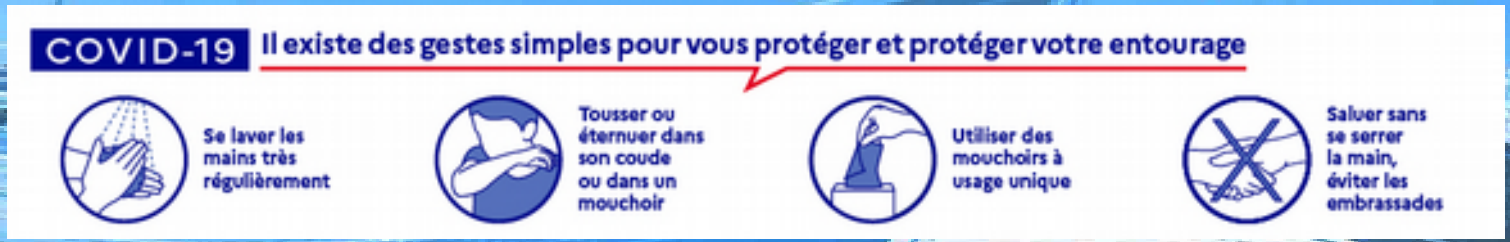
Web-conférence du 16 avril 2020

Sécurité Économique et Protection des entreprises

" Confiné pour la protection des personnes – Sécurité pour la protection de votre entreprise "



Déroulé de la web-conférence :

- Présentation de la cellule Sécurité Économique et Protection des Entreprises (SECOPE) de la Gendarmerie,
- un panel (non exhaustif) des risques d’atteintes, principalement en cette période,
- les solutions de soutien avec les services de l’État,
- échanger sur des cas concrets impactant votre entreprise.

Qu’est ce que la sécurité économique ?

- La **Sécurité Économique** vise notamment à :

- identifier et analyser les risques et menaces pour vos entreprises,

- à protéger vos actifs matériels et immatériels,

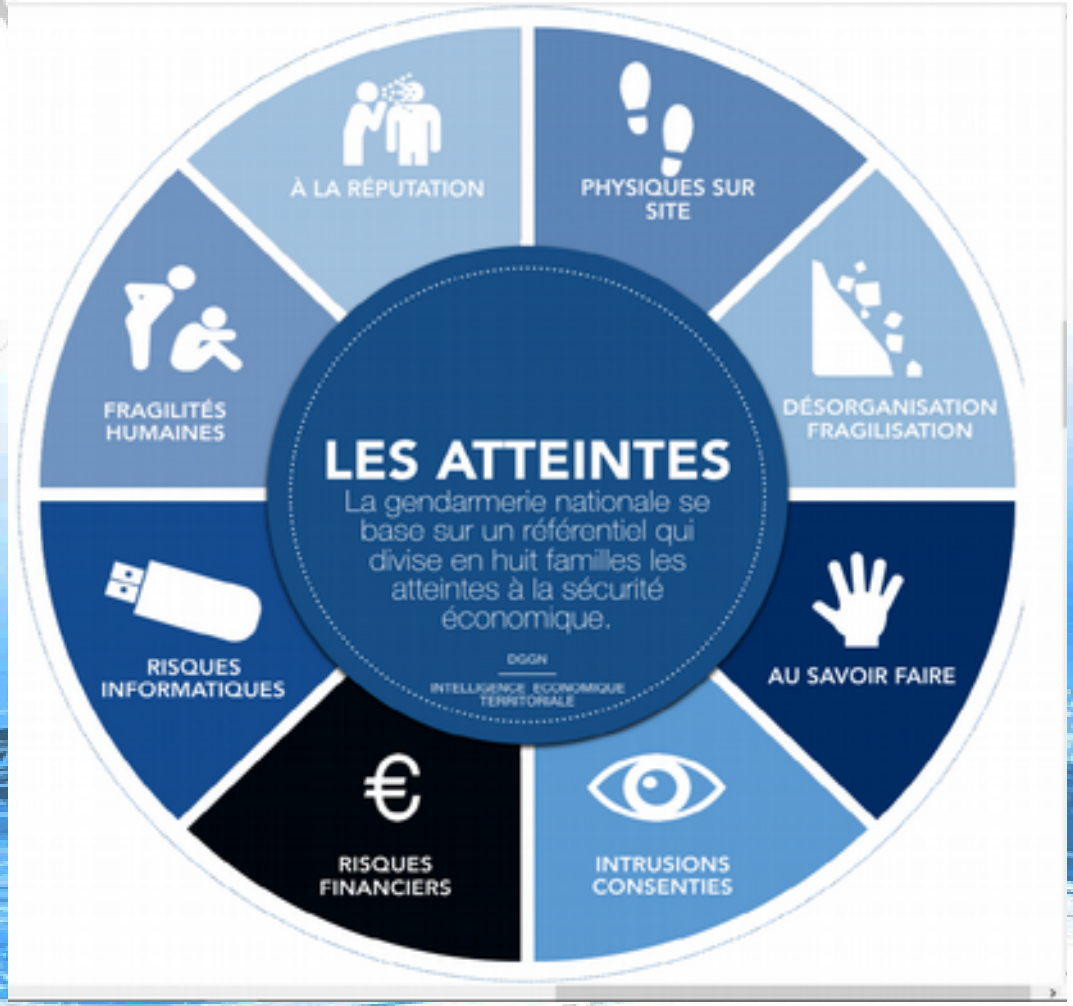
- à promouvoir au sein de vos sociétés une culture de sécurité du patrimoine et des savoir-faire.

Qu’est ce que la sécurité économique ?

- Au niveau Régional, le **Préfet de Région** est chargé du pilotage et de la mise en œuvre de la politique de sécurité économique nationale.

- Au niveau Départemental, l’animation en matière de sécurité économique est confiée au **Pôle Départemental de Sécurité Économique.**

Les 08 types d'atteintes...



Les risques financiers

- **Liés à des sources d'approvisionnement ou / et à une clientèle insuffisamment diversifiés**

- **Liés aux escroqueries financières**

Cybermenaces et Covid-19

Recommandations pour les entreprises et les salariés en télétravail

Faux sites liés au COVID19

• Prenez garde aux faux sites Internet relatifs aux ventes en ligne de masques, gel hydroalcoolique.

Fausses commandes et faux ordre de virement

• Vérifiez la signature de documents ou les tentatives de récupération des mots de passe de vos données d'entreprise.

• Vérifiez les demandes d'un virement exceptionnel ou un changement de RIB d'une facture ou d'un salaire faite par un dirigeant, d'un fournisseur, d'un prestataire, voire d'un collaborateur, pour demander un virement exceptionnel ou un changement de RIB d'une facture ou d'un salaire. Son identité a pu être usurpée suite au piratage d'un compte de messagerie, par message et même téléphone.

L'hameçonnage / Phishing

• méfiez-vous des mails, SMS, chat (réseaux sociaux, messageries instantanées type Whatsapp) et appels téléphoniques non identifiés. Cette technique soustrait des informations personnelles, professionnelles ou bancaires en vous orientant sur de faux sites.

Portails d'information

www.contacterlagendarmerie.fr
www.cybermalveillance.gouv.fr
www.ssi.gouv.fr
www.cnil.fr

Dons frauduleux

• Évitez de cliquer sur les liens des appels aux dons et rendez vous directement sur le site officiel.

Rançongiciel / Ransomware

Cette attaque consiste à empêcher l'accès aux données de l'entreprise et à réclamer une rançon pour les libérer. Elle s'accompagne d'un vol de données et d'une destruction préalable des sauvegardes.

Elles sont possibles par une intrusion sur le réseau de l'entreprise, un accès à distance, par la compromission de l'équipement d'un collaborateur ou un défaut de mise à jour du matériel informatique (pièces jointes ou liens présents dans les courriers électroniques).

Pensez à :

Bilan sécurité et sauvegarde des données

• Profitez du ralentissement de l'activité, faites un bilan complet avec votre responsable informatique ou une entreprise cybersécurité.

• Procédez à des sauvegardes régulières et hors ligne des données. Déconnectez votre support de sauvegarde à l'issue.

Attestation de travail

• Facilitez la mobilité de vos salariés en éditant des attestations de déplacement dérogatoire avec le timbre officiel de l'entreprise.

Déplacements / Télétravail

• Vos collaborateurs et salariés doivent renforcer leur vigilance lors de leurs trajets domicile/lieu de travail, en particulier leurs équipements mobiles.

• Mettez à disposition des solutions de sécurité (VPN, antivirus) et assurez-vous qu'ils connaissent les règles de mise en œuvre et de mise à jour.

• Proscrivez à vos collaborateurs l'emploi d'espaces de partage personnel des documents.

• Rappelez les consignes et contacts en cas d'incident.

Charte informatique

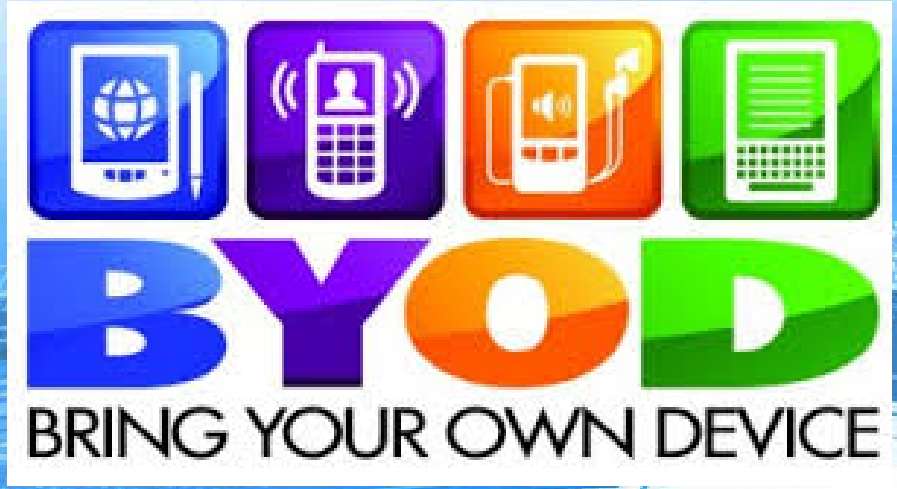
• Faites un rappel sur les droits et devoirs de chacun sur les règles d'utilisation du réseau informatique de l'entreprise.

• Si nécessaire, mettez à jour les consignes et les nouveaux outils du travail à distance.

BYOD

- **Principe**

L’acronyme « BYOD » est l’abréviation de l’expression anglaise «Bring Your Own Device» «Apportez Votre Propre Matériel». Elle désigne l’emploi d’équipements informatiques personnels dans une sphère professionnelle avec les dangers que cela comporte !



BYOD

- **Précaution à prendre : Séparer les usages !**

  - Ne pas faire suivre ses messages électroniques professionnels sur des services de messagerie personnels

  - Ne pas héberger de données professionnelles sur des équipements personnels

  - Éviter de connecter des supports amovibles personnels aux ordinateurs de l’entreprise

VISIO CONFERENCE

Depuis la mise en place du confinement, l’utilisation de logiciels de visioconférences a été démultipliée.

Normalement sécurisés, des failles sont toutefois connues et ont pu être exploitées par des hackers ou des personnes mal-intentionnées (ex. : WEBEX).

VISIO CONFERENCE

Ainsi, le logiciel ZOOM a fait récemment l'objet du « ZOOM-bombing » dont le principe est de pénétrer des conférences professionnelles pour y perpétrer du désordre. La société a depuis corrigé son application.
En outre, des noms d'applications comme WEBEX, SLACK ou SKYPE ont été récemment usurpés.
Téléchargée sur une plateforme non officielle, la fausse application ou le logiciel modifié peut entraîner ensuite l'installation de programmes non autorisés à des fins frauduleuses.

Outil diagnostique

HackerOne est une plateforme de coordination pour la recherche de vulnérabilités informatiques.
Elle met notamment en relation des entreprises avec des testeurs de pénétration et des chercheurs en cybersécurité.
De la découverte de failles peut découler le versement d’une récompense.

https://www.hackerone.com/hack-for-good

Outil diagnostique

Dans le cadre de la crise, la plateforme propose à tous Les « Chapeaux Blancs » de participer aux différentes recherches dans un but humanitaire. En effet, elle leur permet de reverser une partie ou l'intégralité des primes gagnées à des œuvres caritatives. Les premiers dons de ce type seront versés au Fond de solidarité COVID-19 de l'Organisation Mondiale de la Santé

CONSEILS ENTREPRISES ET SALARIÉS EN TÉLÉTRAVAIL

BILAN SÉCURITÉ COMPLET

SAUVEGARDE DES DONNÉES RÉGULIÈRES HORS LIGNE

ATTESTATIONS DE DÉPLACEMENT

DÉPLACEMENTS / TÉLÉTRAVAIL

RENFORCER LEUR VIGILANCE.
SOLUTIONS DE SÉCURITÉ *(VPN, ANTIVIRUS)*

CHARTE INFORMATIQUE

RAPPEL SUR:

- *UTILISATION DU* **RÉSEAU INFORMATIQUE**
- **PROTECTION DES DONNÉES** *PERSONNELLES ET CONFIDENTIELLES*
- *CONSIGNES QUANT AUX CIRCONSTANCES ET* **NOUVEAUX OUTILS DU TÉLÉTRAVAIL** *(SI NÉCESSAIRE)*

Les dispositifs d’aide et leur fonctionnement

https://www.occitanie.cci.fr/les-dispositifs-daide-et-leur-fonctionnement

- reporter le paiement de vos impôts et cotisations sociales,
- étaler vos créances bancaires,
- obtenir ou maintenir un crédit bancaire, suspendre le paiement de vos factures…
- résoudre des conflits avec vos clients ou fournisseurs,