (Button & Cross, 2017 ; Button, McNaughton, Kerr, & Owen, 2014). C'est ce qui est aujourd'hui connu sous le nom de *crime cybernétique*, à savoir un délit traditionnel qui s'est amélioré avec l'utilisation des TIC (Whitty, 2018 ; Button & Cross, 2017). L'environnement numérique a créé un climat d'anonymat que les auteurs d'escroqueries ont utilisé avec plaisir (Agustina, 2015). Outre cet anonymat (perçu) et ces faibles coûts, le nombre d'objectifs réalisables s'est multiplié à tel point que le monde entier est concerné (Leukfeldt & Stol, 2011). Pis encore, cette mondialisation de la fraude interdit aux services de répression d'identifier et/ou d'appréhender les coupables. Certains sont même devenus des « escrocs professionnels » en prenant conscience de tout le potentiel des changements technologiques (Button & Cross, 2017).

« L'escroquerie industrielle » la plus courante est l'hameçonnage (Europol, 2017 ; Europol, 2016). Les objectifs poursuivis sont identiques à ceux des escroqueries réelles, mais il est fort probable que l'escroc agisse en se présentant comme une entité de confiance ou légitime puisque la victime est trompée pour divulguer des renseignements personnels et/ou financiers (Singh& Imphal, 2018; De Kimpe, Walrave, Hardyns, Pauwels, & Ponnet, 2018;Moreno-Fernández, Blanco, Garaizar, & Matute, 2017). Cette méthode est la plus simple pour atteindre un grand

nombre de victimes potentielles. On rapporte que, dans 95% des cas, les escrocs communiquent avec leurs victimes par courriel. 40 % des États membres ont mis l'accent sur les enquêtes relatives à l'hameçonnage, un phénomène qui ne cesse d'augmenter d'année en année. De 2015 à 2016, le nombre d'attaques d'hameçonnage a connu une augmentation notable de 65 % (Europol, 2017). Nous devons être prudents avec ces chiffres en raison des problèmes de signalement (cf. infra), mais ces chiffres sont néanmoins alarmants.

L'hameçonnage est un phénomène très courant. Plus de 30 % de la population adulte a au moins reçu un courriel d'hameçonnage. Au sein de la population estudiantine, ce nombre est même supérieur à 50 %. De plus, 1 cible sur 14 ouvre effectivement un lien ou une annexe engendrant une victimisation possible (De Kimpe, Walrave, Hardyns, Pauwels, & Ponnet, 2018)

Tout en impliquant un faible risque pour l'agresseur, les pertes pour la victime peuvent être considérables : pertes financières, atteinte à la réputation, vol d'identité,... (Ollmann, 2007)..

Il s'agit ici d'hameçonnage trompeur, impliquant le recours à des tactiques d'ingénierie sociale. Pour être complet, il existe également une forme d'hameçonnage basée sur des logiciels malveillants ou sur la tromperie informatique, utilisant des enregistreurs de clés, le piratage, les chevaux de Troie,... pour atteindre les objectifs des auteurs, comme cela a déjà été mentionné ci-dessus et dans des publications antérieures (REPC, 2017).

Jusqu'à tout récemment, les escroqueries par courriel étaient assez facilement détectables. Elles se caractérisaient par une grammaire déficiente et des fautes d'orthographe et relataient des histoires plutôt étranges. Les escrocs ont réalisé que, en ciblant intelligemment leurs victimes, ils peuvent obtenir un meilleur « retour sur investissement ». Cibler l'attaque multiplie par vingt les probabilités que le courriel soit lu (Jakobsson, 2016). Cette évolution a ouvert la voie à une nouvelle et plus grande variété de formes d'hameçonnage et à des modes opératoires plus professionnels et crédibles (Europol, 2017 ; Jakobsson, 2016 ; Ollmann, 2007). L'hameçonnage est de plus en plus ciblé. Alors que, par le passé, les fraudeurs envoyaient un nombre aussi élevé que possible de courriels, les fraudeurs exécutent désormais leurs recherches et exploitent ces connaissances pour

https://www.pinterest.co.uk/pin/760897299514084725/

paraître plus naturels et plausibles ; la fraude du PDG en est le parfait exemple (Jakobsson, 2016). Le harponnage est un autre terme qui désigne le ciblage d'un groupe spécifique. L'hameçonnage à la baleine, d'autre part, cible les *personnes* de haut niveau (Singh & Imphal, 2018). D'autres variantes existent également, telles que le pharming ; dans ce cadre un faux site Internet est hébergé dans le but de tromper la victime (Europol, 2014) ou le smishing, qui est une forme de hameçonnage utilisant des SMS ou des messages textes en ligne (Europol, 2018).

L'hameçonnage devenant de plus en plus sophistiqué, la dernière étape surprenante est le regain d'intérêt pour une technologie plus ancienne : le téléphone (Maggi, 2010). Ces escroqueries téléphoniques sont de plus en plus connues sous le nom de « vishing », car elles exploitent également le potentiel de l'Internet (Europol, 2017). Abréviation du hameçonnage vocal (voice phishing), le « vishing » utilise le canal téléphonique pour tromper ses victimes (Maggi, 2010). Toutefois, le canal téléphonique a également connu quelques évolutions. Le Voice Over Internet Protocol (VOIP) a permis de passer un appel téléphonique par l'Internet (Singh & Imphal, 2018). Cela propose certains avantages. L'utilisation de ce protocole réduit considérablement le coût des appels, il est plus difficile de retracer les auteurs et ces derniers peuvent usurper les informations de

leur correspondant (Ollmann, 2007). L'usurpation désigne la falsification des informations transmises par l'appelant. Non seulement cela, mais les escrocs peuvent également composer automatiquement le numéro de leurs victimes par ordinateur. Cela nécessite un appareil de composition automatique et informatisé qui transmet un message préenregistré (Marzuoli, Kingravi, Dewey, & Pindrop, 2016). De nos jours, les gens sont habitués à donner des informations à des étrangers, voire même à des machines, car les centres d'appels sont très présents dans la société moderne (Maggi, 2010). Les escrocs utilisent facilement cette évolution.

Les escroqueries téléphoniques offrent un taux d'impact beaucoup plus élevé et le rendement est également plus élevé que le hameçonnage normal (Yeboah-Boateng & Amanor, 2014). Ce succès est dû au fait que le « vishing » combine le meilleur des deux mondes, la relation « interpersonnelle » et les technologies de communication. Le pouvoir du téléphone par l'Internet réside dans le fait qu'il offre à l'escroc la possibilité de créer une personne crédible beaucoup plus rapidement. De plus, la personne à l'autre bout de la ligne peut toujours être celle qu'il souhaite et jouir de l'anonymat. De cette façon, il combine aussi ce cadre intime avec l'impossibilité de repérer l'escroquerie dans la vie réelle par des indices visuels. En effet, il peut adapter son attaque jusqu'aux limites en ayant une conversation en temps réel et contrôler le moment de la délivrance du message (Ollmann, 2007). Les groupes criminels organisés ont même commencé à engager des locuteurs natifs pour qu'ils soient aussi crédibles et professionnels que possible (Europol, 2016).

Combiné à ces avantages, les gens font traditionnellement davantage confiance au canal téléphonique qu'à l'Internet. Selon le dernier Eurobaromètre sur les technologies de communication dans l'UE (Commission européenne, 2018), 60 % des personnes interrogées estiment que le téléphone est plus fiable et leur offre plus de protection que l'Internet. De plus, l'accès au téléphone est presque universel, vu que 97 % en possèdent un à la maison, contre 70 % qui ont un accès à l'Internet à la maison. De plus, téléphoner à quelqu'un demeure également le moyen de communication le plus utilisé, sachant que 92% des répondants reçoivent ou passent fréquemment des appels téléphoniques, contre 72% qui envoient des e-mails (Commission européenne, 2018). Cette confiance inébranlable peut naturellement être facilement exploitée par les escrocs et, en outre, alors que les pourriels ont permis l'avènement d'une industrie anti-spam de plusieurs milliards, les escroqueries et fraudes téléphoniques ne sont pas couvertes par cette protection (Gadhave & Sirsat, 2015).

4. Calculer les chiffres

En général, les chiffres afférents à ce sujet sont peu connus (Button, McNaughton, Kerr, & Owen, 2014). La principale difficulté pour se faire une idée précise de ces types de crimes réside dans le fait qu'une grande partie n'est pas signalée (van de Weijer, Leukfeldt, & Bernasco, 2018 ; Crosman, 2017). Même les données dont nous disposons nous donnent une image faussée, car elles sont probablement une sous-estimation du problème en raison de ce manque de rapports (Bidgoli & Grossklags, 2017). Les raisons de ce problème sont cependant bien connues. L'une d'elles réside dans le fait que, souvent, les victimes ne savent même pas qu'elles ont été contactées par un fraudeur (Bidgoli et Grossklags, 2017 ; Button et Cross, 2017). Dans une enquête menée par Button, Tapley et Lewis (2012) auprès de 745 victimes, 40 % des répondants ne savaient pas qu'ils étaient des victimes avant d'en avoir été avisés par un tiers. Une autre raison expliquant l'absence de signalement réside dans la gravité du crime perçue par la victime. Si le hameçonnage de masse, par exemple, engendre à un montant total important, les cas individuels se limitent à des pertes plutôt faibles. Les victimes croient souvent que le dépôt d'une plainte ne vaut pas la peine et que, en outre, il est peu probable que les escrocs soient appréhendés un jour (Bidgoli et Grossklags, 2017 ; Button et Cross, 2017). De plus, le signalement à la police ne va pas de soi. Les intervenants auxquels la fraude peut être signalée sont nombreux et la police ne la considère pas nécessairement comme une priorité (Button & Cross, 2017). Selon l'Eurobaromètre Cybersécurité (Commission européenne, 2017), seule la moitié des répondants contacteraient la police si elles étaient confrontées à un courriel ou un appel téléphonique frauduleux. 18 pour cent d'entre eux ne le signaleraient pas du tout, 4 pour cent ne savent même pas à qui s'adresser. Cela a également été confirmé par d'autres recherches (Button et Cross, 2017 ; Bidgoli et Grossklags, 2017 ; Button, McNaughton, Kerr et Owen, 2014).

Les effets secondaires positifs les plus importants pour l'escroc qui recourt à l'ingénierie sociale pour contraindre sa victime à se conformer à ses demandes sont les sentiments de culpabilité et d'embarras qu'elle éprouve par la suite. Inversement, il s'agit d'une autre raison pour laquelle les taux de signalement sont aussi faibles (Cross, Richards, & Smith, 2016;Titus et Gover, 2001). Par exemple, dans le cas d'une fraude du PDG, les victimes craignent de porter atteinte à leur réputation au sein de l'entreprise, voire même de perdre leur emploi (Europol, 2016). Les victimes se blâment souvent parce qu'elles ont participé activement à l'accomplissement du délit et sont gênées de s'être fait piéger (Bidgoli et Grossklags, 2017 ; Button, McNaughton, Kerr et Owen, 2014). Se

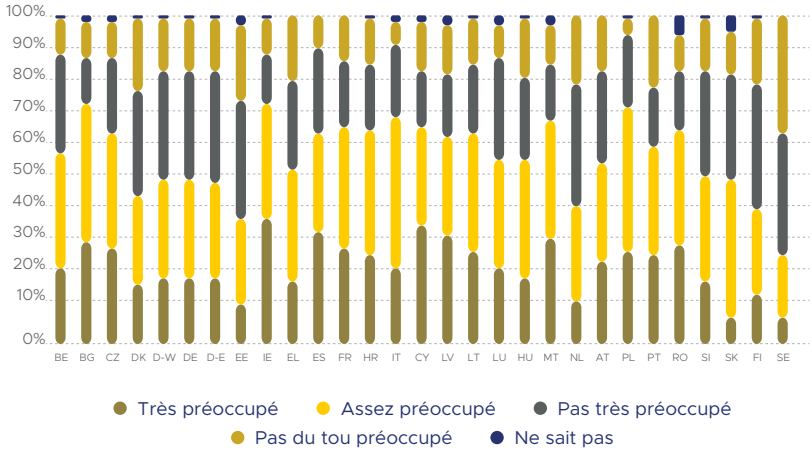
considérant comme indispensables à l'accomplissement au délit et honteuses de leurs actes, elles craignent que la police ne les croira pas ou ne les prendra pas au sérieux (Button, Tapley, & Lewis, 2012). Ainsi, cette implication active de la victime dans le crime occulte non seulement notre vision du problème, mais elle peut également conduire à une victimisation secondaire (Button & Cross, 2017). Certaines escroqueries, telles que l'escroquerie 419, sont dotées d'un mécanisme « anti-déclaration » intégré, car la victime commet également des actes illégaux en transférant de l'argent illégal dans certains cas (Button, Lewis et Tapley, 2009) (voir supra) et les fraudeurs créent spécifiquement des stratagèmes embarrassants pour éviter de signaler les cas (Button, McNaughton, Kerr et Owen, 2014).

Si les escroqueries sont signalées aux organes officiels, il est plus probable qu'elles soient classées sous le libellé plus large de la « fraude », ce qui complique l'isolement de la fraude individuelle (Button & Cross, 2017). Dans un questionnaire qui a été envoyé aux États membres dans le cadre des travaux préparatoires de cette boîte à outils, nous avons trouvé des observations similaires. Dans onze des treize États membres qui ont répondu, les escroqueries téléphoniques sont signalées sous la rubrique « fraude ».

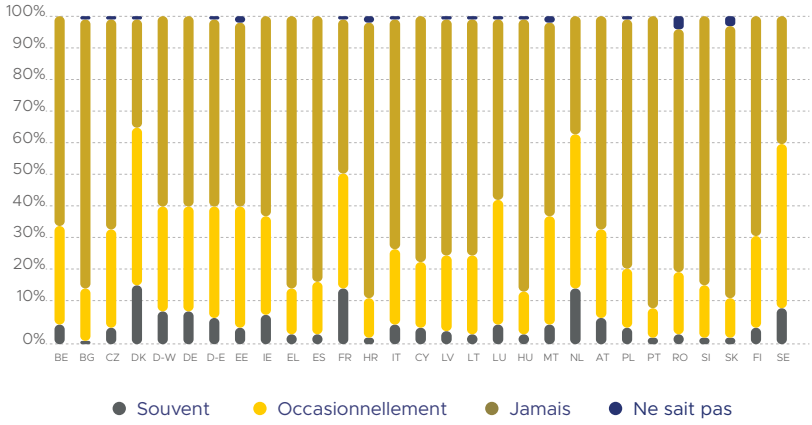
L'utilisation d'enquêtes de victimisation est une solution à ce problème de chiffres gris dans les statistiques officielles. Toutefois, les mêmes problèmes sont à nouveau soulevés par les chercheurs. Bon nombre de ces études ne font pas de distinction entre les fraudes commises en ligne ou par des méthodes « à l'ancienne », ou ne couvrent pas du tout les questions de fraude individuelle. Et, une fois encore, des réticences doivent encore être rapportées dans ce cadre, des victimes ne savent pas qu'elles sont victimes ou pensent que leur cas particulier ne mérite pas d'être signalé (Button & Cross, 2017 ; Button, McNaughton, Kerr, & Owen, 2014). En dépit de ces questions critiques, l'Eurobaromètre spécial sur la cybersécurité (Commission européenne, 2017) a interrogé près de 30 000 citoyens de l'UE à domicile et les a plus spécifiquement questionnés sur les courriers électroniques ou les appels téléphoniques frauduleux. Levi (2017) décrit cette enquête comme « la seule collecte de données comparatives transnationales sur la victimisation par la fraude dans l'UE » (Levi, 2017, p. 4).

Dans tous les États membres, à l'exception de cinq, au moins la moitié des personnes interrogées dans le cadre de l'Eurobaromètre ont exprimé une certaine inquiétude quant au fait d'être les victimes de courriels ou d'appels téléphoniques frauduleux, l'Irlande et la Bulgarie affichant les chiffres les plus élevés (73%). Le Danemark (45%), les Pays-Bas (42%), la Finlande (41%), l'Estonie (38%) et la

Dans quelle mesure êtes-vous personnellement préoccupé(e) ou craignez-vous d'être victime dans les situations suivantes : recevoir des courriels ou des appels téléphoniques frauduleux vous demandant de communiquer vos données personnelles (y compris l'acc



Combien de fois avez-vous été confronté(e) aux situations suivantes ou en avez-vous été victime : recevoir des courriels ou des appels téléphoniques frauduleux vous demandant de communiquer vos données personnelles (y compris l'accès à votre ordinateur, v



Suède (27%) font exception à ces constats généraux. Il est toutefois intéressant de noter que trois de ces pays figurent parmi les pays où le nombre de victimes « auto-déclarées » est le plus élevé. Au Danemark (66%), aux Pays-Bas (64%) et en Suède (61%), plus de la moitié des personnes interrogées ont reçu des courriels ou des appels téléphoniques frauduleux. La Slovaquie (14%), la Croatie (14%) et le Portugal (11%) affichent les pourcentages les plus faibles.

Outre ce chiffre important méconnu, il convient également de souligner la rareté des recherches sur la victimologie de ce crime (Whitty, 2018 ; Button, Lewis et Tapley, 2014). La plupart des études sur les profils de victimes se concentrent également sur les fraudes en ligne, de telle sorte que les déclarations suivantes sont principalement basées sur ces constatations. Comme nous l'avons toutefois montré dans la section sur les différents types d'escroqueries, il existe une grande variété de fraudes, qui confèrent à la quasi-totalité des membres de la société la qualité de victime potentielle. Il est donc difficile de formuler des constatations générales sur une typologie de victimes. Néanmoins, des études ont montré que certains groupes sont particulièrement vulnérables à des escroqueries spécifiques. Les escroqueries à l'investissement des consommateurs sont par exemple plus répandues parmi les personnes âgées et la population active, car elles ont les moyens d'investir (Button & Cross, 2017).

L'apport le plus important des études de victimologie sur ce sujet réside peut-être dans la possibilité de briser le mythe qui existe en matière de prévalence parmi les différents groupes d'âge. Il existe une perception commune, surtout dans les médias, selon laquelle les personnes âgées sont le plus souvent les victimes de ce crime (Button, Lewis, & Tapley, 2009). Contrairement à cette croyance populaire, toutefois, les enquêtes ont montré que les jeunes adultes constituent le groupe de victimes le plus fréquent (Button, Lewis, & Tapley, 2009;Ross, Grossmann, & Schryer, 2014). Cette idée populaire résulte du stéréotype selon lequel les personnes âgées manquent de compétences financières, sont plus confiantes, ont des fonctions cognitives plus lentes, ... Ces constatations sont naturellement avérées dans une certaine mesure, mais il est important de comprendre *pourquoi* les personnes âgées sont ciblées en premier lieu. Si nous nous concentrons sur l'attractivité de la cible, les personnes âgées ont facilement accès à l'épargne de toute une vie, sont plus susceptibles d'avoir des biens privés, un plus grand nombre de lignes de crédit supplémentaires (Barnes, 2017). C'est, selon Button et Cross (2017), la principale raison pour laquelle elles sont davantage ciblées. La population plus jeune et le groupe d'âge moyen sont toutefois plus vulnérables à ces escroqueries (Button et Cross, 2017 ; De Kimpe, Walrave, Hardyns, Pauwels,

& Ponnet, 2018;Whitty, 2018). La plupart des études concluent en effet que les consommateurs âgés courent moins de risques d'être victimes de fraude individuelle. D'autre part, la fraude est, au sein de la population âgée, le délit auquel elle est le plus susceptible d'être confrontée (Button et Cross, 2017). Toutefois, il s'agit là d'un sujet ambivalent qui mérite un examen plus approfondi, car certains types de fraude, tels que la fraude à l'investissement ou les fraudes à la loterie, montrent une prévalence plus élevée chez les personnes âgées (Anderson, 2016).

En élaborant sur ce sujet, les jeunes (15-25 ans) en particulier sont identifiés comme vulnérables (De Kimpe, Walrave, Hardyns, Pauwels, & Ponnet, 2018;Sheng, Holbrook, Kumaragur, Cranor, & Downs, 2010). Cela pourrait indiquer un niveau d'éducation inférieur, ayant passé moins de temps en ligne, une exposition inférieure au matériel de formation et une aversion réduite pour le risque (Sheng, Holbrook, Kumaragur, Cranor, & Downs, 2010). Ce dernier point est également mis en avant par Button, Lewis et Tapley (2009), car les personnes ayant une attitude plus positive à l'égard de la prise de risques financiers et les personnes avec un faible contrôle de soi, sont considérées comme plus vulnérables. Les recherches de De Kimpe, Walrave, Hardyns, Pauwels et Ponnet (2018) affirment qu'un niveau élevé de confiance ou de « conformité » engendre une plus grande vulnérabilité, ce qui est un indicateur positif de réponse aux courriels de hameçonnage. Un sens élevé du devoir est également considéré comme étant positivement lié à la victimisation. Toutefois, les études universitaires se déchirent sur la question de savoir si une plus grande expérience de l'Internet et des connaissances technologiques induisent ou non une vulnérabilité réduite à l'hameçonnage ou exactement l'inverse, parce qu'être techniquement compétent implique également un niveau plus élevé d'exposition aux menaces (De Kimpe, Walrave, Hardyns, Pauwels, & Ponnet, 2018). De plus, Button (2017) affirme que des études ont démontré que, même si les victimes de fraude sont généralement présentées comme des personnes sans instruction et analphabètes sur le plan financier, l'inverse semble être vrai. Il propose trois explications possibles de ce phénomène. Le premier est le « fossé entre le savoir et le faire », en vertu duquel, selon eux, les gens reconnaissent souvent les signes d'une escroquerie, mais n'appliquent pas ces connaissances à leur situation. Une deuxième explication est appelée le « piège de l'expert », qui fait référence au piège dans lequel tombent les gens qui ont des compétences financières, car ils sont trop confiants et ignorent les dangers. Une dernière explication pourrait résider dans le fait que les victimes pourraient avoir des connaissances financières suffisantes, qu'elles ne disposent pas de ce niveau de connaissances en matière de tactiques de persuasion et d'ingénierie sociale (Button et Cross, 2017).

En examinant la façon dont les victimes individuelles sont effectivement contactées, la littérature a également identifié quelques techniques de sélection utilisées par les fraudeurs. Par exemple, dans le cadre de certaines escroqueries téléphoniques, certains fraudeurs composent aléatoirement des numéros à partir d'annuaires téléphoniques ou de registres de sociétés publiques. D'autres, en revanche, utilisent ce qu'on appelle des « listes de dupes ». Ces listes sont des registres qui sont partagés et vendus entre les fraudeurs dont les cibles ont déjà été abusées (Wood, Liu, Hanoch, Xi, & Klapatch, 2018). Levi (2008) les décrit comme suit :

> *" Une fois qu'une personne s'est abonnée à une loterie ou à un autre produit par l'Internet, par la poste ou par téléphone, elle reçoit rapidement des " offres " frauduleuses connexes d'autres fraudeurs "* (Levi, 2008, p. 404).

L'utilisation de telles listes indique également un niveau élevé de victimisation répétée (Button, Lewis, & Tapley, 2009). De même, un nombre relativement restreint d'escrocs semblent être à l'origine de la majorité des escroqueries téléphoniques. Dans une étude réalisée par Marzuoli, Kingravi, Dewey et Pindrop (2016), un système de pot a été utilisé pour analyser l'écosystème de la fraude. Sur les 8 000 000 d'appels reçus, les chercheurs en ont analysé 40 000. Seul 1,8 % des sources d'appel était à l'origine de 66 % des plaintes. Ces résultats vont dans le sens de ce que l'on a appelé les « escrocs professionnels », en faisant référence à l'esprit d'entreprise de certains fraudeurs qui diversifient leur offre d'escroqueries et tentent de maximiser leur efficacité (Button, Lewis, & Tapley, 2009;Button, McNaughton, Kerr et Owen, 2014).

Néanmoins, tous les fraudeurs n'affichent pas un degré de professionnalisme et d'organisation identique. Dans le domaine de l'escroquerie téléphonique, certains fraudeurs opèrent sur une base ad hoc et changent de modus operandi dès que les services de répression semblent les débusquer. D'autres réseaux sont plus grands et prennent des proportions plus « formelles », avec une certaine forme de hiérarchie, de division du travail et de rémunération progressive. Ces types de fraudeurs peuvent également être impliqués dans le crime organisé traditionnel (le domaine de la drogue, par exemple) ou se concentrer uniquement sur les escroqueries (Levi, 2008 ; Barnes, 2017 ; Button, Lewis, & Tapley, 2009).

En ce qui concerne l'origine des escrocs, les Nigérians sont presque par définition impliqués dans l'escroquerie du Prince nigérian, mais, en général, les escrocs des pays d'Afrique de l'Ouest sont actifs dans tous les types d'arnaques (Button, Lewis, & Tapley, 2009;Levi, 2008 ; Button & Cross, 2017). Dans le cadre de la fraude par Internet, les groupes criminels d'Europe de l'Est (Russie, Roumanie, Lituanie,...) ont développé une compétence et une réputation particulières (Button, Lewis, & Tapley, 2009;Levi, 2008). Les fraudes transfrontalières sont particulièrement répandues, ce qui complique la tâche des services de répression et de la police nationale quand elles souhaitent s'attaquer à ces problèmes (Button & Cross, 2017). Raison de plus pour d'abord empêcher la commission de ce délit.

5. Conclusions

Dans la première partie de cette boîte à outils, nous avons résumé **l'image** actuelle de la fraude individuelle dans le cadre des renseignements. Étant donné que la fraude est une infraction très diversifiée, englobant un large éventail d'activités, nous ciblé la fraude individuelle, tout en mettant l'accent sur les caractéristiques mixtes actuelles, en ligne et hors ligne, de ce type de crime.

La plupart des fraudes individuelles reposent sur une technique appelée ingénierie sociale. Cette technique désigne la principale tactique ayant pour objet de gagner la confiance des victimes et les convaincre de participer à l'escroquerie. En tant que telle, la victime joue un rôle très actif dans l'accomplissement du délit, ce qui induit un sentiment de honte et de culpabilité. Nous avons situé **l'ingénierie sociale** dans le cadre d'études en psychologie sociale et démontré certains principes de base dans l'art de la persuasion.

Toutefois, il existe de nombreuses **formes et de nombreux types** différents d'escroqueries. Nous avons classé ces types selon leur contenu ou selon leur mode de prestation (en personne ou à l'aide des TIC). Outre cette grande variété, ils semblent de plus en plus sophistiqués et complexes. De plus, il est fort probable que nous ne faisons qu'effleurer la surface, car les chiffres réels relatifs à ce délit sont **inconnus**. Les victimes ne signalent pas ce crime pour diverses raisons : sentiment de honte, perception de la gravité de leurs pertes, ignorance qu'elles ont été victimes, ignorance des organes à contacter pour le signalement,...

Les enquêtes sur la victimisation, telles que l'Eurobaromètre, offrent toutefois une solution à ce manque de rapports aux organismes officiels. Néanmoins, des recherches plus approfondies sur la gravité de ce crime et le profil des victimes demeurent cruciales. De cette façon, les activités de prévention peuvent être plus ciblées et plus efficaces. Nous allons maintenant passer en revue les bonnes pratiques actuelles dans ce domaine.

02 PARTIE II: BONNES PRATIQUES

1. Introduction

Dans la deuxième partie de cette boîte à outils, nous examinerons en profondeur les méthodes permettant de prévenir les fraudes individuelles. Comme nous l'avons expliqué dans la partie précédente, il est extrêmement difficile pour la police de s'attaquer à ce problème. Button (2017) affirme que la police ne dispose pas des moyens nécessaires pour enquêter sur la majorité de ces fraudes, ce qui rend la prévention d'autant plus importante (Europol, 2016). Outre ce danger, la prévention de la fraude a généralement peu intéressé le monde académique. Il est donc plus difficile de se prononcer sur l'efficacité, même si de nombreuses activités existent dans ce domaine (Button et Cross, 2017). Dans cette partie de la boîte à outils, nous ferons le point sur certaines connaissances théoriques relatives à la prévention de la fraude individuelle, mais exposerons également quelques bonnes pratiques. Enfin, nous formulerons quelques recommandations, en mettant l'accent sur la prévention des escroqueries téléphoniques.

La tactique de prévention la plus courante permettant de prévenir la fraude individuelle consiste à éduquer le public. Les mesures techniques, telles que les filtres anti-spam, les logiciels de vérification orthographique, la surveillance des domaines de sites Internet usurpés,... ont tous leurs propres avantages. Toutefois, ils demeurent réactifs, car ils ont finalement été conçus comme une réponse à certaines méthodes (Jakobsson, 2016 ; Moreno-Fernández, Blanco, Garaizar, & Matute, 2017). Les escrocs peuvent s'adapter à ces mesures, ce qui est illustré par leur niveau de sophistication sans cesse croissant. De plus, ces mesures techniques et procédurales ne sont pas sûres à 100 %, car ces systèmes et ces personnes présenteront toujours des failles. Néanmoins, chaque mesure de sécurité nous amène à une référence plus sûre et est importante pour lutter contre ce crime complexe.

L'élimination de cette « fuite de sécurité » est la raison la plus probable pour laquelle beaucoup d'efforts de prévention sont déployés pour éduquer le public et le sensibiliser (Workman, 2008). Comme nous l'avons déjà mentionné, une grande partie de ces efforts n'a pas encore été évaluée (Mears, Reisig, Scaggs, & Holtfreter, 2016), mais quelques conclusions générales peuvent être tirées. Les formations en ligne, l'apprentissage contextuel1, la formation intégrée2 et les jeux interactifs 3se sont tous avérés efficaces pour améliorer la sécurité des utilisateurs (Sheng, Holbrook, Kumaragur, Cranor, & Downs, 2010). Les personnes sont, par exemple, formées à la reconnaissance de certaines caractéristiques linguistiques (Tabron, 2016) ou aux tactiques de discrimination viscérale (Moreno-Fernández,

Blanco, Garaizar, & Matute, 2017). Ces formations sont essentielles pour combler le fossé entre « savoir et faire » susmentionné. La sensibilisation induit une meilleure compréhension du phénomène, mais pas nécessairement une application accrue de ces connaissances à sa situation particulière (Moreno-Fernández, Blanco, Garaizar, & Matute, 2017). Une combinaison de la sensibilisation et de la formation semble présenter le plus d'avantages (Cross, Richards, & Smith, 2016;Europol, 2016 ; Bullée J.-W. Montoya, Junger et Hartel, 2016). Une étude réalisée par Sheng, Holbrook, Kumaragur, Cranor et Downs (2010) a mélangé ces formations et a montré une amélioration de 40% après l'introduction du matériel de formation par rapport à un groupe témoin (formation en ligne, contextuelle et intégrée et jeux interactifs combinés).

Ce type de crime se caractérise par la participation active de la victime et par un niveau élevé de victimisation répétée (Button, Lewis, & Tapley, 2009;Cross, Richards, & Smith, 2016). En raison de ce rôle actif, la victime est souvent blâmée et honteuse. Les campagnes de sensibilisation devraient également se concentrer sur cet aspect, permettant aux victimes et à leur environnement de reconnaître qu'elles ne sont pas à blâmer, mais qu'il s'agit du résultat d'une action malveillante de l'escroc (Burgard & Schlembach, 2013). Beaucoup de dommages émotionnels peuvent être évités dans ce cadre. En outre, les victimes devraient également être informées du risque d'être abusées une deuxième fois, par exemple en raison de l'existence de « listes de dupes » (Cross, Richards, & Smith, 2016).

« La prévention situationnelle de la criminalité peut être caractérisée comme comprenant des mesures (1) visant des formes très spécifiques de criminalité, (2) qui impliquent la gestion, la conception ou la manipulation de l'environnement immédiat d'une manière aussi systématique et permanente que possible, (3) afin de réduire ainsi les possibilités de criminalité et d'augmenter les risques perçus par un éventail de délinquants » (Lab, 2010, p. 192). Essentiellement, l'idée est de prévenir la criminalité en réduisant les caractéristiques des situations qui facilitent la délinquance. Des caractéristiques situationnelles spécifiques sont manipulées afin de bloquer les opportunités de criminalité (Jacques & Bonomo, 2017).

Une publication universitaire présente un intérêt particulier en la matière. Récemment, Mark Button et Cassandra Cross ont publié un livre intitulé *Cyber frauds, scams and their victims* (2017). En plus d'offrir de nombreux aperçus sur ce type de crime, il contient un chapitre entier consacré à la prévention des fraudes et des escroqueries. Les auteurs ont articulé leur chapitre autour du cadre de la prévention situationnelle du crime. À la suite des travaux de Clarke, ils ont adapté les 25 techniques de prévention situationnelle du crime (Cornish & Clarke, 2003) au contexte des cyberfraudes et des escroqueries.

Ces 25 techniques peuvent être classées en cinq grandes stratégies (ce qui fonctionne dans la prévention du crime) :

1. Accroître l'effort associé à la commission d'une infraction
2. Accroître le risque associé à la commission d'une infraction
3. Réduire les gains de l'action criminelle
4. Réduire les incitations, qui, autrement, pourraient accélérer le délit
5. Supprimer les excuses que les délinquants pourraient invoquer pour justifier une action criminelle.

Button et Cross (2017, p203) ont résumé leur travail dans la figure ci-dessous. Nous invitons tous les lecteurs intéressés à consulter ce livre, car il donne un aperçu très complet des cyber-escroqueries et des fraudes et combine de nombreux résultats de recherche.

	Intensifier les efforts	Accroître les risques
Individu	> Protéger les comptes avec des mots de passe complexes, une protection anti-virus > Enregistrements de protection > Poursuivre la mise en œuvre de mesures visant à compliquer la tâche des tiers recherchant des données à caractère personnel	> Supprimer régulièrement les virus, logiciels espions, etc., présents sur les ordinateurs > Vérifier les sites Internet, les expéditeurs de courriels et les appelants
Organisation	> Contrôles appropriés pour protéger les données personnelles des clients > Vérification des antécédents : vérifier que les clients sont bien ceux qu'ils prétendent être.	> Partage de l'information : couplage et extraction de données > Vérification de la voix et de l'emplacement des clients
Organismes de police	> Perturber les activités des fraudeurs > Escroquerie > Poursuivre les ordonnances et les restrictions à l'encontre des fraudeurs en recourant au droit civil, réglementaire ou pénal.	> Partage de l'information : couplage et extraction de données > Rapports centralisés > Publication d'informations sur des escroqueries présumées, les sites Internet suspects > Fausses escroqueries pour alerter les victimes potentielles

Réduire les gains	Réduire les incitations	Supprimer les excuses
Si le fraudeur est connu et possède des biens, intenter une action civile pour obtenir des dommages-intérêts ou demander réparation par voie pénale.		
Si le fraudeur est connu et possède des biens, intenter une action civile pour obtenir des dommages-intérêts ou demander réparation par voie pénale.		Communiquer avec les clients pour les éduquer sur les risques et les bonnes pratiques afin de réduire les risques.
> Si le fraudeur est connu et possède des biens, intenter une action civile pour obtenir des dommages-intérêts ou demander réparation par voie pénale. > Suivi des transferts financiers vers les pays tiers à haut risque afin d'identifier les victimes potentielles et les avertir en cas de victimisation potentielle.	> Restreindre l'information sur la façon dont certaines escroqueries ont été menées > Réglementation des activités de publicité et de promotion	> Communiquer avec le grand public et les groupes à risque pour mettre en évidence les risques et les bonnes pratiques. > Campagnes publicitaires : télévision, radio, journaux, publications spécialisées, en ligne. > Communiqués de presse pour susciter l'intérêt des médias > Sites Internet de spécialistes > Mailshots > Courriels, textes, tweets sur les réseaux sociaux > Activités communautaires et des groupes d'intérêt > Scénarios des drames

2. Si cela semble trop beau pour être vrai, tel est probablement le cas.

Dans cette section, nous fournirons un aperçu de certaines bonnes pratiques que nous avons découvertes sous la présidence bulgare. Les projets et les campagnes sont discutés sous différentes catégories, chacune représentant le groupe cible : la prévention universelle, sélectionnée ou indiquée, respectivement l'ensemble de la population, un groupe à risque spécifique ou des personnes déjà victimes. Tous ces campagnes et projets peuvent également être consultés dans la troisième partie de cette boîte à outils.

Prévention universelle

La Présidence bulgare a décidé de se concentrer sur les fraudes et les escroqueries et ce sentiment d'urgence se reflète dans la stratégie de la police nationale. Une section « fraude » au sein de la Direction générale de la Police nationale se consacre à cette question, en particulier aux escroqueries par téléphone. Elle travaille de manière réactive, mais la prévention est également une tâche fondamentale pour lutter contre ce crime. Dans le cadre de leur travail, des campagnes d'information permettent d'accroître les connaissances et d'intensifier la sensibilisation de la population à ce crime. Par exemple, des brochures d'informations sont distribuées, mais des conseils sont également donnés durant une émission de radio nationale. Les autocollants qui sont distribués sont un autre exemple provenant de la Bulgarie. Ces autocollants diffusent des messages préventifs et les personnes sont invitées à les coller sur leur téléphone. L'idée est que, lorsqu'elles reçoivent un appel, elles se souviennent du message de prévention, car elles visualisent l'autocollant lorsqu'elles décrochent.

En Suède, un organisme similaire est chargé de la prévention de la fraude : le Centre national suédois de lutte contre la fraude. Son travail de prévention se concentre sur la sensibilisation par le biais des médias traditionnels et des réseaux sociaux, mais également sur la conclusion de partenariats externes avec les autorités et les entreprises. Certaines campagnes

poursuivent un double objectif. Outre la sensibilisation du public aux dangers des escroqueries via des campagnes médiatiques, elle a également eu recours aux médias pour faire pression sur une application qui présentait de graves problèmes de sécurité qui étaient exploités par des fraudeurs. Cette exposition médiatique a incité les concepteurs de l'application à améliorer leur sécurité.

Au niveau européen, le Mois européen de la cybersécurité (ECSM)4 est annuellement organisé au mois d'octobre. Cette campagne européenne vise à promouvoir la cybersécurité parmi les citoyens et les organisations et souligne les mesures simples qui peuvent être prises pour y parvenir. L'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA), la Commission européenne, Europol et, en particulier, le Centre européen de la cybercriminalité (CE3) et un large éventail de partenaires publics et privés des États membres, collaborent pour atteindre cet objectif et organisent de nombreux événements et campagnes durant le mois. Au cours de la troisième semaine de la campagne de 2018, l'accent a été mis sur les cyber-escroqueries. L'objectif était d'éduquer le grand public sur la manière d'identifier les contenus trompeurs afin d'assurer sa sécurité et celle de ses finances en ligne. EC3, la Fédération bancaire européenne (FBE) et d'autres partenaires ont uni leurs forces pour mener une campagne de sensibilisation sur ce sujet. Quelques exemples de ce matériel sont fournis ci-dessous.

Une autre campagne de sensibilisation est la campagne anti-hameçonnage menée par le Centre belge pour la cybersécurité (CCB). Cette campagne classique a fourni des informations sur la façon de reconnaître les courriels frauduleux. La campagne a été diffusée par le biais de vidéos, de signatures électroniques, de bannières, d'affiches, mais également sur une page Internet. Outre des informations et des conseils de prévention, le site Internet a également fourni au public la possibilité de vérifier son degré de « protection contre le hameçonnage ». Au terme du test, des

ROMANCE SCAM

Scammers target victims on online dating websites, but can also use social media or email to make contact.

WHAT ARE THE SIGNS?

Someone you have recently met online professes strong feelings for you, asking to chat privately.

Their messages are often poorly written and vague.

Their online profile is not consistent with what they tell you.

They may ask you to send intimate pictures or videos of yourself.

First they gain your trust. Then they ask you for money, gifts or your bank account/credit card details.

If you don't send the money, they may try to blackmail you. If you do send it, they will ask for more.

ARE YOU A VICTIM?

Don't feel embarrassed!
Stop all contact immediately.
If possible, keep all communication, such as the chat messages.
File a complaint with the police.
Report it to the site where the scammer first approached you.
If you have provided your account details, contact your bank.

WHAT CAN YOU DO?

- **Be very careful** about how much personal information you share on social network and dating sites.
- **Always consider the risks.** Scammers are present on the most reputable sites.
- **Go slow** and ask questions.
- **Research** the person's photo and profile to see if the material has been used elsewhere.
- **Be alert** to spelling and grammar mistakes, inconsistencies in their stories and excuses such as their camera not working.
- **Don't share** any compromising material that could be used to blackmail you.
- If you agree to meet in person, **tell family and friends** where you are going.
- **Beware of money requests.** Never send money or give credit card details, online account details, or copies of personal documents.
- **Avoid sending them upfront payments.**
- **Don't transfer money** for someone else: money laundering is a criminal offence.

EUROPOL EC3 | European Cybercrime Centre

EBF

EUCPN

#CyberScams

BANK VISHING CALLS

Vishing (a combination of the words Voice and Phishing) is a phone scam in which fraudsters try to trick the victim into divulging personal, financial or security information or into transferring money to them.

WHAT CAN YOU DO?

- **Beware** of unsolicited telephone calls.
- **Take the caller's number** and advise them that you will call them back.
- In order to validate their identity, **look up the organisation's phone number** and contact them directly.
- **Don't validate the caller using the phone number they have given you** (this could be a fake or spoofed number).
- Fraudsters can find your basic information online (e.g. social media). **Don't assume a caller is genuine** just because they have such details.
- **Don't share** your credit or debit card PIN number or your online banking password. Your bank will never ask for such details.
- **Don't transfer money** to another account on their request. Your bank will never ask you to do so.
- If you think it's a bogus call, **report it to your bank.**

EUROPOL EC3 European Cybercrime Centre | EBF | EUCPN

#CyberScams

mesures de prévention sont exposées sur les mesures et les actions qui peuvent être prises pour améliorer encore la sécurité. De plus, les gens peuvent également transférer des courriels suspects, selon eux, à une adresse électronique de la CCB. La CCB vérifie ensuite ces courriels et les liens vers des sites Internet frauduleux et inscrit ces sites Internet sur la liste noire des quatre principaux navigateurs (Internet Explorer, Mozilla Firefox, Google Chrome et Safari). Cela est réalisé via l'EU Phishing Initiative Partnership. Une fois ces sites inscrits sur la liste noire, ils sont bloqués pour les autres utilisateurs. Chaque jour, ce mécanisme de la CCB peut inscrire cinq sites Internet sur la liste, ce qui en fait un mécanisme de prévention très intéressant financé par crowdfunding.

Sélectivité

Comme déjà mentionné dans les sections précédentes, une attention soutenue est portée aux personnes âgées lorsqu'il s'agit de ce type de crime. C'est ce qui ressort déjà de la boîte à outils sur les crimes visant les personnes âgées, qui a été mise en place sous la présidence slovaque. Plusieurs projets qui ont participé cette année au concours relatif au Prix européen de la prévention de la criminalité se sont concentrés sur ce type de criminalité ciblant les personnes âgées. Par exemple, le projet allemand « Hello Granny, I need money », qui est arrivé en deuxième position, s'est concentré sur les escroqueries téléphoniques impliquant le truc des petits-enfants. Par le biais d'une pièce de théâtre interactive, les personnes âgées sont informées de ce phénomène criminel tout en poursuivant l'objectif de réduire les sentiments subjectifs d'insécurité.

L'Initiative européenne de lutte contre le hameçonnage est un projet financé par la Commission européenne et dont l'objectif principal est d'éradiquer les sites Internet frauduleux. L'objectif est de prévenir que les escroqueries par hameçonnage puissent tromper les victimes en bloquant les sites Internet utilisés à cette fin. Il repose sur un partenariat public-privé dédié à la lutte contre le hameçonnage.

Plus d'informations :
https://ec.europa.eu/home-affairs/financing/fundings/projects/HOME_2013_ISEC_AG_INT_4000005246_en

De même, le programme tchèque « Nedáme se » (ou « Nous ne serons pas dupes ») est une pièce de théâtre éducative interactive, dans laquelle quatre types de manœuvres frauduleuses courantes utilisées contre les personnes âgées sont jouées sur scène. Il s'agit de campagnes de vente, de vente de parfums dans la rue, de télémarketing et de techniques de vente au domicile de personnes âgées. Outre les acteurs, un policier et l'auteur de la pièce, le psychologue PhDr. Romana Mazalová, dont une apparition sur scène. Ils participent à la pièce et interagissent avec le public, leur apprenant ainsi de nouvelles stratégies de défense. Le jeu n'est donc pas seulement agréable, il devient également une nouvelle forme d'éducation contre ce qui est appelé les « Šmejdi » ou les fraudeurs. Au total, un millier de personnes âgées ont participé au projet. L'effet pédagogique de cette pièce de théâtre sur le public a fait l'objet d'un examen expérimental. Les résultats ont confirmé que les personnes âgées qui avaient vu la pièce étaient mieux armées contre les vendeurs frauduleux. L'expérience a comparé 130 personnes âgées qui ont vu la pièce de théâtre et un groupe témoin. Six mois après avoir vu la pièce de théâtre, le groupe expérimental a refusé un faux contrat 2,5 fois plus souvent que le groupe qui n'avait pas vu la pièce.

Un autre projet qui se concentre sur le travail avec les personnes âgées est le projet « Le prix de l'amitié » de la Roumanie. L'objectif du projet était de réduire le risque de victimisation des personnes âgées en poursuivant les objectifs suivants : connaître le groupe cible dans la perspective des attitudes et des comportements, accroître le niveau de connaissance préventive des personnes âgées et accroître la capacité d'auto-défense. Le groupe cible se composait de personnes de plus de 60 ans, membres de clubs seniors locaux. En 2017, 34 activités d'information préventive ont été menées par la police. Les informations soulignaient les risques liés à l'âge, mais également la prévention de la victimisation en cas de stratagèmes trompeurs, tels que les fausses campagnes téléphoniques. En outre, des cours de formation en ligne ont été dispensés aux personnes âgées. De

plus, un « bal de la sécurité des aînés » a été organisé pour lancer une campagne d'information publique.

Outre la sensibilisation de ce groupe cible, un mécanisme intéressant a été mis en œuvre en Bulgarie. La section anti-fraude bulgare a noué plusieurs partenariats appropriés avec des acteurs privés, tels que le secteur bancaire. Ce mécanisme de prévention, davantage situationnel par nature, introduit un système de contrôle lorsqu'une personne de plus de 50 ans retire un montant supérieur à 3000 euros. Dans ce cas, le préposé à la banque recevra un avertissement en vertu duquel il pourra poser quelques questions afin de vérifier si la personne âgée n'est pas impliquée dans un stratagème manipulateur.

Indiqué

Une autre série d'activités de prévention se concentre sur les personnes qui ont déjà été abusées. Des interventions spécifiques visent à prévenir la persistance de la victimisation et le fait d'être plusieurs fois la victime de différentes escroqueries. Par exemple, le Projet Sunbird en Australie cible les transactions financières entre l'Australie occidentale et certains pays d'Afrique occidentale. La police examine ces transactions et dresse la liste des transactions semblant illégales. Les victimes sont ensuite contactées et sont informées du motif pour lequel la police estime qu'elles pourraient être victimes de fraude. Lors de l'évaluation, 73 % des personnes contactées ont cessé d'envoyer de l'argent vers ces pays (Button & Cross, 2017).

Au Royaume-Uni, Action Fraud, le centre national de signalement des fraudes et de la cybercriminalité, signale régulièrement les dernières fraudes et escroqueries (Button & Cross, 2017). Ils dirigent également les victimes vers des groupes de soutien dédiés pour aider les personnes abusées ou leur fournir les informations quand elles doivent signaler la fraude5. Cela peut participer à la réduction des dommages émotionnels, mais également aider les victimes à récupérer l'argent perdu ou donner des conseils sur la façon d'agir à l'avenir, au cas où elles seraient recontactées. En raison de l'existence des listes de dupes (cf. supra), il s'agit d'une véritable menace.

Comme déjà mentionné, les victimes souffrent d'une variété d'effets négatifs dus à leur victimisation. Entre autres choses, les victimes ont exprimé le besoin pressant d'être simplement écoutées et reconnues comme victimes. Cependant, il existe - même au niveau mondial - peu de services de soutien à ces victimes. Un exemple

rare d'un tel programme de soutien se trouve au Canada : la Senior Support Unit. Via un service téléphonique, assuré par des bénévoles plus âgés et de pairs, ils offrent un soutien aux victimes de fraude. Ils donnent des conseils et des avertissements, sont à l'écoute et rassurent (Cross, 2016). Une telle initiative offre non seulement un soutien aux victimes individuelles, mais elle contribue également à accroître le nombre de signalements, ce qui, à son tour, permet d'améliorer l'information des services de police et la prévention.

3. Prévenir les escroqueries téléphoniques : en quoi puis-je vous aider ?

Le secrétariat du REPC a organisé un atelier sur le thème de la fraude individuelle. Plusieurs experts se sont réunis et ont discuté de leurs idées et de leur travail de prévention dans ce domaine. L'atelier comportait trois parties. Premièrement, l'image de la fraude individuelle dans le domaine des renseignements a été abordée. Elle est abordée dans la première partie de cette boîte à outils. Deuxièmement, différents projets ont été présentés et discutés avec le groupe. La section ci-dessus y est consacrée. Enfin, une méthode World Café a été organisée pour formuler des recommandations en matière de prévention des escroqueries téléphoniques. De cette manière, les experts ont discuté de leurs recommandations en petits groupes. Les experts qui ont participé à l'atelier sont les suivants :

- Mark Button, Université de Portsmouth, Royaume-Uni
- Michael Will, Europol, AP Furtum
- Simeon Dimchev, Section des fraudes de la Direction générale de la police nationale, Bulgarie
- Charlotta Mauritzson, Centre national de la fraude, Suède
- Andries Bomans, Centre pour la cybersécurité, Belgique
- Constantin Lica, Département de lutte contre la fraude, Roumanie
- Aurelian Bocan, Direction générale de la police de Bucarest, Roumanie
- Romana Mazalová, projet « Nedáme se », République tchèque

Nous avons combiné les recommandations suivant l'exemple de Button (2017), cité antérieurement, et avons utilisé les cinq grandes stratégies de Clarke comme cadre directeur. Il va sans dire qu'elles ne s'excluent pas les unes les autres, mais qu'elles peuvent être combinées dans différents projets. Comme déjà mentionné, elles sont :

1. Intensifier les efforts
2. Accroître les risques
3. Réduire les gains
4. Réduire les incitations
5. Supprimer les excuses

Intensifier les efforts

La première stratégie possible consiste à intensifier les efforts qu'un escroc doit déployer pour que l'escroquerie réussisse. En l'occurrence, l'idée implique que, si les efforts sont trop importants, l'escroc s'abstiendra de commettre des infractions. Comme nous l'avons indiqué clairement dans la première partie de cette boîte à outils, les délinquants peuvent trouver leurs victimes potentielles dans des listes légales. En l'occurrence, les organisations publient ouvertement les coordonnées des personnes, mais les gens partagent également leurs numéros de téléphone librement et volontairement. Par exemple, les numéros de téléphone sont disponibles sur les profils Facebook, les pages LinkedIn, ... Restreindre la publication des numéros de téléphone sur ces listes et les profils des réseaux sociaux pourrait déjà compliquer la tâche d'un escroc qui souhaite contacter ses victimes.

Une autre manière d'intensifier l'effort est de restreindre l'accès à l'utilisation des numéros de téléphone. Il est extrêmement facile d'acheter une carte prépayée ou un nouveau numéro de téléphone. Cela permet aux escrocs de changer constamment de numéro, ce qui complique la tâche des services de répression qui souhaitent les retrouver. Une des idées formulées durant l'atelier était de limiter le nombre de numéros de téléphone par personne, en les reliant à leur compte bancaire ou numéro d'identification. Une coopération étroite avec les entreprises de téléphonie mobile serait souhaitable en la matière. Cela nécessite non seulement des efforts accrus de la part de l'escroc, mais cela réduit également l'anonymat et augmente le risque d'être appréhendé.

Avec l'essor des appels en ligne, il est toujours relativement aisé de contacter des victimes potentielles et de dissimuler votre position pour qu'elle semble légitime. L'utilisation accrue de mots de passe, le cryptage et l'impossibilité quasi-totale de dissimuler la localisation devraient également accroître les efforts que le délinquant doit déployer pour contacter les victimes et les escroquer.

L'appâtage a également été désigné comme une tactique possible, bien que cela

ne soit pas suffisant en soi. L'idée est que les services de répression ou d'autres organisations pourraient essayer d'arnaquer les fraudeurs en les attirant dans des voies inutiles et en leur faisant perdre leur temps. Pendant qu'ils sont occupés à suivre ces pistes, ils ne peuvent pas arnaquer des victimes innocentes.

Accroître les risques

Un aspect clé pour prévenir les escroqueries est de savoir à quoi vous être confronté. Le partage de l'information est d'une importance cruciale en la matière. Comme les escroqueries peuvent être signalées à divers acteurs, tels que la police, mais également à des acteurs privés, il est impératif de partager l'information entre les secteurs public et privé. Cela permettrait d'intervenir plus rapidement et de prendre des mesures préventives mieux informées, ce qui augmenterait le risque. Par conséquent, d'autres intervenants que les services de répression doivent être impliqués. Les sociétés de téléphonie mobile, les banques, les associations sans but lucratif,... ont toutes leur rôle à jouer et peuvent compléter le puzzle de l'information. Cette coopération ne doit pas davantage s'arrêter aux frontières nationales. Dans ce cadre, Europol joue un rôle crucial en sa qualité de facilitateur de l'échange d'informations et des activités transfrontalières. Étant donné que ce type de criminalité s'internationalise chaque jour davantage, les pays tiers devraient également être consultés pour échanger des informations. Cette information pourrait également être partagée avec le grand public. S'il est informé au sujet des sociétés que les escrocs prétendent représenter, il peut déjà être sur ses gardes.

Naturellement, ces informations doivent d'abord être recueillies et les victimes doivent être mieux informées au sujet des possibilités de signalement. Par exemple, les campagnes de sensibilisation pourraient également expliquer la manière dont le signalement de l'infraction permet de mener à bien l'enquête et de trouver des solutions adéquates. La mise en place d'un système central de signalement pour les victimes, avec un accès à tous les acteurs du terrain, faciliterait également le processus de signalement et abaisserait considérablement le seuil à partir duquel les victimes peuvent effectivement procéder au signalement.

Une autre stratégie pour augmenter les risques consiste à réduire l'anonymat. Comme mentionné dans la rubrique « intensifier les efforts », l'évolution des TIC a permis de dissimuler le lieu d'où émane l'appel. De cette façon, la victime pourrait croire qu'elle parle à quelqu'un de son pays, alors qu'elle discute plutôt avec quelqu'un établi à l'étranger. Rendre plus difficile la dissimulation de votre position géographique

entraînera une exposition accrue et un risque accru d'être appréhendé. Cela pourrait être un mécanisme pour les banques, par exemple. Ils pourraient disposer de logiciels de reconnaissance vocale et de services de localisation pour vérifier si ces données correspondent ou non aux données normales du client. La comparaison de ces caractéristiques « normales » est également utilisée dans l'exemple de certaines banques en Bulgarie (cf. supra), où le préposé de la banque est alerté lorsqu'une personne de plus de 50 ans souhaite retirer une somme d'argent supérieure à la normale.

Selon les experts participant à l'atelier, les campagnes de sensibilisation devraient également expliquer les risques et les sanctions auxquels les escrocs s'exposent, et ce, afin de les dissuader. Ces sanctions devraient également être renforcées pour contrer les gains perçus par les escrocs. Les sanctions pécuniaires, en particulier, sont jugées appropriées en la matière. Avec une formation et des ressources plus spécialisées pour les services de répression, ce crime devrait être traité comme une forme de criminalité organisée et puni en conséquence.

Réduire les gains

Cette troisième série de mesures visant à prévenir les escroqueries téléphoniques consiste à réduire les gains pouvant être obtenus en commettant ce délit. En l'occurrence, la principale recommandation est de saisir les actifs qui sont obtenus par le biais d'escroqueries téléphoniques. Une étape importante consiste à surveiller les flux monétaires. L'exemple australien susmentionné nous informe sur la nature exacte de ce processus et sur la mesure dans laquelle la détection des transactions suspectes peut être efficace. Les experts ont exprimé la nécessité d'une initiative européenne avec les banques afin de l'adapter à la perspective européenne. Une autre recommandation consiste à confisquer le matériel et les moyens nécessaires afin de commettre le délit.

Réduire les incitations

Au cours de l'atelier, aucune recommandation spécifique n'a été formulée pour réduire les incitations. Toutefois, selon Button (2017), nous pourrions affirmer que, dans certains cas, il est important de ne pas communiquer trop d'informations sur la manière dont l'escroquerie a été organisée afin d'éviter les imitateurs. De plus, il est également de notoriété publique que les fraudeurs contacteront les

victimes avec une offre qui leur permettra de récupérer leurs pertes, par exemple. Naturellement, l'intention est toutefois de procéder à une seconde escroquerie. La sensibilisation à ce problème revêt une importance cruciale.

Supprimer les excuses

La dernière série de recommandations est principalement axée sur la sensibilisation aux escroqueries téléphoniques et sur la manière de se protéger au mieux afin de ne pas être abusé. Cela inclut la campagne d'information classique via une palette de canaux tels que la radio, la télévision, les dépliants,... L'information qui doit être partagée peut expliquer le modus operandi de certaines escroqueries, mais également la manière de s'en prémunir. Les exemples de la Roumanie ou de la République tchèque l'ont déjà clairement montré. Un jeu de rôles, par exemple, désigne une méthode intéressante pour enseigner aux gens comment appliquer des stratégies défensives à leur propre situation. Dans ce cadre, les partenariats public-privé sont tout aussi importants pour diffuser un message de prévention, que le sont le partage de l'information pour identifier les escrocs. Il s'agit d'une responsabilité partagée, qui peut également être assumée au sein de groupes communautaires ou de groupes de pairs.

Naturellement, les campagnes doivent être évaluées pour s'assurer de leur efficacité. Un aspect important à cet égard est la diffusion du même message au sein des différentes organisations, mais également des différents pays. L'exemple d'Europol (cf. supra) en est un bon exemple. De plus, il serait peut-être bon de partager l'information sur la diversité des escroqueries existantes et d'expliquer leur mode de fonctionnement. Toutefois, le message sur la manière de se protéger devrait être constant, afin d'être aussi clair et simple que possible. *Simplement dire non*.

La sensibilisation devrait également se concentrer sur les personnes qui ont déjà été abusées. Il convient non seulement de leur faire prendre conscience des risques d'être escroquées une seconde fois, mais également d'insister sur le besoin évident de soutien pour ces victimes. Les réseaux de soutien qui partagent les informations entre les victimes et se soutiennent mutuellement dans leurs pertes (financières et émotionnelles) doivent être mentionnées ici. Une hotline a également été mentionnée par les experts afin d'offrir aux victimes les informations et les conseils appropriés.

4. Conclusions

Dans cette deuxième partie de la boîte à outils, nous nous sommes intéressés à la prévention de la fraude individuelle. Tout d'abord, certains commentaires généraux ont été formulés sur la base de recherches universitaires. En dépit du manque d'études académiques sur la prévention de la fraude individuelle, nous avons constaté que la tactique de prévention la plus courante consiste à **éduquer le public** sur la façon de reconnaître les escroqueries et de réagir face à ces dernières. Une étude a démontré une amélioration de 40 % après l'évaluation du matériel de formation qui a été fourni à un groupe expérimental. Ces types d'évaluations sont toutefois rares et nous ne pouvons que recommander d'intensifier les recherches et les évaluations en la matière.

Des études ont également illustré la nécessité de se concentrer sur les personnes qui ont déjà été escroquées. Ceci est dû à des niveaux élevés de victimisation répétée, mais également aux dangers de victimisation secondaire par les pairs, la famille, les organismes officiels,... Les **victimes** devraient être soutenues dans leurs pertes et sensibilisées aux dangers d'être escroquées une seconde fois.

Deuxièmement, nous avons fourni un aperçu de certaines **bonnes pratiques** qui existent dans les États membres. Elles ont été classées en fonction de leur groupe cible : activités de prévention universelles, sélectives et indiquées. Dans la troisième partie de cette boîte à outils, le lecteur peut également consulter tous ces projets.

Enfin, à l'issue d'un atelier auquel ont participé divers experts européens, nous avons formulé des **recommandations** sur les moyens de prévenir les escroqueries téléphoniques. Ces recommandations étaient axées sur les cinq grandes stratégies de prévention situationnelle du crime : intensifier les efforts, augmenter le risque, réduire les gains, réduire les incitations et éliminer les excuses.

Factsheet

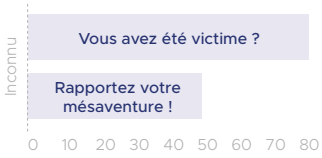
PRÉVENIR LES ESCROQUERIES TÉLÉPHONIQUES

COMMENT PUIS-JE VOUS AIDER ?

INGÉNIERIE SOCIALE

La plupart des fraudes individuelles reposent sur une technique appelée ingénierie sociale. Il s'agit de la principale ayant pour objet de gagner la confiance des victimes et les convaincre de plonger dans l'arnaque. En tant que telle, la victime joue un rôle très actif dans l'accomplissement du délit, ce qui induit un sentiment de honte et de culpabilité.

CHIFFRE INCONNU



VOICI LES ÉTAPES À SUIVRE

01 Intensifier les efforts

> Restreindre la publication des numéros de téléphone
> Protection par mot de passe et cryptage renforcés
> Escroquerie

02 Augmenter le risque

> Partager les informations entre toutes les parties concernées
> Promouvoir l'établissement de rapports
> Réduire l'anonymat de l'appelant

03 Réduire les gains

> Saisir des actifs obtenus illégitimement
> Surveiller les flux d'argent

04 Réduire les incitations

> Éviter les imitateurs
> Sensibiliser aux escroqueries de récupération

05 Éliminer les excuses

> Sensibiliser
> Évaluer les campagnes
> Soutenir les victimes

Vous voulez en savoir plus ?
Consultez le site www.eucpn.org

03 PARTIE III: EXEMPLES TIRÉS DE LA PRATIQUE

“ ESCROQUERIE DE LA GRAND-MÈRE - TU CONNAIS ? ” (AT)

Brève description :
Le téléphone sonne au domicile de la victime (« Grand-mère »). Sans se méfier, la victime suppose que l’appelant est un ami ou un parent. La victime commence à deviner qui appelle, prononce plusieurs noms différents de membres de la famille (dans la plupart des cas, le nom de ses petits-enfants ou de ses neveux), le fraudeur en choisit un et prétend être cette personne. Plus tard, l’appelant décrit sa situation d’urgence financière et demande de l’argent à la victime. Il n’est pas inhabituel dans de tels cas que les victimes perdent toutes leurs économies ; souvent, cette perte entraîne une détresse émotionnelle grave, voire des troubles physiques.

La prévention du crime s’avère difficile ; les victimes potentielles sont souvent fermées aux discours ou aux campagnes. Le personnel de la Banque a joué un rôle crucial dans la prévention ; cette campagne, menée en coopération avec la Banque nationale autrichienne et la Chambre de commerce, a donc pour objectif d’informer et de motiver le grand public et le

personnel de la Banque en particulier ; elle inclut un film d'information intitulé « L'escroquerie de la grand-mère ».

Début/durée :
Date de début du projet : 01.04.2015
Communiqué de presse (conférence de presse) : 18.02.2016
En cours : campagne de sensibilisation avec la presse écrite, sur la base du clip vidéo produit.

Recherche de base :
Le sous-département de la prévention de la criminalité et de l'aide aux victimes a procédé à une évaluation de l'impact, du modus operandi et de l'ampleur de ce type de fraude, en collaboration avec le sous-département de la criminalité économique, le sous-département de la fraude, de la falsification et de la criminalité économique et le département de l'analyse criminelle au Service autrichien de renseignements criminels.

Budget :
Le clip (7 000 euros), financé par le Service autrichien de renseignements criminels et le coût de la campagne via la presse écrite (1 000 euros), étaient les plus coûteux ; de plus, la conférence de presse a été financée par la Banque nationale ; la distribution du contenu a été financée conjointement par les trois parties prenantes.

Type d'évaluation :
Un des partenaires du projet, la Banque nationale autrichienne, a organisé une tournée de présentation qui s'est arrêtée dans toutes les provinces et districts autrichiens au cours de l'été 2016. Au terme de la tournée, le personnel a pris le temps de se rendre dans chaque banque de chaque ville, étape de la tournée de présentation, et a interrogé les employés sur leurs connaissances relatives à l'escroquerie dite de la grand-mère, s'ils avaient vu le clip et s'ils avaient su comment réagir correctement au cas où ils rencontreraient un suspect.

Pour 91% des employés, l'escroquerie dite de la grand-mère était connue et ils savaient également comment réagir en cas de suspicion. En moyenne, seuls 19% connaissaient le clip ; il a donc été décidé de lancer une autre campagne avec des fiches d'information pour promouvoir à nouveau le modus operandi et le clip.

Acteur exécutant l'évaluation/le calendrier :
Externe : Banque nationale autrichienne

Type de méthode de collecte des données :
Évaluation d'impact réalisée par la Banque nationale autrichienne dans 158 banques disséminées dans toute l'Autriche.

Plus d'infos :
http://eucpn.org/document/granny-scam

BONJOUR GRAND-MÈRE, J'AI BESOIN D'ARGENT (DE)

Brève description :
Les personnes âgées attirent les fraudeurs. Une méthode qui est devenue populaire parmi les criminels est « l'escroquerie dite des petits-enfants », dans laquelle les fraudeurs se font passer pour des parents de la victime, prétendant se trouver dans une situation désespérée et avoir un besoin urgent d'argent.

Le projet « Bonjour Grand-mère, j'ai besoin d'argent » propose un concept innovant pour la prévention du crime en matière de fraude. Il s'agit d'une pièce de théâtre interactive qui offre une vue d'ensemble des techniques les plus répandues et des mesures à prendre pour se protéger afin de ne pas devenir une victime potentielle. Il réduit également la peur subjective envers les escrocs et encourage à avoir davantage confiance en soi.

Le public participe activement au spectacle. Des spectateurs choisis au hasard prennent part au spectacle en tant que participants actifs, tandis que les acteurs improvisent et réagissent spontanément à l'intervention du public. Le contexte de cas réalistes aide à transmettre l'urgence et le facteur divertissant assure une impression durable.

Début/durée :
Le projet a démarré le 28/03/2012 et est toujours en cours.

Recherche de base :
Le PKS (Statistiques criminelles de la police) a constaté une augmentation statistique des « escroqueries dites des petits-enfants ». Le nombre de cas était frappant, à l'instar des dommages qui en ont résulté.

Le nombre de cas dans le Land de Bade-Wurtemberg est passé de 95 (2007), 64 (2008), 143 (2009) à 311 en 2010.

Les pertes financières dans le Land de Bade-Wurtemberg sont passées de 234 890 euros (2007), 45 870 euros (2008), 557 900 euros (2009) à 1 108 131 euros en 2010.

Budget :
L'écriture et le développement de la pièce sont le fruit du travail bénévole d'Allan Mathiasch, soutenu par son ensemble théâtral et les partenaires coopérant (police et ville). Le coût d'un spectacle - comprenant deux acteurs

et le matériel - s'élève à 790-890 €, outre les frais de déplacement.

Type d'évaluation :
Évaluation du processus et de l'impact.

Acteur exécutant l'évaluation/le calendrier :
Externe : Theresa Siegler, étudiante à l'université des sciences appliquées de Kehl.

Type de méthode de collecte des données :
Enquête par questionnaire.

Plus d'infos :
https://eucpn.f2w.fedict.be/document/hello-granny-i-need-money

SILVER SURFER (LU)

Brève description :
Le projet « Silver Surfer » est un projet conçu par les seniors pour les seniors. Des seniors bénévoles reçoivent une formation spécifique sur la sensibilisation à l'utilisation sûre de l'Internet. Ils transmettent leurs connaissances à d'autres personnes âgées via des conférences, par exemple lors d'évènements réservés aux personnes âgées, dans des clubs de personnes âgées ou dans des associations de personnes âgées. Les « Silver Surfers » agissent comme des multiplicateurs.

En 2014, le projet a été créé à l'initiative de BEE SECURE et repose sur une collaboration entre le Ministère de la Famille, de l'Intégration et la Grande Région du Luxembourg, SECURITYMADEIN.LU, RBS-Center fir Altersfroen et le SenioreSécherheetsBeroder.

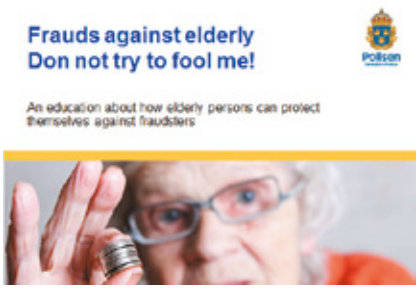
Début/durée :
Le projet a démarré en 2014 et est toujours en cours.

Recherche de base :
En 2013, le partenaire SECURITYMADEIN.LU a lancé une enquête lors d'un salon réservé aux seniors. Le résultat a démontré que les personnes âgées interrogées n'utilisaient le PC que pour échanger des e-mails (94%) ou pour discuter par Skype (32%) avec des membres de leur famille. À peine la moitié d'entre-eux étaient informés des fraudes sur l'Internet. 32% d'entre eux avaient déjà

été victimes de hameçonnage et 12% d'une fraude impliquant le paiement d'une « rançon ». La même étude a été répétée en 2014 à la même foire. Les résultats étaient comparables et illustraient que les seniors utilisaient l'Internet plus souvent (5% de plus qu'en 2013).

Plus d'infos :
https://eucpn.org/document/silver-surfer

N'ESSAYEZ PAS DE ME BERNER (SE)



Brève description :
Le projet « N'essayez pas de me berner » a été créé pour prévenir les délits de fraude à l'encontre des personnes âgées via une sensibilisation accrue à ces délits et pour permettre aux victimes éventuelles de reconnaître plus facilement les tentatives de fraude et de se protéger contre ces dernières.

La méthode choisie pour le projet a consisté à créer un package d'informations et une structure sur la manière d'utiliser le matériel lors de réunions actives durant lesquelles les participants peuvent se former à différentes situations dans lesquelles ils pourraient être victimes de fraude et sur la manière dont ils peuvent agir pour éviter d'être victimes de fraude.

Le matériel est censé être utilisé lors de trois réunions différentes et comprend un guide pour l'animateur de la réunion, trois courts métrages différents et trois guides d'apprentissage différents. Chaque réunion permet de travailler avec un film et un guide d'apprentissage. Le matériel permet un auto-apprentissage et repose sur différents cas pouvant être utilisés pour des discussions et des exercices pratiques.

Début/durée :
Le projet a officiellement démarré le 16/09/2015 et est toujours en cours.

Recherche de base :
Le centre national de lutte contre la fraude de la police suédoise a analysé l'évolution de la fraude en Suède et a constaté une forte augmentation de la fraude à l'encontre les personnes âgées. L'analyse approfondie a illustré le modus operandi utilisé dans ces crimes ainsi que les sources privilégiées. Cette analyse a été utilisée pour élaborer le

matériel et les études de cas dans le matériel du projet. L'analyse reposait principalement sur les données relatives aux délits signalés à la police suédoise.

Budget :
Le coût du projet n'est pas précisé. Le projet ayant été priorisé, toutes les ressources ont été prélevées sur le cadre financier ordinaire et n'ont donc pas été spécifiées. La police et les organisations ont produit elles-mêmes les films et autres matériels, ce qui a permis de maintenir les coûts relativement bas.

Type d'évaluation :
L'évaluation du processus n'est pas encore terminée, mais la méthode sera évaluée en mesurant le nombre de réunions qui ont été tenues et en menant un sondage auprès des personnes qui ont participé au projet sur leur perception du projet et sur les changements qui en ont résulté pour ce qui concerne leur sensibilisation à la fraude et les mesures à prendre pour éviter d'être escroquées. L'évaluation d'impact n'a pas encore été réalisée, mais une analyse sera effectuée et les travaux ont commencé par l'analyse de l'évolution dans les délits de ce type signalés et des différences concernant les crimes et tentatives de délits finalisés.

Plus d'infos :
https://eucpn.f2w.fedict.be/document/do-not-try-fool-me

AUTRICHE : LA LISTE DE SURVEILLANCE DE L'INTERNET

Watchlist Internet
Internet-Betrug, Fallen & Fakes im Blick

Brève description
La Liste de surveillance de l'Internet est un projet visant à prévenir et à combattre la criminalité en ligne telle que la fraude et les autres pièges en ligne. Depuis 2013, l'équipe du projet mène des recherches sur les faux sites et les cas de fraude en ligne, dans le but d'informer sérieusement le grand public en publiant des articles de presse sur son site Internet. Ses arguments de vente uniques sont la continuité et l'optimisation efficace des moteurs de recherche. Le projet contribue également à la lutte contre la criminalité en ligne dans son ensemble grâce au réseau qu'il a mis en place entre les plates-formes de commerce électronique, les banques privées, les organismes gouvernementaux et les services de répression en Autriche. L'étroite coopération avec l'organe de règlement des litiges en ligne « Ombudsmann Internet » ainsi qu'avec les parties prenantes et les utilisateurs du site Internet, ce qui contribue au signalement des cas, est également essentielle à la réussite du projet.

Début/Durée
Le projet a démarré le 3 juillet 2013 et est toujours en cours.

Recherche de base
L'équipe de l'ombudsman de l'Internet a analysé le contexte. L'augmentation constatée des cas de fraude sur l'Internet a mis en exergue la nécessité de redoubler d'efforts en matière de sensibilisation. Le nombre de cas a augmenté de 18 pour cent en 2012 par rapport à l'année précédente. Sur la base de ces données, l'Institut autrichien des télécommunications appliquées a créé la Liste de surveillance de l'Internet.

Budget
La Liste de surveillance de l'Internet est financée par le ministère fédéral autrichien du Travail, des Affaires sociales et de la Protection des consommateurs, la Chambre du travail autrichienne, le plus grand marché en ligne autrichien, willhaben.at, et la Bank Austria. Les coûts annuels du projet s'élèvent à quelque 65 000 euros.

Type d'évaluation
Une évaluation interne du processus a été réalisée au mois d'août 2014 sous la forme d'un sondage en ligne auprès des lecteurs du site Internet Watchlist Internet. Sur la base de ces résultats, le projet a été affiné, par exemple en utilisant un langage plus simple à l'égard du public plus âgé. Aucune évaluation externe des résultats ou de l'impact n'a été réalisée, mais une évaluation interne de l'impact est exécutée annuellement.

Acteur exécutant l'évaluation/le calendrier
Interne : par l'équipe de projet et un comité consultatif composé d'intervenants publics et privés.

Type de méthode de collecte des données
L'évaluation annuelle est basée sur Google Analytics, comme les statistiques des utilisateurs, les visiteurs du site Internet, la durée de la visite,..., le feed-back des utilisateurs et des partenaires financiers, ainsi que sur des contrôles permanents de la disparition d'un faux site à la suite de la publication d'articles sur une fraude sur l'Internet.

Liens vers plus d'infos
http://eucpn.org/document/watchlist-internet

SECTION DES FRAUDES DE LA DIRECTION GÉNÉRALE DE LA POLICE NATIONALE BULGARE (BG)

Brève description :
En Bulgarie, une section « fraude » au sein de la Direction générale de la Police nationale se consacre aux escroqueries par téléphone. Outre

leur travail policier réactif, elle assume également la tâche fondamentale de la prévention. Dans le cadre de son travail, des campagnes d'information permettent d'accroître les connaissances et d'intensifier la sensibilisation de la population à ce crime. Par exemple, des brochures d'informations sont distribuées, mais des conseils sont également donnés durant une émission de radio nationale. Les autocollants qui sont distribués sont un autre exemple provenant de la Bulgarie. Ces autocollants diffusent des messages préventifs et les personnes sont invitées à les coller sur leur téléphone. L'idée est que, lorsqu'elles reçoivent un appel, elles se souviennent du message de prévention, car elles visualisent l'autocollant lorsqu'elles décrochent.

MÉCANISME ANTI-DE LA FIRST INVESTMENT BANK EN BULGARIE (BG)

Fibank
Първа инвестиционна банка

Brève description :
En Bulgarie, cette banque dispose d'un mécanisme de détection et de prévention des cas de fraude téléphonique. Si des montants importants sont retirés et s'ils ne correspondent pas à une liste de critères de la banque, le préposé est alerté et invité à vérifier auprès du client s'il subit ou non des pressions. Un algorithme enverra un rapport au préposé si ces critères semblent indiquer un cas possible de fraude téléphonique. Le préposé peut ensuite vérifier auprès du client, selon une « Liste de vérification de fraude téléphonique », en posant des questions, par exemple sur l'objet du retrait ou en surveillant les actions du client.

#CYBERSCAMS (EC3, EUROPOL)

Brève description :
Le Mois européen de la cybersécurité (ECSM) est annuellement organisé au mois d'octobre. Il s'agit d'une campagne européenne de sensibilisation qui promeut la cybersécurité auprès des citoyens et des organisations, en soulignant les mesures simples qui peuvent être prises pour protéger leurs données personnelles, financières et professionnelles. L'objectif principal est de sensibiliser, de changer les comportements et de communiquer des moyens permettant de se protéger en ligne. Chaque semaine, un thème spécifique est abordé et au cours de la troisième semaine de l'édition 2018, le Centre européen de la cybercriminalité (EC3), la Fédération bancaire européenne (FBE) et des partenaires des secteurs public et privé ont uni leurs forces pour présenter les « cyber-escroqueries » comme thème.

7 escroqueries financières courantes en ligne sont présentées sur des fiches d'informations et il est expliqué comment les éviter. Ces documents ont été diffusés dans toute l'UE par le biais d'une campagne sur les réseaux sociaux. Après le lancement, une journée a été consacrée à chaque escroquerie.

Début/durée :
La campagne a été officiellement lancée le 17 octobre 2018. Les documents resteront disponibles en ligne.

Plus d'infos :
https://www.europol.europa.eu/cyberscams

DANS QUELLE MESURE ÊTES-VOUS À L'ABRI DU HAMEÇONNAGE ? (BE)

Brève description :
Cette campagne a été lancée par le Centre belge pour la cybersécurité (CCB) pendant le Mois européen de la cybersécurité (ECSM) de 2017. Le but de la campagne était d'informer le public sur les courriels d'hameçonnage

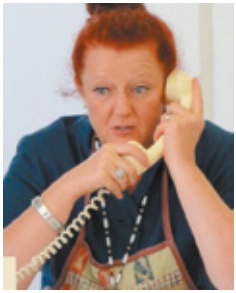
et sur la façon de les reconnaître. En distribuant des dépliants, des affiches, mais en procédant également à une vaste campagne médiatique (sur les réseaux sociaux), le projet affirme avoir atteint quelque 2 millions d'internautes en Belgique.
Outre cette campagne d'information, le public a également été invité à transmettre les courriels suspects à la CCB. En analysant ces courriels et en les vérifiant à l'aide d'un logiciel sophistiqué, 5 liens suspects sont bloqués quotidiennement.

Début/durée :
La campagne a été officiellement lancée le 2 octobre 2017. Les documents sont toujours disponibles en ligne et le mécanisme de transfert est toujours actif.

Plus d'infos :
www.safeonweb.be

NEDÁME SE (NOUS NE LE PRENDRONS PAS) (CZ)

Brève description :
Le programme « Nedáme se » est une pièce de théâtre interactive et éducative, dans laquelle quatre types de techniques de manipulation trompeuses



les plus courantes, utilisées contre les personnes âgées, sont représentées sur scène. Il s'agit de campagnes de vente, de vente de parfums dans la rue, de télémarketing et de techniques de vente au domicile de personnes âgées. Outre les acteurs, un policier et l'auteur de la pièce, le psychologue PhDr. Romana Mazalová, font une apparition sur scène. Ils participent à la pièce et interagissent avec le public, leur apprenant ainsi de nouvelles stratégies de défense. Le jeu est donc non seulement agréable, mais il est également converti en une nouvelle forme d'éducation contre ce qui est appelé les « Šmejdi » (fraudeurs). L'effet pédagogique sur le public a fait l'objet d'un examen expérimental. Les résultats ont confirmé que les personnes âgées qui avaient vu la pièce étaient mieux armées contre les vendeurs frauduleux.

Début/durée :
2015

Plus d'infos :
https://eucpn.org/document/czech-elderly-dont-swallow-bait

LE PRIX DE L'AMITIÉ (RO)

Brève description :
L'objectif du projet était de réduire le risque de victimisation des personnes âgées en poursuivant les objectifs suivants : connaître le groupe cible dans la perspective des attitudes et des comportements, accroître le niveau de connaissance préventive des personnes âgées et accroître la capacité d'auto-défense. Le groupe cible se composait de personnes de plus de 60 ans, membres de clubs seniors locaux. En 2017, 34 activités d'information préventive ont été menées par la police. Les informations soulignaient les risques liés à l'âge, mais également la prévention de la victimisation en cas de stratagèmes trompeurs, tels que les fausses campagnes téléphoniques. En outre, des cours de formation en ligne ont été dispensés aux personnes âgées. De plus, un « bal de la sécurité des aînés » a été organisé pour lancer une campagne d'information publique.

Début/durée :
Janvier 2017

Plus d'infos :
https://eucpn.org/document/price-friendship-project

GUIDE DE SÉCURITÉ POUR LES AÎNÉS (FI)

Brève description :
En Finlande, l'Association finlandaise pour le bien-être des personnes âgées dispose de spécialistes régionaux du bâtiment qui proposent des conseils gratuits aux personnes âgées. Ils interviennent dans les situations où une personne âgée est persuadée de commander une rénovation coûteuse de son logement.
Les personnes âgées peuvent les contacter pour :

- Les vendeurs frauduleux (téléphone, visites à domicile).

- Les escroqueries à la rénovation et la réparation (surévaluées, inutiles, etc.)
- Des conseils sur la **façon d'agir** si le vendeur exerce des pressions en vue de la vente
- Des conseils sur les **contrats et la résiliation** dans un délai de 2 semaines, etc.

acquises. Par exemple, une simulation d'une arnaque à la loterie sera présentée. L'aîné peut alors répondre dans la vie réelle et l'application évaluera le niveau d'assertivité de sa réponse.

" TRUCS CONTRE LES BEAUX PARLEURS " (NL)

Brève description :
Une organisation de personnes âgées aux Pays-Bas a créé une application pour les personnes âgées qui leur apprend les dangers des escroqueries. L'application simule des « situations d'escroquerie » pour que les personnes âgées puissent immédiatement tester leurs compétences nouvellement

ACTION FRAUD (ROYAUME-UNI)

ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040

Brève description :
Action Fraud est le centre national de signalement de la fraude et de la cybercriminalité du Royaume-Uni, où toute fraude doit être signalée en cas d'escroquerie, de fraude ou de cybercriminalité en Angleterre, au Pays de Galles et en Irlande du Nord. Il dirige également les victimes vers des groupes de soutien dédiés pour aider les personnes abusées ou leur fournir les informations quand elles doivent signaler la fraude.

Plus d'infos :
https://www.actionfraud.police.uk/

ENDNOTES

1 Par exemple, les utilisateurs reçoivent des courriels simulés de hameçonnage pour tester leur vulnérabilité ; à la fin du test, ils reçoivent des informations supplémentaires sur la manière de les prévenir à l'avenir (Sheng, Holbrook, Kumaragur, Cranor, & Downs, 2010).

2 En l'occurrence, les utilisateurs reçoivent immédiatement des informations supplémentaires lorsqu'ils cliquent sur un faux lien (Sheng, Holbrook, Kumaragur, Cranor, & Downs, 2010).

3 Anti-Phishing Phill est un bon exemple de jeu en ligne qui enseigne aux utilisateurs de bonnes habitudes pour les aider à éviter les attaques de hameçonnage. Au terme de la formation, les utilisateurs reconnaissaient mieux le site Internet frauduleux que le groupe témoin et connaissaient mieux les stratégies afin d'éviter d'en être victimes (Sheng, et al., 2007).

4 https://cybersecuritymonth.eu/about-ecsm/whats-ecsm

5 https://www.actionfraud.police.uk/support-and-prevention/ive-been-a-victim-of-fraud

BIBLIOGRAPHIE

Agustina, J. (2015). Understanding Cyber Victimization: Digital Architectures and the Disinhibition Effect. International Journal of Cyber Criminology, 9(1), 35-54.

Anderson, K. (2016). Mass-market consumer fraud: who is most susceptible to becoming a victim? Washington D.C.: FTC Bureau of Economics.

Atkins, B., & Huang, W. (2013). A study of social engineering in online frauds. Open Journal of Social Sciences, 1(3), 23-32.

Barnes, P. (2017). Stock market scams, shell companies, penny shares, boiler rooms and cold calling: the UK experience. International Journal of Law, Crime and Justice, 48, 50-64.

Bidgoli, M., & Grossklags, J. (2017). « Hello, This is the IRS calling » : une étude de cas sur les escroqueries, l'extorsion, la mystification et l'usurpation d'identité au téléphone. 2017 APWG Symposium on Electronic Crime Research (eCrime) (pp. 57-69). Scottsdale: AZ.

Bullée, J.-W., Montoya, L., Junger, M., & Hartel, P. (2016). Telephone-based social engineering attacks: an experiment testing the success and time decay of an intervention. Singapore Cyber-Security Conference, (pp. 107-114). Singapour.

Bullée, J.-W., Montoya, L., Pieters, W., Junger, M., & Hartel, P. (2018). On the anatomy of social engineering attacks: a literature-based dissection of successful attacks. J Investig Psychol offender Profil, 15, 20-45.

Burgard, A., & Schlembach, C. (2013). Frames of Fraud: a qualitative analysis of the structure and process of victimization on the internet. International journal of Cyber Criminology, 7(2), 112-124.

Button, M., & Cross, C. (2017). Cyber frauds, scams and their victims. London: Routledge.

Button, M., Lewis, C., & Tapley, J. (2009). Fraud typologies and the victims of fraud: literature review. National Fraud Authority.

Button, M., Lewis, C., & Tapley, J. (2014). Not a victimless crime: The impact of fraud on individual victims and their families. Security Journal, 27(1), 36-54.

Button, M., McNaughton, N., Kerr, J., & Owen, R. (2014). Online frauds: Learning from victims why they fall for these scams. Australian & New Zealand Journal of Criminology, 47(3), 391-408.

Button, M., Tapley, J., & Lewis, C. (2012). The 'fraud justice network' and the infra-structure of support for individual fraud victims in England and Wales. Criminology and Criminal Justice, 13(1), 37-61.

Cialdini, R. (2001). Influence: Sciende and practice. Boston : Allyn & Bacon.

Cornish, D., & Clarke, R. (2003). Opportunities, precipitators and criminal decisions: a reply to Wortley's critique of situational crime prevention. Crime prevention Studies, 16, 41-96.

Crosman, K. (2017). Phone and Television Scams in the Age of the Internet. Lewis & Clark L.Rev., 21, 791.

Cross, C. (2016). 'I'm anonymous, I'm a voice at the end of the phone': a Canadian case study into the benefits of providing telephone support to fraud victims. Crime Prevention and Community Safety, 18, 228-243.

Cross, C., Richards, K., & Smith, R. (2016). The reporting experiences and support needs of victims of online fraud. Trends & issues in crime and criminal justice, 518, 1-14.

De Kimpe, L., Walrave, M., Hardyns, W., Pauwels, L., & Ponnet, K. (2018). You've got mail! Explaining individual differences in becoming a phishing target. Telematics and Informatics, 35(5), 1277-1287.

EUCPN. (2017). Cyber Safety: A theoretical insight. . In E. Secretariat, EUCPN Theoretical Paper Series. Brussels: European Crime Prevention Network.

EUCPN. (2017). Organised Crime Targeting Elderly People: a theoretical overview. In E. Secretariat, EUCPN Theoretical Paper Series. Brussels: European Crime Prevention Network.

Commission européenne (2017). Eurobaromètre spécial 464a : attitudes des Européens à l'égard de la cybersécurité. Bruxelles : Commission

européenne.

Commission européenne (2018). Eurobaromètre spécial 462 : Communications électroniques et marché unique numérique. Bruxelles : Commission européenne.

Europol. (2014). Internet organised Crime Threat Assessment. La Haye : Europol.

Europol. (2016). Internet Organised Crime Threat Assessment. La Haye : Europol.

Europol. (2017). Internet Organised Crime Threat Assessment . La Haye : Europol.

Europol. (2018). Internet Organised Crime Threat Assessment. La Haye : Europol.

Ferreira, A., Coventry, L., & Lenzini, G. (2015). Principles of persuasion in social engineering and their use in phishing. International Conference on Human Aspects of Information Security, Privacy, and Trust (pp. 36-47). Cham: Springer.

Gadhave, U., & Sirsat, S. (2015). Review of Cyber-crimes and their impacts over the society. international Journal of Electronics, Communication & Soft Computing Science and Engineering, 357-359.

Harley, D., Grooten, M., Burn, S., & Johnston, C. (2012). My PC has 32,539 errors: how telephone support scams really work. Virus Conference, (pp. 1-8).

Jacques, S., & Bonomo, E. (2017). Learning from the Offenders' perspective on crime prevention. In B. Leclerc, & E. Savona, Crime Prevention in the 21st Century: insightful approaches for crime prevention initiatives (pp. 9-18). Springer.

Jakobsson, M. (2016). Understanding Social Engineering based scams. New York: Springer.

Lab, S. (2010). Crime prevention: approaches, practices and evaluations. LexisNexis Group.

Leukfeldt, E., & Stol, W. (2011). De marktplaats-fraudeur ontmaskerd: Internetfraudeurs vergeleken met klassieke fraudeurs. Secondant, 25(6), 26-31.

Levi, M. (2008). Organized fraud and organizing frauds: Unpacking research on networks and organization. Criminology & Criminal Justice, 8(4), 389-419.

Levi, M. (2017). Assessing the trends, scale and nature of economic cybercrimes: overview and issues. Crime, law and social change, 67, 3-20.

Levi, M., & Burrows, J. (2008). Measuring the impact of fraud in the UK. British Journal of Criminology, 48, 293-318.

Maggi, F. (2010). Are the con artists back? A preliminary analysis of modern phone frauds. 10th IEEE International Conference on Computer and Information Technology, (pp. 824-831).

Marzuoli, A., Kingravi, H., Dewey, D., & Pindrop, R. (2016). Uncovering the landscap of fraud and spam in the thelephony channel. 15th IEEE international Conference on Machine Learning and Applications, (pp. 853-858).

Mba, G., Onaolapo, J., Stringhini, G., & Cavallaro, L. (2017). Flipping 419 cybercrime scams: targeting the weak and the vulnerable. International World Wide Web Conference, (pp. 1301-1310). Perth.

Mears, D., Reisig, M., Scaggs, S., & Holtfreter, K. (2016). Efforts to reduce consumer fraud victimi-zation among the elderly: the effect of information access on program awareness and contact. Crime & Delinquency, 62(9), 1235-1259.

Moreno-Fernández, M., Blanco, F., Garaizar, P., & Matute, H. (2017). Fishing for phsihers. Improving internet users' sensitivity to visual deception cues to prevent electronic fraud. Computers in Human Behavior, 69, 421-436.

Murphy, D. R., & Murphy, R. H. (2007). Phishing, Pharming, and Vishing: Fraud in the Internet Age. In T. Fowler, & J. Leigh, The Telecommunications Review (pp. 37-45). VA: Noblis.

Ollmann, G. (2007). The vishing guide. IBM Global Technology Services.

Petty, R., & Cacioppo, J. (1986). The elaboration likelihood model of persuasion. Communication and persuasion, 1-24.

Petty, R., & Cacioppo, J. (2012). Communication and persuasion: Central and peripheral routes to attitude change. Springer Science & Business

Media.

Rauti, S., & Leppänen, V. (2017). "You have a potential hacker's infection": a study on technical support scams. IEEE International Conference on Computer and Information Technology, (pp. 197-203).

Ross, M., Grossmann, I., & Schryer, E. (2014). Contrary to psychological opinion, there is no compelling evidence that older adults are disproportionately victimized by consumer fraud. Perspectives on psychological science, 9(4), 427-442.

Rusch, J. (1999). The "social engineering" of internet fraud. Internet Society Annual Conference. Consulté à l'adresse http://www. isoc. org/isoc/conferences/inet/99/proceedings/3g/3g/3g_2. htm.

Sheng, S., Holbrook, M., Kumaragur, P., Cranor, L., & Downs, J. (2010). Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. Privacy Behaviors, 373-382.

Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L., Hong, J., & Nunge, E. (2007). Anti-Phishing Phil: The Design and Evaluation of a Game that teaches people not to fall for phish. Proceedings of the 3rd symposium on Usable privacy and security (pp. 88-99). ACM.

Singh, L., & Imphal, N. (2018). A survey on phishing and anti-phishing techniques. International Journal of Computer Science Trends and Technology, 6(2), 62-68.

Stajano, F., & Wilson, P. (2011). Understanding scam victims: seven principles for systems security. Communications of the ACM, 54(3), 70-75.

Tabron, J. (2016). Linguistic features of phone scams: a qualitative survey. 11th Annual symposium on information assurance, (pp. 52-58).

Titus, R., & Gover, A. (2001). Personal Fraud: The Victims and the Scams. In F. G., & K. Pease, Repeat Victimization (pp. 133-152). New York: Criminal Justice Press.

van de Weijer, S., Leukfeldt, R., & Bernasco, W. (2018). Determinants of reporting cybercrime: a comparison between identity theft, consumer fraud, and hacking. European Journal of Criminology, 1-23.

Whitty, M. (2013). The scammers persuasive techniques model: Development of a stage model to explain the online dating romance scam. British Journal of Criminology, 53(4), 665-684.

Whitty, M. (2015). Anatomy of the online dating romance scam. Security Journal, 28(4), 443-455.

Whitty, M. (2018). Do you love me? Psychological characteristics of romance scam victims. Cyberpsychology, behavior, and social networking, 21(2), 105-109.

Wood, S., Liu, P., Hanoch, Y., Xi, P., & Klapatch, L. (2018). Call to claim your prize: perceived benefits and risk drive intention to comply in a mass marketing scam. Journal of Experimental Psychology: applied, 24(2), 196-206.

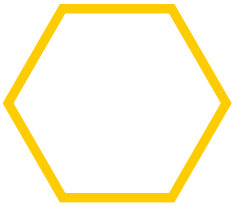
Wood, S., Liu, P., Hanoch, Y., Xi, P., & Klapatch, L. (2018). Call to claim your prize: perceived benefits and risk drive intention to comply in a mass masketing scam. Journal of Experimental Psychology: Aplied, 24(2), 196-206.

Workman, M. (2008). Wisecrackers: a theory-grounded investigation of phishing and pretext social engineering threats to information security. Journal of the american society for information science and technology, 59(4), 1-12.

Yeboah-Boateng, E., & Amanor, P. (2014). Phishing, SMishing & Vishing: an assessment of threats against mobile devices. Journal of Emerging Trends in Computing and Information Sciences, 5(4), 297-307.

CONTACT DETAILS

EUCPN Secretariat
Phone: +32 2 557 33 30
Email: eucpn@ibz.eu
Website: www.eucpn.org



TWITTER.COM/EUCPN
FACEBOOK.COM/EUCPN
LINKEDIN.COM/COMPANY/EUCPN