



GROUPEMENT
DE SERVICES
ASSURANCE

CYBER ATTAQUE

Information collaborateurs GSA+ 07 Novembre 2023

LES BONS REFLEXES
LES PROTECTIONS
LA BONNE PRATIQUE



SENSIBILISATION A LA CYBER ATTAQUE

- DEFINITION
- DEROULEMENT D'UNE CYBER ATTAQUE
- PROCEDURE EN CAS D'USURPATION D'IDENTITE

DEFINITION D'UNE CYBER ATTAQUE

Une cyberattaque est un acte malveillant envers un dispositif informatique. Elle peut émaner de personnes isolées, d'un groupe de pirates ou de vastes organisations ayant des objectifs géopolitiques.

De : Koffivi TONA <fay.alessia@themastifm.com>
Envoyé : mardi 13 avril 2021 11:45
À : Koffivi TONA <koffivi.tona@assurpol.fr>
Objet : Re: r

Bonjour,
Récemment, nous avons signé un accord avec votre entreprise. Veuillez corriger les informations de transfert de fonds dans la dernière clause. Vous pouvez le trouver dans le fichier joint.

-----Original Message-----
On Wednesday, 7 April 2021, 08:53, wrote:

Annule et remplace le mail envoyé à 08:39 :

Bonjour,

Comme a dû déjà vous l'indiquer Alexandra, Elie sera absents tout le mois d'avril .

Néanmoins jusqu'au 20/04 tous les mails arrivant pour lui seront répartis selon le tableau figurant dans

De : Stéphanie SOENE [<mailto:fay.alessia@themastifm.com>]
Envoyé : mardi 13 avril 2021 11:44
À : Emmanuelle GROSGEORGE
Objet : Re: TR: Contrat RC2003561 - GMS ENROBES // N

Bonjour!
Veuillez remail cet accord à partir du 12/03. Des modifications doivent être apportées au deuxième paragraphe. Vous pouvez le vérifier dans le fichier joint.

-----Original Message-----
On Thursday, 8 April 2021, 15:42, wrote:

Bonjour,

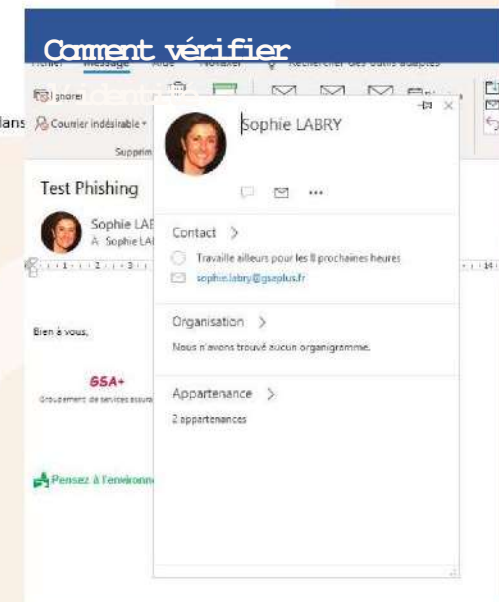
Nous accusons réception de votre demande et vous en remercions.

Le souscripteur en charge de votre dossier est Stéphanie SOENE ; Elle reviendra vers vous dans les meilleurs délais.
Toutefois, je vous remercie de noter que les mesures d'organisation prises pour faire face aux dispositions gouvernementales sur le mois d'avril risquent d'allonger nos délais de réponse.

Restant à votre disposition,

Cordialement,

 Impossible d'afficher l'image liée. Le fichier a peut-être été déplacé, renommé ou supprimé. Vérifiez que le lien pointe vers le fichier et l'emplacement corrects.



DEROULEMENT TYPE D'UNE CYBER ATTAQUE

1. INTRODUCTION MALVEILLANTE

- Émail de spam ou de phishing avec pièce jointe malveillante, ou téléchargement via site Web ou d'un document contenant un virus
- Fonctionnalités de partage ou gestion de fichiers à distance telles que le protocole RDS

2. OBJECTIF DU MALVEILLANT

Les cybercriminels exploitent des failles du système pour obtenir des niveaux de privilèges qui leur permettent de contourner le logiciel de sécurité.
D'où le fait que votre compte d'accès ne soit **administrateur** du poste.

3. DÉSACTIVATION ET CONTOURNEMENT DE LA SÉCURITÉ

À défaut, ils tenteront de pénétrer dans la console de gestion de la sécurité et de désactiver les systèmes de sécurité (Antivirus par exemple).

6. Résultat

- Les Cybercriminels menacent de vendre sur le Dark Web les données subtilisées si la rançon n'est payée, et ainsi obtention de la clef de décryptage.
- Les échanges se passent via mail ou « Dark Web ».

5. Activation du RANSOMWARE

Chiffrement des données de l'entreprise, via encryptage sur les systèmes d'exploitation et sur la totalité des fichiers du réseau en mode partage.

4. DÉPLOIE LA CHARGE VIRALE

Déploiement méthodique en débutant par la suppression des sauvegardes stockées sur le réseau, puis exfiltrent les données sensibles de l'entreprise par des actions minimales afin de n'éveiller les outils de sécurité de transfert de flux.

LA PROCEDURE EN CAS D'ATTAQUE

1. Modifiez immédiatement votre mot de passe

- Vous êtes sur site Tour W : En cliquant sur ctrl/Alt/suppr simultanément puis sur modifier mot de passe
- Vous êtes en télétravail RDS: En cliquant sur ctrl/Alt/Fin simultanément puis sur modifier mot de passe (Attention : identifiant initiale du prénom et nom tout en minuscule)

Nous pouvons tous être victimes d'une cyberattaque.

L'important est d'adopter la bonne pratique en le signalant immédiatement à l'équipe informatique pour limiter les dégâts liés à l'intrusion.

2. Déconnectez l'appareil du réseau

Si vous êtes sur le site Tour W , débranchez votre ordinateur de la station d'accueil et du WIFI pour ne pas contaminer l'ensemble du réseau (Equivalent de la «Mise en mode avion»). Contacter l'Informatique en cas de doute

5. Consignes à Suivre

Cette procédure ne doit pas connaître de résistance ou d'hésitation. Elle doit être appliquée de façon immédiate et responsable.

L'équipe informatique (administrateurs et référents) fera le nécessaire rapidement pour vous trouver une solution de secours.

3. Arrêt et Mise en Sécurité

- **N'Eteignez pas votre appareil !** Cette action peut complètement bloquer votre matériel et impossible de le relancer en cas d'investigation ou de récupération.
- Prévenir le service Informatique ou votre référent.

4. Informez l'équipe informatique

Contactez tout de suite :

Abilio MATIAS 01 47 76 53 27
Gaëlle BONTET 01 47 76 53 55
Et votre correspondant informatique .





OUTILS DE PROTECTION GSA+

- AUTHENTIFICATION FORTE
- VADE SECURE
- CAMPAGNE DE PHISHING
- AIDE SENSIBILISATION
- SERVEUR D'ARCHIVAGE
- INTERDICTION DES CLÉS USB
- SYNTHÈSE DES BONS REFLEXES

L' AUTHENTIFICATION FORTE – Mise en place 2021

L'authentification forte ou multi-facteurs (MFA) est une procédure d'identification qui fait appel à au moins deux authentifications pour vérifier l'identité de l'utilisateur qui souhaite se connecter.

Elle a pour objectif de rendre plus difficile, voire impossible, l'accès d'une personne qui aurait usurpé notre identité. Elle nous protège ainsi contre le vol d'identité, l'usurpation de compte et le phishing.

Il faut retenir que :

81% des cyberattaques seraient liées à des mots de passe insuffisamment sécurisés

99,9% de ces attaques peuvent être bloquées grâce à l'authentification Forte.

1. Accès RDS
1.1 – Lancement du RDS
1.2 – Entrée User / Passe

2. Accès INWEBO
2.1 – Ouverture sur les supports souhaités
2.2 – Entrez CODE PIN

3. Résultat
3.1 – Ouverture de RDS.

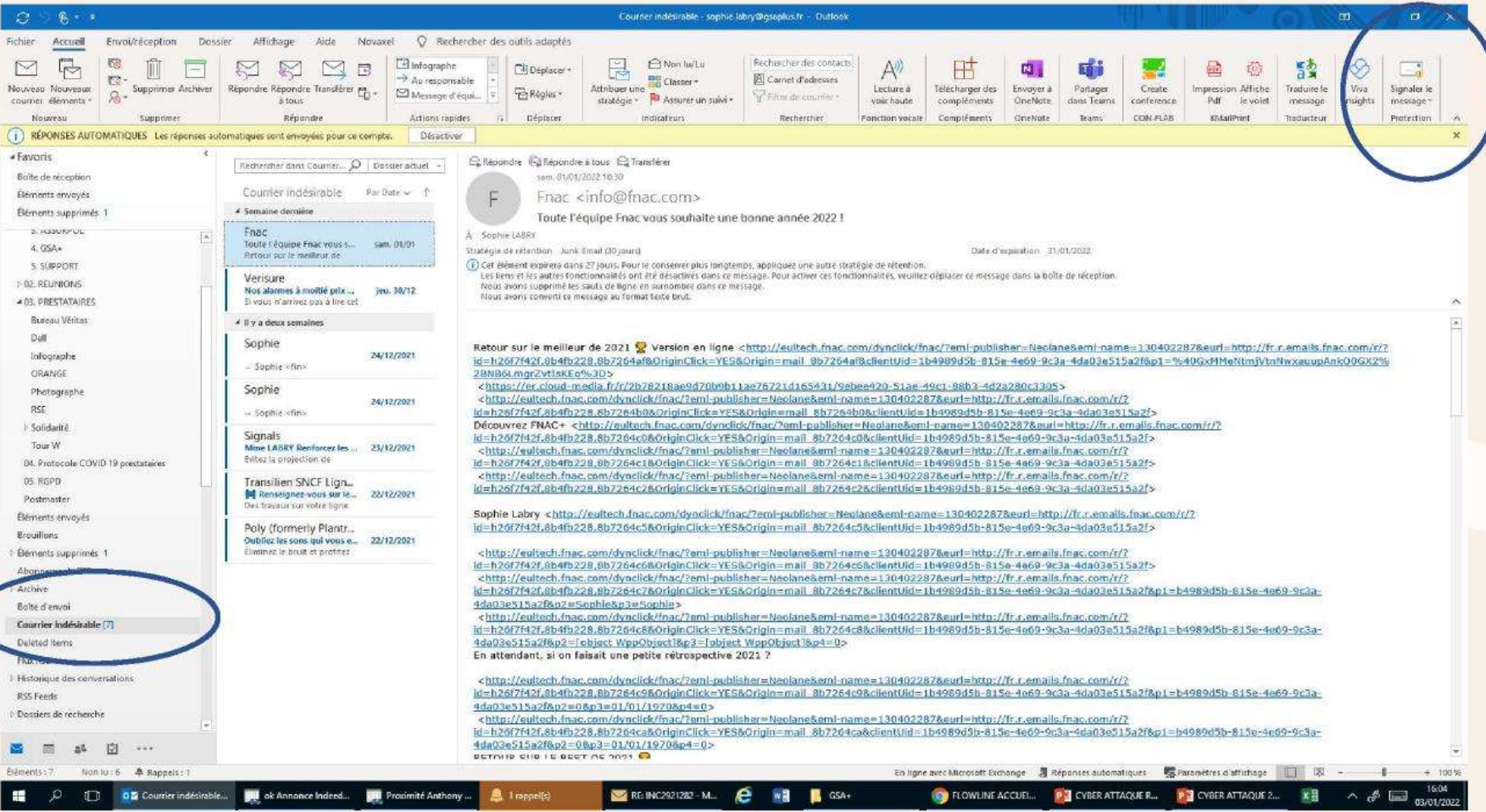


VADE SECURE

L'usurpation d'identité passe le plus souvent par le phishing via nos BAL professionnelles,

Pour éviter au maximum ce vol d'identité, le GSA+ a mis en place l'outil Vade Secure qui écarte de nos BAL les mails suspects, spam, phishing...

Vous pouvez également signaler un message suspect en cliquant sur l'icône en haut à droite.



 La campagne de formation / sensibilisation VADE SECURE est réalisée en début de chaque trimestre

CAMPAGNE DE PHISHING

La sensibilisation au phishing de ou hameçonnage est une priorité pour la sécurité.

Le phishing est responsable de 94% des ransomwares.

Face à ce constat, depuis 2020, le GSA+ a mis en place une campagne de phishing. Elle est résiliée une fois par an.

Son but est avant tout pédagogique, il faut s'assurer que l'utilisateur maîtrise les processus pour reconnaître un phishing.



Caractéristiques du phishing

- Expéditeurs
- Liens
- Pièces jointes
- Contenu du mail ou l'objet du mail



Reconnaître l'expéditeur

- Vérifier le nom de l'expéditeur
- Vérifier l'adresse en cliquant dessus
- En général le bon format doit être utilisateur@entreprise.com



Liens

- De préférence ne pas cliquer sur un lien dans un mail
- Passer la souris dessus pour vérifier le chemin du lien
- Chercher sur un moteur de recherche pour atteindre le site en question
- Contacter l'expéditeur si vous le connaissez



Les pièces jointes

- Redoubler de vigilance lorsque la pièce jointe contient un fichier avec une fin en .zip, .rar ou .exe
- Ne pas ouvrir si vous avez un doute sur l'expéditeur
- Contacter l'expéditeur si vous le connaissez

CAMPAGNE DE PHISHING


Le prénom est mal orthographié
La partie de l'adresse avant le @ ne correspond pas à l'identité.
Le nom de l'entreprise (après le @ - domaine) n'est pas correct

Via indique un relais,
l'expéditeur n'envoie donc pas du serveur GSA+
L'adresse après le via est suspecte car inconnue

En plaçant la souris sur le lien, le chemin apparaît.
Ce lien m'est inconnu, il est donc suspect je ne clique pas.

URL d'origine :
https://www.onlineservicetech.services/link/1/362utkwshmsdtLqed8tnavf0lenoglgayhw_ywc43sqtoborg1seoy7gsdgnaxgjkruclwv8qf54zozw3lqtrmdib96-q9h3x_xahwickxcomz_oy-hrkM4sduInpagzyn602qrmzymtkvubv36h9e0z9yazpys05kzatr5_1lbubjxgm8p-0ybhcnn
Cliquez ou appuyez pour suivre le lien.

Mail de sécurité de la tour W - Important

 **gaele bontet** <galebontet@gsaplus.fr> (gaelle bontet via mailrelaysrv.com)

Nous n'avons pas pu vérifier l'identité de l'expéditeur. Cliquez ici pour en savoir plus.
Le véritable expéditeur de ce message n'est pas le même que l'expéditeur normal. Cliquez ici pour en savoir plus.

Bonjour Jean-Wandrille ,

Je viens de recevoir un mail des services de sécurité de la tour W.

Merci d'en prendre connaissance, ci-dessous le lien d'accès.

[Lien d'accès](#)

Très bonnes fêtes de fin d'année !

Take care !

Bien cordialement,

GSA+
Groupement de services assurances

Gaëlle Bontet
Directeur GSA+
01 47 76 53 55
gaelle.bontet@gsaplus.fr
Tour W - 102, terrasse Boieldieu - 92085 Paris La Défense cedex

Si vous connaissez bien l'expéditeur, demandez-vous s'il s'exprime souvent ainsi.
En cas de doute n'hésitez pas à l'appeler



NOUVELLE AIDE A LA PRISE DE DECISION

Après validation du comité de direction d'octobre 2023, une nouvelle information va vous aider dans la prise de décision en cas de doute d'un mail frauduleux. Cette information se présentera sous forme de message dans l'entête du mail et qui vous signalera la provenance au niveau externe du mail reçu.

Cette information vous sera utile en cas de tentative d'usurpation du « Prénom/Nom » d'un collaborateur ou des domaines reconnus plus bas.

Cette information a pour objectif de vous sensibiliser lors de la vue de ce message.

« Attention mail externe , suspicion de phishing »

Ce contrôle va se réaliser via le domaine de l'expéditeur et validé par le service informatique de GSA+. Tout autre domaine en dehors des reconnus, seront considérés comme externes et donc susceptibles d'être dangereux. Voici à ce jour, les domaines considérés comme validés :

•@amsre.fr,	•@amsre.com	•@assuratome-app.com
•@assuratome.fr,	•@assuratome.com	•@assuratome.net
•@assuratome.eu	•@assuratome.org	•@assurpol.com
•@assurpol.eu	•@assurpol.fr	•@geiechs.eu
•@gsaplus.fr	•@gsaplus.eu	•@gsaplus.onmicrosoft.com

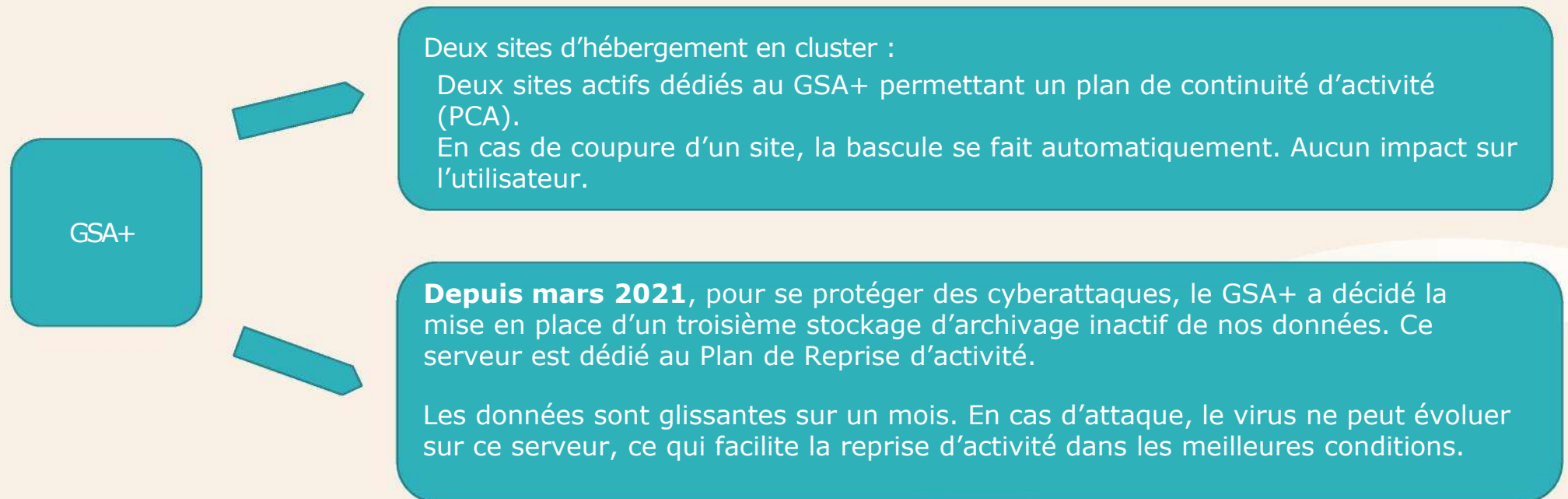
Pour information, les domaines sont validés, car ils ont des comptes mails associés. Si un domaine n'a pas de compte mail géré, il est inutile de l'ajouter.

Pour toute demande d'intégration de domaine à valider, merci de contacter le Responsable Informatique de GSA+.



SERVEUR D'ARCHIVAGE - S3 SUR SITE HERBERGEMENT DE LYON

Notre infrastructure est active depuis fin mars 2021 additionnée d'un serveur d'archivage :



INTERDICTION DES CLES USB OU PERIPHERIQUES EXTERNES SUR TOUS LES PC INFORMATIQUES

Les périphériques et clés USB sont rapidement devenus un des principaux vecteurs d'attaque, au 2^{ème} rang du classement des Cybermenaces. Utiliser une clé USB n'est donc pas sans risque et peut causer de graves préjudices :

- **prise de contrôle** de votre appareil,
- **espionnage** à distance,
- **blocage** ou même destruction totale grâce à la " Killer Key " qui détruit instantanément le système informatique du dispositif (tour, écran, etc.) grâce à une surcharge électrique.
- récupérer en quelques secondes, **les mots de passe enregistrés** en clair et de les faire transiter par la messagerie de la victime.

Le Comité de Direction a donc décidé d'interdire les clés USB sur l'ensemble des postes des collaborateurs du GSA+.

Seuls les correspondants informatiques pourront dans un cadre très exceptionnel, en avoir l'usage.

Les outils de remplacement :

SharePoint ou WeTransfert peuvent remplacer la clé USB et permettre l'échange de documents avec son correspondant.



SYNTHESE DES BONS REFLEXES

	Les bons réflexes des collaborateurs	Les protections infrastructure GSA+
L'hameçonnage	<p>Au moindre doute ou interrogation sur le mail reçu (objet du mail, pertinence des propos...):</p> <ul style="list-style-type: none">• vérifier la provenance avant l'ouverture des pièces jointes ou le clic sur le lien.• Vérifier par appel téléphonique du correspondant en cas de doute	<p>L'organisation de campagnes de phishing</p> <p>La mise en place de l'outil VADE SECUR, pour maximiser nos BAL.</p> <p>La relecture régulière des procédures pour une meilleure application en temps réel des bons réflexes.</p>
Le programme malveillant	<p>Il est important de s'assurer de la bonne provenance des installations de logiciels lorsqu'ils sont autorisés sur nos postes.</p>	<p>Nous sommes très limités dans l'installation de logiciels ou d'applications.</p> <p>Le service informatique limite fortement les risques en mettant en place des protections d'installations.</p>
L'usurpation d'identité	<p>Ne jamais renseigner son identifiant / Mot de passe suite à un clic sur un lien en provenance d'un mail avant d'avoir vérifié sa provenance réelle. (vérifier par appel téléphonique si doute)</p>	<p>L'outil INWEBO est installé sur tous les postes</p> <p>La double authentification empêchera l'accès à notre réseau en cas d'usurpation d'identité.</p>



QUE FAIRE EN CAS D'ATTAQUE

L'assurance des risques de cyberattaques a fait son entrée dans le code des assurances.

Pour obtenir une indemnisation des pertes et dommages causés par une atteinte à un système de traitement automatisé de données, la **victime devra avoir déposé plainte dans un délai de 72 heures après sa connaissance de l'infraction.**

[Loi n° 2023-22 du 24 janv. 2023, art. 5 et 29, JO 25 janv.](#)

Article 5

I. – Le titre II du livre Ier du code des assurances est complété par un chapitre X ainsi rédigé :

« CHAPITRE X »

« L'ASSURANCE DES RISQUES DE CYBERATTQUES »

« Art. L. 12-10-1. – Le versement d'une somme en application de la clause d'un contrat d'assurance visant à indemniser un assuré des pertes et dommages causés par une atteinte à un système de traitement automatisé de données mentionnée aux articles 323-1 à 323-3-1 du code pénal est subordonné au dépôt d'une plainte de la victime auprès des autorités compétentes au plus tard soixante-douze heures après la connaissance de l'atteinte par la victime. »

« Le présent article s'applique uniquement aux personnes morales et aux personnes physiques dans le cadre de leur activité professionnelle. »

II. – Le I **entre en vigueur trois mois après la promulgation de la présente loi.**

Cette Plainte doit être réalisée par le responsable de l'entreprise ou toute personne ayant une signature permettant de l'engager.



VOS REFERENTS INFORMATIQUES

GSA+

Abilio MATIAS 01 47 76 53 27

Ou en son absence

Gaëlle BONTET 01 47 76 52 50

Référents

ASSUROL - Delphine Guay 01 47 76 53 24

ASSURATOME – Philippe RENAUT 01 47 76 53 50

AMSRE – Céline MAISON 01 47 76 89 52





GROUPEMENT
 DE SERVICES
 ASSURANCE

TOUR WINTERTHUR
100 TERRASSE BOIELDIEU
PUTEAUX 92000

WWW.GSAPLUS.FR