

CYBERSÉCURITÉ

Fiche cyber- crise

[Procédure CYBER CRISE](#)

Procédure CYBER CRISE

- 01 OBJET
- 02 DOMAINE D'APPLICATION ET PERSONNEL CONCERNE
- 03 DESCRIPTION
- 04 RÉACTION DE L'UTILISATEUR FACE AU PROBLÈME

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 êtes confrontés à l'un des problèmes cités ci-dessous, vous êtes probablement victime d'une cyberattaque, dans ce cas réalisez 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**

Votre ordinateur est bloqué.

ATTENTION!

Votre ordinateur est bloqué en raison du délit de la loi de la France


On révérait les violations suivantes :


- le fait d'une prise de vues du film, l'inscription ou la transmission des documents du contenu pornographique avec la participation des mineurs, la pornographie mettant en scène des enfants, de la sodomie et des actions violentes en ce qui concerne les enfants. La punition est prévue par l'article (art. 227-23) du Code pénal de la France. Cela est puni par une réclusion pendant de 2 à 5 ans.
- l'exploitation du logiciel avec la violation des droits d'auteur. La punition est prévue par l'article (art. 323-2) du Code pénal de la France. Cela est puni par une réclusion pendant de 1 à 3 ans.
- l'envoi de 3 fichiers multimédia avec la violation des droits d'auteur. La punition est prévue par l'article (art. 323-3) du Code pénal de la France. Cela est puni par une réclusion pendant de 1 à 3 ans.

Pour débloquer l'ordinateur, il vous faut payer l'amende conformément par la législation française dans la mesure de 100 euros aux 3 jours à venir. La punition en forme de l'amende est possible seulement à la première violation. À la violation réitérée suivra la responsabilité pénale. Si vous ne payez pas l'amende au délai exactement indiqué, votre ordinateur sera confisqué et votre affaire sera déferé au tribunal. Vous pouvez payer l'amende à notre partenaire avec l'aide des vouchers Ukash. Acquérez ces vouchers Ukash sur la somme 100 euros, puis remplissez une forme avec les codes et les sommes des vouchers, appuyez sur un bouton «Payer l'amende». Votre ordinateur sera débloqué à la fois après un contrôle de l'authenticité Ukash du voucher. D'habitude 1-4 heures. Trouvez un point de vente plus proche Commandez Ukash: 100 euros Recevez un code Ukash (de 19 chiffres)

Où puis-je acheter un voucher Ukash?


Acheter Ukash dans plus de 20 000 points de vente en France. Vous pouvez obtenir Ukash dans des centaines de milliers d'endroits du monde entier, sur Internet, des portefeuilles, kiosques GAB, y compris les bureaux de tabac, Presse et stations service.

 **Tabac presse** – Ukash est disponible dans des milliers Bureaux de tabac.

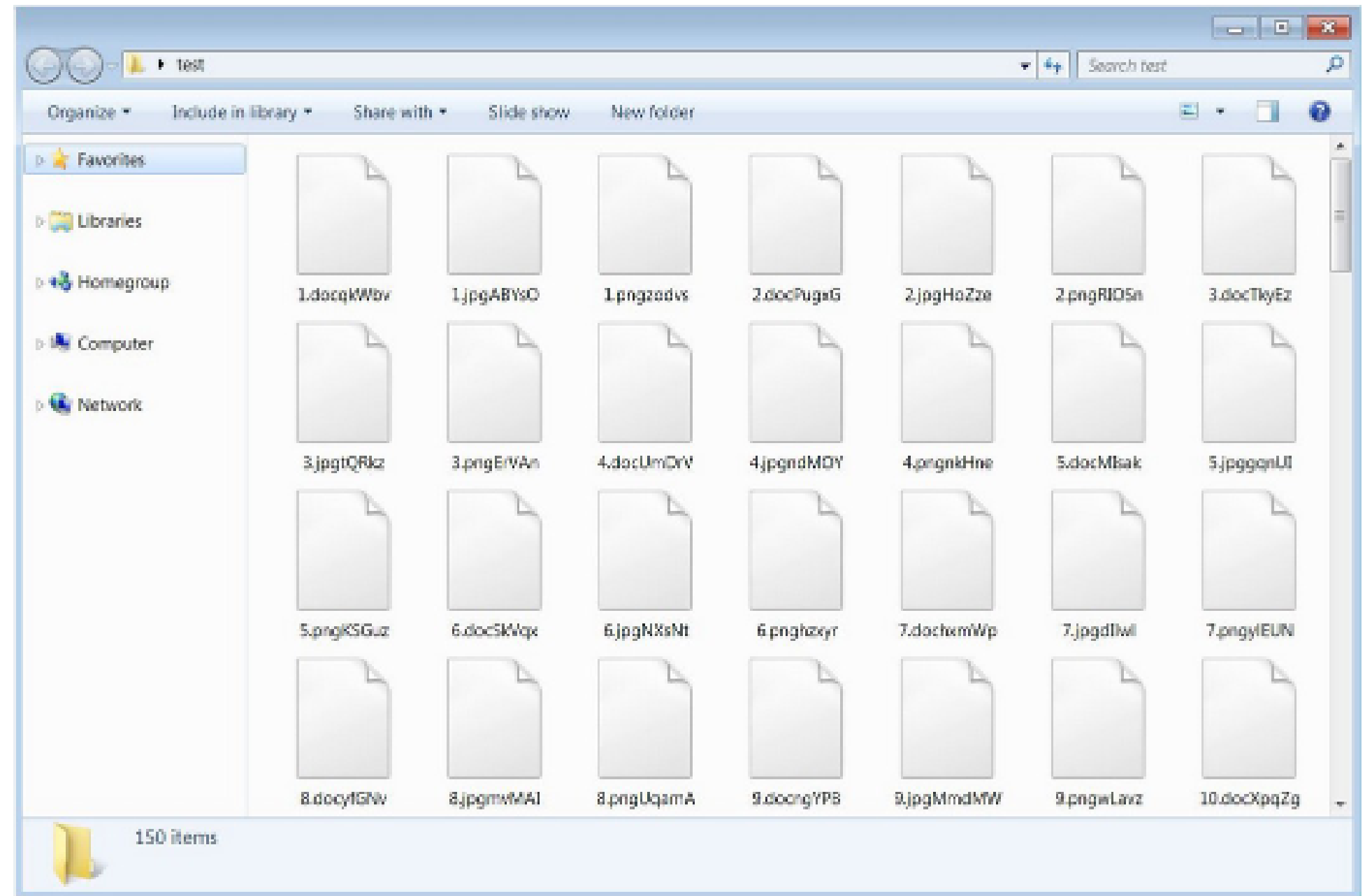
 **Tonéo** – Ukash est maintenant disponible avec la Carte Tonéo.

www.lecharge.fr **Becharge** – Utilisez Ukash en ligne 24/7 avec Visa / MasterCard ou Carte Bancaire.

payer une amende de 100 €

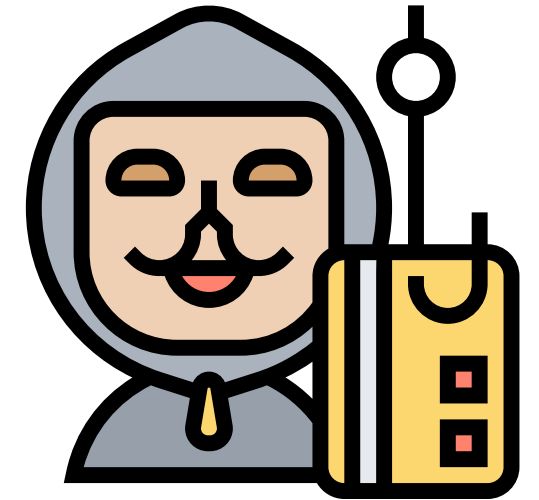


- ✓ **Vos fichiers ou programmes ont été renommés avec des suites des caractères et il est impossible des les ouvrir**
- ✓ **Vos fichiers ou dossiers sont impossibles à ouvrir avec leurs programmes habituels**



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 méfier, 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 déterminé 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 retardé 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 : Chers Utilisateurs,
Date : Mon, 25 Jan 2021 10:05:14 +0000 (GMT)
De : Laborier Dominique <dominique.rousseau@ac-illanges.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 précédent 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.

Cliquez 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) : *

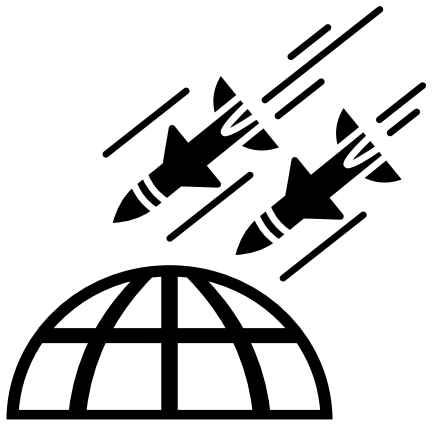
Après avoir répondu au questionnaire et après vérification par nos services votre compte continuera de fonctionner normalement. Nous vous remercions pour votre bonne compréhension et nous exerçons à améliorer nos services pour nos utilisateurs. Tout en nous excusant pour ces désagréments.



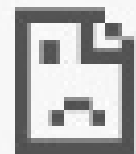
Atteinte à l'image :

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**



Page Web inaccessible

Actualiser

Standard 03 22 08 80 00

DÉCOUVREZ L'HÔPITAL PATIENTS ET VISITEURS ÉTUDIANTS PROFESSIONNELS CHERCHEURS

Rechercher sur le site...

NUMÉROS D'URGENCES

L'excellence à taille humaine pour chaque patient

#LeDéfiDeJanvier

Et si en janvier, on faisait une pause avec l'alcool?

DRY JANUARY

Et si en janvier, on faisait une pause avec l'alcool?

Rejoignez #LeDéfiDeJanvier

BIOBANQUE PICARDIE

CERTIFICATION ISO 20387

La Biobanque certifiée ISO20387

DÉMÉNAGEMENT

Déménagement du Hall 3 – Fontenoy

Découvrir le CHU

Consulter l'annuaire

Notre agenda

SERVICES ET CONTACTS

Trouver un service, une spécialité

NOUS REJOINDRE

Consulter les offres d'emploi

Effectuez votre recherche dans l'annuaire du CHU

Entrez votre recherche...

19 JAN 2023 8ème JARS

> Réservé aux personnels de la recherche en santé...

19 JAN 2023 Dry January

> Quart à tous (gratuit) Et en

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.

The site ahead contains malware

Attackers currently on [redacted] might attempt to install dangerous programs on your computer that steal or delete your information (for example, photos, passwords, messages, and credit cards).

Automatically report details of possible security incidents to Google. [Privacy policy](#)

[DETAILS](#) [Back to safety](#)



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

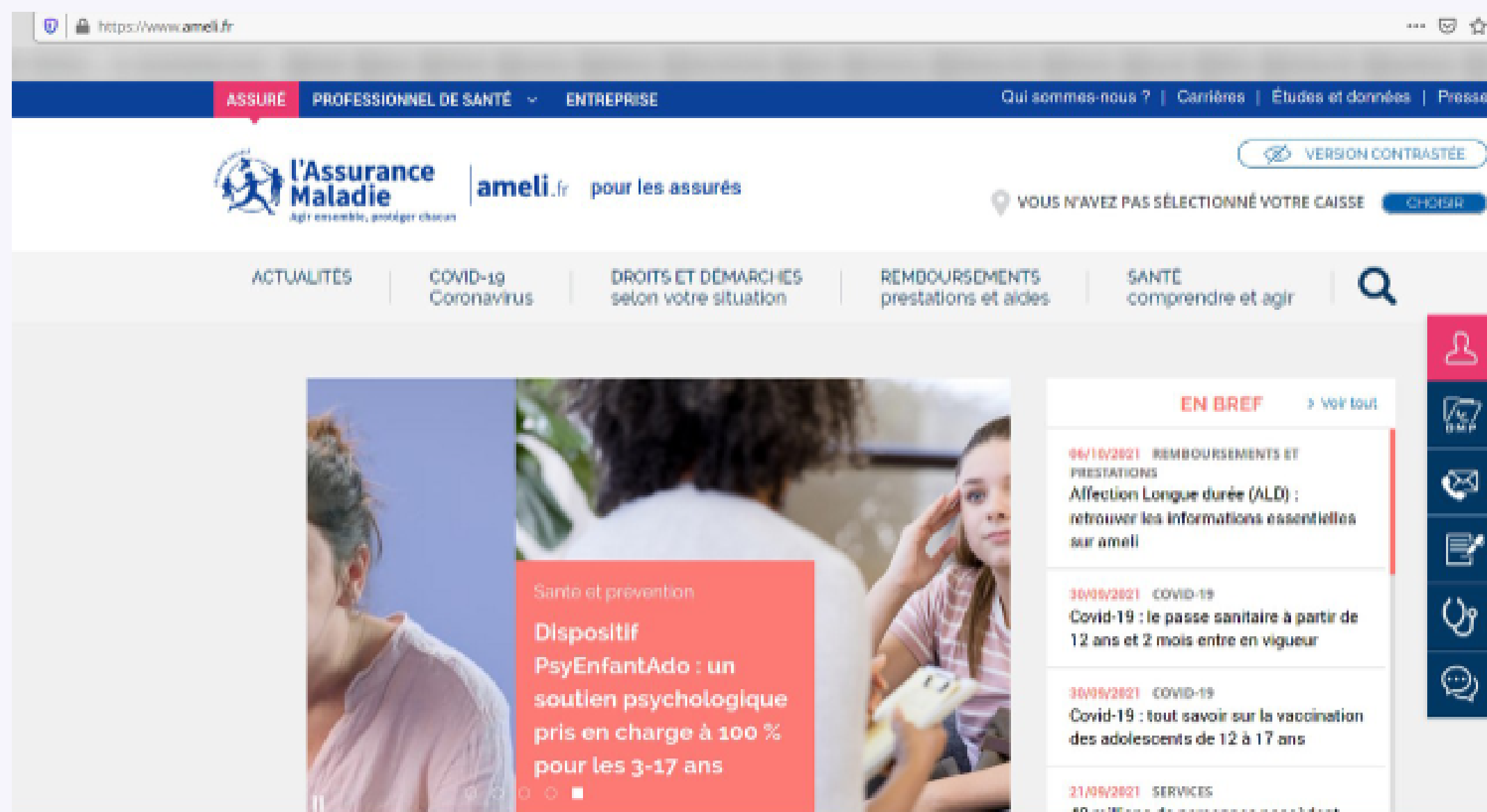
Espionnage :

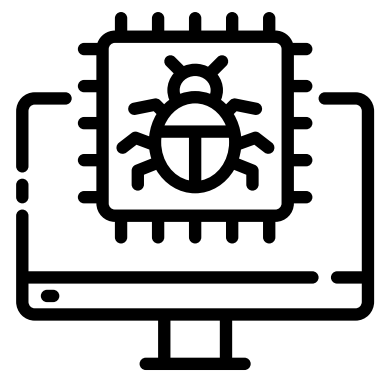


Attaque par point d'eau (watering hole) :

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 souhaitent 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 ciblée 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 méfier, 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



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

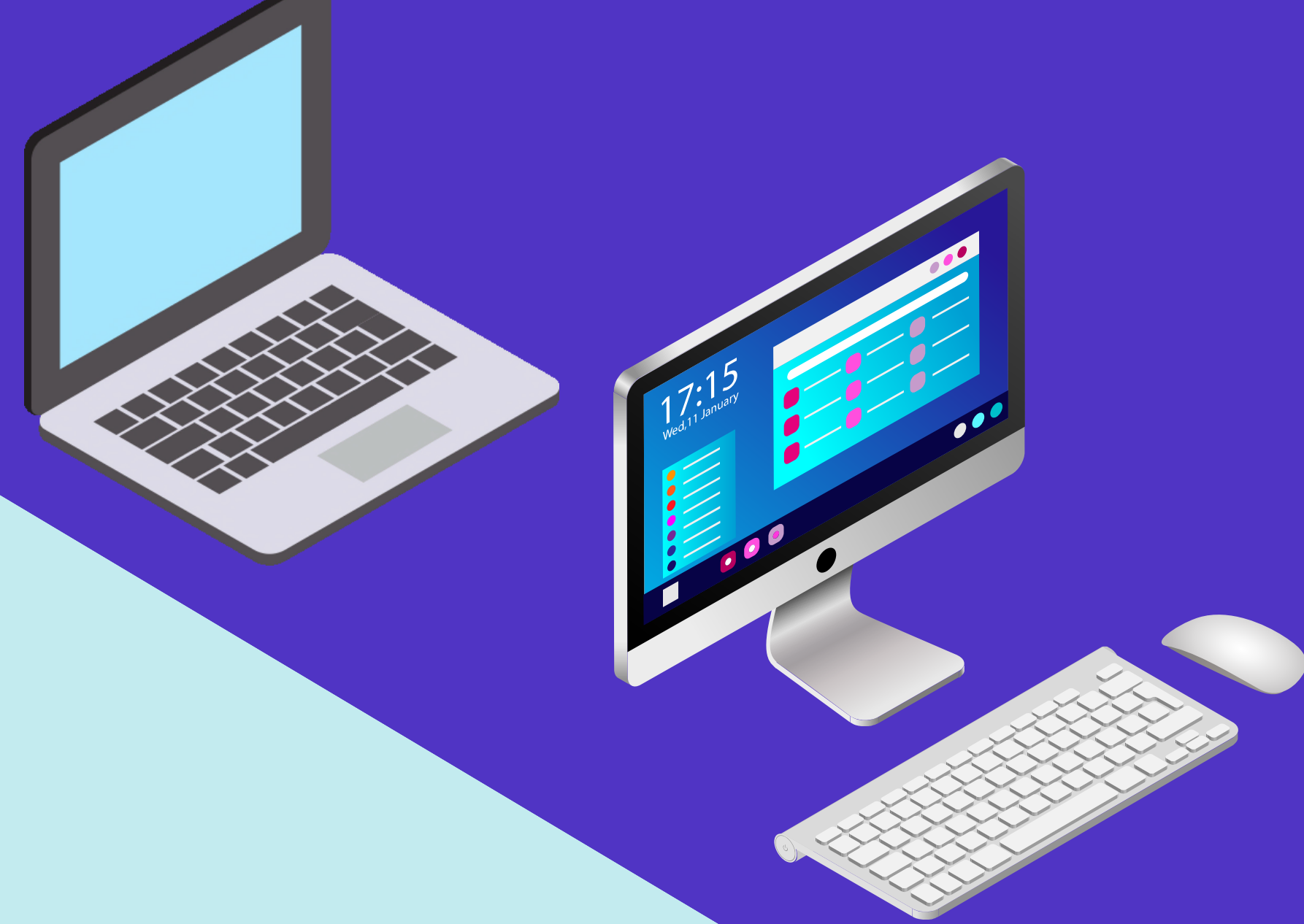
Your account has been blocked.
219 You have exceeded the number of three (3) failed login attempts.

To unlock your account, please [your account](#)

Thank you for your cooperation.

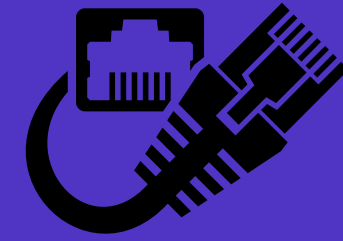
Sincerely Yours,
Letha Cox
Letha.Cox@citibank.com

- ✓ 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 :

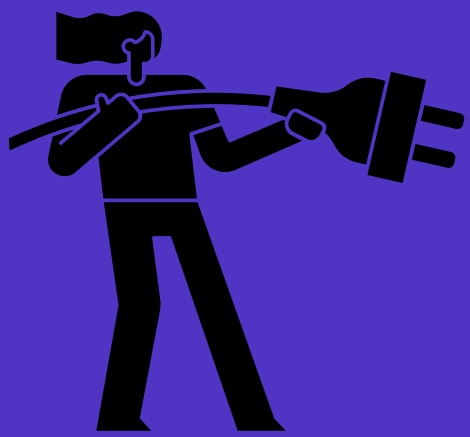
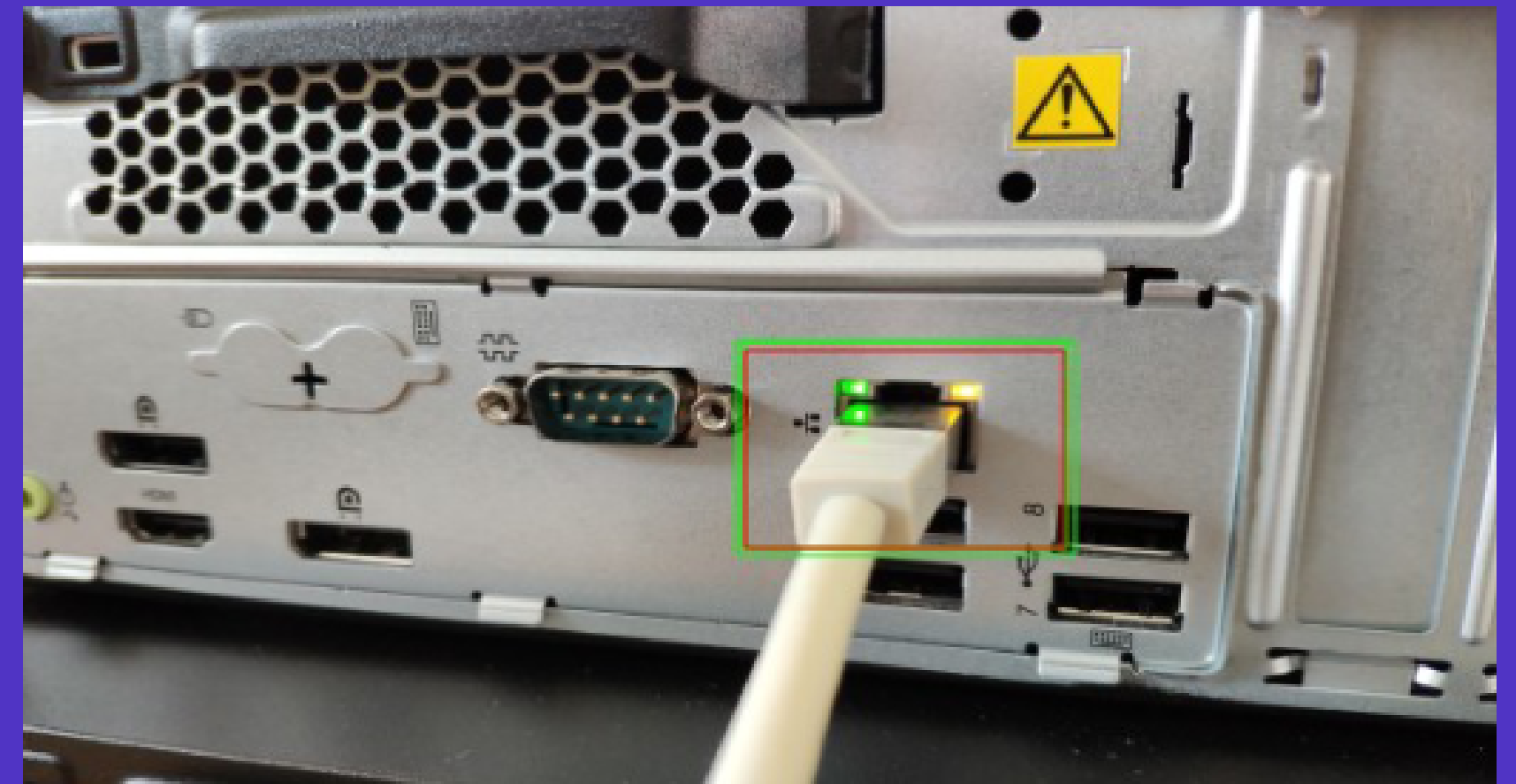


PC fixe (de bureau) :

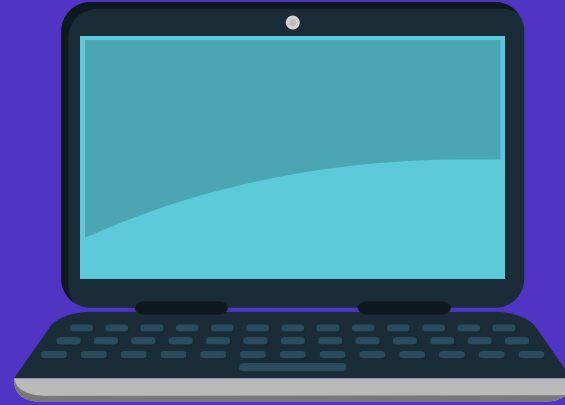
➤ En 1ère intention, afin de limiter la propagation des virus informatiques sur l'infrastructure de l'établissement, il suffit de débrancher le câble réseau derrière le PC relié à la prise qui clignote.



➤ 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



 **Attention aux tentatives de Cyberattaque**

Que faut-il faire ?

- Déconnecter la machine suspecte du réseau
Afin de limiter la propagation des virus informatiques sur l'infrastructure de l'établissement
- 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

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

