

PRÉVENTION CONTRE LES VOLS DANS HABITATIONS ET LES ESCROQUERIES

dont
la criminalité
informatique



Kinepolis
Imagibraine
12 et 26/06/2024



Karin Marique

*Service d'Assistance Policière aux Victimes
Service Prévention Vols*

Alain Desmet

*Premier Inspecteur Principal
Directeur Adjoint du Département Judiciaire
Enquêteur*

BL'A
Braine-l'Alleud
ma commune à vivre



SOMMAIRE

01 Les vols dans habitations

02 Les vols par ruse
et escroqueries “à domicile”

03 Les escroqueries “à distance”
et la criminalité informatique

Infractions et Modus Operandi

Astuces, conseils et bonnes pratiques

Victime ? Que faire immédiatement ?

Éléments utiles pour la police

04 Questions ?



LES VOLS DANS HABITATIONS



LES VOLS DANS HABITATIONS

Modus
Operandi

Le tournevis ou le pied de biche



La chignole



LES VOLS DANS HABITATIONS

Modus
Operandi

Le bris
de barillet



Le bris
de vitre



Le vol par
le 1^{er} étage

LES DIFFÉRENTES MESURES PRÉVENTIVES

Mesures
comportementales
ou organisationnelles

Des mesures
mécaniques

Des mesures
électroniques



MESURES COMPORTEMENTALES

Fermez bien
vos **portes**
et **fenêtres**

*Même si vous
ne quittez
votre domicile
que pour
un court instant*

Ne gardez pas
de fortes
sommes
d'argent
ou
trop de **bijoux**
chez vous

Prenez
des **photos**
de vos bijoux
et relevez
le **numéro**
de série de
vos appareils
électroniques

Ne laissez pas
en évidence vos
biens attrayants
et facilement
transportables

*GSM, tablettes,
PC portables,
consoles de jeux...*

Placez
des **minuteries**
sur
quelques-unes
de vos **lampes**
et **radio**

(Domotique)

Taillez
régulièrement
les **haies** et
la **végétation**

Ne laissez pas
à portée
de main
des **objets**
pouvant servir
à cambrioler
votre maison

Echelle, pavés,
outils, clés, ...

**SI VOUS PARTEZ EN VACANCES,
N'HÉSITEZ PAS À SIGNALEZ VOTRE ABSENCE
À NOTRE ZONE DE POLICE**

Passage de connaissances - Relevé de la boîte aux lettres

MESURES MÉCANIQUES

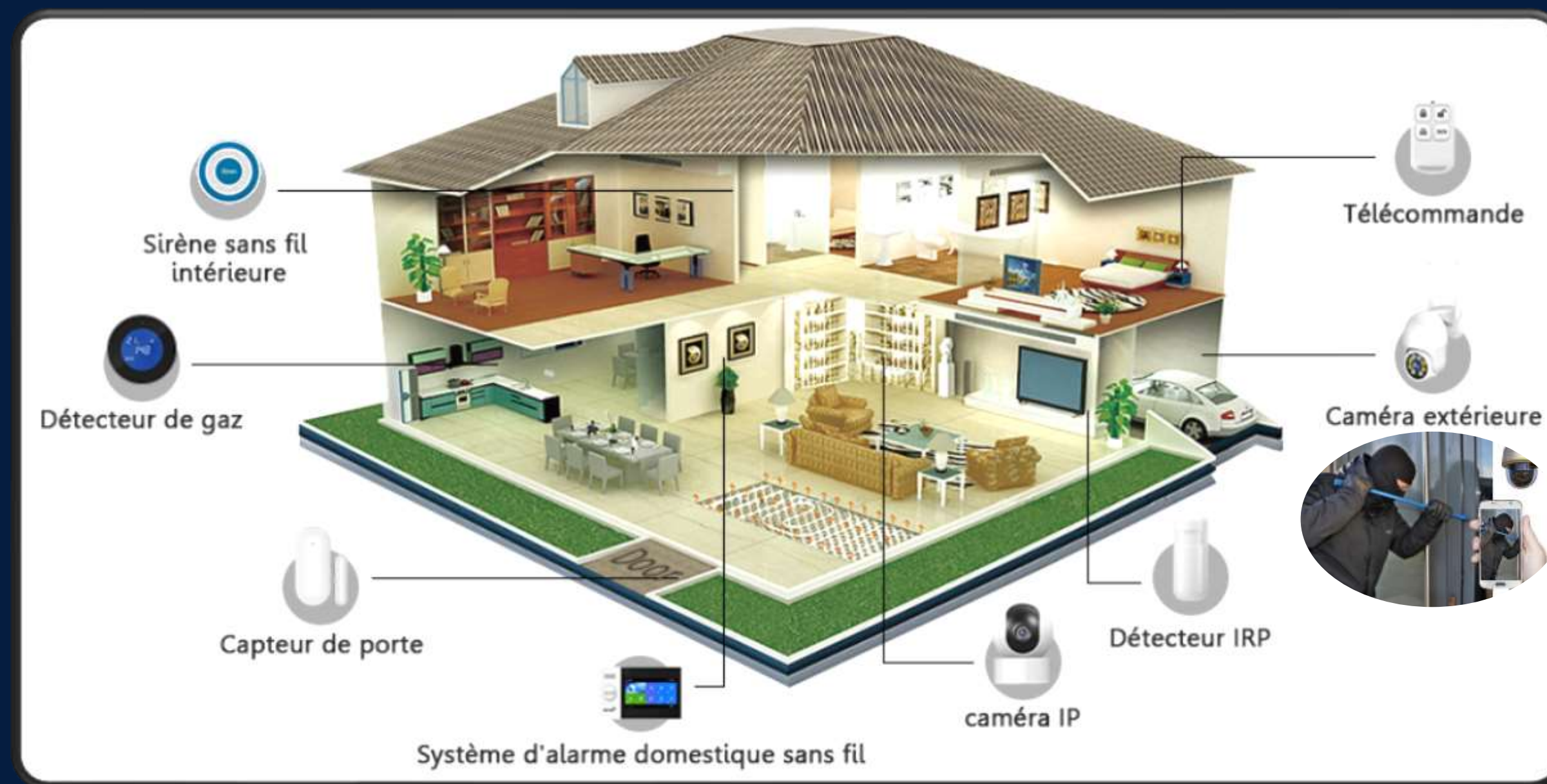
Renforcez
par des moyens
mécaniques
vos **portes,**
fenêtres,
portails et
barrières

Verrous,
cylindres de sécurité,
poignées de fenêtres
à clé



MESURES ELECTRONIQUES

Placement
d'un système d'**alarme**,
de **caméras**,...



Conseiller en prévention vol

Karin Marique

Service d'Assistance Policière aux Victimes

Service Prévention Vols

Zone de Police de Braine-l'Alleud

Tél : 02.389.44.07

karin.marique@police.belgium.eu



Prime communale en matière de sécurisation (Mesures mécaniques)

Pour les victimes de vols ou tentatives de vols dans habitations
ainsi que pour les personnes de plus de 60 ans

Intervention de maximum 500 €

BL'A
Braine-l'Alleud
ma commune à vivre

LES VOLS PAR RUSE ET ESCROQUERIES À DOMICILE



LE VOL PAR RUSE

Une personne usurpe
une identité professionnelle
ou utilise un faux, une astuce
ou une ruse

Pour obtenir, ou tenter
d'obtenir, l'accès à l'habitation
... en vue d'y **commettre un vol**

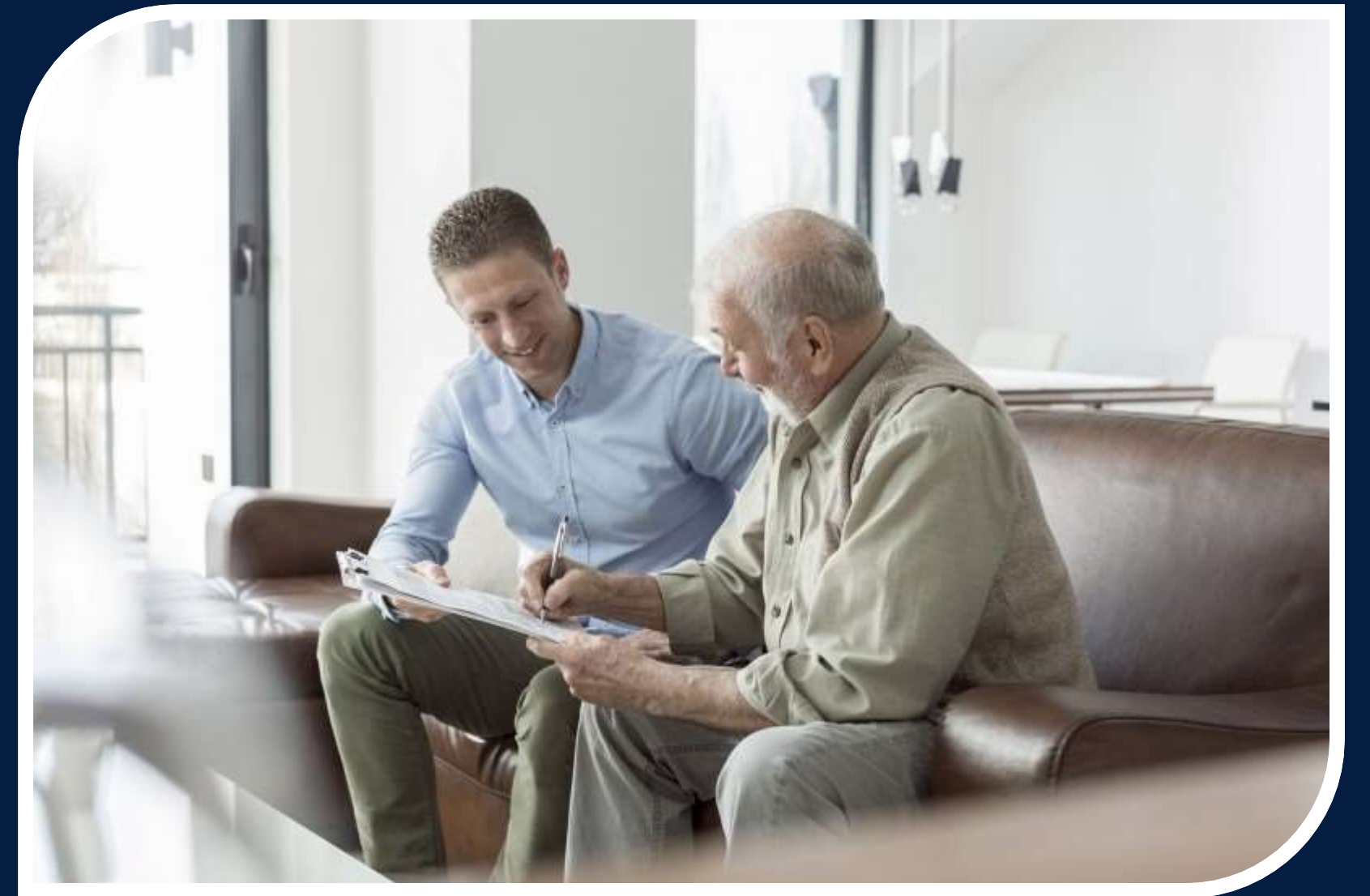


L'ESCROQUERIE

Une personne fait usage de faux noms ou fausses qualités et/ou emploie des manœuvres frauduleuses

... afin de

se faire remettre quelque chose
et donc éventuellement de l'argent
ou la signature d'un contrat



DIFFÉRENTES “RUSES” UTILISÉES

Faux employé public

(Policier, employé de la commune, de services sociaux, de l'Etat, ...)



Faux employé
(électricité, gaz,
compagnie
des eaux, facteur)



“Faux” travailleur

(démousseur, couvreur,
nettoyeur de vitres,
jardinier)



DIFFÉRENTES “RUSES” UTILISÉES

Faux titres, faux métiers

(collecteur de fonds
pour une œuvre de
bienfaisance,...)



Vendeurs de produits divers

(ballotins de pralines au
profit d'une association,
bouteilles de vin,
matelas, tapis,...)



Faux prétextes

(demander à boire,
pour téléphoner,
se rendre aux toilettes)



QUE FAIRE LORSQU'ON SONNE À LA PORTE

**En cas de doutes,
ne laissez pas rentrer**



1 Identifiez toujours vos visiteurs
Fenêtre, judas, visiophone
ou entrebâilleur

2 Prenez garde aux fausses qualités
Carte de légitimation, de commerce ambulant

3 Contactez la compagnie dont il est
question ou le 101
Pas le numéro donné par le « visiteur »

4 Donnez l'impression aux inconnus que
vous n'êtes pas seul chez vous

5 Méfiez-vous des inconnus qui sonnent à votre porte
pour vous demander à boire, à manger,
de téléphoner, ou d'aller aux toilettes

6 Ne laissez jamais un inconnu seul chez vous ou dans une pièce !
Ne le laissez pas détourner votre attention

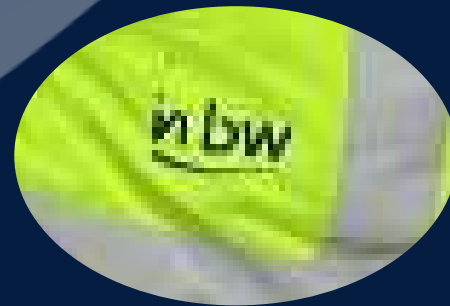
NE MONTREZ JAMAIS OÙ VOUS GARDEZ VOTRE ARGENT ET VOS OBJETS DE VALEUR

COMMENT RECONNAÎTRE UN AGENT D'UTILITÉ PUBLIQUE ?

Une fois par an ou tous les 2 ans,
vous recevez la visite d'un agent
qui vient relever vos compteurs
(électricité, gaz et eau)



Gaz et électricité : En Wallonie, c'est la société **ORES (078/15.78.01)** qui relève vos compteurs et transmet ces données à votre fournisseur d'énergie



Eau : C'est la société à laquelle vous payez la facture qui se rend chez vous pour relever votre compteur (**in BW 067/280.111**)



Téléphone et Internet : Vous n'avez pas de raison d'avoir la visite d'un agent de cette société sauf si c'est à votre demande

Le relevé de vos compteurs a toujours lieu en semaine pendant les heures de bureau

 L'agent doit toujours être en mesure de vous montrer sa carte de service

 Il ne vous demande jamais d'argent, sa visite est gratuite
Le paiement de la facture ne s'effectue jamais directement chez vous

DÉMARCHEURS ET VENTE DE BIENS À DOMICILE

Conseils supplémentaires



Méfiez-vous des occasions uniques,
des chances à saisir,...



Ne décidez pas et **ne signez pas**
dans l'urgence !



Ne payez jamais **rien** immédiatement,
pas même un acompte.



DÉMARCHEURS ET VENTE DE BIENS À DOMICILE

Si la personne se présente chez vous
avec un **terminal Bancontact** :

- Ne communiquez jamais le code de votre carte de banque et vérifiez toujours le montant introduit
- Composez toujours votre code secret à l'abri des regards
- Méfiez-vous si on vous demande un second retrait sous prétexte que le 1^{er} ne serait pas passé



**NE VOUS LAISSEZ JAMAIS ACCOMPAGNER À LA BANQUE
POUR RETIRER DE L'ARGENT**

DÉMARCHEURS ET VENTE DE BIENS À DOMICILE

 Qui frappe à votre porte ? **Rusez !**

RETOUR DES PSEUDO-DÉMOUSSEURS, TECHNICIENS, RAMONEURS, JARDINIERS, AGENTS DIVERS... ATTENTION AUX ARNAQUES !



Les escrocs n'ont qu'à bien se tenir !

   www.gouverneurbw.be/mamierusée

 Qui frappe à votre porte ? **Rusez !**

UN DOUTE ? REFUSEZ L'ACCÈS À VOTRE DOMICILE.
VOUS ÊTES CHEZ VOUS !



Les escrocs n'ont qu'à bien se tenir !



   www.gouverneurbw.be/mamierusée

LES ESCROQUERIES À DISTANCE



... ET LA CRIMINALITÉ
INFORMATIQUE

LA CRIMINALITÉ INFORMATIQUE

Quelques infractions pénales

La fraude
informatique

Ex :
*l'utilisation frauduleuse
d'une carte bancaire*

Le hacking

Ex :
*accéder à un système
informatique
sans y être autorisé*

Le sabotage
informatique

Ex :
bloquer un PC

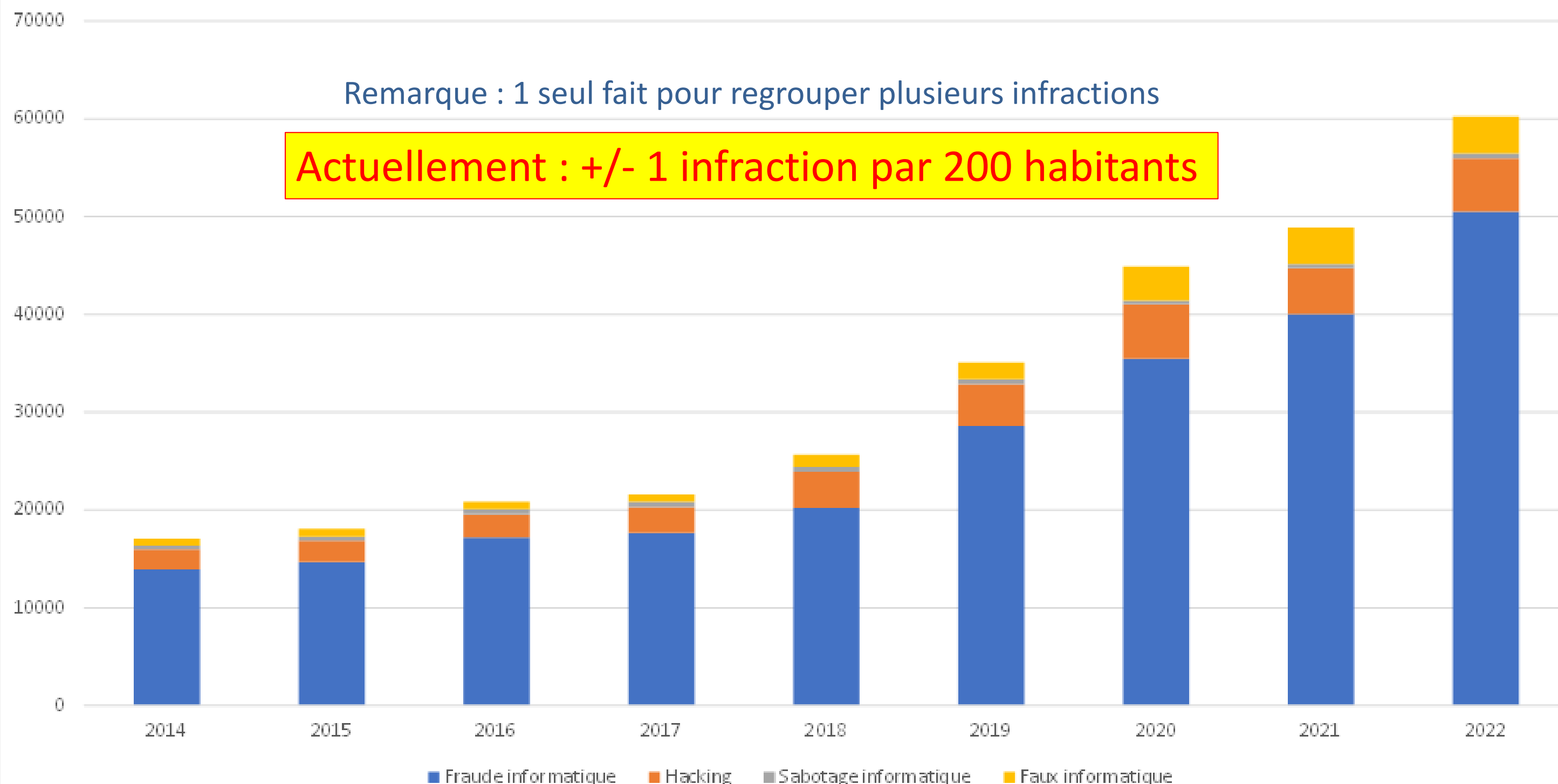
Le faux
informatique
(un faux
en écritures mais
dans un système
informatique)

...

Evolution de la criminalité informatique sur le plan national

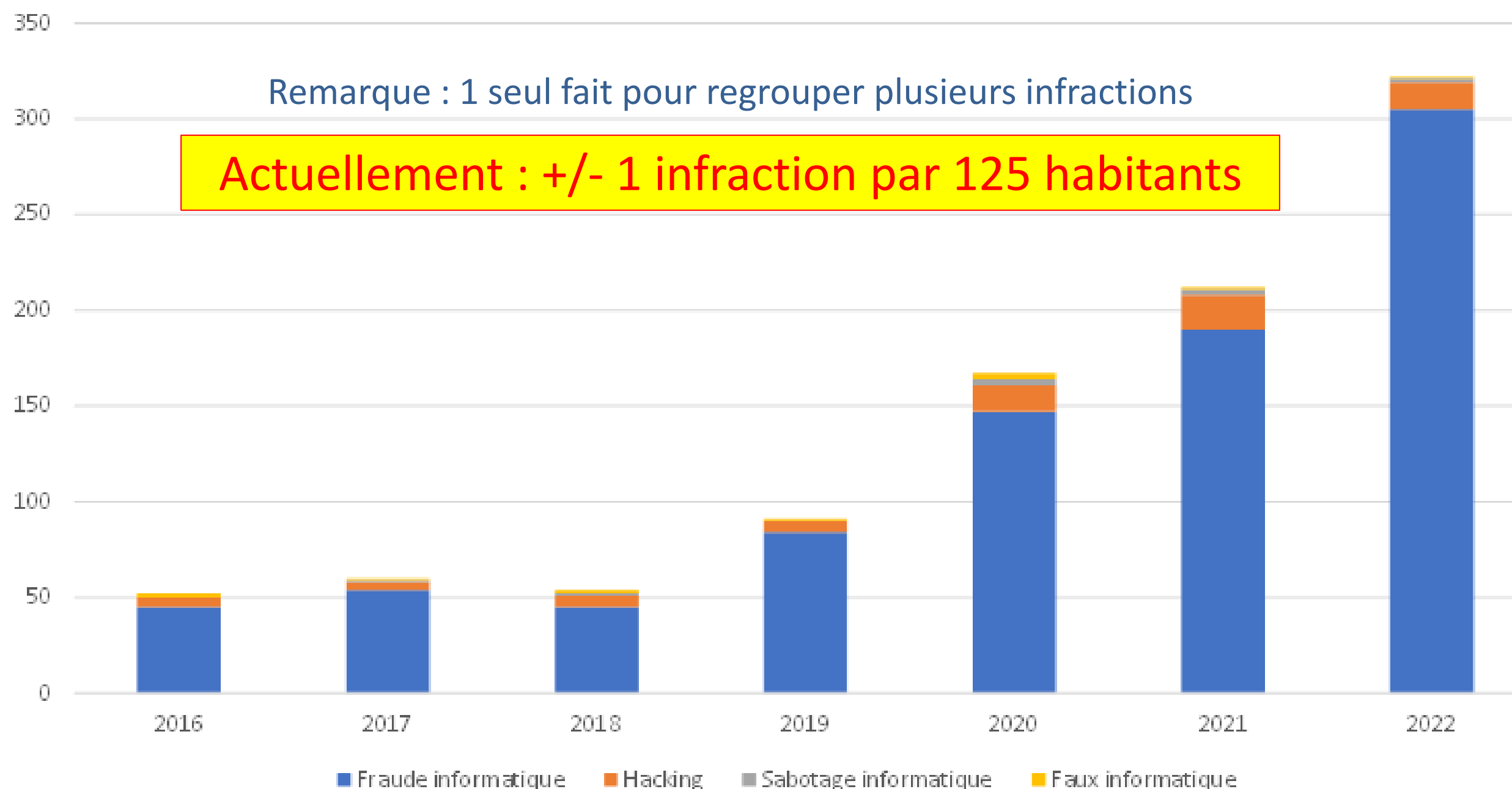
Remarque : 1 seul fait pour regrouper plusieurs infractions

Actuellement : +/- 1 infraction par 200 habitants



	2014	2015	2016	2017	2018	2019	2020	2021	2022
Fraude informatique	13904	14677	17194	17645	20217	28597	35463	40019	50504
Hacking	2055	2174	2367	2643	3660	4264	5572	4701	5476
Sabotage informatique	431	426	508	511	514	501	412	404	445
Faux informatique	647	797	764	806	1256	1739	3417	3727	3816
TOTAL	17037	18074	20833	21605	25647	35101	44864	48851	60241

Evolution de la criminalité informatique pour la Zone de Police de Braine-l'Alleud



	2016	2017	2018	2019	2020	2021	2022
Fraude informatique	45	54	45	84	147	190	305
Hacking	5	4	6	6	14	18	14
Sabotage informatique	0	1	1	0	3	3	2
Faux informatique	2	1	2	1	3	1	1
TOTAL	52	60	54	91	167	212	322

Quelques Modus Operandi



Shoulder Surfing



L'auteur **regarde le code**
et **éjecte la carte**
à l'insu de la victime
pour ensuite l'utiliser
(retraits / achats)

Skimming



Dispositif placé sur le terminal
permettant de **copier**
les données de la **carte**
et d'enregistrer le **code**

Card & Cash Trapping



Dispositif permettant de
bloquer la carte
et/ou les **billets**

Quelques Modus Operandi



Card Stop



FAUX

Votre banque ou Card Stop signale
un problème sur votre compte ou avec vos cartes

Votre interlocuteur demande de confirmer vos données bancaires
ou même de remettre votre carte munie de son code afin de l'annuler



Quelques Modus Operandi



Phishing



Faux message pour obtenir
des informations confidentielles
(identité, données bancaires,
codes et mots de passe)

Vishing



FAUX

FAUX

Phishing
en téléphonant à la victime

Quishing



Phishing
via de faux QR Code

Quelques Modus Operandi



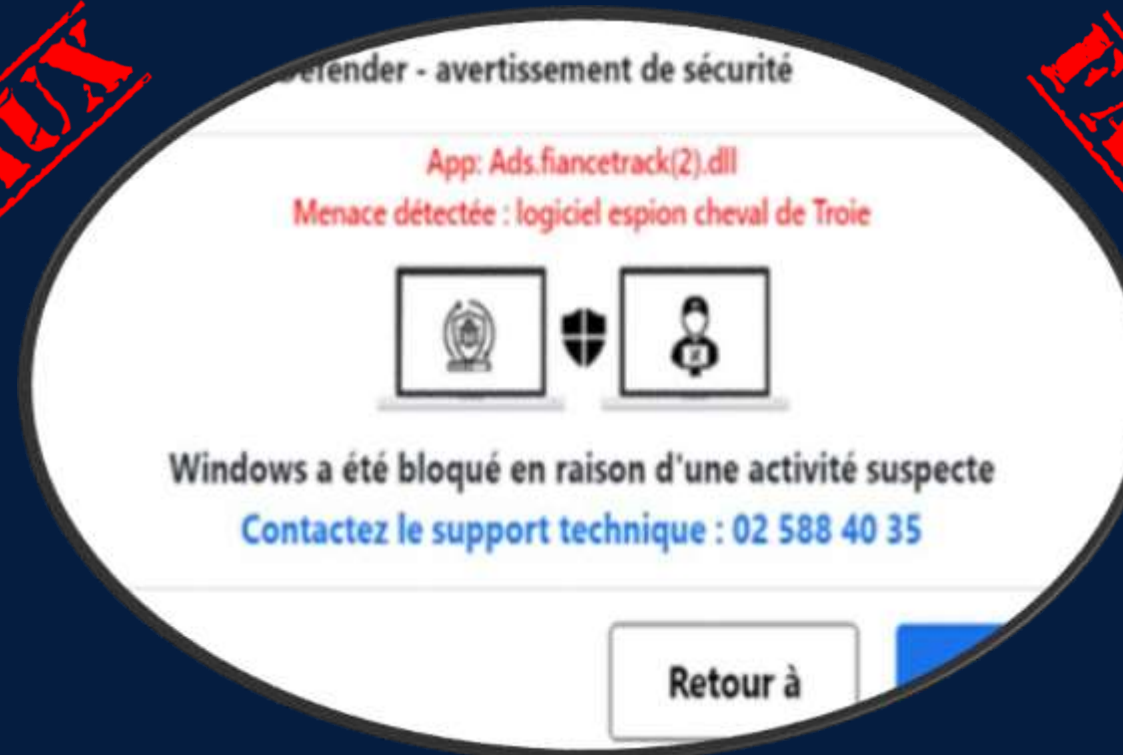
Ransomware



Votre **PC** est **bloqué** et/ou **crypté**
Une **rançon** vous est **demandée**

Tech Support Scam

FAUX



L'arnaque
au **faux support technique**
(*Microsoft, Apple,
antivirus,...*)

FAUX

Secure Account



L'escroc se fait passer
pour un employé de votre banque et
vous invite à **transférer**
votre **argent** vers un **compte sécurisé**

Quelques Modus Operandi



Fraude à l'achat



La victime **paie** son achat
(objets, places de concert,...)
mais **ne reçoit rien**
car il s'agissait d'une **fausse annonce**

Fraude à la vente

FAUX



L'acheteur vous transmet une **fausse preuve de paiement**
ou, afin de récupérer vos données bancaires,
vous demande de **créer un compte** sur le **site**
(qui s'avérera **faux**) d'une **société de transport**

Parfois, pour un motif quelconque, l'acheteur **paie plus** et
vous demande de lui **rembourser la différence**,
mais ensuite vous découvrez que son **paiement** est **faux**

Quelques Modus Operandi

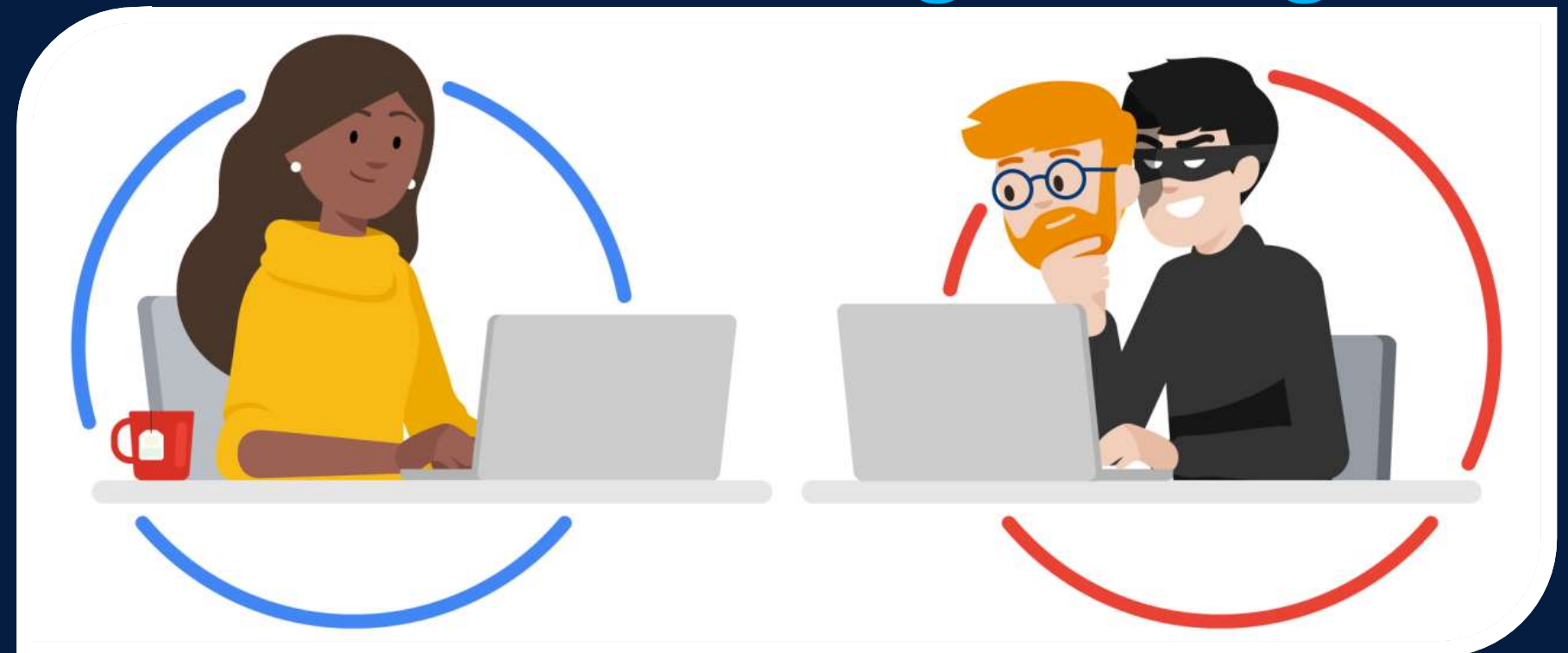


Fraude à l'émotion



Pour un motif généralement grave, quelqu'un qui se fait passer pour une de vos connaissances vous demande de l'**aider financièrement** ou d'effectuer un **virement urgent**

Fraude « Social Engineering »



L'escroc **se fait passer pour** le directeur ou le responsable financier d'une société et demande à un employé de la comptabilité de faire des **virements urgents**

FAUX

Quelques Modus Operandi



Arnaque aux sentiments



L'escroc recherche (sur les réseaux sociaux et les sites de rencontre)
une **personne** de préférence seule et **ayant besoin d'amour**
afin de gagner sa confiance et ensuite lui **demande de l'argent**
(pour venir la rejoindre en Belgique, car elle doit être hospitalisée,...)



Dans certains cas, il convainc même la victime
d'**ouvrir des comptes bancaires**
et/ou de **conclure des prêts bancaires**

Parfois, il se fait passer pour une **célébrité** (chanteur, acteur,...)



FAUX

Quelques Modus Operandi



Les faux sites et fausses annonces internet



Banque, cryptomonnaies,
organismes officiels (*impôts, remboursements / primes*),
sociétés de livraison (*DPD, DHL, UPS, GLS,...*)
vente de bois / pellets, vente de voitures, autres magasins en ligne,

...

Tout est bon pour les escrocs !

Leur but est de nouveau d'obtenir
vos **données personnelles** et/ou votre **argent**

Dans certains cas, ils **n'hésitent pas à vous recontacter**
pour vous escroquer encore plus
(*faux service de défense des consommateurs, avocats spécialisés,...*)



QUELQUES EXEMPLES EN DÉTAILS

ASTUCES ET
CONSEILS



ATTENTION

ARNAQUES

LES ESCROQUERIES PAR TÉLÉPHONE



- Appels de Microsoft, Apple, antivirus,... signalant un problème technique ou un logiciel malveillant sur votre ordinateur
- Appels de votre banque ou de Card Stop signalant un problème sur vos comptes ou avec vos cartes et/ou demandant de confirmer vos données bancaires
- Appels pour vous rembourser ou vous octroyer une prime
- Appels de vendeurs aux offres alléchantes
- Appels rapidement interrompus
Incitations à rappeler un n° qui s'avèrera payant
- ...

LES ESCROQUERIES PAR TÉLÉPHONE

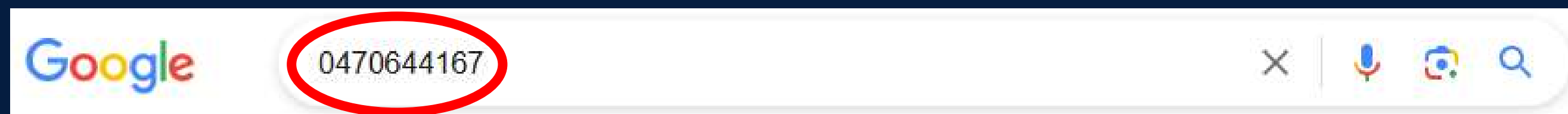
ASTUCES ET
CONSEILS



- Microsoft et Apple ne vous appelleront jamais d'initiative pour signaler un problème.
- Votre banque ne vous demandera jamais des informations confidentielles par téléphone.
Raccrochez et téléphonez à votre banque.
- Votre banque et Card Stop ne vous demanderont jamais de leur remettre ou de leur faire parvenir votre carte bancaire avec son code.
- Méfiez-vous du n° d'appel de votre interlocuteur.
Le n° qui apparaît n'est pas forcément celui qui vous appelle.
Il peut également s'agir d'un n° virtuel (faussement belge).
- Faites une recherche sur internet sur base du n° concerné.

LES ESCROQUERIES PAR TÉLÉPHONE

ASTUCES ET
CONSEILS



Tous Images Vidéos Actualités Livres Plus Outils

 Il semblerait qu'il n'y ait **aucun résultat pertinent** associé à votre recherche

Essayez d'utiliser des mots susceptibles de figurer sur la page que vous recherchez. Par exemple, "recettes de gâteaux" au lieu de "comment faire un gâteau".

Besoin d'aide ? Découvrez d'autres conseils concernant les recherches sur Google.

 Telefonförsäljare.nu
<https://www.telefonforsaljare.nu> > ... - Traduire cette page

Se vem som ringde dig från 047063XXXX - Vi har svaret

... **0470644167** - 0470644168 - 0470644169 - 0470644170 - 0470644171 - 0470644172 - 0470644173 - 0470644174 - 0470644175 - 0470644176 - 0470644177 - 0470644178 ...

*Afin d'afficher les résultats les plus pertinents, nous avons omis quelques entrées qui sont très similaires aux 1 entrées actuelles.
Si vous le souhaitez, vous pouvez [relancer la recherche pour inclure les résultats omis](#).*

LES ESCROQUERIES PAR TÉLÉPHONE

ASTUCES ET
CONSEILS



Google **32470644167**

Tous Produits Images Vidéos Actualités

 Signal-Arnaques
<https://www.signal-arnaques.com/scam/view> ⋮
contact@bdc-bois.com | Site internet
8 sept. 2022 — Site internet frauduleux. bdc-bois.com
+32 470 64 41 67 (ou 0032470644167) (+ d'infos) · B

Essayez plusieurs encodages

0470644167

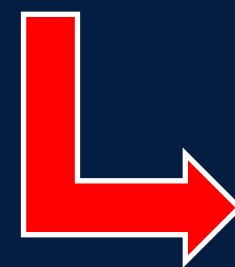
32470644167

+32470644167

0470 64 41 67

470 644 167

...



ARNAQUE SUSPECTÉE !!!	
 Site internet frauduleux bdc-bois.com contact@bdc-bois.com +32470644167	
☆ Suivre ce signalement	
Date	08/09/2022
Email	contact@bdc-bois.com
Pseudonyme utilisé	BDC bois de chauffage
Url / Site internet	https://bdc-bois.com/ ? Score fiabilité Scamdoc Info Contact / Whois

LES ESCROQUERIES PAR TÉLÉPHONE

- **Ne rappelez jamais** un n° que vous ne connaissez pas. Il peut être fortement surtaxé.
- **Signalez/bloquez** les n° indésirables.
- Le **message** de votre **boîte vocale** peut signaler que vous ne répondez pas aux appels non identifiés et/ou qui vous sont inconnus. Vous pouvez également bloquer les n° secrets.
- Ce n'est pas parce que **votre interlocuteur connaît** certaines de vos données personnelles, qu'il est fiable.
- **Ne communiquez jamais les codes** de vos cartes, ni ceux de votre Digipass ou itsme.
- Il en est de même pour vos **mots de passe** et vos **données** client ou personnelles.



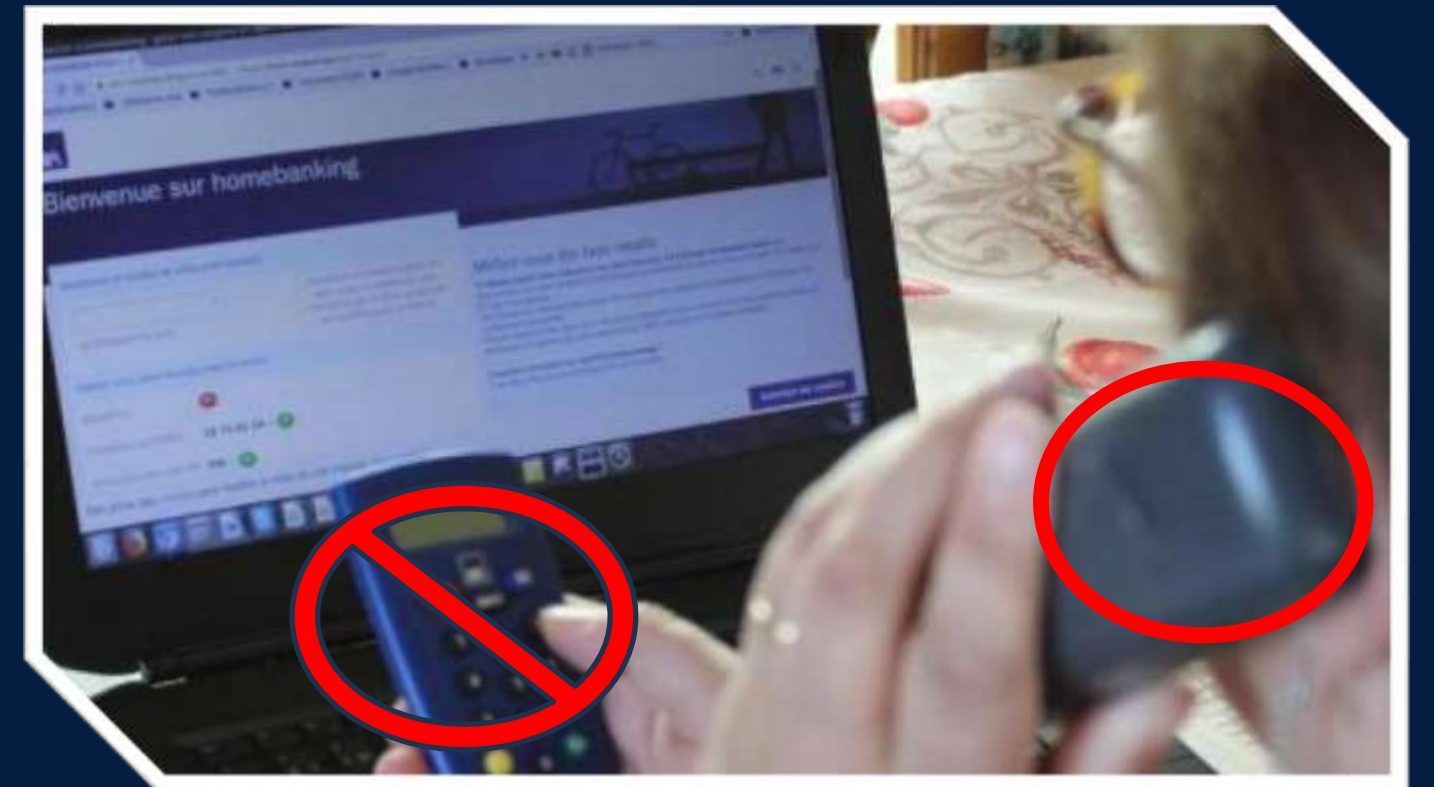
ASTUCES ET
CONSEILS



LES ESCROQUERIES PAR TÉLÉPHONE

- Votre **Digipass** ne sert **pas pour recevoir** de l'argent.
- Ne faites **pas de manipulations** sur votre PC ou smartphone **à la demande** de votre interlocuteur.
- Ne vous laissez **pas influencer** par son ton insistant ou directif.
- Enregistrez votre n° d'appel sur la liste "**Ne m'appellez plus**" en téléphonant au 02 882 19 75.
- ...

ASTUCES ET
CONSEILS



LES ESCROQUERIES PAR TÉLÉPHONE

- **Signalez** l'appel téléphonique (ou message) suspect sur le site du **SPF Economie** (<https://cc.consumerconnect.be>)



ASTUCES ET
CONSEILS



Signalements

*Quel est l'objet de votre signalement ?

Arnaques à la consommation

*Faites votre choix dans la liste

Appel téléphonique suspect

*Faites votre choix dans la liste

Demande de données personnelles par téléphone / utilisation du digipass (phishing)

Rappeler des numéros surtaxés

Télévendeurs frauduleux

Appel téléphonique suspect : autre

LES MESSAGES FRAUDULEUX

- SMS, email ou autre message écrit avec un lien vous dirigeant vers un faux site et/ou une pièce jointe installant un fichier malveillant sur votre matériel



C'est toi dans la vidéo ? 😨😨😨😨
<https://i1i.eu/VhXg6pFdM0>

INFORMATION

Une infraction à la réglementation du stationnement a été relevée à votre rencontre.

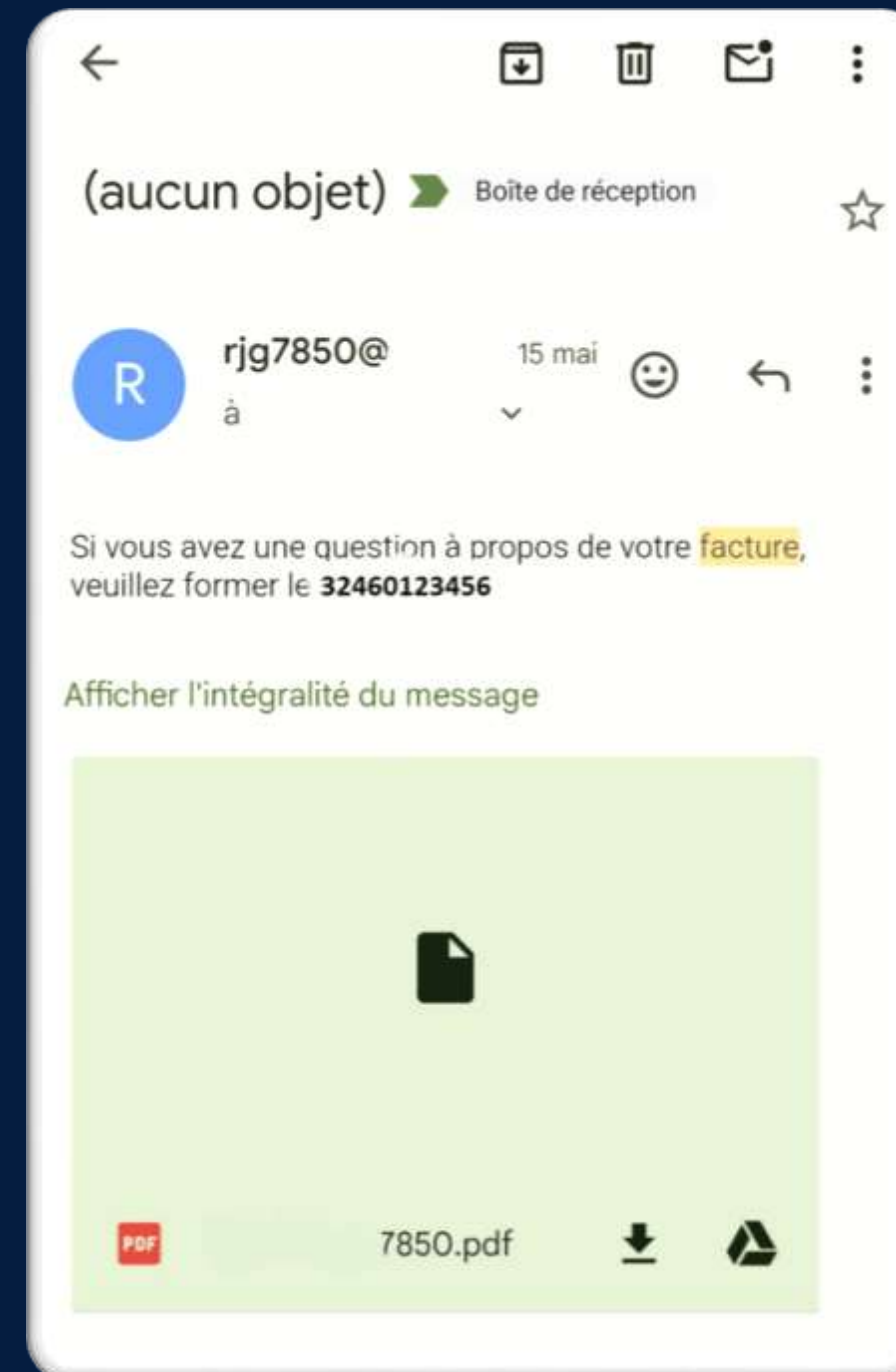
Vous allez prochainement recevoir par courrier, à l'adresse figurant sur le certificat d'immatriculation du véhicule, un avis de contravention.

Sur cet avis sont indiquées les modalités de paiement de la contravention. Il vous est donc possible de régler cette amende en suivant les instructions qui y sont précisées.

Pour régler cette contravention :

Utilisez l'appareil photo de votre smartphone pour scanner le QR Code situé ci-dessous.

Cliquez sur la notification qui s'affiche pour accéder à la page de règlement et régler votre amende.



LES MESSAGES FRAUDULEUX



- SMS, email ou autre message écrit avec un lien vous dirigeant vers un faux site et/ou une pièce jointe installant un fichier malveillant sur votre matériel
- SMS, email ou autre message écrit d'une connaissance ayant une extinction de voix qui vous demande de l'aide pour un virement urgent
- Courrier postal afin de faire un virement vers un n° de compte erroné ou vous invitant à scanner un QR Code
- ...



RECONNAÎTRE LES MESSAGES FRAUDULEUX



- Le message est-il inattendu ?
- Est-ce urgent ?
- Connaissez-vous l'expéditeur ?
- L'adresse de l'expéditeur est-elle étrange ?
- La question qui vous est posée vous paraît-elle étrange ?
- Où mène le lien sur lequel on vous invite à cliquer ?
- Le message contient-il des fautes d'orthographe et/ou de grammaire
- Est-ce que l'email s'adresse à vous personnellement ?
- Le message était-il dans vos spams ?
- Vous demande-t-on d'effectuer un paiement ?

RECONNAÎTRE LES MESSAGES FRAUDULEUX



INFORMATION

Une infraction à la réglementation du stationnement a été relevée à votre rencontre.

Vous allez prochainement recevoir par courrier, à l'adresse figurant sur le certificat d'immatriculation du véhicule, un avis de contravention.

Sur cet avis sont indiquées les modalités de paiement de la contravention. Il vous est donc possible de régler cette amende en suivant les instructions qui y sont précisées.

Pour régler cette contravention :

Utilisez l'appareil photo de votre smartphone pour scanner le QR Code situé ci-dessous.

Cliquez sur la notification qui s'affiche pour accéder à la page de règlement et régler votre amende.



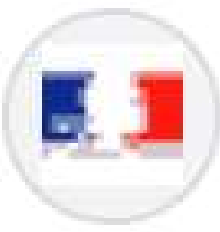
Site web

<http://antai-gouv-fr.fr>

Copier **Ouvrir le lien**

Google

Tous Images

 **ANTAI.gouv**

<https://www.antai.gouv.fr>

ANTAI.gouv
<https://www.antai.gouv.fr>

ANTAI : Agence nationale de traitement automatisé des ...

PAIEMENT DE VOTRE Amende. Si vous souhaitez payer ou consigner en ligne, cliquez ci-dessous pour accéder au site sécurisé de télépaiement. · Actualités · Le ...

 **scamdoc**

Evaluation de confiance numérique

Analyse du site internet "Antai-gouv-fr.fr"

Score de confiance **Très faible**

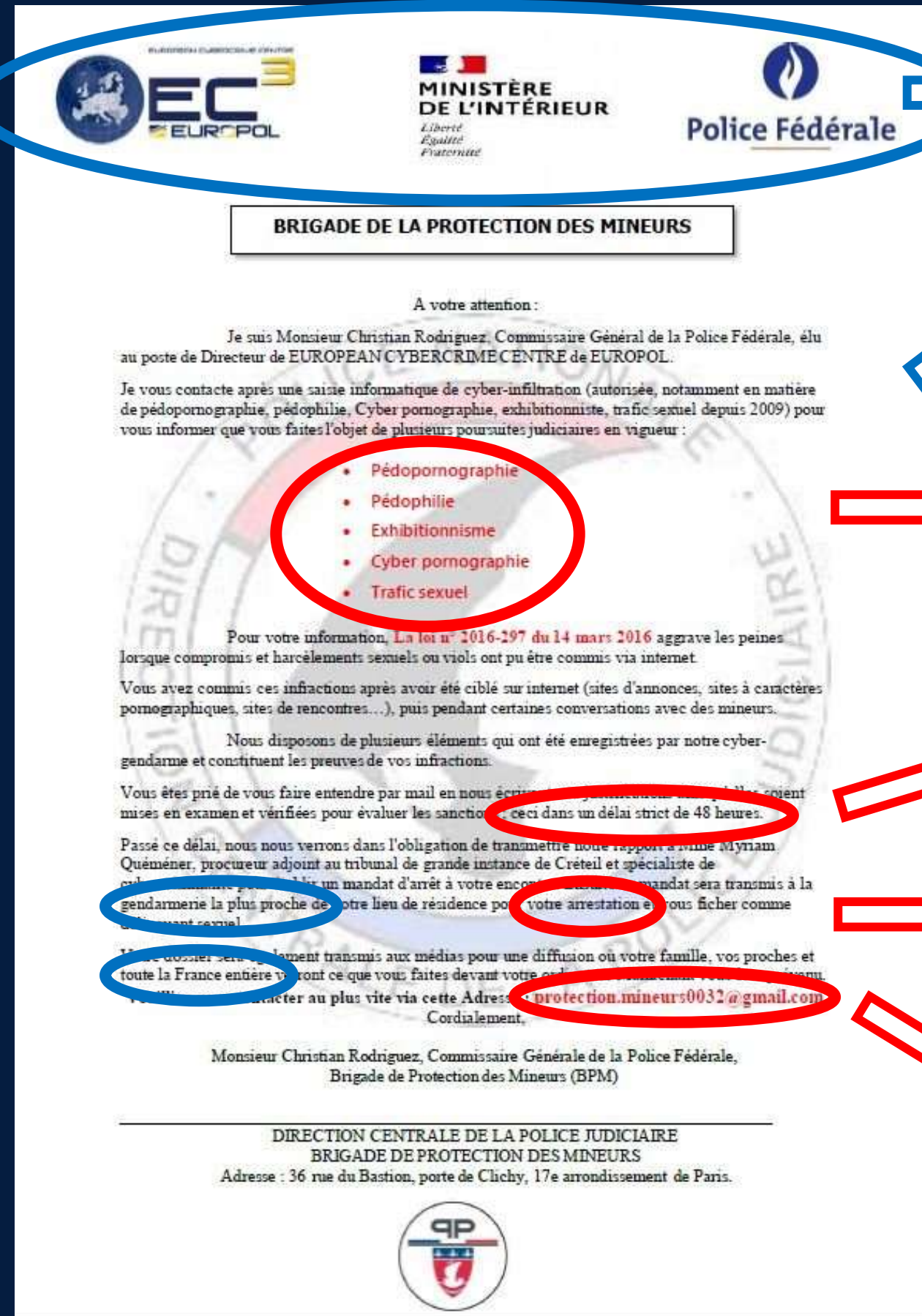
1% 

Réservé aux internautes très expérimentés

Points négatifs

- Un malware a été détecté sur le site (source AlienVault) [Consulter la source](#)
- Ce domaine est marqué comme **dangereux chez Phishing Initiative.**
- Le **nom de domaine** associé à ce site internet est **relativement récent.** ?
- Le **mail de contact** du site fait référence à un service de **messaging gratuit** ?
- Le nom du domaine affiche **une faible espérance de vie** ?

RECONNAÎTRE LES MESSAGES FRAUDULEUX



Nombreux logos
d'autorités différentes

Courrier adressé en Belgique
mais avec des données françaises

Infractions graves
mises en évidence en rouge

URGENCE

Ceci dans un délai strict de 48 heures

MENACES - PEUR

Passé ce délai... votre arrestation

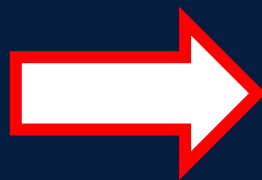
Adresse email gratuite Gmail
pour un organisme officiel ??? !!!

RÉAGIR AUX MESSAGES FRAUDULEUX

Ne cliquez pas sur un lien
et n'ouvrez pas les documents joints



Envoyez par mail la **capture d'écran**
du SMS suspect



suspect@safeonweb.be



Transférez simplement le mail suspect



Pour ceux qui veulent aller plus loin dans les vérifications

ASTUCES ET
CONSEILS



L'en-tête technique d'un email

ASTUCES ET
CONSEILS



Permet dans certains cas d'obtenir des informations
comme l'**ID** et l'**adresse IP d'origine** du message,
l'**horodatage** exact,
une **adresse email de réponse**
qui serait différente de celle de l'expéditeur,...

Utile pour détecter un email suspect

Mais également
pour des suites d'enquête plus rapides
lorsqu'on est victime



L'en-tête technique d'un email



Pour obtenir cet en-tête technique, il faut généralement :

- Consulter le message depuis un ordinateur
- Cliquer sur les trois petits points en haut à droite du message

11:00 (il y a 1 heure)



ou aller dans les options

- Afficher l'original, la source ou l'en-tête

Signaler comme spam

Signaler comme hameçonnage

Afficher l'original



Plus ▾

Marquer comme lu(s) Q

Marquer comme non lu(s) Maj.+Q

Étoile L

Retirer l'étoile Maj.+L

Imprimer P

Filtrer les mails semblables à celui-ci...

Afficher l'en-tête complet

Sélectionner un encodage...

ASTUCES ET
CONSEILS



Procédure variable en fonction
de la messagerie utilisée

L'en-tête technique d'un email



ASTUCES ET
CONSEILS



Procédure variable en fonction
de la messagerie utilisée

Message d'origine



ID du message	<oj8mb.lwxdfxvrs7ote8l@email.opticien24.com>
Date de création :	2 juin 2024 à 12:00 (Temps d'envoi : 5 secondes)
De :	Votre opticien en ligne <update@email.opticien24.com> Message envoyé avec eC-Messenger Build 6.90.5768
À :	alain [REDACTED]@gmail.com
Objet :	📢 Tous les Suppléments Lunettes à Moitié Prix !
SPF :	PASS avec IP 209.85.220.41 En savoir plus
DKIM :	'PASS' avec le domaine email.opticien24.com En savoir plus
DMARC :	'PASS' En savoir plus

[Télécharger l'original](#)

[Copier dans le presse-papiers](#)

L'en-tête technique d'un email



ASTUCES ET
CONSEILS

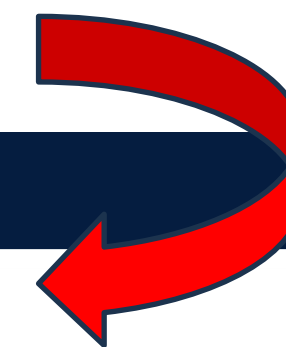


Procédure variable en fonction
de la messagerie utilisée

```
Received: from duoquattuorduo.zeta.ec-cluster.com (duoquattuorduo.zeta.ec-cluster.com. [195.140.184.242])
  by mx.google.com with ESMTPS id 5b1f17b1804b1-421270795fcsi45446835e9.98.2024.06.02.03.00.46
  for <alain[REDACTED]@gmail.com>
  (version=TLS1_3 cipher=TLS_AES_256_GCM_SHA384 bits=256/256);
  Sun, 02 Jun 2024 03:00:46 -0700 (PDT)
Received-SPF: pass (google.com: domain of g-3896181582-3716-355770452-1717322443335@bounce.email.opticien24.com designates
  195.140.184.242 as permitted sender) client-ip=195.140.184.242;
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=email.opticien24.com; q=dns/txt; s=ecm1;
bh=IMm37hVKDyQfJ7EbVC6RAbn6pb/xTGEwAA+vrTdPdC8=; h=date:from:reply-to:to:subject:message-id:mime-version:content-
type:content-transfer-encoding:list-id:list-help:list-unsubscribe:list-unsubscribe-post:x-csa-complaints;
b=q6JMV1pz+MRPSeJ9X+1XPY00FigagfOnMIVzUng7M6qdVzX7rQBVF4+1I8+/boP+bWMC6ZKwP
WJLahpXFJukV55oAn7tXSUwR7e94DtmQqFrZyujOKV3Y4Dm3Seq4FpGvOniy2BIWe2z1JdWVTfM
Received: from app01.muc.ec-messenger.com (app01.muc.ec-messenger.com [172.
  <g-3896181582-3716-355770452-1717322443335@bounce.email.opticien24.com>) by
  ESMTP id BK1UAVeVrjwT for <alain[REDACTED]@gmail.com>; Sun, 02 Jun 2024 12:00:43 +0200 (CEST)
Date: Sun, 2 Jun 2024 12:00:43 +0200 (CEST)
From: Votre opticien en ligne <update@email.opticien24.com>
Reply-To: update-embedded@email.opticien24.com
To: alain[REDACTED]@gmail.com
Message-ID: <oj8mb.lwxdfxvrs7ote8l@email.opticien24.com>
Subject: Tous les Suppléments Lunettes à Moitié Prix !
```



```
Date: Sun, 2 Jun 2024 12:00:43 +0200 (CEST)
From: Votre opticien en ligne <update@email.opticien24.com>
Reply-To: update-embedded@email.opticien24.com
To: alain[REDACTED]@gmail.com
Message-ID: <oj8mb.lwxdfxvrs7ote8l@email.opticien24.com>
```



Vérification d'une URL

ASTUCES ET
CONSEILS



²
https://www.nomdusite.be/xyz

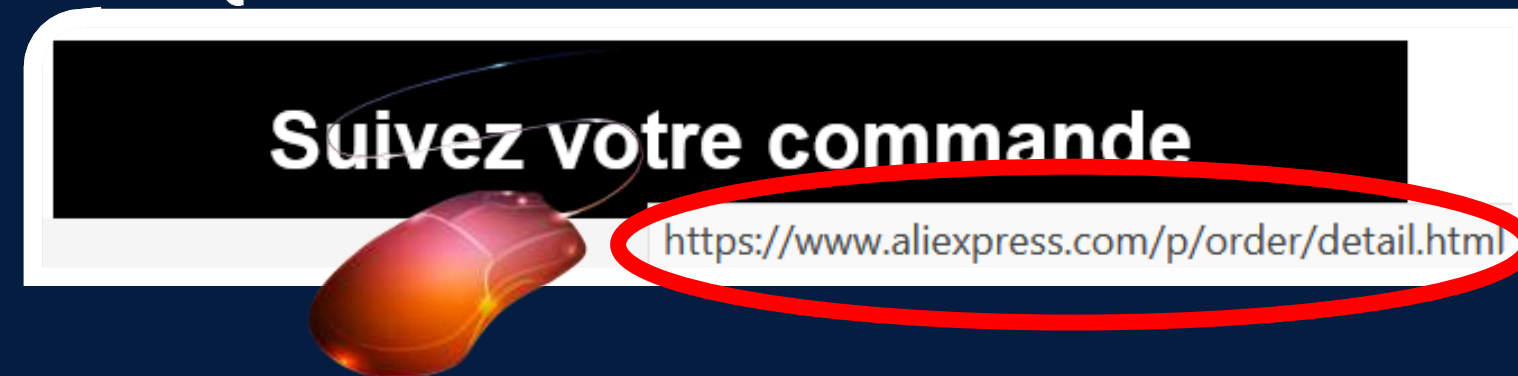
¹

Two hand-drawn green arrows. One arrow points from the number '1' to the path '/xyz'. The other arrow points from the number '2' to the domain 'www.nomdusite.be'.

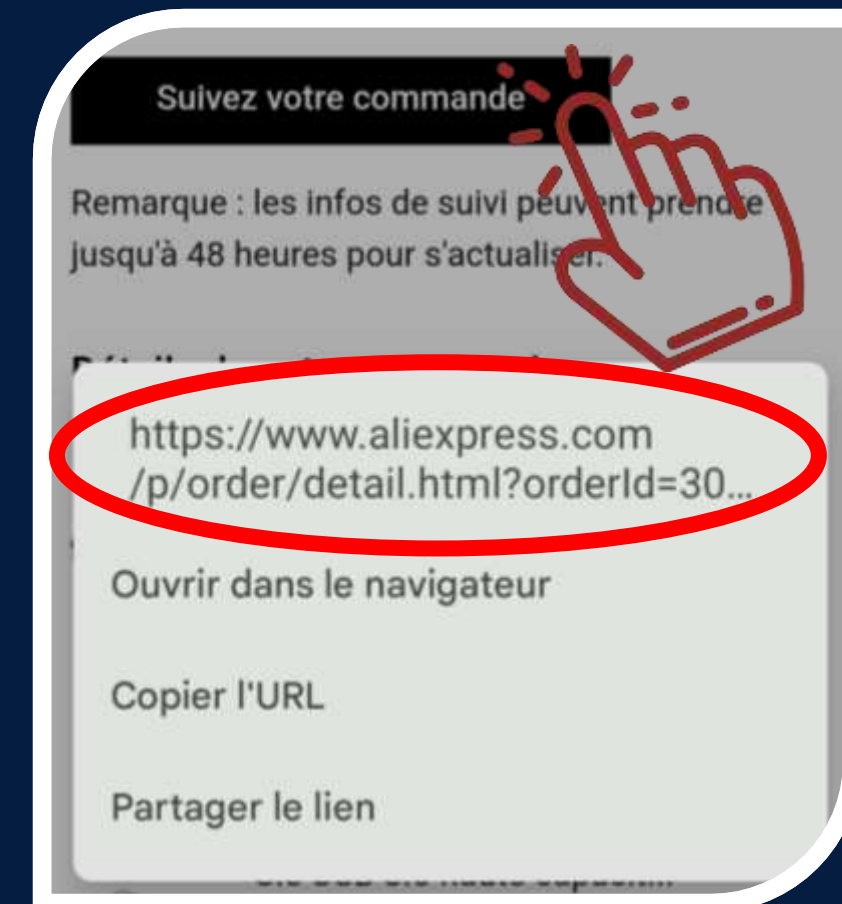
Vérification d'une URL

Avant de cliquer sur un lien, vérifiez l'URL

- Dans un SMS, l'URL apparaît entièrement
- Dans un mail ou sur une page web sur ordinateur, l'URL apparaît (dans le bas de votre écran) lorsque vous survolez un lien avec la souris



- Dans un mail ou sur une page web sur smartphone, l'URL apparaît lorsque vous appuyez longuement sur le lien



ASTUCES ET
CONSEILS



Vérification d'une URL

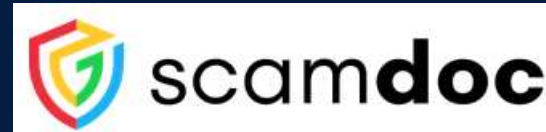
Et d'un nom de domaine

Des « outils » existent afin de vérifier la **fiabilité** et/ou les **données** concernant un **site internet** / **nom de domaine**

ASTUCES ET
CONSEILS



Des sites tels que



Des sites tels que



ou



pour un nom de domaine .be vous permettent d'obtenir les données d'enregistrement d'un site comme notamment sa **date de création** qui est toujours **suspecte si récente**





Vérification d'une URL

Et d'un nom de domaine

ASTUCES ET
CONSEILS



Recherche

aliexpress.com

Analyser

Analyse du site internet
"Aliexpress.com"



Score de confiance

Excellent

Vous pouvez y aller les yeux fermés !

Informations détaillées concernant
Aliexpress.com

Date 1ère analyse : 25/12/2018

Date de création du nom de domaine 16/04/2006 (Plus de 5 ans)
(Source)

Date d'expiration du nom de domaine 16/04/2025 (Moins d'un an restant)
(Source)

Le registrant du nom de domaine est identifié **partiellement** :

Identification du Propriétaire
(ou registrant) dans le Whois

Nom/Société ✗

Adresse postale ✗

Téléphone ✗

Mail ✓

Pays (Chine) ✓

(Voir les infos disponibles)

Avis négatifs détectés sur Internet



le 12 aout j'ai acheté sur aliexpress a la société ShanDisk Global Sales Store 2 clés USB en fer de taille d...

Avis des utilisateurs sur Scamdoc



(Note moyenne de 2.8 basée sur 13 Avis)

Laisser un avis



Vérification d'une URL

Et d'un nom de domaine

ASTUCES ET
CONSEILS



Recherche

vstrc20.com

Analyser

Analyses du site internet
"Vstrc20.com"

Informations détaillées concernant
Vstrc20.com

Date 1ère analyse : 09/05/2024

Score de confiance : **Très faible**

Réservé aux internautes très expérimentés

1%

Points positifs

- Un protocole de sécurité **HTTPS** a été **détecté** sur ce site internet. Attention, cet indicateur n'est pas systématiquement synonyme de sécurité !

Points négatifs

- Le nom du site a été **acquis très récemment** (moins de 6 mois)
- Le nom du domaine affiche **une faible espérance de vie**

Date de création du nom de domaine : 07/05/2024 (Moins de 6 mois)

Date d'expiration du nom de domaine : 07/05/2025 (Moins d'un an restant)

Identification du Propriétaire (ou registrant) dans le Whois

Le registrant du nom de domaine est identifié **partiellement** :

- Nom/Société ✗
- Téléphone ✗
- Pays (États-Unis) ✓
- Adresse postale ✗
- Mail ✗

Avis des utilisateurs sur Scamdoc

Actuellement **aucun avis** n'a été laissé concernant ce site internet.



Vérification d'une URL

Et d'un nom de domaine

ASTUCES ET
CONSEILS



vstrc20.com

Domain Information

Domain:	vstrc20.com
Registrar:	ALIBABA.COM SINGAPORE E-COMMERCE PRIVATE LIMITED
Registered On:	2024-05-07
Expires On:	2025-05-07
Updated On:	2024-05-07
Status:	ok
Name Servers:	cash.ns.cloudflare.com liberty.ns.cloudflare.com

Registrant Contact

State:	CA
Country:	US
Email:	https://whois.aliyun.com/whois/whoisForm

Raw Whois Data

```
Domain Name: vstrc20.com
Registry Domain ID: 2879010026_DOMAIN_COM-VRSN
Registrar WHOIS Server: grs-whois.aliyun.com
Registrar URL: http://www.alibabacloud.com
Updated Date: 2024-05-07T06:58:02Z
Creation Date: 2024-05-07T06:56:36Z
Registrar Registration Expiration Date: 2025-05-07T06:56:36Z
Registrar: ALIBABA.COM SINGAPORE E-COMMERCE PRIVATE LIMITED
Registrar IANA ID: 3775
Reseller:
Domain Status: ok https://icann.org/epp#ok
Registrant City:
Registrant State/Province: CA
Registrant Country: US
Registrant Email:https://whois.aliyun.com/whois/whoisForm
Registry Registrant ID: Not Available From Registry
Name Server: CASH.NS.CLOUDFLARE.COM
Name Server: LIBERTY.NS.CLOUDFLARE.COM
DNSSEC: unsigned
Registrar Abuse Contact Email: domainabuse@service.aliyun.com
Registrar Abuse Contact Phone: +86.95187
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>>Last update of WHOIS database: 2024-06-02T19:50:29Z <<<
```

Registrar = Bureau d'enregistrement

Registrant = Titulaire nom de domaine



Vérification d'une URL

Et d'un nom de domaine .be



ASTUCES ET
CONSEILS



dnsbelgium

Remplissez le nom de domaine dont vous cherchez les données

braine-lalleud.be

Montrer les données

Nom de domaine

Nom de domaine	braine-lalleud.be
Statut	Enregistré (Qu'est-ce que le statut d'un nom de domaine ?)
Enregistrement	31 mai 1996 1:00 CEST
Dernière mise à jour	2 mai 2024 12:36 CEST

Titulaire du nom de domaine

Statut de vérification	Non vérifié (Qu'est-ce que le statut de vérification ?)
Organisation	Adm. Com. de Braine l'Alleud
Langue	Anglais
Adresse	Grand-Place Baudouin 1er 3 1420 Braine-l'Alleud Belgique



Signaler un faux site ou une fausse annonce

ASTUCES ET
CONSEILS



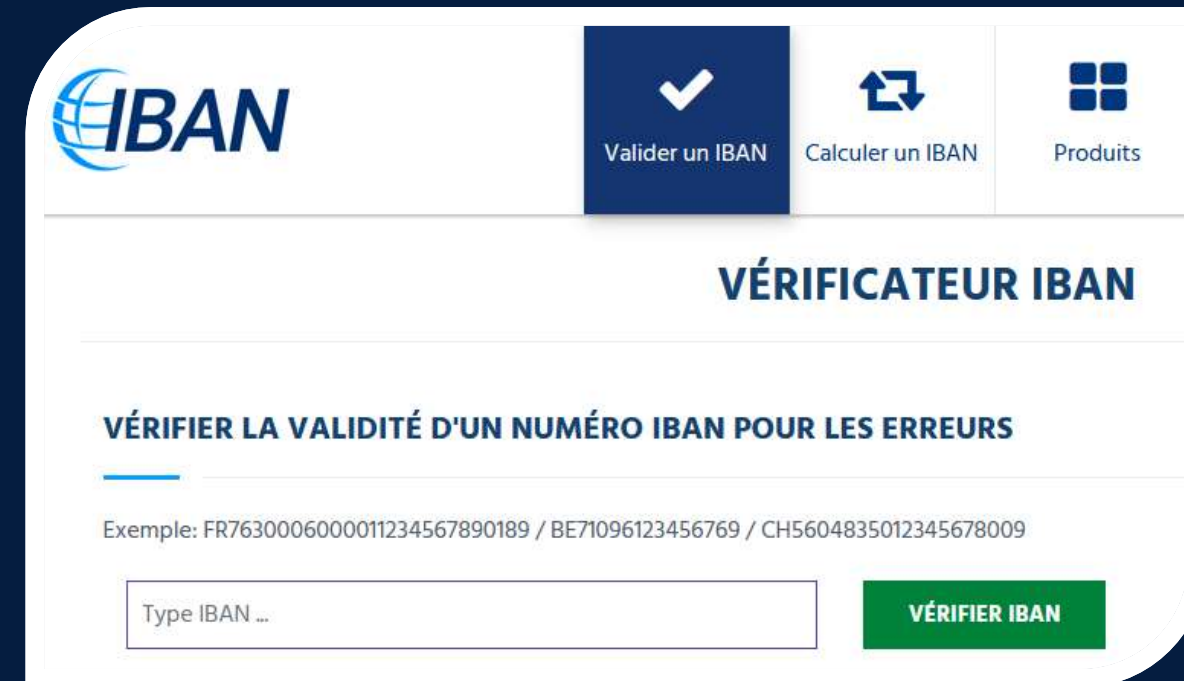
Signalements

- S'il s'agit d'un faux **site .be**, contactez [DNS Belgium](#)
- S'il s'agit d'un faux **site autre que .be**, contactez le **Registrar** (*bureau ou l'agent d'enregistrement*) via son adresse **abuse@...**
- S'il s'agit d'une **fausse annonce** mais que le **site** est **réel** (*2ememain, AutoScout24,...*), contactez le site ou le réseau social concerné
- Partagez vos expériences sur des sites comme [Signal-Arnaques](#)



Vérification d'un n° de compte

<https://fr.iban.com/iban-checker>



The image shows the French version of the IBAN checker website. At the top, there is a navigation bar with the IBAN logo, a 'Valider un IBAN' button with a checkmark icon, a 'Calculer un IBAN' button with a refresh icon, and a 'Produits' button with a grid icon. Below this is a section titled 'VÉRIFICATEUR IBAN'. Underneath, it says 'VÉRIFIER LA VALIDITÉ D'UN NUMÉRO IBAN POUR LES ERREURS'. An example of an IBAN is provided: 'Exemple: FR7630006000011234567890189 / BE71096123456769 / CH5604835012345678009'. There is a text input field labeled 'Type IBAN ...' and a green button labeled 'VÉRIFIER IBAN'.



https://www.ibancalculator.com/iban_validieren.html



The image shows the German version of the IBAN calculator website. At the top, it says 'Check IBAN / show more information'. Below this, it says 'To check whether an IBAN is correct, please enter it here:'. There is a label 'IBAN:' followed by a text input field. At the bottom, there is a blue button labeled 'validate IBAN, look up BIC'.



ASTUCES ET
CONSEILS



Vérification d'un n° de compte

ASTUCES ET
CONSEILS



Check IBAN / show more information

You entered:

IBAN to check: BE08964001007213

Checks

- ✓ This IBAN has the correct length for this country (Belgium).
- ✓ Bankleitzahl (bank code) 964: This Bankleitzahl (bank code) is correct.
- ✓ Account number 964001007213: The account number contains a valid checksum.
- ✓ IBAN BE08964001007213: The IBAN checksum is correct.

Result

This is a valid IBAN.

IBAN: BE08964001007213 [IBAN into the clipboard](#)

BIC: FPEBBEB2 [BIC into the clipboard](#)

Bank: FINANCIERE DES PAIEMENTS ELECTRONIQUES SAS - NICKEL BELGIUM

SEPA Credit Transfer is supported.

SEPA Direct Debit is supported.

B2B is *not* supported.

SEPA Instant Credit Transfer is supported.

Data valid as of: 8. 2. 2024 (February 8, 2024).



Nickel

<https://www.nickel.eu>



Nickel : Compte de proximité - Compte en librairie

Nickel, c'est 1 Compte + 1 Carte, pour payer et être payé en toute simplicité. Avec **Nickel**, profitez d'une carte de Débit Mastercard pour seulement 20€/an. Utile. Ouvert à Tous.

Vérification d'un n° de compte

Check IBAN / show more information

You entered:

IBAN to check: FR7616908000010200285053339

Checks

- ✓ This IBAN has the correct length for this country (France).
- ✓ Account number 02002850533: The account number contains a valid checksum
- ✓ Bankleitzahl (bank code) 16908: This Bankleitzahl (bank code) is correct.
- ✓ IBAN FR7616908000010200285053339: The IBAN checksum is correct.

Result

This is a valid IBAN.

IBAN: FR7616908000010200285053339

BIC: LBDIFRP1

Bank: MA FRENCH BANK

3 RUE PAUL DUEZ
59800 LILLE

Branch number: 00001

AG SIEGE SOCIAL

SEPA Credit Transfer is supported.

SEPA Direct Debit is supported.

B2B is *not* supported.

SEPA Instant Credit Transfer is *not* supported.

Data valid as of: 27. 5. 2024 (May 27, 2024).

Aussi pour un n° de compte étranger



La Banque Postale

<https://www.labanquepostale.fr> > comptes-et-cartes > m...



Ma French Bank - Banque en Ligne 100% Mobile

Ma French Bank est une banque digitale accessible, ouverte à tous, sans conditions de ressources. Une expérience 100 % mobile et des services utiles au ...



FR7616908000010200285053339



Aucun document ne correspond aux termes de recherche spécifiés (FR7616908000010200285053339).



FR76 1690 8000 0102 0028 5053 339



Signal-Arnaques

<https://www.signal-arnaques.com> > scam > view

IBAN: FR76 1690 8000 0102 0028 5053 339

3 mai 2020 — Voici mes informations bancaires: Nom: MESGUEN Prénom: CLAUDE IBAN: FR76 1690 8000 0102 0028 5053 339 BIC: LBDIFRP1XXX Une fois le virement ...



Signal-Arnaques

<https://www.signal-arnaques.com> > scam > view

Arnaque site annonce FR76 1690 8000 0102 0029 0092 392

17 mai 2020 — Bonjour, En ce qui me concerne, il a piraté ma boîte mail et a envoyé des demandes de virement à ma banque ! Vigilance !! Grosse arnaque.

ASTUCES ET
CONSEILS



MATÉRIEL INFORMATIQUE ET INTERNET

ASTUCES ET
CONSEILS



LES BONNES PRATIQUES POUR SE PROTÉGER

ASTUCES ET
CONSEILS



- Procédez aux **mise**s à **jour** du matériel et des logiciels
- **Eteignez vos appareils** tous les jours
- Utilisez un **antivirus**
- Utilisez uniquement des applications et des **programmes sûrs**
- **Limitez les accès** accordés (localisation, contacts, caméra,...) et uniquement lorsque vous en avez besoin
- N'acceptez de préférence que les **cookies essentiels**
- Utilisez éventuellement les **extensions** de votre navigateur pour **supprimer les cookies** (et les publicités)

LES BONNES PRATIQUES POUR SE PROTÉGER

ASTUCES ET
CONSEILS



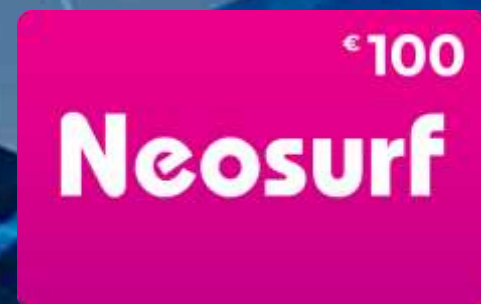
- Supprimez régulièrement les **applications que vous n'utilisez pas**
- Utilisez régulièrement un **nettoyeur** (style Ccleaner ou d'origine)
- Choisissez des **mots de passe** différents et complexes qui n'ont pas de liens directs avec vous. Gardez-les si nécessaire dans une application style KeePass.
- Si possible, choisissez l'**authentification à deux facteurs**
- Activez le **verrouillage automatique** en cas d'inactivité
- En présence d'autres personnes, soyez **discret** lorsque vous introduisez vos codes et mots de passe
- **Evitez le dessin pour déverrouiller** votre smartphone ou du moins les traces laissées sur l'écran

LES BONNES PRATIQUES POUR SE PROTÉGER

ASTUCES ET
CONSEILS



- Méfiez-vous des **offres** alléchantes, **trop belles** pour être vraies
- N'achetez et n'introduisez des données confidentielles que sur des **sites officiels** avec cadenas commençant par **https://**  https://
- Méfiez-vous des personnes qui revendent des **places de concert**
Privilégiez les sites officiels et en cas de revente des personnes que vous connaissez
- Ne payer pas des personnes inconnues via **Western Union, Neosurf, PaysafeCard**,... ou des **applications** qui vous sont inconnues

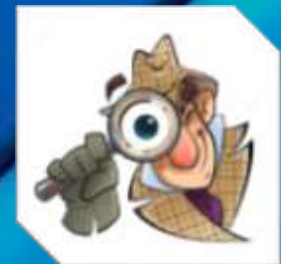


LES BONNES PRATIQUES POUR SE PROTÉGER

ASTUCES ET
CONSEILS



- Vérifiez les **URL des sites consultés** (orthographe, extension,...)
Attention aux caractères (I (i majuscule) au lieu de l (L minuscule),
rn au lieu de m,...)
- Vérifiez la **fiabilité des sites** via
<https://fr.scamdoc.com/>,
<https://franceverif.fr/fr/verifier-site-web> ou
<https://antidrop.fr/>
- Vérifiez si nécessaire les URL ou noms de domaine via des sites
tels que <https://whois.domaintools.com> et
<https://www.whois.com/whois/>.
Un **site créé récemment** est généralement suspect.
- Vérifiez les **avis des autres acheteurs** (sur les sites
mais également dans les moteurs de recherche)

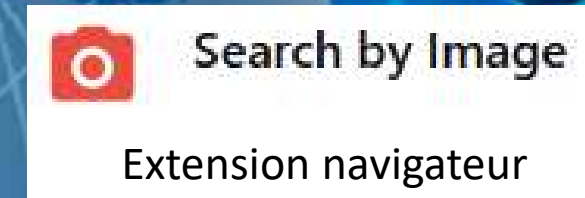
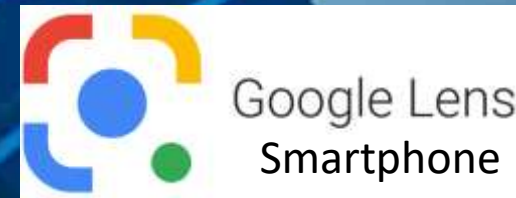


LES BONNES PRATIQUES POUR SE PROTÉGER

ASTUCES ET
CONSEILS



- Vérifiez les **coordonnées** présentes sur les sites de vente en ligne (localisation, n° de TVA, conditions générales,...)
- Vérifiez si les **images** ne proviennent pas d'un autre site (fausse location pour les vacances, fausse vente de voiture,...)



- Soyez très prudent lorsque vous utilisez un réseau **Wi-Fi public** non sécurisé. Si possible, utilisez plutôt vos données mobiles.
- Méfiez-vous également du **matériel mis à votre disposition**.
- Effectuez des **copies de vos fichiers** importants (back-ups) ce qui sera bien utile si vous devez réinitialiser vos appareils.

LES BONNES PRATIQUES POUR SE PROTÉGER

- Faites très **attention à ce que vous publiez sur internet** (réseaux sociaux, avis concernant vos achats,...)

ASTUCES ET
CONSEILS



facebook

Vincent Matalon

Profil <https://www.facebook.com/...>

Date d'inscription lundi 28 mai 2007, 22:13 UTC+02

Emails [\(E-mail précédent\)](#) [\(E-mail précédent\)](#)

Profil

- Coordonnées
- Journal
- Photos
- Vidéos
- Amis
- messages
- Pokes
- Événements
- Sécurité
- Publicités
- Applications

Adresse

Quartier

Téléphones [\(Mobile\)](#)

Date de naissance

Sexe Homme

Lieu de résidence Paris

Relations précédentes

Formation Sciences Po Aix

Workplace Franceinfo juillet 2011 - Journaliste

Fanny Dujoux de Braine-l'Alleud ★★★★★ 5/5

Super contente de ma nouvelle PS 5 !!!
Commande reçue rapidement malgré les jours fériés.

 se sent chanceuse
avec  à **Bahia Principe Sunlight Costa Adeje.**
12 mars · Adeje, Canarias, Spain ·



On vous envoie du bleu... que du bleu
   

    +6

   74

28 commentaires

LES BONNES PRATIQUES POUR SE PROTÉGÉR

ASTUCES ET
CONSEILS



- Pensez à configurer vos **paramètres de confidentialité** (réseaux sociaux, sites, navigateurs)

Sélectionnez l'audience

- ☒ **Public**
Tout le monde sur ou en dehors de Facebook
- ☐ **Amis**
Vos amis sur Facebook
- ☐ **Moi uniquement**
- ☐ **Personnalisé**
Incluez et excluez des amis et des listes
- ☐ **Amis proches**
Votre liste personnalisée
- ☐ **Collègues**
Votre liste personnalisée

Vie privée

Protection renforcée contre le pistage



Les traqueurs vous suivent en ligne pour collecter des informations sur vos habitudes de navigation et vos centres d'intérêt. Firefox bloque un grand nombre de ces traqueurs et de scripts malveillants. [En savoir plus](#)

Gérer les exceptions...

☒ Standard

Équilibré entre protection et performances. Les pages se chargeront normalement.

Firefox bloque les éléments suivants :

- Traqueurs de réseaux sociaux
- Cookies intersites dans toutes les fenêtres
- Contenu utilisé pour le pistage dans les fenêtres de navigation privée
- Mineurs de cryptomonnaies
- Détecteurs d'empreinte numérique

Inclut la protection totale contre les cookies, notre fonctionnalité de protection de la vie privée la plus puissante

La protection totale contre les cookies restreint les cookies au site sur lequel vous vous trouvez et les traqueurs ne peuvent donc pas s'en servir pour vous pister de site en site. [En savoir plus](#)

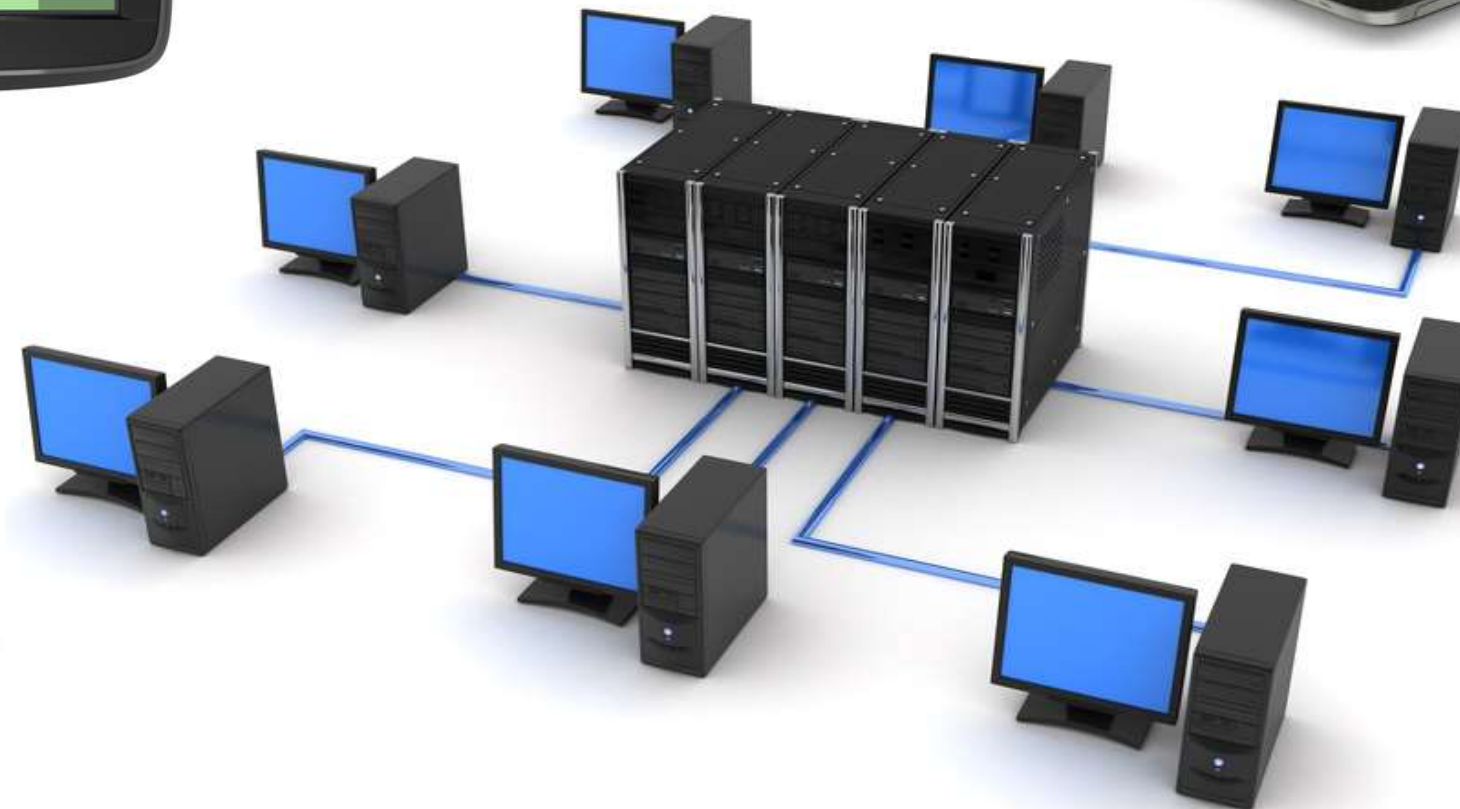
☐ Stricte

Protection renforcée, mais certains sites ou contenus peuvent ne pas fonctionner correctement.

☐ Personnalisée

Choisissez les traqueurs et les scripts à bloquer.

MATÉRIEL INFORMATIQUE ET INTERNET



MATÉRIEL INFORMATIQUE

ET INTERNET



De plus en plus d'objets connectés !!!

VICTIME ? QUE FAIRE IMMÉDIATEMENT ?



VICTIME ? QUE FAIRE IMMÉDIATEMENT ?

- Faites des **captures** ou, si ce n'est pas possible, prenez des **photos** des **transactions frauduleuses** sur vos comptes
- Notez les **n° de comptes et de cartes** concernés
- Prévenez immédiatement **Card Stop** (078 170 170 ou Appli) ainsi que votre **banque** (et si ça s'applique American Express ou Worldline / macarte.be)
- Si vous avez fourni une copie de votre document d'identité belge, afin d'éviter tout usage frauduleux, prévenez **Doc Stop** (00800 2123 2123), comme si le document avait été perdu



VICTIME ? QUE FAIRE IMMÉDIATEMENT ?

- Transférez le mail suspect ou une capture d'écran du SMS suspect à suspect@safeonweb.be
- Supprimez le **SMS** suspect uniquement si vous êtes certain d'en avoir une **capture d'écran** complète avec son horodatage (*sinon demandez à quelqu'un d'expérimenté*)
- Supprimez le **mail** suspect uniquement si vous êtes certain d'en avoir une **sauvegarde complète avec son en-tête technique en version numérique** (copier/coller) (*sinon demandez à quelqu'un d'expérimenté*)
- Mettez en garde **vos proches** qui seraient également destinataires du message suspect



VICTIME ? QUE FAIRE IMMÉDIATEMENT ?



- Faites des **captures** des **sites**, réseaux sociaux ou annonces concernés ainsi que des **données liées au(x) suspect(s)**.
- Effectuez un **scan antivirus** sur vos appareils qui pourraient être infectés.
Si un problème est détecté, faites une capture d'écran avant d'y remédier.
- **Changez les mots de passe** que vous auriez communiqués (et ce depuis un appareil « sain »)
- Le cas échéant, ne touchez plus à votre matériel avant qu'il soit vérifié si des **traces exploitables** par la police sont toujours présentes





VICTIME ? N° UTILES ?



Card Stop Online

Bloquer vos cartes de débit et de crédit en ligne en cas de perte ou de vol.

[Bloquer des cartes](#)

Signaler une fraude

Transaction suspecte, carte volée, réception d'un appel ou d'un SMS vous demandant vos données bancaires? Alors vous avez peut-être été victime d'une fraude. Prenez quelques précautions pour protéger vos finances et vos moyens de paiement.

[Continuer](#)

← Card Stop



Comment bloquer vos cartes?

- Sélectionnez les cartes que vous voulez bloquer.
- Indiquez la raison.
- Vos nouvelles cartes seront créées automatiquement. Choisissez l'adresse où vous souhaitez les recevoir.

[BLOQUER DES CARTES](#)

← Card Stop

Carte bloquée!

Cette carte a été bloquée avec succès. Votre nouvelle carte sera créée automatiquement. Cliquez sur 'suivant' et choisissez l'adresse où vous souhaitez la recevoir.



CARTE BANCAIRE

6703 0510 0169 1100

ROBERT/SCHUMAN

[SUIVANT](#)



VICTIME ? N° UTILES ?

Votre banque

- Argenta
- Axa
- Bank de Kremer
- Banque Van Breda
- Banx
- Belfius
- Beobank
- BNP Paribas Fortis
- bpost bank
- CBC
- CPH
- Crelan
- Deutsche Bank
- Europabank
- Fintro
- Hello Bank
- ING
- KBC
- Keytrade Bank
- Medirect
- Nagelmackers
- Triodos
- vdb bank

Pendant les heures d'ouverture

- 03 285 53 33
- 03 286 66 55
- 03 294 23 09
- 03 217 52 00
- 02 222 91 00
- 02 222 46 00
- 02 622 20 00
- 02 762 20 00
- 02 278 50 32
- 016 43 20 00
- 078 170 170*
- 02 558 78 88
- 02 551 99 98
- 09 224 76 90
- Votre agence
- 02 433 41 42
- 02 464 60 60
- 016 43 20 00
- 02 679 90 00
- 02 518 00 00
- 078 170 170*
- 02 548 28 00
- 09 267 33 31

En dehors des heures

- 03 285 53 33
- 03 286 66 55
- 03 217 52 00
- 03 217 52 00
- 02 222 91 00
- 02 222 46 00
- 078 170 170*
- 02 433 43 75
- 02 278 50 32
- 016 43 20 00
- 078 170 170*
- 02 558 78 88
- 02 551 99 98
- 09 224 74 07
- 02 433 43 75
- 02 433 43 75
- 02 464 60 60
- 016 43 20 00
- 02 679 90 00
- 02 518 00 01
- 078 170 170*
- 02 548 28 00
- 078 170 170*

Liste
disponible
sur le site
Card Stop





VICTIME ? N° UTILES ?

Carte d'identité, passeport ou titre de séjour belge
perdu ou volé ?

Copie transmise à des escrocs ?



00800 2123 2123

+32 2 518 2123



VICTIME ? N° UTILES ?

Appelez le **101**
pour une aide urgente de la police en Belgique

Appelez le **112** dans toute l'Europe

Pensez à installer l'application **112 BE**

App 112 BE

Besoin d'une aide urgente en Belgique ?

Vous pouvez aussi contacter les Centrales d'urgence via App.



1

Télécharger

Allez dans ou Store.
Cherchez " 112 BE ".
Téléchargez et installez l'app.

2

S'enregistrer

Complétez votre nom,
vos coordonnées et
informations
supplémentaires.

3

Appeler

Utilisez l'App en Belgique si
vous avez besoin d'urgence
de l'aide des pompiers,
d'une ambulance ou de
la police.





VICTIME ? N° UTILES ?

Plainte ou intervention non urgente ?



Zone de Police de Braine-l'Alleud



02/389.44.00

Avenue Albert 1^{er} n° 117



VICTIME ? N° UTILES ?

Ombudsman.be
Le Réseau belge des ombudsmans



Ombudsfina

Jean CATTARUZZA, Ombudsman

North Gate II
Boulevard du Roi Albert II, n° 8 bte. 2
1000 Bruxelles
Téléphone: 02 545 77 70
E-mail: ombudsman@ombudsfina.be



**Médiateur pour les
télécommunications**

David WIAME

Boulevard du Roi Albert II 8 bte 3
1000 Bruxelles
Téléphone: 02 223 06 06
E-mail: plaintes@mediateurtelecom.be



LES ÉLÉMENTS UTILES POUR LA POLICE ?



ÉLÉMENTS UTILES POUR LA POLICE ?

- Le(s) **numéro(s) de(s) compte(s) bancaire(s)** et éventuellement **de carte(s) concerné(s)**
- Une **copie de vos extraits de comptes** reprenant les transactions frauduleuses
- Les **messages ou courriers échangés** avec votre banque
- Des captures d'écran de votre **journal des appels** reprenant les communications liées aux faits
- Des captures d'écran des **SMS reçus ou échangés** avec le(s) suspect(s)



ÉLÉMENTS UTILES POUR LA POLICE ?

- Si possible en version numérique, le(s) **email(s) suspect(s) reçu(s) avec leur en-tête technique**
(Généralement repris dans les propriétés du message ou dans ses options : Afficher l'original - Afficher la source...)
- Des **captures d'écran** du **site** internet ou réseau social concerné ainsi que des **données liées au(x) suspect(s)**
- Une **copie** de la publication ou de l'**annonce** concernée
(+ n° éventuel)
- Tout autre document ou **élément** qui vous paraît utile



Envie d'en savoir plus, de connaître les nouvelles arnaques ?



Consultez notamment les sites
<https://safeonweb.be> et



[https://economie.fgov.be/fr/themes/protection-
des-consommateurs/stop-arnaques](https://economie.fgov.be/fr/themes/protection-des-consommateurs/stop-arnaques)

**PRÉVENTION CONTRE
LES VOLS DANS HABITATIONS
ET LES ESCROQUERIES
DONT LA CRIMINALITÉ INFORMATIQUE**

DES QUESTIONS?

- Merci pour votre attention -

Karin Marique

Service d'Assistance Policière aux Victimes

Service Prévention Vols

Zone de Police de Braine-l'Alleud

Tél : 02.389.44.07

karin.marique@police.belgium.eu

