CYBERSÉCURITÉ

Fiche cyber-crise

Procédure CYBER CRISE

CHU AMIENS PICARDIE

Procédure CYBER CRISE

01 – OBJET

La présente procédure décrit les actions à mettre en œuvre par chacun des acteurs du système d’information (utilisateur, techniciens, service informatique, responsable, direction…) en cas de crise liée à une cyberattaque.

02- DOMAINE D’APPLICATION ET PERSONNEL CONCERNE

L’ensemble des agents du CHU d’Amiens Picardie sont concernés par cette procédure. Cette dernière
s’applique sur la globalité du système d’information en cas de cyber-attaque

03-DESCRIPTION

3.1 – IDENTIFICATION DU PROBLÈME

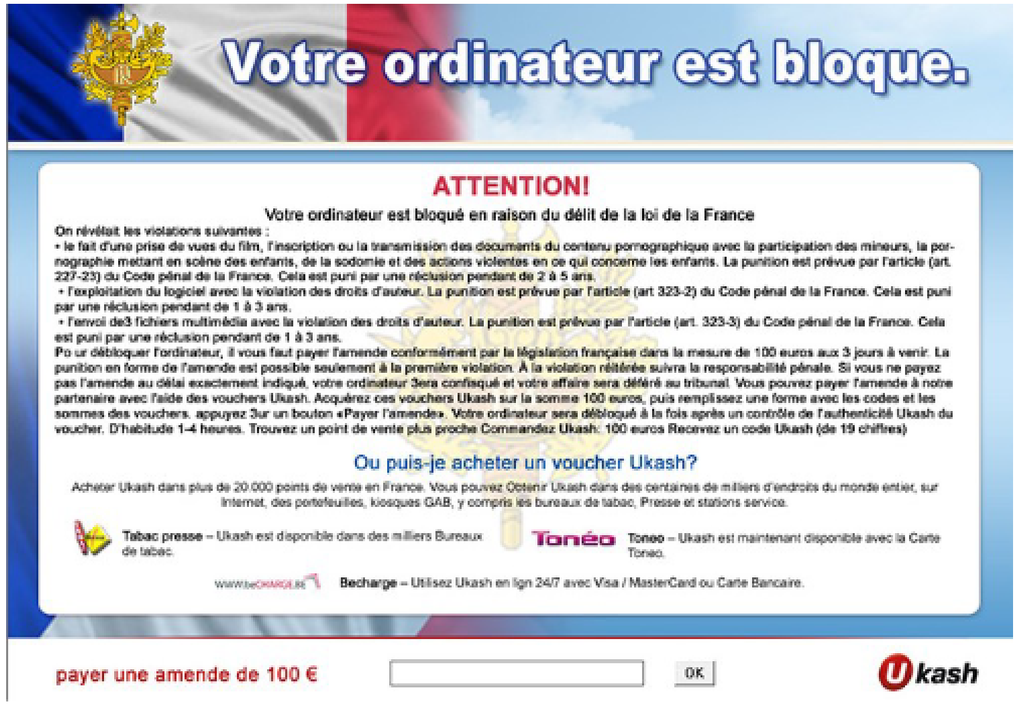
Si vous être confrontés à l'un des problèmes cités ci dessous, vous êtes probablement victime d'une cyberattaque, dans ce cas réaliser sans attendre les actions évoquées dans la section 6.2

Cybercriminalité :

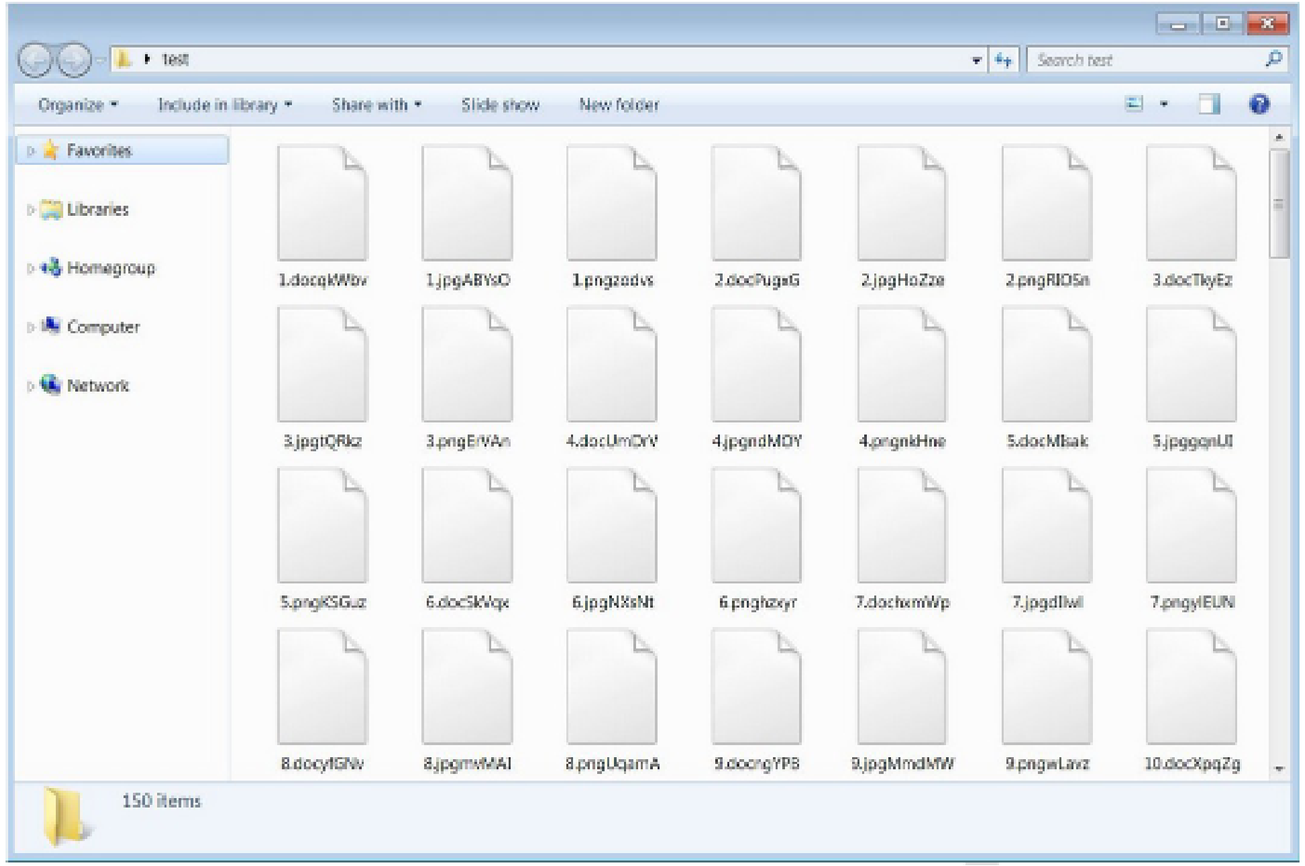
Attaque par rançongiciel :

Les rançongiciels sont des programmes informatiques malveillants (ex : Locky, TeslaCrypt, Cryptolocker, etc.) dont l'objectif est de chiffrer des données puis de demander à leur propriétaire d'envoyer de l'argent en échange de la clé qui permettra de les déchiffrer.

- ✔ **Votre ordinateur est bloqué sur une page vous indiquant de payer une certaine somme d'argent afin de débloquer vos fichiers**

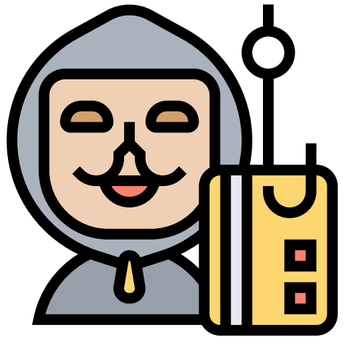


- ✔ **Vos fichiers ou programmes ont été renommés avec des suites des caractères et il est impossible des les ouvrir**
- ✔ **Vos fichiers ou dossiers sont impossibles à ouvrir avec leurs programmes habituels**



Attaque par hameçonnage :

L’hameçonnage, phishing ou filoutage est une technique malveillante dont l’objectif est d’opérer une usurpation d’identité afin d’obtenir des renseignements personnels et des identifiants bancaires pour en faire un usage criminel. Il existe également un type d’hameçonnage par clé usb.



- ✔ **Vous avez reçu un courriel suspect vous invitant à cliquer sur un lien ou à ouvrir une pièce jointe. Vous avez, sans vous méfiez, ouvert les éléments.**

impots.gouv.fr

un site de la direction générale des finances publiques

Bonjour,

Après les derniers calculs annuels de l'exercice de votre activité, nous avons determiné que vous êtes admissible à recevoir un remboursement de 50.80 €.
Veuillez nous soumettre s'il vous plaît la demande de remboursement d'impôt pour nous permettre de la traiter dans un plus bref délai.

>> Pour accéder au formulaire , cliquez ici .

Un remboursement peut être retadré pour diverses raisons. Par exemple, une soumission de dossiers non valides ou une inscription après une certaine limite.

Vous avez reçu un courriel suspect vous incitant à y répondre et transmettre des éléments personnels (code de carte, téléphone, mot de passe….). Vous avez, sans vous méfier, répondu à ce courriel.

✔

-------- Message transféré --------
Sujet :Tr : Chers Utilisateurs,
Date :Mon, 25 Jan 2021 10:05:14 +0000 (GMT)
De :Labourier Dominique <dominique.rousset@ac-limoges.fr>

Chers Utilisateurs.

Dans le cadre de l'installation définitive des nouveaux paramètres Mail ® et de la réinitialisation de toutes nos adresses, il est procédé à un marquage de tous les comptes actifs à ce jour. Afin de ne pas risquer de perdre votre compte Mail ® lors de l'expiration de notre précédant service de messagerie, vous êtes donc prié de bien vouloir remplir impérativement la grille d'information en dessous.

Passé le délai de 48 heures, nous procéderons à la suppression de toutes les adresses non encore enregistrées.

Cliquer sur " **Répondre**" Remplissez la grille d'informations. Ensuite cliquez sur " **Envoyer**" Une fois le remplissage terminé.

Informations obligatoires *

Nom& Prénoms: *……

Adresse Mail :*……

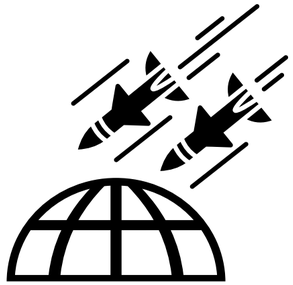
(Mot_Pass): *……

Confirmation du (Mot_Pass): *……

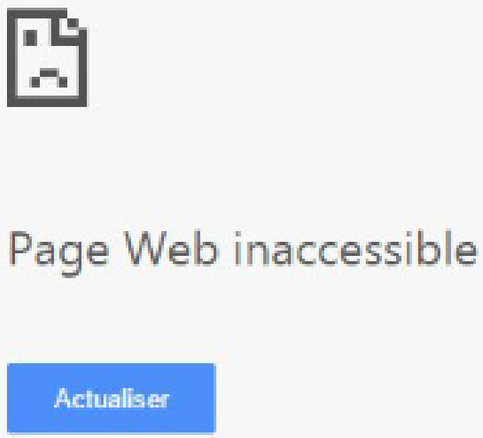
Après avoir répondu au questionnaire et après vérification par nos services votre compte continuera de fonctionner normalement. Nous vous remercions pour votre bonne compréhension et nous exerçons à améliorer nos services pour nos utilisateurs. Tout en nous excusant pour ces désagréments.

Atteinte à l'image :

Attaque par déni de service (DddoS) :
Le déni de service cherche à porter atteinte à l'image de la victime en rendant son site, donc le service attendu, indisponible

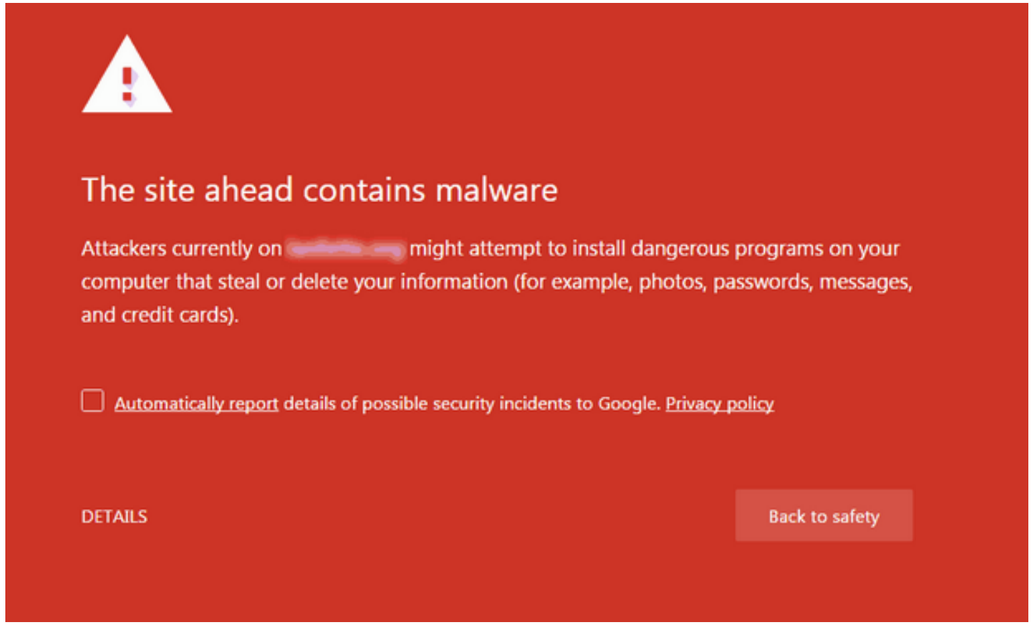


✔ **Votre site Internet est inaccessible ou votre accès Internet ne fonctionne plus**



Attaque par défiguration (défacement) :

L'objectif est de modifier l'apparence ou le contenu d'un site internet, et donc violer l'intégrité des pages en les altérant. Le cybercriminel exploite souvent des vulnérabilités connues (défaut de sécurité), mais non corrigées du site web.

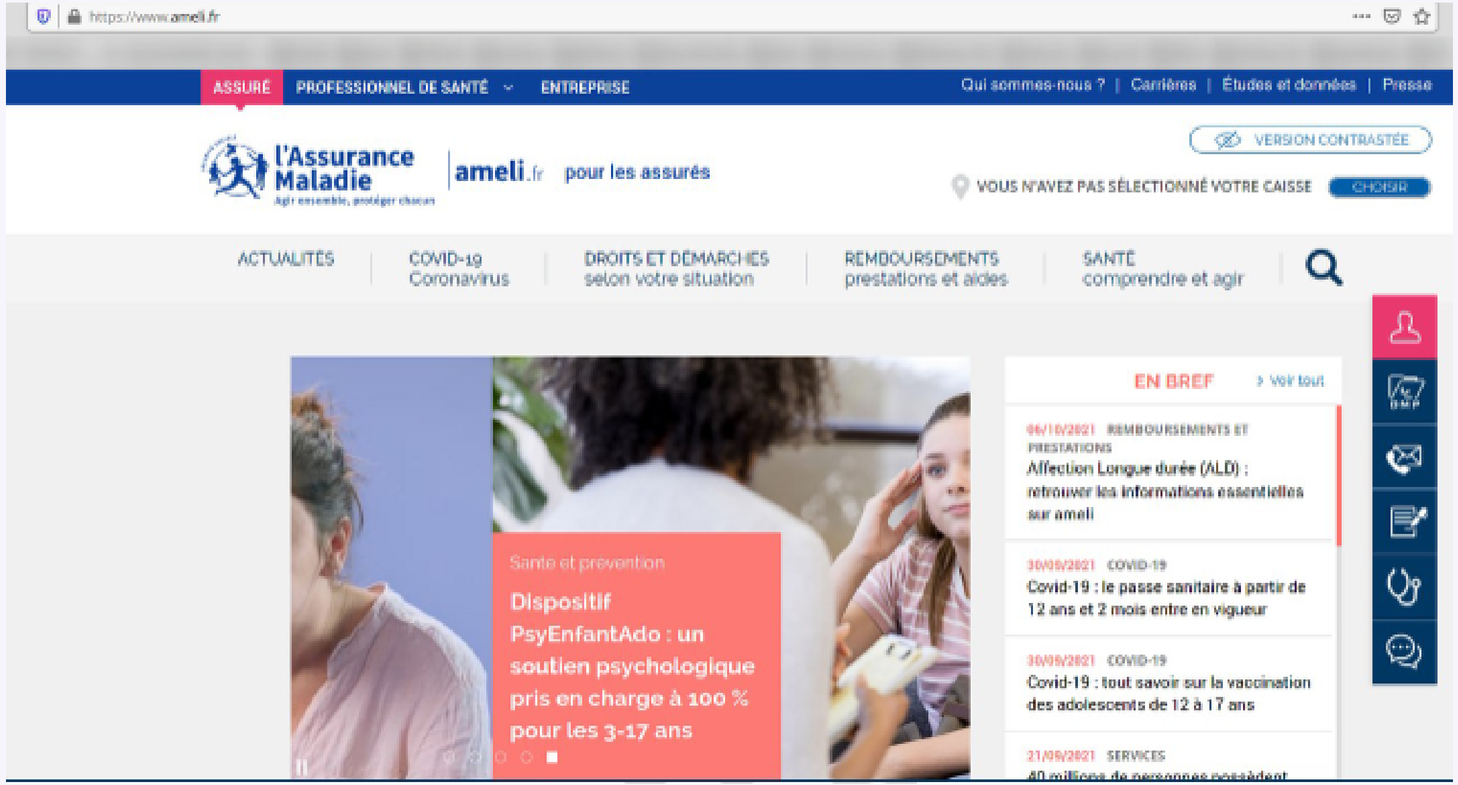


✔ **Votre site Internet a changé d'apparence et semble avoir été piraté**

Espionnage :

Attaque par point d’eau (watering hole) :
La technique du « point d’eau » consiste à piéger un site internet légitime afin d’infecter les équipements des visiteurs du secteur d’activité visé par l’attaquant. Objectif : infiltrer discrètement les ordinateurs de personnels œuvrant dans un secteur d’activité ou une organisation ciblée pour récupérer des données

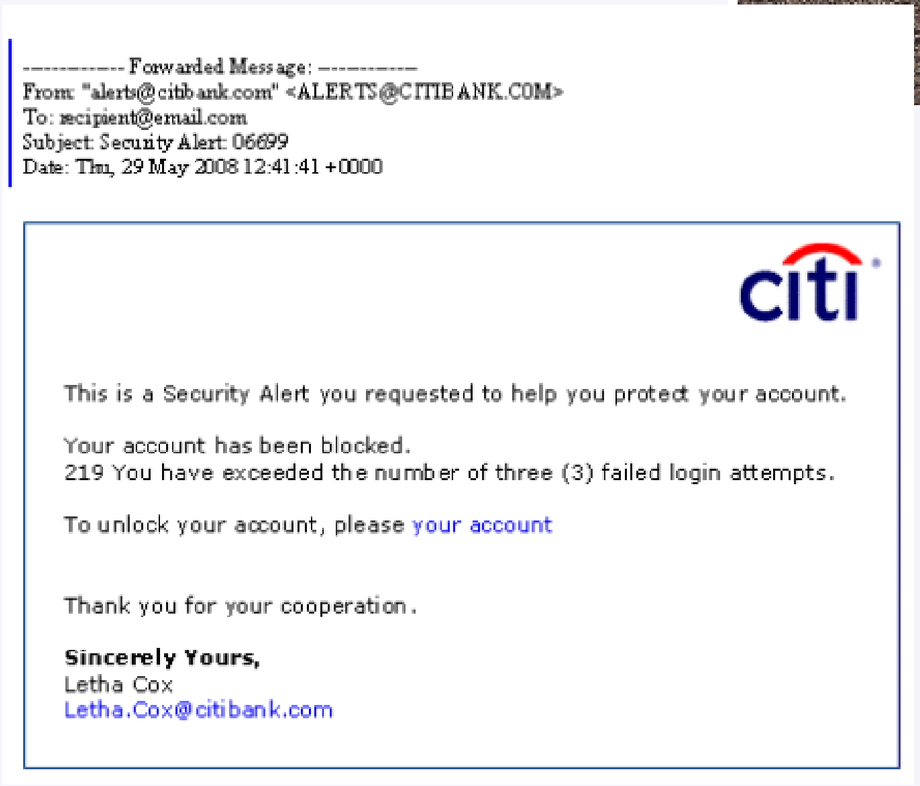
✔ **Vous avez visité un site sur lequel vous avez l’habitude d’aller. Ce dernier a été piégé par des pirates qui souhaitaient que vous fournissiez volontairement des informations personnel ou confidentiel sans vous méfier.**



Attaque par hameçonnage ciblé (spearphishing) :

Cette attaque repose sur une usurpation de l'identité de l'expéditeur et vise à infiltrer le système d'information d'une organisation d'un secteur d'activité ciblé. L'attaque ciblé peut également être réalisée à l'aide de clés usb exposées dans des endroits ciblés.

✔ **Vous avez reçu un courriel suspect mais cependant envoyé par une connaissance ou une société pour laquelle vous êtes client. Ce courriel paraissant légitime, il vous invitait à cliquer sur un lien ou à ouvrir une pièce jointe ou à transmettre des informations confidentiels (code de carte, mot de passe,...) Vous avez, sans vous méfiez, ouvert les éléments ou répondu au courriel**



---------- Forwarded Message: ----------
From: "alerts@citibank.com" <ALERTS@CITIBANK.COM>
To: recipient@email.com
Subject: Security Alert: 06699
Date: Thu, 29 May 2008 12:41:41 +0000

citi

This is a Security Alert you requested to help you protect your account.

Your account has been blocked.
219 You have exceeded the number of three (3) failed login attempts.

To unlock your account, please your account

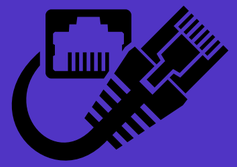
Thank you for your cooperation.

Sincerely Yours,
Letha Cox
Letha.Cox@citibank.com

✔ **Vous avez trouvé un équipement de stockage usb (clé, lecteur, carte, téléphone...) et l'avez branché sur votre pc afin de voir ce qu'il contenait sans vous méfier si un programme malveillant s'y trouvait.**

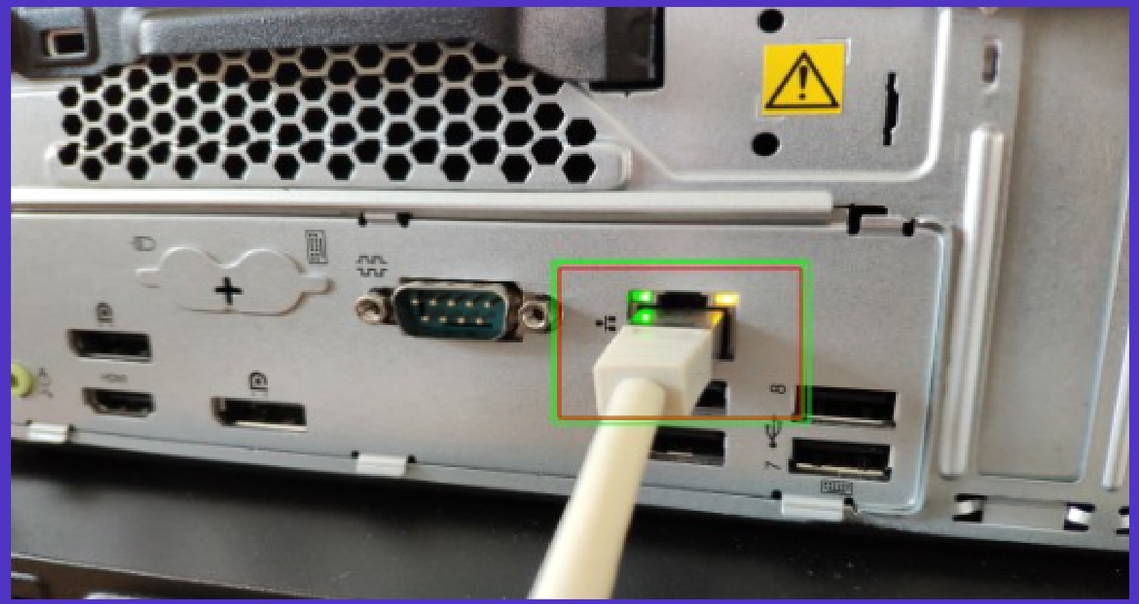
4 – RÉACTION DE L’UTILISATEUR FACE AU PROBLÈME

1. Déconnecter la machine suspecte du réseau :

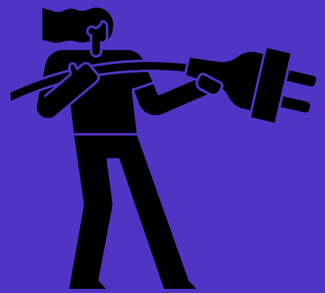


PC fixe (de bureau) :

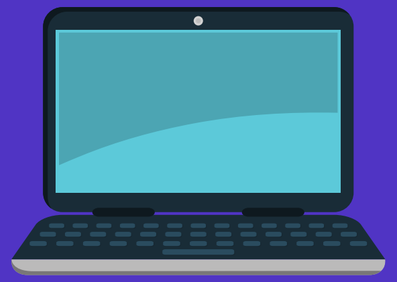
➢ En 1ère intention, afin de limiter la propagation des virus informatiques sur l'infrastructure de l'établissement, il suffit de débrancher le câble réseau derrière le PC relié à la prise qui clignote.



➢ En cas de problème avec la manipulation ou dans le doute, forcer l'arrêt du PC en appuyant au moins 10 secondes sur le bouton de démarrage du PC ou débrancher électriquement le PC.



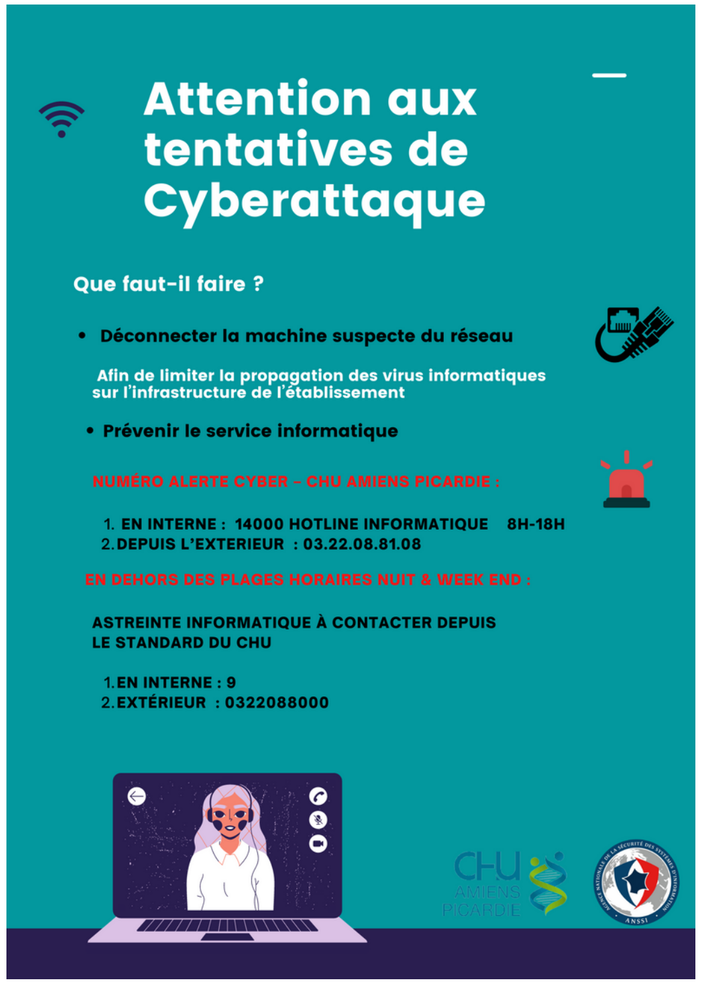
PC portable :



➢ En 1ère intention afin de limiter la propagation des virus informatique sur l'infrastructure de l'établissement, il suffit de couper le wifi en mettant le pc en veille prolongée. Appuyer pour cela sur le bouton de démarrage du pc, l'écran doit s'éteindre. Vérifier en bougeant la souris que l'écran reste éteint.

➢ En cas de problème avec la manipulation ou dans le doute, forcer l'arrêt du PC en appuyant au moins 10 secondes sur le bouton de démarrage du PC

2. Prévenir le service informatique



NUMÉRO ALERTE CYBER – CHU AMIENS PICARDIE :

1. **EN INTERNE : 14000 HOTLINE INFORMATIQUE 8H-18H**
2. **DEPUIS L'EXTERIEUR : 03.22.08.81.08**

EN DEHORS DES PLAGES HORAIRES NUIT & WEEK END :

ASTREINTE INFORMATIQUE À CONTACTER DEPUIS LE STANDARD DU CHU

1. **-EN INTERNE : 9**
2. **-EXTÉRIEUR : 0322088000**