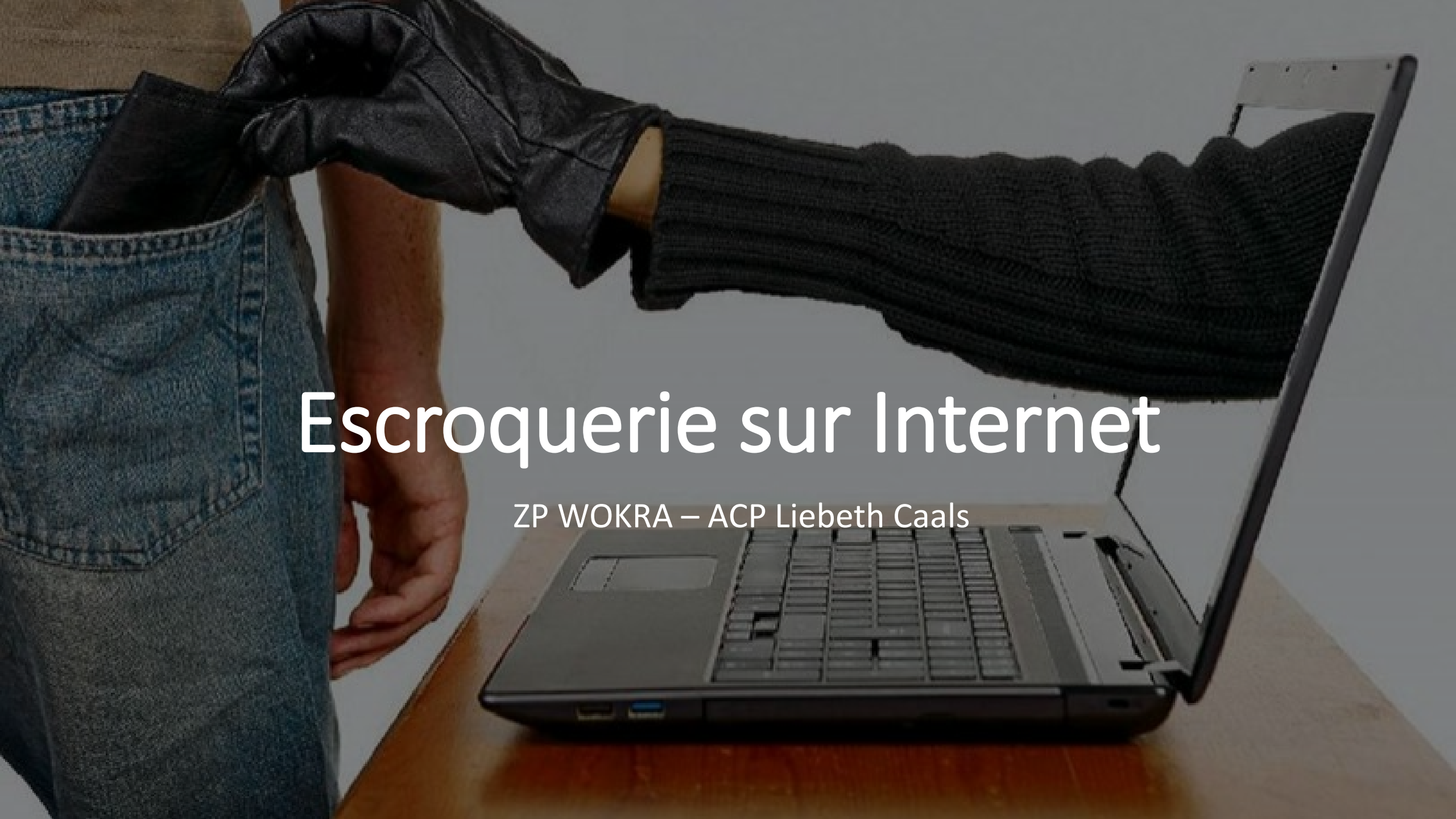


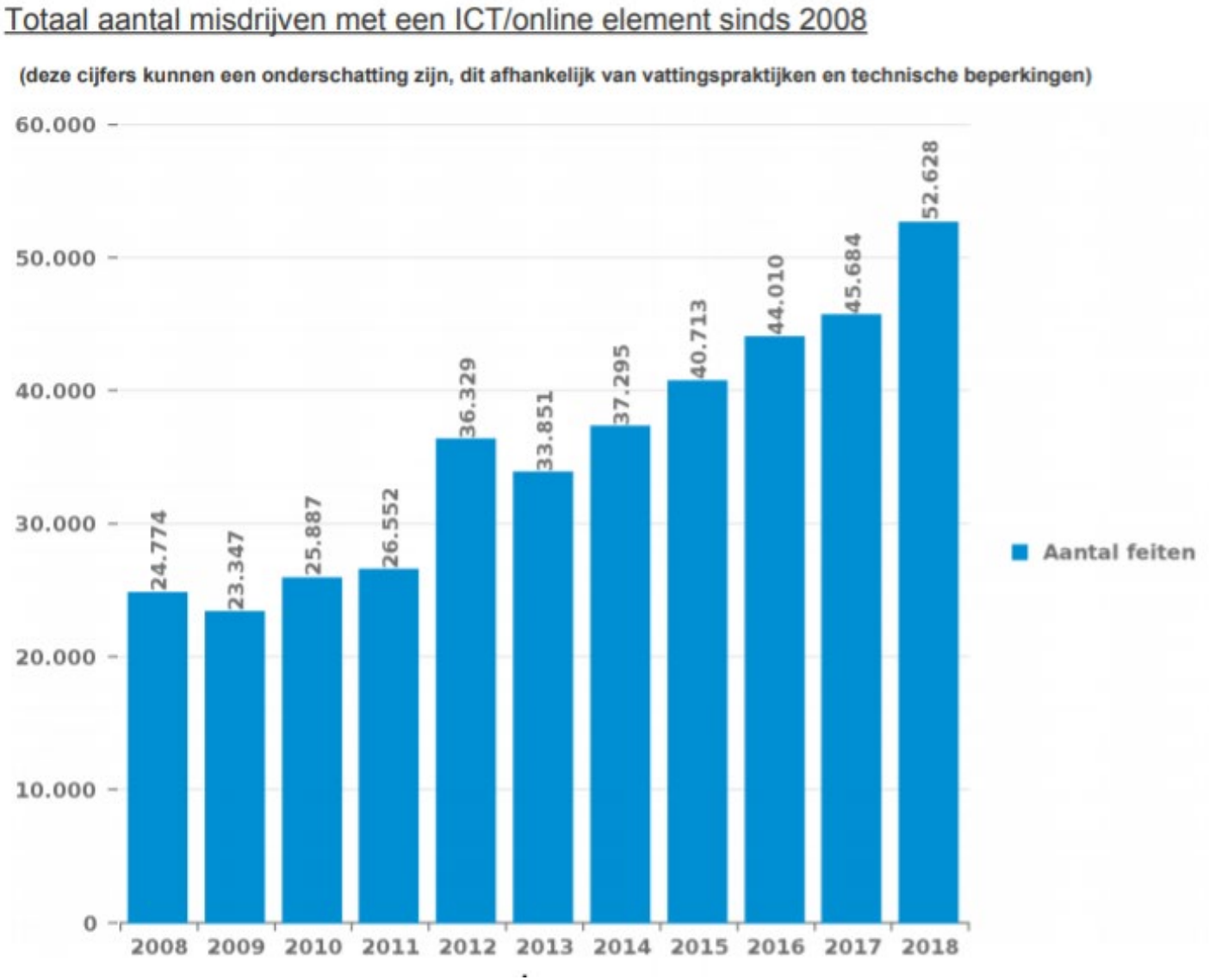
Escroquerie sur Internet

ZP WOKRA – ACP Liebeth Caals

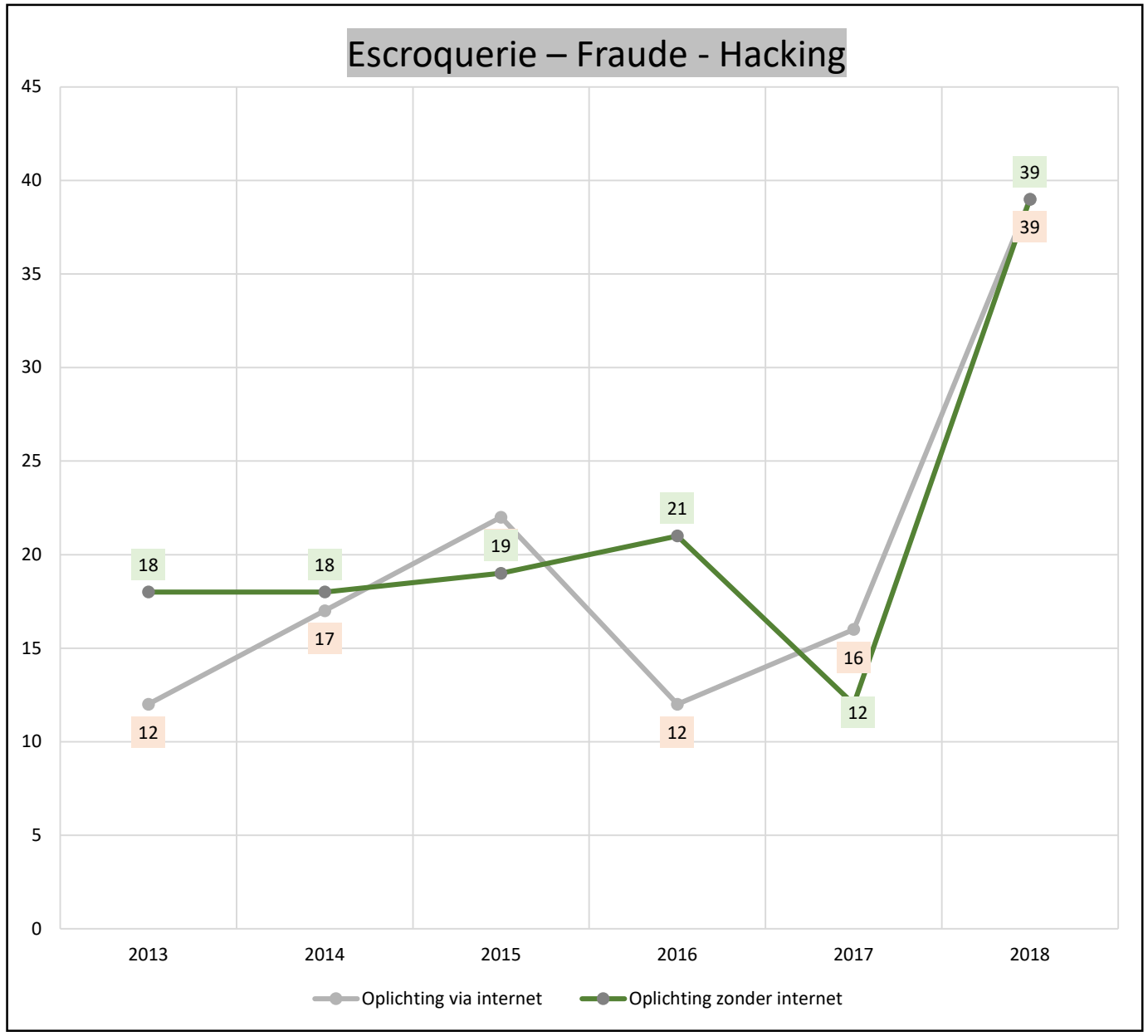
Sommaire

Quelques chiffres

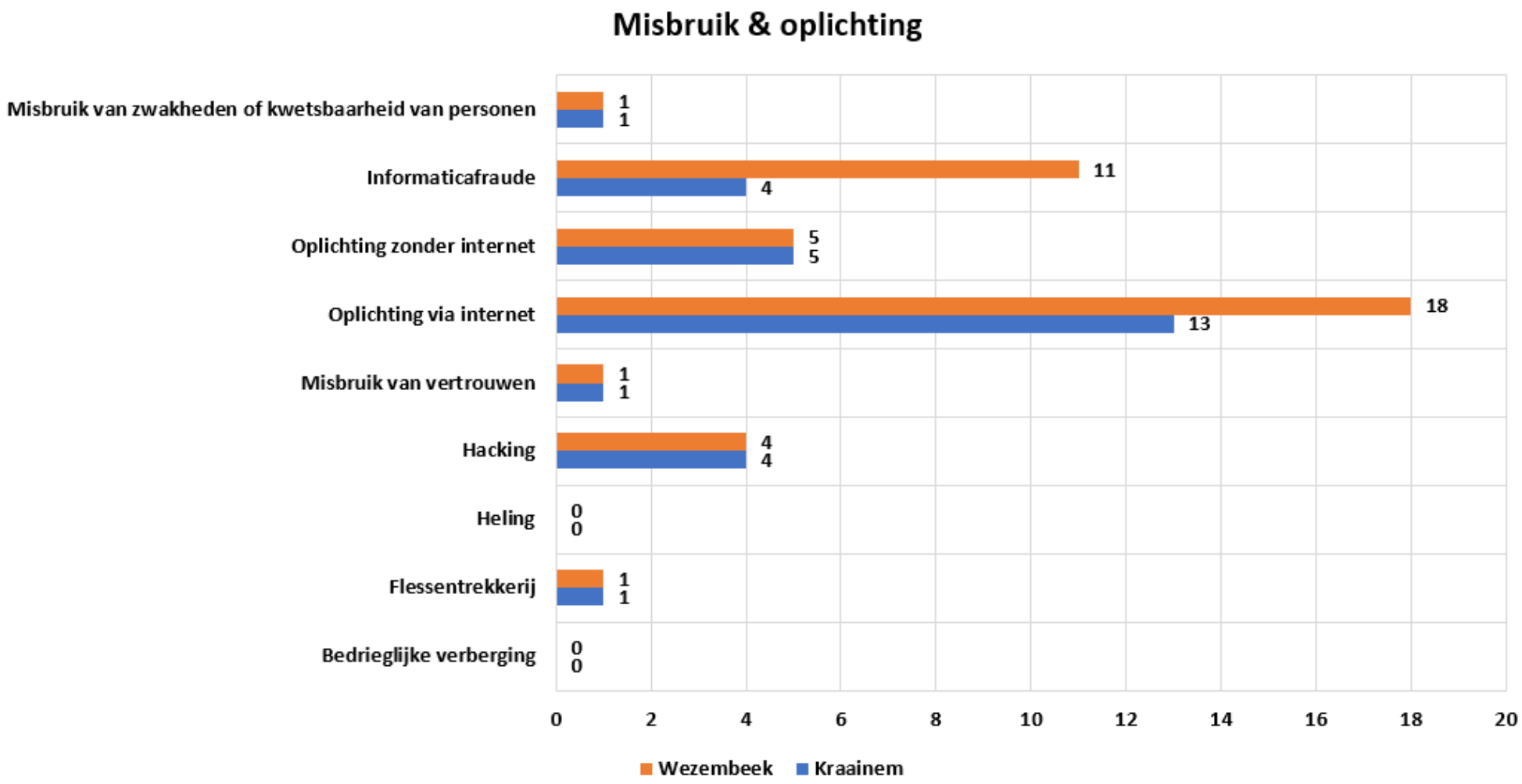
Belgique



Evolution au sein de la zone de police Wokra 2017 - 2018



Chiffres de janvier à septembre 2019



Chiffre noir

- 8% de la population affirme avoir été au moins 1 fois victime en 2018.
- Seulement 20% de ces victimes ont déposé plainte auprès de la police. Le chiffre noir s'élèverait donc à 80%.
- Selon ces statistiques, environ 200 000 faits liés à la criminalité informatique n'auraient pas été dénoncés durant la période 2017-2018.

Causes

- Evolution vers une “cybersociété”
  - Internet est de plus en plus présent dans nos vies :
    - E-mail
    - E-Banking/E-Commerce
    - Médias sociaux
    - Clouds
    - …
  - Internet est de plus en plus accessible :
    - Smartphones
    - Tablets

Causes (2)

- Avantages pour les fraudeurs :
  - Pas de déplacement.
  - Nombreuses victimes potentielles.
  - Temps pour élaborer une tactique.
  - Pas de grands moyens financiers nécessaires.
  - Traces facilement et rapidement effaçables.

Différentes formes d’escroqueries via internet

- Phishing
- Escroqueries à l’achat/vente
- Arnaques aux cryptomonnaies
- Ransomware
- Arnaques faisant appel à l’émotion
  - Arnaque par lien d’amitié
  - Email SOS
  - Fausse charité

Phishing

- Quoi?
  - Provient des termes “fishing” et “phreaking”.
  - Soutirer des données confidentielles en vue d’un usage frauduleux.
  - Forte augmentation entre 2017 et 2018 (de 475 à 1.277).

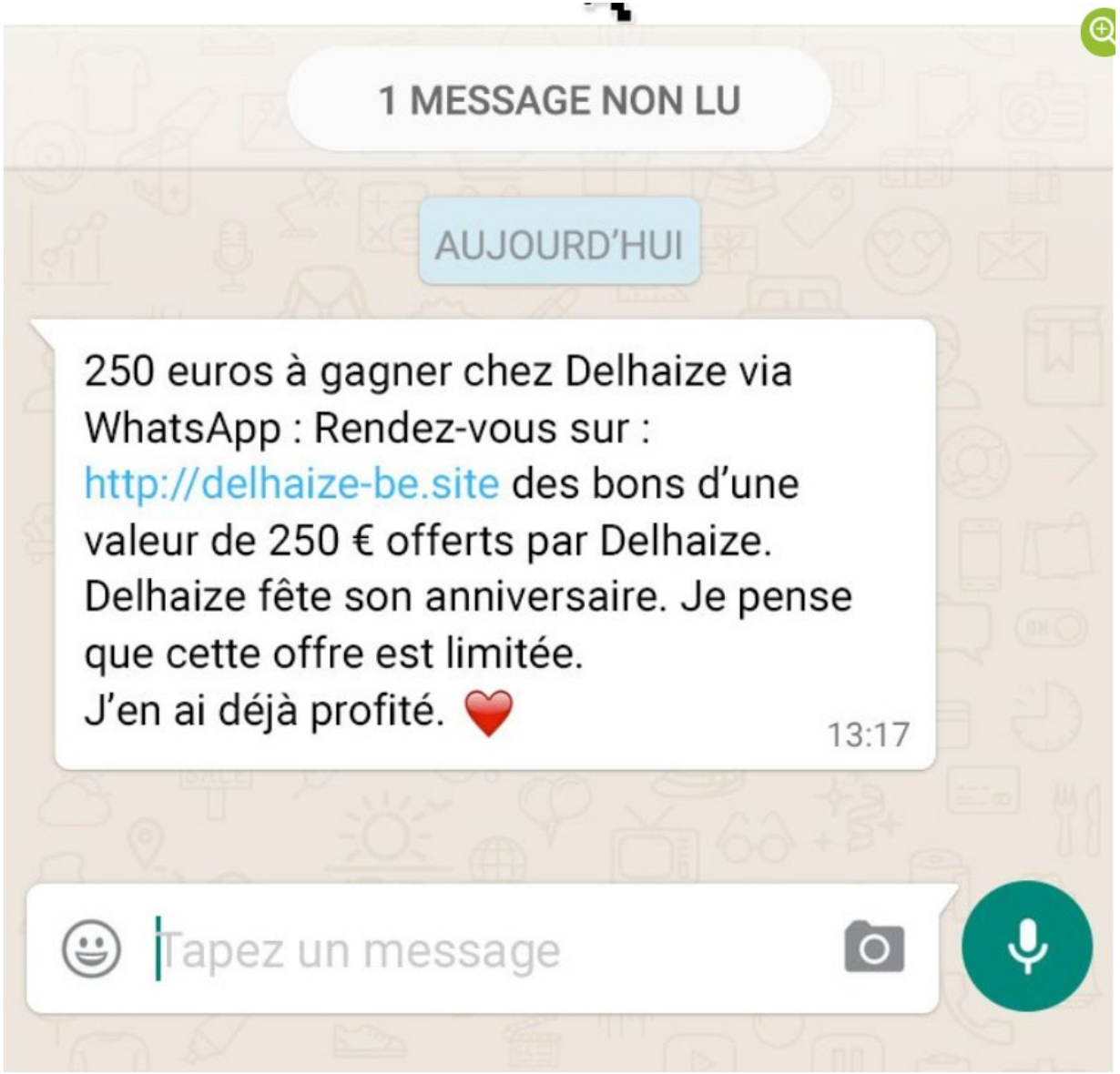
- Comment?
  - Mail/message à en-tête “officielle” envoyé à la victime
  - Instruction à la victime de cliquer sur un lien aboutissant à une page faussement professionnelle
  - Champs à remplir par la victime avec ses données bancaires ou autres
  - Utilisation frauduleuse des données de la victime

6 mythes à propos du phishing

1. Le phishing ne peut pas m’arriver.
2. Les messages de phishing sont remplis de fautes d’orthographe.
3. Le phishing ne fonctionne que par e-mail.
4. Ma banque peut me demander mes codes par téléphone.
5. J’ai plus de chance d’être victime de phishing via une application bancaire mobile.
6. Un antivirus peut me protéger du phishing.

Comment reconnaître le phishing?

- Regarder le nom de domaine: commence-t-il par “https://” et contient-il le vrai nom d’une organisation avant le .be, .com, .eu, .org…. ainsi qu’avant le premier “/”
  - **https://www.ing.be**
  - **http://https.www.argenta.be.madlart.com/nl/aanvraag.**
- Caractéristiques des messages de phishing :
  - Côté inattendu.
  - Caractère urgent.
  - Attise la curiosité
  - En-tête impersonnelle (“Chère Madame”, “Bonjour Monsieur”…).
  - Demande de cliquer sur un lien ou d’ouvrir une pièce jointe.
  - Demande de fournir des données personnelles.


1 MESSAGE NON LU
AUJOURD'HUI
250 euros à gagner chez Delhaize via WhatsApp : Rendez-vous sur : http://delhaize-be.site des bons d'une valeur de 250 € offerts par Delhaize. Delhaize fête son anniversaire. Je pense que cette offre est limitée.
J'en ai déjà profité.
13:17
Tapez un message

Aujourd'hui, la poste vous apporte un colis.

la poste <noreply@xyz542.be>
To YOU

4 septembre à 8 h 29

la poste

Bonjour,

BOLSY vous a envoyé un colis portant la référence 3232000179598199566320 40. La poste vous le livrera aujourd'hui entre 8 h et 17 h. Nous espérons que vous serez présent.

Vous pouvez consulter le statut de votre colis via notre application track & trace. Si vous ne parvenez pas à ouvrir le lien, veuillez télécharger notre outil pour suivre votre colis en direct.

Sincères salutations,
La poste.

Votre nouvelle carte bancaire – importance : élevée

Service clientèle QWT35 Bank <info@vnnabsbns.com>

Pas d'illustration dans cet e-mail ?
Dans ce cas, consultez-la en ligne.

QWT35 BANK

Votre nouvelle carte bancaire

Chère Cathy Jansens,

Notre service administratif nous informe que, malgré nos messages antérieurs, vous utilisez encore votre ancienne carte bancaire QWT35 Bank.

Les détenteurs d'un compte à vue QWT35 Bank ont jusqu'au 21 juillet 2017 pour commander gratuitement une nouvelle carte bancaire QWT35 Bank.

Les détenteurs d'un compte à vue ne profitant pas de cette action exclusive avant le 21 juillet 2017 recevront automatiquement une nouvelle carte bancaire QWT35 Bank. Les frais d'envoi automatique de la nouvelle carte s'élèvent à 17,95 € et sont automatiquement facturés. Les détenteurs d'un compte à vue en seront informés.*

Faites des économies et cliquez ici pour commander gratuitement votre nouvelle carte bancaire.

Avec nos plus cordiales salutations,

Votre équipe QWT35 Bank

Rappel – premier avertissement – Évitez une 2e majoration – importance : élevée

Police Fédérale <policefédérale@hsruhaw.com>

Appelez le **101** pour une assistance policière d'urgence

Police

Madame/Monsieur,

Nous tenons à vous rappeler par cet e-mail que vous nous êtes encore redevable d'une somme résultant d'une infraction au code de la route. Nous vous avons invité à procéder au paiement par courrier. Vous avez par ailleurs déjà reçu un rappel.

Le montant restant dû n'a pas (encore) été acquitté à ce jour.

Informations relatives à l'infraction et au règlement immédiat

Description de l'infraction	Dépassement de 22 k/h de la vitesse maximale sur (auto)routes hors agglomération, routes normales	
Date	12-08-2017	
Heure	19:36	
Vitesse autorisée	100km/h	
Vitesse mesurée	128km/h	
Vitesse corrigée	120km/h	
N° de la pellicule photo	1805076184	
Référence du dossier	1822719	
Sanction imposée	€ 97,50	La sanction tient compte de la vitesse corrigée
Frais administratifs	€ 06,00	
À payer	€ 103,50	

Évitez les frais de rappel

Nous vous invitons une nouvelle fois à acquitter le montant de 103,50 € dû avant le vendredi 8 janvier au plus tard et ce, via Bancontact/Mister Cash associé au 3V Payment Group. Vous ne payerez ainsi que le montant initial de 103,50 € dont vous êtes encore redevable. Vous pouvez acquitter ce montant via le lien suivant.

Cliquez ici pour acquitter le montant restant dû via Bancontact/Mister Cash.

Dès que vous aurez payé le montant restant dû, vous recevrez un code unique de 19 chiffres par e-mail. Afin de procéder au règlement complet et immédiat, il est important que vous entriez ce code de 19 chiffres sur notre site Web. Cliquez ici pour entrer le code à 19 chiffres sur notre site Web et pour procéder immédiatement au paiement.

Lorsque vous aurez soigneusement introduit ce code à 19 chiffres, vous serez automatiquement renvoyé vers notre page d'accueil. Si nous ne recevons pas le paiement du montant susmentionné, le montant restant dû sera une nouvelle fois majoré des frais de rappel légaux.

Nous espérons que ces informations vous seront utiles.

Sincères salutations,

La Police Fédérale

Police

Quelques conseils

- Vérifier l’adresse mail qui envoie le message (fautes d’orthographe éventuelles, nom de l’entreprise…).
- Ne pas accorder de confiance à un message alarmant provenant d’une banque, d’une grande entreprise, d’une société d’assurance…
- Ne pas ouvrir de pièce jointe contenue dans un mail “douteux”
- Une banque ne demandera jamais de fournir des données confidentielles par mail ou par téléphone.
- Aller sur Home Banking uniquement via les sites et applications officielles et pas via un lien internet contenu dans un mail ou un message.
- Au moment d’effectuer un paiement, vérifier que l’URL commence par “https://” , cela indique un environnement sécurisé.

Escroqueries à l’achat/vente

- Quoi?
  - L’acheteur paie mais ne reçoit rien ou reçoit quelque chose de moindre valeur.
  - Le vendeur envoie la marchandise mais n’est pas payé ou l’est avec un faux moyen de paiement.

Voorbeeld

Politie waarschuwt voor valse zoekertjes op immosites: “Sommige van die woningen bestaan helemaal niet”

02/03/2019 om 07:38 door gjs | Bron: VRT NIEUWS - Print - Corrigeer

Modus operandi lorsqu'on est acheteur

- Contact avec l'auteur via:
  - Une fausse publicité sur un site légitime (ex: 2ememain.be, Immoweb,...),
  - Un faux site de vente .
- L'auteur se fait passer pour un vendeur et propose une marchandise à un prix anormalement bas.
- Le vendeur demande en général une transaction via une plateforme de transfert d'argent (ex: Western Union ou MoneyGram).
- Après paiement, le vendeur disparaît et n'est plus contactable.

Modus operandi lorsqu'on est vendeur

- La victime entre en contact avec l'auteur via une annonce sur un site légitime (ex. 2ememain.be, Immoweb,...).
- L' "acheteur" négocie rarement le prix.
- 3 scénario's possibles:
  - L' "acheteur" paie le montant demandé avec un chèque faux ou falsifié provenant d'une banque étrangère. L'article est envoyé. La banque réquisitionne l'argent auprès du vendeur.
  - L' "acheteur" demande d'avancer une somme pour, par exemple, régler des frais de transport. Le montant est payé via un système de transfert d'argent de type Western Union. Après cela, l' "acheteur" disparaît.
  - L' "acheteur" paie plus que prévu à l'aide d'un chèque faux ou falsifié provenant d'une banque étrangère. Il dit que c'est une erreur et demande de lui rembourser le surplus. L'article est envoyé et l' "acheteur" disparaît.

Caractéristiques des annonces frauduleuses

- Trop bon marché.
- Description de la marchandise non-conforme à la photo.
- Fautes d’orthographes dans l’annonce.
- Coordonnées manquantes ou situées à l’étranger.

Quelques conseils

- Ne pas donner d'informations personnelles (documents d'identité, données bancaires…). Les auteurs pourraient les utiliser pour commettre d'autres délits.
- Ne pas accepter une proposition d'utiliser un autre moyen de transaction que celui du site.
- Utiliser éventuellement une carte de crédit qui n'est pas liée aux autres comptes. En cas d'escroquerie, les dégâts seraient moindres.

Les arnaques aux cryptomonnaies

Quoi?

- Fausses annonces dans les medias sociaux dans lesquelles des personnes célèbres disent être devenues riches grâce aux bitcoins.

- Les cryptomonnaies sont en vogue. Il s'agit d'une monnaie digitale et complètement virtuelle sous forme de codes cryptographiques. Les codes changent en fonction des transactions effectuées. Ce principe est appelé "blockchain".

Exemples

SPECIALE BERICHTGEVING: De meest recente investering van Philippe geubels verbaast experts en maakt grote banken doodsbang

Belgen verdienen al miljoenen euro's vanuit huis door gebruik te maken van deze maas in de wet om rijk te worden. Maar is het legaal?

Zoals Bericht Door

NOS | V | d | ELSEVIER | de Gelderlander

Modus operandi

- Les personnes sont dirigées vers des sites à partir desquels ils peuvent investir dans les monnaies virtuelles avec de gros gains à la clé.
- Les auteurs louent les services de compagnies de marketing afin d'attirer les personnes vers leur(s) site(s). Ces compagnies utilisent des intermédiaires qui créent et diffusent ces annonces en évaluant quelles célébrités utiliser pour attirer un maximum de personnes.
- Ex. En Belgique: Philippe Geubels, Gert Verhulst, Marc Coucke, Eddy Planckaert et Stromae.

Quelques conseils

- Savoir à qui on a à faire.
  - Vérifier l'interlocuteur. Utilise-t-il un site web? Depuis quand? Qui est derrière? Y a-t-il des antécédents de fraude.
- Ne jamais partager de données personnelles.
  - Les fraudeurs demandent souvent, sous prétexte que c'est obligatoire légalement, une copie de la carte d'identité, une photo, une "attestation" de domicile ou un numéro de carte de banque ou de crédit.
- Exiger des informations claires sur son interlocuteur.
  - Ne pas se laisser presser ou intimider. Le fait d'avoir rencontré ou entendu la partie en face ne veut pas dire qu'on ne se fera pas arnaquer.
- Rester vigilant par rapport aux promesses de gains extraordinaires.
  - Si le rendement est trop beau pour être vrai, ce qui est souvent le cas, le gain n'est jamais garanti.

Ransomware
(=logiciel d'extorsion)

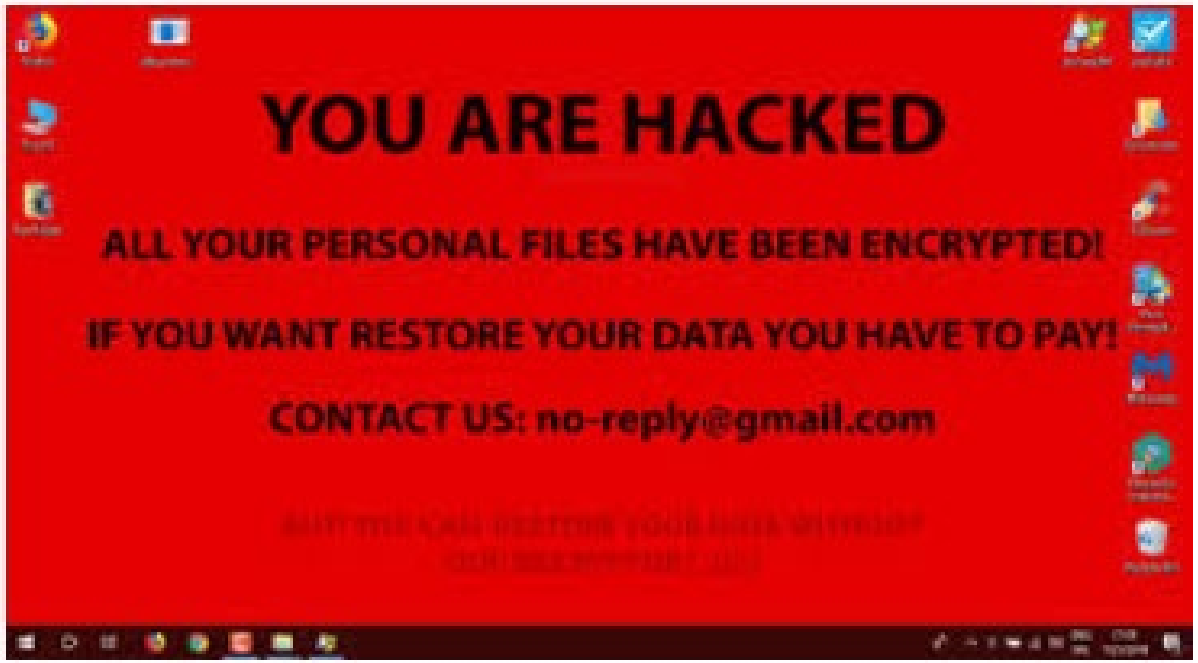
- Malware qui bloque un PC ou des données sur ce PC et qui demande à l'utilisateur de payer pour obtenir un code afin de "libérer" le PC ou les données.

- Payer ne signifie pas d'office que le PC sera débloqué. .

- Même après avoir payé et obtenu le code, le software reste toujours sur le PC et peut être réutilisé par après par l'auteur pour obtenir plus d'argent.

Exemples


BAD RABBIT
If you access this page your computer has been encrypted.
Time left before the price goes up
41:18:14
Price for decryption:
- 0.05
Enter your personal key or your bitcoin address


YOU ARE HACKED
ALL YOUR PERSONAL FILES HAVE BEEN ENCRYPTED!
IF YOU WANT RESTORE YOUR DATA YOU HAVE TO PAY!
CONTACT US: no-reply@gmail.com

Modus operandi

- Les ordinateurs des victimes sont infectés comme s'il s'agissait d'un virus.
- Au démarrage de l'ordinateur apparaît un message comme quoi il est bloqué.
- Souvent, le message donne l'impression de provenir d'une instance officielle et que l'utilisateur doit s'acquitter d'une amende pour avoir fait mauvais usage d'internet (Exemple : avoir téléchargé du matériel protégé par des droits d'auteur).

Quelques conseils

- Utiliser des logiciels actualisés. Les fabricants de logiciels publient régulièrement des mises à jour pour combler les failles de sécurité, telles que Microsoft Windows, Adobe Reader, Flash Player ....
- Ne pas surfer sur internet sans un programme antivirus à jour.
- Utiliser un firewall.
- Ne pas ouvrir de pièce jointe suspecte dans un e-mail.
- Ne pas télécharger ni installer de faux programmes ou logiciels piratés (illégaux).
- Ne pas activer les liens de type “cliquez ici”.

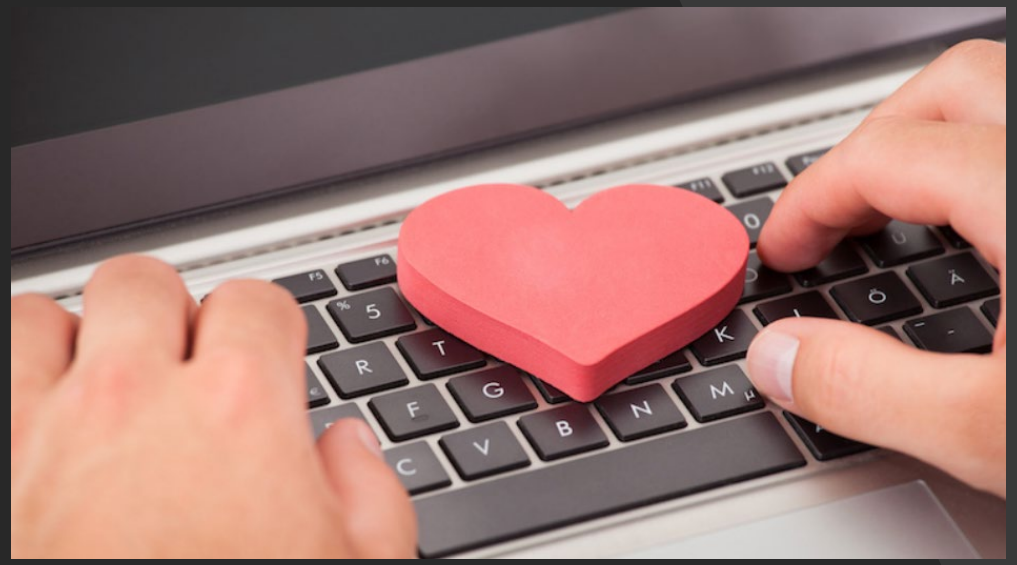
Comment réagir?

- Éteindre le wifi ou débrancher le câble internet.
- Déconnecter les autres appareils liés.
- Regarder sur le site web www.nomoreransom.org si le code pour le ransomware est disponible.
- Réinitialiser l'appareil et utiliser un back-up pour récupérer les données.
- Ne payer en aucun cas.

Arnaque faisant appel à l’émotion

- Quoi?
  - Jeu de l’auteur avec les sentiments de la victime afin de lui soutirer de l’argent.

- Différentes formes:
  - Arnaque par lien d’amitié
  - Email SOS
  - Fausse charité



Arnaque par lien d’amitié

Modus operandi

- Les auteurs recherchent leurs victimes potentielles sur des sites et/ou applications de rencontres. Ils utilisent également les e-mails, les “chats” et les réseaux sociaux.
- Ils utilisent un profil avec un faux nom ou l’identité volée d’une personne.
- Ils déclarent très rapidement leur amour.
- Leur but est de créer très rapidement un lien de confiance.
- Ils essaient de convaincre leur victime de poursuivre les échanges par un canal de communication différent de celui par lequel les premiers contacts ont eu lieu.
- Ils inventent toutes sortes d’histoires afin de se faire transférer de l’argent.
- Ils trouvent toujours un motif pour ne pas rencontrer la victime “en vrai” lorsque celle-ci le demande.
- Parfois “une histoire sans fin”, parfois contacts rompus tout à coup.

Quelques conseils

- Vérifier l’authenticité du profil. Demander assez d’informations et les vérifier par d’autres canaux.
- Ne pas faire confiance à tout le monde et garder les informations personnelles pour soi.
- Se méfier des histoires dramatiques. Les auteurs jouent sur les émotions. Que la personne demande à l’auteur les raisons pour lesquelles il lui demande à elle un soutien financier.
- Garder le portefeuille fermé. Réaliser qu’il s’agit d’un(e) parfait(e) inconnu(e).

Email SOS

- Piratage d’un compte e-mail.
- Le pirate informatique envoie un mail à caractère urgent à tous les contacts du compte.
- Exemple: Quelqu'un a perdu sa carte bancaire en vacances et a un besoin urgent d'argent pour revenir. Bien entendu, le montant dû vous sera remboursé. Il vous sera demandé de transférer l'argent via Western Union ou MoneyGram.

Comment réagir?

- Ne pas répondre au mail.

- Essayer de contacter l’ami en question par un autre moyen pour l’aviser que son compte a été piraté.

Fausse charité

- Quoi?
  - Demande de réaction très rapide par rapport aux évènements de l'actualité.
  - Organisation caritative fictive ou utilisation abusive du nom d'une institution reconnue.
  - Existe aussi le *spam* contenant des histoires déchirantes sur des catastrophes ou sur des enfants gravement malades pour lesquels on demande de faire une généreuse donation.

- Modus operandi?
  - Les auteurs abusent de la sympathie des gens. Ils réagissent aux évènements actuels. Lorsqu'une catastrophe se produit, ils sont là pour récolter des fonds pour une organisation connue ou fictive.

Exemples

PAYPAL.ME

Pay help animals using PayPal.Me

Go to paypal.me/helpanimalsos and type in the amount. Since it's PayPal, it's easy and secure. Don't have a PayPal account? No worries.

Showbizz

Helmut Lotti waarschuwt voor oplichters: "Laat mijn fans en vrienden met rust!"

TDS | 24 juli 2019 | 06u00 | Bron: TV Familie

DEEL 1 REACTIE

Comment différencier le vrai du faux

- Vérifier depuis quand existe l'organisation.
- Voir si l'interlocuteur met une pression pour jouer avec la compassion de la personne.
- Vérifier si les informations sont claires ou floues. Des demandes d'explication sont souvent éludées.
- Être attentif aux références citées.
- Continuer d'aider les autres mais avoir une réflexion critique!

Trucs et astuces

- Ne jamais donner de code PIN ou codes de banque en ligne par mail, médias sociaux, sms…
- Ignorer tous les messages qui dirigent vers un site demandant de payer ou vers une application bancaire.
- Toujours saisir soi-même l'adresse d'un site web dans le navigateur, surtout pour le site de sa banque, ou ouvrir soi-même l'application de sa banque
- Vérifier l'URL: "https://" indique un site web sécurisé.
- S'assurer de savoir à qui on s'adresse.
- Si c'est trop beau pour être vrai, c'est que ça ne l'est pas!

Comment réagir ?

- Contacter immédiatement Card Stop (www.cardstop.be of 070 344 344) si des données personnelles ont été données.
- Contacter sa banque.
- Changer les codes le plus rapidement possible.
- Porter plainte auprès de la police.
- Aller sur le site https://pointdecontact.belgique.be/meldpunt/fr/bienvenue

Sites web intéressants

- **https://www.safeonweb.be/**
- **https://www.safeonweb.be/index.php/fr/faire-le-test-du-phishing**
- **https://tropbeaupouretrevrai.be/**
- **http://www.lokalepolitie.be/5401/**