CONSEILS

Sur la sécurité numérique à la maison pendant la crise du coronavirus

LES CYBERCRIMINELS

PROFITENT DE LA CRISE ÉPIDÉMIQUE, NE VOUS FAITES PAS AVOIR !

- Escroqueries et hameçonnages liés aux masques, gel hydroalcoolique, médicaments.
- Logiciels malveillants et autres virus.
- Application Coronavirus détournée.

En cas de fraude à la carte bancaire, signalez-le à votre banque et sur la plateforme PERCEVAL sur Service-Public.fr

LE TÉLÉTRAVAIL

RENFORCEZ VOTRE VIGILANCE

- Vérifiez par un contre-appel l'identité d'un interlocuteur.
- Utilisez le VPN fourni par votre employeur.
- Assurez-vous de connaître les personnes à contacter et rendez compte de tout incident.
- Séparez vos données personnelles de votre activité professionnelle.

Pour plus de conseils et vous faire assister en cas d'incident, rendez-vous sur le site de notre partenaire : CYBERMALVEILLANCE.GOUV.FR

LES FAUSSES INFORMATIONS

LES QUESTIONS À SE POSER POUR NE PAS TOMBER DANS LE PANNEAU

- Qui est l'auteur ? Quelle est son intention ?
- Quelle est la nature du site ? Qui est son éditeur ?
- Quelle est la source de l'information ?
- A-t-elle été publiée sur d'autres sources de confiance ?
- De quand date l'information ?

Informez-vous auprès des sources officielles : https://www.gouvernement.fr/info-coronavirus

informations CORONAVIRUS

DES ENFANTS PLUS CONNECTÉS

QUELQUES CONSEILS POUR LES PROTÉGER

- Parlez avec vos enfants des risques sur Internet.
- Utilisez les plateformes scolaires officielles.
- Vérifiez les configurations de sécurité et les mises à jour.
- Utilisez le Contrôle Parental.

Pour toute question de sécurité numérique, vous pouvez contacter 24h/24 les gendarmes de la Brigade numérique à l'adresse : www.contacterlagendarmerie.fr

BRIGADE numérique Gendarmerie

GENDARMERIE NATIONALE

La sécurité numérique à la maison pendant la crise du Coronavirus

LES CYBERCRIMINELS

LES PIÈGES

- Escroqueries et hameçonnages liés aux produits sanitaires (masques, gel hydroalcoolique, médicaments)
- Logiciels malveillants et autres virus informatiques
- Application Coronavirus détournées
- Ne cliquez pas sur des liens de sources inconnues
- Méfiez-vous des publicités alléchantes
- Vérifiez à deux fois l'origine des appels aux dons
- Ne donnez pas vos coordonnées bancaires sur des sites inconnus
- Vérifiez les mises à jour de vos systèmes d'exploitation et antivirus
- Sauvegardez régulièrement vos données

En cas de fraude à la carte bancaire, signalez-le à votre banque et sur la plateforme PERCEVAL sur

Service-Public.fr

ATTENTION FAUSSES INFORMATIONS

Beaucoup d'informations circulent, douter permet d'éviter de propager soi-même de fausses informations :

- Qui est l'auteur ? Quelle est son intention ?
- Quelle est la nature du site ? Qui est son éditeur ?
- Quelle est la source de l'information ? A-t-elle été publiée sur d'autres sources de confiance ?
- De quand date l'information ? Est-ce que l'information est cohérente (lieux, dates, personnes) ?
- Que disent les commentaires sur le site et sur les réseaux sociaux qui reprennent cette information ?

INFORMEZ-VOUS AUPRÈS DES SOURCES OFFICIELLES :
https://www.gouvernement.fr/info-coronavirus

information
CORONAVIRUS COVID-19

TÉLÉTRAVAIL

- Respectez les règles de sécurité numérique et les procédures auxquelles vous êtes habitué ; restez attentif et n'hésitez pas à vérifier par un contre-appel l'identité d'un interlocuteur
- Séparez autant que possible vos activités et données personnelles ou professionnelles ; interdisez l'accès de vos équipements professionnels à vos proches
- Utilisez le VPN (réseau privé sécurisé) fourni par votre employeur
- Assurez-vous de connaître les personnes à contacter et rendez-compte de tout incident

POUR PLUS DE CONSEILS ET VOUS FAIRE ASSISTER EN CAS D'INCIDENT, RENDEZ-VOUS SUR LE SITE DE NOTRE PARTENAIRE :

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

DES ENFANTS + CONNECTÉS

- Parlez avec vos enfants **DES RISQUES SUR INTERNET** et soyez toujours à leur écoute.
- Pour l'école à la maison, n'utilisez que les plateformes officielles et évitez les réseaux sociaux réservés aux plus grands.
- Pour les plus jeunes, rappelez-leur de ne jamais discuter avec des inconnus et utilisez des outils de contrôle parental.
- Comme pour les logiciels et matériels des plus grands, changez les mots de passe par défaut, vérifiez les configurations de sécurité et les mises à jour.

BRIGADE numérique

Pour toute question, 24h/24, 7j/7 :

www.contacterlagendarmerie.fr

En cas d'urgence, contactez le 17

Cybermenaces et Covid-19

EN CAS DE DOUTE, LA GENDARMERIE EST À VOS CÔTÉS

Votre contact local

BRIGADE numérique

Pour toute question, 24h/24, 7j/7 :
www.contacterlagendarmerie.fr/

En cas d'urgence, contactez le 17

Signalement

contenu illicite : www.internet-signalement.gouv.fr

courriel, spam ou hameçonnage www.signal-spam.fr

Nous pouvons vous aider à lutter contre :

Intrusion dans votre système informatique ou dans les locaux de l'entreprise

- **Contactez la gendarmerie qui pourra vous conseiller et dépêcher un enquêteur spécialisé.**
- **Préservez les traces et indices laissés par un cambrioleur, en attendant les opérations de police technique gendarmerie.**

Atteinte à l'image

- **Déposez plainte à la gendarmerie pour toute tentative de chantage, ou dénigrement sur le net, notamment en cas de refus de solidarité de votre entreprise suite à un démarchage en ligne.**

Attaque cyber notamment rançongiciel

- **Coupez l'alimentation d'Internet, identifier les postes infectés, lancer l'anti-virus…**
- **Déposez plainte à la gendarmerie.**

Escroquerie ou demande de virement douteux

- **Déposez plainte pour toute tentative de d'escroquerie via notamment les faux ordres de virement.**

Conception graphique Sirpa-gendarmerie C 8889 - 2020

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.

Conception graphique Sirpa-gendarmerie C 8889 - 2020