

The background of the slide features a person wearing a grey hoodie, sitting at a desk with a laptop. The person's face is obscured by the text. The entire scene is overlaid with a dense, semi-transparent pattern of binary code (0s and 1s) in a light blue/cyan color. The title text is centered over the person's upper body.

Introduction à la cybersécurité Réflexes à avoir

Céline Blandin – Mars 2022

Introduction à la cybersécurité

1. La cybersécurité c'est quoi?
2. Les différents types d'attaque, exemples concrets
3. Prévention et 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, etc.



De nombreuses cyberattaques, quelques chiffres :

Global Cybercrime Damage by 2021



\$16.4
Billion per day

\$684.9
Million per hour

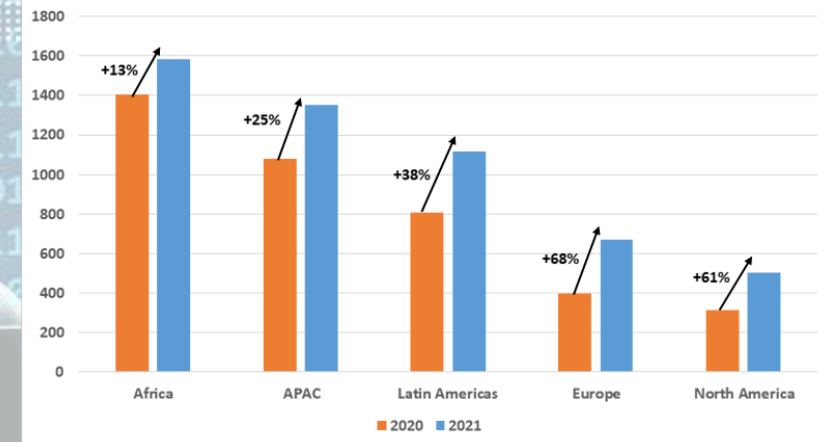
\$11
Million per minute

\$190,000
Per second

Source: Cybersecurity Ventures, 2020

 **FinancesOnline**
REVIEWS FOR BUSINESS

Weekly Attacks per Organization by Region (2020 Vs. 2021)



Introduction à la cybersécurité

1. La cybersécurité c'est quoi?
2. Les différents types d'attaque, exemples concrets
3. Prévention et réflexes à avoir



Classements des cyberattaques en 4 catégories :

1. Cybercriminalité



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...

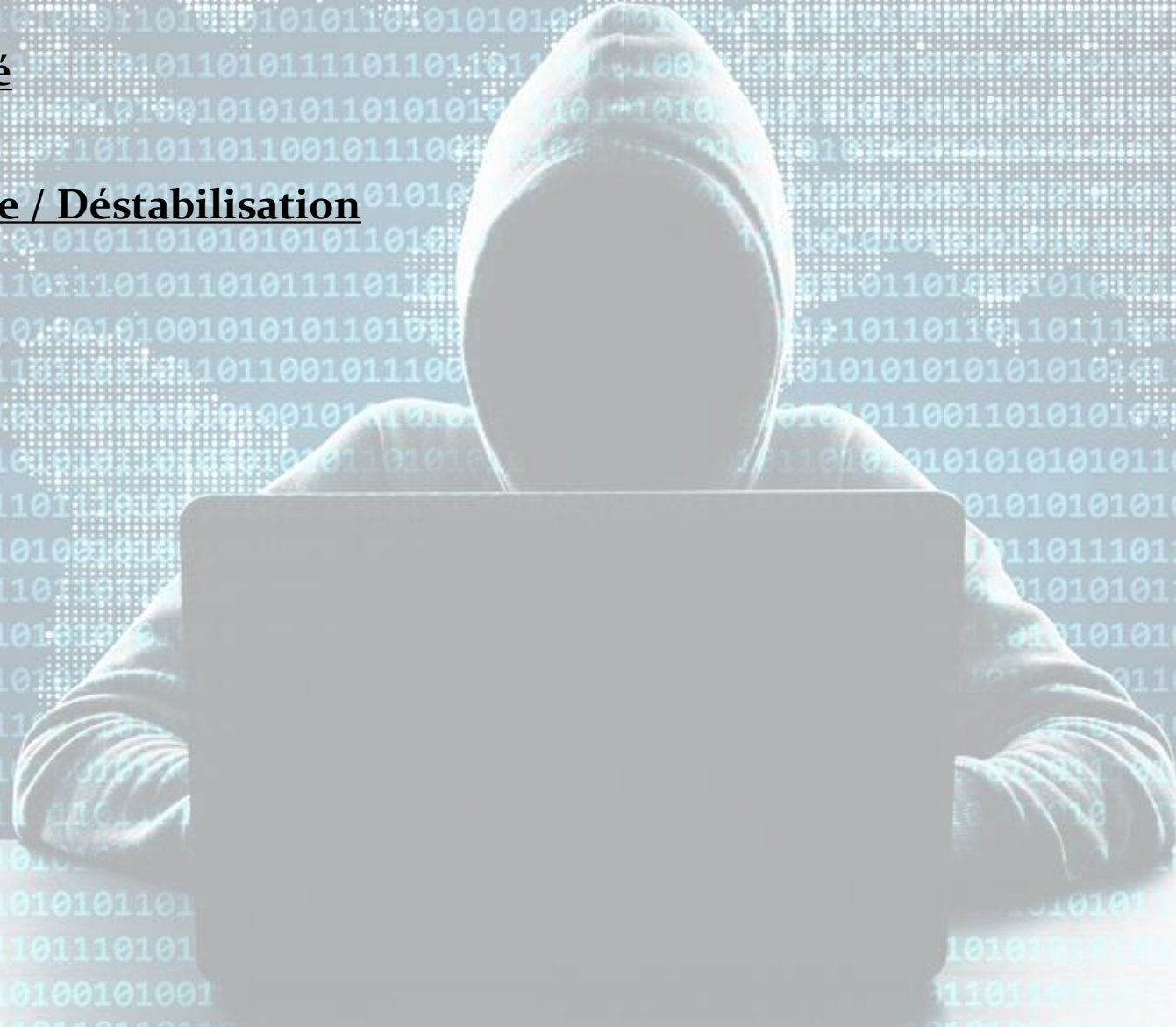
Ransomware, phishing...



Classements des cyberattaques en 4 catégories :

1. Cybercriminalité

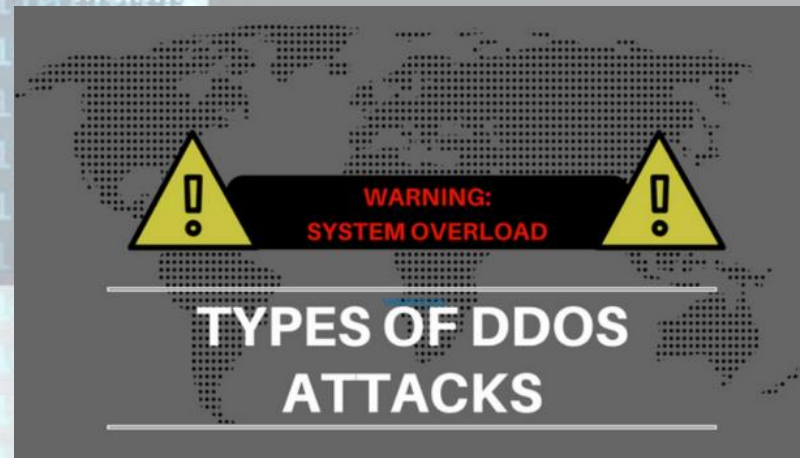
2. Atteinte à l'image / Déstabilisation



2. Atteinte à l'image / Déstabilisation :

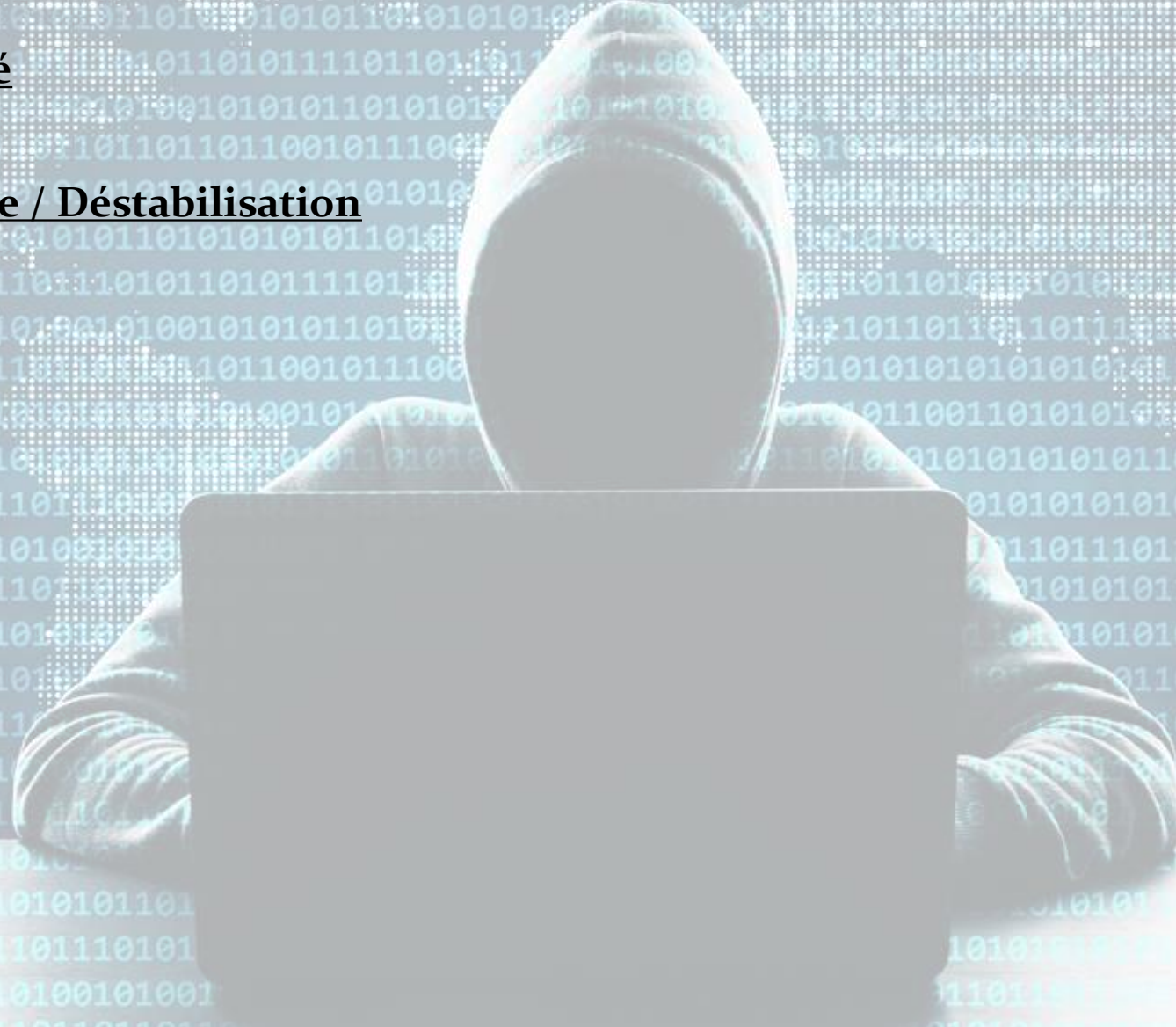
Lancées à des fins de déstabilisation contre des administrations et des entreprises et régulièrement relayées par les réseaux sociaux, les attaques de déstabilisation sont aujourd'hui fréquentes et généralement peu sophistiquées, faisant appel à des outils et des services disponibles en ligne. De l'exfiltration 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)...



Classements des cyberattaques en 4 catégories :

1. Cybercriminalité
2. Atteinte à l'image / Déstabilisation
3. Espionnage



3. Espionnage :

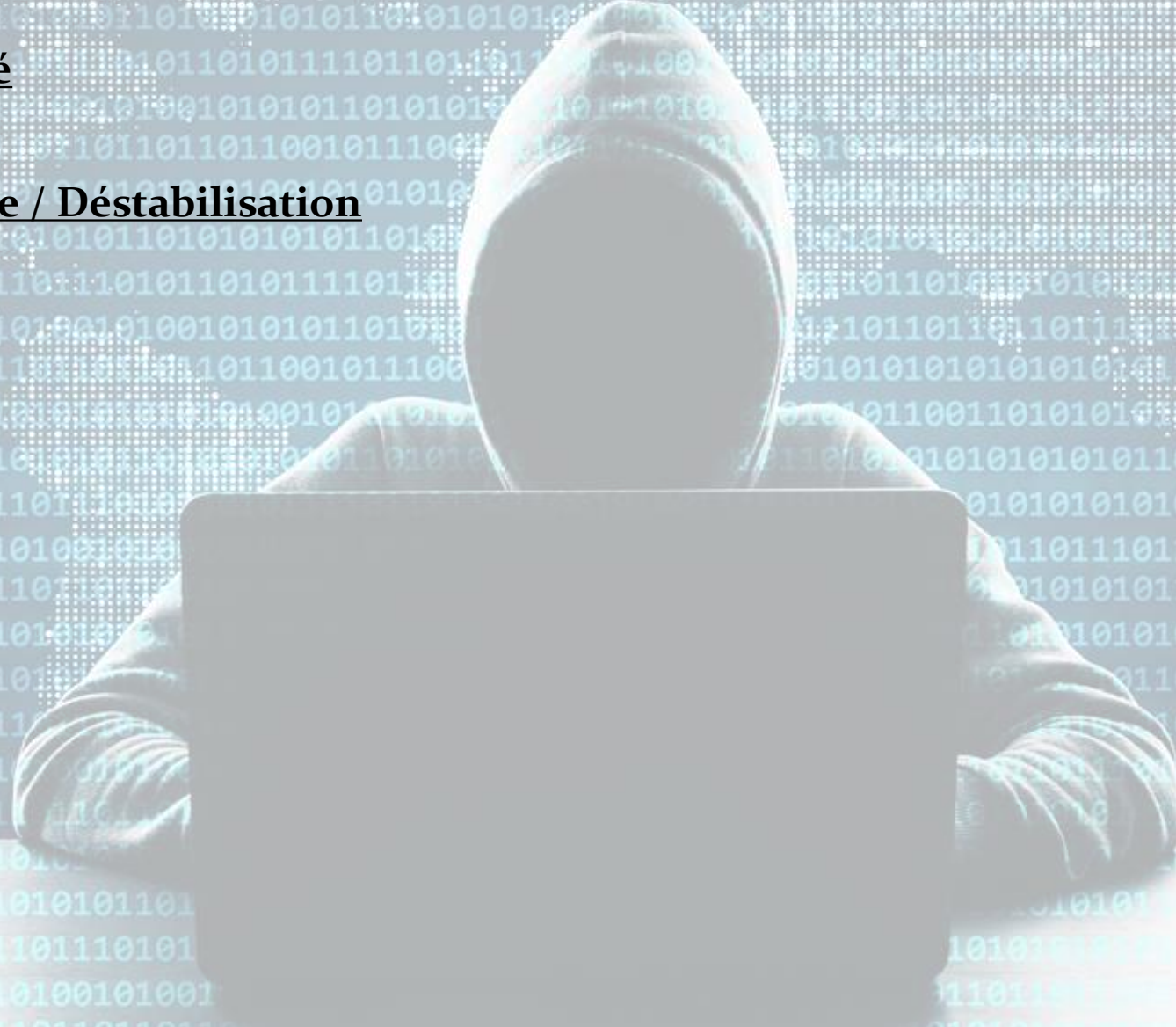
Très ciblées et sophistiquées, les attaques utilisées pour l'espionnage à des fins économiques ou scientifiques sont souvent le fait de groupes structurés et peuvent avoir de lourdes conséquences pour les intérêts nationaux. De fait, il faut parfois des années à une organisation pour s'apercevoir qu'elle 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)



Classements des cyberattaques en 4 catégories :

1. Cybercriminalité
2. Atteinte à l'image / Déstabilisation
3. Espionnage
4. Sabotage



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



Quelques attaques connues :

- Groupe **DarkSide** - **Colonial Pipeline USA** – **4,4 millions de dollars** de rançon, pays bloqué
- **Solarwinds** – logiciel « Orion » – début attaque en **mars 2020**, découvert en **décembre 2020**
- Ransomware **Wannacry** – 2017 – **300 000 ordinateurs** dans **150 pays** – Système santé britannique, Renault, opérateur espagnol Telefonica



Cyberguerre, c'est quoi?

Nous sommes déjà en cyberguerre “froide” depuis longtemps

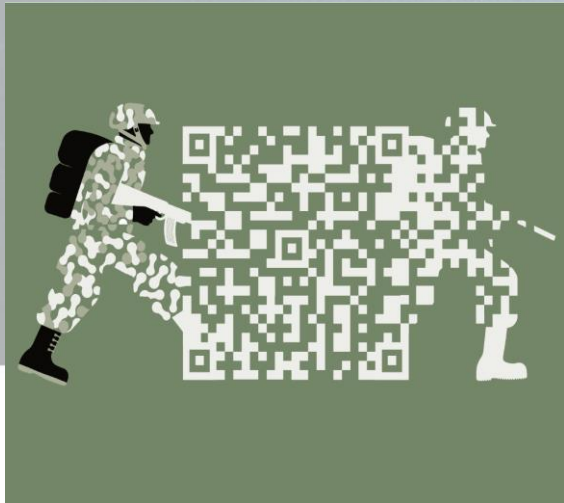
Attaques réelles, mais jamais vraiment revendiquées :
Stuxnet, Shamoon, NotPetya, Hillary Clinton vs Trump election,
Sunburst backdoor (SolarWinds), ...

Concrètement : sabotage, espionnage, subversion



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

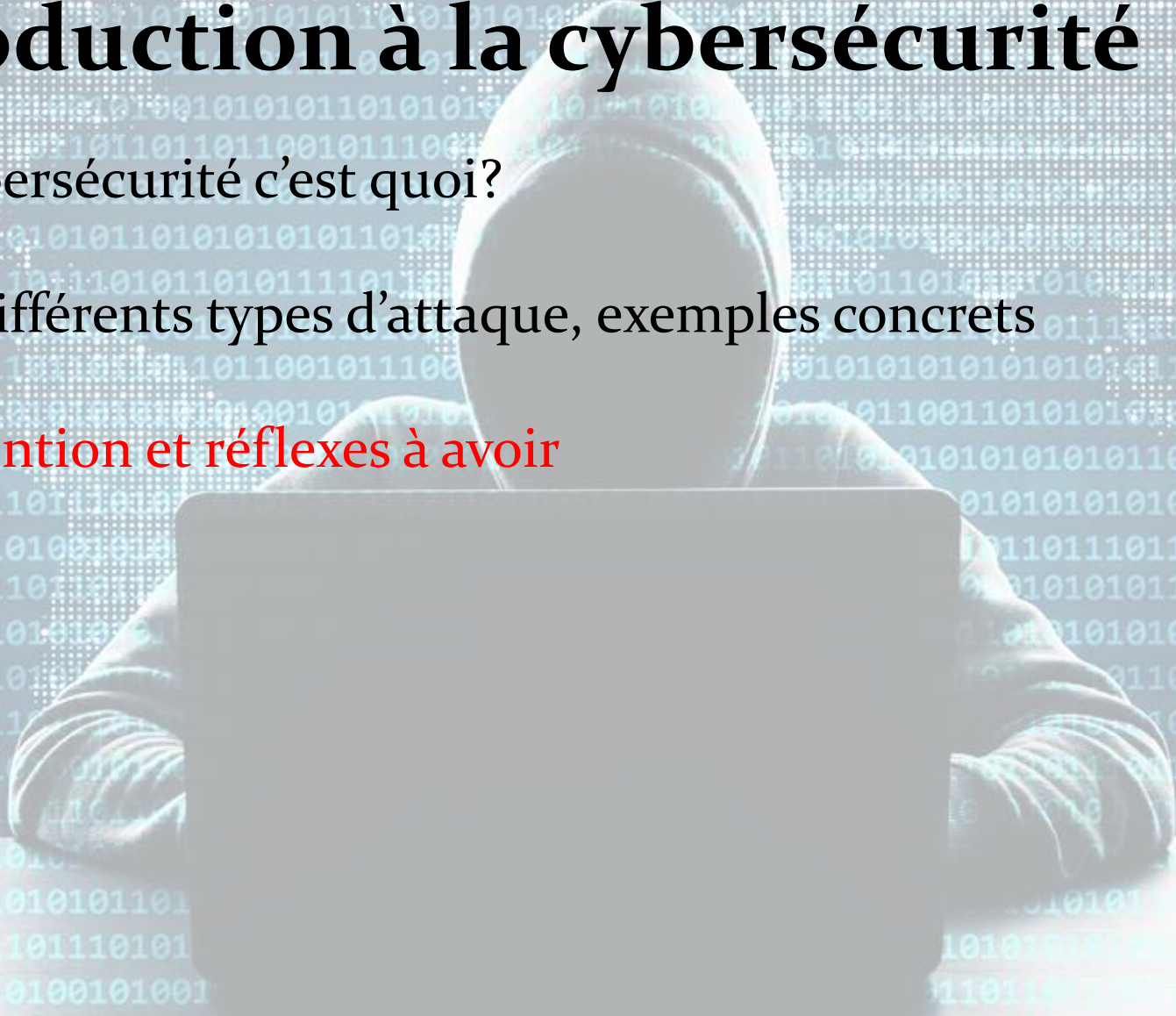
Le cas concret de l'Ukraine :



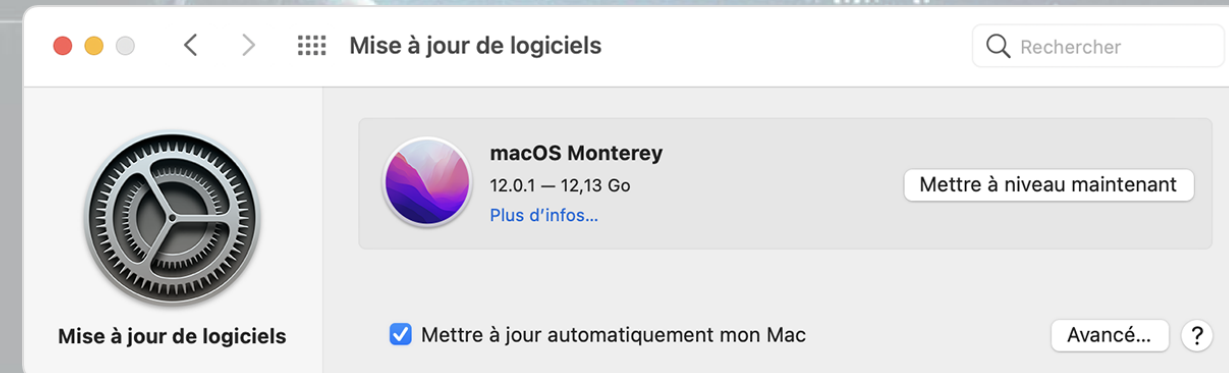
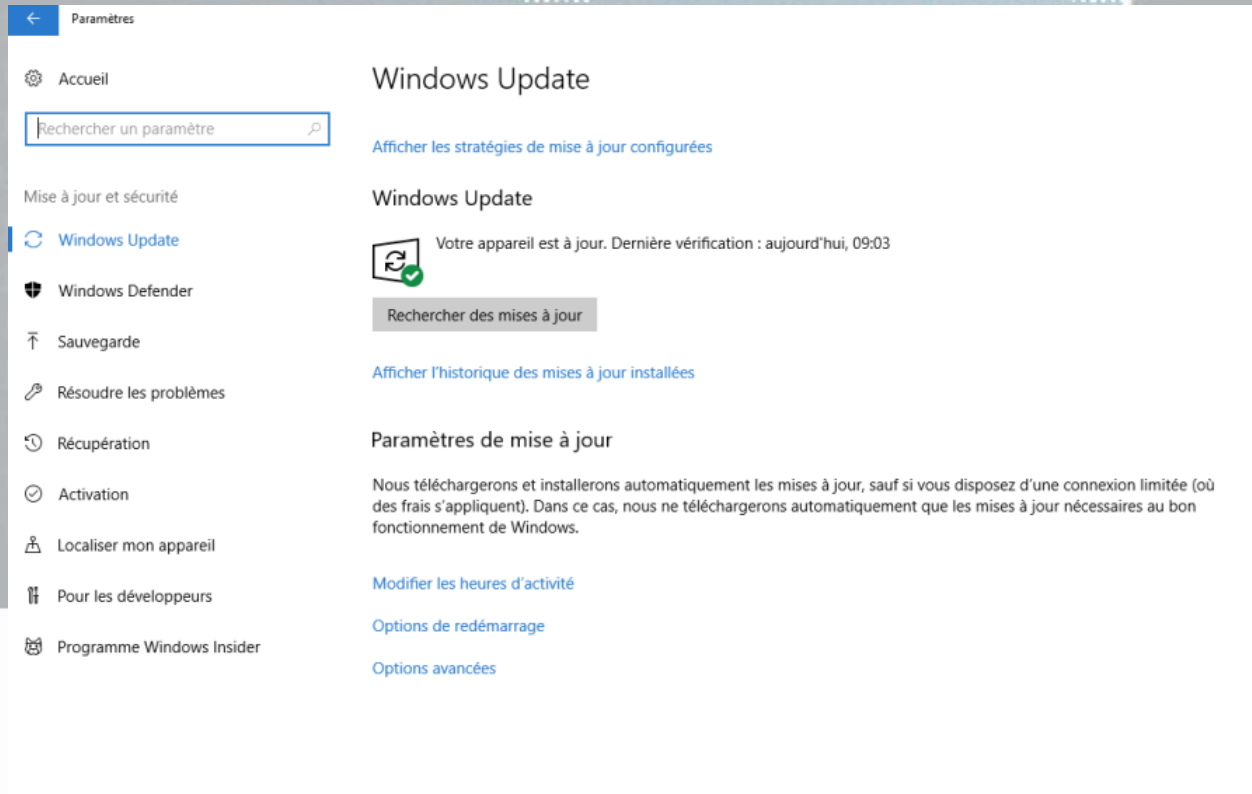
- 13/01/22 : malware/wiper *WhisperGate* découvert sur ordinateurs d'organisations gouvernementales, services de télécommunication...
- 14/01/22 : cyberattaques sur 70 sites web gouvernementaux / propagande de peur
- 15/02/22 : attaque Ddos de grande ampleur sur les sites internet du Ministère de la 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 operation militaire d'envergure sur toute l'Ukraine, 1 heure après le reseau satellite américain KA-SAT subit une cyberattaque.

Introduction à la cybersécurité

1. La cybersécurité c'est quoi?
2. Les différents types d'attaque, exemples concrets
3. Prévention et réflexes à avoir



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



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@o8112003 Motdep@sse

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

JhqlEr@le2+5 J'ai hâte que les Enfants retournent @ l'Ecole en 24/24 + 5/7

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	*****	https://keep...	Notes
Sample En...	Michael321	*****	https://keep...	

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

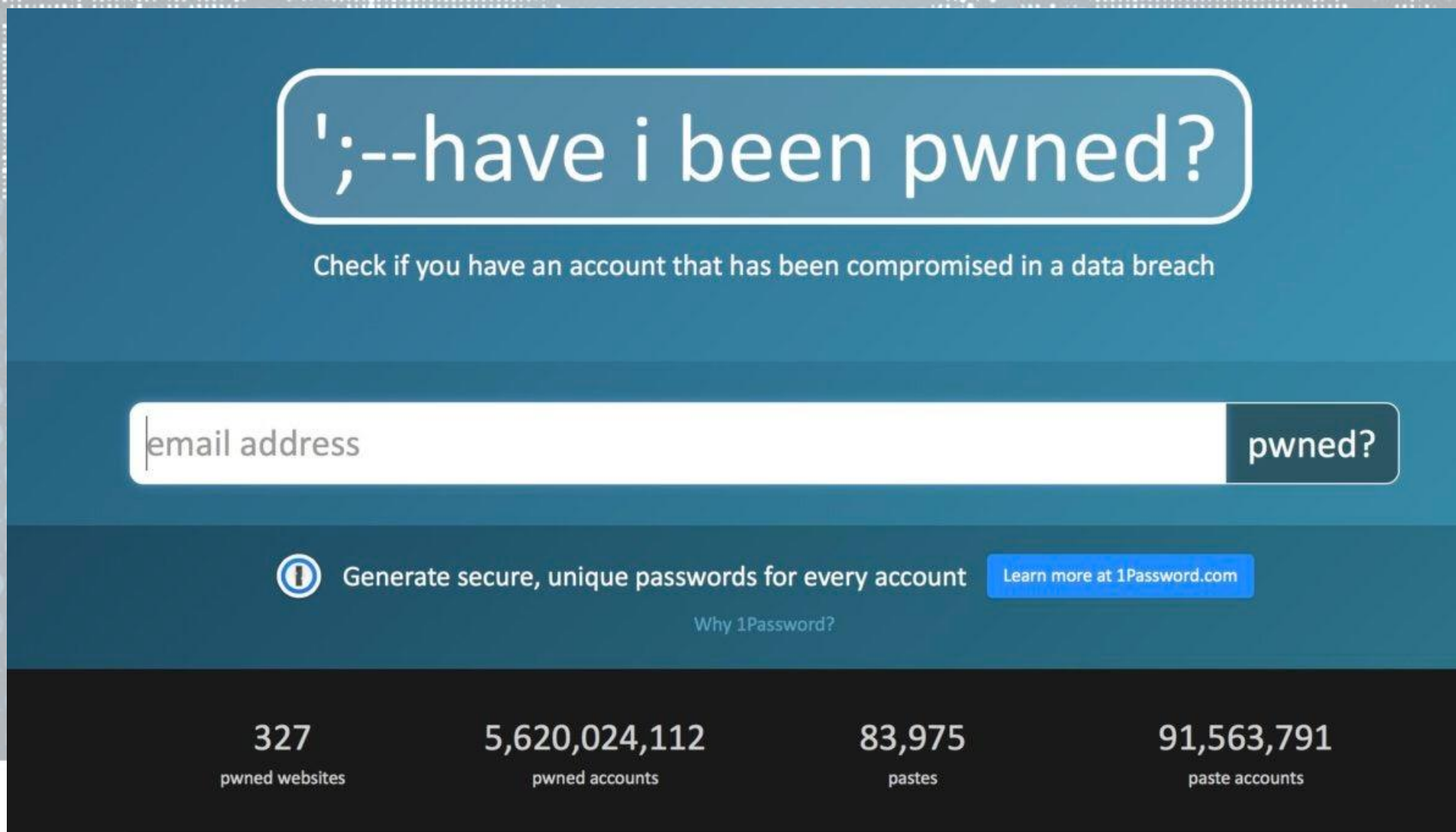
Notes

1 of 2 selected | Ready.

DOUBLE AUTHENTICATION



Comment vérifier si nos données ont été hackées




The image shows the homepage of the 'have i been pwned?' website. The main heading is 'have i been pwned?' in a large, white, rounded box. Below it, a subtitle reads 'Check if you have an account that has been compromised in a data breach'. There is a search bar with the placeholder text 'email address' and a button labeled 'pwned?'. Below the search bar, there is a section for 1Password, which includes a blue button with a white 'i' icon, the text 'Generate secure, unique passwords for every account', and a link 'Learn more at 1Password.com'. At the bottom, there are four statistics: '327 pwned websites', '5,620,024,112 pwned accounts', '83,975 pastes', and '91,563,791 paste accounts'.

';--have i been pwned?

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

email address pwned?

 Generate secure, unique passwords for every account [Learn more at 1Password.com](#)

[Why 1Password?](#)

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

<https://haveibeenpwned.com/>

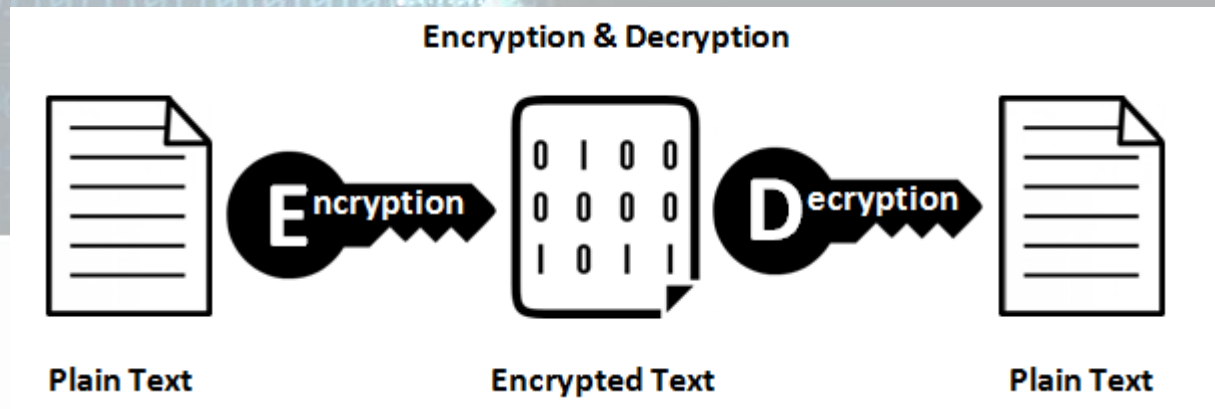
<https://www.avast.com/hackcheck#pc>

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.



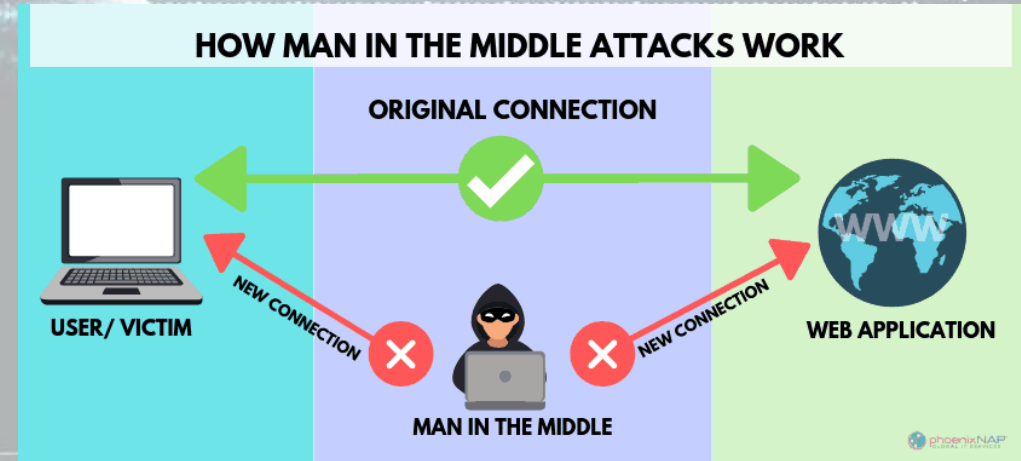
Mieux vaut prévenir que guérir : le **CHIFFREMENT**



Free WIFI = DANGER



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



VPN : Virtual Private Network



Attention au Phishing



- 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 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...

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... eels <rb360600@g

mail.com>

Mar 30-04-19 08:15

@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 pépins 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'écis, 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 prépayés 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 s'il 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 rechargement qui y figurent par mail ou si possible me faire un scan.

NB: pour le remboursement souhaites-tu par virement ?

Je t'appellerai dès que mon portable sera en service

Je compte sur ta discrétion.Tu y vas rapidement stp?

Prends bien soin de toi.

Rançongiciel:

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 [QR code] BX

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

NjJh [QR code] P5

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

Wana Decrypt0r 2.0

Oops, your files have been encrypted!

English

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.

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.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>. And send the correct amount to the address specified in this window. After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT Sat, Monday, Friday

[About bitcoin](#)
[How to buy bitcoins?](#)
[Contact Us](#)

Payment will be raised on
3/28/2019 13:44:14
Time Left
00:00:00:00

Your files will be lost on
4/1/2019 14:44:14
Time Left
00:00:00:00

Send \$300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw [Copy](#)

Check Payment **Decrypt**

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 (**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 :

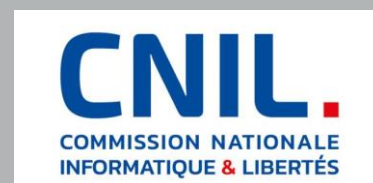
1. Se déconnecter d'internet
2. Éteindre son PC
3. Rallumer le PC et voir si le chiffrement continue
4. **Garder les preuves : message du rançongiciel, fichiers cryptés, log...**
5. **Contactez Windows ou Apple...**
6. Porter plainte
7. **NE PAS PAYER**

Les intervenants gouvernementaux français:

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

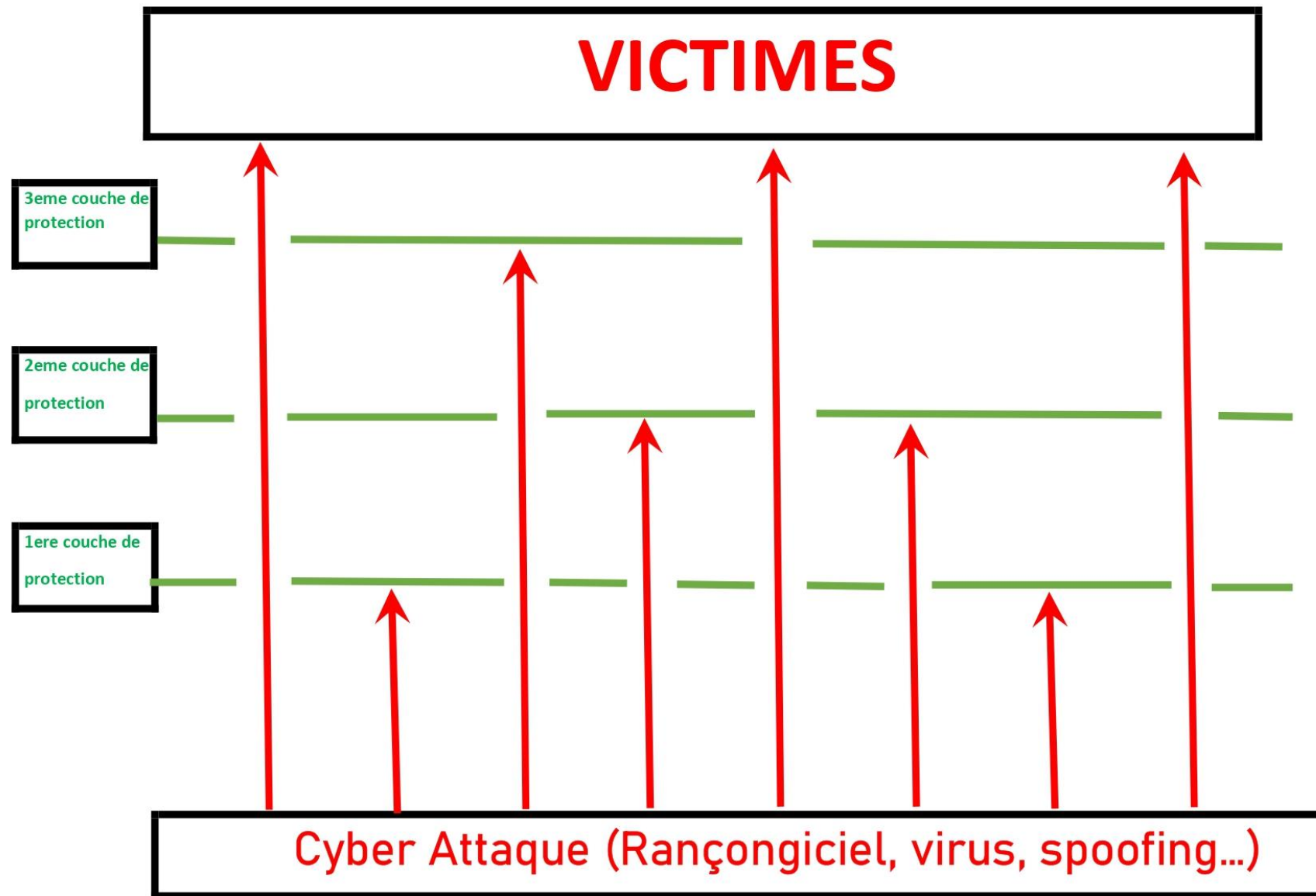


CNIL, Commission Nationale de l'Informatique et des Libertés



CyberMalveillance.gouv.fr : [Diagnostic et assistance aux victimes de cybermalveillance](https://www.cybermalveillance.gouv.fr/)





A person wearing a grey hoodie is sitting at a desk, their face obscured by a black rectangle. They are looking at a laptop screen, which is also blacked out. The background is a light grey wall covered in a pattern of small, glowing blue dots, resembling a digital or binary theme. The overall image has a dark, moody aesthetic.

<https://www.youtube.com/watch?v=ud-5lpUIDnM>

A person wearing a grey hoodie is sitting at a desk, their face obscured by a laptop screen. The background is a dark grey field filled with a pattern of light blue binary code (0s and 1s). The word "Questions" is written in a large, bold, black serif font, centered over the person's face and the laptop screen.

Questions

Introduction à la cybersécurité

1. La cybersécurité c'est quoi?

- Que se passe t'il sur internet en 1 minute
- Quelques chiffres sur les cyberattaques



2. Les différents types d'attaque, exemples concrets

- Cybercriminalité
- Atteinte à l'image
- Espionnage
- Sabotage
- C'est quoi une Cyberguerre?



3. Prévention, réflexes à avoir

- Prévention : que faire et comment?
- Que faire en cas d'attaque, comment réagir

