



Cybersecurité 2025 : Comment se Protéger ?

Céline Blandin -Mars 2025

CyberSécurité 2025 : Comment se Protéger ?

1. La cybersécurité c'est quoi?

- Définition
- Evolution des menaces avec les nouvelles technologies
- Impact du numérique sur la société

1. Les différents types d'attaque, exemples concrets

- Cybercriminalité
 - Atteintes à l'image et désinformation (fake news, manipulation)
 - Espionnage et collectes de données personnelles
 - Sabotages
 - Notion de cyberguerre

1. Prévention et réflexes à adopter

- Sécuriser ses appareils et applications
- Gérer son identité numérique et protéger ses comptes
- Les bons reflexes sur les réseaux sociaux
- Protéger ses données personnelles et sa vie privée
- Les attaques personnelles les plus courantes, que faire en cas d'attaque?
- Les intervenants gouvernementaux

Cybersécurité 2025 : Comment se Protéger ?

1. La cybersécurité c'est quoi?
 - Définition
 - Evolution des menaces avec les nouvelles technologies
 - Impact du numérique sur la société
2. Les différents types d'attaque, exemples concrets
3. Prévention et réflexes à adopter

La cybersécurité c'est quoi?

- La cybersécurité désigne l'ensemble des pratiques, technologies et lois visant à protéger **les systèmes informatiques, les données et les utilisateurs contre les cyberattaques.**
- Avec la numérisation croissante de nos vies, la cybersécurité est devenue un **enjeu majeur pour les individus, les entreprises et les États.**

THE INTERNET IN 2023 EVERY MINUTE



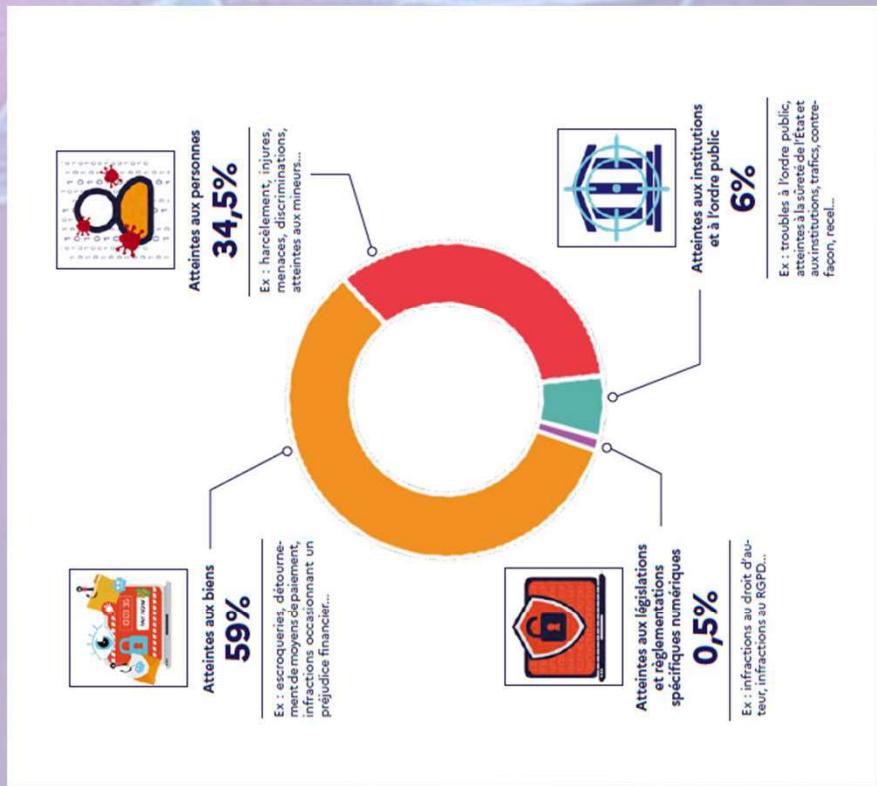
Created by: eDiscovery Today & LTMG

Cybersecurité 2025 - Celine Blandin - Mars 2025

De nombreuses cyberattaques, quelques chiffres :



Source: <https://www.ambient-it.net/>

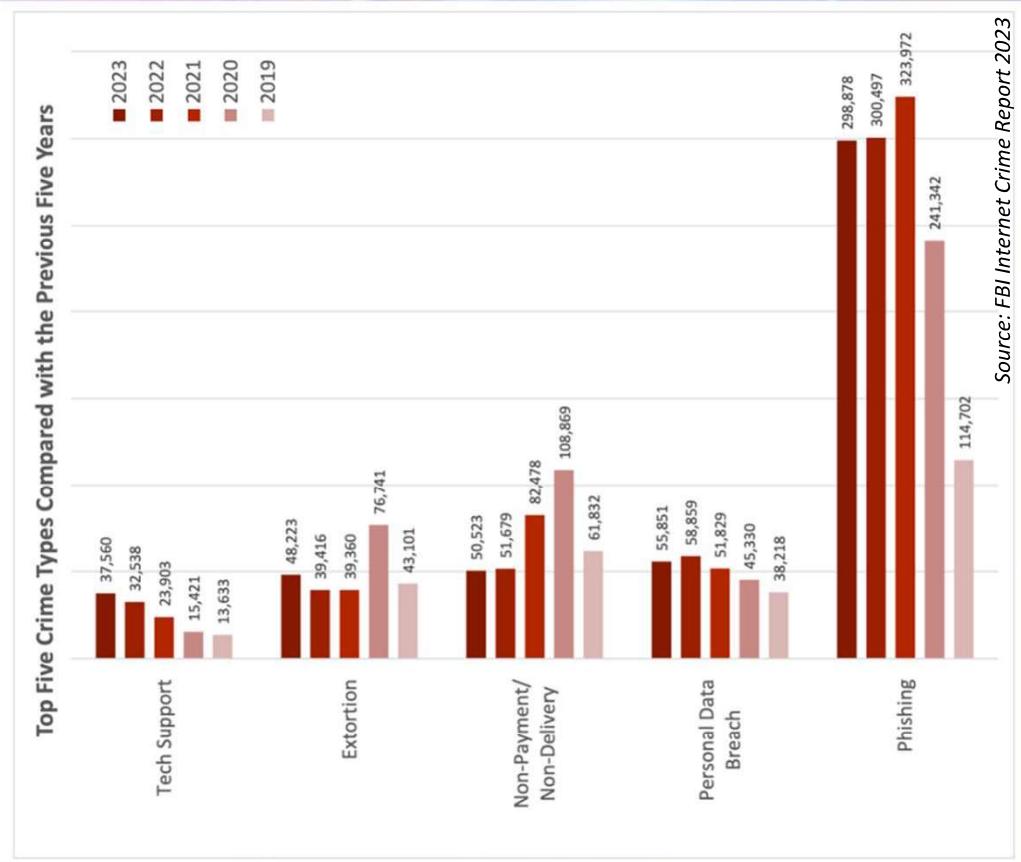


Source: <https://www.interieur.gouv.fr/>

Cybersecurité 2025 - Celine Blandin - Mars 2025

Les types cyberattaques, quelques chiffres :

TOP FIVE CRIME TYPE COMPARISON⁴



Source: FBI Internet Crime Report 2023

Cybersécurité 2025 : Comment se Protéger ?

1. La cybersécurité c'est quoi?
 - Définition
 - Evolution des menaces avec les nouvelles technologies
 - Impact du numérique sur la société
2. Les différents types d'attaque, exemples concrets
3. Prévention et réflexes à adopter

Impact des nouvelles technologies:

➤ **Essor de l'Intelligence Artificielle**
Automatisation du phishing, deepfakes avec usurpation d'identité, attaques de plus en plus sophistiquées sur les entreprises...



➤ **Les smartphones, indispensables à nos vies actuelles**
Collecte d'énormes quantités de données personnelles, fausses applications, applications vulnérables, WIFI public...

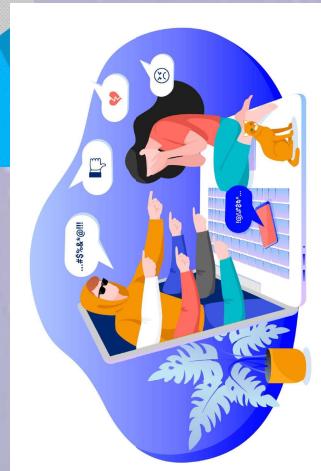
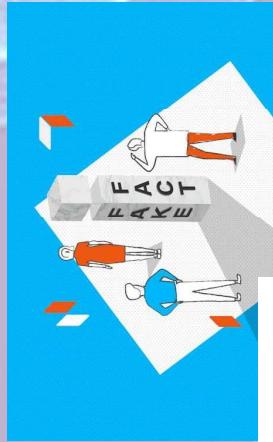


Cybersécurité 2025 : Comment se Protéger ?

1. La cybersécurité c'est quoi?
 - Définition
 - Evolution des menaces avec les nouvelles technologies
 - Impact du numérique sur la société
2. Les différents types d'attaque, exemples concrets
3. Prévention et réflexes à adopter

Impact sur la société → Propagation à une vitesse incontrôlable:

- de la désinformation (fausse information diffusée intentionnellement),
- des fake news,
- du cyberharcèlement,
- des attaques sur entreprises privées et publiques (quelques soit leurs tailles),
- Intensité des cyberguerres



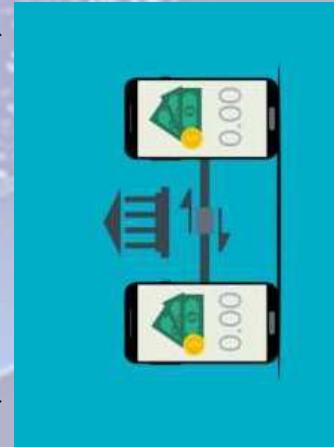
Cybersecurité 2025 : Comment se Protéger ?

1. La cybersécurité c'est quoi?
2. Les différents types d'attaque, exemples concrets
 - Cybercriminalité
 - Atteintes à l'image et désinformation (fake news, manipulation)
 - Espionnage et collectes de données personnelles
 - Sabotages
 - Notion de cyberguerre
3. Prévention et réflexes à adopter

1. Cybercriminalité:

La cybercriminalité regroupe les activités illégales menées sur internet, souvent à des fins financières.

- Phishing
- Rançongiciel/Ransomware
- Arnaque au faux support technique
- Piratage de compte en ligne (vols d'identifiants)
- Faux ordre de virements



Cybersecurité 2025 : Comment se Protéger ?

1. La cybersécurité c'est quoi?
2. Les différents types d'attaque, exemples concrets
 - Cybercriminalité
 - Atteintes à l'image et désinformation (fake news, manipulation)
 - Espionnage et collectes de données personnelles
 - Sabotages
 - Notion de cyberguerre
3. Prévention et réflexes à adopter

2. Atteinte à l'image / Déstabilisation :

Cyberattaques ne visent pas toujours des gains financiers. elles peuvent aussi chercher à nuire à la réputation d'une personne, d'une entreprise ou d'un pays...

- Défacement
- Désinformation
- Fake news
- Cyberharcèlement
- Deepfakes (vidéos modifiées par IA)



CyberSécurité 2025 : Comment se Protéger ?

1. La cybersécurité c'est quoi?
2. Les différents types d'attaque, exemples concrets
 - Cybercriminalité
 - Atteintes à l'image et désinformation (fake news, manipulation)
 - Espionnage et collectes de données personnelles
 - Sabotages
 - Notion de cyberguerre
3. Prévention et réflexes à adopter

3. Espionnage et collectes de données personnelles:

L'espionnage numérique concerne le vol d'informations sensibles à des fins économiques, politiques ou militaires.

- Spearfishing (Phishing ciblé avec usurpation)
- Cheval de Troie (Trojan Horse, malware caché dans un programme)
- Violation de données personnelles:
 - Collecte des PII Personnally Identifiable Information (Facebook)
 - Tracking excessif d'application mobiles (TikTok...)
 - Fuite de base de données
 - Surveillance illégale (Clearview AI, NSA PRISM-Snowden...)



Cybersecurité 2025 : Comment se Protéger ?

1. La cybersécurité c'est quoi?
2. Les différents types d'attaque, exemples concrets
 - Cybercriminalité
 - Atteintes à l'image et désinformation (fake news, manipulation)
 - Espionnage et collectes de données personnelles
 - **Sabotages**
 - Notion de cyberguerre
3. Prévention et réflexes à adopter

4. Sabotage:

Le sabotage informatique est le fait de rendre inopérant tout ou partie d'un système d'information d'une organisation via une attaque informatique.

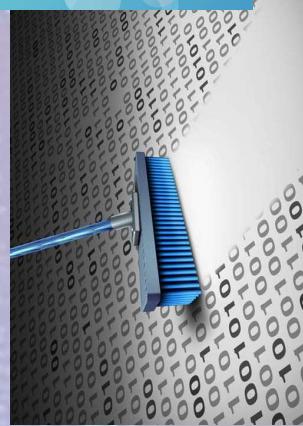
➤ Déni de Service, DDoS (Attaque contre l'Estonie-2007...)



➤ Worm, ver informatique (Code Red-2001, Blaster-2003...)



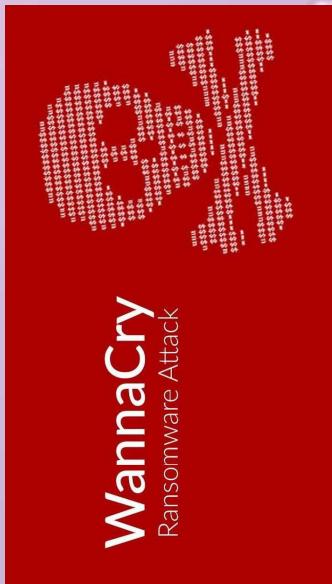
➤ Virus (Stuxnet-2010, ILOVEYOU-2000, Mydoom-2004...)



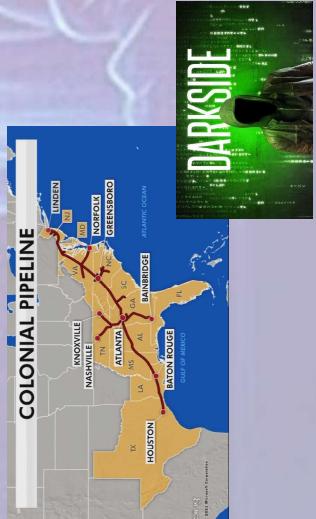
➤ Wiper (NotPetya-2017, HermeticWiper-2022...)

Quelques attaques connues :

- Ransomware Wannacry – 300 000 ordinateurs dans 150 pays –
Système santé britannique, Renault, opérateur espagnol
Telefonica – 2017



- NoName057(16) – Cyberattaques contre les institutions françaises en réaction du soutien de la France à l'Ukraine – mise en évidence de la vulnérabilité des sites web institutionnels - 2023
- Groupe DarkSide - Colonial Pipeline USA – 4,4 millions de dollars de rançon, pays bloqué – 2021



Cybersecurité 2025 : Comment se Protéger ?

1. La cybersécurité c'est quoi?
2. Les différents types d'attaque, exemples concrets
 - Cybercriminalité
 - Atteintes à l'image et désinformation (fake news, manipulation)
 - Espionnage et collectes de données personnelles
 - Sabotages
 - Notion de cyberguerre
3. Prévention et réflexes à adopter

Cyberguerre, c'est quoi?

Nous sommes déjà en cyberguerre “froide” depuis longtemps

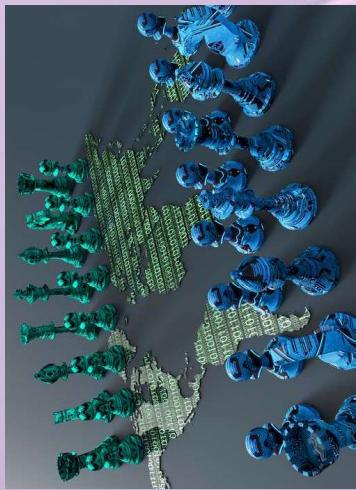
Attaques réelles, mais jamais complètement revendiquées :

- Stuxnet (Iran/US) - 2010,
- Shamoon(Saudi/Iran) – 2012 et 2017,
- NotPetya (Russie/Ukraine) - 2017,
- Hillary Clinton vs Trump election (Russie/US),
- ...
- Sunburst backdoor (Russie/US) - 2020,
- ShadowPad et PlugX (Chine/Europe) - 2024,
- Babar (France) -2009
- ...

Qu'est ce qui change si le conflit cyber est en support d'un conflit dans la réalité?

Le cas concret de l'Ukraine :

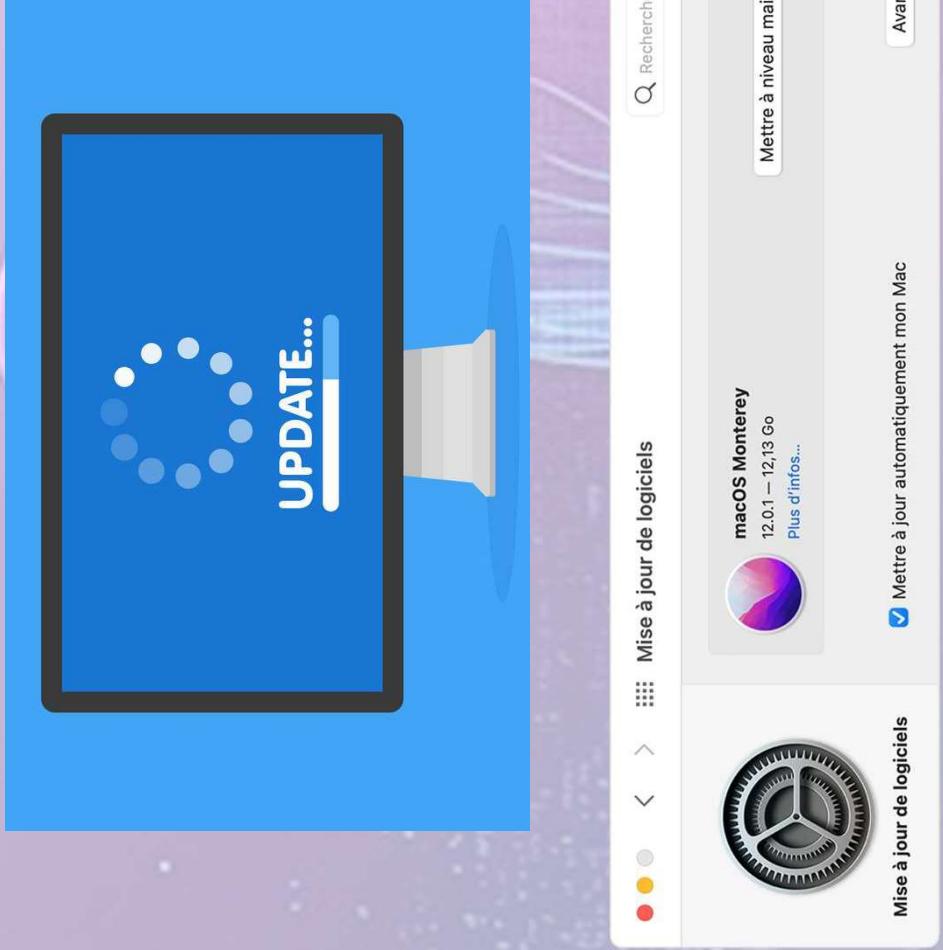
- 13/01/22 : malware/wiper *WhisperGate* découvert sur ordinateurs d'organisations gouvernementales, services de télécommunication...
- 14/01/22 : cyberattaques sur 70 sites web gouvernementaux / propagande de peur
- 15/02/22 : attaque DDos de grande ampleur sur les sites internet du Ministère de la Défense, l'armée et 2 importantes banques
- 23/02/22 : 3ème attaque DDos et malware/wiper *HermeticWiper* détecté dans multiples organisations ukrainiennes : finance, défense, aviation, IT...
- 24/02/22 : La Russie annonce leur opération militaire d'envergure sur toute l'Ukraine, 1 heure après le réseau satellite américain KA-SAT subit une cyberattaque.



Cybersecurité 2025 : Comment se Protéger ?

1. La cybersécurité c'est quoi?
2. Les différents types d'attaque, exemples concrets
3. Prévention et réflexes à adopter
 - Sécuriser ses appareils et applications
 - Gérer son identité numérique et protéger ses comptes
 - Les bons reflexes sur les réseaux sociaux
 - Protéger ses données personnelles et sa vie privée
 - Les attaques personnelles les plus courantes, que faire en cas d'attaque?
 - Les intervenants gouvernementaux

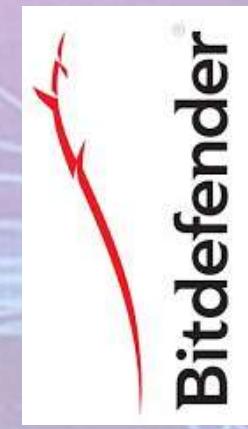
Les updates, c'est pénible, mais ça peut sauver!



This screenshot shows the Windows Update interface in the Windows Settings app:

- Left sidebar:** Includes links for "Paramètres", "Accueil", and a search bar.
- Middle section:** Shows sections for "Windows Update", "Windows Update", "Windows Defender", "Sauvegarde", and "Résoudre les problèmes".
- Right section:** Shows a "Paramètres de mise à jour" section with a note about automatic updates, and links for "Récupération", "Activation", "Localiser mon appareil", "Pour les développeurs", "Programme Windows Insider", "Modifier les heures d'activité", "Options de redémarrage", and "Options avancées".

Installer un antivirus



Cybersecurité 2025 - Celine Blandin - Mars 2025

CyberSécurité 2025 : Comment se Protéger ?

1. La cybersécurité c'est quoi?
2. Les différents types d'attaque, exemples concrets
3. **Prévention et réflexes à adopter**
 - Sécuriser ses appareils et applications
 - Gérer son identité numérique et protéger ses comptes
 - Les bons reflexes sur les réseaux sociaux
 - Protéger ses données personnelles et sa vie privée
 - Les attaques personnelles les plus courantes, que faire en cas d'attaque?
 - Les intervenants gouvernementaux

LES MOTS DE PASSE C'EST COMME LES SOUS-VÊTEMENTS



Ça se change
régulièrement

Ça ne se donne pas à un
inconnu

Ça ne se laisse pas
traîner au bureau



Face à la cybercriminalité, adoptez les bons réflexes !

C'est quoi un mot de passe fort?

12345

celineblandin@08112003

Motdep@sse

10 à 15 caractères, sans suite logique, avec Majuscule, minuscule, chiffre et caractères spéciaux

JhqlEr@lE52p1Bv2v+eMm!

J'ai hâte que les Enfants redévoient @ l'Ecole 5/7 de prendre un Bon verre de vin et écouter Ma musique !

Règles :

- 10 à 15 caractères, sans suite logique, avec Majuscule, minuscule, chiffre et caractères spéciaux
- Ne pas utiliser le même mot de passe partout
- Ne pas donner son mot de passe
- Toujours se déconnecter de sa session quand on a terminé
- Changer son mot de passe régulièrement, et au moindre doute d'avoir été hacké

Les coffres fort de mot de passe

The screenshot shows the KeePass application interface. At the top, there's a menu bar with File, Edit, View, Tools, Help, and a toolbar with various icons. The main window displays a database titled "masterDatabase". The database tree on the left shows categories: General, Windows, Network, Internet, eMail, and Homebanking. The main table lists two entries:

Title	User Name	Password	URL	Notes
Sample En...	User Name	*****	https://keep...	Notes
Sample En...	Michael321	*****	https://keep...	

At the bottom right, there are status messages: "1 of 2 selected", "Ready.", and "Notes". On the far right, there's a vertical sidebar with "Group: masterDatabase", "Title: Sample Entry, User Name: User Name, Password: *****", "URL: https://keepass.info/", "Creation Time: 27.12.2018 2.22.42", "Last Modification Time: 27.12.2018 2.22.42", and "Notes".

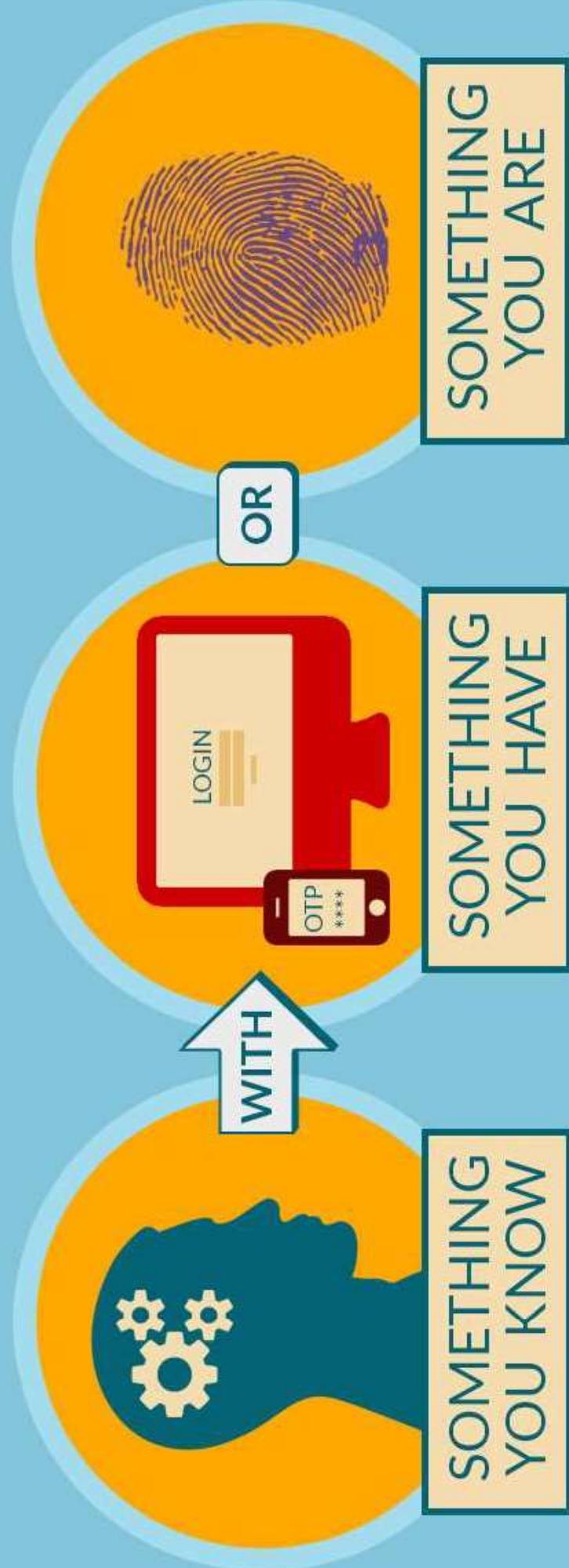


<https://keepass.fr/>

<https://keepass.info/download.html>

DOUBLE AUTHENTICATION

MFA Multi Factor of Authentication



Comment vérifier si nos données ont été hackées

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

email address

pwned?

Learn more at 1Password.com

Generate secure, unique passwords for every account
Why 1Password?

327

owned websites

5,620,024,112

owned accounts

83,975

pastes

91,563,791

paste accounts

<https://haveibeenpwned.com/>

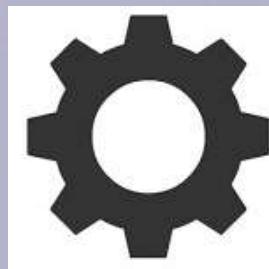
Cybersecurité 2025 - Celine Blandin - Mars 2025 <https://www.avast.com/hackcheck#pc>

Cybersecurité 2025 : Comment se Protéger ?

1. La cybersécurité c'est quoi?
2. Les différents types d'attaque, exemples concrets
3. **Prévention et réflexes à adopter**
 - Sécuriser ses appareils et applications
 - Gérer son identité numérique et protéger ses comptes
 - **Les bons reflexes sur les réseaux sociaux**
 - Protéger ses données personnelles et sa vie privée
 - Les attaques personnelles les plus courantes, que faire en cas d'attaque?
 - Les intervenants gouvernementaux

Les bons réflexes sur les réseaux sociaux

🔒 1. Protéger ses informations personnelles



paramètres de confidentialité

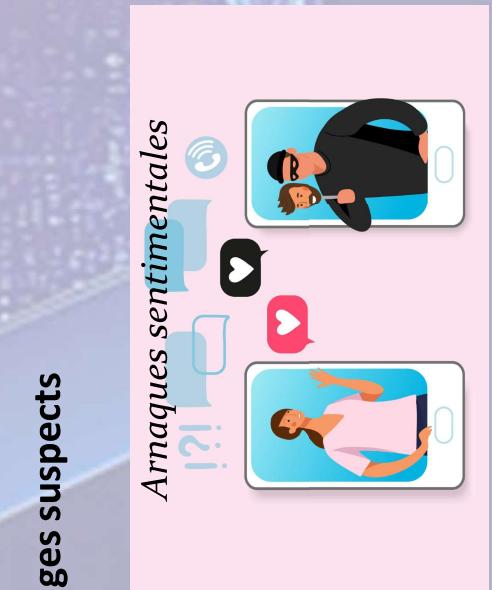


Ne pas partager données sensibles



Metadata, photos géolocalisées

😊 2. Se méfier des inconnus et des messages suspects



Faux profils

Les bons reflexes sur les réseaux sociaux

3. Réfléchir avant de publier



IF YOU POST IT ONLINE, IT STAYS ONLINE FOREVER
THINK BEFORE YOU POST OR COMMENT.

Attention, internet ne s'efface pas!

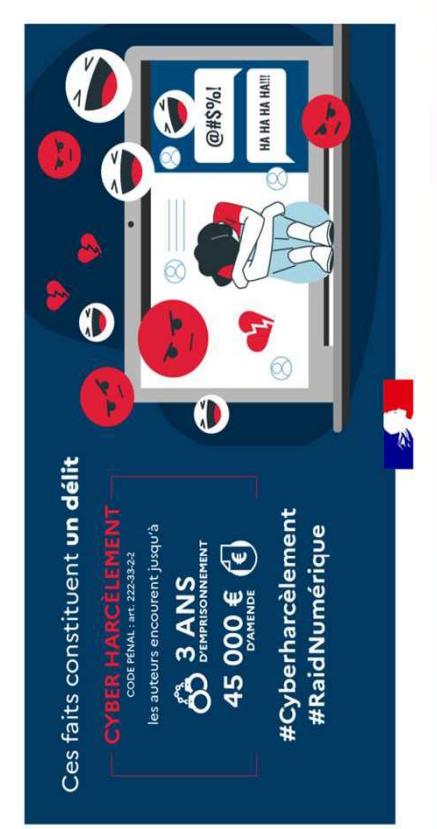


Vérifier ses sources

4. Sécuriser son compte

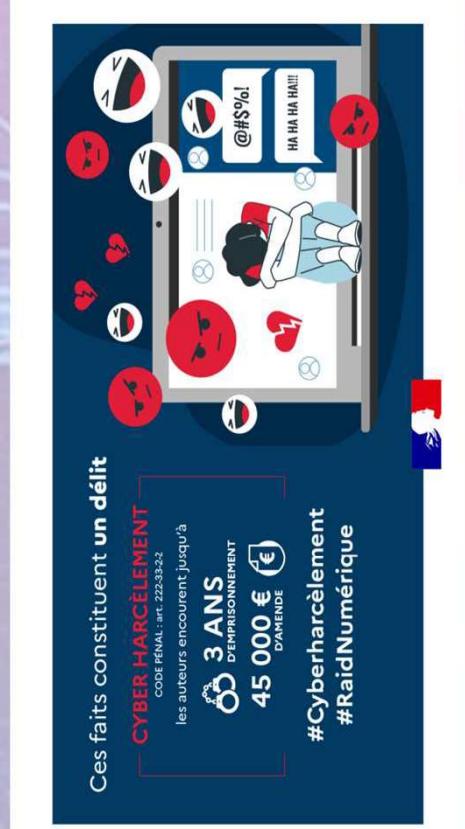


Permission des apps



Soyez responsable

5. Signaler et bloquer les comportements inappropriés



Cybersecurité 2025 : Comment se Protéger ?

1. La cybersécurité c'est quoi?
2. Les différents types d'attaque, exemples concrets
3. **Prévention et réflexes à adopter**
 - Sécuriser ses appareils et applications
 - Gérer son identité numérique et protéger ses comptes
 - Les bons reflexes sur les réseaux sociaux
 - **Protéger ses données personnelles et sa vie privée**
 - Les attaques personnelles les plus courantes, que faire en cas d'attaque?
 - Les intervenants gouvernementaux

Naviguer sur Internet en toute sécurité

- 🛡️ 1. Utiliser un navigateur à jour
- 🍪 2. Gérer les cookies intelligemment
- 🔒 3. Se déconnecter des comptes sensibles
- 🌐 4. Naviguer en mode sécurisé (HTTPS, ne pas cliquer sur n'importe quoi!)



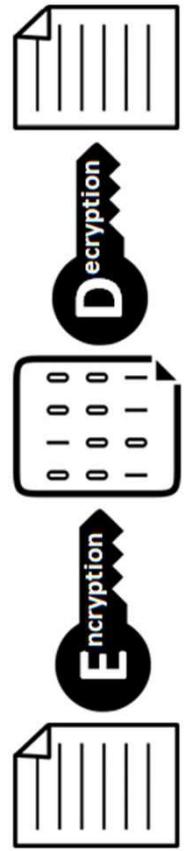
Mieux vaut prévenir que guérir : **BACKUP**

Avoir un backup physique ou sur le cloud, déconnecté de votre ordinateur, à mettre à jour au moins 1 fois par mois.



Mieux vaut prévenir que guérir : le **CHIFFREMENT**

Encryption & Decryption



Plain Text

Encrypted Text

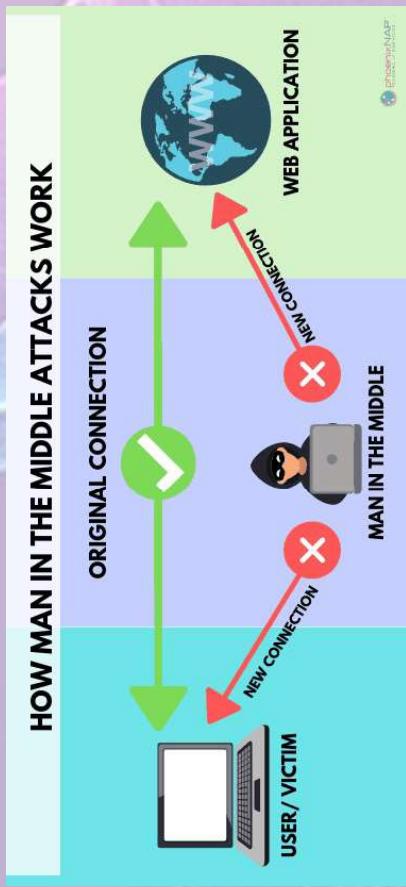
Plain Text

Cybersecurité 2025 - Celine Blandin - Mars 2025



Free WIFI = DANGER

Faux WIFI gratuit, l'attaque de l'homme du milieu



VPN : Virtual Private Network



Cybersecurité 2025 : Comment se Protéger ?

1. La cybersécurité c'est quoi?
2. Les différents types d'attaque, exemples concrets
3. **Prévention et réflexes à adopter**
 - Sécuriser ses appareils et applications
 - Gérer son identité numérique et protéger ses comptes
 - Les bons reflexes sur les réseaux sociaux
 - Protéger ses données personnelles et sa vie privée
 - **Les attaques personnelles les plus courantes, que faire en cas d'attaque?**
 - Les intervenants gouvernementaux

Attention au Phishing

INFO@IMPOTS.GOUV.FR <INFO@aut.autoextractor.co.uk>

mardi 7 novembre 2017 à 14:12
Afficher les détails

Une copie de ce message se trouve sur le serveur.

 MINISTÈRE DE L'ÉCONOMIE,
DES FINANCES ET DU NUMÉRIQUE

 MINISTÈRE DE L'ÉCONOMIE
ET DES FINANCES

impots.gouv.fr
Un site de la Direction générale des Finances publiques

Cher (e) Client (e)

Après les derniers calculs de l'exercice de votre activité, nous avons déterminé que vous êtes admissibles à recevoir un remboursement de 791,00 Euro. Veuillez nous soumettre si l vous plait la demande de remboursement pour nous permettre de la traiter dans un plus bref délai (**le délai de traitement est de 10 jours ouvrés**).

Pour accéder au formulaire de votre remboursement d'impôt cliquez [ici](#). Un remboursement peut être retardé pour diverses raisons. Exemple : la soumission de dossiers non valides ou inscriptions hors délai..

Conciliateur fiscal adjoint
Philippe BERGER
Cordialement

<https://www.virustotal.com/gui/home/upload>

- Examiner l'email (**adresse expéditeur**, caractère urgent, fautes, adresses cachées des liens, pièces jointes)
- Ne pas cliquer sur les liens, aller directement sur le site via votre navigateur
- Vérifier pièces jointes avant de les ouvrir



- Rester pragmatique, vous avez peu de chance que les impôts vous remboursent 791€, ou de gagner à une loterie que vous ne connaissez pas par mail...
- Rester en alerte, les emails frauduleux sont toujours de plus en plus réaliste, exemple : mail jeux pour Noël, 1 seul caractère de différence...

Attention au Phishing

SPAM EMAIL SPOT THE DIFFERENCE

there are 6 differences between the fake and real one, can you spot them?

SPAM EMAIL

SPOT THE DIFFERENCE

there are 6 differences between the fake and real one, can you spot them?

From: support@microsoft.co.uk
Sent: 16/01/2023 11:44
To: Bob Smith <Bob.Smith@company.com>
Subject: Urgent Action Needed!

From: support@microsoft.co.uk
Sent: 16/01/2023 11:44
To: Bob Smith <Bob.Smith@company.com>
Subject: Unusual Sign In Activity

o Outlook
Microsoft Account

Verify your account

We detected some unusual activity about a recent sign in for your Microsoft account bo*****@company.com, you might be signing in from a new location app or device.

To help keep your account safe, we've blocked access to your inbox, contacts list and calendar for that sign in. Please review your recent activity and we'll help you secure your account. To regain access you'll need to confirm that the recent activity was yours.

<http://account.live.com/ResetPassword.aspx>

Thanks,
The Microsoft Team

Cybersecu

Attention au Phishing

SPAM EMAIL SPOT THE DIFFERENCE

there are 6 differences between the fake and real one, can you spot them?

FAKE

From: support@microsoft.co.uk
Sent: 16/01/2023 11:44
To: Bob Smith <Bob.Smith@company.com>
Subject: Urgent Action Needed!

REAL

From: support@microsoft.co.uk
Sent: 16/01/2023 11:44
To: Bob Smith <Bob.Smith@company.com>
Subject: Unusual Sign In Activity

Outlook

Microsoft Account

Verify your account

We detected some unusual activity about a recent sign in for your Microsoft account. You might be signing in from a new location app or device.

To help keep your account safe, we've blocked access to your inbox, contacts list and calendar for that sign in. Please review your recent activity and we'll help you secure your account. To regain access you'll need to confirm that the recent activity was yours.

<http://account.live.com/ResetPassword.aspx>

Thanks,
The Microsoft Team

Cybersecu

From: support@microsoft.co.uk
Sent: 16/01/2023 11:44

Piratage boîte mail :

Processus de blocage très rapide :

- Changement langage dans boîte mail
- Changement mot de passe
- Mail de paiement

Autre piratage possible : utilisation de votre email à votre insu:

- section messages envoyés vides mais vous voyez des non delivery report
- notification trop de message envoyé par jour/heure

Re: Santé !!:

bar [REDACTED] eels <rb360600@gmail.com> ← ↵ → ...
B [REDACTED] @hotmail.com ↴ **PIRATAGE BOÎTE EMAIL**

Je te remercie pour ta réponse rapide ,
Pour tout te dire ces dernières semaines n'ont pas été faciles pour moi.
J'ai quelques pepins de santé.

Des crampes intestinales et des douleurs abdominales que je n'arrive pas à calmer depuis un certain temps.
Je m'interroge sans cesse sur ce qui va bien arriver ? Et quelles seront les conséquences ?

Ce sont toutes ces interrogations qui m'ont poussé à avoir un autre avis extérieur en consultant un spécialiste en la matière pour des analyses plus poussées. Nous avons eu un premier contact. Et demain, nous devons nous revoir pour les résultats d'analyses. J'espère que mes doutes ne seront pas confirmés et que tout ceci sera un souvenir lointain ... Bref, je t'en dirai plus dès la sortie des examens, ne t'inquiète pas avant la sortie des résultats s'il te plaît.

Mais je t'écris, car j'ai une sérieuse demande à te faire , j'ai du mal à trouver des (C O U P O N S - NEOSURF) comme je le fais habituellement, c'est compliquer ici d'en trouver impossible d'en trouver.

Ces cartes prépayées sont vendues dans les Librairies et chez les buralistes (T A B A C) où dans les kiosques à journaux, j'en ai vraiment besoin dans l'urgence maintenant, il suffit juste de demander, ils sauront de quoi, il est question.

j'ai si l te plaît besoin de 15 (RECHARGE - NEOSURF) de 100 € chacune pour ma carte prépayée que j'utilise pour mes déplacements et mes achats Internet. En fait, ce sont des recharges que j'utilise pour mes achats via le net et régler certaines dépenses.

Une fois que tu les as, il faudra me faire parvenir les codes de recharge qui y figurent par mail ou si possible me faire un scan. NB: pour le remboursement souhaitez-tu par virement ? Je t'appellerai dès que mon portable sera en service Je compte sur ta discréction.Tu y vas rapidement stp? Prends bien soin de toi.

Rançongiciel:

The screenshot shows a ransomware attack interface with the following sections:

- Header:** Wanna Decryptor 2.0
- Title:** Oops, your files have been encrypted!
- Language:** English
- Section 1: What Happened to My Computer?**

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
- Section 2: Can I Recover My Files?**

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
- Section 3: Payment Information**

Payment will be raised on 3/28/2019 13:44:14
Time Left 00:00:00
- Section 4: File Loss Information**

Your files will be lost on 4/10/2019 14:44:14
Time Left 00:00:00
- Section 5: Instructions**

Please follow the instructions:

 - Send \$300 worth of Bitcoin to following address:
1Mz7...
BX
 - Send your Bitcoin wallet ID and personal installation key to e-mail: wowsmith123456@posteo.net. Your personal installation key: NjJ...
PS
- Section 6: Key Purchase**

If you already purchased your key, please enter it below.
Key:
- Buttons:** Send \$300 worth of bitcoin to this address!, Check Payment, Decrypt, Contact Us, About Bitcoin, How to buy Bitcoin?, Copy

Que faire quand on est victime d'une attaque :

Piratage boîte mail / autres comptes :

1. Changer mot de passe si on a encore accès
2. Créer une identification double facteur
- 3. Contacter votre service messagerie (gmail, Hotmail, Yahoo, Orange, Facebook, Instagram, Snapchat, Twitter...)**
4. Trouver les informations sur les récupérations possibles de données
5. Vérifier que vos autres comptes ne sont pas affectés (**changement email et mot de passe – vérifier qu'aucune commande n'a été effectuée – prévenez votre banque**)
6. Faire un scan avec antivirus
7. Informer vos contacts que vous avez été pirate
8. Porter plainte
- 9. NE PAS PAYER**

Piratage ordinateur :

1. Se déconnecter d'internet
2. Éteindre son PC
3. Rallumer le PC et voir si le chiffrement continue
- 4. Garder les preuves : message du rançongiciel, fichiers cryptés, log...**
- 5. Contacter Windows ou Apple...**
6. Porter plainte
- 7. NE PAS PAYER**

Cybersecurité 2025 : Comment se Protéger ?

1. La cybersécurité c'est quoi?
2. Les différents types d'attaque, exemples concrets
3. **Prévention et réflexes à adopter**
 - Sécuriser ses appareils et applications
 - Gérer son identité numérique et protéger ses comptes
 - Les bons reflexes sur les réseaux sociaux
 - Protéger ses données personnelles et sa vie privée
 - Les attaques personnelles les plus courantes, que faire en cas d'attaque?
 - **Les intervenants gouvernementaux**

Les intervenants gouvernementaux français:

L'ANSSI, l'Agence Nationale de la Sécurité des Systèmes d'Information



CNIL, Commission Nationale de l'Informatique et des Libertés



CyberMalveillance.gouv.fr : Diagnostic et assistance aux victimes de cybermalveillance



US: Vol de SSN Social Security Number = usurpation d'identité

<https://www.ssa.gov/number-card/report-stolen-number>

<https://www.ssa.gov/pubs/EN-05-10064.pdf>

The screenshot shows the official website of the Social Security Administration (SSA) at [ssa.gov/number-card/report-stolen-number](https://www.ssa.gov/number-card/report-stolen-number). The page has a blue header bar with the SSA logo and navigation links for Social Security, Benefits, Medicare, Card & record, and Espanol. A sign-in link is also present. Below the header, there's a yellow banner with the text: "If you need to visit an office, schedule an appointment first. Find out how." and a link to "Information about the Social Security Fairness Act (WEP/GEI)". The main content area has a light green background and features a large button labeled "Report stolen Social Security number". To the right of this button, there's a section titled "Tell the Federal Trade Commission what happened" with a checkbox and a "Start report" button. At the bottom left, there's a "Report stolen number" link. The footer contains social media icons for Facebook, Twitter, Instagram, YouTube, and LinkedIn, along with the text "SSA.gov" and "Cybersecurité 2025 - Celine Blandin - Mars 2025".

Cyber sécurité 2025: Comment se protéger?

- 
1. La cybersécurité c'est quoi?
 - Définition
 - Evolution des menaces avec les nouvelles technologies
 - Impact du numérique sur la société
 2. Les différents types d'attaque, exemples concrets
 - Cybercriminalité
 - Atteintes à l'image et désinformation (fake news, manipulation)
 - Espionnage et collectes de données personnelles
 - Sabotages
 - Notion de cyberguerre
 3. Prévention et réflexes à adopter
 - Sécuriser ses appareils et applications
 - Gérer son identité numérique et protéger ses comptes
 - Les bons reflexes sur les réseaux sociaux
 - Protéger ses données personnelles et sa vie privée
 - Les attaques personnelles les plus courantes, que faire en cas d'attaque?
 - Les intervenants gouvernementaux