RÉPUBLIQUE FRANÇAISE
*Liberté*
*Égalité*
*Fraternité*

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en cybersécurité

# MÉMENTO DE CYBERSÉCURITÉ

## à l'attention des dirigeants de TPE-PME

Étude, témoignages et recommandations

www.cybermalveillance.gouv.fr

CLUB EBIOS
cpme CONFÉDÉRATION DES PME
Mouvement des Entreprises de France
U2P union des entreprises de proximité

# SOMMAIRE

ÉDITORIAL ..... 3

L'ÉTUDE IMPACTCYBER TPE-PME ET SON CONSTAT ..... 4

RÉCITS, TÉMOIGNAGES ET RECOMMANDATIONS ..... 6

LA CAMPAGNE : VISUELS, KIT ..... 36

SE SECURISER AVEC MON EXPERTCYBER ..... 38

QUI EST DERRIÈRE L'OPÉRATION IMPACTCYBER ? ..... 40

REMERCIEMENTS ..... 43

RÉPUBLIQUE FRANÇAISE
*Liberté*
*Égalité*
*Fraternité*

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en cybersécurité

# ÉDITO

La nécessaire transformation numérique a largement contribué à augmenter la surface d'exposition des organisations aux risques cyber. Aujourd'hui, plus aucun secteur d'activité ni entité, quelle qu'en soit la taille, n'échappe aux cyberattaques.

Or, de plus en plus sophistiquées, les cyberattaques sont susceptibles d'entraîner de multiples répercussions pour les entreprises et leurs collaborateurs : impacts financier, commercial, réputationnel, juridique…, voire la cessation d'activité pour les plus fragiles. Pourtant, malgré la succession d'attaques et leur médiatisation, toutes les entreprises n'ont pas réellement pris la mesure des enjeux qu'elles représentent ni décidé par conséquent de mettre en œuvre les mesures nécessaires pour se protéger. C'est dans ce contexte que Cybermalveillance.gouv.fr a initié une réflexion avec ses membres dans le cadre d'un groupe de travail composé du Club EBIOS, de la CPME, du MEDEF et de l'U2P.

Son ambition ? Accompagner les TPE-PME, souvent les moins armées face aux menaces, de la prise de conscience des risques jusqu'à la sécurisation de leurs systèmes d'information. Cette démarche a donné naissance à l'opération ImpactCyber, articulée en 3 volets.

### 1. L'ÉTUDE IMPACTCYBER

Pour dresser un état des lieux précis, une étude sur le niveau de maturité cyber des TPE-PME a été réalisée par OpinionWay.

### 2. LA CAMPAGNE IMPACTCYBER

Fort de ces enseignements, une campagne de communication a été imaginée sous l'angle original des impacts d'une cyberattaque pour rappeler aux entreprises l'importance de sécuriser leurs systèmes d'information.

### 3. LE MÉMENTO IMPACTCYBER

Enfin, un mémento destiné aux TPE-PME avec des scénarios d'attaques inspirés de faits réels, des conseils cyber utiles pour se protéger et des témoignages de pairs représente le troisième volet de l'initiative ImpactCyber, lancée par Cybermalveillance.gouv.fr

Jérôme Notin,

*Directeur Général de Cybermalveillance.gouv.fr*

# L'ÉTUDE IMPACTCYBER TPE-PME

Ces dernières années, la cybersécurité est un enjeu sociétal qui s'est imposé à de nombreuses organisations. Les TPE-PME n'y ont pas échappé.

Mais quel est réellement leur niveau de maturité en matière de cybersécurité ? Pour établir ainsi un état des lieux précis de leur gestion de la sécurité informatique, Cybermalveillance.gouv.fr, le Club EBIOS, la CPME, le MEDEF et l'U2P ont souhaité lancer un baromètre. Réalisé par OpinionWay entre le 2 juin et le 7 juillet 2025 auprès de 588 entreprises de moins de 250 salariés, voici les principales conclusions de la 2ème édition.

## UNE AMÉLIORATION DE LA PERCEPTION DES ENJEUX ET DES USAGES CYBER

La tendance pour cette 2ème édition démontre que **les entreprises interrogées sont plus nombreuses à penser qu'elles sont fortement exposées, 44 %** (38 % en 2024) et mieux protégées avec **58 % des TPE-PME qui pensent bénéficier d'un bon ou très bon niveau de protection** (39 % l'an passé).

**Ces constats coïncident d'ailleurs avec les dispositifs de sécurité mis en place dont le nombre moyen augmente** de 3,62 en 2024 à 4,06.

Cette évolution semble permettre aux TPE-PME **de mieux comprendre les incidents avec 7 entreprises victimes sur 10 en capacité d'en identifier les causes contre 35 % l'an dernier.** Ainsi, 43 % ont déclaré que ces attaques étaient liées à l'hameçonnage contre 24 % l'an dernier, 18 % à des failles de sécurité (14 % en 2024) et 11 % à des consultations de sites Internet vérolés (5 % en 2024) .

Par ailleurs, ces résultats démontrent **une plus grande capacité des entreprises à faire face aux conséquences des incidents de sécurité.**

En effet, les TPE-PME ont tendance à moins accuser d'interruptions de service (29 % contre 35 %), de pertes financières (11 %/15 %) ou de vol de données (22 %/25 %) cette année.

**Enfin, cette conscience des enjeux est également perceptible en termes budgétaires.**

En 2025, les entreprises ont en effet témoigné d'une **augmentation significative de leur budget informatique par rapport à 2024 (19 vs 13 %).** Côté cybersécurité, même si les investissements restent faibles avec moins de 2000 € pour les 3/4 d'entre elles, **15 % prévoient néanmoins de faire évoluer à la hausse ce budget, soit 5 points de plus.**

# ...ET SON **CONSTAT**

## MALGRÉ CETTE ÉVOLUTION DE LA PERCEPTION CYBER DES ENTREPRISES, DE VRAIES RÉSISTANCES SUBSISTENT

Si elles semblent plus avisées face aux risques, les TPE-PME n'en restent pas moins lucides. Ainsi, même si la tendance met en avant des TPE qui déclarent être plus exposées, **80 % reconnaissent qu'elles ne sont toujours pas préparées aux attaques (49 % + 3 points) ou l'ignorent (31 %).**

D'ailleurs, **16 % des entreprises interrogées affirment avoir été victimes d'un ou plusieurs incidents au cours des 12 derniers mois.**

D'autre part, **près de 6 entreprises sur 10 (58 %) admettent encore qu'elles ne sauraient pas évaluer les conséquences d'une cyberattaque.** Les principales inquiétudes concernent la perte ou le vol de données (94 %), les répercussions financières (88 %), l'interruption d'activité (87 %) et leur réputation (82 %).

En termes d'offres, si 2/3 des TPE-PME prétendent connaître les solutions techniques, notamment les plus grandes, **1/2 seulement les juge réellement adaptées.** En dépit de la bonne connaissance qu'elles ont du marché et de son offre, l'étude révèle qu'**encore 1/4 des entreprises ne fait appel à aucun acteur spécialisé.**

Parmi les principaux obstacles à un niveau satisfaisant de sécurité informatique, les TPE-PME font état d'un **manque de connaissances et d'expertise (63 %), de contraintes budgétaires (61 %), et d'un manque de temps (59 %).** Près de 3 entreprises sur 10 considèrent ce sujet comme non prioritaire, un chiffre qui augmente auprès des entreprises répondantes cette année (+11 points).

## DES ATTENTES FORTES ET UNE SENSIBILISATION ESSENTIELLE

**Les TPE-PME sont une majorité -près de 6 sur 10- à reconnaître que la cybersécurité concerne tout le monde.** Pour y répondre, la moitié d'entre elles expriment des **besoins concrets en outils de sécurisation et en accompagnement.** Le soutien financier est également plébiscité et il arrive juste après la sensibilisation, qui demeure légèrement priorisée par les répondants.

**Ainsi, 6 TPE-PME sur 10 ont engagé des actions** de sensibilisation et de façon plus régulière, les plus mâtures étant dans les structures de plus de 10 salariés (90 %) ou celles du domaine des services (71 %).

# RÉCIT

## HÉLÈNE

*victime d'une intrusion dans le réseau informatique de son agence*

Hélène est la fondatrice et directrice d'une agence d'événementiel, une entreprise de 8 personnes, située à Lyon. Alors que l'équipe est en pleine préparation d'une série de conférences pour un nouveau client, un événement inattendu va survenir.

Ce jour-là, Pauline, l'une des employées d'Hélène qui travaille sur la préparation d'un congrès international, reçoit un e-mail contenant une pièce jointe intitulée « Détails de l'événement ». Pauline ouvre la pièce jointe sans se méfier.

Quelques minutes plus tard, tout disparaît : les commandes, les factures et les propositions commerciales pour les appels d'offres en cours. Tout le travail méticuleux de planification et de gestion de l'équipe est réduit à néant.

Hélène et son équipe tentent de restaurer les données à partir des sauvegardes. Mais à leur grand désarroi, ils découvrent que leurs sauvegardes ne fonctionnent pas correctement et qu'elle ne peut plus récupérer ses données.

L'entreprise est paralysée, incapable de tenir ses engagements envers ses clients.

Certains de ses clients se détournent d'Hélène. Cet incident porte atteinte à l'image de marque de l'agence et entraîne une perte financière conséquente pour l'entreprise.



RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en cybersécurité

L'ŒIL de l'expert

Jean-Jacques LATOUR

*Directeur Expertise Cybersécurité de Cybermalveillance.gouv.fr*

## *Que s'est-il vraiment passé ?*

« Dans ce scénario, l'entreprise rencontre plusieurs problèmes à la fois d'ordre technique mais aussi humain.

Pauline n'a pas été en mesure d'identifier un message malveillant. Elle en a ouvert une pièce jointe infectée ce qui a déclenché un virus destructeur. Ce virus n'a pas été détecté et a supprimé toutes les données de l'entreprise.

Enfin, avec un système de sauvegardes défaillant, l'entreprise n'a pas pu récupérer ses données dans un état stable. »

# REGARDS
# DE DIRIGEANTS

Cybermalveillance.gouv.fr s'est tourné vers des dirigeants d'entreprise pour recueillir leur avis sur ce récit et les faire réagir face aux impacts métiers subis par Hélène, dirigeante d'une agence d'événementiel.

**Alain**
*gérant d'une entreprise d'ingénierie de 8 personnes dans les Vosges*

« *Je pourrais parfaitement être touché par cet incident car je n'identifie pas les risques et donc ne les maîtrise pas correctement. Par ailleurs, je n'ai pas trouvé jusqu'à ce jour de prestataire informatique de confiance qui puisse correctement me conseiller sur le sujet.*

*J'ai pris conscience de la nécessité d'établir et de tester régulièrement un plan de reprise. Mais malheureusement faute de temps et de moyens pour une aide externe, je n'ai encore rien fait.*

*Mes premiers réflexes seraient de trouver un vrai prestataire informatique qui puisse à la fois être à l'écoute et m'apporter des conseils avant de vouloir placer des logiciels ou du matériel. Ensuite, mettre en place une gestion des mots de passe et enfin, élaborer un plan de reprise et des tests réguliers.* »



RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en cybersécurité

**Guillaume**
*fondateur d'une Fintech de 60 collaborateurs spécialisée dans l'épargne*

*« L'installation d'un logiciel malveillant ou la prise de contrôle d'ordinateur est totalement envisageable, notamment via la faille humaine. Pour l'éviter on met pas mal de choses en place, notamment des formations pour nos salariés. On imagine les conséquences des attaques dans nos plans de continuité d'activité et pas mal de scénarios figurent dans notre procédure. On est dans un métier de confiance et avoir des incidents de cybersécurité, au-delà des données personnelles qui pourraient fuiter, engendrerait des problèmes réglementaires avec notre autorité de tutelle. Notre image de marque sur laquelle on investit beaucoup et notre réputation, en ressortiraient ternies.*

*En tout état de cause, une attaque nous pousserait à encore plus investir en cybersécurité – tant dans les outils que dans la formation pour avoir des dégâts relativement mesurés. Notre infrastructure est en cours de construction générale autour de nos produits numériques et l'enjeu, c'est de régulièrement s'assurer que quelqu'un de mal attentionné n'arrive pas à pénétrer nos systèmes, à pirater nos données, à télécharger nos bases ou à piéger nos collaborateurs. »*

# L'ESSENTIEL

## Pour ÉVITER ce genre de scénario, ADOPTEZ CES BONNES PRATIQUES :

**Faites les mises à jour de l'ensemble de vos équipements** (ordinateurs, serveurs, téléphones mobiles, logiciels…) pour corriger leurs failles de sécurité.

**Utilisez un antivirus sur tous vos équipements** (ordinateurs, serveurs, téléphones mobiles…) et filtrez les accès à votre réseau avec un pare-feu.

**Sensibilisez vos collaborateurs aux différentes cybermenaces** et apprenez-leur à savoir repérer et réagir face à un message d'hameçonnage (*phishing*).

**Faites des sauvegardes régulières de vos informations,** conservez-en une copie déconnectée de votre système informatique et assurez-vous de leur bon fonctionnement en faisant des tests de restauration.

MON EXPERT CYBER

**Sécurisez-vous et faites-vous accompagner par un prestataire de confiance** labellisé en cybersécurité grâce à **Mon ExpertCyber**, le service de sécurisation de Cybermalveillance.gouv.fr



RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en cybersécurité

# Que FAIRE si vous êtes victime D'UN VIRUS ?

**Déconnectez l'équipement infecté d'Internet ou du réseau** pour éviter que le virus ne se propage à d'autres appareils.

**Identifiez la source de l'infection et son étendue** (faille de sécurité, message malveillant) et prenez les mesures nécessaires pour qu'elle ne puisse pas se reproduire.

**Récupérez ou tentez de faire récupérer par un professionnel les preuves disponibles** et séquestrez les équipements touchés.

Avant de remettre en état votre système, et en fonction du préjudice subi, **déposez plainte.**

**Faites une analyse antivirale complète (scan) de vos appareils**.

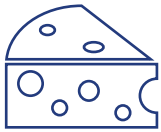
**Réinitialisez et réinstallez complètement les machines infectées** si le virus persiste.

Retrouvez l'intégralité des conseils :

# RÉCIT

## ANTOINE

*dirigeant d'une fromagerie, victime d'un rançongiciel*



Antoine est à la tête d'une fromagerie, une PME située dans le Puy-de-Dôme. Avec 50 employés, son entreprise produit 200 000 saint nectaires par an. Mais alors que l'entreprise fonctionne parfaitement, un imprévu va bouleverser son équilibre.

Un cybercriminel s'introduit dans le réseau de l'entreprise en forçant un mot de passe utilisé pour le télétravail. Exploitant des failles de sécurité non corrigées, l'attaquant prend rapidement le contrôle du réseau. Il déploie alors un rançongiciel qui chiffre toutes les données et les sauvegardes en ligne. Toute la chaîne de production, de la collecte du lait à la vente des fromages, est paralysée. La bureautique et la gestion commerciale ne répondent plus.

Antoine et son équipe découvrent rapidement l'étendue des dégâts. Les ordinateurs affichent tous le même message : une demande de rançon en échange de la clé de déchiffrement.

Les conséquences sont considérables. Antoine estime rapidement l'impact de l'incident : entre les tournées de lait qui n'ont pas été faites auprès des fournisseurs, les commandes non livrées, et le chômage technique pour la plupart de ses ouvriers, la cyberattaque entraîne un manque à gagner très important.

**Sans perspective de retour à la normale, Antoine perd plusieurs clients distributeurs qui ne l'ont pas attendu pour réapprovisionner leurs rayons. Les répercussions psychologiques sur toute l'équipe sont majeures.**

L'ŒIL de l'expert

## Jean-Jacques LATOUR

*Directeur Expertise Cybersécurité de Cybermalveillance.gouv.fr*

### *Que s'est-il vraiment passé ?*

Les attaques de type rançongiciel sont un des modes opératoires privilégié des cybercriminels. Ils représentent la 3e cause de recherche d'assistance des professionnels sur Cybermalveillance.gouv.fr et touchent tous types d'entreprises, y compris les plus modestes et moins protégées.

Dans ce cas, un des principaux vecteurs d'intrusion des cybercriminels dans le réseau de leurs victimes passe par leurs accès externes souvent insuffisamment sécurisés (mots de passe trop faibles, absence de double authentification, défaut de mise à jour de sécurité des points d'accès…).

Une fois implantés dans le réseau de leur victime, les cybercriminels vont prendre en otage leurs données en les chiffrant. Mais ils vont également chercher à détruire leurs sauvegardes pour empêcher toute perspective de retour à la normale, et ainsi accentuer la pression pour obtenir une rançon.

# REGARDS DE DIRIGEANTS

Cybermalveillance.gouv.fr s'est tourné vers des dirigeants d'entreprise pour recueillir leur avis sur ce récit et les faire réagir face aux impacts métiers subis par Antoine, dirigeant d'une fromagerie.

**Michèle**
*directrice d'une société de transport logistique dans les Vosges avec 1 collaborateur*

« *Ce scénario pourrait nous arriver. L'entreprise va se doter d'un serveur avec protection des données et sauvegarde journalière. Cela va apporter un certain avantage mais je me rends compte que cela ne sera pas suffisant en matière de cybersécurité. En tant que dirigeante d'entreprise, je réalise que les risques d'une cyberattaque ne sont pas évalués à leur juste niveau dans mon entreprise.*

*On entend souvent parler de cybersécurité, mais on se croit invincible jusqu'à ce qu'un incident survienne. Ma première décision serait de procéder à un audit approfondi des risques avec identification des actifs, des menaces et des éventuelles failles du système déjà en place.* »



RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en cybersécurité

**Mickaël**
*directeur d'une imprimerie de 43 salariés à Limoges*

*« Nous avons constaté à plusieurs reprises que des malwares avaient crypté notre serveur. Des sauvegardes journalières effectuées automatiquement permettent de le restaurer sans perte de données. Ce type de problème n'affecterait que nos activités administratives, commerciales et comptables.*

*Le véritable scénario catastrophe, au-delà d'un rançongiciel, ce serait qu'un attaquant s'introduise dans les systèmes informatiques des machines de production et supprime les applicatifs permettant de les faire fonctionner. On devrait faire un reset, ce qui entraînerait in fine l'immobilisation des outils de production pendant plusieurs jours, et là on ne pourrait pas livrer nos clients dans les temps.*

*Faire un état des lieux avec notre prestataire informatique n'est jamais la priorité et c'est peut-être un tort. On appelle quand il y a le feu car on est trop pris par le quotidien. »*

# L'ESSENTIEL

## Pour ÉVITER ce genre de scénario, ADOPTEZ CES BONNES PRATIQUES :


**Protégez les connexions à votre réseau depuis l'extérieur** en mettant en place une double authentification et en limitant le nombre de tentatives de connexions.

**Faites les mises à jour de l'ensemble de vos équipements** (ordinateurs, serveurs, téléphones mobiles, logiciels…) pour corriger leurs failles de sécurité.

**Utilisez un antivirus sur tous vos équipements** et filtrez les accès à votre réseau avec un pare-feu.

**Faites des sauvegardes régulières de vos informations,** conservez-en une copie déconnectée de votre système informatique et assurez-vous de leur bon fonctionnement en faisant des tests de restauration.

MON EXPERT CYBER

**Sécurisez-vous et faites-vous accompagner par un prestataire de confiance** labellisé en cybersécurité grâce à **Mon ExpertCyber**, le service de sécurisation de Cybermalveillance.gouv.fr



RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en cybersécurité

# Que FAIRE si vous êtes victime D'UN RANÇONGICIEL ?

**Débranchez les machines touchées d'Internet** ou du réseau informatique pour éviter que l'attaque ne se propage à d'autres appareils.

**Ne payez pas la rançon** réclamée car vous n'êtes pas certain de récupérer vos données et vous alimenteriez le système mafieux.

**Récupérez ou tentez de faire récupérer par un professionnel les preuves disponibles** : message piégé, fichiers de journalisation (logs) de votre pare-feu, copies physiques des machines touchées ; à défaut, conservez les disques durs.

Avant de remettre en état votre système, **déposez plainte** en fournissant toutes les preuves en votre possession.

**Notifiez l'incident à la CNIL** s'il y a eu une violation de données personnelles.

**Identifiez la source de l'infection** et prenez les mesures nécessaires pour qu'elle ne puisse pas se reproduire.

**Appliquez une méthode de désinfection et de déchiffrement**, lorsqu'elle existe.

**Reformatez et réinstallez un système sain** sur les machines touchées, puis restaurez les sauvegardes des données disponibles.

**Faites-vous assister au besoin par des professionnels spécialisés en cybersécurité.**

Retrouvez l'intégralité des conseils :

# RÉCIT

## SAM

*dirigeant d'une maçonnerie, victime d'un piratage de messagerie*

Sam est le propriétaire d'une entreprise de BTP d'une dizaine de personnes située dans une commune rurale des Hautes-Pyrénées. Depuis plus de dix ans, Sam est réputé pour la qualité de son travail et son professionnalisme. En pleine période de chantiers, un incident vient perturber la stabilité de son entreprise.

La plupart du temps, Sam et ses collaborateurs sont sur le terrain et sinon, c'est au bureau qu'ils se retrouvent. Là-bas, il n'y a qu'un ordinateur et qu'une boîte e-mail. Tout le monde y a accès. Quand un client envoie une demande, il faut répondre rapidement.

Un jour, l'un des salariés reçoit un message de demande de connexion pour valider les identifiants de la boite e-mail de l'entreprise. Il s'exécute et les saisit, machinalement, entre 2 chantiers. 15 jours plus tard, Sam est contacté par l'un de ses maîtres d'œuvre.

Ce dernier s'étonne d'être relancé pour une facture de l'entreprise de maçonnerie qu'il a déjà payée. En reprenant ses comptes, Sam constate que le virement n'a pas été effectué, mais en confrontant les factures avec son client, il découvre que la première était à son nom mais contenait un RIB inconnu.

Sam est stupéfait, il réalise qu'un escroc a falsifié son RIB et qu'il a détourné des règlements à son insu. Résultat : les clients qui avaient déjà honoré leur facture refusent de la régler une seconde fois et l'entreprise est confrontée à une perte financière majeure.

**Cette fraude compromet gravement la trésorerie de l'entreprise. Les chantiers en cours sont menacés de retard, ce qui nuit à l'image de fiabilité que Sam a construite au fil des années et à sa réputation. Pire encore, des litiges juridiques s'annoncent car les clients lésés rejettent la faute sur l'entreprise.**



RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en cybersécurité

L'ŒIL de l'expert

Jean-Jacques LATOUR

*Directeur Expertise Cybersécurité de Cybermalveillance.gouv.fr*

## *Que s'est-il vraiment passé ?*

Les fraudes au virement sont l'une des principales causes de recherche d'assistance des entreprises sur Cybermalveillance.gouv.fr

Comme dans ce récit, elles sont généralement causées par le piratage d'un compte de messagerie qui ne dispose pas d'une double authentification suite à un message d'hameçonnage.

Une fois qu'il a obtenu l'accès au compte de messagerie de sa victime, le cybercriminel va pouvoir fouiller dans ses messages pour rechercher des transactions en cours, récupérer des modèles de factures pour les modifier avec son propre RIB et les envoyer aux clients qui les régleront sans se douter de la supercherie.

Pour masquer son activité, le cybercriminel mettra généralement en place de règles de filtrage et de transfert discrètes dans les paramètres de la messagerie de la victime afin qu'elle ne s'aperçoive pas des opérations frauduleuses qui sont commises en usurpant son identité.

# REGARDS DE DIRIGEANTS

Cybermalveillance.gouv.fr s'est tourné vers des dirigeants d'entreprise pour recueillir leur avis sur ce récit et les faire réagir face aux impacts métiers subis par Sam, dirigeant d'une entreprise de maçonnerie.

**François**
*dirigeant d'une entreprise de couverture de 18 salariés à Tours*

« *Cette situation pourrait tout à fait nous arriver. Il y a encore quelques mois, nous avions une IP fixe, pas de cryptage pour les accès distants et tous le même mot de passe : le nom de l'entreprise ! Depuis que nous avons changé de prestataire, nous avons des mots de passe différents et structurés, nous avons changé le serveur, créé des accès distants sécurisés et équipé l'entreprise d'un pare-feu. On sous-estime trop souvent ces petits détails, mais nos mails, notre serveur, contiennent des RIB et des coordonnées : il est très facile de se faire passer pour nous.*

*Si des attaquants veulent de l'argent ils le trouveront. L'entreprise, elle, doit ensuite honorer ses échéances. Un défaut de paiement et la relation bancaire ou fournisseur auraient un impact majeur sur le long terme, sur les projets et le développement et de l'entreprise.*

*Sensibiliser les équipes me paraît prioritaire ; et ensuite, avoir des outils informatiques à jour et un partenaire sérieux à ses côtés, essentiel.* »



RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en cybersécurité

**Michèle**
*directrice d'une société de transport logistique dans les Vosges avec 1 collaborateur*

*« Une usurpation de messagerie aurait des conséquences désastreuses pour notre entreprise qui gère des flux logistiques à l'échelle mondiale. Nous envoyons des instructions cruciales aux différents acteurs de la chaîne pour garantir que les marchandises arrivent à temps et au bon endroit. Sans ces communications, la chaîne logistique serait paralysée et entraînerait une perte de clients. »*

**Arnaud**
*directeur d'une Maison de bijouteries en région Centre*

*« Oui, cet incident pourrait nous arriver de façon probable. Nous ne sommes pas à l'abri car il nous arrive de payer les fournisseurs par virement et de recevoir des RIB par mail, même si j'ai l'habitude de rappeler les gens. Mon premier réflexe cyber serait de vérifier avec un prestataire informatique à quel endroit il peut y avoir une faille. »*

# L'ESSENTIEL

## Pour ÉVITER ce genre de scénario, ADOPTEZ CES BONNES PRATIQUES :

**Sensibilisez vos collaborateurs aux différentes cybermenaces** et apprenez-leur à savoir repérer et réagir face à un message d'hameçonnage (*phishing*).


**Activez la double authentification pour les accès à votre messagerie** afin d'éviter que quelqu'un puisse s'y connecter votre insu.

**Informez vos clients que vous n'envoyez jamais de RIB par mail** ou mettez en place avec eux une procédure de confirmation du numéro de RIB par appel téléphonique par exemple.

MON EXPERT CYBER

**Sécurisez-vous et faites-vous accompagner par un prestataire de confiance** labellisé en cybersécurité grâce à **Mon ExpertCyber**, le service de sécurisation de Cybermalveillance.gouv.fr



RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en cybersécurité

# Que FAIRE si vous êtes victime D'UN PIRATAGE DE COMPTE OU DE MESSAGERIE ?

Si vous ne pouvez plus vous connecter à votre compte, **contactez le service concerné ou votre support informatique pour signaler votre piratage et demandez la réinitialisation de votre mot de passe.**

Dans vos paramètres de récupération de compte, **assurez-vous que votre numéro de téléphone et votre adresse mail de récupération soient les bons**. Si ce n'est pas le cas, changez-les immédiatement.

**Vérifiez également l'absence de règle de filtrage ou de redirection des messages** qui auraient pu être mises en place par le cybercriminel pour intercepter ou se faire renvoyer automatiquement vos messages.

**Changez au plus vite votre mot de passe et activez si possible la double authentification**. Changez également sans tarder le mot de passe piraté sur tous les autres sites ou comptes sur lesquels vous pouviez l'utiliser.

**Déconnectez ou supprimez de votre compte** tout appareil ou session active inconnus .

**Prévenez tous vos contacts de ce piratage** pour qu'ils ne soient pas victimes à leur tour des cybercriminels qui les contacteraient en usurpant votre identité.

En fonction du préjudice subi, **déposez plainte** en fournissant toutes les preuves en votre possession.

Retrouvez l'intégralité des conseils :

# RÉCIT

## JEAN

*dirigeant d'une boulangerie, victime d'un faux conseiller bancaire*

Jean est un artisan boulanger réputé, installé dans le quartier de Montmartre, à Paris. Quand il n'est pas dans son atelier, Jean s'occupe de l'administratif, depuis son ordinateur. Un jour, il reçoit un e-mail aux couleurs de sa banque l'invitant à se connecter à son compte en ligne pour vérifier une information.

Jean, préoccupé, clique sur le lien et saisit ses identifiants. Quelques heures plus tard, il reçoit un appel téléphonique de sa banque. L'individu se présente comme un conseiller anti-fraude. Il dispose de nombreuses informations détaillées concernant son compte bancaire et lui demande de confirmer des transactions frauduleuses sur celui-ci. Il réussit à convaincre Jean de la nécessité d'effectuer des opérations immédiates pour bloquer les transactions suspectes et pour sécuriser son compte.

Le boulanger, soucieux, suit les instructions du conseiller bancaire. En fin de journée, il se reconnecte sur son compte pour vérifier que tout est rentré dans l'ordre. Mais il est déjà trop tard. Quand il découvre la supercherie, ses économies et les fonds nécessaires pour faire tourner son entreprise ont disparu.

La situation est critique pour Jean. La boulangerie se retrouve soudainement sans liquidités nécessaires pour payer les fournisseurs, les employés et les dépenses courantes. L'attaque compromet gravement ses activités et menace la stabilité de son commerce.



RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en cybersécurité

L'ŒIL de l'expert

Jean-Jacques LATOUR

*Directeur Expertise Cybersécurité de Cybermalveillance.gouv.fr*

## *Que s'est-il vraiment passé ?*

Le message d'hameçonnage reçu par Jean est d'apparence et de prétexte crédibles.

Il se laisse donc abuser sans vérifier et saisit ses identifiants qui permettent au cybercriminel de se connecter au compte bancaire en ligne de Jean. L'escroc y découvre de nombreuses informations sur l'identité de Jean, les numéros et soldes de ses comptes, l'historique de ses transactions.

Muni de ces informations qui vont lui permettre de crédibiliser son arnaque, l'escroc appelle Jean en usurpant le numéro de téléphone de sa banque et en se présentant comme un conseiller du service antifraude. Il demande à Jean de confirmer de pseudo-transactions frauduleuses en cours sur ses comptes.

Avec un discours alarmiste mais professionnel et rassurant, le cybercriminel va mettre Jean en confiance pour lui faire valider diverses opérations (achats par carte bancaire, virements) pour soi-disant les annuler et mettre son argent en sécurité. En réalité, le cybercriminel aura ainsi détourné tous les fonds des comptes de Jean.

# REGARDS DE DIRIGEANTS

Cybermalveillance.gouv.fr s'est tourné vers des dirigeants d'entreprise pour recueillir leur avis sur ce récit et les faire réagir face aux impacts métiers subis par Jean, artisan boulanger.

**Fabienne**
*traductrice freelance à Montpellier*

« *Je me rends compte que cette situation pourrait tout à fait m'arriver surtout si je suis mise en confiance par l'appel de mon « supposé » banquier. La situation d'urgence que cette personne me présente et la panique face à une éventuelle fraude sur mon compte bancaire me feraient réagir rapidement et aller dans son sens.* »

**Henry**
*traiteur italien à Paris*

« *J'y ai déjà été confronté. Comme je ne connaissais pas mon interlocuteur, j'ai prétexté d'avoir des clients à servir pour mettre un terme à la conversation. Et dans la foulée, j'ai contacté mon chargé de clientèle qui lui doit s'identifier par code à chaque conversation (c'est ce qui m'avait mis la puce à l'oreille) et qui a infirmé les dires du faux conseiller.* »



RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en cybersécurité

**Catherine**
*fondatrice d'une conciergerie administrative*

*Cette situation me parle d'autant mieux qu'elle m'est déjà arrivée. Un jour, un conseiller du département anti-fraude de ma banque m'a téléphoné pour me dire qu'il y avait des mouvements suspects sur mon compte. Il m'a dit qu'il fallait tout bloquer pour que je récupère les fonds et m'a fait faire des validations sur mon application bancaire. Mon interlocuteur connaissait par cœur mon dossier. C'est en me rendant à la banque le lendemain que j'ai réalisé que j'avais été victime d'une arnaque.*

*C'est très humiliant de s'être fait avoir comme cela et j'avais sous-estimé l'impact psychologique en plus de l'aspect financier. Il y a un avant et un après : je suis beaucoup plus méfiante depuis. Mais je n'ai pas mis en place des mesures de protection pour autant, essentiellement par manque d'information. Je pense aussi que le sujet n'est pas abordable techniquement et financièrement parlant parce que ma structure est trop petite pour être concernée : à mon sens, c'est pour les grosses administrations ou les très gros groupes.*

# L'ESSENTIEL

## Pour ÉVITER ce genre de scénario, ADOPTEZ CES BONNES PRATIQUES :

**Apprenez à savoir repérer un message d'hameçonnage (*phishing*)** et à y réagir.

**Ne donnez jamais de codes, de mots de passe au téléphone** ou ne confirmez jamais d'opération sur votre application bancaire dont vous ne seriez pas à l'origine. Votre banque n'en a pas besoin pour bloquer une opération.

En cas d'appel d'un conseiller anti-fraude de votre banque, **raccrochez et rappelez votre conseiller bancaire** sur son numéro habituel pour vérifier l'information.



RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en cybersécurité

# Que FAIRE si vous êtes victime D'UN FAUX CONSEILLER BANCAIRE ?

**Méfiez-vous des appels ou messages (sms…) alarmants** qui vous informent d'opérations frauduleuses sur vos comptes et vérifiez l'information par vous-même en contactant votre banque par vos moyens habituels.

**Ne fournissez jamais de mots de passe, de codes et ne validez en aucun cas des opérations dont vous n'êtes pas à l'origine** même sous prétexte de les annuler.

**Faites opposition à votre carte bancaire sans délai et changez le mot de passe de votre compte bancaire en ligne** si les escrocs y ont accédé ou si vous le soupçonnez.

**Alertez votre banque** des opérations frauduleuses identifiées pour en demander l'annulation.

**Conservez les preuves** (numéros de téléphone, messages ou mails reçus, ordres de virement, relevés de paiements, etc.).

**Déposez plainte** en fournissant toutes les preuves en votre possession.

**Réalisez une analyse (scan) antivirale complète de vos appareils** pour rechercher d'éventuelles infections qui auraient pu être à l'origine de la fraude.

Retrouvez l'intégralité des conseils :

# RÉCIT

**JULIE**
*dirigeante d'un cabinet de conseil en stratégie, victime d'un vol de données sur ses serveurs*

Julie est dirigeante d'un cabinet de conseil en stratégie établi à Toulouse. Depuis des années, elle accompagne plusieurs entreprises, et entretient une relation de confiance avec ses clients.

Un matin, en arrivant au bureau, Julie prend connaissance d'un message alarmant reçu par mail. Si elle ne paie pas la somme de 10 000 €, on la menace de rendre publiques les infos de ses clients : bilans, audits, plans d'actions, données personnelles des salariés… Et même des projets ultra-confidentiels.

Julie réalise qu'elle s'est vraiment fait pirater au moment où le cybercriminel lui montre des preuves de ce qu'il détient. Consciente des conséquences désastreuses que pourrait entraîner la divulgation de ces informations vis-à-vis de ses clients, Julie prend la décision difficile de payer la rançon exigée. Mais malgré le paiement effectué, l'escroc publie les informations volées, exposant ainsi les dossiers personnels de ses clients.

Cette attaque est lourde de conséquences : la réputation de Julie est gravement ternie. Certains de ses clients décident de mettre fin à leur collaboration avec le cabinet, par peur de compromettre leur propre sécurité et réputation.

L'ŒIL de l'expert

Jean-Jacques LATOUR

*Directeur Expertise Cybersécurité de Cybermalveillance.gouv.fr*

## *Que s'est-il vraiment passé ?*

« Le serveur de fichiers sur lequel Julie stocke toutes les données confidentielles de ses clients et qui est accessible à distance sur Internet a été piraté.

Les causes les plus fréquentes de ce type de piratage sont des accès à distance insuffisamment sécurisés et une absence de mises à jour des équipements exposés sur Internet qui laissent accessibles des failles de sécurité.

Le pirate qui réussit à accéder au système comprend vite l'avantage qu'il peut tirer des informations sensibles auxquelles il accède pour faire chanter sa victime. Mais considérer que payer une rançon est une solution est une fausse bonne idée. En effet, les cybercriminels sont avant tout motivés par l'appât du gain et ils n'hésiteront pas à revendre des données à des personnes qui pourraient être intéressées pour faire chanter ou escroquer les clients.

Lorsque l'on détient des données confidentielles, des mesures de sécurité renforcées et pas toujours très coûteuses, sont à mettre en place pour éviter ce type de situation qui peut porter préjudice, non seulement à une entreprise, mais également aux personnes qui lui ont confié leurs informations. »

# REGARDS
# DE DIRIGEANTS

Cybermalveillance.gouv.fr s'est tourné vers des dirigeants d'entreprise pour recueillir leur avis sur ce récit et les faire réagir face aux impacts métiers subis par Julie, dirigeante d'un cabinet de conseil.

**Mickaël**
*directeur d'une imprimerie de 43 salariés à Limoges*

*« Nous, on n'a pas beaucoup de données clients. Les fichiers, ça rentre, ça sort donc on n'est pas concernés car on ne stocke pas les données. Le seul truc délicat, c'est quand on communique des fichiers de routage. Pour certains clients, on a des données confidentielles envoyées par e-mail. C'est à la marge mais ça pourrait nous arriver.*

*On est considérés comme une cible mineure, peut être à tort. Depuis le Covid, on a l'impression d'avoir vécu le pire, tout le reste est anecdotique. Et si on nous bloque les fichiers, les clients nous les renverront. C'est vrai que cela pourrait entraîner une altération du lien de confiance. Mais c'est une question de probabilité, de priorités et surtout de coût. »*



RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en cybersécurité

**Benoît**
*dirigeant d'un cabinet d'expert-comptable de 4 personnes*

*« Nous espérons que ce type d'incident ne nous touchera pas car notre organisation repose essentiellement sur notre hébergeur depuis 2016. Tout ce qui est à l'intérieur de nos sessions est sous son contrôle et sa surveillance. Aucun fichier n'est enregistré en local et les fichiers sensibles sont également protégés par un mot de passe assez fort (au moins 12 caractères, chiffres lettres et caractères spéciaux), changé tous les 90 jours et après toute intervention. Pour accéder à nos outils, il est donc indispensable de s'authentifier ; aucune application n'est autorisée en local, les mails sont consultables directement sur la session de travail. Mes collaborateurs et moi-même respectons le protocole qu'il a défini et sommes sensibilisés.*

*Mais personne n'est à l'abri – la preuve, la semaine dernière notre hébergeur nous a informés d'une attaque qui n'a eu aucun impact sur nos données, puisque le trafic a été immédiatement stoppé.*

*Et si c'était le cas, je stopperais tout trafic et ne communiquerais en aucun cas avec les hackeurs. Je ne paierais aucune rançon, je contacterais mon hébergeur pour faire le point sur l'ampleur de l'attaque et les données impactées. J'appellerais mon assureur pour la marche à suivre car dans notre contrat Responsabilité Civile, nous avons une garantie spécifique « Cyber Risques ». En ma qualité de co-traitant et co-responsable de certaines données, si le piratage est avéré, j'informerai les clients concernés dans un délai de 72 heures pour qu'eux aussi puissent à leur tour entamer des démarches. »*

# L'ESSENTIEL

## Pour ÉVITER ce genre de scénario, ADOPTEZ CES BONNES PRATIQUES :

**Faites régulièrement les mises à jour de l'ensemble de vos équipements** (ordinateur, serveurs, téléphones mobiles, logiciels…) pour corriger leurs failles de sécurité.


**Protégez les connexions à votre réseau depuis l'extérieur** en mettant en place une double authentification et en limitant le nombre de tentatives de connexions.

**Filtrez les accès extérieurs** à votre réseau avec un pare-feu.

MON EXPERT CYBER

**Sécurisez-vous et faites-vous accompagner par un prestataire de confiance** labellisé en cybersécurité grâce à **Mon ExpertCyber**, le service de sécurisation de Cybermalveillance.gouv.fr



RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en cybersécurité

# Que FAIRE si vous êtes victime D'UN PIRATAGE INFORMATIQUE ?

**Mettez en quarantaine les équipements** concernés par l'incident.

**Identifiez la source de l'intrusion** (faille de sécurité, message malveillant…) pour la corriger.

**Récupérez ou tentez de faire récupérer par un professionnel les preuves disponibles :** journaux (logs) des pare-feu et serveurs, copie complète (physique) des équipements compromis et de leur mémoire…

**Déposez plainte** avec toutes les preuves en votre possession.

**Réalisez une analyse antivirale complète** de l'ensemble de vos équipements.

**Réinstallez le système** compromis depuis une sauvegarde antérieure à l'attaque.

**Changez les mots de passe** d'accès aux équipements touchés.

**Mettez à jour les logiciels et équipements** avant la remise en service de votre système.

**Notifiez l'intrusion à la CNIL** en cas de violation de données à caractère personnel.

Retrouvez l'intégralité des conseils :

# LA CAMPAGNE
## VISUELS, KIT

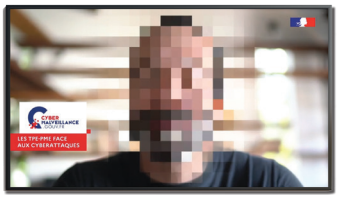
Les récits d'Hélène, d'Antoine, de Sam, de Jean et de Julie sont fictifs mais inspirés de faits réels.

Trois d'entre eux ont été utilisés pour créer une campagne de communication sous un angle original : celui des clients.

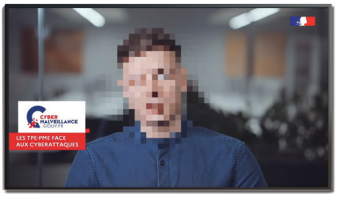
En effet, pour responsabiliser les TPE-PME, déclencher une prise de conscience et les convaincre de faire de l'enjeu cybersécurité une priorité, l'agence de création a décidé d'utiliser l'angle de leur réputation auprès de leurs clients, avec le message « Pour garder vos clients, protégez-vous dès maintenant ».

Les trois films réalisés pour cette campagne sont par ailleurs déclinés à travers des affiches, des prospectus, des kakémonos et des bannières pour être largement diffusés.

Nous vous invitons à les découvrir et à les relayer dans votre entourage professionnel afin d'inciter vos interlocuteurs à se protéger.









Retrouvez l'intégralité de la campagne :



RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en cybersécurité


DAVID,
MAÎTRE D'ŒUVRE
"NOTRE MAÇON
S'EST FAIT PIRATER SA BOÎTE MAIL.
DU COUP, LE CHANTIER EST BLOQUÉ."
Cybermalveillance.gouv.fr
TPE-PME FACE AUX CYBERATTAQUES
POUR GARDER VOS CLIENTS,
PROTÉGEZ-VOUS DÈS MAINTENANT.
Cybermalveillance.gouv.fr
Découvrez 4 conseils simples
et efficaces pour vous protéger.
CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en cybersécurité
→ RDV SUR
CYBERMALVEILLANCE.GOUV.FR/SAM


RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité
CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en cybersécurité
DAVID,
MAÎTRE D'ŒUVRE
"NOTRE MAÇON
S'EST FAIT PIRATER SA BOÎTE MAIL.
DU COUP, LE CHANTIER EST BLOQUÉ."
TPE-PME, FACE AUX CYBERATTAQUES
Pour garder vos clients,
protégez-vous dès maintenant.
Pour découvrir des conseils simples à adopter ou vous faire accompagner par un prestataire labellisé en cybersécurité grâce à « Mon ExpertCyber ».
Campagne réalisée en partenariat avec :
CLUSIF
cpme
U2P


RÉPUBLIQUE FRANÇAISE
MARC,
CHEF DE RAYON
FROMAGES
"ON AVAIT UN SUPER FOURNISSEUR.
MAIS IL A SUBI UNE CYBERATTAQUE.
RÉSULTAT : ON N'A PAS PU
APPROVISIONNER NOTRE RAYON".
TPE-PME, FACE AUX CYBERATTAQUES
Pour garder vos clients,
protégez-vous dès maintenant.
Découvrez 5 conseils simples et efficaces
Campagne réalisée en partenariat avec
TPE-PME face aux cyberattaques,
5 conseils simples à adopter !
1 Activez la double authentification pour limiter les intrusions.
2 Faites les mises à jour de l'ensemble de vos ordinateurs, serveurs, téléphones mobiles, logiciels... pour corriger les failles de sécurité.
3 Utilisez un antivirus sur tous vos équipements et filtrez les accès à votre réseau avec un pare-feu.
4 Faites des sauvegardes régulières de vos informations, conservez-en une copie déconnectée de votre système informatique et assurez-vous de leur bon fonctionnement en faisant des tests de restauration.
5 Sécurisez-vous en vous faisant accompagner par un prestataire labellisés en cybersécurité grâce à « Mon ExpertCyber ».

MON EXPERT CYBER

# Protégez les systèmes d'information de votre organisation

# GRÂCE À MON EXPERTCYBER

Pour accompagner les professionnels dans la gestion de leur cybersécurité et dans la sécurisation de leurs systèmes d'information, Cybermalveillance.gouv.fr propose une mise en relation avec des professionnels labellisés ExpertCyber qualifiés.

## **Qu'est-ce que Mon ExpertCyber,** le service de sécurisation de Cybermalveillance.gouv.fr ?

Face aux graves préjudices que peuvent entraîner les cybermalveillances, il est essentiel de protéger son organisation en amont contre le risque cyber. C'est pourquoi Cybermalveillance.gouv.fr a créé sur sa plateforme Mon ExpertCyber, un service dédié à la sécurisation des systèmes d'information. Il permet aux publics professionnels de bénéficier d'une mise en relation directe avec un prestataire de confiance qualifié et certifié dans l'installation de nouveaux systèmes d'information ou la sécurisation de systèmes existants.



RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en cybersécurité

MON EXPERT CYBER

## En quoi les professionnels labellisés ExpertCyber sont-ils qualifiés ?

Les prestataires sont labellisés ExpertCyber à l'issue d'un audit réalisé par l'AFNOR. Le label ExpertCyber est ainsi un gage de qualité pour les organisations qui peuvent en attendre :

- un niveau d'expertise et de compétences en cybersécurité ;
- un conseil de qualité pour prévenir la survenue d'actes de cybermalveillance et sécuriser leurs installations informatiques ;
- une conformité administrative (respect du cadre législatif et réglementaire, traitement des données personnelles conforme au RGPD…) ;
- un sens de l'intérêt général (veille et remontée d'incidents, conservation de la preuve numérique…).

## Qui peut faire appel à un professionnel labellisé ExpertCyber ?

Les prestataires ExpertCyber s'adressent à un public professionnel, soit toute entité justifiant d'une activité professionnelle (entreprise, association, collectivité), quels que soient son secteur, sa taille ou encore le nombre de salariés…

## Protéger mon organisation grâce à Mon ExpertCyber ?

Vous êtes un professionnel et souhaitez sécuriser vos systèmes d'information ? Grâce à Mon ExpertCyber, il vous suffit de répondre à quelques questions pour être mis en relation avec des prestataires labellisés ExpertCyber via la plateforme Cybermalveillance.gouv.fr

# QUI EST DERRIÈRE L'OPÉRATION IMPACTCYBER ?

**Ce mémento s'inscrit dans le cadre de l'opération ImpactCyber menée par Cybermalveillance.gouv.fr, le Club EBIOS, la CPME, le MEDEF et l'U2P. Voici une présentation de chacune de ces entités.**

Cybermalveillance.gouv.fr est la plateforme du Groupement d'Intérêt Public Action contre la cybermalveillance (GIP ACYMA). Créé en 2017, ce dispositif national a pour missions l'assistance aux victimes d'actes de cybermalveillance, la protection des organisations, la sensibilisation aux risques numériques, et l'observation de la menace sur le territoire français, qui s'illustrent notamment au travers des services suivants : Mon ExpertCyber, SensCyber et AlerteCyber. Ses 65 membres issus du secteur public, du privé et du domaine associatif contribuent à sa mission d'intérêt général pour ses 3 publics : particuliers, entreprises et collectivités. Cybermalveillance.gouv.fr a accueilli, en 2023, 3,7 millions de visiteurs uniques sur son site Internet et 280 000 personnes sont venues y rechercher une assistance.

Créé en 2006, le Club EBIOS est une association indépendante à but non lucratif (Loi 1901), composée d'experts individuels et d'organismes. Il supporte et enrichit le référentiel de gestion des risques français depuis 2003, avec le soutien de l'ANSSI. Il promeut et développe EBIOS RiskManager. En outre, son champ d'action s'étend à tous les usages de cette méthode et leurs dérivés dans le domaine de la gestion des risques. Le Club organise des réunions périodiques pour favoriser les échanges d'expériences, l'homogénéisation des pratiques et la satisfaction des besoins des usagers. Il constitue également un espace pour définir des positions et exercer un rôle d'influence dans les débats nationaux et internationaux.

La Confédération des Petites et Moyennes Entreprises est l'organisation patronale dédiée exclusivement aux TPE-PME françaises, tous secteurs confondus : industrie, services, commerce, artisanat et professions libérales. La CPME est implantée dans tous les départements et régions, y compris l'outre-mer, à travers 117 unions territoriales et 200 fédérations professionnelles. Parce que les PME subissent un véritable retard dans la digitalisation de leur activité, la CPME œuvre pour démontrer à leurs dirigeants l'importance vitale de réaliser leur transition numérique rapidement. Et parce que le numérique implique nécessairement des risques de cybermalveillance, la CPME s'investit également dans des actions de sensibilisation à la cybersécurité.

Le Mouvement des entreprises de France est la première organisation représentative des entreprises. Porte-parole de toutes les entreprises, il est l'interlocuteur privilégié des décideurs et des pouvoirs publics. Avec 119 organisations territoriales en France Métropolitaine et dans les outre-mer, 101 fédérations représentant 400 syndicats professionnels regroupant l'ensemble des secteurs d'activité, et 13 organisations associées et partenaires, il compte 190 000 entreprises adhérentes, dont une majorité de TPE-PME. En France, plus d'un salarié du privé sur deux travaille dans une entreprise affiliée au réseau Medef ».

L'U2P est l'une des trois organisations patronales interprofessionnelles françaises. Elle représente 3 millions d'entreprises de proximité dans les secteurs de l'artisanat, du commerce de proximité et des professions libérales, soit les 2/3 des entreprises françaises et réunit 5 organisations : la CAPEB (bâtiment), la CGAD (alimentation et hôtellerie-restauration), la CNAMS (fabrication et services), l'UNAPL (professions libérales) et la CNATP (travaux publics et paysage). L'U2P fédère 120 organisations professionnelles nationales et ses actions sont relayées par 115 U2P territoriales. En tant que partenaire social, l'U2P est régulièrement consultée par les pouvoirs publics et participe aux négociations nationales entre organisations d'employeurs et syndicats de salariés.

RÉPUBLIQUE FRANÇAISE
*Liberté*
*Égalité*
*Fraternité*

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en cybersécurité


# "ON AVAIT UN SUPER FOURNISSEUR. MAIS IL A SUBI UNE CYBERATTAQUE. RÉSULTAT : ON N'A PAS PU APPROVISIONNER NOTRE RAYON".

**Les conséquences d'un rançongiciel sont nombreuses pour une TPE-PME.
Blocage de l'informatique, de la production et des livraisons.
L'activité de l'entreprise est arrêtée. Les clients sont impactés.
Heureusement, il existe des réflexes simples à adopter pour se protéger.**

1. Activez la double authentification pour limiter les intrusions.
2. Faites les mises à jour de l'ensemble de vos ordinateurs, serveurs, téléphones mobiles, logiciels... pour corriger les failles de sécurité.
3. Utilisez un antivirus sur tous vos équipements et filtrez les accès à votre réseau avec un pare-feu.
4. Faites des sauvegardes régulières de vos informations, conservez-en une copie déconnectée de votre système informatique et assurez-vous de leur bon fonctionnement en faisant des tests de restauration.
5. Sécurisez-vous en vous faisant accompagner par un prestataire labellisé en cybersécurité grâce à « Mon ExpertCyber ».

## TPE-PME, FACE AUX CYBERATTAQUES
## Pour garder vos clients, protégez-vous dès maintenant.

Campagne réalisée en partenariat avec CLUB EBIOS, cpme, Mouvement des Entreprises de France, U2P

RÉPUBLIQUE FRANÇAISE
*Liberté*
*Égalité*
*Fraternité*

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en cybersécurité

# REMERCIEMENTS

**Ce mémento est le fruit de la collaboration entre Cybermalveillance.gouv.fr, le Club EBIOS, la CPME, le MEDEF et l'U2P que nous remercions pour leur implication au sein de l'opération ImpactCyber.**

Nous adressons nos sincères remerciements à tous les dirigeants d'entreprises et aux experts qui ont accepté de se rendre disponibles pour partager leur expérience et également leurs conseils afin de sensibiliser les TPE-PME aux enjeux cyber.

Enfin, nous remercions également plus largement celles et ceux qui soutiennent cette initiative et contribuent au rayonnement de ce mémento et de l'opération ImpactCyber.

## Les membres étatiques

- Premier Ministre (ANSSI) ;
- Ministère de l'Économie, des Finances et de la Souveraineté industrielle et numérique ;
- Ministère de l'Intérieur et des Outre-Mer ;
- Ministère de l'Éducation nationale et de la Jeunesse ;
- Ministère des Armées ;
- Ministère de la Justice ;
- Secrétariat d'état chargé du numérique.

## Les membres hors étatiques

**Aéma Groupe**, **AFCDP** (Association française des correspondants à la protection des données à caractère personnel), **Afnic** (Association française pour le nommage Internet en coopération), **AMF** (Association des maires de France et des présidents d'intercommunalité), **ANCT** (Agence Nationale de la cohésion des territoires), **APVF** (Associations des petites villes de France), **Assemblée nationale**, **Atempo**, **Avant de Cliquer**, **Avicca** (Association des Villes et Collectivités pour les Communications électroniques et l'Audiovisuel), **AWS** (Amazon Web Services), **Banque des Territoires** (groupe Caisse des Dépôts), **BNP Paribas**, **Bouygues Telecom**, **CAMF** (Commercants et artisans des métropoles de France), **CCI France** (Chambre de Commerce et d'Industrie), **CCR** (Caisse centrale de réassurance), **CDSE** (Club des directeurs de sécurité des entreprises), **CESIN** (Club des Experts de la Sécurité de l'Information et du Numérique), **Cinov Digital**, **CISCO**, **CLCV** (Association Consommation, Logement et Cadre de Vie), **Club EBIOS**, **CLUSIF** (Club de la sécurité de l'information français), **CNIL** (Commission nationale de l'informatique et des libertés), **CNLL** (Union des entreprises du logiciel libre et du numérique ouvert), **coTer numérique**, **Covéa**, **CPME** (Confédération des Petites et Moyennes Entreprises), **Déclic**, **EBEN** (Fédération des Entreprises du Bureau et du Numérique), **e-Enfance/3018**, **FEVAD** (Fédération du e-commerce et de la vente à distance), **France Assureurs**, **France Télévisions**, **France Victimes**, **Google France**, **Groupe SNCF**, **INC** (Institut National de la Consommation), **Institut des Actuaires**, **Kaspersky**, **La Poste Groupe**, **MAIF** (Mutuelle assurance des instituteurs de France), **MEDEF** (Mouvement des entreprises de France), **Mercatel**, **Microsoft France**, **Neuflize OBC**, **Nomios**, **Numeum**, **Orange Cyberdefense**, **Ordre des Experts Comptables**, **Palo Alto Networks**, **Régions de France**, **Signal Spam**, **SNCF**, **Stormshield**, **U2P** (Union des entreprises de proximité), **UFC-Que Choisir**, **Unaf (Union nationale des associations familiales)**.

RÉPUBLIQUE
FRANÇAISE
*Liberté*
*Égalité*
*Fraternité*

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en cybersécurité

# TPE-PME, FACE AUX CYBERATTAQUES POUR GARDER VOS CLIENTS PROTÉGEZ-VOUS DÈS MAINTENANT

**GIP ACYMA**
6 rue Bouchardon, 75010 Paris
**www.cybermalveillance.gouv.fr**

Suivez-nous sur :

V240927