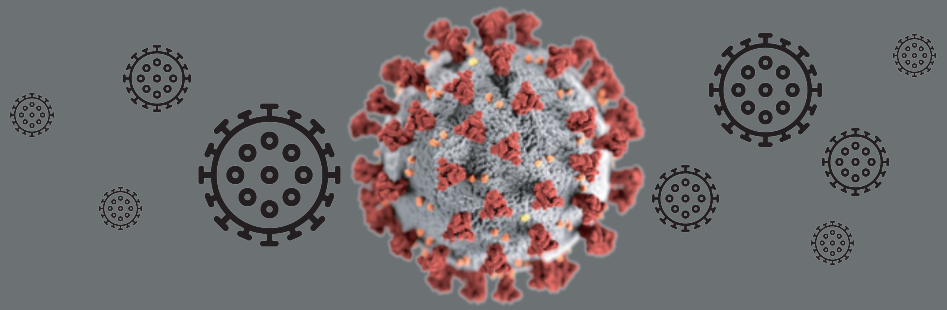
Bulletin d'alerte

STOP AUX CYBER-MENACES

GROUPEMENT DE GENDARMERIE DE LA GIRONDE

EN PERIODE DE COVID-19

Les mesures de confinement obligent certains collaborateurs à avoir recours au télétravail. Mal équipés, mal préparés, il convient pourtant dans l'urgence de rester très vigilants et d'adopter les bonnes pratiques pour réduire son exposition face aux cybermenaces qui prolifèrent ces derniers jours.



COMMENT S'ORGANISER POUR MINIMISER L'EXPOSITION AUX CYBER-RISQUES ?

- **Désigner un responsable** (informatique de préférence) qui aura pour mission de superviser le déploiement des postes de télétravail et d'accompagner techniquement à la résolution des problèmes de sécurité informatique.

- Être particulièrement vigilant et **signaler toute activité ou demande inhabituelle**, par rapport au fonctionnement de votre entreprise.

- S'appuyer sur **la « charte informatique »** (droit et devoir du collaborateur) pour rappeler les règles d'utilisation du réseau notamment en télétravail.

- **Communiquer, former et sensibiliser les collaborateurs** au changement à venir, aux risques encourus ainsi qu'aux nouveaux outils mis en place.

- Suivre les **conseils** de l'agence chargée de la sécurité des systèmes d'information **(« recommandations ANSSI »)** sur l'utilisation d'équipements personnels pour un usage professionnel (https://www.ssi.gouv.fr).

QUELQUES EXEMPLES DE CYBER-MENACES COVID-19 :

- **Des sollicitations providentielles** (sms, chat, email, …) ou appels téléphoniques inconnus ou inattendus (fourniture de masque FFP2, Chloroquine, dons aux hôpitaux, nouvelles démarches « facilitantes » administratives, etc.).

- **L'hameçonnage** (ou phishing) pour vous dérober des informations personnelles, professionnelles ou bancaires en vous attirant sur de faux sites officiels (promesse d'une (trop) bonne affaire, d'un remboursement, d'un colis en attente, d'un problème de sécurité, etc.).

- **Des escroqueries à la fausse commande** ou aux modifications de coordonnées de virement bancaire - FOVI (usurpation de l'identité d'un employé, d'un fournisseur ou d'un dirigeant sous le sceau du secret, etc.).

- **Des demandes accompagnées de pièces jointes** qui peuvent furtivement compromettre votre ordinateur voire chiffrer ces données afin de vous réclamer une rançon pour en retrouver l'accès (rançongiciels).

Gendarmerie nationale
200 Rue Judaïque, 33000 Bordeaux

10 BONNES PRATIQUES A ADOPTER POUR SE PRESERVER DES CYBER-MENACES COVID-19

1- Réduire au strict minimum le recours à des ordinateurs personnels et privilégier l'utilisation d'un **VPN** pour se connecter au TSE (resté dans l'entreprise).

2- Activer toutes les **mises à jour** de votre système d'exploitation, de vos logiciels et antivirus (endpoint) ainsi que les **configurations et fonctionnalités de sécurité** du cloud. Penser au firewall.

3- Utiliser l'ordinateur depuis une **session dédiée** (cf. invitée et non administrateur).

4- **Chiffrer** l'ensemble des données sensibles de l'entreprise que vous utilisez.

5- **Centraliser** les données en un seul et même endroit pour en faciliter l'identification et la destruction à l'issue du confinement.

6- Attribuer un **mot de passe unique** pour chaque application (minimum 12 caractères alphanumériques, caractères spéciaux, inintelligible et périodique). A défaut utiliser un « gestionnaire de mot de passe ».

7- Recourir dès que cela est possible à la **double authentification** surtout si vous utilisez des applications personnelles (boîte email, réseaux sociaux, etc.).

8- Veiller à utiliser un **réseau WiFi** séparé pour le travail afin d'isoler les données et penser à se tenir à l'écart du WiFi public utilisé par de nombreuses personnes.

9- Effectuez des **sauvegardes régulières** de toutes vos données, sur un support externe qui n'est en aucun cas relié à internet.

10- **Isoler** le poster infecté, **couper** l'accès au réseau et à internet et **alerter** la gendarmerie en cas d'attaque malveillante via internet.

REFERENTS GENDARMERIE

Le dispositif qui regroupe les 2000 enquêteurs cyber de la gendarmerie (260 enquêteurs NTECH et 1700 correspondants-NTECH) est désormais fédéré sous l'appellation « CYBERGEND ».

Ce réseau décentralisé assure un maillage sur tout le territoire national, aussi bien en métropole qu'outre-mer. Il constitue un ensemble de points de contact et de capacité d'action de proximité, doté de véritables capacités d'investigation. Il est piloté par le centre de lutte contre la cybercriminalité numérique (C3N) de Pontoise.

CONTACTS

Pour aller plus loin ou obtenir de l'information :

www.gendarmerie.interieur.gouv.fr
www.ssi.gouv.fr

Pour signaler :

- des piratages dans une entreprise : cyber@gendarmerie.interieur.gouv.fr
- des contenus illégaux sur internet : https://www.internet-signalement.gouv.fr
- des courriels ou sites d'escroquerie : https://www.internet-signalement.gouv.fr ou 0811 02 02 17
- des spams : https://www.signal-spam.fr
- des sites de phishing : https://phishing-initiative.fr
- des actes malveillants : https://www.cybermalveillance.gouv.fr
- pour les collectivités territoriales: https://www.ssi.gouv.fr/administration/guide/securite-numerique-des-collectivites-territoriales-lessentiel-de-la-reglementation/

EN CAS D'URGENCE, COMPOSEZ LE 17

Votre point de contact local ?
Selon la gravité de votre incident, ce point de contact local sera en mesure de faire intervenir des enquêteurs spécialisés en cybercriminalité.

En cas d'intrusion sur votre système, de campagne de dénigrement (refus de solidarité ou de don), atteinte à l'image de l'entreprise, ou toute autre tentative, alertez et déposez plainte auprès des autorités compétentes. **Conservez toutes les preuves nécessaires** à la bonne poursuite des investigations (en-tête d'émail, logs de journalisation, captures écran, ordinateurs, etc.).