



# La cybersécurité et ses impacts

Céline Blandin – novembre 2022

# La cybersécurité et ses impacts

1. La cybersécurité c'est quoi?

2. Les différents types d'attaque

3. Impacts de cyber attaques

4. Cybersécurité, Tips, réflexes à avoir

# La cybersécurité et ses impacts

**1. La cybersécurité c'est quoi?**

**2. Les différents types d'attaque**

**3. Impacts de cyber attaques**

**4. Cybersécurité, Tips, réflexes à avoir**

# La cybersécurité c'est quoi?

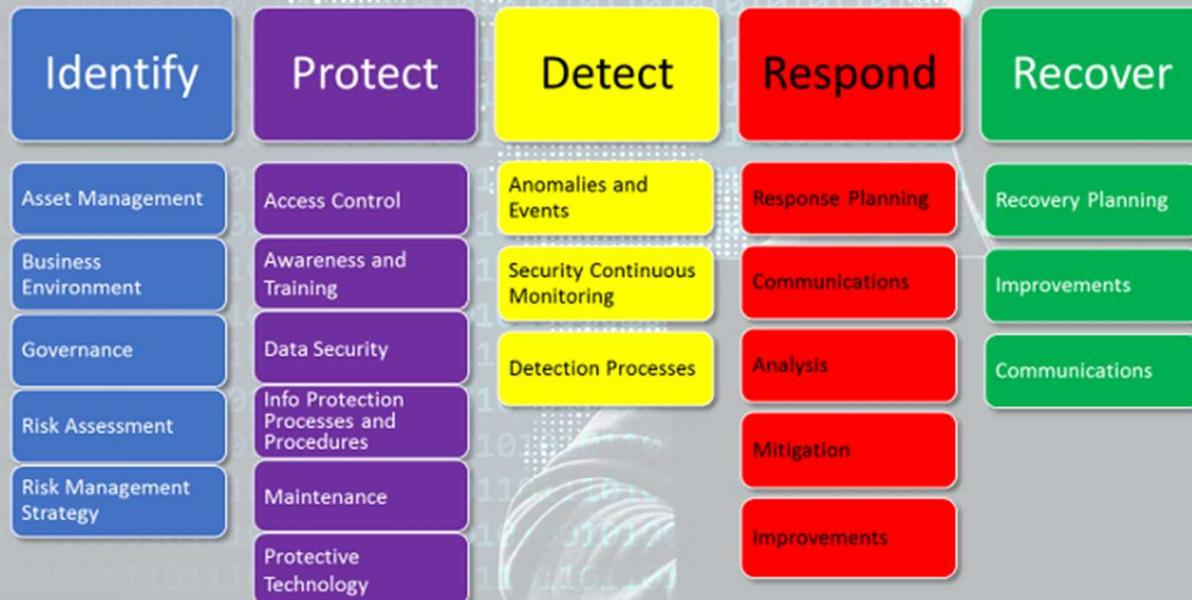
Définition :

Ensemble des moyens utilisés pour assurer la sécurité des systèmes et des données informatiques d'un État, d'une entreprise, d'un particulier, etc.



# La cybersécurité en entreprise

## NIST Cyber Security Framework

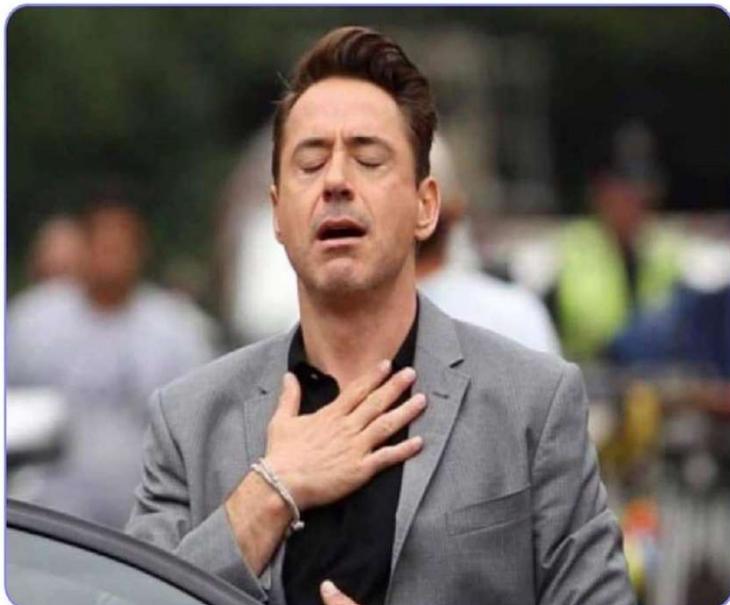


# La cybersécurité pour les particuliers

Manque de formation du grand public

Hacker: I have all of your passwords

Me who forgot them:



Manque de connaissance des outils en sécurité informatique



# Une surface d'attaque gigantesque



**\$50 MILLION**  
THE LARGEST RANSOM DEMAND

\*Made to computer giant Acer in March 2021



### RANSOMWARE STATISTICS BY THE NUMBERS

**37%**  
OF BUSINESSES

WERE HIT BY RANSOMWARE IN 2021

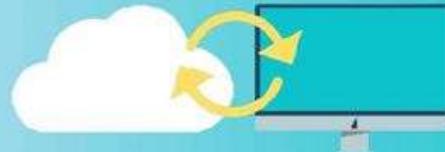
IN 2031, RANSOMWARE WILL COST THE WORLD  
**\$265 BILLION**



**32% OF VICTIMS**  
PAID A RANSOM DEMAND IN 2021

ON AVERAGE, PAYING VICTIMS RECOVERED ONLY  
**65% OF THEIR DATA**

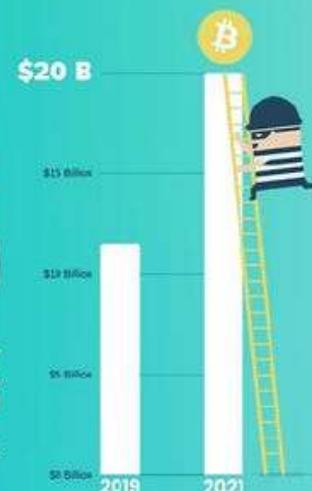
**57% OF COMPANIES**  
RECOVERED THEIR DATA USING A CLOUD BACKUP



A COMPANY IS HIT BY RANSOMWARE

IN 2021, EVERY  
**11 SECONDS**

**\$20 BILLION**  
THE TOTAL COST OF RANSOMWARE IN 2021



ON AVERAGE, IT COST BUSINESSES  
**\$1.85 MILLION**  
TO RECOVER FROM AN ATTACK IN 2021

### Global Ransomware Damage Costs\*

- **2015: \$325 Million**
- **2017: \$5 Billion**
- **2021: \$20 Billion**
- **2024: \$42 Billion**
- **2026: \$71.5 Billion**
- **2028: \$157 Billion**
- **2031: \$265 Billion**

 CYBERSECURITY  
VENTURES



Ransomware is expected to attack a business, consumer, or device every 2 seconds by 2031, up from every 11 seconds in 2021.

\* SOURCE: CYBERSECURITY VENTURES



# La cybersécurité et ses impacts

1. La cybersécurité c'est quoi?

2. Les différents types d'attaque

3. Impacts de cyber attaques

4. Cybersécurité, Tips, réflexes à avoir

## 1. Cybercriminalité :

Cyberattaques qui visent à obtenir des informations personnelles afin de les exploiter ou de les revendre (données bancaires, identifiants à des sites marchands, etc.). Ça va de la demande du rançongiciel, vol de données bancaires... à la pédopornographie, haine raciale...

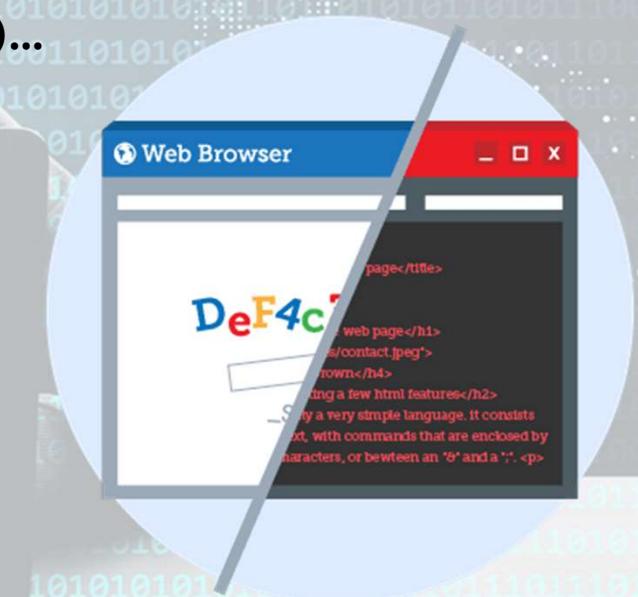
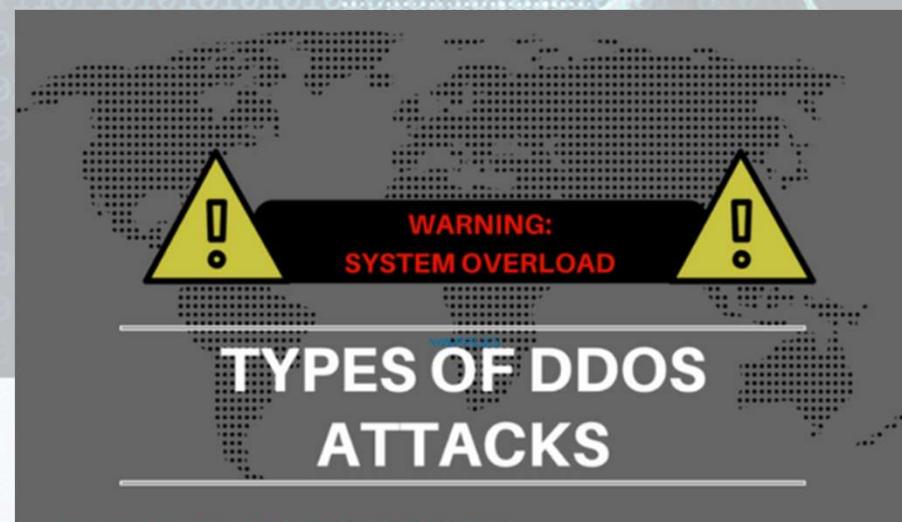
**Ransomware, phishing...**



## 2. Atteinte à l'image / Déstabilisation :

Lancées à des fins de déstabilisation contre des administrations et des entreprises et régulièrement relayées par les réseaux sociaux, les attaques de déstabilisation sont aujourd’hui fréquentes et généralement peu sophistiquées, faisant appel à des outils et des services disponibles en ligne. De l'exfiltration de données personnelles à l'exploitation de vulnérabilité, elles portent atteinte à l'image de la victime en remplaçant le contenu par des revendications politiques, religieuses, etc.

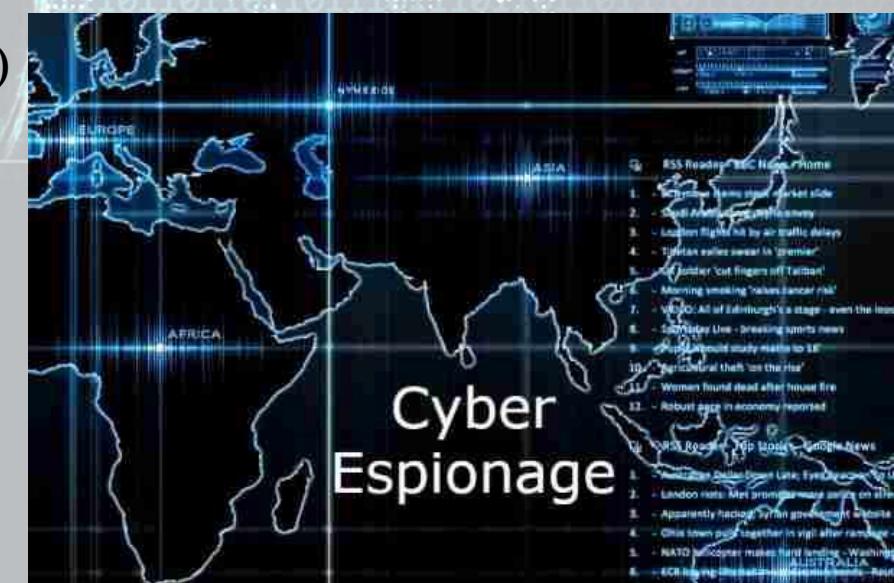
**Deni de Service (DDoS), défiguration,(defacement)...**



### 3. Espionnage :

Très ciblées et sophistiquées, les attaques utilisées pour l'espionnage à des fins économiques ou scientifiques sont souvent le fait de groupes structurés et peuvent avoir de lourdes conséquences pour les intérêts nationaux. De fait, il faut parfois des années à une organisation pour s'apercevoir qu'elle a été victime d'espionnage, l'objectif de l'attaquant étant de maintenir discrètement son accès le plus longtemps possible afin de capter l'information stratégique en temps voulu.

#### Spearfishing, cheval de troie (Trojan Horse)



#### **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.

**Panne, attaque terroriste**



# La cybersécurité et ses impacts

1. La cybersécurité c'est quoi?

2. Les différents types d'attaque

3. Impacts de cyber attaques

4. Cybersécurité, Tips, réflexes à avoir

# Les différents type d'attaquants (HACKER) :

1. Les **script Kiddies** : pirate junior avec hobby



2. Les **hacktivistes** : point de vue different, protestation



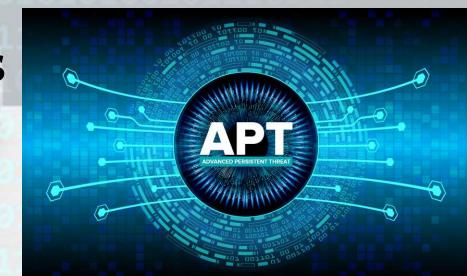
3. Les **organisations criminelles** : 1 seul but, l'argent



4. La **competition** : espionnage industriel...



5. Les **APTs, Advanced Persistent Threats** : les gouvernements de pays



# Stuxnet virus

Stuxnet est un worm qui s'attaque aux systèmes industriels utilisant Microsoft Windows et qui cible les systèmes Siemens. Il est fortement possible que ce **cyberweapon** a été conçu par les Etats Unis et l'Israël sous le projet *Opération Olympic Games*.



Stuxnet est connu pour avoir fortement endommagé les centrales nucléaires d'Iran en novembre 2007. Ce sabotage a entre autres considérablement ralenti les opérations iraniennes pour obtenir l'**arme nucléaire**.

# Le scandale des emails d'Hillary Clinton

## Impact sur les élections présidentielles américaines 2016

Hillary Clinton a été accusée d'avoir utilisé un serveur public pour ses emails professionnels (2009-2013). Environ 31000 emails ont ensuite été effacés après qu'une assignation fut déposée.

En parallèle, le DNC (Democratic National Committee) est victime d'une cyberattaque menée par des groupes russes. En Juillet 2016, des données du DNC sont diffusées sur WikiLeaks. Cet évènement ravive le sujet des emails d'Hilary Clinton et Trump a utilisé cet argument pendant la campagne électorale :

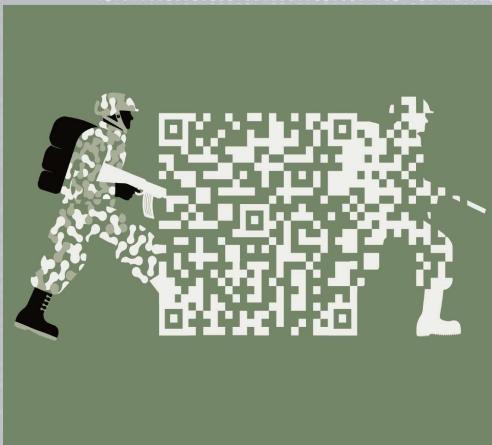
*"Look at the crimes that Clinton did with the emails and she deletes 33,000 emails after she gets a subpoena from Congress, and this Justice Department does nothing about it?"*

Le 9 novembre 2016, Trump est élu président des Etats Unis.

En décembre 2016, la CIA conclut dans son rapport que des opérations russes ont été menées pour aider Trump à gagner les élections présidentielles.



# Comment une guerre physique est préparée et supportée par la Cyberguerre exemple de l'Ukraine



## 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.

# Le groupe hactiviste Anonymous vs China – US visit to Taïwan



# Le groupe hactiviste **Anonymous** vs **China** – US visit to Taïwan

<https://www.youtube.com/watch?v=A8DI1Y6QGqM>

**Regarder jusqu'à la minute 1:20**

# **La cybersécurité et ses impacts**

**1. La cybersécurité c'est quoi?**

**2. Les différents types d'attaque**

**3. Impacts de cyber attaques**

**4. Cybersécurité, Tips, réflexes à avoir**

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

Paramètres

Accueil

Rechercher un paramètre

Mise à jour et sécurité

Windows Update

Votre appareil est à jour. Dernière vérification : aujourd'hui, 09:03

Rechercher des mises à jour

Afficher l'historique des mises à jour installées

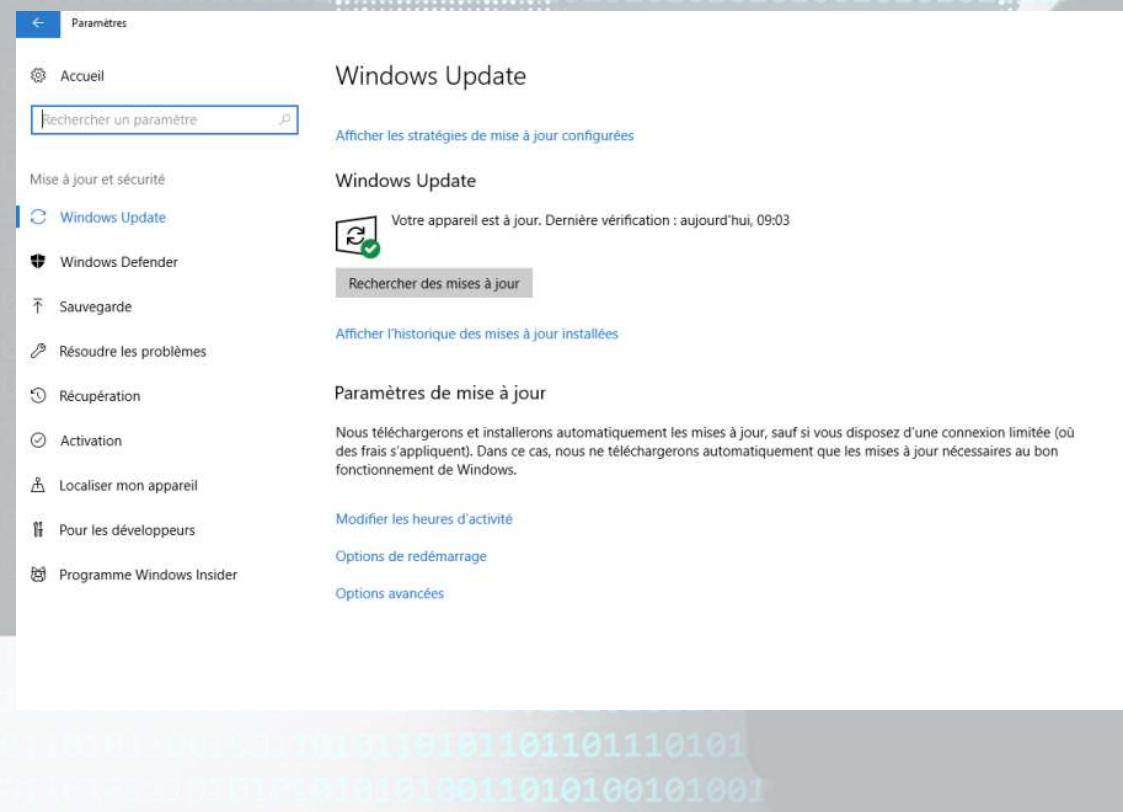
Paramètres de mise à jour

Nous téléchargerons et installerons automatiquement les mises à jour, sauf si vous disposez d'une connexion limitée (où des frais s'appliquent). Dans ce cas, nous ne téléchargerons automatiquement que les mises à jour nécessaires au bon fonctionnement de Windows.

Modifier les heures d'activité

Options de redémarrage

Options avancées



Mise à jour de logiciels

macOS Monterey

12.0.1 — 12,13 Go

Plus d'infos...

Mettre à niveau maintenant

Mise à jour de logiciels

Mettre à jour automatiquement mon Mac

Avancé... ?



# Installer un antivirus



# 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@17112003

Motdep@sse

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

Jhd'eevm+c@3dm!

J'ai hâte d'être en Vacances et me coucher à 3h du mat !  
+ @

Règles :

- **8 à 10 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

# Les coffres fort de mot de passe



KeePass

<https://keepass.fr/>

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

masterDatabase.kdbx\* - KeePass

File Edit View Tools Help

Search...

masterDatabase

- General
- Windows
- Network
- Internet
- eMail
- Homebanking

Title	User Name	Password	URL	Notes
Sample En...	User Name	*****	<a href="https://keepass.info/">https://keepass.info/</a>	Notes
Sample En...	Michael321	*****	<a href="https://keepass.info/">https://keepass.info/</a>	

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

Notes

1 of 2 selected | Ready.

# DOUBLE AUTHENTICATION



SOMETHING  
YOU KNOW

WITH



SOMETHING  
YOU HAVE

OR



SOMETHING  
YOU ARE

# Comment vérifier si nos données ont été hackées

The screenshot shows the homepage of the [Have I Been Pwned?](https://haveibeenpwned.com/) website. At the top, a large button contains the text '';--have i been pwned?'. Below it, a sub-header reads 'Check if you have an account that has been compromised in a data breach'. A search bar is labeled 'email address' and has a 'pwned?' button to its right. Below the search area, there's a promotional message for 1Password: 'Generate secure, unique passwords for every account' with a 'Learn more at 1Password.com' link. A 'Why 1Password?' link is also present. At the bottom, four statistics are displayed: '327 pwned websites', '5,620,024,112 pwned accounts', '83,975 pastes', and '91,563,791 paste accounts'.

Category	Value
pwned websites	327
pwned accounts	5,620,024,112
pastes	83,975
paste accounts	91,563,791

<https://haveibeenpwned.com/>

<https://www.avast.com/hackcheck#pc>

# Ne pas connecter une clef USB inconnue

Toujours savoir d'**où** provient la clef USB avant de la connecter.  
Peux t'on avoir confiance?

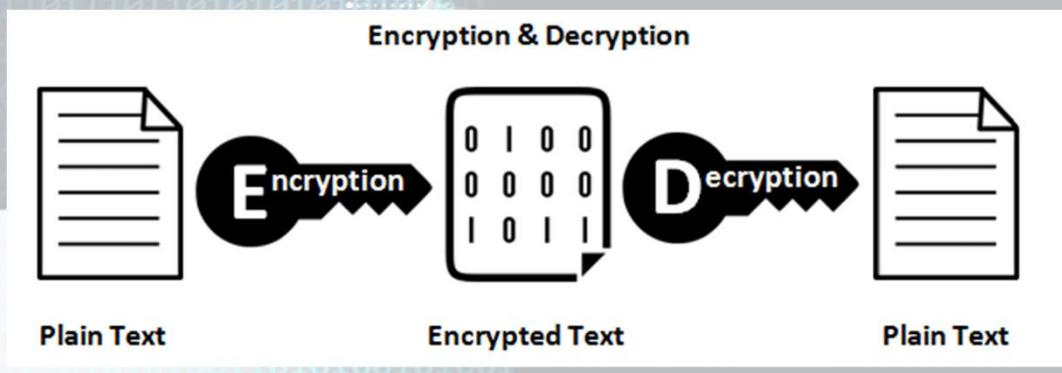


# Mieux vaut prévenir que guérir : **BACKUP**

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

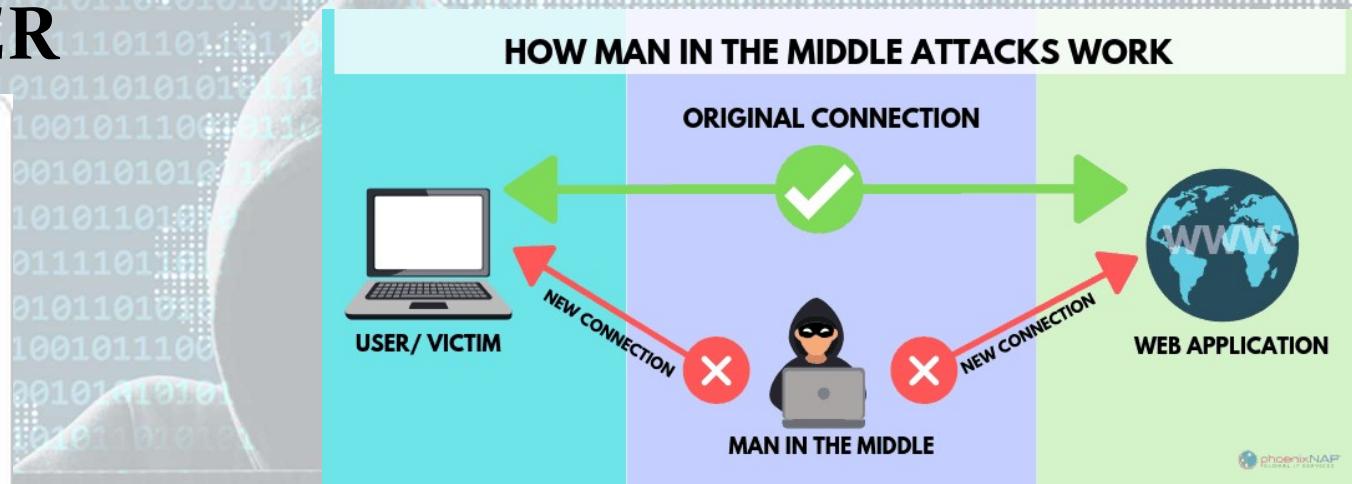


# Mieux vaut prévenir que guérir : le **CHIFFREMENT**



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

**Free WIFI = DANGER**



**VPN : Virtual Private Network**



# 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.

  
  
**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 s'il vous plaît la demande de remboursement  
pour nous permettre de la traiter dans un plus bref délai  
(le délai de traitement est de 10 jours ouverts).

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

- 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 :



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

- Rester pragmatique, vous avez peu de chance que les impôts vous remboursent 791€, ou de gagner à une loterie dont vous n'avez pas participé.
- Rester en alerte, les emails frauduleux sont toujours de plus en plus réaliste, exemple : mail jeux pour Noël...

# Rançongiciel, Ransomware:

Oops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.

We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send \$300 worth of Bitcoin to following address:

1Mz7... BHX

2. Send your Bitcoin wallet ID and personal installation key to e-mail [wowsmith123456@posteo.net](mailto:wowsmith123456@posteo.net). Your personal installation key:

NjH... P5

If you already purchased your key, please enter it below.

Key:



# 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. **Contactez 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 (**changez email et mot de passe – vérifiez qu'aucune commande n'a été effectuée – prévenez votre banque**)
6. Faire un scan avec antivirus
7. Informer vos contacts que vous avez été piraté
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, screenshot, log...**
5. **Contactez Windows ou Apple...**
6. Porter plainte
7. **NE PAS PAYER**

## 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**





# La cybersécurité et ses impacts

## 1. La cybersécurité c'est quoi?

- Internet minute
- Cout 265 milliards en 2031

## 3. Impacts de cyber attaques

- Les différents types d'attaquant
- Stuxnet
- Les emails d'Hillary Clinton
- La guerre en Ukraine
- Anonymous vs China - Taïwan

## 2. Les différents types d'attaque

- Cybercriminalité
- Atteinte à l'image
- Espionnage
- Sabotage

## 4. Cybersécurité, Tips, réflexes à avoir

- Update
- Antivirus
- Mot de passe – offre fort
- Double authentification
- haveibeenpwned.com
- BACKUP
- Free WIFI = DANGER
- Phishing – Virus Total
- Ransomware
- La cybersécurité en France