

La Gendarmerie nationale
en mode gestion de crise

COVID – 19

#RépondrePrésent
pour les entreprises



GENDARMERIE

 *NOTRE ENGAGEMENT, VOTRE SÉCURITÉ* 



Mot du général d'armée Christian Rodriguez,
Directeur général de la Gendarmerie nationale

« La crise inédite que nous connaissons nous oblige, comme vous, à transformer nos modes d'action, de communication et de relations avec les usagers. Pour conseiller et accompagner en sécurité les entreprises, leurs dirigeants et leurs salariés en liaison avec le MEDEF que je remercie de son appui, nous vous proposons cette newsletter. A vocation informative, elle permet aussi de vous rappeler notre offre de service pour la protection de vos activités professionnelles, dans ce contexte particulier où les bouleversements de la crise renforcent leur sensibilité face aux menaces physiques ou cyber. Soyez-en assurés, pour votre sécurité, aujourd'hui comme hier la gendarmerie répond présent. #RépondrePrésent »

LA SÉCURITÉ ÉCONOMIQUE ET LA PROTECTION DES ENTREPRISES PENDANT LA PANDÉMIE: UNE MISSION SENSIBLE PRISE EN COMPTE PAR LA GENDARMERIE

La crise sanitaire liée au Covid-19 exacerbe les risques auxquels sont traditionnellement exposées les entreprises. Au-delà des atteintes habituelles, les entreprises sont confrontées à des difficultés diverses et pour certaines, inédites (protection des stocks, concurrence déloyale, contrefaçon etc). La gendarmerie, en tant qu'acteur à part entière de la politique publique d'intelligence économique se doit, en ce temps de crise, de conforter son rôle d'acteur des solidarités locales en faisant effort sur les acteurs économiques les plus fragiles et/ou les plus critiques sur sa zone de compétence.

À cet effet, la gendarmerie est dotée d'un réseau de 200 référents « sécurité économique et protection des entreprises (SECOPE) » sur l'ensemble du territoire, dans chaque région, dans chaque département en métropole et outre-mer. Ces référents sont à la disposition des entreprises pour les accompagner en leur proposant des actions de sensibilisation et des diagnostics de sécurité économique. Ces référents sont joignables en leur adressant vos questions à l'adresse mail correspondant à votre région d'appartenance (cf. dépliant joint).



QUELS RISQUES ET MENACES PEUVENT VOUS CONCERNER?

On distingue traditionnellement 8 familles d'atteintes à la sécurité économique. Celles-ci sont présentées dans le kit pédagogique de sensibilisation réalisé conjointement par la gendarmerie nationale et l'INHESJ : « [le jeu des 8 familles d'atteintes à la sécurité économique](#) ».

Dans le contexte de la crise du COVID-19 et dans la perspective de la sortie du confinement, certains risques sont accrus et parfois relativement inédits pour les entrepreneurs. En particulier, les cyber-menaces se font plus prégnantes.

La généralisation du **télétravail** affaiblit les dispositifs de sécurité en exposant les bases de données aux risques d'intrusion et de captation d'informations sensibles (personnelles, bancaires etc.) et de rançonnage. De nombreuses attaques par phishing débouchant sur des vols d'identifiants, de mots de passe, de numéros de carte bancaire ont été constatées depuis le début de l'épidémie.

En cas d'atteinte avérée, il est possible de signaler les faits sur la plateforme <https://www.cybermalveillance.gouv.fr/>

Le recours accru aux **visioconférences** en cette période de crise sanitaire engendre de nouvelles vulnérabilités. En effet, beaucoup de sujets sensibles pour la vie économique et de l'entreprise transitent sur des canaux non sécurisés. Ainsi, sur certaines plateformes, des failles permettent d'enregistrer les conversations, capter des données de connexions, connaître l'emploi du temps et la localisation des utilisateurs. Pour limiter les risques, il est recommandé d'utiliser des plateformes agréées par l'ANSSI (comme TIXEO) en allant sur le site ci-dessous : <https://www.ssi.gouv.fr/uploads/liste-produits-et-services-qualifies.pdf>

L'utilisation du **matériel informatique personnel** ou **familial** à des fins professionnelles est parfois inévitable mais nécessite des mesures de sécurité spécifiques : il convient ainsi d'éviter de faire suivre ses messages électroniques professionnels sur une messagerie personnelle (type gmail, yahoo, ...), ou d'héberger des données de l'entreprise sur les équipements personnels. Nous vous recommandons de visiter la fiche pratique à ce sujet.

VOUS ÊTES VICTIMES D'UNE CYBER-ATTEINTE? LE RÉSEAU CYBERGEND EST LÀ POUR VOUS AIDER !

Le réseau CyberGEND est composé de plus de 5000 personnels et se développe selon deux axes : la conduite d'enquêtes sur les réseaux numériques et l'appui aux unités en matière de criminalistique.

À sa tête, le Pôle national de lutte contre les cybermenaces de la direction générale de la gendarmerie nationale est chargé de piloter l'ensemble du dispositif de la gendarmerie en matière de lutte contre la cybercriminalité et de prévention des cybermenaces.

Le centre de lutte contre les criminalités numériques (C3N) au sein du service central de renseignement criminel (SCRC) est la tête de la chaîne d'investigation et réalise les enquêtes les plus complexes. Il s'appuie dans les sections de recherches sur neuf antennes régionales. Le C3N contribue à la détection des phénomènes émergents, tandis que l'observatoire central de la sécurité des systèmes de transports intelligents (OCSTI) et le plateau d'investigation sur les objets connectés (PIOC) complètent cette vision dans le champ des véhicules et des objets connectés.

D'autre part, les expertises complexes d'exploitation et de recueil de la preuve numérique sont menées par le département informatique-électronique (INL) de l'institut de recherche criminelle de la gendarmerie nationale (IRCGN). La criminalistique numérique du quotidien est réalisée dans les sections opérationnelles de lutte contre les cybermenaces, armées par des NTECH au niveau de chaque département, qui sont relayés pour l'analyse des téléphones mobiles par les enquêteurs numériques de proximité dans les compagnies et brigades de gendarmerie départementale

Devant le risque d'une sur-crise cyber, la gendarmerie renforce sa posture opérationnelle consistant à PRÉVENIR et SE PROTÉGER, RENSEIGNER et INFORMER, COMMUNIQUER, SE PROJETER et ENQUÊTER, le tout dans une logique de partenariat avec le monde associatif et professionnel et en coordination avec l'ensemble des acteurs ministériels et interministériels, au niveau central et territorial.

Depuis le début du mois, des personnels confinés ou en télétravail et des réservistes citoyens et opérationnels participent à la mission « prévention des cybermenaces » en prenant contact téléphonique avec les élus locaux et les entreprises pour diffuser des recommandations indispensables à leur sécurité numérique.



N.B. : lors de ces contacts, aucune information sensible (mots de passe, code personnel, etc.) ni aucune opération n'est demandée par la gendarmerie. Si vous avez un doute sur l'identité de votre interlocuteur, appelez la gendarmerie pour vous en assurer.

- **consulter le numéro de la gendarmerie (unité locale ou groupement de gendarmerie départementale) sur <https://lannuaire.service-public.fr> .**

Actuellement, on observe une recrudescence de faits tels que les escroqueries, hameçonnages* et diffusion de logiciels malveillants facilités par la thématique du Coronavirus ou par les changements d'organisation des entreprises et administrations liés notamment au télétravail. Les escroqueries visent aussi bien les entreprises que les particuliers, ont trait à la vente de produits de protection, des cagnottes, mais aussi aux stratégies classiques de l'arnaque dit du faux président ou du changement de coordonnées bancaires. A noter que les logiciels malveillants de type rançongiciel ciblent non seulement des entreprises, mais aussi parfois les organisations les plus critiques dans le cadre de cette crise, à savoir des établissements de santé ainsi que des collectivités locales.

***phishing ou hameçonnage ou filoutage**

(Cf Glossaire de l'ANSSI <https://www.ssi.gouv.fr/entreprise/glossaire/>) :
vol d'identités ou d'informations confidentielles
(codes d'accès, coordonnées bancaires) par subterfuge.

Retrouvez nos conseils à travers les infographies en pièces jointes.
N'hésitez pas à les diffuser largement!

Dans la perspective du déconfinement,
découvrez les 10 conseils de notre partenaire cybermalveillance
[https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/
cybersecurite-preparer-la-reprise-dactivite-au-deconfinement](https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/cybersecurite-preparer-la-reprise-dactivite-au-deconfinement)



Enfin, on note une augmentation des plaintes pour injures et outrages, et un phénomène de propagation de fausses informations soit pour mettre en cause l'action d'un acteur économique ou politique, soit risquant de perturber l'ordre public (cas de rumeurs autour du développement de la téléphonie 5G et son impact allégué sur la crise sanitaire et l'environnement).

Pour signaler :

- Des piratages dans une entreprise : cyber@gendarmerie.interieur.gouv.fr
- Des contenus illégaux sur Internet : www.internet-signalement.gouv.fr
- Des courriels ou sites d'escroqueries : www.internet-signalement.gouv.fr ou 08 05 805 817
- Des spams : www.signal-spam.fr
- Des sites de phishing : www.phishing-initiative.fr
- Dispositif national d'assistance aux victimes de cybermalveillance : www.cybermalveillance.gouv.fr

Webinar Cybersécurité:

À l'initiative de Maxence Demerlé, directrice du numérique du MEDEF national, et en partenariat avec Wavestone et la mission numérique de la Gendarmerie nationale, un webinar cybersécurité a réuni, jeudi 9 avril 2020, plus de 160 participants.

Jules Haddad, consultant senior expert cyber de Wavestone, et le colonel Eric Fressynet, chef du pôle national de lutte contre les cybermenaces à la Direction générale de la Gendarmerie Nationale ont abordé notamment les questions de sécurisation des accès distants et la protection des collaborateurs contre les phishings*.

En effet, la crise sanitaire COVID-19 a conduit les entreprises à revoir leur organisation et à mettre en place, parfois dans l'urgence, le travail à distance en omettant, dans certains cas, les enjeux de sécurité.

Un webinar cybersécurité sera organisé prochainement par le MEDEF en Pays de la Loire avec le concours, notamment, de la Gendarmerie nationale.



VOUS SOUHAITEZ ÊTRE MIS EN CONTACT AVEC UN GENDARME SANS AVOIR À VOUS DÉPLACER ? LA BRIGADE NUMÉRIQUE CONTACTERLAGENDARMERIE.FR EST LÀ POUR VOUS AIDER !

Depuis février 2018, la brigade numérique répond 24 heures sur 24, 7 jours sur 7, à toutes les questions du quotidien. Elle a déjà répondu à plus de 200 000 demandes, avec un taux de satisfaction de 9/10.

C'est une démarche innovante, dont l'objectif est de proposer aux usagers un contact simplifié et rénové avec la gendarmerie nationale, en tout lieu et en tout temps, pour répondre à leurs interrogations. En intégrant les nouvelles technologies, la gendarmerie adapte ses modes d'action pour repenser sa façon d'interagir avec la population. Les gendarmes de la brigade numérique complètent et démultiplient ainsi les capacités d'accueil des unités territoriales.

Les urgences restent de la compétence des plateformes des services idoines (17, 18, 15 et 112).

Le citoyen peut ainsi, depuis l'appareil de son choix, contacter en permanence la gendarmerie. Plusieurs canaux lui sont proposés tels les réseaux sociaux Twitter, Facebook ou le chat en ligne sur le site internet de la gendarmerie. Un opérateur de la gendarmerie évalue la demande et propose soit une assistance en ligne, soit un rendez-vous avec un gendarme dans le lieu de son choix. En complément, ces mêmes usagers peuvent accéder à un centre d'aide (type FAQ) qui leur permet de rechercher, en autonomie, des réponses à des questions d'ordre général.

Depuis peu, la brigade numérique est aussi accessible depuis le site www.cybermalveillance.gouv.fr, qui accueille, conseille et oriente les victimes de cyber-malveillances. Les gendarmes de la brigade numérique ont été spécialement formés pour prendre en charge ces victimes.



SCOOP !

Un canal dédié aux entreprises vient tout juste d'être ouvert : les gendarmes qui répondent vous orienteront vers le bon téléservice ou interlocuteur pour toutes les questions liées à la protection économique et à la sécurité/sûreté.
<https://www.gendarmerie.interieur.gouv.fr/Brigade-numerique?service=entreprise>

Depuis le début de la crise COVID-19, la Brigade numérique de la gendarmerie nationale est passée de 250 à 2 000 sollicitations quotidiennes.

www.contacterlagendarmerie.fr



EN CAS D'URGENCE, FAITES LE 17.

Au quotidien, votre brigade de gendarmerie la plus proche est à votre disposition

Pour les questions portant sur le coronavirus et les mesures gouvernementales dans ce domaine, il est préférable d'utiliser les outils dédiés :

<https://www.gouvernement.fr/info-coronavirus>

ou par téléphone :
0800 130 000

Pour les règles de restriction de déplacement, consulter : <https://www.gouvernement.fr/sites/default/files/contenu/piece-jointe/2020/03/faq-restrictions.pdf>

Pour en savoir plus sur la brigade numérique :

<https://www.gendarmerie.interieur.gouv.fr/Zooms/Ayez-le-reflexe-brigade-numerique>

VOUS SOUHAITEZ PROTÉGER L'UN DE VOS SITES DE PRODUCTION ? L'OPÉRATION «TRANQUILLITÉ ENTREPRISES» EST LÀ POUR VOUS AIDER !

En situation de crise sanitaire d'intensité inédite, la gendarmerie renouvelle son offre de service et de protection au profit des entreprises. Pour répondre présent, elle adapte ses modes d'actions à la nouvelle cartographie des risques : fermetures de sites, recours massif au télétravail, sécurisation accrue de certaines plateformes logistiques, prise en compte de menaces touchant certains secteurs d'activité en lien direct avec la gestion de crise, *etc.*

Le dispositif tranquillité entreprise offert par la gendarmerie nationale permet ainsi, à tout chef d'entreprise qui le souhaite, de faire connaître ses préoccupations et ses besoins spécifiques, notamment par l'intermédiaire de la brigade locale ou du référent SECOPE de son ressort (cf. encadré relatif à la mission de sécurité économique).

Le site concerné par la demande est ensuite référencé dans une cartographie interactive. En fonction de l'acuité de la menace, des surveillances physiques, par l'intermédiaire de patrouilles dédiées, sont déterminées et orientées sur les secteurs concernés. Chaque passage de la gendarmerie est référencé dans la cartographie puis un code couleur permet d'en connaître la fréquence. Si une intrusion ou un acte malveillant est constaté, les gendarmes disposent de tous les moyens nécessaires pour alerter immédiatement les chefs d'entreprises et les entrepreneurs.

La connaissance mutuelle gendarmerie/chef d'entreprise qu'induit l'inscription à ce dispositif permet concomitamment de faciliter d'éventuelles investigations ultérieures.

Enfin, cette relation étroite permet aussi, dès l'inscription et si besoin est, la délivrance immédiate de conseils de sûreté, de sécurité économique voire numérique.

L'opération « Tranquillité entreprises» dans le département du Haut-Rhin, une initiative saluée

Le groupement de gendarmerie départementale du Haut – Rhin (GGD 68) a su #RépondrePrésent aux côtés des entreprises dès le début de la crise sanitaire COVID – 19.

Ce dernier a fait preuve d'anticipation dans un contexte de crise extrême. Le GGD 68 a mobilisé l'ensemble de ses ressources, et a déployé, entre autres, des actions de prévention auprès de l'écosystème économique par l'intermédiaire de ses cellules de prévention technique de la malveillance et renseignement. Plus de 2200 commerces et 791 entreprises ont été contactés depuis le 16 mars 2020.

Par ailleurs, des patrouilles sont organisées au quotidien au profit des entreprises. Elles permettent de vérifier l'intégrité des sites et de prévenir d'éventuels cambriolages.

Le monde économique salue l'engagement du GGD 68. Ainsi, des élans de solidarité ont vu le jour. Des entreprises ont offert des masques de protection et du gel hydroalcoolique au GGD68.

VOUS ÊTES CONCERNÉS PAR DES FLUX LOGISTIQUES ? LE CENTRE NATIONAL DE SÉCURITÉ DES MOBILITÉS EST LÀ POUR VOUS AIDER !

Les premiers convois de masques de Santé Publique France ont fait l'objet d'un suivi rigoureux et en temps réel de la part des unités territoriales de la gendarmerie nationale et du centre national de sécurité des mobilités (CNSM) de la Direction générale de la gendarmerie nationale. Les principaux lieux de stockage de ces matériels, désormais devenus sensibles, ont fait l'objet d'un diagnostic de sûreté de la part d'un référent sûreté de la gendarmerie nationale.

Depuis le tout début de cette crise, l'engagement de la gendarmerie nationale en matière de sécurisation des flux logistiques ne faiblit pas.

Ainsi, le CNSM, en lien direct et permanent avec les plateformes logistiques et les transporteurs, reste en mesure d'obtenir la localisation précise d'un convoi et de solliciter, le cas échéant, un centre opérationnel départemental (CORG) pour toute levée de doute ou intervention.

Le déploiement des matériels de dépistage et des traitements médicamenteux feront aussi, le moment venu, l'objet des mêmes égards.

**SAUVEZ DES VIES
RESTEZ
CHEZ VOUS**

**LES NUMÉROS
À CONNAÎTRE
COVID19**

0 800 130 000
NUMÉRO VERT
POUR TOUTE SITUATION
ET DEMANDE
D'INFORMATION
GÉNÉRALE

BRIGADE NUMÉRIQUE
POUR TOUTE
QUESTION
NON
URGENTE
RELATIVE À LA
SÉCURITÉ



LES NUMÉROS D'URGENCE HABITUELS

**15
SAMU**
LE SERVICE D'AIDE MÉDICALE URGENTE
Pour obtenir l'assistance d'un médecin
qualifié lors d'une situation de détresse
médicale, appelez sans délai le numéro
régional de permanence de nuit.

**17
POLICE
SECOURS**
Pour signaler une infraction qui nécessite
l'intervention immédiate de la police
ou de la gendarmerie.

**18
SAPEURS-
POMPIERS**
Pour signaler une situation qui nécessite
l'intervention immédiate de la police
ou de la gendarmerie.

AU QUOTIDIEN, SUIVEZ LA GENDARMERIE SUR



GENDinfo.fr