

AC Hotton

Menace du Cyberespace



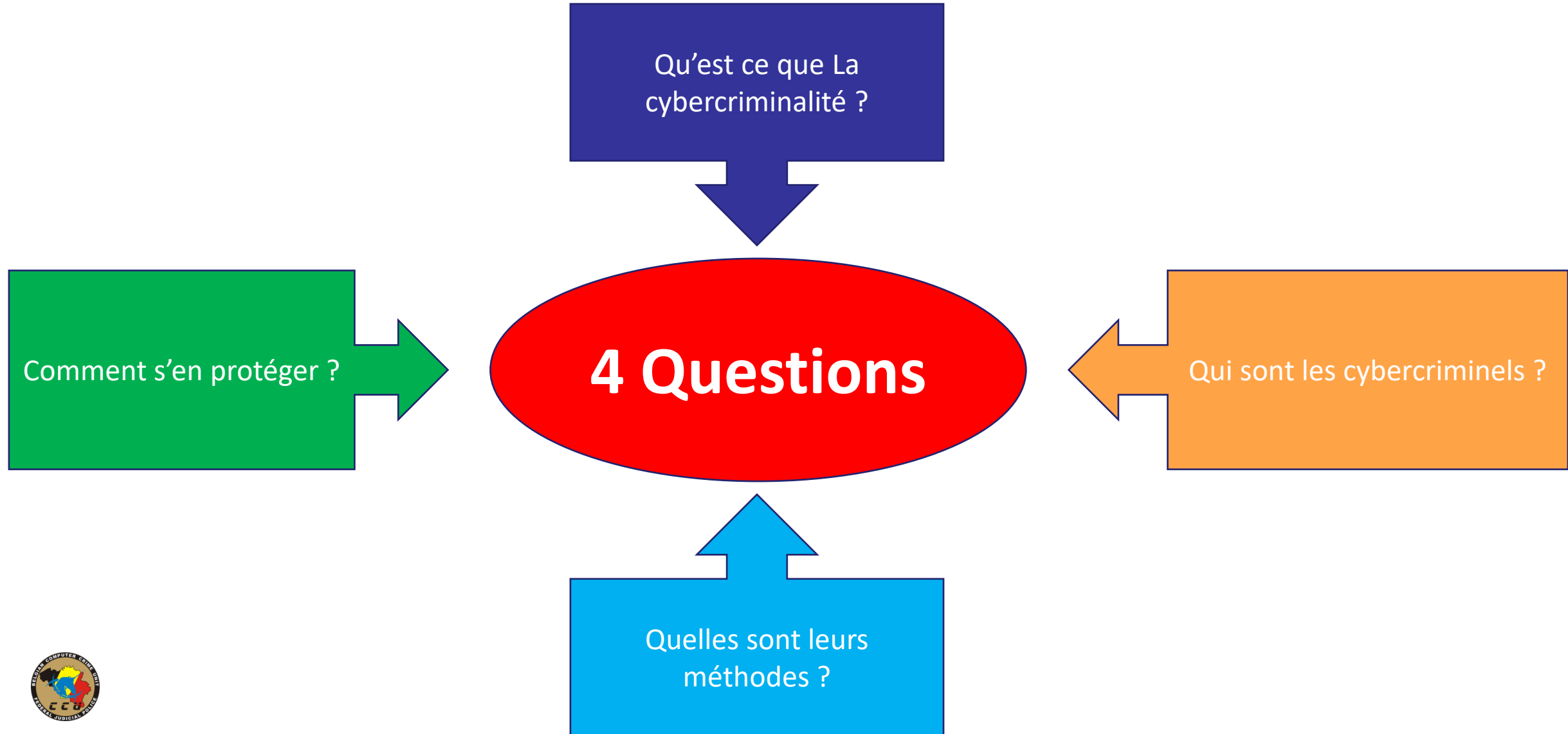
Auteur: 1^{er} Commissaire David WARNENT
Police Judiciaire Fédérale
RCCU Namur

Intervenant: Inspecteur Loic Flohimont
Police Judiciaire Fédérale
RCCU Arlon



Police Fédérale

Programme



A person wearing a dark hoodie is standing in a server room. The room is dimly lit with blue and purple light. In the background, there are rows of server racks. Overlaid on the scene is a digital network diagram with nodes and connecting lines, some of which are highlighted in pink. The overall atmosphere is mysterious and technological.

Qu'est ce que la
cybercriminalité ?

Internet : multitude de services



Internet en 60 Sec

2020 This Is What Happens In An Internet Minute



2021 This Is What Happens In An Internet Minute



Médias sociaux : quelques chiffres



2,93 milliards de compte



1,39 milliards de compte



436 millions de compte



800 millions de compte

Au final

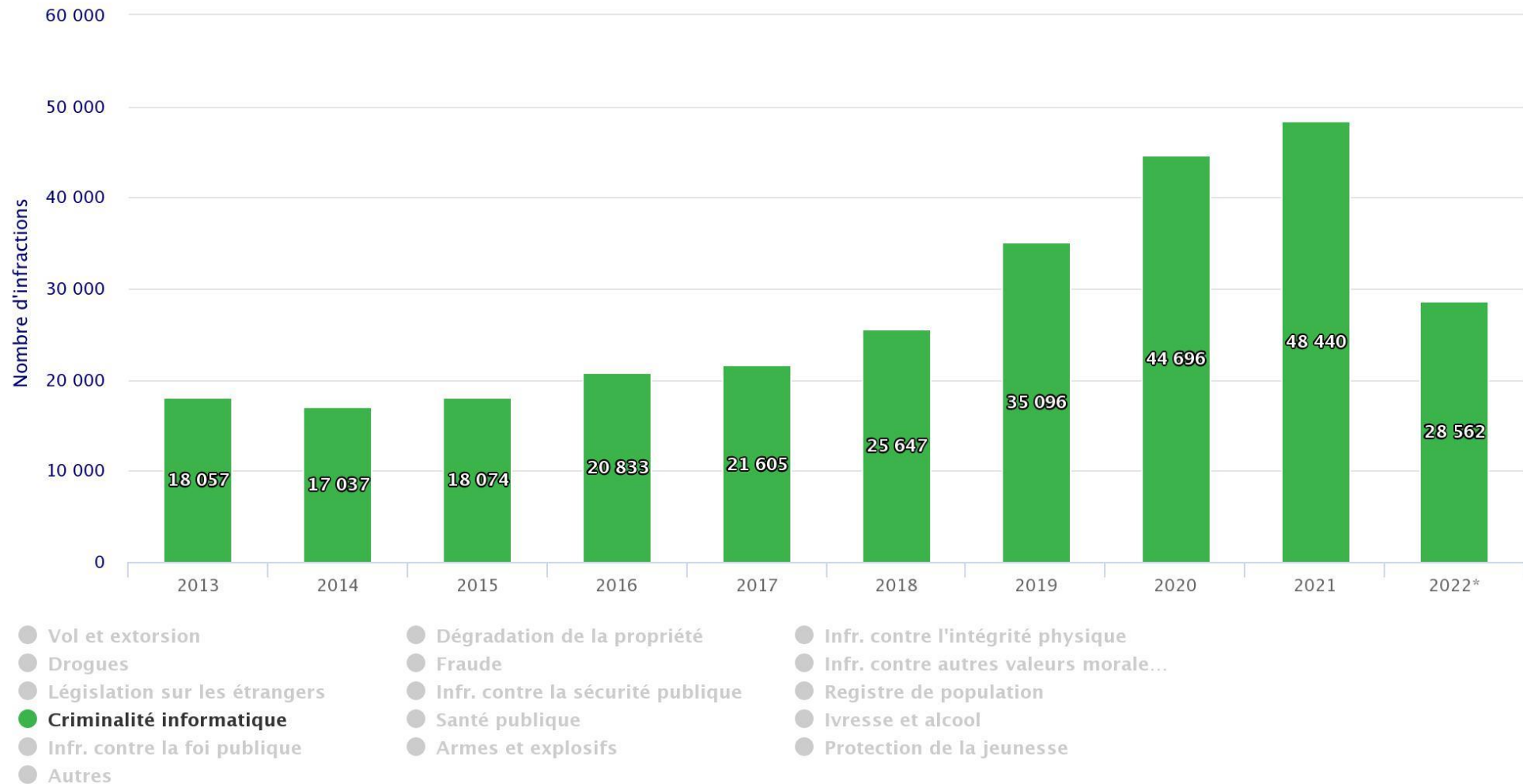
La cybercriminalité est constituée de **cybercrimes**.

Un cybercrime est une infraction pénale commise par le biais d'un système informatique ou d'Internet.

- Escroquerie avec Internet
- Hacking
- Etc

Etat de la situation en Belgique

Graphique des statistiques de faits criminels





Qui sont les
cybercriminels?

Typologie



Anomymous



Organisation criminelle





Quelles sont leurs méthodes ?

Fraude à l'achat / Investissement



Objet commandé et non reçu



Objet Livré / faux paiement



Fraude avec transporteur



Fraude cryptomonnaies
(FSMA)




AUTO

SCOUT 24

Arnaque trop perçu

Conseil Prévention

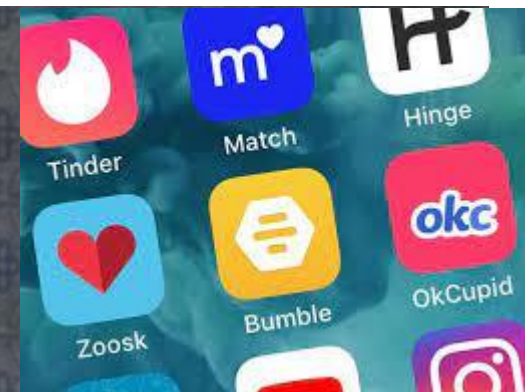
- Vérifier l'existence/fiabilité du site d'achat (nom du domaine / url du site)
Exemple : « <http://store-zalando.com> »
- S'assurer du profil du vendeur en demandant quelques données élémentaires (nom, prénom, adresse, ...)
- Demander d'autres photos du produit mis en vente
- Annonce trop alléchante = Méfiance
- Utiliser uniquement le moyen de transaction du site (pas de lien)
- Utiliser des moyens de paiement garantis (Paypal, Klarna, etc)
- Un acheteur « honnête » ne proposera jamais plus que le montant demandé (dans un premier temps sauf si enchère)
- Arnaque connue ? 

Fraude à l'émotion / sextorsion / Etc

happn meetic

badoo adopteunmec

Elite RENCONTRE tinder



PARFAIT AMOUR

OU PARFAITE ARNAQUE ?



Conseil Prévention

- Vérifier le profil en général :
 - Vérifier la photo de profil sur Internet
 - Vérifier l'adresse mail ou numéro de téléphone
 - Vérifier le nom
- Rencontre physique acceptée ?
- Arrêter dès qu'il y a demande d'argent
- Eviter de faire toute chose qui pourrait se retourner contre vous sans être sûr de son interlocuteur !



Phishing / Smishing



From: ING - HOME BANK <home.bank@ing.nl>
 Sent: 25 December 2020 17:00
 To: [REDACTED]
 Subject: Une mise à jour est disponible pour votre ING Card Reader



From: "Home Bank" <home.bank@ing.nl>
 Sent: Wednesday, 23 December 2020 16:00:04
 Subject: Une mise à jour est disponible pour votre ING Card Reader



Phishing



Europol
 Création 1er juillet 1999
 C/Anno Eisenhowerlaan 73
 s-Bas La Haye
 : 52° 05' 34" N, 4° 16' 53" E
 55 (décembre 2016)1
 el € 116.4 million (2017)2
 onnable Drapeau de la Belgique Catherine De Bolle (Directrice)
 an 73 Drapeau : Pays-Bas La Haye



de betaling voor uw laatste Netflix factuur is mislukt.
 1 op:



Vous êtes prié de vous faire entendre par mail en nous écrivant vos justifications afin qu'elles soient mises en examen et vérifiées de sorte à évaluer les sanctions ; cela dans un délai strict de 72 heures. Passé ce délai, nous nous verrons dans l'obligation de transmettre notre rapport au siège d'Europol à La Haye aux Pays-Bas pour établir un mandat d'arrêt à votre encontre, et vous serez fiché comme délinquant sexuel. Votre dossier sera également transmis aux médias pour une diffusion où votre famille, vos proches et toute l'Europe entière verront ce que vous faites devant votre ordinateur.

Maintenant vous êtes prévenu, Cordialement.
 CATHERINE DE BOLLE
 COMMISSAIRE

Message
 Hier 17:24

Proximus : Votre facture est PAYEE 2 fois par erreur, rendez-vous sur <https://bit.ly/Proximus20>

Phishing

za 9 mei 2020, 11:04

[FOD Financien Brussel] openstaande schuld met kenmerk 5008293 is na meerdere herinneringen, niet voldaan. Op 10 Mei 2020 zal de gerechtsdeurwaarder overgaan tot conservatoir beslag. U kunt de beslag procedure voorkomen door direct het gehele bedrag van €184,87 over te maken op:

BE91 0635 8160 6476
 T.A.V: LEO VAN WELLEN

Phishing



De : BNP PARIBAS FORTIS <boga.dokkar@ziggo.nl>
 Envoyé : dimanche 1 novembre 2020 08:30
 À : clientes@fortis.be <clientes@fortis.be>
 Objet : Une mise à jour est disponible pour votre lecteur de carte

Une mise à jour est disponible pour votre lecteur de carte.
 Pour continuer à bénéficier de tous nos services en ligne, vous devez mettre à jour votre lecteur de carte via votre espace easy banking.

Mettre à jour mon lecteur carte



Conseil Prévention

De : BNP PARIBAS FORTIS <boga.dokkar@ziggo.nl>

Envoyé : dimanche 1 novembre 2020 08:30

À : clientes-@fortis.be <clientes-@fortis.be>

Objet : Une mise à jour est disponible pour votre lecteur de carte

Une mise à jour est disponible pour votre lecteur de carte.

Pour continuer à bénéficier de tous nos services en ligne, vous devez mettre à jour votre lecteur de carte via votre espace easy banking.

Mettre à jour mon lecteur carte

Escroqueries diverses



Fausse loteries

Solicitors LLP
Attorney: Barr. Richard Grater Herwit
+44 20 35148052
office@netc.eu

Faux héritages

REF: BTO/00-189/1017
Date: 26-10-2017

Switzerland

Cher Alexandre

Tout d'abord, faut que je sollicite votre confiance dans cette transaction, ce qui est raisonnable en vertu de sa nature comme étant tout à fait confidentiel et secret. Bien que je sache qu'une transaction de cette ampleur subitera une quelconque crainte et inquiétude de votre part, mais je vous assure que tout ira bien à la fin de celle-ci.

Permettez-moi de me présenter. Cela peut vous surprendre de recevoir cette lettre car il n'y avait pas de correspondance précédente entre nous. Mon nom est M. Richard Grater Herwit, l'avocat de M. Philip qui est décédé à l'année 2010.

La raison pour laquelle je rentre en contact avec vous est pour que vous m'aidiez à sécuriser les fonds laissés par mon client, afin d'éviter qu'ils soient confisqués par la société de sécurité/Banque à la Espagne, d'où ces fonds évalués à US\$10.500.000 (Dix millions cinq cent mille US Dollars) ont été déposés par mon client avant sa mort. La société de sécurité a émis un avis pour contacter le plus proche parent ou le compte sera déclaré hors service et les fonds détournés à la trésorerie de la Banque. Jusqu'à présent, tous mes efforts pour obtenir une prise de contact avec quelqu'un lié à mon client est vaine.

Par conséquent, Je suis rentré en contact avec vous pour vous demander votre consentement pour vous présenter à la société de sécurité en tant que proche parent / bénéficiaire des fonds de mon client décédé, puisque vous avez le même nom, de sorte que la société puisse immédiatement vous libérer ces fonds. Je fournirai à la société toutes les documentations juridiques nécessaires vous permettant de bénéficier de ces fonds. Tout ce dont j'ai besoin est votre coopération honnête pour nous permettre d'atteindre notre but dans cette transaction.

Je tiens à souligner que 10% de cet argent ira aux organisations de charité, tandis que les 90% restants seront partagés à parts égales entre vous et moi. Cette transaction est entièrement exempté de risques. Je vais utiliser mon poste d'avocat du client pour garantir la bonne exécution de cette transaction. Si vous êtes intéressé, vous pouvez me contacter par; Tel: +442035148052 Email: richgrater@gmail.com J'attends votre réponse, je peux vous fournir plus de détails et documents pertinents qui vous aideront à mieux comprendre cette transaction.

*From: Politië België <noreply@politie3v.com>
*Sent: Saturday, January 24, 2015 2:58 PM
*To: xxxxxxxx.xxxxxxx <xxxxxxx.xxxxxxx@skynet.be>
*Subject: Opgelegde administratieve sanctie | Federale Politie
Aanvankelijk Proces-Verbaal TU.95.C5.473629/2014 Dienst Verkeer
*Datum van het feit*Datum: 24/11/2014
Geachte bestuurder,

U hebt een beschikking en twee aanmaningen ontvangen voor het overtreden van een verkeersvoorschrift. Wij hebben u per brief verzocht om de betaling alsnog te voldoen. Tot op heden hebben wij helaas nog geen betaling van u ontvangen. Wij hebben u hierover al een brief gestuurd. Wij attenderen u erop dat het betalingstermijn is verstreken.

*Informatie over de overtreding en de **opgelegde administratieve sanctie**
Omschrijving overtreding Overschrijding maximum snelheid op autosnelwegen, met 14 km/h
Datum 24 november 2014

Openstaand bedrag € 43,97
Incassokosten € 11,53
Te betalen € 52,50

Faux délits

*Technische vaststelling(en)
Camera: GATSO TYPE 24-C-AUS-2P,[5165GATS06]. Max. toegelaten snelheid:70km/u
Spec.: serienr.:A 2426/C 2426/L 2426/AUS 5165,
Gemeten snelheid: 84km/u
datum ijkng:12/06/2009, ijkingsnr.:103312-B-09,
Geldigheidsdatum:11/06/2016. Film: 1039/Foto: 38.
Onbemande camera geïnstalleerd en gebruikt conform Art. 62 KB 16/03/1968.
Goedkeuring en homologatie toestel conform KB 11/10/1997.
Plaatsing en gebruiksomstandigheden overeenkomstig de voorschriften KB 11/10/1997.
De verbalisatie werd specifiek gevormd voor de hantering van het gebruikte apparaat.
De feiten zijn gefotografeerd. De foto kan, op vraag van uw ambt, aangewend worden voor alle nuttige doeleinden.

U kunt direct online betalen met bancontact via 3V Payment Group. Klik hier op *online betalen* <<http://www.herladen.com/3v/>> om het openstaande bedrag te voldoen. Let op dat u de juiste waarde selecteert. Zodra u het openstaande bedrag heeft betaald via 3V Payment Group ontvangt u een unieke 19-cijferige code Om de betaling succesvol te registreren, dient u de 19-cijferige code invullen via de link hieronder. *Vul hier uw 19-cijferige code* <<http://politie.dx.am/p/>> in om de betaling succesvol te registreren. Indien wij het volledige bedrag niet voor dinsdag 27 januari van u ontvangen zal het bedrag worden verhoogd met buitenrechtelijke incassokosten ter hoogte van €146,79. Daarnaast loopt u het risico op een gerechtelijke procedure. Hoogachtend, Bert Dijk, Directeur Politie



Microsoft / Apple SCAM



Fausse identités

Messages SOS



Conseil Prévention

- Etes-vous sûr de connaître votre interlocuteur ? Non, alors méfiance !
- Pas d'utilisation du Digipass ; à aucun moment un organisme officiel ne vous le demandera, même pour vous « aider »
- Il est rare de gagner de l'argent venant du ciel (héritage, lotterie, etc)
- Vérifier les informations :
 - Vérifier l'adresse mail ou numéro de téléphone
 - Vérifier le nom
 - Arnaque connue ?
- Etes-vous dans la situation de ... ?
- Aucun document officiel de l'Etat par mail : eBox



RANSOMWARE



ALL YOUR IMPORTANT FILES ARE STOLEN AND ENCRYPTED!

All your files stolen and encrypted
for more information see
RESTORE-MY-FILES.TXT
that is located in every encrypted folder.

Would you like to save millions of dollars?
Our company acquires access to networks of various companies, as well as other information that can help you find the most valuable data of any company.
You can provide us accounting data for the access to any company. For example, login and password to RDP, VPN, corporate email, etc.
Open our letter if you want! Launch the provided virus on any computer in your company.
Companies pay us the ransomware to the decryption of files and prevention of data leak.
You can communicate with us through the live messenger.

Using this messenger, we will help you and your privacy is guaranteed.
If you cannot be reached, we will contact you through the live messenger.

If this content is encrypted, and we do not receive any feedback for the ransomware, please contact our support via Telegram channel.

Conseil Prévention

Voici les étapes à suivre pour supprimer un ransomware :



1. Déconnectez les appareils et les systèmes d'Internet
2. Effectuez une analyse antivirus des systèmes et des appareils
3. Supprimez les fichiers et les programmes malveillants

<🔒/>
NO MORE RANSOM

<https://www.nomoreransom.org/fr/index.html>

1. Appliquez de manière régulière et systématique les mises à jour de sécurité

du système et des logiciels installés sur votre machine.



3. N'ouvrez pas les courriels, leurs pièces jointes et ne cliquez pas sur les liens

provenant de chaînes de messages, d'expéditeurs inconnus ou d'un expéditeur connu, mais dont la structure du message est inhabituelle ou vide.



5. Évitez les sites non sûrs ou illicites

tels ceux hébergeant des contrefaçons (musique, films, logiciels...) ou certains sites pornographiques qui peuvent injecter du code en cours de navigation et infecter votre machine.



7. N'utilisez pas un compte avec des droits « administrateur »

pour consulter vos messages ou naviguer sur Internet.



9. Éteignez votre machine lorsque vous ne vous en servez pas.

2. Tenez à jour l'antivirus et configurez votre pare-feu.

Vérifiez qu'il ne laisse passer que des applications, services et machines légitimes.



4. N'installez pas d'application ou de programme « piratés »

ou dont l'origine ou la réputation sont douteuses.



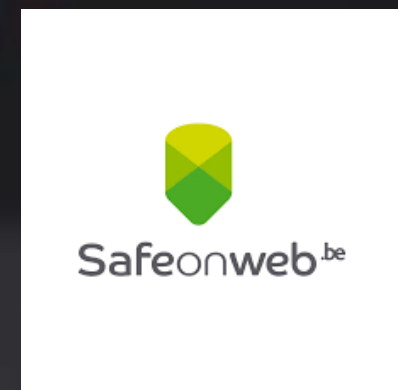
6. Faites des sauvegardes régulières

de vos données et de votre système pour pouvoir le réinstaller dans son état d'origine au besoin.



8. Utilisez des mots de passe suffisamment complexes et changez-les régulièrement,

mais vérifiez également que ceux créés par défaut soient effacés s'ils ne sont pas tout de suite changés.



Comment se protéger ?





Safeonweb^{.be}

ACTUALITÉ BLOG CONSEILS MATÉRIEL DE CAMPAGNE LIENS CONTACT SAFEONW



Soyez malin. Déjouez le phishing.

Découvrez la campagne



Au secours

Avez-vous un problème?



Testez votre sécurité

Faites nos tests !



Surfez en toute sécurité

Conseils pour surfer en toute sécurité



SI C'EST TROP BEAU
POUR ÊTRE VRAI

C'EST QUE ÇA NE L'EST PAS

[Matériel de campagne](#)

[Contact](#)

[Vérifier la fiabilité](#)

[Partager votre témoignage](#)

[NL](#) [FR](#)

[Fraudes à l'amitié](#)

[Arnaques à l'investissement](#)

[Arnaques aux cryptomonnaies](#)

[Actualités](#)

[FAQ](#)

[Victime d'une arnaque en ligne ? Signalez-le ici](#)



être trouvée.

Médias sociaux et téléchargements



Facebook
SPF Economie



Visionnez
nos vidéos



Téléchargez nos
supports de campagne

[Inscrivez-vous à notre newsletter](#)



Cette campagne est une initiative de :

[Conditions générales](#)

[Vie privée](#)

[FAQ](#)

© 2022

 **economie**

 **wikifin**

.be





Dépôt de plainte si victime

Politie Police

NL | FR | DE | EN



POINT DE CONTACT

Signalement si tentative

Vous êtes victime d'une tromperie, d'une arnaque, d'une fraude ou d'une escroquerie, ou vos droits en tant que consommateur ou entreprise n'ont pas été respectés ?

Choisissez alors le scénario qui s'applique à votre problème et suivez les étapes successives afin de signaler votre problème aux services compétents.

Vous recevrez toujours un avis dans lequel nous nous efforcerons de répondre au mieux à vos questions.

Les services compétents analyseront votre signalement et procéderont éventuellement à une enquête. Ceci peut impliquer la communication de vos données à d'autres autorités compétentes. Ils n'interviennent pas dans le cadre de votre problème individuel et ne fournissent aucune information sur l'enquête. En ce qui concerne votre problème individuel, nous nous référons exclusivement à l'avis qui vous sera envoyé.

J'accepte les [conditions d'utilisation](#) (obligatoire)

Nouveau signalement 



Merci de votre attention

