FICHE RÉSUMÉE

USAGES ET BONNES PRATIQUES DE SÉCURITÉ

I) La sécurité de vos équipements

1) Mettre à jour son outil

Sous windows

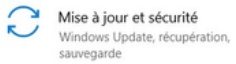
1) Ouvrez le menu windows

2) Ouvrez les paramètres

3) Ouvrez le menu windows Uptdate



Ou ce menu sous windows 10

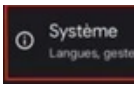


Sous Android

1) Ouvrez les paramètres

Sous Samsung

2)



3)



Sous Huawei et Redmi

2)



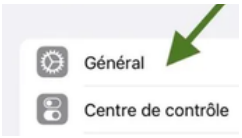
3)



Sous Iphone

1) Ouvrez les paramètres

2)



3)



Sous linux

1) Ouvrez le menu de démarrage en bas à gauche

2) Cliquez sur cette icône



Contact :
conseillernumerique@cmnc03.fr
06.07.71.87.83

Financé par GOUVERNEMENT Liberté Égalité Fraternité
FRANCE RELANCE
Financé par l'Union européenne NextGenerationEU

1b) Mettre à jours ses logiciels et applications

Sous windows

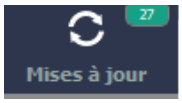
1) Installer le logiciel de mise jour Ucheck, mettant à jour tous les logiciels facilement

Adlice Software UCHECK

2) En ouvrant le logiciel, cliquer sur scanner

Scanner

3) Cliquer sur la catégorie mise à jour



Mettre à jour les logiciels de Microsot

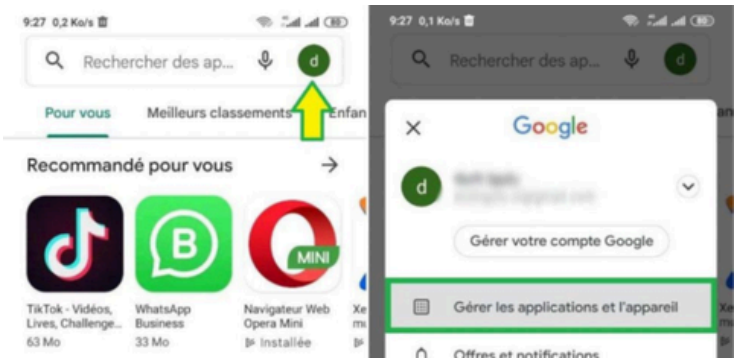
1) Ouvrir le microsoft store

2) Cliquez sur l'onglet téléchargements



Sous android

1) Ouvrir le play store



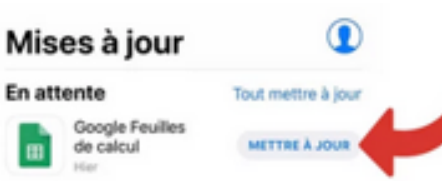
Sous iphone

1) Ouvrir l'App store

2) Cliquez sur votre profil en haut à droite



3) Cliquez sur le bouton Mettre à jour



Sous linux

2) Ouvrez l'icône correspondant à votre boutique

1) Ouvrez le menu de démarrage en bas à gauche

3) Cliquez sur le bouton Mettre à jour

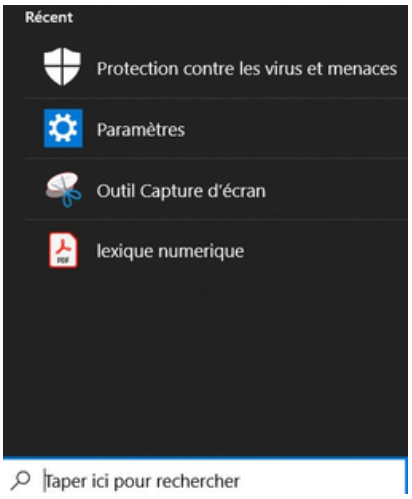
II) Avoir un antivirus à jour sous Windows



Des versions payantes ou gratuites existent, sur son ordinateur mais aussi sur ses appareils mobiles.
Il faut effectuer des scans et des mises à jour régulièrement

Lancer un scan de l'antivirus windows

1) Inscrire dans la barre de recherche antivirus et cliquer sur protection contre les virus



2) Cliquer sur analyse rapide



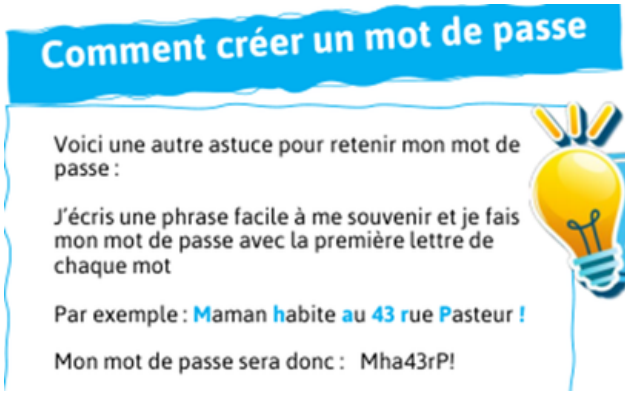
III) La sécurité d'un bon mot de passe

Chiffres +lettres

Majuscules et Minuscules

8 caractères minimum...
mais 12 c'est mieux

Si possible des Caractères Spéciaux



Avoir une routine de mots de passe. Par exemple mon mot de passe habituel est Milou22.
Je décide que ma routine de mot de passe sera de mettre devant mon mot de passe habituelle les 3 premières lettres du site internet auquel je me connecte en majuscule, suivi d'un « ! »
Pour Facebook mon mot de passe sera donc FAC!Milou22
Pour Youtbube, ce sera YOU!Milou22

Combien de temps, faut-il à un pirate pour trouver votre mot de passe ?

Nombre de caractères	Nombres seulement	Lettres minuscules	Lettres majuscules et minescules	Nombres, lettres majuscules et minuscules	Nombres, lettres majuscules et minuscules, symboles
4	Instantané	Instantané	Instantané	Instantané	Instantané
5	Instantané	Instantané	57 minutes	2 heures	4 heures
6	Instantané	46 minutes	2 jours	6 jours	2 semaines
7	Instantané	20 heures	4 mois	1 an	2 ans
8	Instantané	3 semaines	15 ans	62 ans	164 ans
9	2 heures	2 ans	791 ans	3k ans	11k ans
10	1 jour	40 ans	41k ans	238k ans	803k ans
11	1 semaine	1k ans	2M ans	14M ans	56M ans
12	3 mois	27k ans	111M ans	917M ans	3Md ans
13	3 ans	705k ans	5Md ans	56Md ans	275Md ans
14	28 ans	18M ans	300Md ans	3Bn ans	19Bn ans
15	284 ans	477M ans	15Bn ans	218Bn ans	1Bd ans
16	2k ans	12Md ans	812Bn ans	13Bd ans	94Bd ans
17	28k ans	322Md ans	42Bd ans	840Bd ans	6Tn ans
18	284k ans	8Bn ans	2Tn ans	52Tn ans	463Tn ans

CNIL. FantomApp

FantomApp est un outil de la Cnil pour tester son mot de passe.

Utilisation d'un gestionnaire de mots de passe

Un gestionnaire de mots de passe permet de mémoriser à votre place.
exemple : KeePassXc, Dashlane, Password

Les bonnes attitudes

- Avoir un mot de passe par service
- Activez la double authentification
- Choisir un mot de passe qui n'a pas de lien avec vous

IV) Vérifier la fiabilité d'un site Internet, mail, numéro de téléphone

ScamDoc

Site Internet qui permet d'évaluer la confiance d'une "identité numérique" (adresse mail ou site internet).

scamtel

Le deuxième onglet du site scam doc offre une évaluation automatique de la confiance d'un numéro de téléphone.

33700
La plateforme de lutte contre les SMS et appels indésirables

La plateforme de lutte contre les SMS et appels indésirables

V) Les Différentes menaces

1) le phising



En français, le phishing se traduit par hameçonnage.
C'est une technique employée par des pirates informatiques pour récupérer mes
données personnelles.
Par exemple :

- mes identifiants est mot de passe
- mon numéro de sécurité sociale
- ou mon numéro de carte bleu

En règle général, le pirate va se faire passer pour une administration ou une entreprise
que je connais.
Par exemple : ma banque, la CAF (la Caisse d'Allocation Familiale), les impôts etc.
Je reçois un mail ou un texte qui me demande de cliquer sur un lien pour donner ou
confirmer mes informations personnelles.

2) Les mails frauduleux

Comme pour l'arnaque du phishing, je peux recevoir un mail frauduleux.
Cette fois, cela n'est pas pour récupérer mes données mais pour me demander de l'argent.
Cela peut être par exemple :

- une promesse d'héritage
- un gain à une loterie
- une livraison de colis en attente
- un ami qui a des problèmes





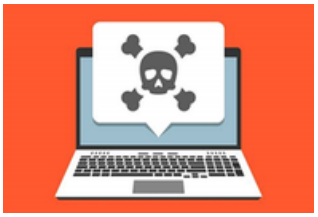
Les arnaqueurs ont beaucoup d'imagination. Ils peuvent inventer encore d'autres excuses pour me soutirer de l'argent.

Ce qui doit attirer l'attention

- Le mail de l'expéditeur
- L'objet du mail
- Les fautes d'orthographe
- Demande d'informations personnels
- L'adresse du site
- Des liens qui ne fonctionnent pas

3) Les malware

Tous les types de malwares suivent le même schéma de base : votre appareil est infecté après avoir téléchargé ou installé involontairement un malware, souvent en cliquant sur un lien infecté ou en visitant un site Web infecté.



Logiciel à télécharger pour éliminer les malaware



Le cheval de Troie

Est **un type de malware** qui se télécharge sur un ordinateur, déguisé en programme légitime.

Il va s'installer sur mon ordinateur et crypter tout ce qu'il y a dedans.



Conseil : soyez attentif à vos téléchargement

Rendez-vous sur le site Offurl pour trouver et télécharger les logiciels directement sur leur site officiel.



4) Les Rançongiciel

Les rançongiciel sont des logiciels malveillants qui bloque l'accès à l'ordinateur et qui extorquent les victimes en échange de promesse



Conseil :

Pour résoudre ce problème, il est recommandé de forcer l'ordinateur à s'éteindre en appuyant pendant une dizaine de secondes sur le bouton d'allumage.

5) Le Quishing

Cette technique d'arnaque de plus en plus répondue consiste à dérober vos coordonnées bancaires par des QR Code falsifiés. Les escrocs impriment ces faux QR Codes renvoyant à des sites frauduleux et les disséminent un peu partout dans les rues, par mails ou sms.

Comment éviter les pièges ?

1) Tout d'abord, avant de scanner un QR Code avec l'aide d'un téléphone, il faut ouvrir l'oeil ou demander des renseignements directement aux commerçants concernés.

2) Si un QR Code est mal imprimé, avec des bords irréguliers, il est plutôt considéré comme suspect, de même si des informations personnelles sont à renseigner.

3) Aussi, il faut s'assurer aucun autre QR n'a été collé par-dessus celui d'origine. C'est l'arnaque la plus répandue qui sévit principalement dans les restaurants où les cartes ont laissé place à des menus numérisés.

4) Enfin, il est fortement déconseillé de scanner un QR Code envoyé par mail car car ils peuvent souvent contenir un lien frauduleux. Il est impératif de toujours vérifier l'URL du site vers lequel il renvoie. Ces arnaques ne sont pas filtrées par les spams.



6) Les faux acheteurs, faux vendeurs



C'est une personne qui va être sur les sites de ventes en ligne (par exemple Ebay ou le Bon coin).
Si je vends un objet , il veut me l'acheter, parfois même plus cher.
Mais il a un problème. Soit il a perdu sa carte, soit il est à l'étranger et le seul moyen pour me payer est de passer par un service en ligne. Il faut que je paye pour ouvrir ce service.

Parfois, c'est la personne qui propose de me vendre un objet à un prix super intéressant. Et une fois payé (souvent avec une application), je ne reçois jamais l'objet.
Par exemple, Hélène, la maman de Loic, a voulu louer une maison de vacances sur un site de vente et de location. Elle a payé avec une application la location d'une jolie maison dans le sud de la France.
Mais en arrivant en vacances, la maison louée n'existait pas. C'était une fausse annonce.



7) Un deepfake

Un deepfake est un enregistrement vidéo ou audio réalisé ou modifié grâce à l'intelligence artificielle. Ce terme fait référence non seulement au contenu ainsi créé, mais aussi aux technologies utilisées.
Le mot deepfake est une abréviation de "Deep Learning" et "Fake", qui peut être traduit par "fausse profondeur". En fait, il fait référence à des contenus faux qui sont rendus profondément crédibles par l'intelligence artificielle.

