CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

DOSSIER DE PRESSE

Cybermalveillance.gouv.fr

Lancement du dispositif national d'assistance aux victimes d'actes de cybermalveillance

Expérimentation en région Hauts-de-France

(juin à octobre 2017)

www.cybermalveillance.gouv.fr

MINISTÈRE DE L'ÉCONOMIE ET DES FINANCES
avec
MINISTÈRE DE LA JUSTICE
MINISTÈRE DE L'INTÉRIEUR
PREMIER MINISTRE

SGDSN

ANSSI

SOMMAIRE

Communiqué de presse
Paris, le 30 mai 2017

CYBERMALVEILLANCE.GOUV.FR

LANCEMENT DU DISPOSITIF NATIONAL D'ASSISTANCE AUX VICTIMES D'ACTES DE CYBERMALVEILLANCE

EXPÉRIMENTATION EN RÉGION HAUTS-DE-FRANCE DE JUIN À OCTOBRE 2017

Louis Gautier, Secrétaire général de la défense et de la sécurité nationale, Guillaume Poupard, Directeur général de l'ANSSI et Thierry Delville, Délégué ministériel aux industries de sécurité et à la lutte contre les cybermenaces, annoncent le lancement du dispositif d'assistance aux victimes d'actes de cybermalveillance, expérimenté de juin à octobre 2017 en région Hauts-de-France.

Au regard de l'augmentation du nombre d'attaques informatiques notamment de types rançongiciel et hameçonnage, la prévention et l'assistance technique de proximité portées aux victimes d'actes de cybermalveillance – particuliers, entreprises (TPE/PME) et collectivités territoriales jusqu'alors non accompagnés – constitue un objectif prioritaire.

Le 18 juin 2015, au cours de la présentation de la stratégie numérique du gouvernement, le Premier ministre Manuel Valls annonçait la mise en place d'un dispositif national d'assistance aux victimes d'actes de cybermalveillance. Objectif confirmé le 16 octobre de la même année lors de son intervention relative à la Stratégie nationale pour la sécurité du numérique.

Le dispositif, incubé par l'ANSSI et copiloté avec le ministère de l'Intérieur, qui s'adresse gratuitement aux particuliers, aux entreprises et collectivités territoriales (hors OIV), a pour objectifs :

- la mise en relation des victimes via une plate-forme numérique avec des prestataires de proximité susceptibles de restaurer leurs systèmes ;
- la mise en place de campagnes de prévention et de sensibilisation à la sécurité du numérique ;
- la création d'un observatoire du risque numérique permettant de l'anticiper.

Ce dispositif s'appuie d'une part sur les prestataires techniques de proximité et d'autre part sur les réseaux existants au niveau territorial, qu'il s'agisse des administrations de l'État (Gendarmerie, Police, représentants locaux de l'ANSSI) ou des collectivités et acteurs locaux (chambres consulaires, fédérations professionnelles, réseaux « transition numérique », etc.).

Mise en œuvre du dispositif : expérimentation en région Hauts-de-France

La plate-forme www.cybermalveillance.gouv.fr est disponible dès le 30 mai 2017 avec une phase expérimentale en Hauts-de-France, région représentative du territoire national par la diversité du taux d'urbanisation de ses départements et par l'implication des acteurs locaux dans la sécurité du numérique.

Elle propose deux parcours, un premier pour les victimes d'acte de cybermalveillance et un second pour les prestataires de services de proximité :

- Les victimes seront mises en relation avec des prestataires de proximité susceptibles de les assister grâce à un parcours permettant d'identifier la nature de l'incident.
- Les prestataires de toute la France souhaitant proposer leurs services peuvent d'ores et déjà s'enregistrer sur la plate-forme.

Un espace dédié à la sensibilisation des enjeux de la protection de la vie privée numérique est également accessible aux internautes. À terme, des campagnes de prévention seront lancées à l'échelle nationale.

Grâce au recueil de nombreuses statistiques, un observatoire sera créé en vue d'anticiper le risque numérique.

Création d'un groupement d'intérêt public

Pour remplir ces objectifs, un groupement d'intérêt public (GIP) a été constitué permettant l'implication financière et opérationnelle d'acteurs publics et privés.

Guillaume Poupard a été élu Président de l'Assemblée générale et du Conseil d'administration.

Jérôme Notin a été nommé, sur proposition de l'État, Directeur général du GIP.

Aux côtés du collège étatique, trois collèges représentant les parties prenantes ont été constitués en accord avec la convention constitutive : utilisateurs, prestataires de services de proximité et offreurs de solutions.

Tous les prestataires au niveau national peuvent d'ores et déjà s'inscrire sur la plate-forme

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

APPORTER UNE ASSISTANCE DE PROXIMITÉ AUX VICTIMES D'ACTES DE CYBERMALVEILLANCE

Une volonté gouvernementale

Au regard de l'augmentation du nombre d'attaques informatiques, l'amélioration de la prévention et de l'assistance portées aux victimes constitue un objectif prioritaire pour l'État français.

Le 18 juin 2015, au cours de la présentation de la Stratégie numérique du gouvernement, le Premier ministre annonçait la mise en place d'un dispositif national d'assistance aux victimes d'actes de cybermalveillance.

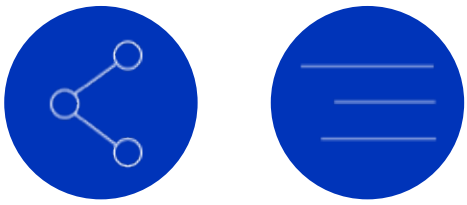
Objectif confirmé le 16 octobre dans la Stratégie nationale pour la sécurité du numérique.

« Un dispositif national sera mis en place destiné à porter assistance aux victimes d'acte de cybermalveillance. Grâce aux technologies mises en œuvre, le dispositif devra proposer aux victimes des solutions techniques s'appuyant sur des acteurs de proximité et faciliter les démarches administratives, notamment afin de favoriser le dépôt de plainte. »

« Ce dispositif aura également une mission de sensibilisation aux enjeux de protection de la vie privée numérique et de prévention »

Un projet interministériel

Incubé par l'ANSSI et copiloté avec le ministère de l'Intérieur, le dispositif Cybermalveillance.gouv.fr s'appuie sur les ministères de l'Économie et des Finances, de la Justice et le secrétariat d'État chargé du Numérique.



LES ACTEURS CONCERNÉS

Comme l'indique la Stratégie nationale pour la sécurité du numérique, « Les victimes d'actes de cybermalveillance [particuliers, entreprises et collectivités territoriales (hors opérateurs d'importance vitale] sont encouragées à déposer une plainte, auprès des services de police et de gendarmerie qui se sont adaptés au traitement de tels contentieux. Toutefois, la réponse qui leur est apportée dans ce cadre est centrée sur l'identification des auteurs présumés de la cybermalveillance et sur l'engagement éventuel de poursuites contre ces auteurs. Les victimes doivent pouvoir être orientées vers un service d'assistance au traitement de l'incident informatique à l'origine de l'acte de cybermalveillance ».

Les particuliers, les entreprises et collectivités territoriales (hors opérateurs d'importance vitale) ont désormais un interlocuteur.

Cybermalveillance.gouv.fr a été conçu pour répondre à leurs besoins.

3 MISSIONS ESSENTIELLES
ACCOMPAGNER - PRÉVENIR - ANTICIPER

Accompagner les victimes d'actes de cybermalveillance

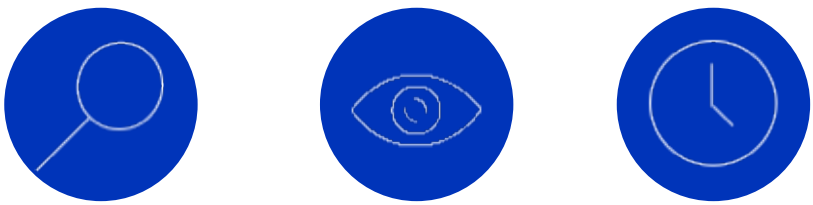
- Accueil via une plate-forme numérique
- En fonction du type d'attaque, mise en relation avec des prestataires de proximité susceptibles d'assister techniquement les internautes victimes ou redirection vers d'autres plate-formes existantes (PHAROS, signal-spam, etc.)
- Mise à disposition de fiches réflexes (comprenant les bonnes pratiques) liées à l'attaque dont les internautes ont été victimes

Prévenir et sensibiliser à la sécurité du numérique

- Contenus créés par le dispositif et disponibles sur la plate-forme
- Recommandations, diffusion de contenus et initiatives tiers
- Lancement de campagnes de sensibilisation sur le modèle de la sécurité routière
- Aide à la formation des policiers et gendarmes qui accueillent les victimes

Anticiper via la création d'un observatoire de la menace numérique

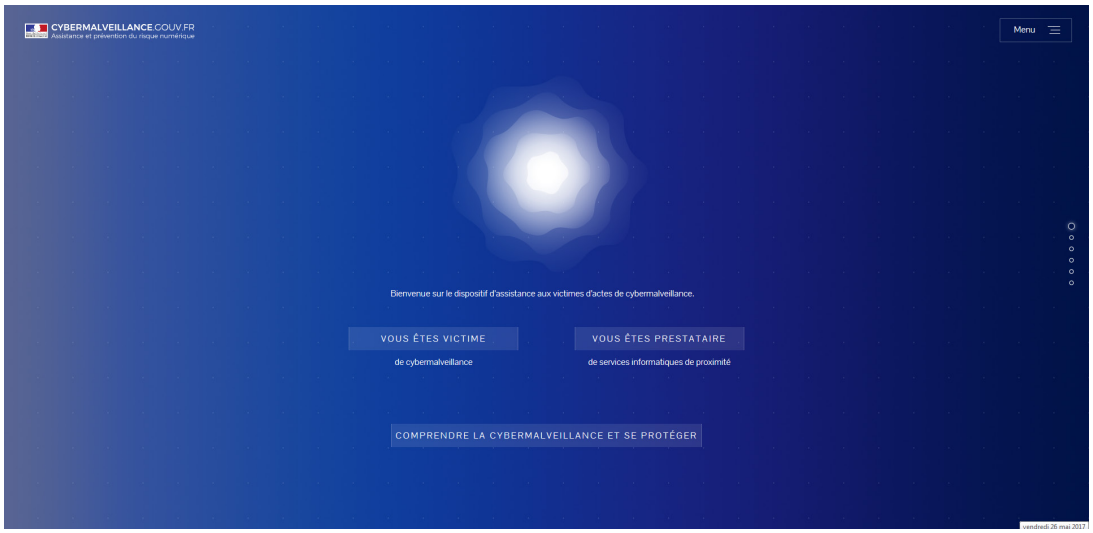
- Remontée d'informations anonymisées par les prestataires référencés
- Partage d'informations techniques avec les centres d'analyses tiers
- Transmission des informations aux autorités et aux prestataires
- Analyse des données et partage de statistiques



LA PLATE-FORME WWW.CYBERMALVEILLANCE.GOUV.FR

La plate-forme www.cybermalveillance.gouv.fr est disponible dès le 30 mai 2017 avec une phase expérimentale de juin à octobre en Hauts-de-France, région représentative du territoire national par la diversité du taux d'urbanisation de ses départements et par l'implication des acteurs locaux dans la sécurité du numérique.

Elle propose deux parcours, un premier pour les victimes d'acte de cybermalveillance et un second pour les prestataires de services de proximité.



1 Parcours « victime »

Après avoir cliqué sur « Vous êtes victime », l'internaute va bénéficier d'un accompagnement à travers un parcours dédié afin d'identifier l'incident de sécurité. Une fois ce dernier repéré, il sera orienté vers les prestataires de proximité susceptibles de restaurer son système.

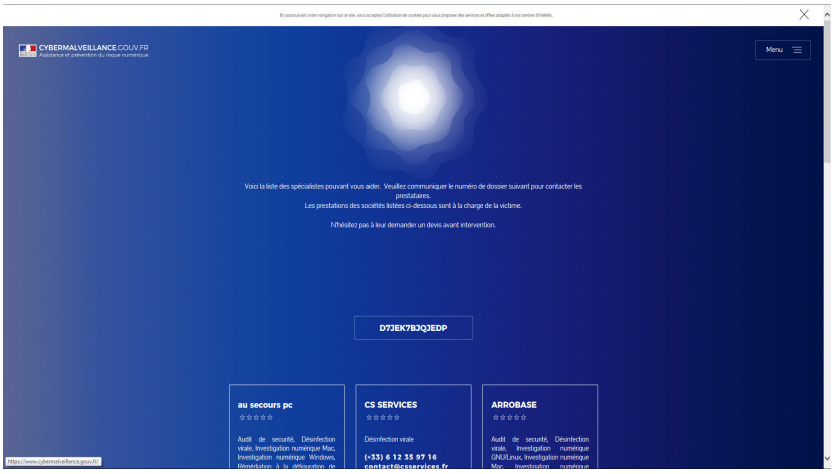
À l'issue de son parcours, il sera mis en relation avec :

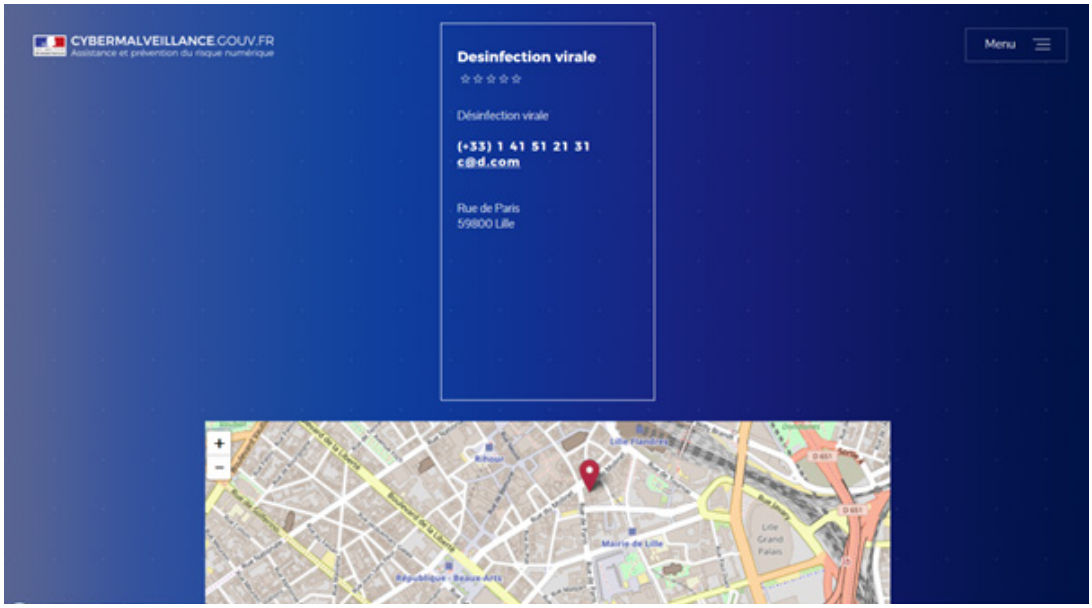
- un service existant qui l'aidera à résoudre son problème (signal spam, net écoute, pharos, etc.)

ou

- un prestataire de proximité. Dans ce cas, un numéro de ticket lui sera attribué.

La victime est fortement incitée à fournir au prestataire ce numéro de ticket qui permettra aux opérateurs de la plate-forme de l'optimiser et de réaliser des statistiques. En effet, le prestataire pourra compléter le diagnostic de la victime en ajoutant par exemple les codes malveillants utilisés pour l'attaque.





À l'issue du parcours, une fiche réflexe liée à l'incident rencontré sera communiquée à la victime, ainsi que les bonnes pratiques pour s'en prémunir. La qualification de l'infraction et/ou du délit lui sera également transmise en vue de l'assister ainsi que l'officier de police judiciaire dans le cadre d'un éventuel dépôt de plainte.

2 Parcours « prestataire »

Tous les prestataires au niveau national peuvent d'ores et déjà s'inscrire en ligne en saisissant les informations sur leur société et en s'engageant à respecter la charte d'engagement.

En acceptant la charte, le prestataire s'engage à :

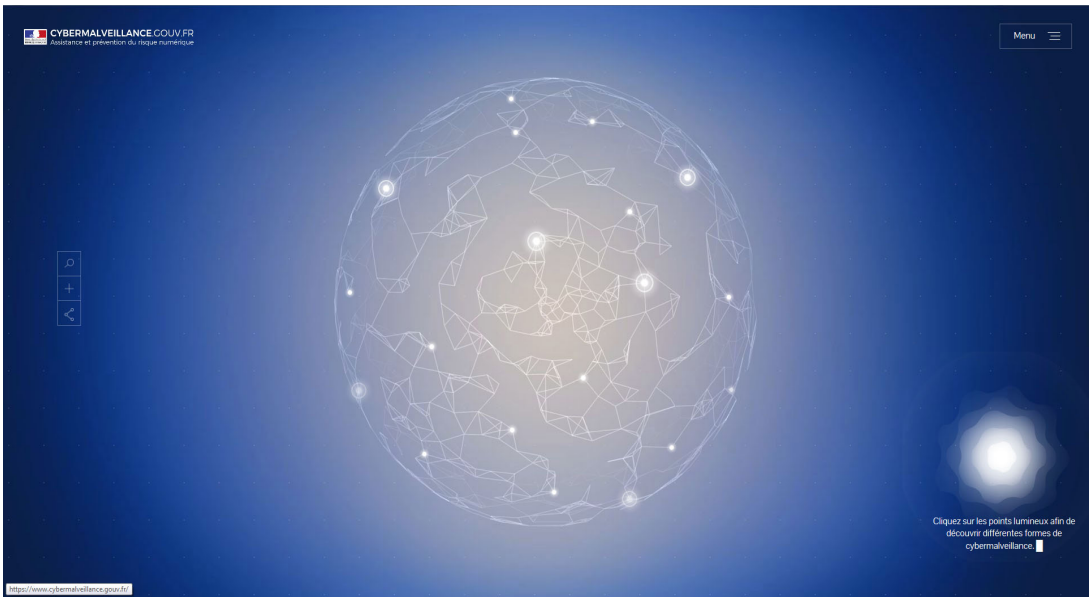
- respecter les bonnes pratiques à caractère commercial, publicitaire ou informatif à destination des clients ou usagers
- conserver les éléments de preuve technique en vue d'un éventuel dépôt de plainte par la victime
- remonter les éléments techniques anonymisés au dispositif à des fins de statistiques et d'analyse de la menace.

Cet engagement est un préalable au référencement sur la plate-forme.
À des fins de performance et de confiance, les utilisateurs seront invités à noter et commenter la prestation.

En cas de non-respect à la charte, le groupement d'intérêt public pourra radier de manière temporaire ou définitive le prestataire du référentiel publié par le dispositif.

3 Espace sensibilisation

La plate-forme propose des contenus de sensibilisation, sous forme de vidéos et de bonnes pratiques afin d'expliquer aux internautes comment se protéger face aux menaces numériques.

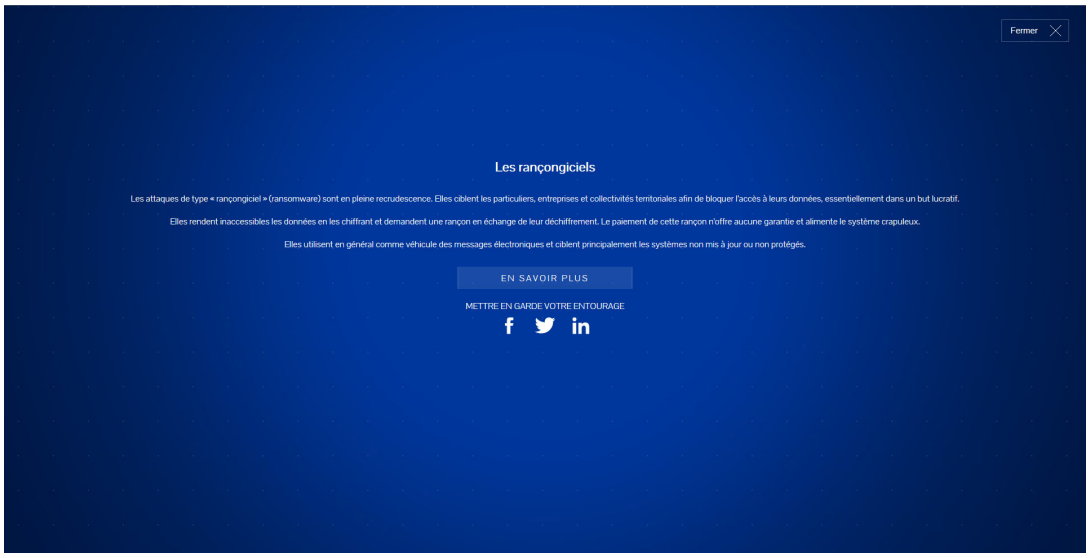


L'internaute n'a qu'à cliquer sur un point lumineux pour se voir proposer de visionner une vidéo sur l'un des thèmes suivant :

- Les messages électroniques peuvent contenir des virus
- Les rançongiciels
- Code de sécurité téléphone mobile
- Mots de passe différents

D'autres contenus seront ajoutés ultérieurement.

Une fois le film terminé, l'internaute bénéficie d'une explication de l'attaque et peut connaître les bonnes pratiques pour s'en prémunir.



Prestataire

La plate-forme a été réalisée par l'agence ISOBAR dans le cadre d'un marché à bon de commande passé par les services du Premier ministre.

LE GROUPEMENT D'INTÉRÊT PUBLIC ACYMA

STRUCTURE JURIDIQUE ADAPTÉE AUX ENJEUX

Pour remplir ces objectifs, un groupement d'intérêt public (GIP) pour le dispositif national d'assistance aux victimes d'actes de cybermalveillance a été constitué. Des acteurs publics et privés pourront ainsi s'impliquer financièrement et opérationnellement dans le dispositif.

À la suite de la publication le 5 mars 2017 de l'arrêté portant approbation de la convention constitutive du GIP, les membres fondateurs se sont réunis le 14 mars 2017 pour l'Assemblée générale constitutive.

M. Guillaume Poupard a été élu en qualité de Président de l'Assemblée générale et du Conseil d'administration.

M. Jérôme Notin a été nommé, sur proposition de l'État, Directeur général.[1]

1 « Après une expérience de plus de 20 ans dans le privé durant laquelle Jérôme a participé à la création et au développement de sociétés dans la sécurité du numérique, il a rejoint l'ANSSI en 2016. Sa mission a été de préfigurer le dispositif national d'assistance aux victimes d'actes de cybermalveillance. Lancé au printemps 2017, Jérôme en est désormais le Directeur général.»

Les membres fondateurs

Ils sont répartis en 4 collèges :

Le collège « étatiques »

- Premier ministre / SGDSN / ANSSI
- Ministère de l'Economie et des Finances
- Ministère de la Justice
- Ministère de l'Intérieur
- Secrétariat d'Etat chargé du numérique

Le collège « utilisateurs »

- Association e-Enfance
- CCI France
- Consommation, logement et cadre de vie (CLCV)
- Confédération des petites et moyennes entreprises (CPME)

Le collège « prestataires »

- Cinov-IT
- Conseil National du Logiciel Libre (CNLL)
- La fédération Entreprises du Bureau et du Numérique (Eben)
- Syntec numérique

Le collège « offreurs de solutions »

- Fédération Française de l'Assurance (FFA)

Inscription de nouveaux membres :

Le GIP étudiera les demandes de participation de nouvelles entités à l'issue de la phase expérimentale en vue de les accueillir dès janvier 2018.

Les ressources

Budget :
2017 : 1 million d'euros issu d'une subvention de l'ANSSI
2019 : estimation 2,5 millions d'euros (25% public et 75% privé)

Ressources humaines :

2017 : 8 personnes (relations partenaires, ressources techniques et administratives, etc.)
Un plan de recrutement est prévu dans les prochaines années avec un objectif cible de 25 à 30 personnes.

ANNEXE 1 : LA CHARTE D'ENGAGEMENT DES PRESTATAIRES

La présente charte est destinée aux prestataires de services informatiques, apportant une réponse aux victimes de cybermalveillances et souhaitant être référencées par le Dispositif national d'assistance aux victimes de cybermalveillances.

Le Dispositif national d'assistance aux victimes de cybermalveillances [dispositif national] met à disposition du public un service d'information en ligne permettant d'accéder, en fonction de sa position géographique sur le territoire national et des cybermalveillances rencontrées, à une liste de prestataires susceptibles d'apporter leur assistance.

Article 1 – Qualité de l'accueil

Le prestataire signataire de la présente charte s'engage à réserver le meilleur accueil aux particuliers, entreprises, collectivités locales qui s'adressent à lui pour résoudre un incident lié à une cybermalveillance. La qualité de cet accueil repose sur la courtoisie, le respect de la confidentialité, l'écoute des attentes de la victime, la clarté des réponses apportées et de l'offre commerciale, puis le respect des délais annoncés.

Article 2 – Respect des bonnes pratiques professionnelles

Le prestataire s'engage à communiquer de façon précise et en des termes simples sur la nature des services proposés de réparation, dépannage ou de réponse à incidents. Il s'agit des informations à caractère commercial, publicitaire ou informatif à destination de ses clients ou usagers, ainsi que celles qui sont mises en ligne via le dispositif national.

Ces informations sont régulièrement tenues à jour. Elles correspondent aux compétences réellement détenues par le prestataire et ses employés.

Un diagnostic complet comporte obligatoirement un dialogue clair et précis avec le client ou l'usager, une description du problème technique alors identifié et des opérations nécessaires à sa remédiation. Cet échange se termine obligatoirement par la fourniture d'un devis précisant les délais nécessaires à la remise en état.

Dans les cas où le prestataire estime qu'un premier examen technique est nécessaire pour établir le devis, il informe le client ou l'usager des frais éventuels encourus et des délais de réalisation.

Le prestataire informe dès que possible le client ou l'usager de tout changement dans la durée prévisible de l'intervention, sa nature ou son coût final. Il doit alors s'assurer de l'accord écrit du client ou de l'usager avant de poursuivre les travaux.

Dans tous les cas, le prestataire s'engage à prendre toutes mesures adaptées et à l'état de l'art, afin de préserver les traces utiles pour les services de l'Etat chargés d'investigations numériques (services enquêteurs saisis d'un dépôt de plainte ou saisis à titre d'information aux fins d'effectuer des recoupements).

Article 3 – Respect de la confidentialité

Le prestataire s'engage à respecter la confidentialité de l'ensemble des données et renseignements confiés par son client ou usager, qu'il s'agisse de la sécurité des moyens de paiement ou des données à caractère personnel et confidentiel. Il prend toutes les mesures raisonnables et nécessaires pour en assurer la protection. Aucune de ces informations ne peuvent être transmises à des tiers non autorisés.

Article 4 – Respect des lois et règlements

Les prestations sont assurées dans le respect des lois et règlements en vigueur. Conformément aux dispositions du code pénal (article 434-1 et suivants), lorsqu'il en a connaissance, le prestataire informe les autorités administratives ou judiciaires de tout crime dont il est encore possible de prévenir ou de limiter les effets ou dont les auteurs sont susceptibles de commettre de nouveaux crimes qui pourraient être empêchés.

Le prestataire s'informe des coordonnées des services de police ou de gendarmerie spécialisés dans la lutte contre la cybercriminalité ou des autres services de l'Etat impliqués dans sa prévention, situés dans son périmètre d'intervention. Sur son initiative ou à l'occasion d'événements auxquels ils participent, le prestataire est invité à prendre contact avec ces acteurs de proximité du dispositif national.

Le prestataire cesse son intervention dans tous les cas où son client ou usager l'inciterait à accomplir des actes illégaux ou contraires à la présente charte.

Article 5 – Remontée d'informations vers le dispositif national

Le prestataire informe son client ou usager des missions du dispositif national et de la possibilité qui lui est offerte de transmettre des données opérationnelles relatives aux cybermalveillances (par exemple un échantillon de virus informatique, les modes opératoires utilisés…).

Cette communication vers le dispositif national permet à l'ensemble des prestataires ainsi qu'aux services de l'Etat en charge de la prévention et de la répression des actes de cybermalveillance d'être le plus rapidement possible informés des nouvelles pratiques et techniques utilisées par les cyberdélinquants. Elle revêt une grande importance pour la collectivité nationale ; l'information reste confidentielle.

Le client ou l'usager peut s'opposer à cette transmission.

Le prestataire s'engage à réaliser régulièrement des remontées d'information.

Article 6 – Information sur les risques numériques et les moyens de prévention

Le prestataire se tient régulièrement informé des risques numériques et des moyens de prévention. Dans le cadre de son activité, le prestataire informe par tout moyen adapté ses clients ou usagers sur les risques numériques encourus. Il pourra notamment s'appuyer sur la documentation fournie par le dispositif national.

Dans la mesure de ses possibilités, le prestataire participe aux échanges avec la communauté des signataires de la présente charte, ainsi qu'avec les autres professionnels publics ou privés, sur le plan local ou si possible au plan régional voire national.

Article 7 – Evaluation et sanction

Le dispositif national accueille plusieurs moyens permettant aux clients ou usagers de faire état de leur satisfaction quant aux interventions réalisées.

Le prestataire est informé que tout manquement à la présente charte pourra entraîner la radiation temporaire ou définitive du référentiel publié par le dispositif national.

ANNEXE 2 : LES MEMBRES FONDATEURS

CCI France

CCI France est la tête de réseau nationale des 125 Chambres de Commerce et d'Industrie de France. Les CCI sont particulièrement impliquées dans la sensibilisation, l'appui et l'accompagnement des TPE-PME en matière de sécurité économique et en cybersécurité. Grâce à leurs réseaux de conseillers d'entreprise « intelligence économique » et « économie numérique », ainsi que leurs établissements de formations, elles s'attachent particulièrement à faire prendre conscience aux entreprises des avantages compétitifs qu'apporte la protection de leurs informations à valeur ajoutée.

Plus d'informations sur : www.cci.fr

CINOV- IT

CINOV-IT, syndicat des TPE/PME du numérique, défend les spécificités de ses membres auprès du législateur, des institutions politiques et économiques, des organismes publics et associatifs, des donneurs d'ordre. Il est également engagé au niveau régional, via ses référents numériques, afin de valoriser les métiers et les expertises de ses adhérents, mais aussi de les soutenir dans l'accès aux marchés et aux financements. CINOV-IT conseille ses adhérents dans leur développement et met à leur disposition des services sur-mesure et exclusifs (service juridique et social, assistance pour les contrôles sociaux ou fiscaux, assurances et financements à des tarifs privilégiés, etc.).

Plus d'informations sur : http://www.cinov-it.fr

CLCV

Consommation, logement et cadre de vie est une association nationale qui défend exclusivement les intérêts spécifiques des consommateurs et des usagers.Créée en 1952, la CLCV intervient, aux niveaux national et local, sur tout ce qui concerne la défense des consommateurs, la représentation des locataires, l'éducation populaire, la défense de l'environnement, l'action éducative complémentaire de l'enseignement public et la représentation des usagers du système de santé dans les instances hospitalières ou de santé publique (2006).

Plus d'informations sur : www.clcv.org

CNLL

Le Conseil National du Logiciel Libre est l'instance représentative, au niveau national, des associations et groupements d'entreprises du logiciel libre en France. Il a pour missions de représenter l'écosystème du logiciel libre auprès des pouvoirs publics et des organisations nationales existantes, d'aider, grâce aux échanges de bonnes pratiques, au développement des organisations régionales, de promouvoir l'écosystème, son offre de logiciels et de services, etc.

Plus d'informations sur : www.cnil.fr

CPME

Organisation patronale nationale interprofessionnelle et partenaire social, la Confédération des Petites et Moyennes Entreprises (CPME) représente, promeut et défend les intérêts des TPE et PME françaises. Forte d'un réseau de 200 fédérations professionnelles, syndicats de métiers, et 116 unions territoriales, la CPME réunit près de 150 000 entreprises employant plus de 3 millions de salariés.

Plus d'informations sur : www.cpme.fr

EBEN

Issue du regroupement de plusieurs associations professionnelles, la Fédération EBEN rassemble les entreprises de distribution de produits et services pour l'environnement de travail :

- Papeterie et fournitures de bureau
- Mobilier de bureau et collectivités
- Solutions d'impression (copieurs et imprimantes)
- Produits et solutions informatiques
- Solutions de communication électronique, télécoms et réseaux

Elle est la seule association professionnelle représentative de la branche. Lieu d'échange et de dialogue, elle représente en toute indépendance et transparence, les intérêts de ses membres pour les accompagner dans leur développement et contribuer à créer un environnement économique et social favorable.

Plus d'informations sur : www.federation-eben.com

e-Enfance

Créée en 2005, e-Enfance est une association reconnue d'utilité publique agréée par le ministère de l'Education nationale.

L'association déploie des intervenants sur tout le territoire pour sensibiliser les enfants et les adolescents aux risques et aux bonnes pratiques du numérique, et conseiller les parents et les professionnels.

Dans le cadre de sa mission e-Enfance opère également la plate-forme nationale Net Ecoute 0 800 200 000, avec le soutien de la Commission européenne et en partenariat avec les réseaux sociaux.

Plus d'informations sur : www.e-enfance.org

Fédération Française de l'Assurance – FFA

La Fédération Française de l'Assurance (FFA) rassemble les entreprises d'assurances et de réassurance opérant en France, soit 280 sociétés représentant plus de 99% du marché. La FFA est le porte-parole de référence de la profession auprès des interlocuteurs publics, privés, ou associatifs, en France comme à l'international.

Plus d'informations sur : www.ffa-assurance.fr

Syntec numérique

Syntec Numérique est le premier syndicat professionnel de l'écosystème numérique français. Ses membres sont des entreprises de services du numérique, des sociétés de conseil en technologie, des éditeurs de logiciels et des acteurs du Web, dont près de la moitié sont implantés en région. Ensemble, ils représentent 80 % du chiffre d'affaires du secteur en France et 427 000 emplois.

Plus d'informations sur : syntec-numerique.fr

ANNEXE 3 : Convention constitutive du groupement d'intérêt public pour le dispositif national d'assistance aux victimes d'actes de cybermalveillance

NB : Le document est joint au dossier de presse.

Rendez-vous sur www.cybermalveillance.gouv.fr

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

Contact presse

Jérôme Notin - 01 71 75 84 60 - dispositif@ssi.gouv.fr