وزارة المالية
MINISTERE DES FINANCES

CTRF CELLULE DE TRAITEMENT DU RENSEIGNEMENT FINANCIER خلية معالجة الإستعلام المالي خ م إ

LETTRE D'INFORMATION : BON A SAVOIR (N°30)

Fraude informatique

La fraude informatique est la variante informatique de l'escroquerie au sens classique du terme. L'escroquerie consiste à soutirer, au moyen de belles paroles et de propositions, des biens ou des fonds à des personnes qui ne se doutent de rien. Quand quelqu'un utilise à cette fin des moyens de communication modernes, le législateur considère qu'il s'agit également d'escroquerie. Internet permet, dans un délai rapide et à moindres frais, de toucher un grand nombre de victimes.

Pratiques connues

1. Transactions financières

Il vous est peut-être arrivé de recevoir un e-mail vous proposant de grosses sommes d'argent à changer ou à blanchir. L'arnaque consiste à vous faire croire qu'il est possible d'encaisser d'importants bénéfices excédentaires d'une instance soi-disant officielle. Cet e-mail sollicite votre aide : on vous demande de verser de l'argent ou transmettre des documents d'entreprise. En échange, on vous promet une participation aux bénéfices de l'ordre de 20 % ou plus.

Il existe, dans cette catégorie, un autre type de criminalité : le "phishing". Par ce procédé, des criminels reproduisent des sites d'entreprises ou d'organisations connues pour voler des données personnelles, des mots de passe et des sommes d'argent.

2. Loteries ou jeux de hasard

Vous recevez par e-mail un avis vous indiquant que vous avez gagné le gros lot à une loterie ou à un jeu de hasard. Pour recevoir votre prix, vous devez d'abord verser une somme d'argent.

Les loteries officielles ne fonctionnent pas de cette manière : vous ne pouvez recevoir un prix qu'après avoir acheté un billet de loterie, un billet à gratter ou un bulletin de loto. La loterie ne prend jamais contact avec le gagnant : ce dernier doit en prendre l'initiative.

Parier n'est pas punissable. En revanche, exploiter des jeux de hasard sans une autorisation de la Commission des jeux de hasard l'est effectivement. Selon la loi sur les jeux de hasard, il est interdit en Belgique d'exploiter des jeux de hasard ou des établissements de jeux de hasard, sous quelque forme, dans quelque lieu et de quelque manière que ce soit. Seul un nombre d'établissements défini par le législateur peuvent organiser des jeux de hasard. Cela signifie donc que les casinos et les jeux d'argent en ligne sont toujours illégaux en Belgique.

3. Héritages

Vous recevez par courriel un avis d'un soi-disant organe officiel étranger ou d'un soi-disant "notaire" étranger. Ce message précise qu'après de longues recherches, on a pu vous identifier comme étant le (seul) héritier d'une personne très riche récemment décédée. Mais attention : pour pouvoir recueillir l'héritage, vous devez d'abord verser une somme d'argent, destinée soi-disant à régler tous les frais administratifs. Vous comprenez dès lors qu'il ne s'agit pas ici d'un vrai notaire, mais bien d'escrocs qui en veulent à votre argent.

4. Investissements exotiques
Vous recevez par e-mail des propositions (malveillantes) d'investissements dans des projets exotiques, avec promesses de gains astronomiques à la clé. Bien entendu, il s'agit ici encore de fraude.
5. Passeports, visas, documents, …
Les escrocs tentent aussi de jouer sur vos sentiments. Dans certains e-mails par exemple, on vous demande de verser de l'argent pour quelqu'un qui a besoin de toute urgence d'un passeport, d'un visa ou d'un autre document officiel. Pour vous apitoyer, l'e-mail décrit avec force détails les conditions de vie déplorables d'un pays situé à l'autre bout du monde. L'argent que vous devriez verser servirait à payer l'intermédiaire chargé de délivrer le document. Il va de soi que vous ne verrez jamais cette personne et que vous aurez tout simplement perdu votre argent …
6. Achats sur Internet
On peut acheter à peu près tout sur Internet. Mais tous les vendeurs ne sont pas fiables. Certains, surtout à l'étranger, ne livrent pas les biens achetés et payés.
7. Ventes sur Internet
Vous placez une annonce sur Internet dans le but de vendre quelque chose. Une personne ou une entreprise accepte l'offre sans même discuter le prix demandé. L'escroc peut alors procéder de différentes manières : il vous donne un chèque sans provision, vous demande de verser une garantie sur un compte à l'étranger …
http://www.belgium.be/fr/justice/securite/criminalite/criminalite_informatique/fraude_informatique

Criminalité informatique

Les ordinateurs font partie intégrante de la vie des citoyens et des entreprises. Internet est devenu l'un des moyens les plus importants d'information et de communication.
Le revers de l'impact grandissant de l'informatique est que la criminalité informatique devient à la fois de plus en plus rentable et peut causer toujours plus de dégâts. Un virus informatique relativement simple peut rapidement entraîner une perte économique de plusieurs millions d'euros.
Cette évolution s'explique, en grande partie, par les caractéristiques d'Internet :

- Le réseau Internet est immatériel : les actions ne sont pas vraiment tangibles mais occasionnent de réels préjudices ou dégâts.
- Il est mondial : les frontières disparaissent.
- Tout se produit en temps réel : les résultats se font sentir instantanément.
- La loi décrit quatre nouveaux délits relatifs à la criminalité informatique :
- le faux en informatique
- la fraude informatique
- la manipulation de données
- le "hacking"

Lorsque vous avez affaire à ce type de criminalité informatique, déclarez-le le plus rapidement à la police. Vous pouvez porter plainte auprès de la police locale mais aussi en ligne via Police on Web.
http://www.belgium.be/fr/justice/securite/criminalite/criminalite_informatique

Faux en informatique

Constituer un faux en informatique consiste à modifier ou à effacer des données d'un système informatique ou à modifier l'utilisation de ces données, de manière à entraîner également la modification de leur portée juridique.
Cette notion a été introduite pour mettre fin aux problèmes que suscitait la notion de "faux en écriture" appliquée aux données informatiques. Des exemples de faux en informatique sont la falsification de cartes de crédit, de moyens de paiement numériques, de signatures électroniques.
http://www.belgium.be/fr/justice/securite/criminalite/criminalite_informatique/faux_en_informatique

Escroquerie sur Internet

Lors d'une escroquerie sur internet, l'imposteur change délibérément des données électroniques pour soutirer de l'argent. L'escroquerie sur internet ressemble très fort à la fraude sur internet mais dans ce dernier cas, l'imposteur ne manipule pas des données mais bien des personnes.
Quelques exemples d'escroquerie sur internet :

- l'utilisation d'une carte de crédit volée pour retirer de l'argent à un distributeur automatique
- le dépassement illicite du crédit octroyé par une carte de crédit
- l'installation ou la modification de programmes dans le système d'autrui afin d'obtenir régulièrement des paiements par l'intermédiaire de ces programmes

http://www.belgium.be/fr/justice/securite/criminalite/criminalite_informatique/escroquerie_sur_internet

Sabotage informatique

Le sabotage informatique peut se définir comme du vandalisme informatique. On peut par exemple parler de sabotage informatique lorsque quelqu'un met délibérément un virus en circulation mais aussi lorsque quelqu'un détruit les données clients d'un concurrent même sans en tirer d'avantage financier.
A la différence de la fraude informatique, le sabotage informatique n'a pas nécessairement pour but l'enrichissement. Modifier des données sans autorisation constitue déjà, en soi, un délit. La conception et la diffusion d'outils de sabotage de données sont également punissables. Le législateur vise ainsi principalement les concepteurs de virus qui développent ou diffusent des programmes préjudiciables.

"Hoax"

"Hoax" est l'équivalent anglais de canular. Dans le contexte informatique, il désigne une information fausse ou invérifiable propagée sur Internet par e-mail. Il peut, par exemple, s'agir d'une fausse alerte au virus, de lettres en chaînes ou de messages vous annonçant que vous avez gagné le gros lot ...

Le principe est très simple : quelqu'un envoie un "hoax" à quelques personnes. Celles-ci transmettent ce message à leurs contacts, qui à leur tour le transmettent, etc. Le message se propage ainsi toujours plus loin. Les "hoaxes" envoyés massivement peuvent considérablement surcharger le réseau Internet. De plus, ils semblent avoir la vie dure : ils peuvent faire plusieurs fois le tour du monde, disparaître et après quelques années, soudainement resurgir.
Pour plus d'information sur les "hoaxes", consultez le site de la police fédérale.

Virus

Il est interdit en Belgique de détruire ou d'endommager intentionnellement des programmes informatiques et des données informatiques en propageant des virus, même quand il n'y a pas de dommages permanents.
Il est d'ailleurs possible de propager un virus sans s'en apercevoir.

Harcèlement obsessionnel

Un harceleur est quelqu'un qui, de manière systématique, importune une autre personne, en général en raison d'une admiration obsessionnelle ou par vengeance. Les harceleurs qui se servent d'un ordinateur peuvent, par exemple, envoyer des e-mails menaçants ou envahir la boîte de messagerie de leur victime par une surabondance de messages. Il s'agit souvent de messages au contenu indésirable comme des photos pornographiques, des virus ou des chevaux de Troie. Parfois la victime est constamment importunée par des personnes qui réagissent à une fausse annonce.
http://www.belgium.be/fr/justice/securite/criminalite/criminalite_informatique/sabotage_informatique

Spamming

Le spamming consiste en l'envoi massif d'un e-mail vers des destinataires qui ne l'ont pas demandé. Il s'agit le plus souvent de messages commerciaux à caractère érotique. Les spammeurs envoient des messages simultanément à des milliers, voire des millions de destinataires. Le spamming est interdit.
Les serveurs mail de la plupart des Internet Service Providers (ISP) refusent tous les e-mails qui proviennent d'adresses incorrectes. De nombreux spammeurs utilisent différentes adresses, essayant ainsi de cacher leur véritable lieu d'envoi. Certains ISP proposent à leurs utilisateurs un filtre anti-spam. Ce filtre contrôle la présence de spams dans tous les e-mails entrants.
http://www.belgium.be/fr/justice/securite/criminalite/criminalite_informatique/spamming

"hacking"

Hacking est une notion très vague. Même les informaticiens ne tombent pas d'accord sur la signification exacte du mot. Hacking consiste à pénétrer illégalement dans un système informatique. Cette "effraction" implique généralement une intention frauduleuse. Mais établir involontairement une connexion et la maintenir volontairement est également considéré comme du piratage. Même pirater un système informatique qui n'est pas ou à peine sécurisé est punissable.
Dans l'évaluation de hacking, la loi distingue les 'insiders' des 'outsiders'. Les insiders sont des personnes qui ont une autorisation d'accès, mais qui outrepassent cette autorisation. Ces personnes ne sont punissables que si leur piratage cache une intention de nuire ou une

intention frauduleuse. Pour les ‘outsiders’, cette restriction n'existe pas : ils sont dans tous les cas passibles de sanctions, même s'ils s’introduisent dans un système avec "de bonnes intentions".
Il est interdit de collecter ou d'offrir - contre rétribution ou non - des données permettant des violations informatiques. Cette interdiction vise surtout à juguler le commerce de codes d'accès et de 'hacking tools'.
Les pirates informatiques utilisent parfois un grand nombre "d'ordinateurs zombies". Il s'agit d'ordinateurs individuels ou de sociétés mal protégés et infectés par un "cheval de Troie". Le cheval de Troie est un programme qui permet à un malfaiteur de prendre le contrôle d'un ordinateur relié à Internet et de l’utiliser. Votre ordinateur peut lui aussi être intégré dans un tel réseau. Le pirate a ainsi le contrôle total sur votre ordinateur et a accès à vos données.
Protégez votre ordinateur contre le piratage, car une fois que quelqu'un y a accès, tout est possible : le pirate peut non seulement fureter à sa guise mais également utiliser votre ordinateur à des fins illégales ou détruire vos fichiers.
http://www.belgium.be/fr/justice/securite/criminalite/criminalite_informatique/hacking

Focus sur la lutte contre la fraude documentaire liée au blanchiment d'argent

Les avancées spectaculaires en matière de technologie informatique et de communication offre une large gamme de possibilités, avantages, inconvénients et risques. Des réseaux d’ordinateurs et de télécommunications (Internet) augmentent l’efficacité des services et améliorent la vie quotidienne. L’utilisation de ces technologies comporte également de nouveaux dangers, non seulement pour notre vie privée et nos libertés, mais également lors de nos transactions financières.
Afin de répondre de manière appropriée à la lutte contre la fraude documentaire, qui va souvent de pair avec des infractions pénales plus graves, ce qui affecte encore plus notre société, les acteurs financiers (banques, compagnies d’assurances et de cartes de crédit,… mais également d‘autres acteurs du circuit économique comme les sociétés commerciales,…) doivent se munir de moyens de détection et de contrôle sophistiqués et adéquats. Acquérir une attitude critique et disposer de connaissances actualisées sur la fraude (documentaire) par leurs membres du personnel sont d’autres facteurs-clé. Via une approche professionnelle de scepticisme, nous devons être capables de reconnaître et de détecter les indicateurs et les typologies de tentatives de contrefaçon et de falsification.
Les pratiques et le mode opératoire des contrefacteurs ont évolués avec l’actuel progrès technique exponentiel, ce qui gêne énormément la détection et la prévention. A titre d’exemple, le “spear phishing”, où les escrocs contactent des administrateurs de sociétés par mail ciblé grâce aux informations récoltées sur Internet et les réseaux sociaux (social engineering).
La fraude documentaire (passeports ou factures falsifié(e)s) vise souvent à soutenir d’autres crimes (escroqueries, blanchiment, financement du terrorisme, …). Il est essentiel que les acteurs des services financiers soient bien informés sur ses différents aspects et typologies.
Primordial est de savoir quels sont les outils de lutte contre ces délits (fraude) afin de réagir de la manière la plus propice.
Lors du blanchiment de capitaux, le but final est de dissimuler l’origine de l’argent criminel.
Une des techniques pratiquées est la fraude documentaire afin de cacher le lien entre le délit sous-jacent et l’auteur. Dans ce sens, la fraude documentaire peut être considérée comme une des typologies afin de détecter le blanchiment.

Par ailleurs, il est capital d'acquérir des connaissances sur les documents qui sont susceptibles d'être falsifiés. Les questions suivantes doivent être posées: qui, quand, comment? Une fois que des faux documents ont été détectés; quelle procédure doit être suivie?
L'objectif de cette formation est d'apprendre comment adopter une attitude professionnelle de scepticisme, ce qui inclut entre autres: accepter que la fraude (documentaire) puisse exister, développer un esprit critique et faire une évaluation pertinente en cas de preuves potentielles. Suivre une telle formation est donc fondamentale si vous voulez pouvoir déceler une fraude et disposer d'une vigilance professionnelle.
https://www.febelfin-academy.be/fr/actu/detail/focus-sur-la-lutte-contre-la-fraude-documentaire-liee-au-blanchiment-d-argent

Sécurité bancaire : Les principales fraudes et arnaques des moyens de paiement

Carte bancaire, prélèvement, chèques, paiements en ligne, etc., tous ces supports de paiement vous exposent à la convoitise de nombreux escrocs.
Ces derniers développent tous les moyens (vol, arnaque, falsification, etc.) pour vous subtiliser un maximum de vos disponibilités financières.
Parfois il ne s'agit pas de vous voler vos supports de paiement mais de se procurer vos coordonnées bancaires voire simplement votre nom, prénom et adresse.

Une menace au quotidien

Les fraudes relatives aux moyens de paiement sont en constante progression. En 2012, les fraudes concernant les attaques de distributeur automatique de billets ont progressé de 73% et les fraudes sur les points de vente ont augmentés de 250%.
En France, 61% des opérations frauduleuses sont sur internet alors que les transactions sur internet ne représentent que 9,2% des transactions.
Il existe une multitude de moyens de subtiliser vos outils de paiement voire votre bien. Il est donc important de les connaitre pour éviter de se les faire subtiliser.

Vol de carte bancaire

Le saint Graal de tout fraudeur qui use des techniques les plus farfelues et les plus poussées pour se procurer toutes les informations relatives à votre carte bancaire

Piéger le distributeur automatique de paiement :

Le fraudeur installe un faux clavier sur le clavier du distributeur automatique de billet ou installe une fausse caméra de surveillance. Il récupère ainsi votre code secret que vous aurez tapé. Il lui suffit plus qu'à vous subtiliser votre carte bancaire. Souvent par la manière forte.
Certains vont encore plus loin en captant les informations directement sur votre carte bancaire en piégeant à la fois le clavier mais également le support de réception de votre carte bancaire du distributeur automatique de paiement ainsi il scanne votre carte bancaire à distance sans avoir besoin de vous voler votre carte bancaire.

L'œil qui louche

Lors de vos paiements chez des commerçants, dans une entreprise de restauration rapide par exemple, vous devez effectuer votre code secret en public. C'est à ce moment précis que l'œil « attentif » d'un fraudeur tente d'observer discrètement votre code. Il lui suffira par la suite de subtiliser votre carte.

Détournement du terminal de paiement chez le commerçant.

Certains fraudeurs poussent l'art du vol directement sur le lieu de vente. Cela fut le cas dans le sud de la France et plus particulièrement à Béziers où des terminaux de paiement chez des commerçants ont été discrètement échangés par des terminaux piégés.

Les fraudeurs récupéraient à distance toutes les informations relatives à votre carte bancaire y compris le code secret.
C'est près d'une dizaine de millions d'euros qui ont été détournés ainsi.

Complicité du commerçant

Certains fraudeurs arrivent à convaincre des commerçants de participer à leurs arnaques. Après avoir subtilisées les coordonnées d'une carte bancaire, les fraudeurs se rendent chez le commerçant-collaborateur pour effectuer des paiements nécessitant qu'une simple signature.

Détournement du courrier postal

Souvent les banques, particulièrement les banques en ligne, envoient votre carte bancaire par courrier postal. Il n'en suffit pas plus pour un fraudeur pour récupérer sans trop d'effort votre carte bancaire. Pour se faire, il intègrera les services postaux pour récupérer votre courrier ou bien il disposera d'un moyen pour accéder à votre courrier dans votre boite aux lettres.
Les distributeurs de courriers, de magazines et autres annuaires disposent d'une clé ouvrant le panneau des boites aux lettres. Une personne mal intentionnée peut ainsi accéder à votre courrier et parfois il aura la surprise d'y trouver vos clés de domicile qui lui permettront de rechercher tranquillement chez vous tous vos moyens de paiement sans que vous vous en rendiez compte.

Vol de chèque

Les chèques bancaires sont également un moyen de paiement que cherche à se procurer le fraudeur. En effet, votre chéquier présente votre nom, prénom et vos coordonnées. Il suffit alors de fabriquer une fausse carte d'identité reprenant ces informations pour ensuite l'utiliser à volonté.

Vol de votre chéquier

Le principal canal d'action pour récupérer votre chéquier reste bien entendu le vol. Le fraudeur tentera de récupérer celui-ci dans votre bagage (sac à main, sacoche d'ordinateur), dans votre vêtement (veste, manteau) ou dans votre véhicule de transport.
Mais certains fraudeurs n'ont pas froid aux yeux et peuvent aller jusqu'à la source pour récupérer votre chéquier. En témoigne l'exemple de ce fraudeur qui subtilisa à un client de la BNP Paribas du 13ème arrondissement de Paris, son courrier de convocation pour la récupération de son chéquier. Le voleur s'est présenté à l'agence avec une carte d'identité présentant toutes les coordonnées du client mais avec une photo différente. Il a fallu toute la vigilance de la conseillère d'agence qui connaissait particulièrement bien son client pour éviter que ce dernier devienne la victime d'une fraude bancaire.

Faux chèque bancaire

Certains fraudeurs sortent tout droit du film « Attrape moi si tu peux » et sont capables de recréer des chéquiers à l'image d'une banque.
L'arnaque au faux chèque repose sur trois acteurs, l'expéditeur du chèque, le destinataire du chèque et la banque.
Dans le cadre d'une transaction, l'expéditeur (ou acheteur) fait parvenir un chèque avec une somme supérieure au montant de la transaction négociée. Il prétexte une erreur et demande à ce que le destinataire (le vendeur) lui retourne la différence moins les frais liés au dérangement dès que celui-ci aura déposé le dit chèque.
Une fois déposé, la banque du vendeur crédite la somme sur son compte. Rassuré le vendeur accepte alors de renvoyer l'excédent à son acheteur.
Ce dernier demande alors de passer exclusivement par des organismes tels que Western Union afin de récupérer au plus vite la différence.
Et ce n'est que quelques jours plus tard que votre banque vous informe que le chèque est faux.

Faux chèque de banque

Lors d'une transaction vous demandez un chèque de banque qui est pour vous une garantie. Une fois la transaction réalisée, vous déposez votre chèque de banque dans votre banque et découvrez que celui-ci est faux.

Vol des informations bancaires

Le vol de vos données est la principale activité des fraudeurs. Les fraudeurs s'ingénient à développer toutes les techniques possibles pour les récupérer.

En voici quelques unes :

Piratage informatique de votre ordinateur

Le classique du classique : Vous téléchargez un fichier qui contient un virus ou un cheval de Troie qui infecte votre ordinateur de manière soit à prendre le contrôle de celui-ci pour y récupérer des informations bancaires ; soit à vous observer en espérant que vous effectuerez un paiement en ligne afin d'enregistrer le plus simplement du monde les informations de la carte bancaire que vous taperez sur votre clavier.

Piratage d'un commerçant : Le commerçant se fait pirater son serveur. Et vos coordonnées bancaires se retrouvent entre les mains du pirate.

Email frauduleux

Vous recevez un email vous invitant à mettre à jour vos informations chez un de vos fournisseurs (EDF, Opérateurs téléphoniques, Banque, etc.) voire même des services des impôts.

Vous vous retrouvez sur une page quasi similaire à celle de votre fournisseur ou service des impôts dans lequel vous êtes invité à remplir vos coordonnées et vos informations bancaires.

Toutes ces informations sont récupérées en règle générale à l'étranger par un pirate informatique qui les utilise immédiatement pour réaliser des achats voire des virements bancaires.

Récupération via Wifi, NFC

Le développement des technologies permettant l'accès à distance favorisent la tentation des fraudeurs d'accéder à vos données.

Vos appareils de communication sont vulnérables à des attaques de pirates extrêmement bien équipés pour tenter de récupérer vos données lorsque vos appareils sont branchés en mode Wifi ou NFC.

Le développement du paiement mobile NFC qui permet de réaliser un paiement avec sa carte de paiement ou son téléphone portable équipée sans avoir à taper son code est une véritable aubaine pour les fraudeurs. Ces derniers n'ont plus besoin de vous subtiliser votre code secret ou de vous voler votre carte bancaire. Il leur suffit de développer les bons outils pour tenter de récupérer les informations de votre carte bancaire ou de votre mobile, puis de les dupliquer sur un support.

Arnaque sur Paypal

Paypal est un moyen de paiement prisé par toutes celles et tous ceux qui ne souhaitent pas communiquer leurs informations bancaires sur des sites de vente.

Le compte paypal étant limité par un montant défini, il est impossible pour un fraudeur ayant accès à ce compte de se servir sans limite.

Toutefois, les arnaques utilisant le service de paiement paypal sont nombreuses. Principalement sur les sites de vente de particulier à particulier.

Sur ces sites, l'escroc se porte rapidement acquéreur d'un objet en vente. Il propose l'envoi de la somme via paypal. Le vendeur reçoit une confirmation du transfert par email. Cet email peut être à la fois un vrai courrier provenant de paypal ou un faux courrier provenant de l'escroc.

Rassuré, le vendeur envoie alors l'objet à une adresse souvent un point relais ou à l'étranger.

Après l'envoi, le vendeur se rend compte que son compte paypal n'est pas réellement crédité. Ou bien il reçoit un vrai courrier de Paypal quelques jours plus tard lui indiquant que le transfert est bloqué car basé sur 'un moyen de paiement douteux.
Entretemps, le fraudeur disposera de votre bien qu'il pourra revendre ou utiliser à loisir.
Comme nous avons pu le voir les techniques de détournement de vos disponibilités financières sont très nombreuses.
Prendre connaissance de ces techniques d'escroquerie via les moyens de paiement est indispensable pour pouvoir les éviter.
http://www.challenges.fr/services/choisir-ma-banque/20140326.CHA1982/securite-bancaire-les-principales-fraudes-et-arnaques-des-moyens-de-paiement.html

Fraude informatique

La fraude informatique est la variante informatique de l'escroquerie au sens classique du terme. L'escroquerie consiste à soutirer, au moyen de belles paroles et de propositions, des biens ou des fonds à des personnes qui ne se doutent de rien. Quand quelqu'un utilise à cette fin des moyens de communication modernes, le législateur considère qu'il s'agit également d'escroquerie. Internet permet, dans un délai rapide et à moindres frais, de toucher un grand nombre de victimes.

Pratiques connues

1. Transactions financières

Il vous est peut-être arrivé de recevoir un e-mail vous proposant de grosses sommes d'argent à changer ou à blanchir. L'arnaque consiste à vous faire croire qu'il est possible d'encaisser d'importants bénéfices excédentaires d'une instance soi-disant officielle. Cet e-mail sollicite votre aide : on vous demande de verser de l'argent ou transmettre des documents d'entreprise. En échange, on vous promet une participation aux bénéfices de l'ordre de 20 % ou plus.
Il existe, dans cette catégorie, un autre type de criminalité : le "phishing". Par ce procédé, des criminels reproduisent des sites d'entreprises ou d'organisations connues pour voler des données personnelles, des mots de passe et des sommes d'argent.

2. Loteries ou jeux de hasard

Vous recevez par e-mail un avis vous indiquant que vous avez gagné le gros lot à une loterie ou à un jeu de hasard. Pour recevoir votre prix, vous devez d'abord verser une somme d'argent.
Les loteries officielles ne fonctionnent pas de cette manière : vous ne pouvez recevoir un prix qu'après avoir acheté un billet de loterie, un billet à gratter ou un bulletin de loto. La loterie ne prend jamais contact avec le gagnant : ce dernier doit en prendre l'initiative.
Parier n'est pas punissable. En revanche, exploiter des jeux de hasard sans une autorisation de la Commission des jeux de hasard l'est effectivement. Selon la loi sur les jeux de hasard, il est interdit en Belgique d'exploiter des jeux de hasard ou des établissements de jeux de hasard, sous quelque forme, dans quelque lieu et de quelque manière que ce soit. Seul un nombre d'établissements défini par le législateur peuvent organiser des jeux de hasard. Cela signifie donc que les casinos et les jeux d'argent en ligne sont toujours illégaux en Belgique.

3. Héritages

Vous recevez par courriel un avis d'un soi-disant organe officiel étranger ou d'un soi-disant "notaire" étranger. Ce message précise qu'après de longues recherches, on a pu vous identifier comme étant le (seul) héritier d'une personne très riche récemment décédée. Mais attention : pour pouvoir recueillir l'héritage, vous devez d'abord verser une somme d'argent, destinée soi-

disant à régler tous les frais administratifs. Vous comprenez dès lors qu'il ne s'agit pas ici d'un vrai notaire, mais bien d'escrocs qui en veulent à votre argent.

4. Investissements exotiques

Vous recevez par e-mail des propositions (malveillantes) d'investissements dans des projets exotiques, avec promesses de gains astronomiques à la clé. Bien entendu, il s'agit ici encore de fraude.

5. Passeports, visas, documents, …

Les escrocs tentent aussi de jouer sur vos sentiments. Dans certains e-mails par exemple, on vous demande de verser de l'argent pour quelqu'un qui a besoin de toute urgence d'un passeport, d'un visa ou d'un autre document officiel. Pour vous apitoyer, l'e-mail décrit avec force détails les conditions de vie déplorables d'un pays situé à l'autre bout du monde. L'argent que vous devriez verser servirait à payer l'intermédiaire chargé de délivrer le document. Il va de soi que vous ne verrez jamais cette personne et que vous aurez tout simplement perdu votre argent …

6. Achats sur Internet

On peut acheter à peu près tout sur Internet. Mais tous les vendeurs ne sont pas fiables. Certains, surtout à l'étranger, ne livrent pas les biens achetés et payés.

7. Ventes sur Internet

Vous placez une annonce sur Internet dans le but de vendre quelque chose. Une personne ou une entreprise accepte l'offre sans même discuter le prix demandé. L'escroc peut alors procéder de différentes manières : il vous donne un chèque sans provision, vous demande de verser une garantie sur un compte à l'étranger …

http://www.belgium.be/fr/justice/securite/criminalite/criminalite_informatique/fraude_informatique

Criminalité informatique

Les ordinateurs font partie intégrante de la vie des citoyens et des entreprises. Internet est devenu l'un des moyens les plus importants d'information et de communication.

Le revers de l'impact grandissant de l'informatique est que la criminalité informatique devient à la fois de plus en plus rentable et peut causer toujours plus de dégâts. Un virus informatique relativement simple peut rapidement entraîner une perte économique de plusieurs millions d'euros.

Cette évolution s'explique, en grande partie, par les caractéristiques d'Internet :

- Le réseau Internet est immatériel : les actions ne sont pas vraiment tangibles mais occasionnent de réels préjudices ou dégâts.
- Il est mondial : les frontières disparaissent.
- Tout se produit en temps réel : les résultats se font sentir instantanément.
- La loi décrit quatre nouveaux délits relatifs à la criminalité informatique :
- le faux en informatique
- la fraude informatique
- la manipulation de données
- le "hacking"

Lorsque vous avez affaire à ce type de criminalité informatique, déclarez-le le plus rapidement à la police. Vous pouvez porter plainte auprès de la police locale mais aussi en ligne via Police on Web.

http://www.belgium.be/fr/justice/securite/criminalite/criminalite_informatique

Faux en informatique

Constituer un faux en informatique consiste à modifier ou à effacer des données d'un système informatique ou à modifier l'utilisation de ces données, de manière à entraîner également la modification de leur portée juridique.
Cette notion a été introduite pour mettre fin aux problèmes que suscitait la notion de "faux en écriture" appliquée aux données informatiques. Des exemples de faux en informatique sont la falsification de cartes de crédit, de moyens de paiement numériques, de signatures électroniques.
http://www.belgium.be/fr/justice/securite/criminalite/criminalite_informatique/faux_en_informatique

Escroquerie sur Internet

Lors d'une escroquerie sur internet, l'imposteur change délibérément des données électroniques pour soutirer de l'argent. L'escroquerie sur internet ressemble très fort à la fraude sur internet mais dans ce dernier cas, l'imposteur ne manipule pas des données mais bien des personnes.
Quelques exemples d'escroquerie sur internet :

- l'utilisation d'une carte de crédit volée pour retirer de l'argent à un distributeur automatique
- le dépassement illicite du crédit octroyé par une carte de crédit
- l'installation ou la modification de programmes dans le système d'autrui afin d'obtenir régulièrement des paiements par l'intermédiaire de ces programmes

http://www.belgium.be/fr/justice/securite/criminalite/criminalite_informatique/escroquerie_sur_internet

Sabotage informatique

Le sabotage informatique peut se définir comme du vandalisme informatique. On peut par exemple parler de sabotage informatique lorsque quelqu'un met délibérément un virus en circulation mais aussi lorsque quelqu'un détruit les données clients d'un concurrent même sans en tirer d'avantage financier.
A la différence de la fraude informatique, le sabotage informatique n'a pas nécessairement pour but l'enrichissement. Modifier des données sans autorisation constitue déjà, en soi, un délit. La conception et la diffusion d'outils de sabotage de données sont également punissables. Le législateur vise ainsi principalement les concepteurs de virus qui développent ou diffusent des programmes préjudiciables.
"Hoax"

"Hoax" est l'équivalent anglais de canular. Dans le contexte informatique, il désigne une information fausse ou invérifiable propagée sur Internet par e-mail. Il peut, par exemple, s'agir d'une fausse alerte au virus, de lettres en chaînes ou de messages vous annonçant que vous avez gagné le gros lot ...
Le principe est très simple : quelqu'un envoie un "hoax" à quelques personnes. Celles-ci transmettent ce message à leurs contacts, qui à leur tour le transmettent, etc. Le message se

propage ainsi toujours plus loin. Les "hoaxes" envoyés massivement peuvent considérablement surcharger le réseau Internet. De plus, ils semblent avoir la vie dure : ils peuvent faire plusieurs fois le tour du monde, disparaître et après quelques années, soudainement resurgir.
Pour plus d'information sur les "hoaxes", consultez le site de la police fédérale (link is external).

Virus

Il est interdit en Belgique de détruire ou d'endommager intentionnellement des programmes informatiques et des données informatiques en propageant des virus, même quand il n'y a pas de dommages permanents.
Il est d'ailleurs possible de propager un virus sans s'en apercevoir.

Harcèlement obsessionnel

Un harceleur est quelqu'un qui, de manière systématique, importune une autre personne, en général en raison d'une admiration obsessionnelle ou par vengeance. Les harceleurs qui se servent d'un ordinateur peuvent, par exemple, envoyer des e-mails menaçants ou envahir la boîte de messagerie de leur victime par une surabondance de messages. Il s'agit souvent de messages au contenu indésirable comme des photos pornographiques, des virus ou des chevaux de Troie. Parfois la victime est constamment importunée par des personnes qui réagissent à une fausse annonce.
http://www.belgium.be/fr/justice/securite/criminalite/criminalite_informatique/sabotage_informatique

Spamming

Le spamming consiste en l'envoi massif d'un e-mail vers des destinataires qui ne l'ont pas demandé. Il s'agit le plus souvent de messages commerciaux à caractère érotique. Les spammeurs envoient des messages simultanément à des milliers, voire des millions de destinataires. Le spamming est interdit.
Les serveurs mail de la plupart des Internet Service Providers (ISP) refusent tous les e-mails qui proviennent d'adresses incorrectes. De nombreux spammeurs utilisent différentes adresses, essayant ainsi de cacher leur véritable lieu d'envoi. Certains ISP proposent à leurs utilisateurs un filtre anti-spam. Ce filtre contrôle la présence de spams dans tous les e-mails entrants.
http://www.belgium.be/fr/justice/securite/criminalite/criminalite_informatique/spamming

"hacking"

Hacking est une notion très vague. Même les informaticiens ne tombent pas d'accord sur la signification exacte du mot. Hacking consiste à pénétrer illégalement dans un système informatique. Cette "effraction" implique généralement une intention frauduleuse. Mais établir involontairement une connexion et la maintenir volontairement est également considéré comme du piratage. Même pirater un système informatique qui n'est pas ou à peine sécurisé est punissable.
Dans l'évaluation de hacking, la loi distingue les 'insiders' des 'outsiders'. Les insiders sont des personnes qui ont une autorisation d'accès, mais qui outrepassent cette autorisation. Ces personnes ne sont punissables que si leur piratage cache une intention de nuire ou une

intention frauduleuse. Pour les ‘outsiders’, cette restriction n'existe pas : ils sont dans tous les cas passibles de sanctions, même s'ils s’introduisent dans un système avec "de bonnes intentions".
Il est interdit de collecter ou d'offrir - contre rétribution ou non - des données permettant des violations informatiques. Cette interdiction vise surtout à juguler le commerce de codes d'accès et de 'hacking tools'.
Les pirates informatiques utilisent parfois un grand nombre "d'ordinateurs zombies". Il s'agit d'ordinateurs individuels ou de sociétés mal protégés et infectés par un "cheval de Troie". Le cheval de Troie est un programme qui permet à un malfaiteur de prendre le contrôle d'un ordinateur relié à Internet et de l’utiliser. Votre ordinateur peut lui aussi être intégré dans un tel réseau. Le pirate a ainsi le contrôle total sur votre ordinateur et a accès à vos données.
Protégez votre ordinateur contre le piratage, car une fois que quelqu'un y a accès, tout est possible : le pirate peut non seulement fureter à sa guise mais également utiliser votre ordinateur à des fins illégales ou détruire vos fichiers.
http://www.belgium.be/fr/justice/securite/criminalite/criminalite_informatique/hacking

Focus sur la lutte contre la fraude documentaire liée au blanchiment d'argent

Les avancées spectaculaires en matière de technologie informatique et de communication offre une large gamme de possibilités, avantages, inconvénients et risques. Des réseaux d’ordinateurs et de télécommunications (Internet) augmentent l’efficacité des services et améliorent la vie quotidienne. L’utilisation de ces technologies comporte également de nouveaux dangers, non seulement pour notre vie privée et nos libertés, mais également lors de nos transactions financières.
Afin de répondre de manière appropriée à la lutte contre la fraude documentaire, qui va souvent de pair avec des infractions pénales plus graves, ce qui affecte encore plus notre société, les acteurs financiers (banques, compagnies d’assurances et de cartes de crédit,… mais également d‘autres acteurs du circuit économique comme les sociétés commerciales,…) doivent se munir de moyens de détection et de contrôle sophistiqués et adéquats. Acquérir une attitude critique et disposer de connaissances actualisées sur la fraude (documentaire) par leurs membres du personnel sont d’autres facteurs-clé. Via une approche professionnelle de scepticisme, nous devons être capables de reconnaître et de détecter les indicateurs et les typologies de tentatives de contrefaçon et de falsification.
Les pratiques et le mode opératoire des contrefacteurs ont évolués avec l’actuel progrès technique exponentiel, ce qui gêne énormément la détection et la prévention. A titre d’exemple, le “spear phishing”, où les escrocs contactent des administrateurs de sociétés par mail ciblé grâce aux informations récoltées sur Internet et les réseaux sociaux (social engineering).
La fraude documentaire (passeports ou factures falsifié(e)s) vise souvent à soutenir d’autres crimes (escroqueries, blanchiment, financement du terrorisme, …). Il est essentiel que les acteurs des services financiers soient bien informés sur ses différents aspects et typologies.
Primordial est de savoir quels sont les outils de lutte contre ces délits (fraude) afin de réagir de la manière la plus propice.
Lors du blanchiment de capitaux, le but final est de dissimuler l’origine de l’argent criminel. Une des techniques pratiquées est la fraude documentaire afin de cacher le lien entre le délit sous-jacent et l’auteur. Dans ce sens, la fraude documentaire peut être considérée comme une des typologies afin de détecter le blanchiment.

Par ailleurs, il est capital d'acquérir des connaissances sur les documents qui sont susceptibles d'être falsifiés. Les questions suivantes doivent être posées: qui, quand, comment? Une fois que des faux documents ont été détectés; quelle procédure doit être suivie?
L'objectif de cette formation est d'apprendre comment adopter une attitude professionnelle de scepticisme, ce qui inclut entre autres: accepter que la fraude (documentaire) puisse exister, développer un esprit critique et faire une évaluation pertinente en cas de preuves potentielles. Suivre une telle formation est donc fondamentale si vous voulez pouvoir déceler une fraude et disposer d'une vigilance professionnelle.
https://www.febelfin-academy.be/fr/actu/detail/focus-sur-la-lutte-contre-la-fraude-documentaire-liee-au-blanchiment-d-argent