GUARDEA
CYBERDEFENSE COMMUNITY

# 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

1er Niveau du parcours Cyber : Formation et Informations

# Intervention

**Ely de Travieso**
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 > Mougon-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.

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

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.

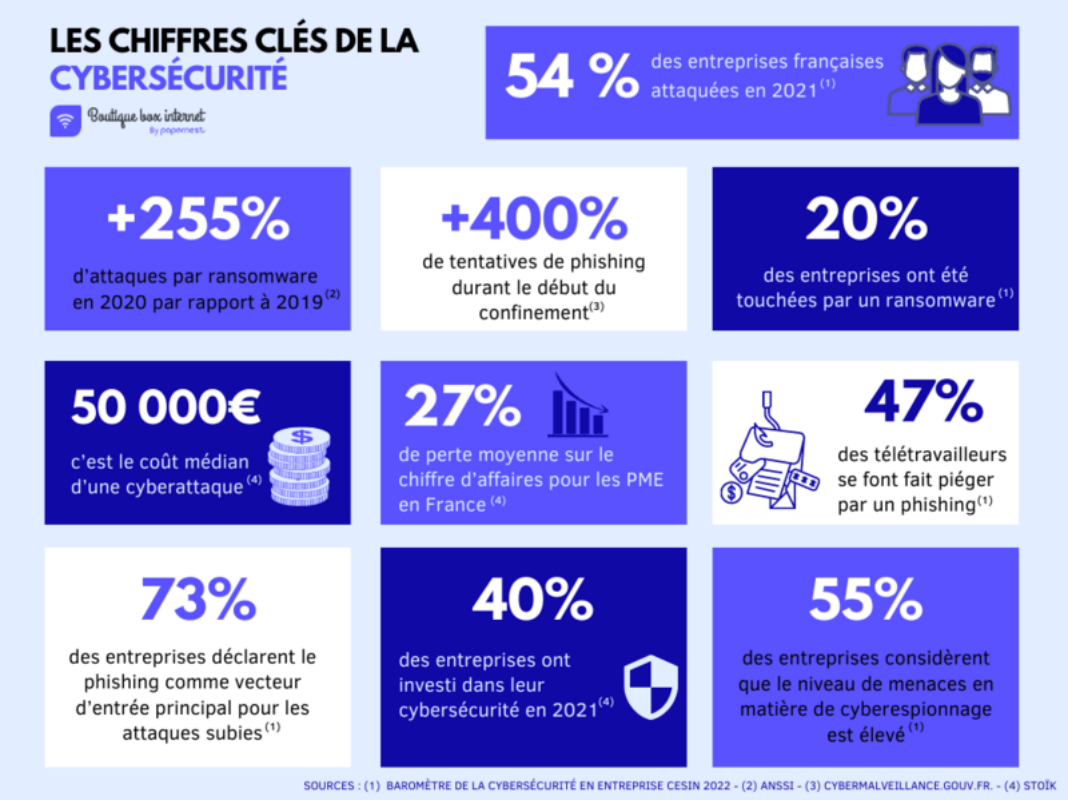
Le groupe national d'expertise comptable In Extenso, présent à Niort pour les Deux-Sèvres, a essuyé une cyberattaque qui a paralysé une grande partie de son activité, système informatique et lignes téléphoniques. Selon le site LeMagIT, La directrice de la communication du groupe a confirmé que l'entreprise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

L'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



# Risques liés aux Réseaux Sociaux

LinkedIn facebook Instagram









Sécurisé par GUARDEA

# Risques liés aux Réseaux Sociaux

LinkedIn facebook Instagram

LInkedin

Bonjour Alexandre,

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

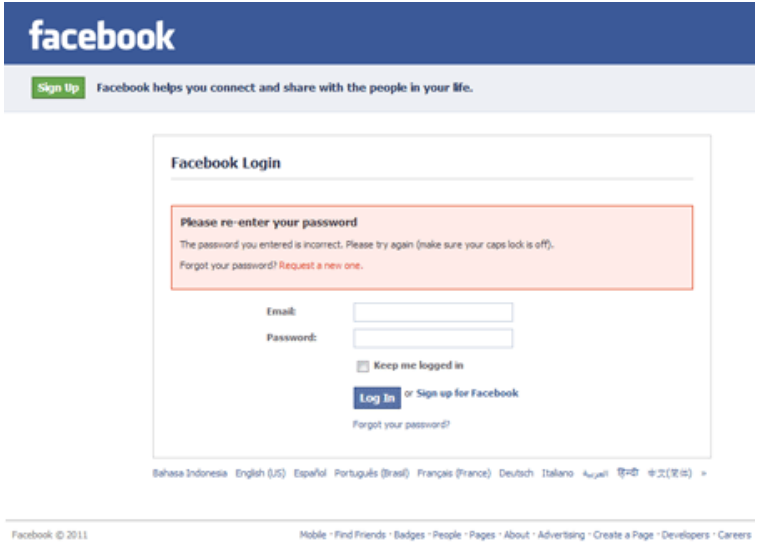
Pour confirmer cette adresse veuillez cliquer sur ce lien ou le coller dans votre navigateur :

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



# 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.**

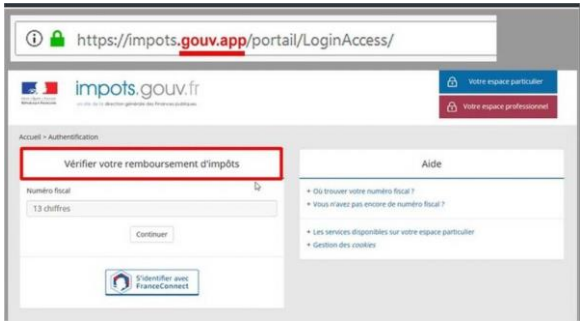
**Modus Operandi :**

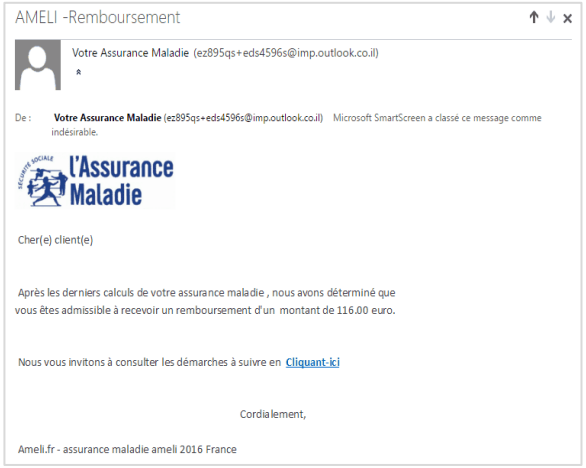
- Envoi de fichiers malicieux
- Intrusion sur le poste de travail
- Diverses attaques possibles (Vol d'informations, ransomware, attaque rebond)

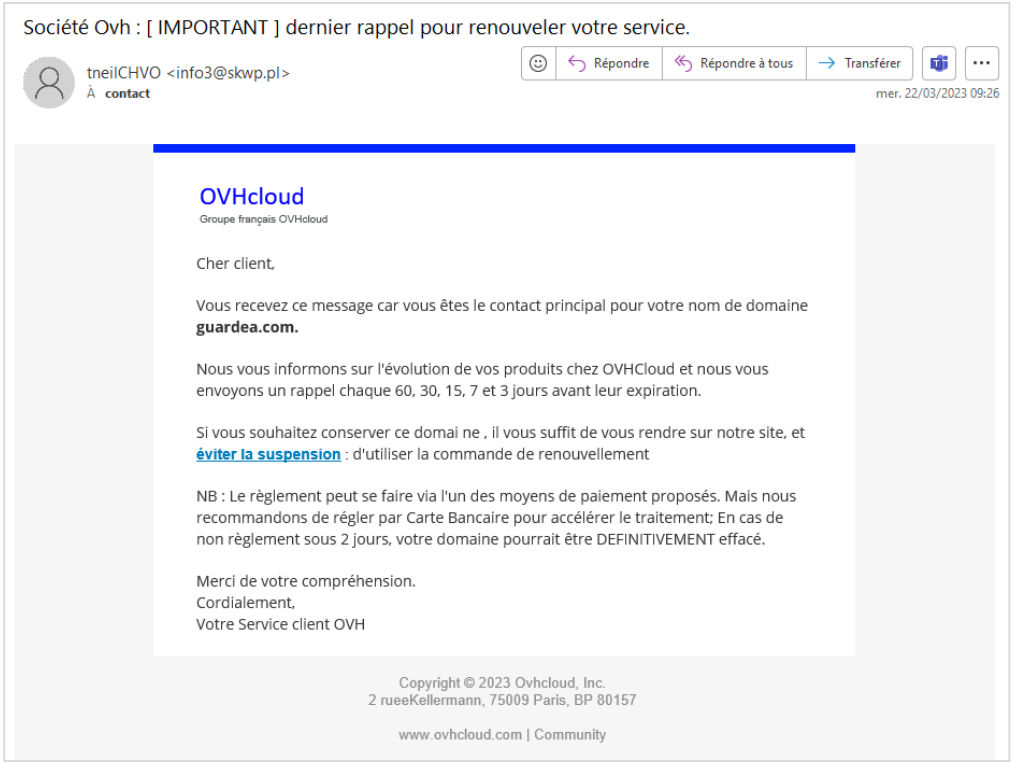
**Bonnes pratiques :**

- **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



# 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.**
- **Informer 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

# 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 :**

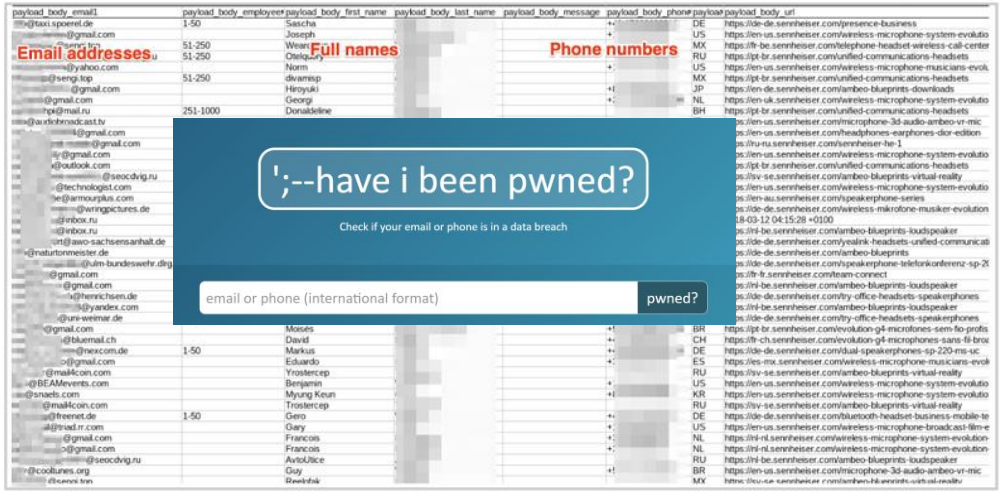
- **Être vigilant(e) dans les demandes entrantes par email, appel ou courrier**
- **Vérifier l'identité de l'interlocuteur nouveau**
- **Demander confirmation ou questionner ses collaborateurs**

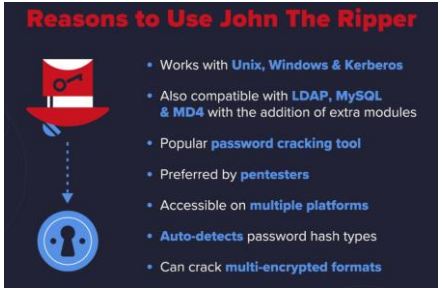
# La faiblesse des mots de passe

## Les pires mots de passe utilisés en France

Classement des mots de passe français les plus courants en 2019 *

1. 123456
2. 123456789
3. azerty
4. 1234561
5. qwerty
6. marseille
7. 000000
8. 1234567891
9. doudou
10. 12345
11. loulou
12. 123
13. password
14. azertyuiop
15. 12345678
16. soleil
17. chouchou
18. 1234
19. 1234567
20. 123451




| NOMBRE DE CARACTÈRES | UNIQUEMENT DES CHIFFRES | LETTRES MINUSCULES | LETTRES MINUSCULES ET MAJUSCULES | LETTRES MINUSCULES ET MAJUSCULES + CHIFFRES | LETTRES MINUSCULES ET MAJUSCULES + CHIFFRES + CARACTÈRES SPECIAUX |
|---|---|---|---|---|---|
| 4 | IMMÉDIATEMENT | IMMÉDIATEMENT | IMMÉDIATEMENT | IMMÉDIATEMENT | IMMÉDIATEMENT |
| 6 | IMMÉDIATEMENT | IMMÉDIATEMENT | IMMÉDIATEMENT | 1 sec | 5 sec |
| 8 | IMMÉDIATEMENT | 5 sec | 22 min | 1 heure | 9 heures |
| 10 | IMMÉDIATEMENT | 58 min | 1 mois | 7 mois | 5 ans |
| 12 | 45 sec | 3 semaines | 300 ans | 2000 ans | 34 000 ans |
| 14 | 41 min | 51 ans | 800 000 ans | 9 millions d'années | 200 millions d'années |

*source : SCSP Community (Seasoned Cyber Security Professionnals)

# 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

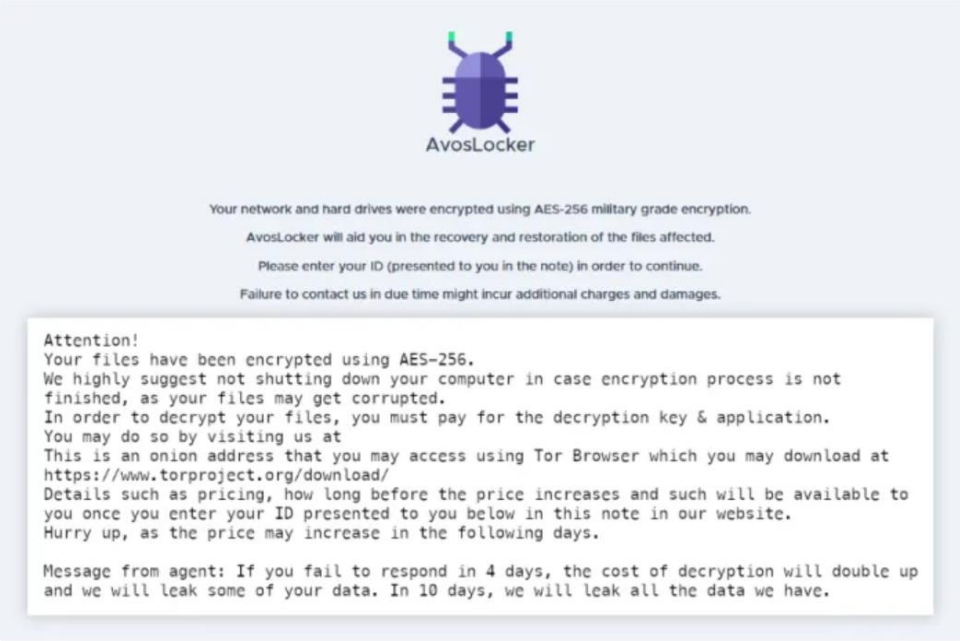
Le vol de session

Le cassage / crackage

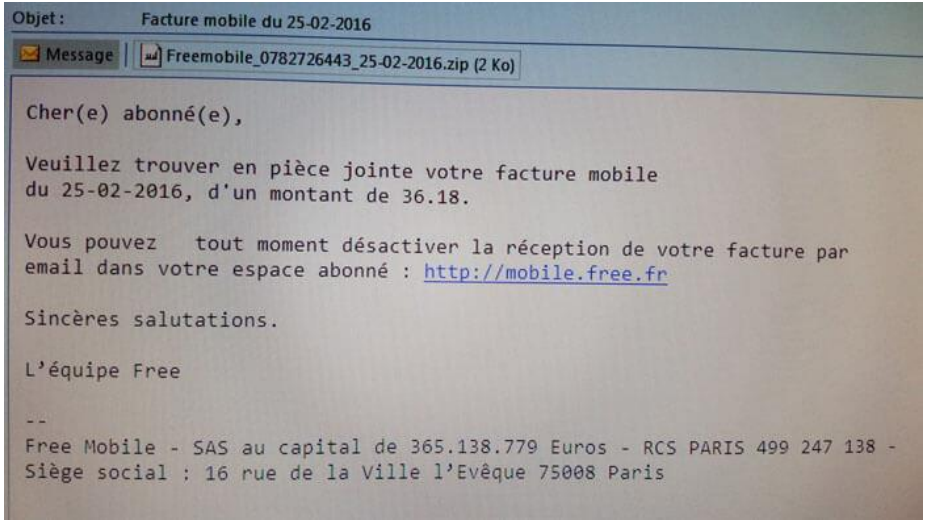
**Bonnes pratiques :**

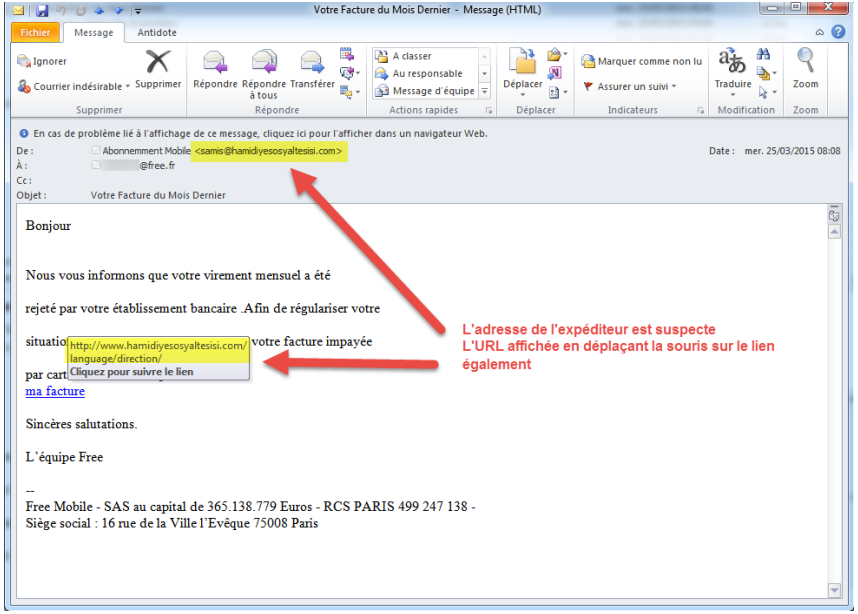
- **Utiliser des techniques simples de génération et changer tous les 3 mois ses mots de passe**
- **Dissocier les mots de passe professionnels et personnels**
- **Toujours être vigilant(e) lorsqu'on vous demande de saisir ou communiquer un mot de passe**

# Les attaques par ransomware




# 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

2ème 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.

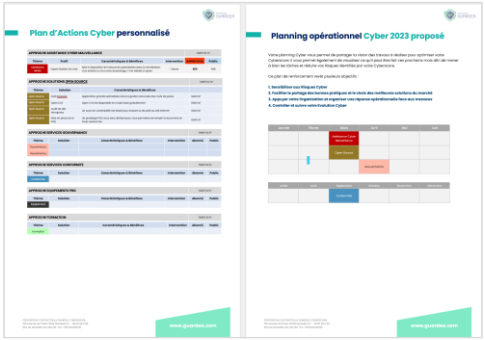
## Obtenez votre accès libre


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**

## Déployez 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.





Sécurisé par GUARDEA

# GUARDEA

CYBERDEFENSE COMMUNITY

contact@guardea.com