

# Apprenez à vous défendre contre toute cyber malveillance

Sensibilisation au Piratage et à la Cybercriminalité

Juin 2023

# Apprenez à vous défendre contre toute cyber malveillance

1<sup>er</sup> Niveau du parcours Cyber : Formation et Informations



# Intervention



**Ely de Travieso**

[e.detravieso@guardea.com](mailto:e.detravieso@guardea.com)

**Expert en Cyberdéfense depuis 1998**  
**Directeur Services & Sinistres Guardea**

Président du Clusir Paca  
Conférencier & Formateur

*« Au sein de Guardea, je pilote l'ensemble des interventions de prévention et de réponse à incidents auprès de plus de 300 entreprises que nous protégeons 7j/7.*

*A travers cette formation, je souhaite partager mes retours d'expérience et mon expertise »*

## Actualité & Chiffres de la cybercriminalité

### Les risques majeurs

- Usurpation sur les réseaux sociaux
- Attaques de phishing
- Fraude par ingénierie sociale
- Insécurité des mots de passe
- Infection par ransomware

## L'avis d'expert pour mieux vous protéger

## La suite du Parcours de Cyberdéfense

# Dans le presse

la Nouvelle  
République.fr

DEUX-SÈVRES > Commune > Mougou-Thorigné > Niort : une troisième victime de piratage par virement pour un préjudice de 26.700 €

## Niort : une troisième victime de piratage par virement pour un préjudice de 26.700 €

Publié le 23/02/2022 à 13:00 | Mis à jour le 23/02/2022 à 13:06

Leur banque nie toute responsabilité et ne veut pas rembourser

Le problème dorénavant pour ce couple, c'est que leur banque locale (à Niort) nie toute responsabilité dans cette fraude et refuse le remboursement du montant. "Ce n'est pas une fraude de notre fait puisque ce n'est pas nous qui avons saisi le Rib en direction duquel vous avez envoyé l'opération. C'est vous qui avez réalisé cette opération dans votre espace personnel", leur explique leur conseiller bancaire.

ouest  
france

## Deux-Sèvres. Le groupe In Extenso victime d'une cyberattaque

Le groupe national d'expertise comptable In Extenso, présent notamment en Deux-Sèvres, a essuyé une cyberattaque qui a paralysé une partie de ses activités.

Le groupe national d'expertise comptable [In Extenso](#), présent à Niort pour les Deux-Sèvres, a essuyé une cyberattaque qui a paralysé une grande partie de son activité, système informatique et lignes téléphoniques. Selon le site [LeMagIT](#), La directrice de la communication du groupe a confirmé que l'entreprise a subi une cyberattaque conduite

## L'USINEDIGITALE

### SFR vous demande de changer votre carte Sim : attention à cette nouvelle arnaque

Depuis la fin de l'année, des escrocs utilisent la méthode du "SIM swapping" pour voler le numéro de téléphone de leurs victimes et élaborer d'autres arnaques via la ligne volée. Les clients de l'opérateur SFR en font aujourd'hui les frais.

Par Margaux Menu

Publié le 13/02/2023 à 14h06 & mis à jour le 13/02/2023 à 20h29

## L'union

### Le CDER, cabinet d'expertise comptable basé à Châlons-en-Champagne, victime d'une cyberattaque

L'association de gestion et de comptabilité CDER, qui compte près de 700 salariés et 12 000 clients adhérents, a subi une importante attaque informatique le 22 décembre. Il y a deux ans, le CDER avait déjà été victime d'une vaste escroquerie en ligne.



# La Cybercriminalité en 2022

## LES CHIFFRES CLÉS DE LA CYBERSÉCURITÉ



**54 %** des entreprises françaises  
attaquées en 2021<sup>(1)</sup>



**+255%**

d'attaques par ransomware  
en 2020 par rapport à 2019<sup>(2)</sup>

**+400%**

de tentatives de phishing  
durant le début du  
confinement<sup>(3)</sup>

**20%**

des entreprises ont été  
touchées par un ransomware<sup>(1)</sup>

**50 000€**

c'est le coût médian  
d'une cyberattaque<sup>(4)</sup>



**27%**

de perte moyenne sur le  
chiffre d'affaires pour les PME  
en France<sup>(4)</sup>



**47%**



des télétravailleurs  
se font faire piéger  
par un phishing<sup>(1)</sup>

**73%**

des entreprises déclarent le  
phishing comme vecteur  
d'entrée principal pour les  
attaques subies<sup>(1)</sup>

**40%**

des entreprises ont  
investi dans leur  
cybersécurité en 2021<sup>(4)</sup>



**55%**

des entreprises considèrent  
que le niveau de menaces en  
matière de cyberespionnage  
est élevé<sup>(1)</sup>

SOURCES : (1) BAROMÈTRE DE LA CYBERSÉCURITÉ EN ENTREPRISE CESIN 2022 - (2) ANSSI - (3) CYBERMALVEILLANCE.GOUV.FR. - (4) STOIK

# Risques liés aux Réseaux Sociaux

LinkedIn

facebook

Instagram



# Risques liés aux Réseaux Sociaux

## LinkedIn

Bonjour Alexandre,

Vous avez ajouté une nouvelle adresse e-mail à votre compte LinkedIn.

Pour confirmer cette adresse veuillez cliquer sur [ce lien](#) ou le coller dans votre navigateur :

<https://www.linkedin.com/psettings/sign-in-and-security>

Nous vous demanderons ensuite de vous identifier. Assurez-vous d'utiliser l'adresse e-mail sur laquelle vous souhaitez recevoir les messages, les invitations et les demandes.

Merci d'utiliser LinkedIn !  
L'équipe LinkedIn

[Se désinscrire](#) | [Aidez-moi](#)

LinkedIn

facebook

Instagram

## facebook

[Sign Up](#) Facebook helps you connect and share with the people in your life.

### Facebook Login

#### Please re-enter your password

The password you entered is incorrect. Please try again (make sure your caps lock is off).  
[Forgot your password?](#) [Request a new one.](#)

Email:

Password:

Keep me logged in

or [Sign up for Facebook](#)

[Forgot your password?](#)

[Bahasa Indonesia](#) [English \(US\)](#) [Español](#) [Português \(Brasil\)](#) [Français \(France\)](#) [Deutsch](#) [Italiano](#) [العربية](#) [हिन्दी](#) [中文\(简体\)](#) [+](#)

Facebook © 2011

[Mobile](#) [Find Friends](#) [Badges](#) [People](#) [Pages](#) [About](#) [Advertising](#) [Create a Page](#) [Developers](#) [Careers](#)



# La sécurité sur les réseaux sociaux

## Définition :

**L'usage des réseaux sociaux personnels peut agir sur la sécurité globale de l'entreprise si l'utilisateur se connecte à partir d'un support de l'entreprise.**

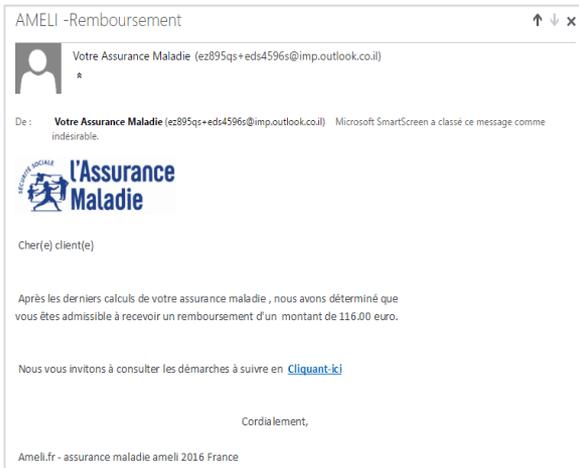
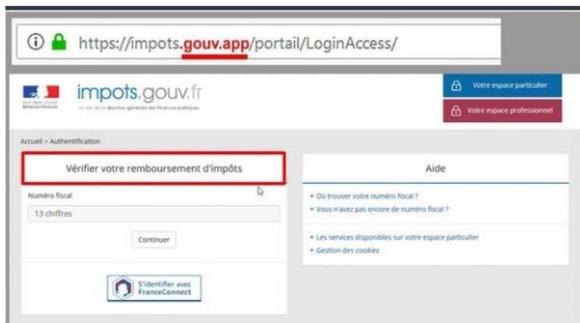
## Modus Operandi :

- Envoi de fichiers malicieux
- Intrusion sur le poste de travail
- Diverses attaques possibles (Vol d'informations, ransomware, attaque rebond)

## Bonnes pratiques :

- **Être vigilant aux discussions ou articles douteux dont la source est peu connue**
- **Utiliser un smartphone personnel en se connectant à travers le réseau 4/5G**

# Les attaques de Phishing



Société OvH : [ IMPORTANT ] dernier rappel pour renouveler votre service.



tneilCHVO <info3@skwp.pl>  
À contact



↳ Répondre

↳ Répondre à tous

→ Transférer



mer. 22/03/2023 09:26

## OVHcloud

Groupe français OVHcloud

Cher client,

Vous recevez ce message car vous êtes le contact principal pour votre nom de domaine **guarda.com**.

Nous vous informons sur l'évolution de vos produits chez OVHCloud et nous vous envoyons un rappel chaque 60, 30, 15, 7 et 3 jours avant leur expiration.

Si vous souhaitez conserver ce domaine, il vous suffit de vous rendre sur notre site, et [éviter la suspension](#) ; d'utiliser la commande de renouvellement

NB : Le règlement peut se faire via l'un des moyens de paiement proposés. Mais nous recommandons de régler par Carte Bancaire pour accélérer le traitement; En cas de non règlement sous 2 jours, votre domaine pourrait être DEFINITIVEMENT effacé.

Merci de votre compréhension.

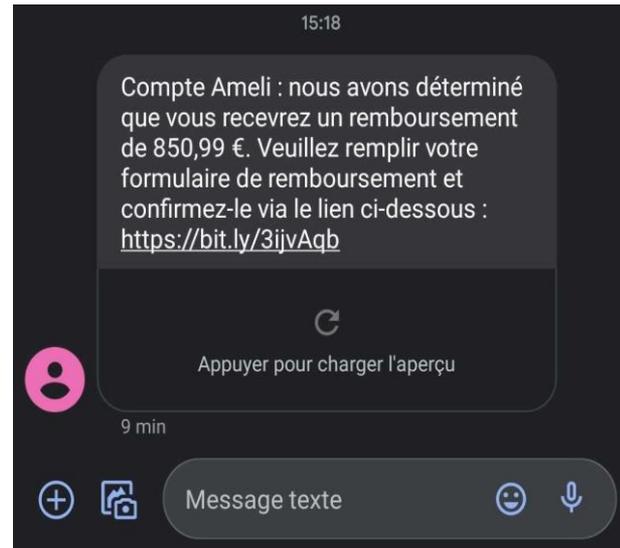
Cordialement,  
Votre Service client OVH

Copyright © 2023 OvHcloud, Inc.  
2 rueeKellermann, 75009 Paris, BP 80157

www.ovhcloud.com | Community



# Les attaques de Phishing



# Attaque Phishing

## Définition :

**le phishing est une attaque qui consiste à demander à un utilisateur son mot de passe pour prendre le contrôle du service concerné.**

## Modus Operandi :

- Par email
- Par téléphone
- Par SMS/MMS
- Par messageries
- Contrefaçon de supports numériques

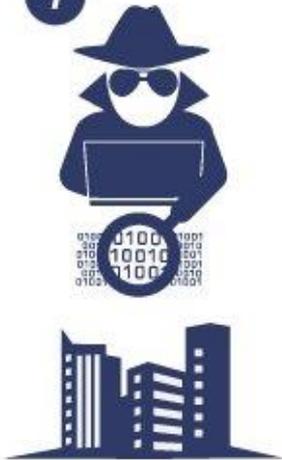
## Bonnes pratiques :

- **Ne pas accepter de changer son mot de passe par un mot de passe qui vous est recommandé.**
- **Informez le responsable ou les collaborateurs, chaque fois que l'on vous demande de changer ou communiquer votre mot de passe**

# Les attaques par ingénierie sociale

## Fraude aux Faux Ordres de Virement #FOVI

1



L'escroc collecte des informations pour connaître l'entreprise et ses dirigeants (réseaux sociaux, organigramme)

2



Se faisant passer pour le dirigeant de l'entreprise, l'escroc prétexte une opération financière urgente et confidentielle

3



Sous la pression ou en confiance, l'entreprise exécute la transaction

4



L'escroc transfère l'argent vers des comptes basés à l'étranger



NOTRE VOCATION, C'EST VOUS !



# Les attaques par Ingénierie Sociale

## Définition :

**une attaque par ingénierie sociale associe une approche psychologique et technique et a pour objectif de contourner des processus, des barrages ou règles pour atteindre un privilège non autorisé**

## Modus Operandi :

Analyse d'informations publiques

Mise en scène de l'attaque

Exploitation de la relation

Attaque possible à distance comme en proximité

## Bonnes pratiques :

- **Être vigilant(e) dans les demandes entrantes par email, appel ou courrier**
- **Vérifier l'identité de l'interlocuteur nouveau**
- **Demander confirmation ou questionner ses collaborateurs**



# Mots de passe & Authentification

## Définition :

**un mot de passe est une clé professionnelle et personnelle permettant de s'authentifier pour avoir accès à un environnement privilégié**

## Modus Operandi :

Le phishing

L'ingénierie sociale

Le vol de session

Le cassage / crackage

## Bonnes pratiques :

- **Utiliser des techniques simples de génération et changer tous les 3 mois ses mots de passe**
- **Dissocier les mots de passe professionnels et personnels**
- **Toujours être vigilant(e) lorsqu'on vous demande de saisir ou communiquer un mot de passe**

# Les attaques par ransomware



Your network and hard drives were encrypted using AES-256 military grade encryption.

AvosLocker will aid you in the recovery and restoration of the files affected.

Please enter your ID (presented to you in the note) in order to continue.

Failure to contact us in due time might incur additional charges and damages.

## Attention!

Your files have been encrypted using AES-256.

We highly suggest not shutting down your computer in case encryption process is not finished, as your files may get corrupted.

In order to decrypt your files, you must pay for the decryption key & application.

You may do so by visiting us at

This is an onion address that you may access using Tor Browser which you may download at

<https://www.torproject.org/download/>

Details such as pricing, how long before the price increases and such will be available to you once you enter your ID presented to you below in this note in our website.

Hurry up, as the price may increase in the following days.

Message from agent: If you fail to respond in 4 days, the cost of decryption will double up and we will leak some of your data. In 10 days, we will leak all the data we have.

CryptoLocker

## Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents, etc. [Here](#) is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key **RSA-2048** generated for this computer. To decrypt files you need to obtain the **private key**.

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

**To obtain** the private key for this computer, which will automatically decrypt files, you need to pay **300 USD / 300 EUR / similar amount** in another currency.

Click «Next» to select the method of payment.

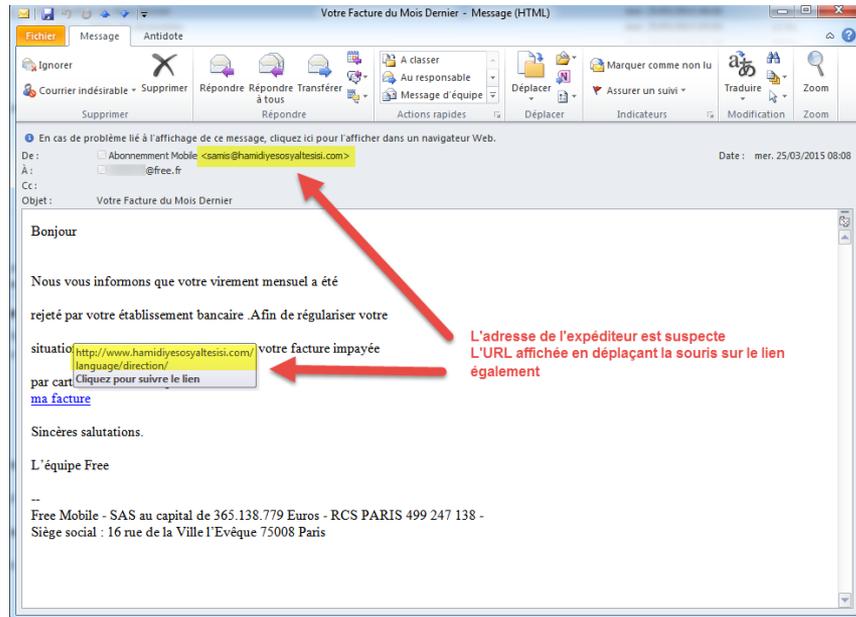
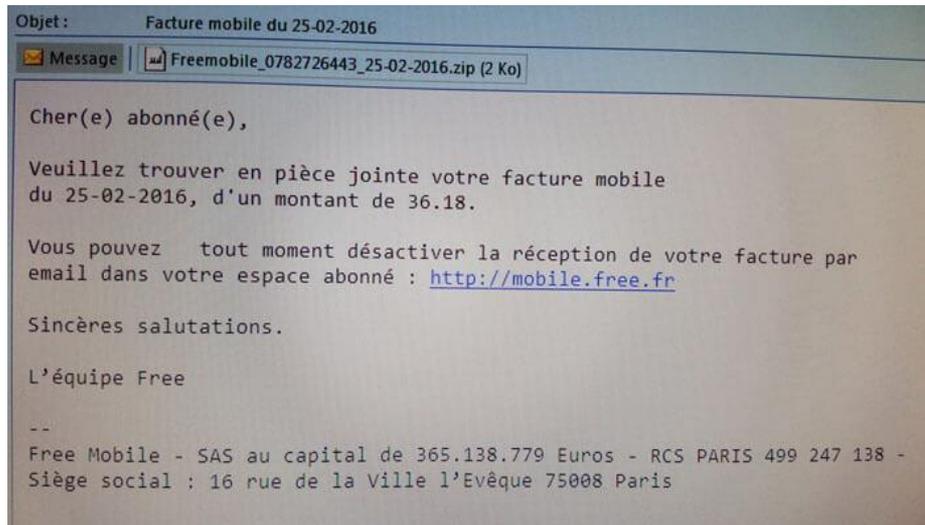
**Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.**

Private key will be destroyed on  
10/19/2013  
6:09 PM

Time left  
**71 : 59 : 33**

Next >>

# Les attaques par ransomware



*Mais aussi par intrusion informatique sans intervention humaine ...*

# Attaque Ransomware

## Définition :

**Le Ransomware est un virus qui va se déployer sur l'ensemble du réseau de l'entreprise pour s'approprier l'ensemble des données et bloquer le fonctionnement global du système d'information contre la demande d'une rançon financière.**

## Modus Operandi :

Intrusion sur le réseau

Déploiement du virus

Activation du virus

Négociation de la rançon

## Bonnes pratiques :

- **Être vigilant dans la lecture d'emails possédant des pièces jointes**
- **Respecter la politique de sauvegarde de l'entreprise en évitant la sauvegarde locale**
- **Être à jour des mises à jour de sécurité**

# Risque de Piratage & de Cybercriminalité

# Avis d'Expert



# Partez du bon pied avec 6 bonnes pratiques

1

## Un gestionnaire de mots de passe

1 mot de passe unique par service

2

## Maintenir à jour tous vos outils informatiques

(applications, matériels)

3

## Un antivirus EDR

Protection de votre poste de travail

4

## Vigilant sur les comportements anormaux

(emails, sms, appels, réseaux sociaux)

5

## Respect des lois et de la conformité RGPD

Traitement des données et la protection informatique - RGPD

6

## Savoir réagir à une attaque en moins de 2H

Référentiels, exercices & Partenaires

# Votre évaluation Cyber & Actions personnalisées

2<sup>ème</sup> Niveau du parcours Cyber : Cyberscore + Rdv Expert



# Votre Parcours d'amélioration et de sécurisation



Améliorez vos connaissances



Pour **vous permettre de mieux appréhender les risques cybers** et bonnes pratiques associées.

Obtenez votre accès libre



Votre accès personnel et sécurisé pour **approfondir vos connaissances et celles de vos collaborateurs** (Fiches bonnes pratiques, outils et services Open source, Actualités, Animations...).



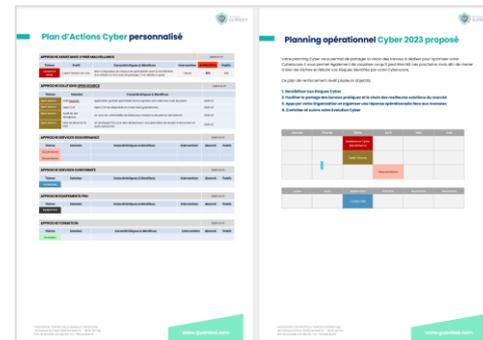
Evaluez votre Cyber Score



Réalisez votre analyse de risques pour **identifier votre niveau de protection contre les cyber malveillances** en répondant au questionnaire du **Cyber Score**



Deployez nos conseils Expert



**Conseils personnalisés pour votre Business et votre sécurité.** Echange privé avec un conseiller Guardea, parfait pour prévenir et anticiper les attaques informatiques.





# GUARDEA

CYBERDEFENSE COMMUNITY

[contact@guardea.com](mailto:contact@guardea.com)



Prestataire Terrain Parcours Cybersécurité du Programme France Relance  
Société recommandée en cas d'attaques, fraudes et cybermalveillances

© 2023 GUARDEA  
All rights reserved.

