



Introduction à la cybersécurité et les dangers d'Internet

Tristan POMMERY

Introduction

Pourquoi la sécurité en ligne est-elle importante?

01

Les bonnes pratiques

Quelles sont les bonnes pratiques de sécurité?

04

Les Cyberattaques et dangers d'internet

Qu'est-ce que c'est et quels sont les types les plus courants?

02

Outils

Quels sont les outils gratuits pour se protéger ?

05

Reconnaître les menaces

Comment identifier et réagir à une cyberattaque ?

03

Conclusion

06

01

Introduction



Pourquoi est-ce important?

- De plus en plus d'attaques ont lieu de nos jours
- Les données personnelles sont très prisées
- Les cyberattaques peuvent avoir des conséquences graves
- Vol d'identité, le vol de données personnelles, la fraude en ligne, etc.
- Tout le monde est concerné



02

Les

Cyberattaques

et dangers

d'internet



La cybersécurité, qu'est-ce que c'est?

- **Définition : La cybersécurité est la pratique qui consiste à protéger les systèmes critiques et les informations sensibles contre les attaques numériques.**
- Cyber- : Élément servant à former des composés en rapport avec le multimédia, Internet, le web
- Sécurité : Situation dans laquelle quelqu'un, quelque chose n'est exposé à aucun danger, à aucun risque

Comment opère un pirate informatique?

Définition: Un Hacker est une personne ayant des connaissances en informatiques qui les utilise pour mettre en défaut un système informatique et obtenir des informations.

Leur mode opératoire :

1. Identification de la cible / victime
2. Armement (utilisation de logiciels)
3. Livraison (type d'attaque)
4. Installation
5. Contrôle
6. Déplacements
7. Attaque réussie et effaçage des traces



Non malheureusement ce n'est pas une représentation de la réalité

Quelles sont les différents types de cyberattaques?



Virus informatique



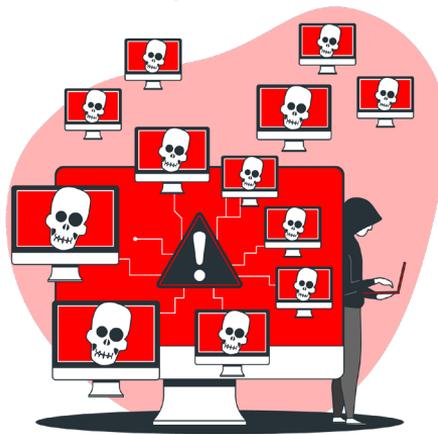
Cassage de mot de passe



Hameçonnage



Rançongiciel



Déni de service



“Homme au milieu”

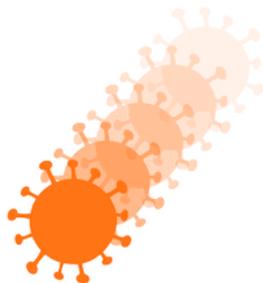
Premier danger : les virus

Définition : Un virus désigne, dans l'univers informatique, un programme malveillant dont l'objectif principal est de perturber le bon fonctionnement d'un appareil, la plupart du temps un ordinateur.

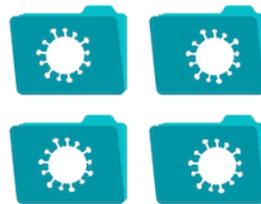
La définition d'un virus en quelques points clés :



programme
informatique



généralement
auto-répliquant



contamine
des fichiers



se transmet à
d'autres appareils

Deuxième danger : le hameçonnage et l'arnaque en ligne

Définition : Technique de fraude sur Internet visant à obtenir des renseignements confidentiels (mot de passe, informations bancaires...) afin d'usurper l'identité de la victime.

AMELI -Remboursement



Votre Assurance Maladie (ez895qs+eds4596s@imp.outlook.co.il)



De : **Votre Assurance Maladie** (ez895qs+eds4596s@imp.outlook.co.il) Microsoft SmartScreen a classé ce message comme indésirable.



Cher(e) client(e)

Après les derniers calculs de votre assurance maladie, nous avons déterminé que vous êtes admissible à recevoir un remboursement d'un montant de 116.00 euro.

Nous vous invitons à consulter les démarches à suivre en [Cliquant-ici](#)

Cordialement,

Ameli.fr - assurance maladie ameli 2016 France

Votre compte est Suspendu !!

Services Clients Health (ez895qs+eds4596s@imp.outlook.co.il)

To: you Details

⚠ Votre compte est suspendu.

Vos informations de paiement doivent être mises à jour

Bonjour,

Nous rencontrons des difficultés avec vos informations de facturation. Nous allons réessayer, mais il est possible que vous deviez mettre à jour vos détails de paiement.

[METTRE LE COMPTE A JOUR](#)

Besoin d'aide ? N'hésitez pas à consulter le [Centre d'aide](#) ou à [nous contacter](#).

L'équipe Health

Troisième danger : le cassage de mots de passe

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2022

| Number of Characters | Numbers Only | Lowercase Letters | Upper and Lowercase Letters | Numbers, Upper and Lowercase Letters | Numbers, Upper and Lowercase Letters, Symbols |
|----------------------|--------------|-------------------|-----------------------------|--------------------------------------|---|
| 4 | Instantly | Instantly | Instantly | Instantly | Instantly |
| 5 | Instantly | Instantly | Instantly | Instantly | Instantly |
| 6 | Instantly | Instantly | Instantly | Instantly | Instantly |
| 7 | Instantly | Instantly | 2 secs | 7 secs | 31 secs |
| 8 | Instantly | Instantly | 2 mins | 7 mins | 39 mins |
| 9 | Instantly | 10 secs | 1 hour | 7 hours | 2 days |
| 10 | Instantly | 4 mins | 3 days | 3 weeks | 5 months |
| 11 | Instantly | 2 hours | 5 months | 3 years | 34 years |
| 12 | 2 secs | 2 days | 24 years | 200 years | 3k years |
| 13 | 19 secs | 2 months | 1k years | 12k years | 202k years |
| 14 | 3 mins | 4 years | 64k years | 750k years | 16m years |
| 15 | 32 mins | 100 years | 3m years | 46m years | 1bn years |
| 16 | 5 hours | 3k years | 173m years | 3bn years | 92bn years |
| 17 | 2 days | 69k years | 9bn years | 179bn years | 7tn years |
| 18 | 3 weeks | 2m years | 467bn years | 11tn years | 438tn years |

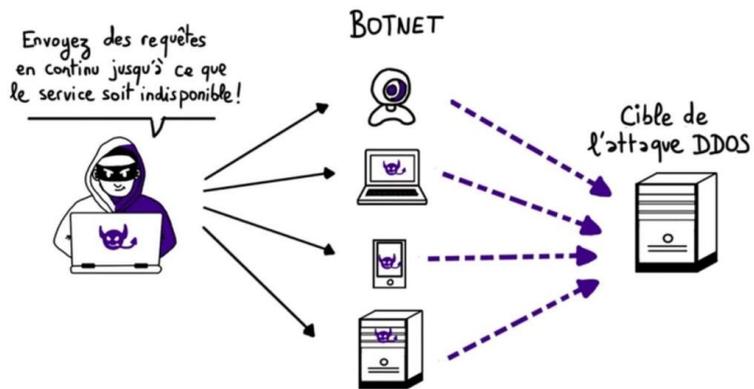


> Learn about our methodology at hivesystems.io/password

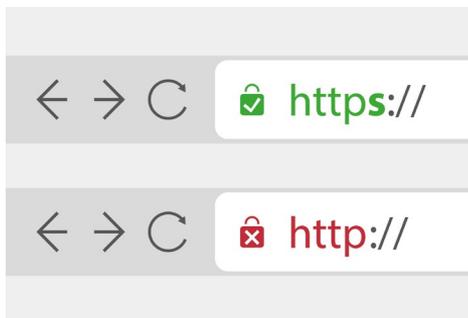
| CLASSEMENT | MOT_DE_PASSE | TEMPS_NÉCESSAIRE_POUR_LE_DÉCHIFFRER | DÉCOMPTE |
|------------|--------------|-------------------------------------|----------|
| 1 | 123456 | < 1 Seconde | 86 639 |
| 2 | 123456789 | < 1 Seconde | 41 915 |
| 3 | azerty | < 1 Seconde | 37 981 |
| 4 | 1234561 | 1 Seconde | 14 955 |
| 5 | azertyuiop | 1 Minute | 12 774 |
| 6 | avf2013 | 11 Secondes | 12 048 |
| 7 | loulou | < 1 Seconde | 11 997 |
| 8 | 000000 | < 1 Seconde | 11 295 |
| 9 | password | < 1 Seconde | 10 685 |
| 10 | doudou | < 1 Seconde | 10 412 |
| 11 | marseille | 1 Jour | 9 654 |

Quatrième danger : les cyberattaques de manière générale

Le déni de service



"L'homme au milieu"



Les rançongiciels



03

Reconnaitre les menaces



Comment reconnaître un mail de hameçonnage ?

- Une notification de la messagerie ou de l'antivirus
- Un email d'un service ou d'une société dont vous n'êtes pas client
- Un nom d'expéditeur inhabituel
- Une adresse d'expédition fantaisiste

De : E-service Clients BRED <BRED_secureID9593.noreply@zwina.com>

Envoyé : Thursday, October 29, 2020 9:51:42 AM

À : prenom.nom@courriel.fr

Objet : Au sujet de la sécurité de votre compte! #Re-664366

Comment reconnaître un mail de hameçonnage ?

Message du 20/10/21 02:10

De : "Group Service" <pimkies@dfyoxc.owler.com>

A :

Copie à :

Objet : Assurance Maladie | Ameli.fr

[Version en HTML](#) | [Se connecter](#)



Bonjour

Votre caisse d'assurance maladie vous informe que vos remboursements de frais à recevoir

Nous vous demandons de mettre à jour vos données pour que votre remboursement soit effectué dans les plus délais.

Montant: 249.98 Euro

Référence: Ameli-A8005W

<https://www.assure.ameli.fr>

Nous vous remercions et nous vous prions agréer nos salutations distinguées.

Votre caisse d'assurance maladie Ameli

Comment reconnaître un hameçonnage ?

- Un objet d'email trop alléchant ou alarmiste

De : 947588321 [mailto:947588321] De la part de sav.orange.fr - actu
Envoyé : mardi 12 octobre 2021 22:31
A : [redacted]
Objet : Dernier jour 🚨 Echangez vos points de fidélité avant l'échéance des gains le 15/10/2021



Chers clients, chères clientes,

En tant que client **Orange** vous êtes automatiquement enregistré dans le programme de **fidélité**.

Nous vous informons que depuis votre souscription chez **Orange** le total de vos points cumulés s'élève à **61 135** expirant le **15/10/2021**.

Grâce à ces derniers, vous recevrez un **mobile** pour vous remercier de votre fidélité.

L'expédition aura lieu après la confirmation de votre adresse ainsi que le paiement du service de livraison .

Echangez vos points de fidélité en vous référant au catalogue produits.

*Aucun abonnement ne sera souscrit sans votre accord préalable.

Cordialement,

En Savoir Plus

[Twitter](#)[Instagram](#)[LinkedIn](#)

Comment reconnaître un hameçonnage ?

- Une apparence suspecte

envoyé : 18 octobre 2021 à 18:16
de : Sylviane <ferencziimre@t-online.hu>
à : f.d.j@capital.fr
objet : Informations



Pour résumer : Exemples de mails qui doivent vous alerter

- Demande de mise à jour ou de confirmation de données personnelles – identifiants, mots de passe, coordonnées bancaires... – par un prétendu organisme public ou commercial de confiance, sous peine de sanction.
- Défaut de paiement ou problème de facturation : un faux mail vous informe qu'un bien ne peut être expédié en raison d'un problème de facturation ou que vous devez régler un impayé.
- Demande d'informations inattendue pour un remboursement, une annulation de commande, une livraison, etc.
- Demande d'informations contre l'envoi d'un cadeau ou pour participer à un jeu-concours avec un gain attrayant, ou encore pour récupérer le gain d'une loterie.
- Demande de règlement pour éviter la fermeture d'un accès, la perte d'un nom de domaine ou une prétendue mise en conformité RGPD.
- Appel aux dons frauduleux.
- Appel à l'aide : le cybercriminel se fait passer pour un proche, expliquant qu'il se trouve dans une situation désastreuse qui requiert votre aide financière.
- Les chaînes d'emails type porte-bonheur, pyramide financière, appel à solidarité ou alerte virale, peuvent dissimuler une tentative de phishing.

• Pour résumer : Les identités susceptibles d'être empruntées

- Les administrations comme le Trésor public (les impôts), la Sécurité sociale (ameli), la Caisse d'assistance familiale (Caf), etc.
- Les banques
- Les fournisseurs d'énergie
- Les opérateurs télécoms
- Les réseaux sociaux
- Les services de messagerie et stockage en ligne (Cloud)
- Les sites de commerce en ligne
- Les sociétés de livraison
- Les systèmes de paiement en ligne

Comment reconnaître un virus ?

- Ralentissement de l'appareil
- Blocage
- Fenêtres qui s'affichent sans raison
- Modification de logiciels ou programmes, comme votre navigateur Internet, logiciel de traitement de texte, etc.
- Boîte de dialogue ou messages inconnus
- Sites Internet qui apparaissent automatiquement
- Etc.



Comment reconnaître un site frauduleux ?

- L'URL et si HTTPS
- Qualité du site
- Conditions générales de vente
- Les mentions légales
- Tarifs proposés
- L'orthographe
- Informations aguicheuses ou demandant une intervention urgente
- Etc.

Free Enquête

ticketsurveys.com/7df90e37efab08dfc157dec540aca56ab

★ Récompenses Exclusives ★

free
Client Enquête
Décembre 12, 2019

Félicitations Cher Client **Free!**

Votre adresse [redacted] a été sélectionné pour recevoir GRATUITEMENT un **Samsung Galaxy S10** ou un **Apple iPhone X**.

Pour recevoir votre cadeau, il vous suffit de répondre à notre sondage anonyme. Mais dépêchez-vous! Il ne reste qu'un nombre limité de cadeaux pour aujourd'hui!

Disponible pour les **4:38 minutes** à venir

Commencer

 **Deniel Couture**
Je viens d'appeler le transporteur. Il m'a dit qu'il m'apporterait le colis aujourd'hui. Mais quand même, j'attends d'avoir l'iPhone entre les mains pour y croire vraiment :)

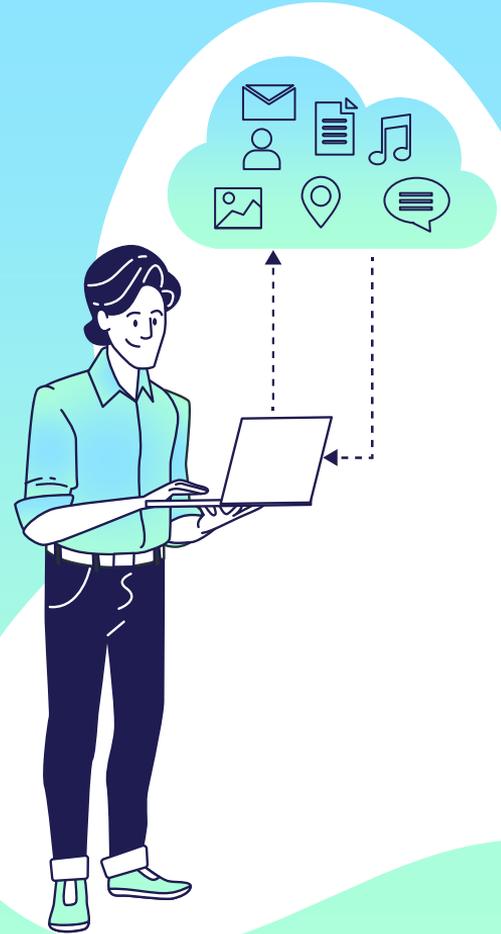
Décembre 12, 2019 at 12:01 am

Que faire en cas de cyberattaque?

- Déconnectez vous d'internet
- Faites un balayage avec votre logiciel antivirus
- Restaurez votre ordinateur si besoin
- Faites appel a un expert si besoin
- Changez vos mots de passe
- Déposez plainte → Conservez des images / preuves
- Listez tous les préjudices subis

04

Les bonnes pratiques



Bonne pratique n°1 : Utiliser des mots de passe complexes

Liste "d'exigences":

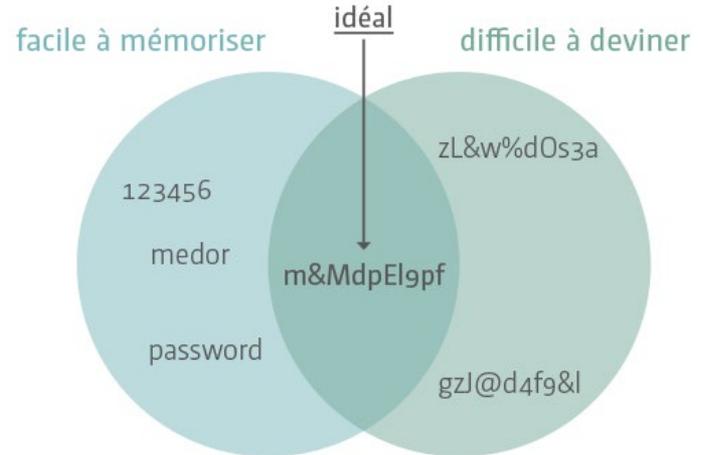
- Longueur d'au moins 8 caractères
- Présence de caractères alphanumériques
- Présence de caractères spéciaux
- Présence de majuscules
- Ne pas inclure d'informations personnelles
- Ne pas utiliser une suite de caractères

Mais SURTOUT :

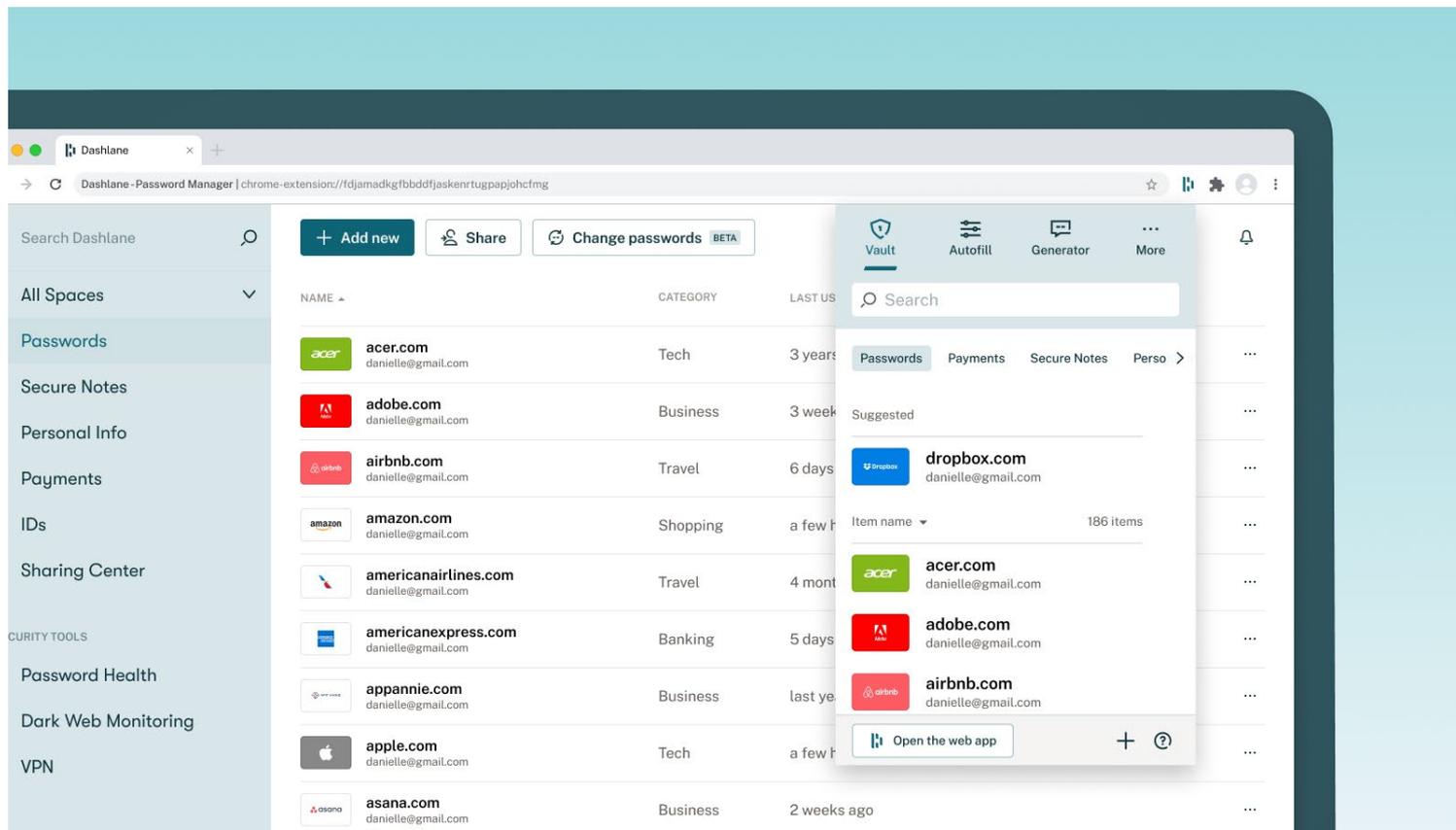
- **Ne pas réutiliser ses mots de passe**

Mangez au moins 5 fruits et légumes par jour !

Mam5felpj!



Bonne pratique n°2 : Utiliser un gestionnaire de mots de passe



- Bonne pratique n°3 : Ne pas partager ses infos personnelles



Bonne pratique n°4 : Ne pas cliquer sur des liens suspects

✕ Ordre d'arrestation



Votre solde CPF est arrivé à échéance. Veuillez remplir le formulaire ci-dessous sous 24h, pour convertir vos droits acquis en 2021
<https://cutt.ly/XGCf2FL>

NETFLIX: Expiration de votre abonnement, à mettre à jour impérativement avant le 01/11/2022. Rendez-vous vite sur:
<https://abonnement-espace-fr.com>

Crit'Air :
Nos agents ont constaté que votre véhicule n'était pas muni de la vignette réglementaire Crit'Air 2022 veuillez la récupérer sous peine de contravention dans les prochaines 48 h sur le lien ci-joint :

<https://critair-france.com/>

Ministère du Travail et de l'Insertion : URGENT: réclamez vos droits de formation CPF avant l'expiration de vos heures le 25 juillet 2022: <https://gouv-espace.eu>

Tous les 90 jours calendaires, une authentification forte sera nécessaire. Pour continuer à rester connecté à votre Espace Client sera bloqué !

Pour continuer à rester connecté à <http://messagerieclient.fr> Cliquez ou appuyez pour suivre le lien. [Je reconferme mon numéro de mobile](#)

Votre numéro de mobile, c'est la première condition indispensable pour rester c

Si possible se connecter sur le site officiel plutôt que d'utiliser un raccourci reçu par mail/messagerie

Bonne pratique n°5 : Utiliser un antivirus et mettre à jour



The screenshot shows the Windows Settings application with the 'Windows Update' section selected. The left sidebar lists various settings categories, with 'Windows Update' highlighted. The main content area displays the 'Windows Update' settings, including a search bar, a list of update options, and the current update status.

Paramètres

Accueil

Rechercher un paramètre

Mise à jour et sécurité

- Windows Update
- Optimisation de la distribution
- Sécurité Windows
- Sauvegarde
- Résolution des problèmes
- Récupération

Windows Update

Mises à jour disponibles
Dernière vérification : aujourd'hui, 13:28

2019-10 Mise à jour cumulative pour .NET Framework 3.5 pour et 4.8 pour Windows 10 Version 1909 pour les systèmes x64 (KB4522742)
Statut : Téléchargement - 0%

- Suspendre les mises à jour pendant 7 jours
Consultez les options avancées pour modifier la période de suspension
- Modifier les heures d'activité
Actuellement 08:00 à 17:00
- Afficher l'historique des mises à jour
Voir les mises à jour installées sur votre appareil
- Options avancées
Paramètres et contrôles de mise à jour supplémentaires

Bonne pratique n°6 : Eviter les réseaux Wi-Fi publics



Bonne pratique n°7 : Les paiements en ligne

Paiements en ligne

Ce qu'il faut retenir



Éviter les réseaux
Wi-Fi publics



Ne pas donner ses
données bancaires
par téléphone ou SMS



Vérifier la mention
HTTPS



Activer la double
authentification



Prendre garde aux sites
frauduleux imitant
les sites légitimes



Ne pas sauvegarder
de données bancaires
dans le navigateur

Bonne pratique n°8 : Bloqueurs de publicités



05

Les Outils

Quels sont les outils pour se protéger ?



Quelques solutions

- **Antivirus gratuits** : Avast, AVG, Bitdefender, Malwarebytes, Comodo, MS Defender
- **Gestionnaires de mots de passe** : keepass, bitwarden, dashlane
- **Bloqueurs de publicités et de traçage** : uBlock Origin ou Privacy Badger ou adblock
- **Utilisation de VPN** : ProtonVPN et Windscribe.
- **Utilisation de logiciels de pare-feu** : Comodo
- **Utilisation de la double authentification** : Google authenticator par exemple
- **Utilisation de la navigation privée** : la navigation privée n'offre pas une protection complète de votre vie privée en ligne, mais elle peut aider à prévenir le traçage et les attaques de phishing.
- **Sensibilisation à la sécurité** : Les utilisateurs doivent être conscients des risques en ligne et savoir comment éviter les pièges (ANSSI par exemple)
- **Sauvegarde régulière des données** : Google Drive, Dropbox, clés USB.
- **Outils de vérification de la sécurité des sites Web** : PhishTank, Google Safe Browsing
- **Outils de gestion des mises à jour** : Patch My PC

Quelques liens utiles

<https://www.cybermalveillance.gouv.fr/cybermenaces> – Comprendre les menaces et agir

<https://www.cybermalveillance.gouv.fr/bonnes-pratiques> – Adopter les bonnes pratiques

<https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/liste-des-ressources-mises-a-disposition> – Liste des ressources

<https://www.cybermalveillance.gouv.fr/diagnostic/accueil#signaler> – Diagnostic en ligne

<https://www.cybermalveillance.gouv.fr/diagnostic/accueil#plainte> – Dépôt de plainte

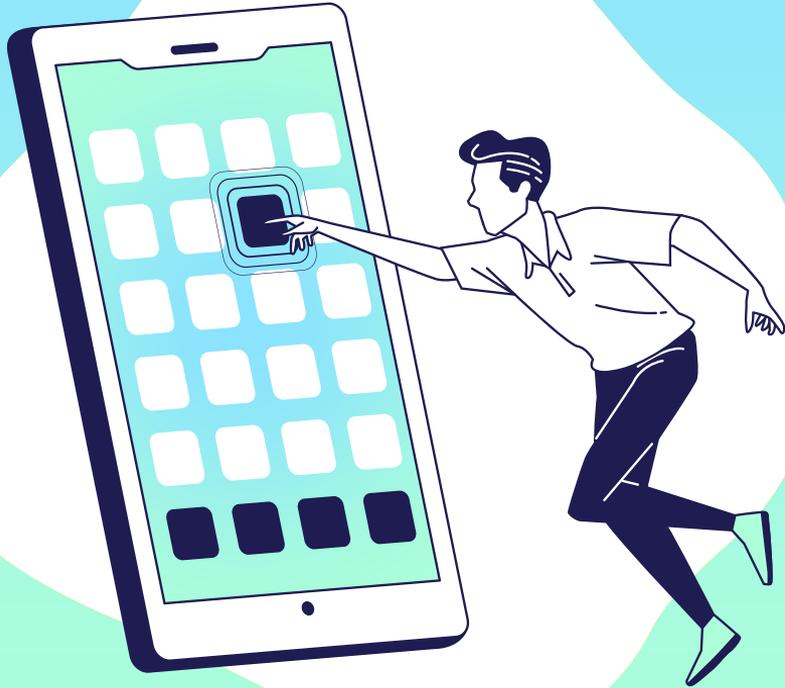
https://www.cybermalveillance.gouv.fr/medias/2020/10/FicheA4_premiers-gestes-en-cas-cyberattaque.pdf – Premiers gestes en cas de cyberattaque

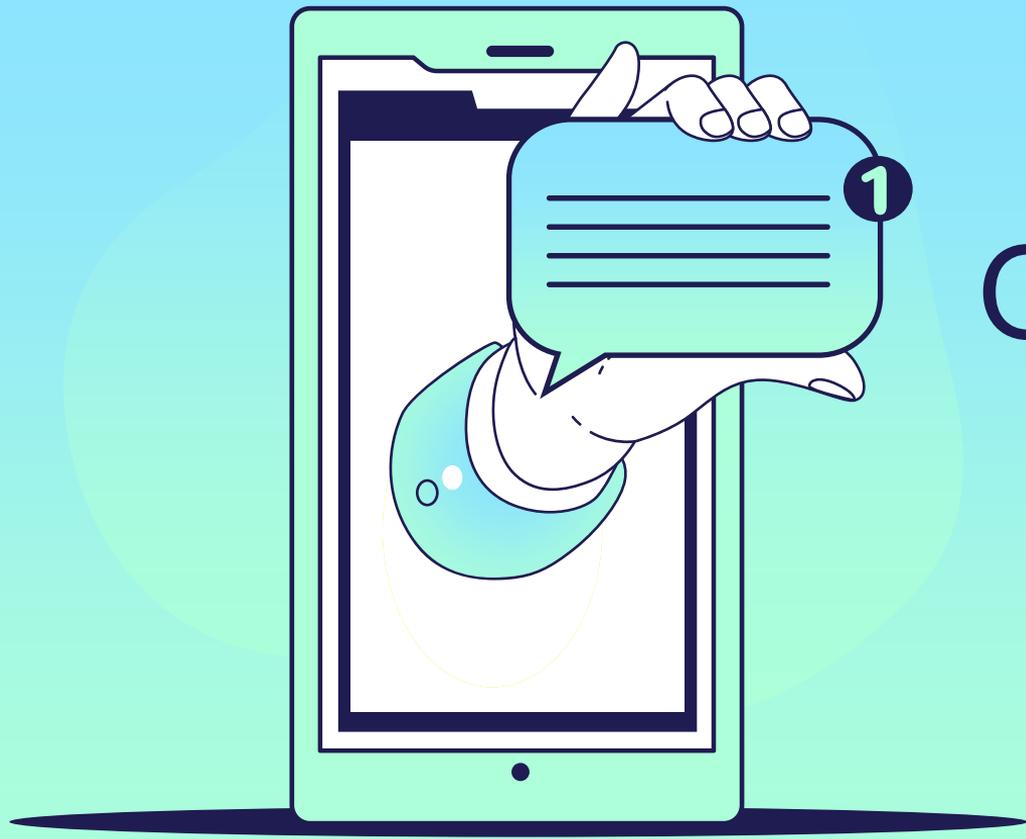
<https://www.cybermalveillance.gouv.fr/> – Tous les contenus

06

Conclusion

Comment rester vigilant
en ligne?





07

Questions & Réponses