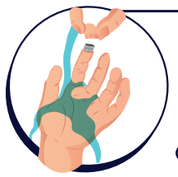
MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER

Liberté
Égalité
Fraternité

GESTES BARRIÈRES FACE AUX CYBERMENACES

Attention aux génériques

Choisissez des mots de passe personnels, différents et complexes. Renouvelez-les régulièrement et en cas de compromission.



Lavage des mains

Passez au scanner antivirus tout support amovible avant utilisation.

Attention aux contrefaçons

Vérifiez la provenance et la légitimité des courriels avant de répondre ou de cliquer sur un lien.

Port du masque

Verrouillez vos sessions en cas d'absence (⊞ + L ou ctrl + ⌘ + Q). Appliquez sur votre écran un filtre de confidentialité.

Provenance des produits

Ne téléchargez jamais un logiciel ou une mise à jour ailleurs que sur le site officiel de l'éditeur.

Contre-indications

Ne mélangez pas les usages professionnels et personnels pour éviter les effets indésirables.

Limite de confidentialité

Protégez vos données en chiffrant vos disques durs (Ex. : BitLocker sur Windows, FileVault sur MacOS).

Consentement médical

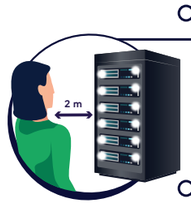
Signez la charte informatique de votre employeurs précisant les bonnes pratiques, vos droits et vos devoirs.

Vaccination

Injectez un antivirus dans votre système d'information. Effectuez les rappels pour maintenir à jour les effets.

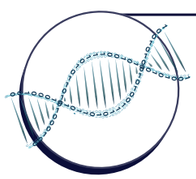
Renouvellement de l'air

Appliquez régulièrement les mises à jour de sécurité de votre système d'exploitation et de vos logiciels.



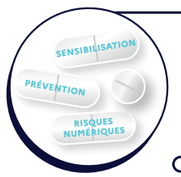
Distanciation physique

Limitez au strict besoin les accès aux zones contenant vos systèmes d'information.



Préservation de l'ADN

Réalisez des sauvegardes régulières de vos données et déconnectez-les de votre système d'information. Testez périodiquement leur bon fonctionnement.



Respect des doses prescrites

Sensibilisez vos utilisateurs aux risques numériques en vous attardant sur les zones sensibles.

Maintien à jour des droits

Administrez les droits utilisateurs en les réduisant au strict minimum et à la durée nécessaire.

Défenses immunitaires

Implantez des dispositifs de sécurité comme un pare-feu. Activez les protocoles de sécurité pour votre messagerie, votre site internet et vos accès distants.

Bilan de santé complet

Consultez un spécialiste pour faire un état des lieux de votre système d'information.

CERTAINS GESTES TECHNIQUES PEUVENT NÉCESSITER LE RECOURS À UN SPÉCIALISTE

POUR ALLER PLUS LOIN

Ma Sécurité
Application Grand Public

Application

Site internet

di@G⊜Nal

Pour évaluer votre
IMMUNITE CYBER
n'hésitez pas à demander
un diagnostic élémentaire
auprès de la gendarmerie

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

CYBER
MALVEILLANCE
.GOUV.FR

En cas d'urgence retournez le document

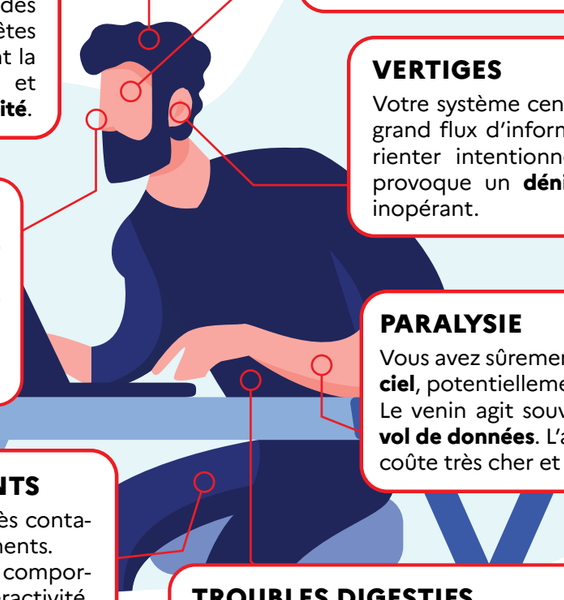
Création graphique : ComCyberGend © Gendarmerie 2023-010

SYMPTÔMES

DÉDOUBLEMENT DE LA PERSONNALITÉ
Vous attendez un virement qui n'arrive pas ? Vos contacts vous prêtent des actions ou des écrits dont vous n'êtes pas à l'origine ? Vous êtes sûrement la proie d'un **piratage de compte** et peut-être d'une **usurpation d'identité**.

ÉRUPTIONS CUTANÉES
Vous êtes victime d'un **défiguration** de votre site profitant d'une faiblesse de son système immunitaire pour porter atteinte à votre image ou pour faire passer un message.

FRISSONS ET TREMBLEMENTS
Un **logiciel malveillant**, souvent très contagieux, peut expliquer ces dérèglements.
Il pousse votre système à avoir un comportement inhabituel (atonie, hyperactivité, destruction de cellules, recopie d'ADN...)
Il peut faciliter de nouvelles infections.



TROUBLES VISUELS
Une attaque par **hameçonnage** est peut-être la cause de vos soucis. Sous des apparences trompeuses, elle vous a amené à révéler des données sensibles, à payer une somme d'argent ou à affaiblir vos défenses.

VERTIGES
Votre système central a été victime d'un trop grand flux d'informations visant à vous désorienter intentionnellement. Cette surcharge provoque un **déni de service** et vous rend inopérant.

PARALYSIE
Vous avez sûrement été mordu par un **rançongiciel**, potentiellement mortel.
Le venin agit souvent bien plus tard, après un **vol de données**. L'antidote qui vous est proposé coûte très cher et n'est pas fiable.

TROUBLES DIGESTIFS
Il peut s'agir d'un parasite qui a pénétré votre système pour agir à son gré de l'intérieur. Il peut, par exemple, utiliser votre énergie pour ses propres besoins. Vous êtes alors victime d'un **piratage de système d'information**.

DÉPOSEZ PLAINTE !

SI VOUS ÊTES VICTIME

Prévenez immédiatement les forces de l'ordre

17

Ma Sécurité
Application Grand Public

Ma Sécurité
Site internet

POURQUOI DÉPOSER PLAINTE ?

- Être reconnu comme victime et faire valoir vos droits,
- Être informé des processus d'indemnisation (assurance),
- Se prémunir d'une usurpation d'identité,
- Être accompagné dans des situations complexes (rançon, etc.),
- Bénéficier des résultats de l'enquête (connaître l'auteur des faits, être indemnisé, récupérer des données dérobées ou chiffrées, etc.),
- Participer à la lutte contre la cybercriminalité.

COMMENT S'Y PRENDRE ?

En se rendant dans une brigade de gendarmerie ou un commissariat de police.

OU

En écrivant au procureur de la République de mon lieu de domicile.

UNE PLAINTE BIEN PRÉPARÉE, C'EST DU TEMPS GAGNÉ !

- Pensez à vous munir des éléments de preuve que vous avez récoltés dans l'appréciation de l'état de la victime,
- Si le représentant légal ne peut se déplacer, venez avec un extrait du KBIS, une copie de sa pièce d'identité et un mandat daté et signé : « Je soussigné, [Nom] [Prénom] né le [Date de naissance] à [Lieu de naissance] [Nationalité] [Profession] [Adresse], représentant légal de [entité] donne tous pouvoirs pour déposer plainte à [Nom] [Prénom] né le [Date de naissance] à [Lieu de naissance] [Nationalité] [Profession][Adresse] ».

PREMIERS SECOURS

1 SÉCURISATION DES LIEUX DE L'ACCIDENT ET DES PERSONNES IMPLIQUÉES

Isolez chaque victime
Si votre système est atteint, coupez toutes les connexions à Internet et au réseau local afin d'éviter que l'attaque se propage.

Maintenez-les éveillées
N'éteignez pas les équipements infectés pour conserver des éléments de preuve situés dans la mémoire volatile.

Alertez les personnes alentours
Prévenez avec le juste niveau de transparence vos collaborateurs, clients, partenaires, fournisseurs...

2 APPRÉCIATION DE L'ÉTAT DE LA VICTIME

Recourez à la téléconsultation
Pour affiner votre diagnostic, suivez le parcours victime sur le site : ***cybermalveillance.gouv.fr***

Rassemblez le plus d'élements sur l'état de la victime
Préservez toutes les traces, pour éviter que les choses ne disparaissent : captures d'écran, fichiers, images, vidéos, clés USB, CD/DVD, disque dur, ordinateur infecté, journaux de connexions ou d'événements, etc.
Consignez toute les actions entreprises en datant les événements marquants.

3 DEMANDE D'AIDE

Faites appel à des spécialistes
Sollicitez immédiatement votre support informatique, interne ou externe, afin qu'il prenne en compte l'incident. Au besoin, recourez à un des prestataires proposés par ***cybermalveillance.gouv.fr***.

Prévenez immédiatement les forces de l'ordre
Alertez au plus vite les gendarmes ou les policiers. Par la suite **déposez plainte.**

Entourez-vous des personnes nécessaires pour gérer l'accident
Constituez une équipe de gestion de crise afin de piloter les actions des différentes composantes concernées (technique, RH, financière, communication, métiers, juridique...). Alertez, le cas échéant, votre banquier ou votre assureur.

4 RÉALISATION DES GESTES DE PREMIERS SECOURS

Ne pratiquez aucune action que vous ne maîtrisez pas
Le « remède » peut être pire que le mal ! Suivez scrupuleusement les recommandations de ***cybermalveillance.gouv.fr***. En particulier, ne cherchez pas à négocier vous même avec les cybercriminels.

Maintenez les constantes vitales
Mettez en place des solutions de secours pour pouvoir continuer à assurer les services indispensables. Activez vos plans de continuité et de reprise d'activité (PCA-PRA) si vous en disposez.

Evitez le suraccident
Notifiez **obligatoirement** l'incident à la CNIL dans les 72 heures si des données à caractère personnel ont pu être consultées, exfiltrées, modifiées ou détruites.

5 RÉÉDUCATION APRÈS L'OPÉRATION

Faites une remise en service progressive et contrôlée après vous être assuré que le système attaqué a été corrigé de ses vulnérabilités et en surveillant son fonctionnement pour pouvoir détecter toute nouvelle attaque. Tirez les enseignements de l'attaque et prenez toutes les mesures correctrices nécessaires.

Après retour à la normale, retournez ce document

Création graphique : ComCyberGend © Gendarmerie 2023-010