# A l’abordage des pirates du web

Pierre Delporte
19/03/2026

# Agenda

- Qui suis-je
- Quelles sont les menaces courantes
- Dans la peau d’un hacker et d’une victime
- Comment reconnaître une menace
- Les bonnes pratiques

# Qui suis-je

- Pierre Delporte – ALF-Solution
- Membre de l’équipe CISO chez Infrabel (Deputy-CISO)
- Responsable de la sécurisation des « End-points »
- Responsable de la gestion des Incidents de sécurité (CSIRT Coordinator)
- Membre du CECI de Villers-la-Ville
- Mais aussi, là pour vous aider

# Quelles sont les menaces courantes

**Phishing et hameçonnage**

Le phishing utilise des emails, SMS et appels frauduleux pour dérober des informations sensibles et compromettre la sécurité des utilisateurs.

**Piratage et rançongiciels**

Le piratage des comptes expose les données personnelles, tandis que les rançongiciels bloquent l'accès et exigent une rançon.

**Arnaques et virus**

Les arnaques au faux support, virus et spams exploitent la confiance pour voler des informations ou installer des logiciels malveillants.

- Violation de données personnelles
- Piratage des comptes en ligne
- Arnaque au faux support technique
- Rançongiciels ou ransomwares
- Phishing ou hameçonnage (+ sms + appel)
- Spams
- Faux ordres de virement
- Arnaque aux sentiments
- Fraude à l'investissement

# Violation de données personnelles

- 🔒 **Qu’est-ce qu’une violation de données personnelles ?**
- Une **violation de données personnelles** se produit lorsque des informations privées sont **volées, divulguées ou utilisées sans autorisation** à la suite d’un piratage ou d’une négligence de sécurité.
- Dans le cadre des **arnaques en ligne**, ces données deviennent une **matière première pour les fraudeurs**.

# Violation de données personnelles : Quoi ? Comment ? Pourquoi ?

📂 **Quelles données sont concernées ?**

- Les informations volées peuvent inclure :
- Nom, prénom, adresse, date de naissance
- Adresse email et numéro de téléphone
- Identifiants et mots de passe
- Données bancaires ou numéros de carte
- Copies de documents (carte d'identité, passeport)
- Habitudes de connexion ou d'achat

👉 Même une **simple adresse email** a de la valeur pour un escroc.

🎯 **Comment ces données sont obtenues ?**

- Les violations de données surviennent notamment via :
- Piratage de sites ou de bases de données mal sécurisées
- Campagnes de phishing ou faux formulaires
- Logiciels malveillants installés à l'insu de l'utilisateur
- Fuites de données revendues sur Internet

➡️ La victime n'est souvent **pas consciente** que ses données aient été compromises.

💥 **À quoi servent ces données pour les arnaqueurs ?**

- Une fois les données en circulation, elles servent à :
- Personnaliser des arnaques (emails, SMS, appels très crédibles)
- Usurper l'identité de la victime
- Accéder à d'autres comptes (effet domino)
- Préparer des fraudes financières ou administratives

# Comment les comptes en ligne sont piratés

**Ce n’est pas une faille informatique,**
**c’est une faille humaine.**

### 🎧 1. Tromper la victime

Email, SMS ou appel se faisant passer pour un service officiel
(Banque, colis, Microsoft, administration…)

### 🔑 2. Vol des identifiants

- Mot de passe saisi sur un faux site
- Code de validation (SMS / app)
- Mot de passe déjà utilisé ailleurs (fuite de données)

### 🔒 3. Prise de contrôle du compte

Le pirate se connecte comme vous
→ change le mot de passe
→ bloque le vrai propriétaire

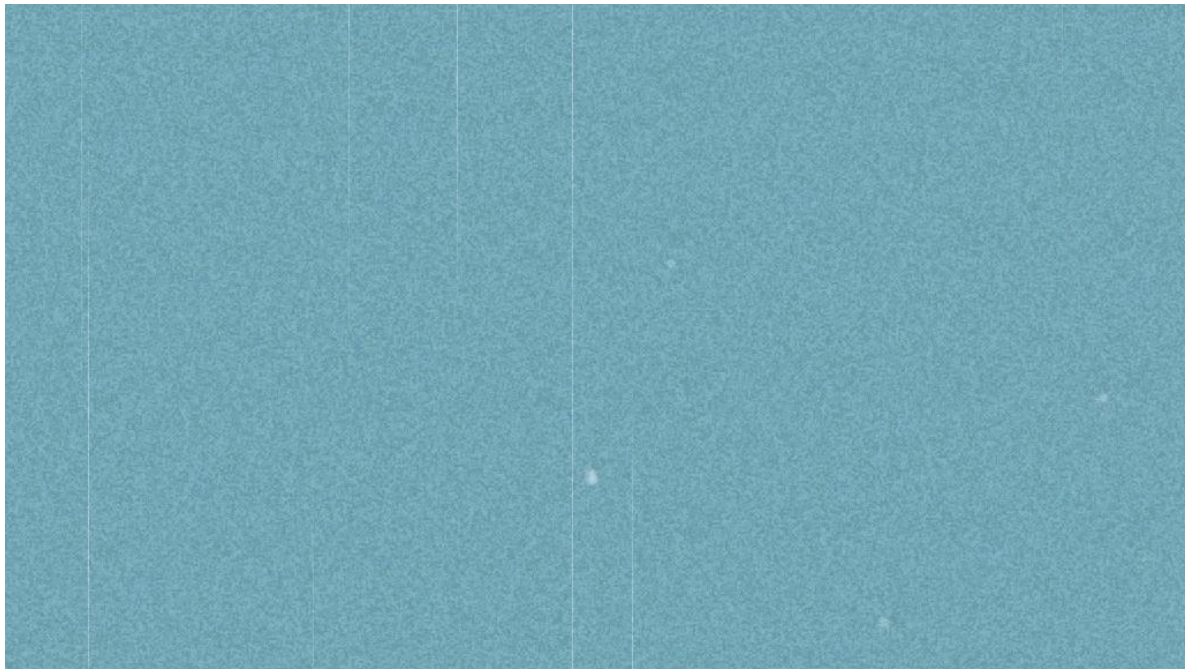
### 💥 4. Exploitation

- Vol d’argent ou de données
- Usurpation d’identité
- Accès à d’autres comptes via l’email

# Dans la peau ...

d’un hacker

d’une victime




# Arnaque au faux support technique

🥉 **3e arnaque la plus fréquente**

🖥️ **Comment fonctionne l'arnaque ?**

🚨 **1. Message alarmant**
Un message bloque l'écran et annonce un **grave problème de sécurité**
(*virus détecté, ordinateur infecté, données en danger…*)

📞 **2. Faux support "officiel"**
La victime est incitée à **appeler un numéro** se faisant passer pour Microsoft, Apple, un fournisseur Internet, etc.

💳 **3. Faux dépannage payant**
Le faux technicien rassure… puis demande de payer un **pseudo-dépannage inutile ou inexistant**

🎯 **Qui est le plus ciblé ?**

- 👵 **Seniors** peu à l'aise avec l'informatique
- 👨💼 **Professionnels** sans support IT de proximité

# Rançongiciels ou ransomwares

🛑 **Le rançongiciel : comment ça fonctionne ?**

1️⃣ **Infection**
→ Email, lien ou pièce jointe piégée

2️⃣ **Blocage**
→ Les fichiers sont chiffrés, l'ordinateur devient inutilisable

3️⃣ **Rançon**
→ Message alarmant demandant un paiement

4️⃣ **Conséquences**
→ Données bloquées, activité à l'arrêt, stress

🎯 **Qui est ciblé ?**
- Particuliers
- PME et indépendants
- Grandes organisations

➡️ **Tout le monde peut être touché**


# Comprendre le faux ordre de virement

**Usurpation d’identité**

Les fraudeurs se font passer pour un responsable afin de tromper la victime et obtenir un transfert d’argent non autorisé.

**Manipulation psychologique**

Des techniques de manipulation psychologique sont souvent utilisées pour inciter la victime à agir rapidement et sans réflexion.

**Prévention et vigilance**

La vérification des instructions et la sensibilisation des employés sont essentielles pour éviter ce type de fraude.

# La fraude au président (ou CEO fraud)

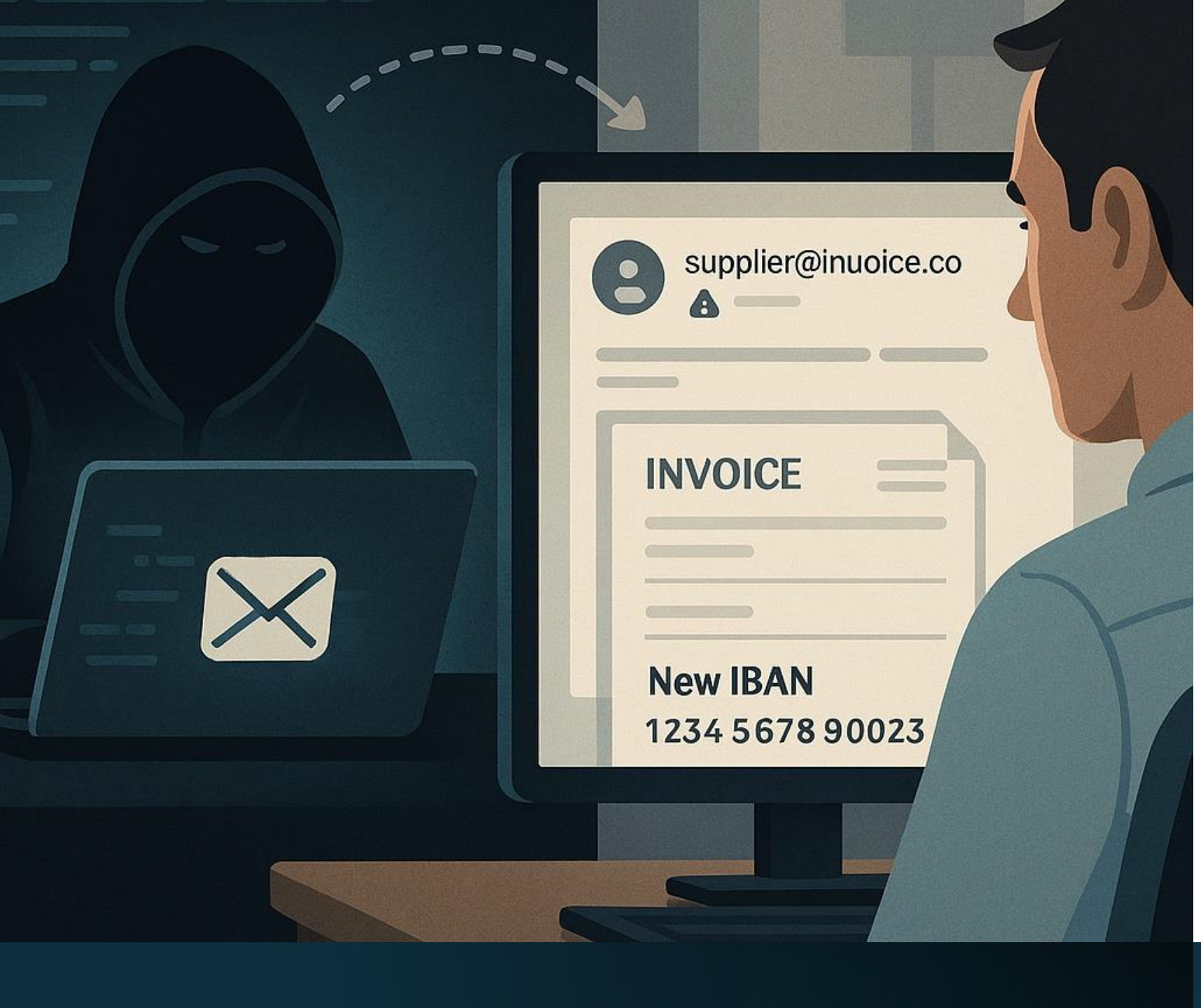
C'est l'exemple le plus connu ciblant les entreprises.

**Scénario :** Un escroc se fait passer pour un dirigeant de l'entreprise (PDG, directeur financier) et contacte un employé (souvent du service comptabilité) par e-mail ou téléphone.

**Pression exercée :** L'escroc invoque une opération financière "urgente" et "hautement confidentielle" (par exemple, une acquisition secrète, un audit important) nécessitant un virement immédiat vers un compte étranger.

**Conséquence :** L'employé, sous la pression de la hiérarchie et de l'urgence, exécute le virement sans les vérifications d'usage, et les fonds sont perdus.

**Se prémunir :** Parlez-en avec une personne de confiance de l’entreprise, l’urgence, dans ce cas est rarement une vérité.




# L'arnaque au faux fournisseur

Cette fraude cible également les entreprises en détournant les paiements destinés aux créanciers.

**Scénario :** L'escroc intercepte des communications ou pirate la boîte e-mail d'un fournisseur légitime. Il envoie ensuite une fausse demande de changement de coordonnées bancaires (IBAN) à l'entreprise cliente, prétextant une modification de banque ou une erreur administrative.

**Conséquence :** Les paiements futurs dus au fournisseur sont transférés sur le compte bancaire contrôlé par le fraudeur.

**Se prémunir** : Contactez le fournisseur par téléphone et demandez confirmation de la modification

# L'arnaque au virement de salaire

Les employés peuvent aussi être victimes.

**Scénario :** Un escroc se fait passer pour un employé auprès du service des ressources humaines (RH) ou de la paie et demande, via un e-mail frauduleux, de modifier son RIB pour les prochains virements de salaire.

**Conséquence :** Le salaire de l'employé est versé sur le compte de l'escroc.

**Se prémunir :** Contacter l’employé par téléphone ou via son adresse mail professionnel


# L'arnaque à l'irlandaise (pour les particuliers)

Ce scénario vise les particuliers qui veulent aider quelqu'un.

**Scénario :** Une personne accoste une victime potentielle dans la rue, prétextant avoir été volée (papiers, portefeuille) et avoir besoin d'argent liquide pour un hôtel ou un billet de retour. En échange, elle propose de faire un virement immédiat sur le compte de la victime, montrant une fausse confirmation sur une application bancaire frauduleuse.

**Conséquence :** La victime, faisant confiance, retire l'argent et le donne à l'escroc, mais le virement promis n'arrive jamais car il était fictif.

**Se prémunir** : redirigez là vers la police

# Identifier un courriel frauduleux

**Failles dans le contenu**

Les courriels frauduleux comportent souvent des fautes d'orthographe ou des adresses électroniques suspectes, ce qui doit éveiller la vigilance.

**Demandes urgentes d'informations**

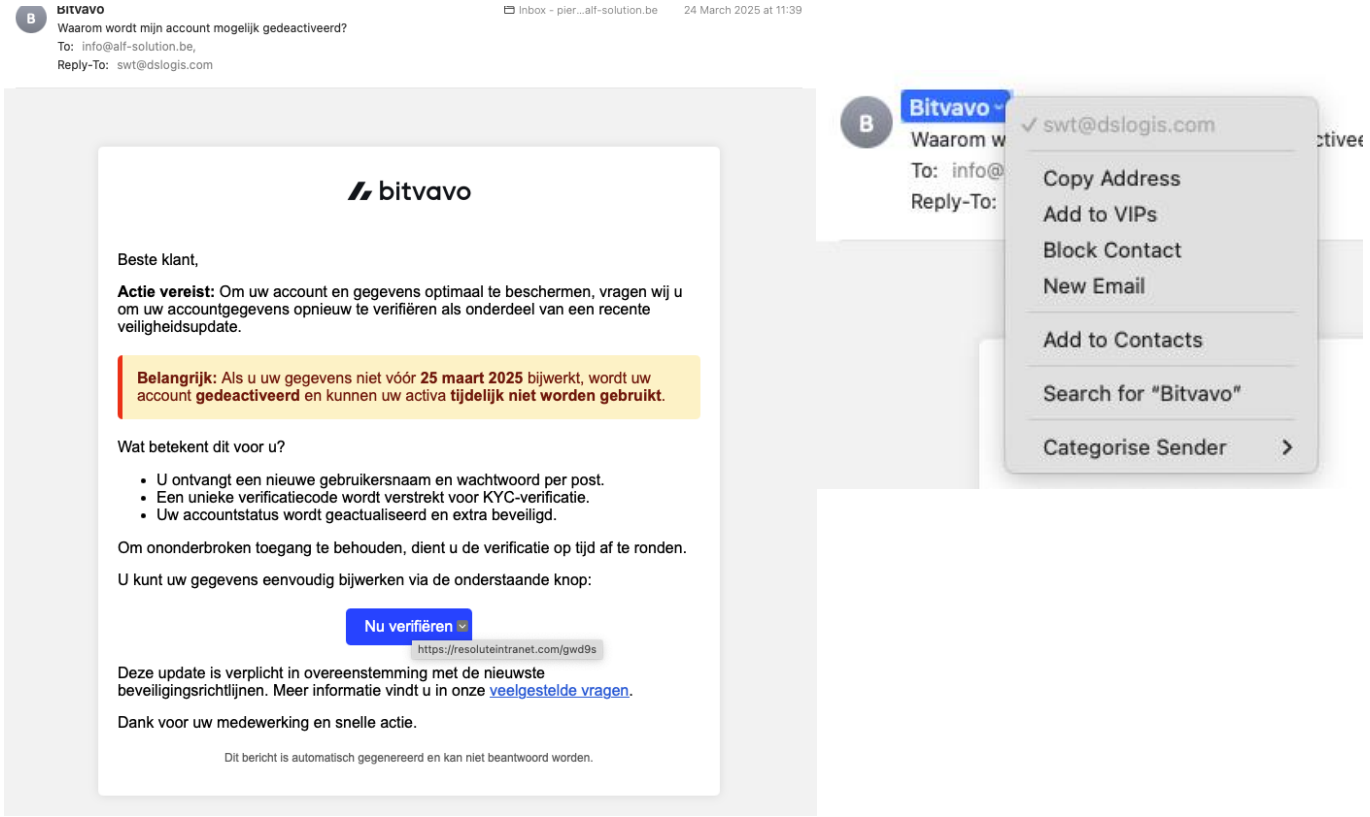
Un courriel frauduleux peut demander des informations personnelles telles que des mots de passe ou des données bancaires de manière pressante.

**Liens et pièces jointes suspects**

Un message frauduleux incite souvent à cliquer sur un lien non officiel ou à ouvrir une pièce jointe inconnue.

# Comment reconnaître un mail frauduleux ?

- Langue ?
- Est-ce que vous connaissez ?
- Adresse mail de l'expéditeur
  - swt@dslogis.com
- url de destination
  - https://resoluteintranet.com/gwd9s
- **Attention ne cliquez pas sur les liens !**
- Ne répondez pas au mail
- Consulter le site officiel
- Vérifier les liens avec un outil




# Exemple de phishing

- Expéditeur :
- contact-emvmqc3gzd@concessionariaunica.com

- Lien :
- http://iazd36rewe.pieczatki-olsztyn.pl/?id=alf-solution.be

Cher client Alf solution,

Nous tenons à attirer votre attention sur le fait que la facture n° FR8549865 n'a pas encore été réglée. Il est impératif que ce paiement soit effectué promptement pour garantir le renouvellement de votre domaine alf-solution.be.

Pour éviter toute interruption ou désactivation de votre domaine, nous vous encourageons à procéder au paiement immédiatement. Vous pouvez régler votre facture en toute sécurité par carte de crédit via le lien ci-dessous :

Payez votre facture

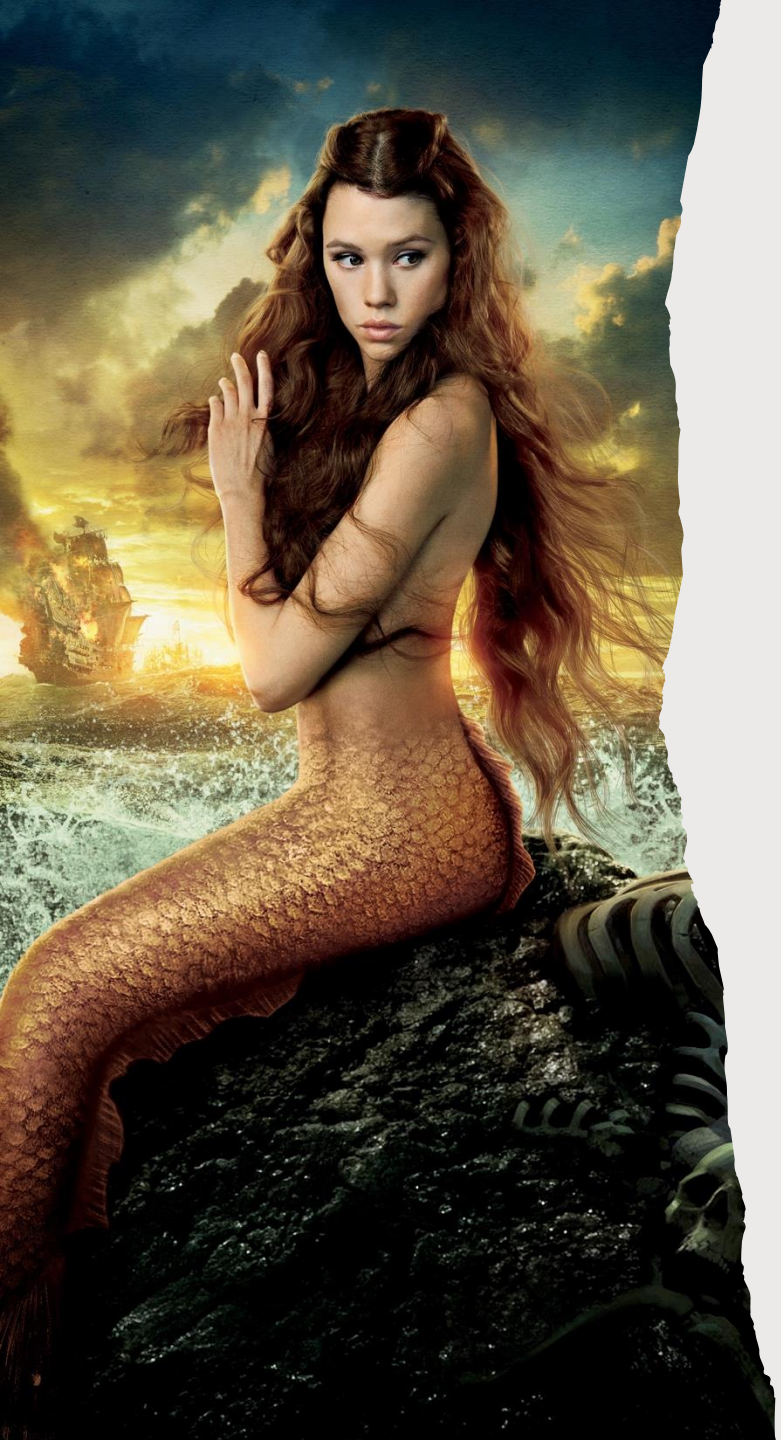
Si vous avez des questions ou si vous avez besoin d'assistance concernant le paiement, notre service clientèle est disponible à l'adresse suivante : facture@ovhcloud.com.

Nous vous prions de bien vouloir traiter cette demande avec la plus grande priorité afin d'éviter tout désagrément.

Nous vous remercions de votre coopération.

Cordialement,
Service Client OVHcloud

Remarque : Il s'agit d'un courriel généré automatiquement. Veuillez ne pas répondre directement à ce courriel.



# Outils de contrôle

- Vérifier les liens avec un outil :
- https://jbxcloud.joesecurity.org
- https://urlscan.io/
- https://sitereview.symantec.com/

- Vous pouvez transmettre les mails frauduleux à suspect@safeonweb.be.
- Vous pouvez également envoyer des sms suspects. Pour ce faire, il vous suffit de faire une capture d'écran et de l'envoyer à suspect@safeonweb.be. Le contenu de votre signalement sera ensuite traité de manière automatique.


# Résultat de contrôle

https://sitereview.symantec.com/

WebPulse Site Review Request

Check another URL

URL submitted:

http://iazd36rewe.pieczatki-olsztyn.pl/?id=alf-solution.be

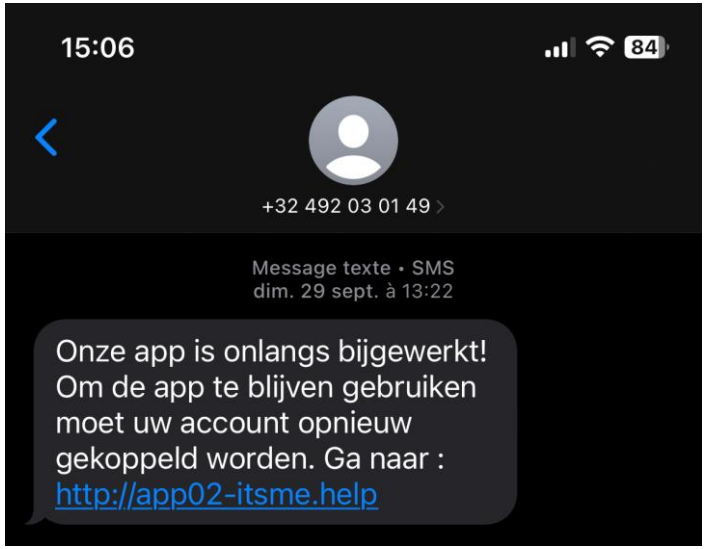
This URL is categorized as a security risk

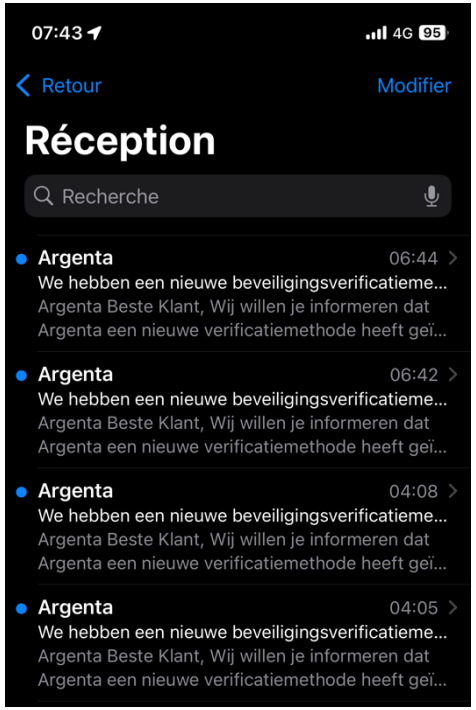
**Suspicious**
This page was rated by our WebPulse system

**If you feel these categories are CORRECT** , click here to learn more about your Internet access policy.
**If you feel these categories are INCORRECT**, please fill out the form below to have the URL reviewed.

Do you agree with the current categorization? If not, how would you categorize it?

# Smishing - exemples






# Arnaque aux sentiments en ligne

**Création de faux profils**

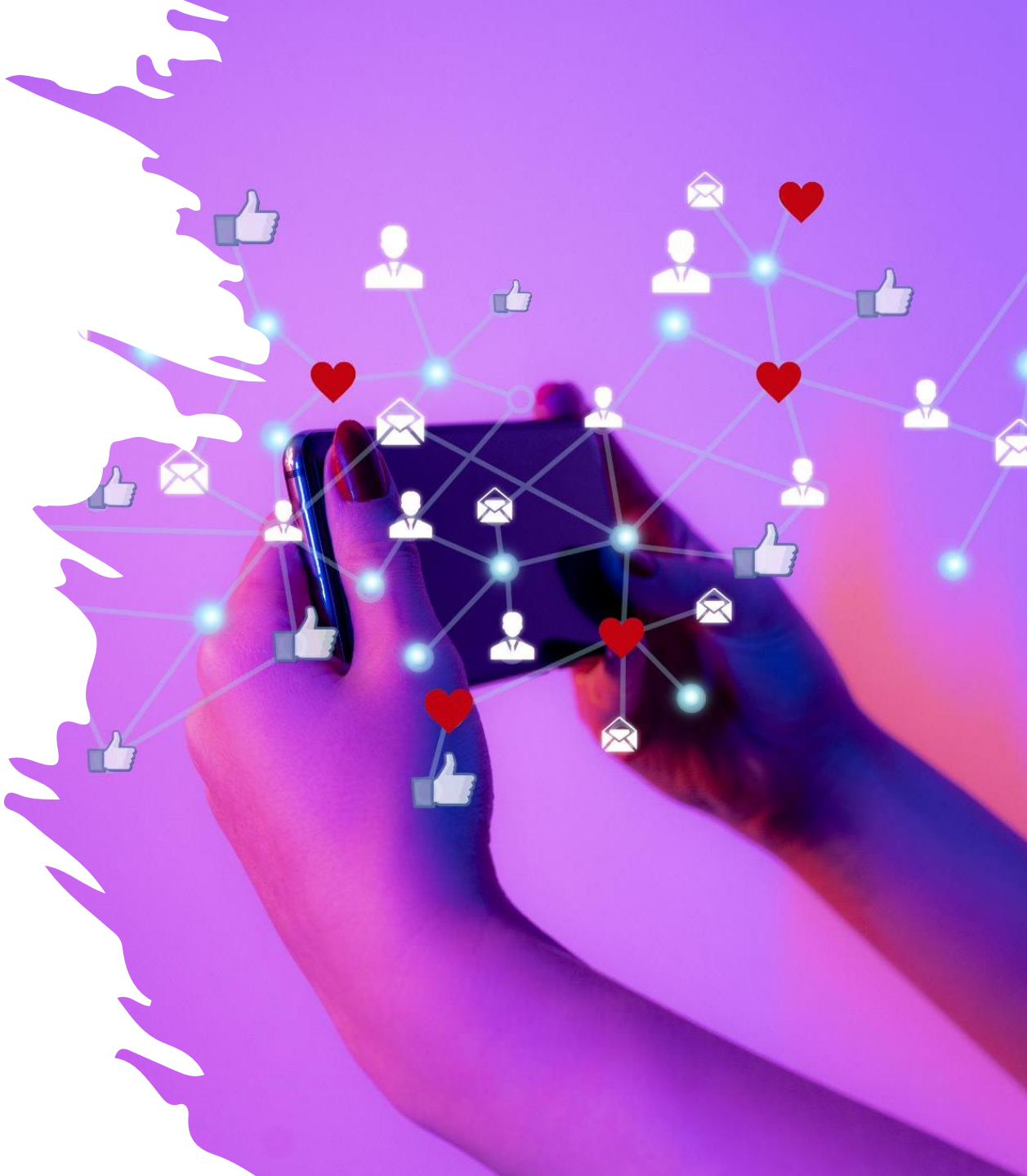
Les arnaqueurs conçoivent de faux profils attrayants sur les réseaux sociaux ou sites de rencontres pour tromper les victimes.

**Manipulation émotionnelle**

Après avoir établi une relation, ils inventent des histoires émouvantes pour susciter la confiance et obtenir de l’argent.

**Disparition après paiement**

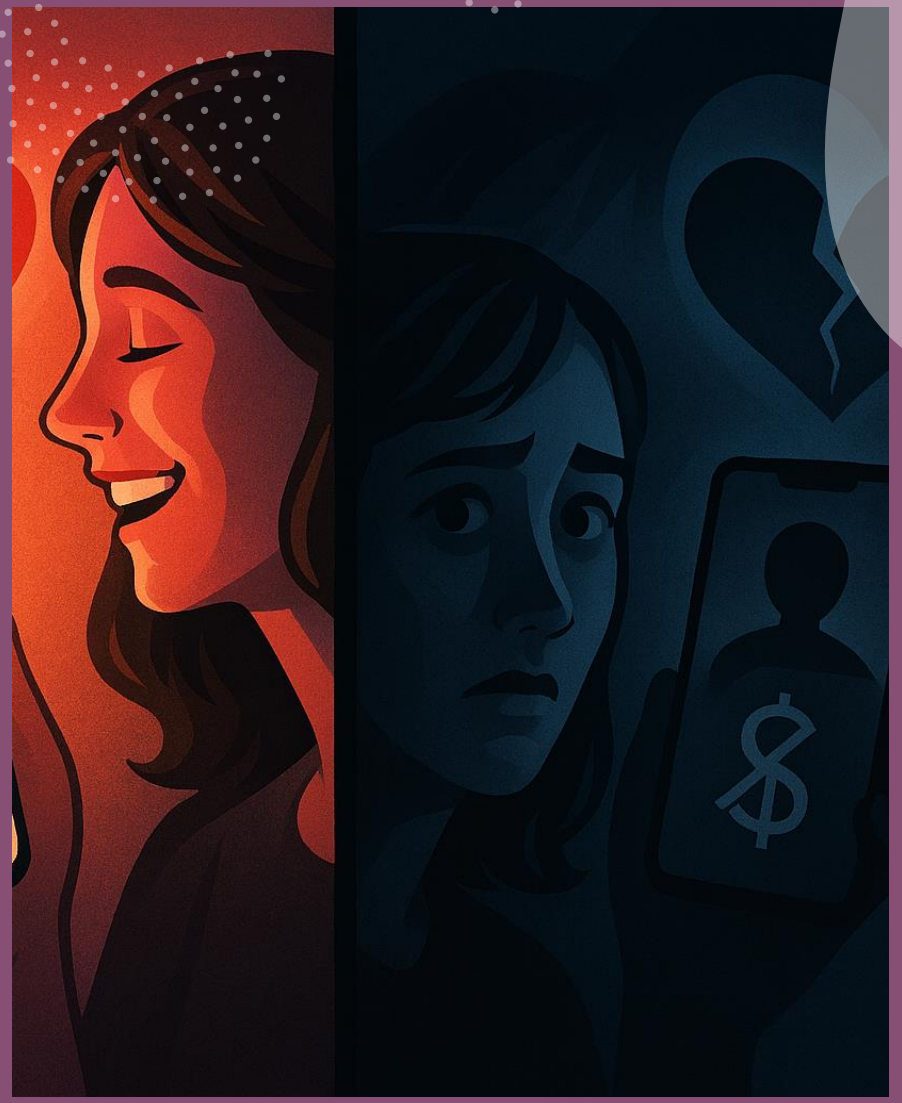
Les victimes sont souvent abandonnées après avoir envoyé de l’argent, l’arnaqueur cesse tout contact.



# Modus operanti

- Tout le monde est potentiellement une victime, mais les personnes âgées, ayant perdu un conjoint sont plus vulnérables
- Vous serez flatté(e), pour qu'il gagne votre confiance
- Vous recevrez beaucoup de message, rempli de compliments, d'amour
- Il ou elle a un beau profil : médecin, militaire, chef d'entreprise, …
- Si vous recherchez sur internet son profil, à base de sa photo par exemple, vous verrez qu'il y a des dizaines de profils similaires, avec les mêmes photos… mais lui, bien sûr, c'est le vrai profil, les autres ont volés ses photos

# De “l’amour” à la “désilusion”



Une fois la confiance établie, il se passera un événement et il vous demandera de l'argent pour l'aider

Il est coincé à l'étranger, il doit payer un loyer, rembourser une dette, un de ses enfants est malade,...

Une première somme sera demandée, ... mais ce ne sera pas suffisant, rapidement il faudra un complément

Vous lui poserez des questions pour en savoir plus... il évitera de vraiment y répondre...

tu ne veux pas m'aider ? Tu ne m'aimes plus ?

Par ses nombreux messages, vous serez acroc à lui... une forme de dépendance s'installera, car il vous fait du bien par ses messages

Tout est bien sûr faux ... il niera biensûr qu'il vous ment et vous vous serez probablement dans le déni !

# Que faire pour se protéger ?

- Un inconu vous contact ?
  -> Vérifiez son profil
- Recherchez sur base des photos qu'il vous donne
- Réfléchissez à la crédibilité de ce qu'il vous dit
- Restez dans le monde réel
- Parlez-en avec vos proches

# A surtout ne pas faire

- Donnez des informations personnelles comme:
  - Votre adresse
  - Des photos de vous, surtout suggestives
  - Des photos de vos proches
- Lui envoyer de l'argent par quelque moyen que ce soit

# Fraude à l ‘investissement

Comment reconnaître une fraude à l'investissement ?

Notez les signes d'avertissement suivants :

- **Contact non sollicité :** Vous êtes contacté par téléphone, par courriel ou par les médias sociaux.
- **Promesses excessives** : Des profits élevés sont promis sans risque.
- **Pression pour décider rapidement :** Vous êtes contraint d'investir rapidement.
- **Manque de transparence :** peu ou pas d'informations sont données sur le produit ou le prestataire. Le fournisseur n'est pas agréé.
- **Demandes de paiement étranges :** On vous demande de transférer de l'argent sur des comptes étrangers ou par le biais de méthodes de paiement inhabituelles, par exemple en crypto-monnaie.


Source : https://safeonweb.be/fr/ne-vous-laissez-pas-pieger-par-la-fraude-linvestissement

# Comment prévenir la fraude à l'investissement ?

- **Vérifiez le fournisseur :** vérifiez si l'entreprise est agréée par la FSMA. Vérifiez également si le nom figure sur la liste des sociétés douteuses (Liste des sociétés opérant irrégulièrement en Belgique | FSMA). Si vous avez des doutes, contactez la FSMA via le formulaire de contact.
- **Soyez critique :** Vous recevez à l'improviste une belle offre d'investissement ? Prenez toujours le temps de dissiper vos doutes ou votre méfiance.
- **Demandez au** fournisseur des **informations claires et compréhensibles**. N'investissez pas dans un produit financier si vous ne comprenez pas exactement ce qu'il implique**.**
- **N'effectuez pas de paiements précipités :** Prenez le temps d'étudier l'offre et ne vous laissez pas forcer la main.
- **Protégez vos données personnelles :** Ne communiquez jamais vos données d'identité, vos coordonnées bancaires ou d'autres informations personnelles.
- **Vérifiez en quelques minutes si vous avez affaire à un escroc.** Faites le test de la fraude. Même si vous pensez connaître le fournisseur, revérifiez-le et vérifiez les coordonnées de l'entité avec laquelle vous êtes en contact. De nombreux escrocs utilisent abusivement le nom d'une entreprise connue qui possède une licence.

# Bonnes pratiques


- Est-ce que vous attendez un coli ?
- Vous avez un doute ?
  - N’ouvrez pas, ne cliquez pas, ne répondez pas
  - Effectuez une recherche en ligne, consultez le site official, prenez vous même contact avec l’organisme
- Utilisez un gestionnaire de mot de passe
  - Pas un plugin dans votre navigateur !
  - Keeper Security, Keepass, 1Password, …
- Utilisez des mots de passe différents/code pin pour
  - Votre PC
  - Votre/vos emails
  - Votre banque
- Des mots de passe long (>12) avec des chiffres et des caractères spéciaux
  - J’a!0ubli3m0nM0td3p@ss3
  - M0nCh!3n3stl3plusgent!l
- Ayez un antivirus et à jour
- Mettez vos systèmes à jour (PC/Mac, Smartphones, tablettes, applications, …)
- Réalisez des copies de sauvegarde

# Combien de temps faut-il à un pirate pour trouver votre mot de passe ?

| Nombre de caractères | Nombres seulement | Lettres minuscules | Lettres majuscules et minescules | Nombres, lettres majuscules et minuscules | Nombres, lettres majuscules et minuscules, symboles |
|---|---|---|---|---|---|
| 4 | Instantané | Instantané | Instantané | Instantané | Instantané |
| 5 | Instantané | Instantané | 57 minutes | 2 heures | 4 heures |
| 6 | Instantané | 46 minutes | 2 jours | 6 jours | 2 semaines |
| 7 | Instantané | 20 heures | 4 mois | 1 an | 2 ans |
| 8 | Instantané | 3 semaines | 15 ans | 62 ans | 164 ans |
| 9 | 2 heures | 2 ans | 791 ans | 3k ans | 11k ans |
| 10 | 1 jour | 40 ans | 41k ans | 238k ans | 803k ans |
| 11 | 1 semaine | 1k ans | 2M ans | 14M ans | 56M ans |
| 12 | 3 mois | 27k ans | 111M ans | 917M ans | 3Md ans |
| 13 | 3 ans | 705k ans | 5Md ans | 56Md ans | 275Md ans |
| 14 | 28 ans | 18M ans | 300Md ans | 3Bn ans | 19Bn ans |
| 15 | 284 ans | 477M ans | 15Bn ans | 218Bn ans | 1Bd ans |
| 16 | 2k ans | 12Md ans | 812Bn ans | 13Bd ans | 94Bd ans |
| 17 | 28k ans | 322Md ans | 42Bd ans | 840Bd ans | 6Tn ans |
| 18 | 284k ans | 8Bn ans | 2Tn ans | 52Tn ans | 463Tn ans |

Hive Systems

› hivesystems.com/password

L’I.A. rend les arnaques de plus en plus réaliste

Vous vous êtes fait avoir ?
Prévenez immédiatement votre banque,
et puis portez plainte à la police.
Ne soyez pas honteux, au contraire,
parlez-en autour de vous, cela pourra certainement aider ou protéger une autre personne

Restez vigilants !

# Merci

Pierre Delporte
ALF-Solution – info@alf-solution.be