



# Cyber - (.\*)

25 octobre 2023



« Le seul système informatique vraiment sûr est un système éteint et débranché, enfermé dans un blockhaus sous terre, entouré par des gaz mortels et des gardiens hautement payés et armés.



Même dans ces conditions, je ne parierais pas ma vie dessus. »

Pr .Eugene Spafford  
Purdue University

## Quelques données

## 1.

## Une persistance de la menace



+ 43% de procédures judiciaires cyber ouvertes par la Gendarmerie nationale en 5 ans



Au total, plus de 500 000 procédures cyber depuis 2018



112 000 procédures judiciaires cyber en 2022



## Escroqueries

80% des procédures judiciaires cyber ouvertes en 2022 par la gendarmerie



## Haine en ligne et atteintes aux personnes

10% des procédures judiciaires cyber ouvertes en 2022



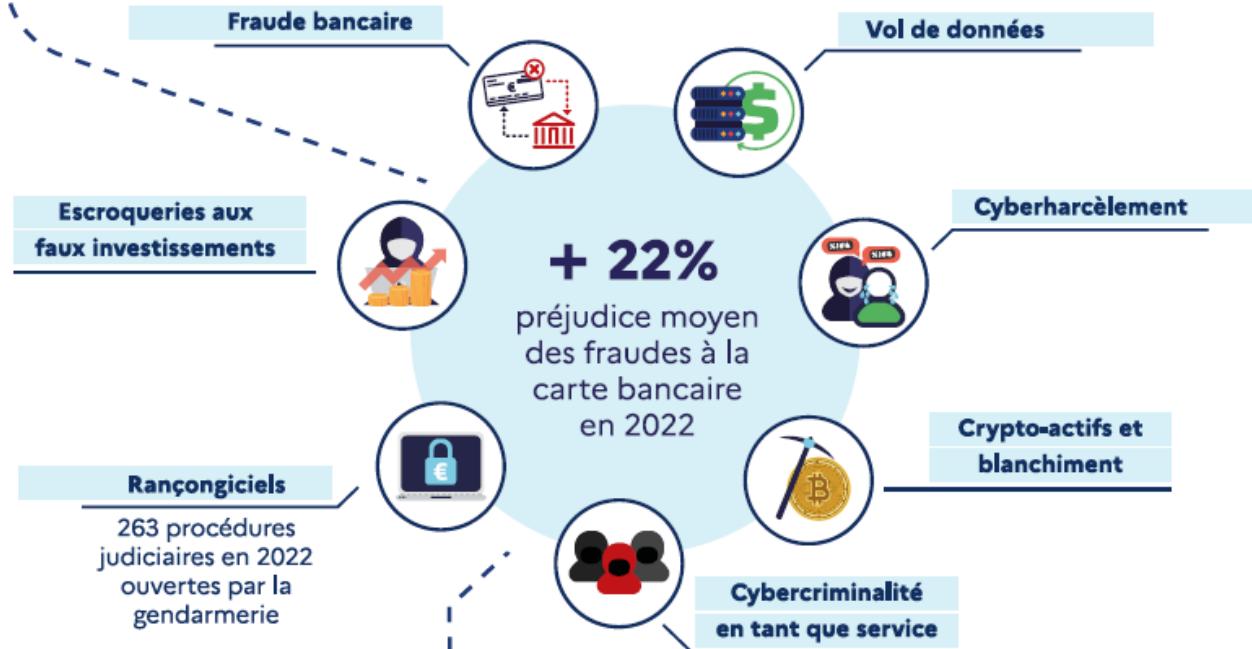
## Atteintes aux systèmes d'information

10 % des procédures cyber, en augmentation

# Quelques données

## 2.

### Des phénomènes cybercriminels récurrents et multiples



## LES PRÉJUDICES

En 2022

**161 350 088 €**

(contre 140 109 653,25 € en 2021)



hausse du préjudice total

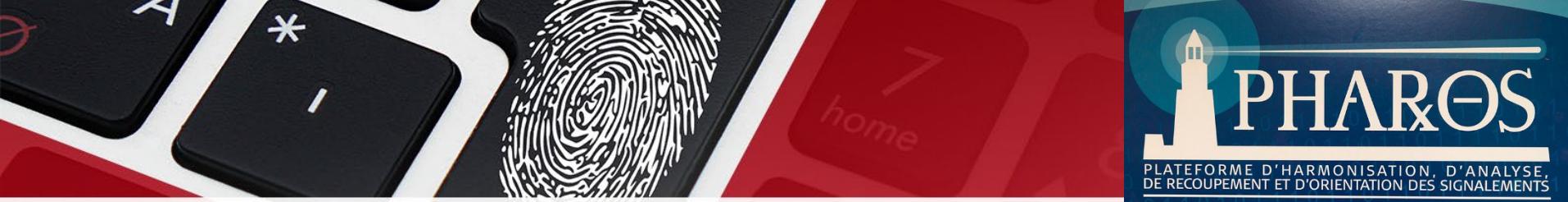
**+ 15 %**

*Le montant moyen s'est élevé à 529 € en 2022.*

# Quelques données

## Acteurs cybercriminels

	Individu seul	Bande organisée	Groupe en lien avec un Etat
Atteintes aux systèmes d'information et/ou atteintes aux biens	Pirates informatiques Cybermilitants ou hacktivistes Spécialistes des escroqueries Trafiquants, commerces illicites Intermédiaires, mules Néophytes ou <i>script kiddies</i>		
Atteintes aux personnes	Harceleurs / violences morales Proxénètes Pédocriminels		



# Plateforme d'harmonisation, d'analyse, de recouplement et d'orientation des signalements

<https://www.internet-signalement.gouv.fr/PharosS1>

#PHAROS  
LUTTE CONTRE  
LA RADICALISATION  
SUR INTERNET

LES SIGNALER

PHAROS

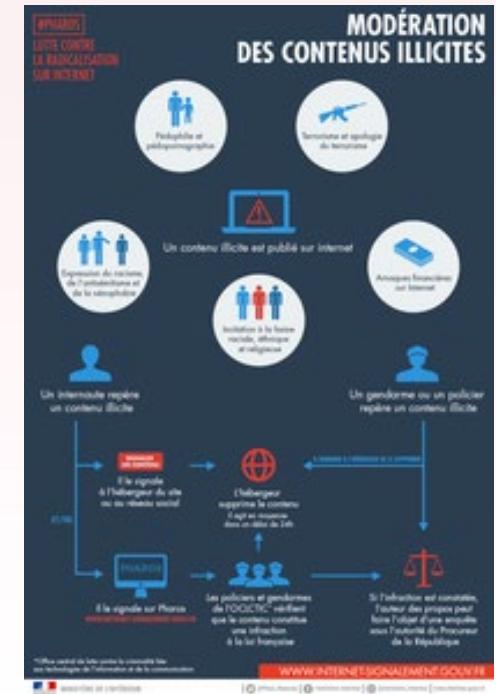
www.internet-signalement.gouv.fr

QUE FAIRE ?

NE PAS LES DIFFUSER

- Ne pas les partager
- Ne pas les liker
- Ne pas le retweeter

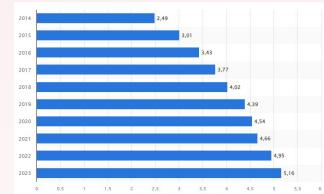
WWW.INTERNETSIGNALLEMENT.GOUV.FR



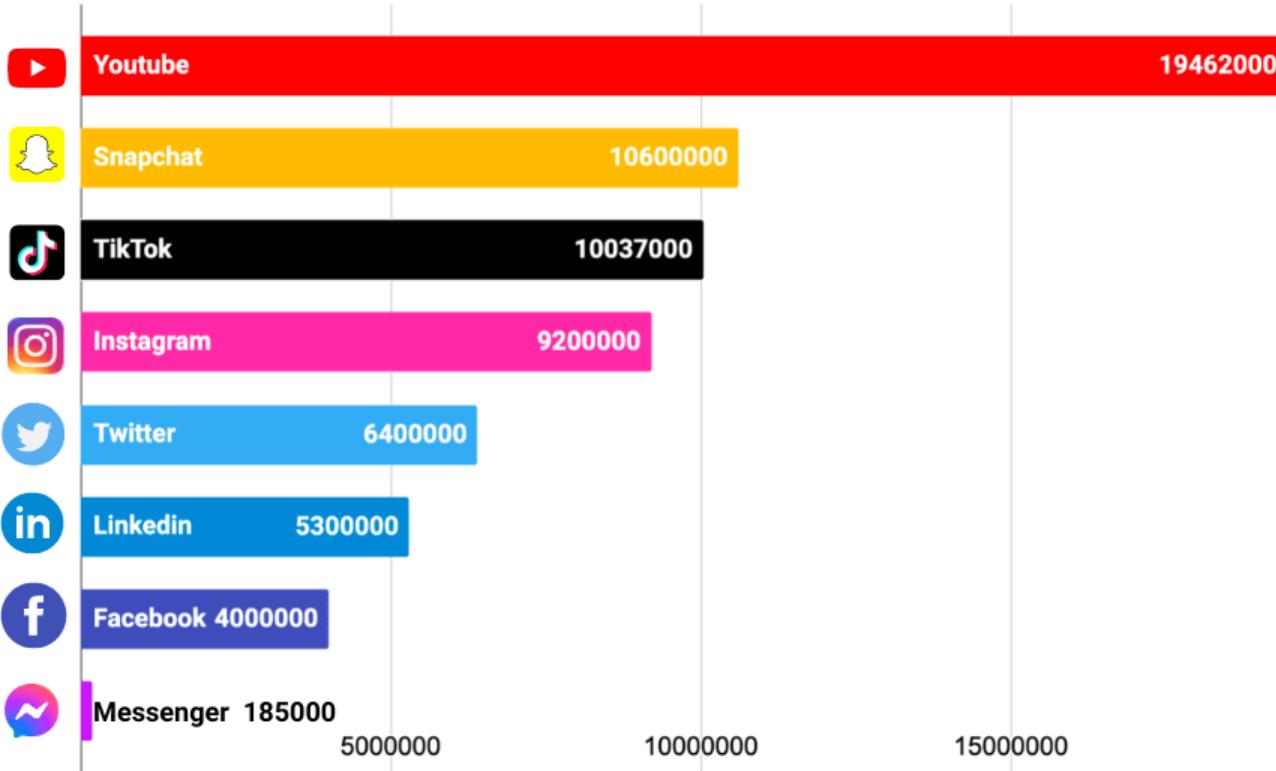
# Internet

## (chiffres janvier 2023)

- ↪ 5,16 milliards d'utilisateurs dans le monde (54,5 millions en France)
  - ↪ 32% des utilisateurs d'internet ont entre 25 et 34 ans, 19% entre 35-44 ans
  - ↪ 28,5 milliards d'appareils connectés dans le monde
  - ↪ Temps passé sur les réseaux sociaux par les 15-24 ans : **2h19 par jour**
  - ↪ **5h01** de temps passé en ligne par jour !
  - ↪ 1,4 milliard d'emails envoyés en France par jour (333,2 milliards d'emails dans le monde] et 85% sont des spams !
- ↪ 92,2 % des utilisateurs utilise le moteur de recherche de Google (100 Millions de Go indexés)



# Les utilisateurs de moins de 25 ans sur les réseaux sociaux (2023)



Une infographie



Sources : Meta ads, LinkedIn ads, Snapchat ads, Tik Tok ads, Twitter ads, Google ads



# L'actualité

The collage consists of several overlapping browser windows and tabs from French news sites:

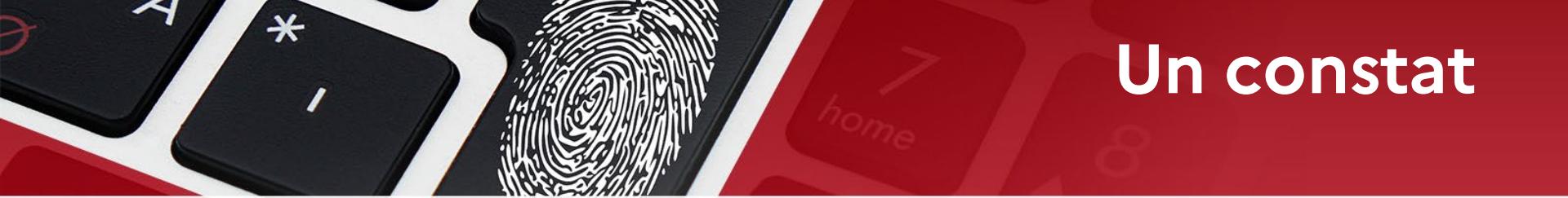
- Top Left:** L'EXPRESS - "Une cyberattaque 'chirurgicale' a visé des groupes français du BTP et de la sphère publique"
- Middle Left:** lemagit.fr - "Nouveau sabotage des infrastructures Internet en France"
- Center:** Challenge.fr - "Risque de coupure : Russie : les câbles sous-marins cherchent leur boussole"
- Bottom Center:** numerama.com - "Logiciel espion Pegasus : la Russie est officiellement accusée sur des malwares"
- Bottom Left:** lefigaro.fr - "Logiciel espion Pegasus : l'application a été confiée à un juge d'instruction"
- Right Side:** la-croix.com - "Cyberattaque : la CPI probablement victime d'une tentative d'espionnage en septembre"
- Bottom Right:** midi-libre.fr - "Nos systèmes ont été HS durant plusieurs heures : une cyberattaque 'très violente' contre l'aéroport de Toulouse"
- Far Right:** franceinfo.fr - "Le club de l'Asvel victime d'une cyberattaque"

The news items cover topics such as surgical cyberattacks on construction and public groups, new infrastructure sabotage in France, the International Criminal Court being targeted, the use of Pegasus spyware by Russia, and significant downtime at the Toulouse airport due to a violent cyberattack.



# Des faits (récents) en France

- ⇨ des logiciels ou matériel espions
  - ⇨ des faits de guerre et de désinformation
  - ⇨ des sabotages
- 
- ⇨ des vols de données
  - ⇨ des demandes de rançon (ransomware)



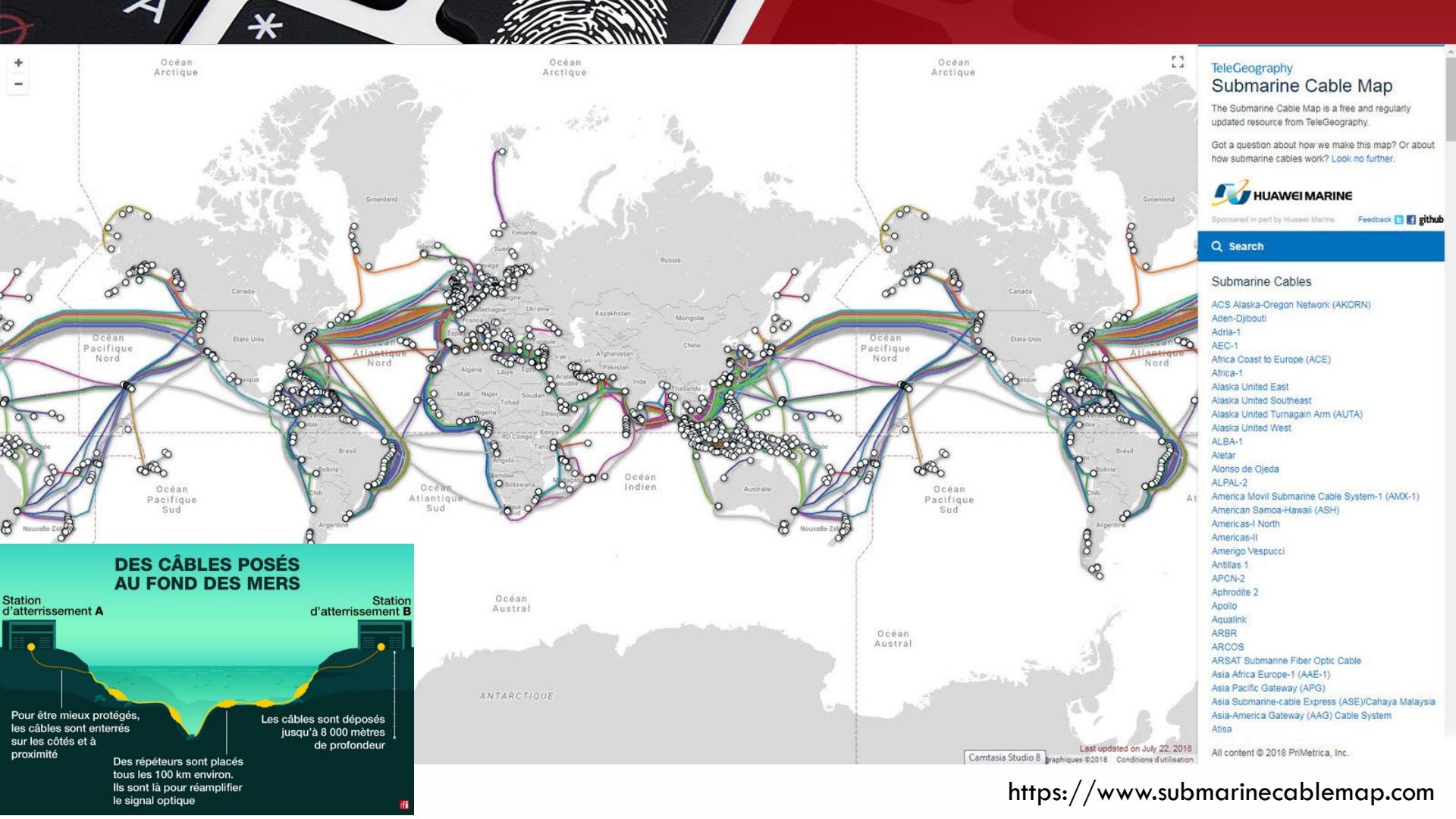
# Un constat

- ☞ Une motivation principale : **l'argent**  
**(1 280 milliards de \$ générés / an)**
- ☞ Un levier majeur : la mise en **confiance**

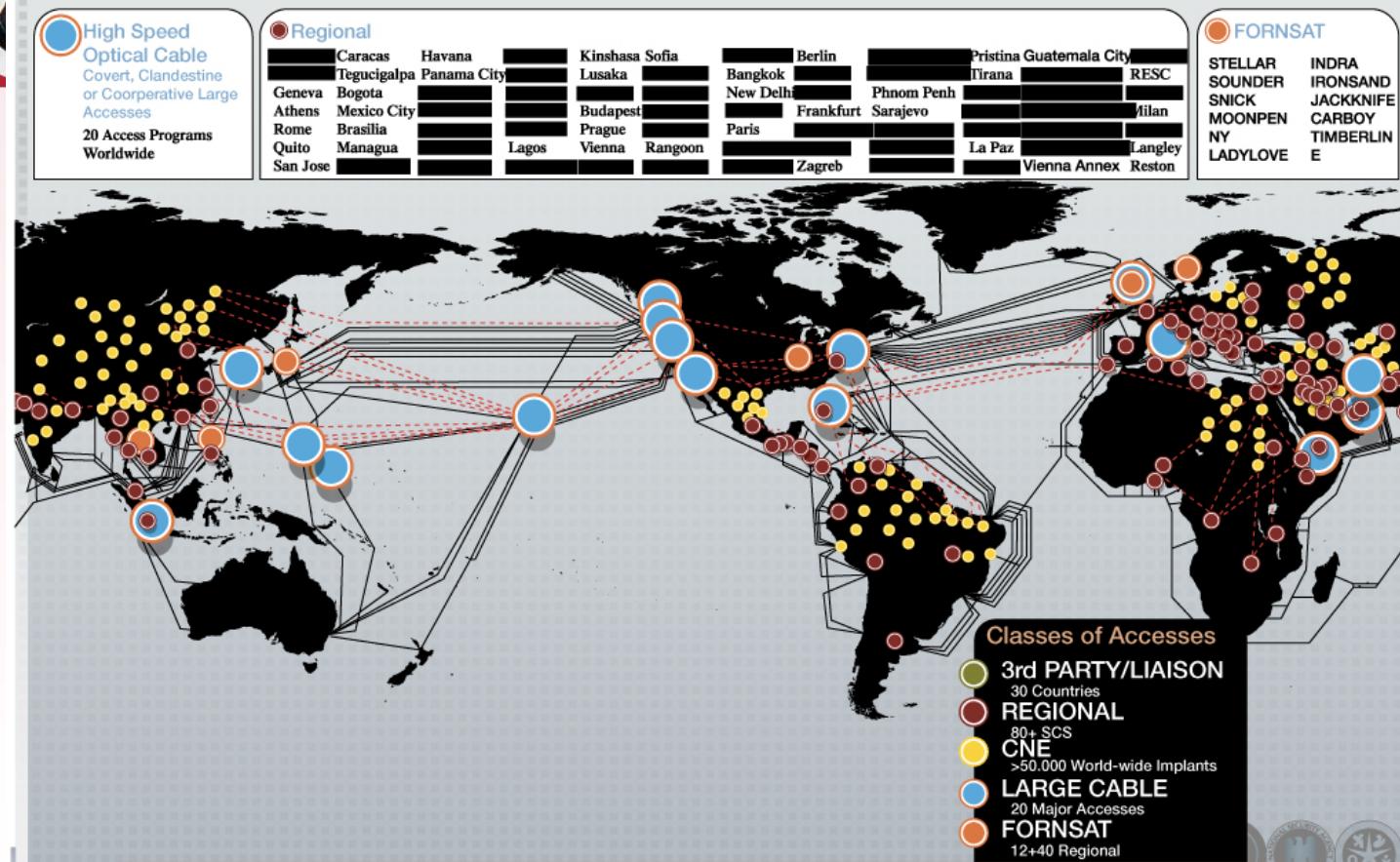


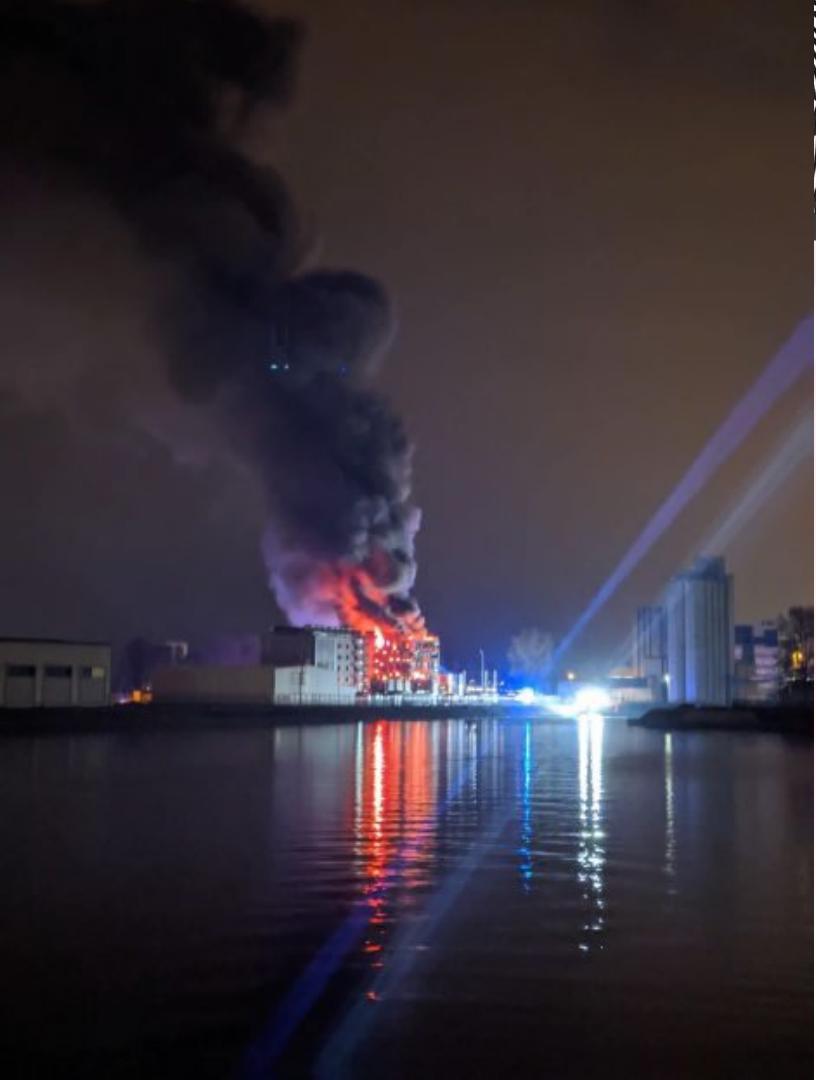
# Un constat

➡ Confiance dans les **réseaux** utilisés (infrastructure)



# Driver 1: Worldwide SIGINT/Defense Cryptologic Platform





**Incendie OVHCloud (Strasbourg) : 9-10 mars 2021**  
→ 3,6 millions de sites impactés





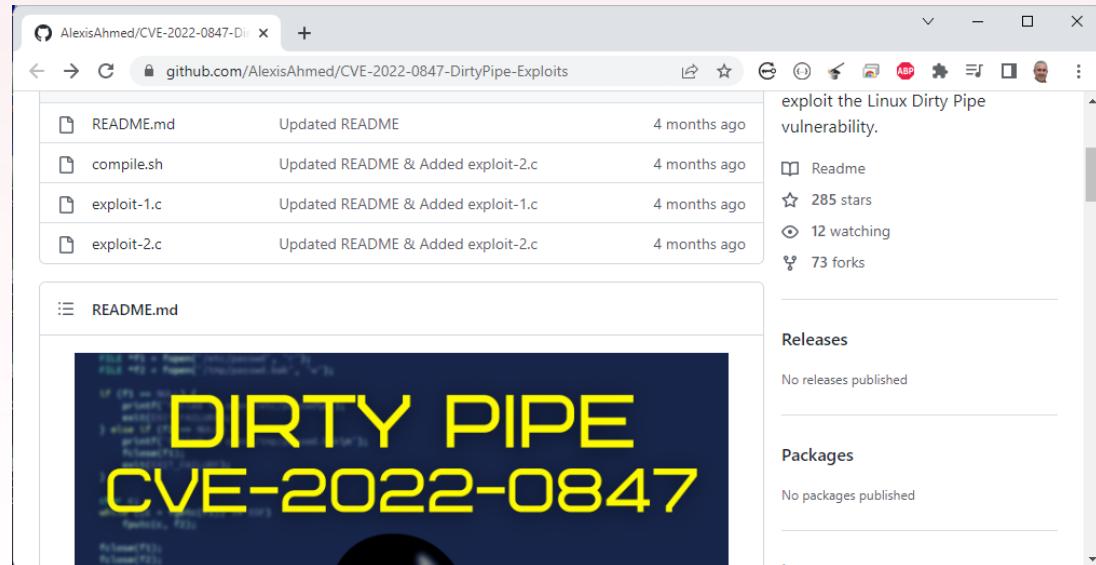
# Un constat

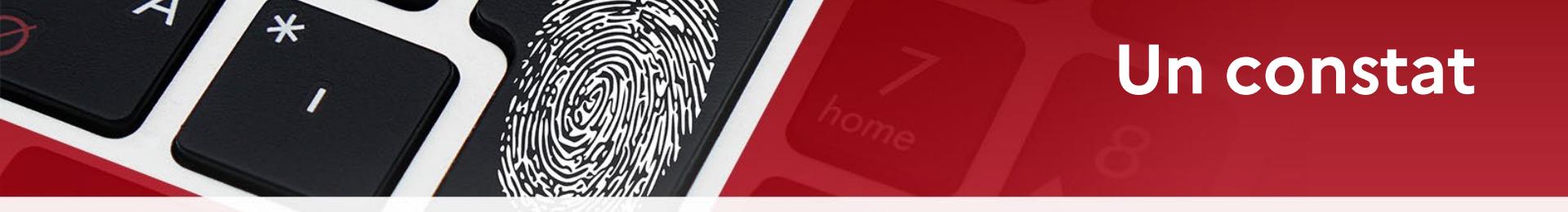
- ☞ Confiance dans les **réseaux** utilisés (infrastructure)
- ☞ Confiance dans les **machines** (PC, smartphones, ...)

# Types of malware



- Des « *exploits* » liés à la qualité du code (CVE – Common Vulnerabilities and Exposures)





# Un constat

- ☞ Confiance dans les **réseaux** utilisés (infrastructure)
- ☞ Confiance dans les **machines** (PC, smartphones, ...)
- ☞ Confiance dans les **personnes** derrière les machines

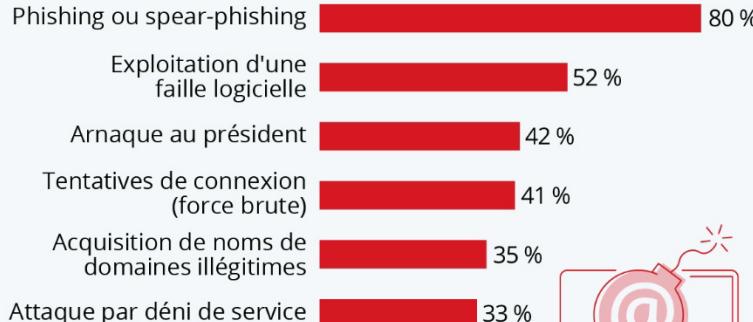


*"On the Internet, nobody knows you're a dog."*

Peter Steiner, New Yorker, 05/07/1993

# Les cyberattaques les plus courantes contre les entreprises

Types d'attaques les plus courants constatés par les entreprises françaises en 2020 \*



## Principales conséquences des attaques :



\* Plusieurs réponses possibles, sélection des plus fréquentes. Les entreprises ciblées ayant répondu à l'enquête ont subi en moyenne 3,6 attaques et 2,3 conséquences.

Sources : CESIN, OpinionWay

# Un constat

## TYPES OF CYBER-ATTACKS

### PHISHING

- Whale Phishing
- Spear Attack
- Pharming

### MAN-IN-THE-MIDDLE ATTACK

- Session Hijacking
- IP Spoofing
- Replay

### SQL INJECTION THREAT

### CROSS-SITE SCRIPTING (XSS)

### DISTRIBUTED DENIAL OF SERVICE ATTACK (DDOS)

### AI-POWERED ATTACKS

- Brute Force Guessing
- Dictionary Attack

### EAVESDROPPING ATTACK

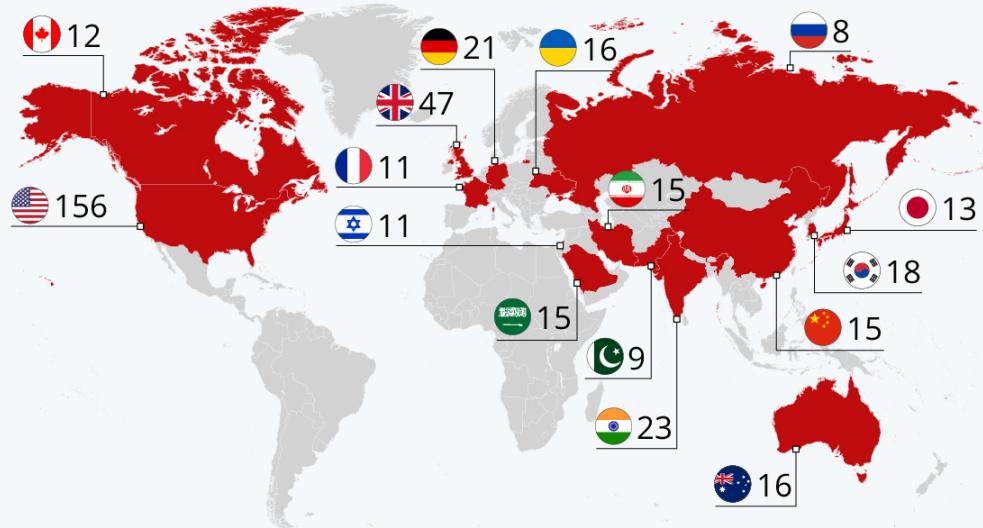
### DRIVE-BY ATTACK

### RANSOMWARE ATTACK



# Les pays cibles de cyberattaques majeures

Nombre de cyberattaques majeures (perte de plus d'1 million \$) ayant visé des gouvernements et entreprises tech/défense \*

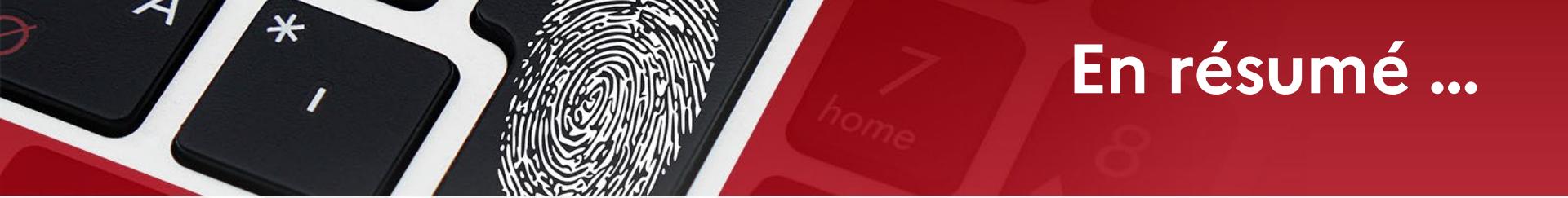


\* sur la période 2006-2020. Sélection des pays avec au moins 8 attaques de ce genre recensées.

Source : Specops Software

# Un constat



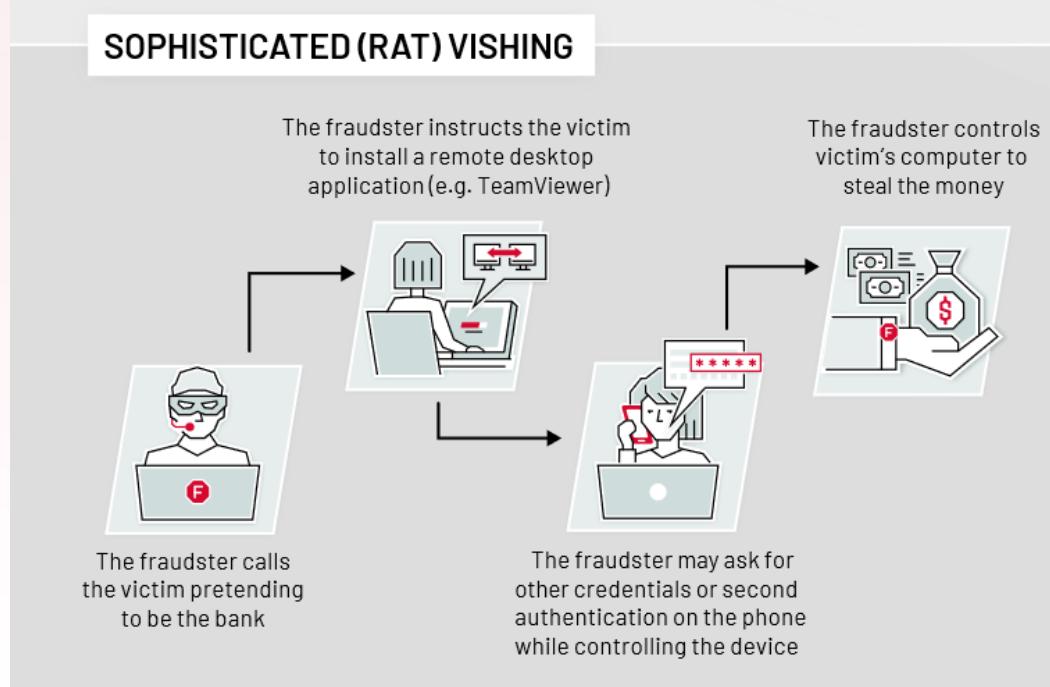


## En résumé ...

- ⇨ Comment se protéger en tant que citoyen et/ou professionnel ?
  - ⇨ Souvent, grâce au « **GBS** » !
  - ⇨ Et en respectant quelques règles ...

# En résumé ...

- Menace 1 : on parle beaucoup ... trop !



# Mots de passe



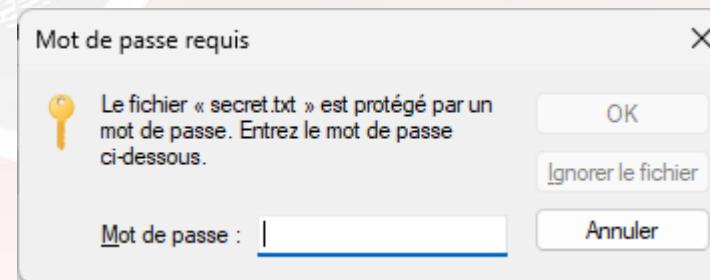
Login: admin  
Password: admin



NOMBRE DE CARACTÈRES	UNIQUEMENT DES CHIFFRES	LETTRES MINUSCULES	LETTRES MINUSCULES ET MAJUSCULES	LETTRES MINUSCULES ET MAJUSCULES + CHIFFRES	LETTRES MINUSCULES ET MAJUSCULES + CHIFFRES + CARACTÈRES SPECIAUX
4	IMMÉDIATEMENT	IMMÉDIATEMENT	IMMÉDIATEMENT	IMMÉDIATEMENT	IMMÉDIATEMENT
6	IMMÉDIATEMENT	IMMÉDIATEMENT	IMMÉDIATEMENT	1 sec	5 sec
8	IMMÉDIATEMENT	5 sec	22 min	1 heure	9 heures
10	IMMÉDIATEMENT	58 min	1 mois	7 mois	5 ans
12	45 sec	3 semaines	300 ans	2000 ans	34 000 ans
14	41 min	51 ans	800 000 ans	9 millions d'années	200 millions d'années

\*source : SCSP Community (Seasoned Cyber Security Professionals)

# Démo : « Force brute »



```
truillet@Enkidu: ~/demo_cyber$ fcrackzip -u -c a -p aaaa secret4.zip

PASSWORD FOUND!!!!: pw == pass
truillet@Enkidu:~/demo_cyber$ |
```

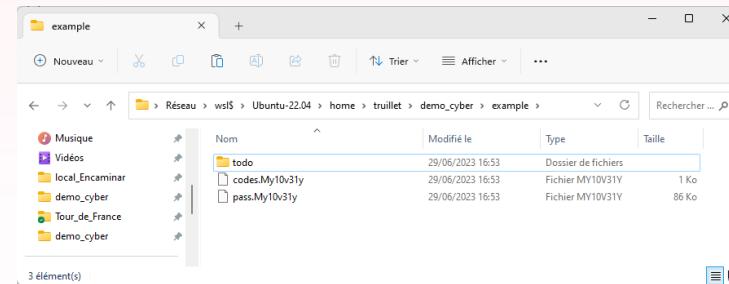
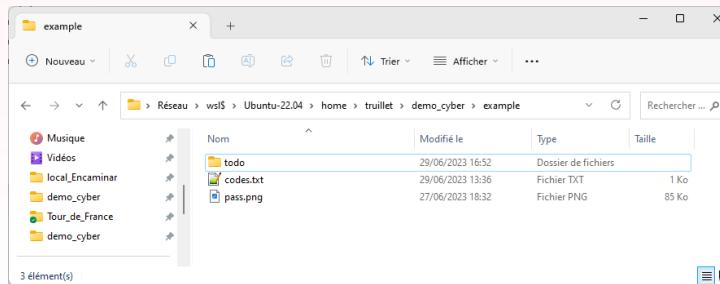
# En résumé ...

## • Menace 2 : on clique beaucoup (trop) ...

### Comment fonctionne une attaque de ransomware



# Démo : ransomware



```
illet@Enkidu:~/demo_cyber$ python3 Ransom.py
```





# SMiShing



+33 6 14 57 48 50

Bonjour Philippe, votre commande a ete livree  
le 13.10.2021 au point de collection. Voir la ou  
vous pouvez prendre vos colis:  
[ytov.me/9Ygnl2](https://ytov.me/9Ygnl2)



+33 7 44 52 26 06

Votre solde C.P.F. a ete mis a jour !  
Consultez votre solde et reclamez votre  
formation integralement financee.  
--> <https://cutt.ly/ZRyl89R>  
NoPub=stop



+33 6 01 35 08 93

Ameli : Votre nouvelle carte vitale est  
disponible. Veuillez suivre les  
indications ci-dessous pour  
confirmer l'expédition : <https://fr-macartevitale.com/>

# Phishing

Eichier Edition Affichage Aller à Messages Evènements et tâches Outils Aide

Courrier entrant - Philippe.Trulliet [MESSAGE MARQUE SPAM : ]

Relever Écrire Messagerie instantanée Adresses Étiquette Filtre rapide Rechercher <Ctrl+K> Config

De Cdiscount <anniversaire@cdiscoun.com>

Sujet [MESSAGE MARQUE SPAM : MOYEN] Félicitations ! Vous avez été choisi pour gagner un smartphone .

Pour philippe.truillet@irit.fr

06:39



## Félicitations !

Aujourd'hui, **28-10-2021**, nous célébrons donc le 22e anniversaire de notre activité en ligne. Cette journée auquelles on sélectionne 1000 clients pour recevoir des cadeaux. Félicitations vous faites partie des personnes sélectionnées pour recevoir un cadeau de notre part

Cela ne vous prendra qu'une minute et vous pourrez choisir n'importe quel cadeau parmi nos **Articles** disponible En stock cadeaux !

[Dépêchez-vous, le nombre d'offres gratuites en stock disponibles est limité !](#)

**Il reste une quantité d'articles limite en stocks.**

Veuillez ajouter votre choix au panier et valider votre adresse de livraison afin de recevoir votre cadeau sous 2 à 3 jours ouvrés.

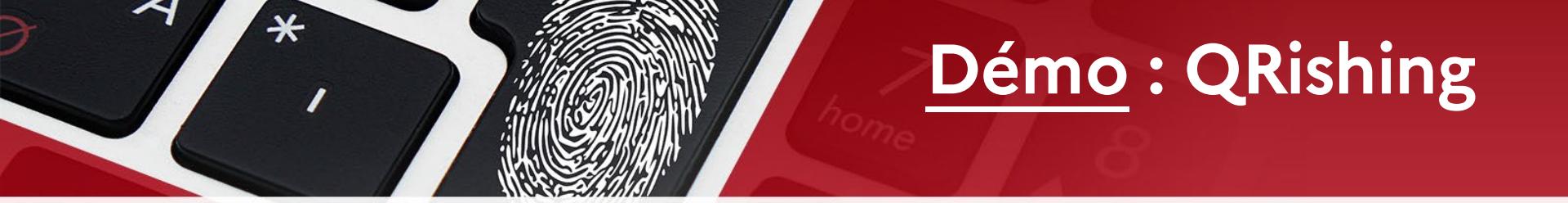
Merci pour votre confiance.

# Phishing

This screenshot shows a browser window with a URL starting with "cdiscount-deal.com/web/". The page content is identical to the official Cdiscount website, featuring a header with the Cdiscount logo and a search bar. The main content area displays a "Félicitations!" message and a promotional offer for a Samsung Galaxy S20 FE smartphone. The offer includes a price of 949€00, a note about free shipping, and a button to add the item to the cart. On the left side, there are sidebar filters for categories like "CATEGORIES", "AFFINER PAR", and "Pays de Livraison". The overall layout is designed to trick users into believing they are on the legitimate Cdiscount site.

This screenshot shows the official Cdiscount website at "cdiscount.com". The homepage features a large banner with the text "ALORS ON JOUE ?" and "DES OFFRES POUR LES PETITS ET LES GRANDS ENFANTS", advertising up to 60% off for children's products. Below the banner, there are sections for "Univers playmobil" and "Univers Lego". At the bottom, there are banners for "L'OFFRE DU JOUR!" featuring a Samsung TV and "VENTE FLASH" with a 72H offer. The top navigation bar includes links for "Tous nos rayons", "Voyages", "Mes Courses", "Forfait Mobile", "Spectacles", "Occasion", and "Mutuelle". The right side of the page shows a red decorative graphic with the word "home".

# Démo : QRishing



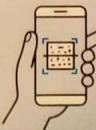
To celebrate and thank our supporters, we are giving away a

## Free Wireless Bluetooth Earbuds

*Shipping and handling on us too!*

\*Limited quantities. Promotion valid while supplies last. You will be asked to present a valid Amazon order ID. Not valid with other promotions.

To get started just scan the QR CODE



A small 'NEW' badge is visible in the bottom right corner of the QR code area.

SCAN  
ME!

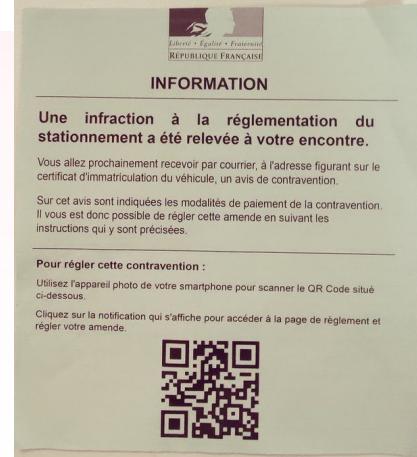
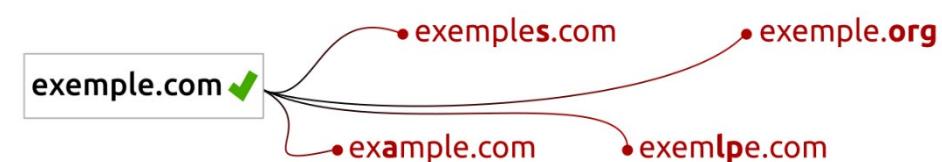


- typosquatting
- cybersquatting

#### Caractères autorisés pour la réservation d'un

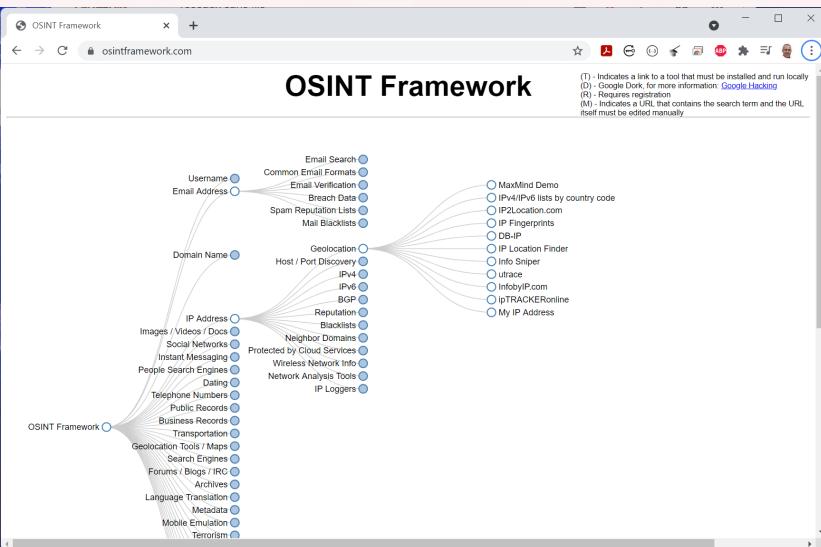


## Différence entre **Google** et **Google ?**



# En résumé ...

- Menace 3 : on laisse beaucoup (trop) de traces  
(\rightarrow OSINT)



The screenshot displays three separate web pages:

- PimEyes Face Recognition Search:** A browser window showing the PimEyes website with a blue header. It features a "Face Search Engine" and "Reverse Image Search" section. Below is a form with a camera icon, a "Upload a photo" button, and a search icon. To the right is a cartoon illustration of a person holding a smartphone with a woman's face on its screen.
- The role of OSINT in the war in Ukraine:** A browser window showing a comment from "army-technology.com" dated May 6, 2022, last updated on May 13, 2022, at 1:11pm. The comment discusses how OSINT has helped the Ukrainian Armed Forces through the fog of war by disclosing Russian actions.
- GlobalData:** A browser window showing the GlobalData logo and social media icons for LinkedIn, Twitter, and Facebook.



- Données EXIF (géoloc)
- Réseaux sociaux,
- ...

Afficher Exif en ligne, supprimer +

verexif.com/fr/ver.php

EXIF DONNÉES

Fabricant de la caméra : Xiaomi  
Modèle de caméra : Redmi Note 7

Date et heure : 2021/04/03 17:14:11

Résolution : 4000 x 2250

Il a utilisé Flash : No

Distance focale : 4.7mm

Temps d'exposition : 0.0003 s (1/2904)  
Ouverture : f/1.8

ISO equiv. : 250

Balance des blancs : Auto

Mode de mesure : center weight

Latitude GPS : N 43° 27' 11.4084"

Longitude GPS : E 1° 12' 54.1007"

Altitude GPS : 254.11m

JPEG Quality : 78

[Retirer Exif](#) [Une autre photo](#)

LIEU OÙ LA PHOTO A ÉTÉ PRISE

43°27'11.4"N 1°12'54.1"E  
377 Rte de Saint-Clar, 31600 Lherm

[Itinéraires](#) [Agrandir le plan](#)

Map showing the location of the photo taken at 43°27'11.4"N 1°12'54.1"E, 377 Rte de Saint-Clar, 31600 Lherm, France. The map includes major cities like Toulouse, Montauban, and Albi, and regional features like the Parc naturel régional des Grands Causses.

# Démo : GeolINT



VIAPROTECT

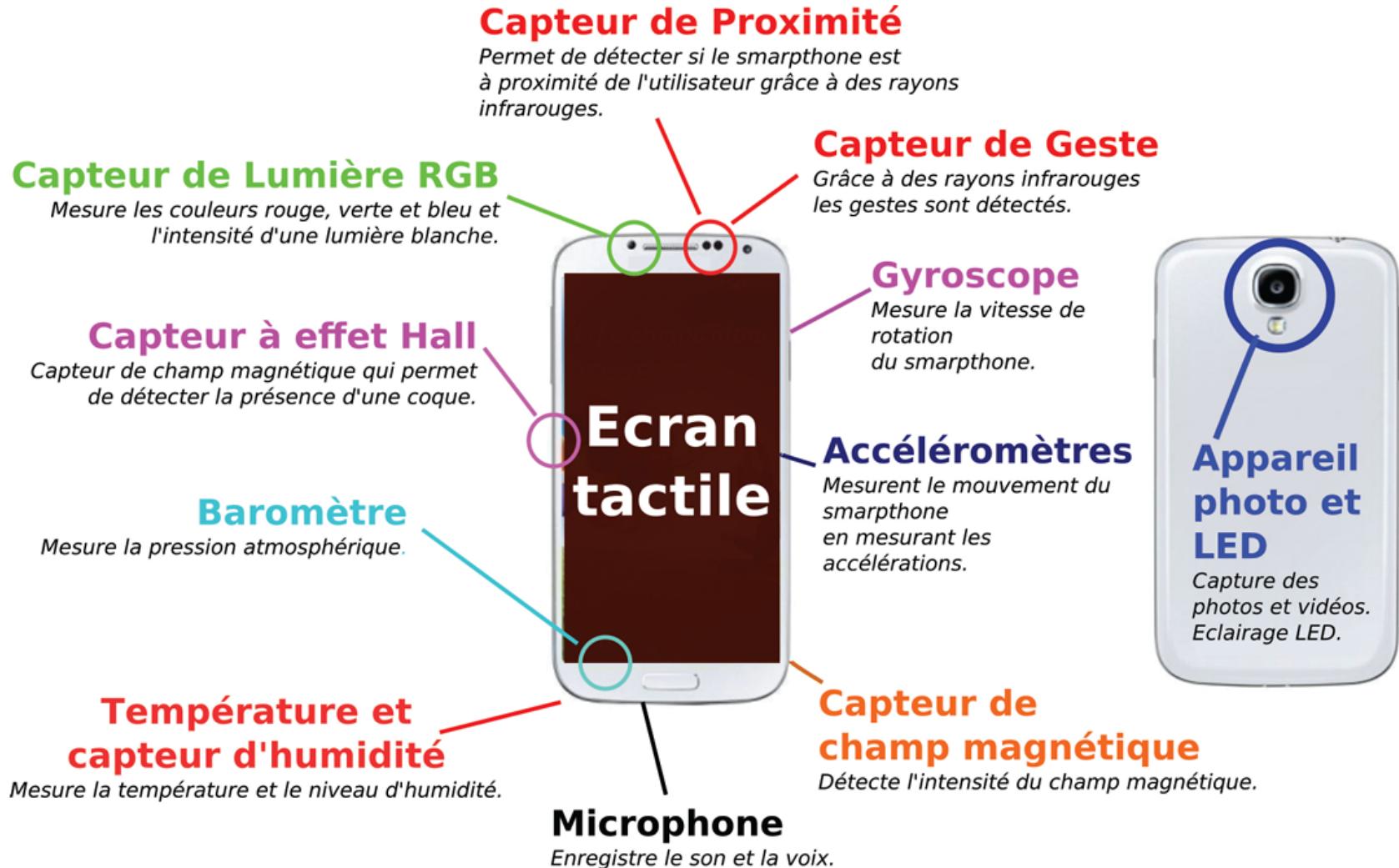
- Où est-ce ?
  - Indice(s) dans l'image
  - Outils
    - <https://overpass-turbo.eu>
    - Google Maps



# En résumé ...

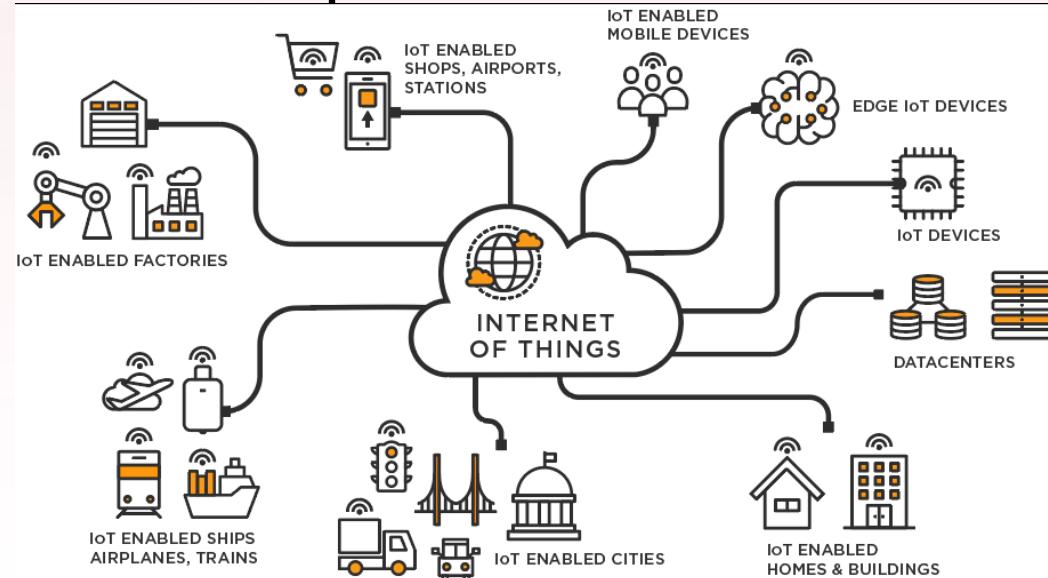
- **Menace 4 : notre « double » numérique ... Le smartphone !**
  - Il contient notre vie privée et notre vie publique
  - Bourré de capteurs
  - Facile à pirater (spyware)





# En résumé ...

- Menace 5 : l'IoT
  - des milliards (25 ?) de capteurs disséminés
  - des problèmes de sécurité





Mobile

Fonctionnalités

Inscription

Blog

S'inscrire

Se connecter

## Carte mondiale des activités

Chercher



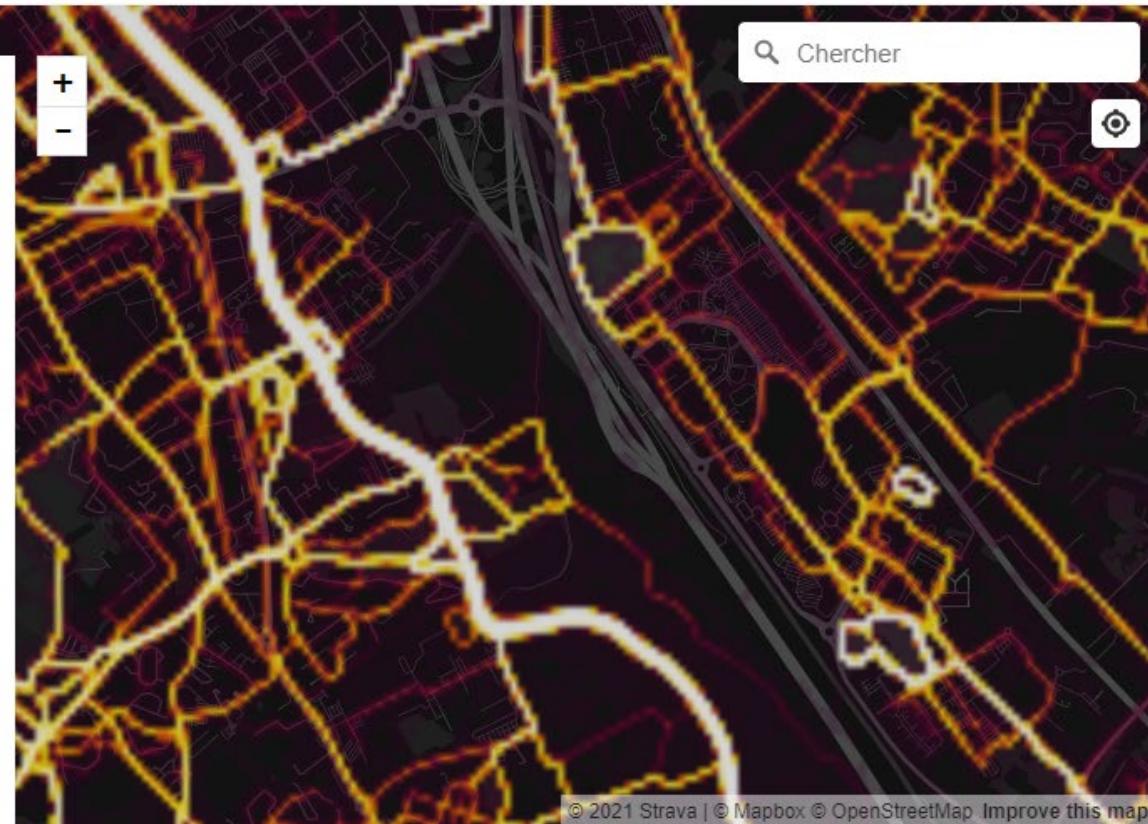
### Couleur de la carte des activités

### Type d'activité

### Opacité

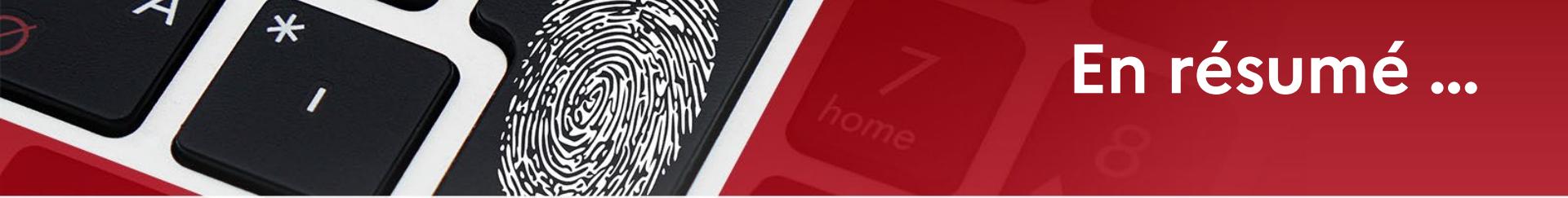
### Couches

### Styles de carte



# En résumé ...

## • Menace 6 : les IA génératives et deepfakes



ChatGPT

+ New chat

Today

Cadets de la gendarmerie

En tant qu'intelligence artificielle, je n'ai pas d'opinions personnelles ni de sentiments. Cependant, je peux vous fournir des informations générales sur les cadets de la gendarmerie.

Les cadets de la gendarmerie sont des étudiants qui suivent une formation spécifique au sein de l'école de gendarmerie pour devenir gendarmes. Ils sont recrutés après avoir réussi un concours et doivent remplir certaines conditions, telles que l'âge et le niveau d'éducation requis.

La formation des cadets de la gendarmerie comprend des cours théoriques et pratiques sur divers sujets tels que le droit, la sécurité, la gestion des crises, les techniques d'enquête, la maîtrise des armes à feu, etc. Ils acquièrent également une expérience pratique lors de stagiaires sur le terrain.

Les cadets de la gendarmerie sont formés pour assumer des responsabilités dans le maintien de l'ordre, la sécurité publique et la lutte contre la criminalité. Ils peuvent être déployés dans différentes régions et participer à des missions variées, allant de la surveillance de la circulation routière à l'intervention lors d'incidents graves.

Dans l'ensemble, les cadets de la gendarmerie sont des futurs professionnels de l'application de la loi qui reçoivent une formation complète pour remplir leurs fonctions. Ils jouent un rôle important dans le maintien de la sécurité et de l'ordre public.

Regenerate response

Send a message

Philippe Truillet

Free Research Preview. ChatGPT may produce inaccurate information about people, places, or facts. ChatGPT May-2d Version

Deepswap - AI Face swap App en +

DeepSwap

Face swap Features Tarification Se connecter Théâtre Français

FIRST SUBSCRIPTION up to 50% off

54 : 10 : 41 Min Sec MS

Deepswap - Fabricant de Faceswap pour l'échange de visage en ligne

Deepswap est une application faceswap en ligne pour générer des vidéos, des photos et des GIF's d'échange de visage. Plus de 150 millions d'utilisateurs font des faceswaps ici, y compris des faceswaps de célébrités, des échanges de sexe, des mèmes, etc.

Faceswap Maintenant →

Obtenez la Prime >

Nous Contacter

cadet de la gendarmerie analyse x

Microsoft Bing

Créateur d'image par DALL-E

cadet de la gendarmerie analysant un ordinateur

Créer une image Bing | 1024 x 1024 (px) | 8 x 4 h

Partager Enregistrer Télécharger

cadet de la gendarmerie analysant un ordinateur

Confidentialité et cookies Stratégie de contenu Conditions d'utilisation Votre avis

© 2023 Microsoft Corporation

# Démo : Image Creator

- Algorithme « Stable Diffusion » : Dall-E, MidJourney, ...



A screenshot of a web browser window titled "Créateur d'image à partir de Mic" with the URL "bing.com/images/create". The page features a search bar and a "Créateur d'image par DALL-E" button. Below the search bar, there's a message: "Vous voulez voir comment fonctionne le Créateur d'image ? Sélectionnez Surprise Me, puis Crée...". A large section titled "Démarrage rapide de votre créativité" suggests prompts like "Les mots corrects sont difficiles à trouver. Voici quelques idées pour vous permettre de commencer." It includes a "Preview" button and several thumbnail images for inspiration: a landscape with hot air balloons, a classical statue, and tropical foliage. At the bottom, there are links for "Confidentialité et cookies", "Stratégie de contenu", "Conditions d'utilisation", "Votre avis", and "Créé avec Microsoft". A "Commentaires" button is also present.



# En résumé ...

- Les techniques utilisées sont nombreuses
- Elles évoluent avec la technologie et les usages
- Un mot d'ordre :  
**la vigilance**



# Des liens



<https://www.cnil.fr/fr/securite-des-donnees>

→ 3 niveaux

**PROTECTION DES DONNÉES  
ADOPTEZ LES 6 BONS RÉFLEXES**

**1 NE COLLECTEZ QUE LES DONNÉES VRAIMENT NÉCESSAIRES POUR ATTEINDRE VOTRE OBJECTIF**

Les données sont collectées pour un but bien déterminé et limité. Elles doivent être collectées de manière nécessaire, c'est-à-dire de façon inséparable du but poursuivi. Le principe de finalité limite la manière dont vous utilisez les données collectées. Il est donc important de faire clairement la distinction entre le but et celle la collecte de données : « ne casse pas l'arbre pour atteindre les fruits ». Les données doivent être collectées pour des fins et des usages données exactement nécessaires à la finalisation de votre objectif.

**2 SOYEZ TRANSPARENT**

Les administrés doivent conserver la nature des données qu'ils conservent. Cela suppose que l'administré informe ses administrés de ce que sera fait de leurs données dès leur collecte. Lorsque les données sont collectées, il faut être transparent sur leur utilisation et leur finalité. Les personnes doivent également être informées de leurs droits et des modalités d'exercice de ces droits.

**3 ORGANISEZ ET FACILITEZ L'EXERCICE DES DROITS DES ADMINISTRÉS**

Vous devez organiser des modalités permettant aux personnes de exercer leurs droits au sein de votre administration. Vous devez établir une procédure pour répondre aux demandes d'accès, de rectification, de suppression des données, voire d'opposition, soit à la demande d'un administré, soit à la demande d'un tiers. Un administré ne peut s'opposer à l'usage de ses données à des fins statistiques si ce dernier a donné son consentement à l'exception de l'obligation d'en informer l'autorité de la protection des données. Des droits doivent également être mis en place pour exercer ces droits.

**4 FIXEZ DES DURÉES DE CONSERVATION**

Vous ne pouvez pas conserver les données indéfiniment. La législation courante prévoit que le temps d'archivage soit proportionnel au temps nécessaire pour exercer les droits des personnes. Elles doivent être purgées par la suite, détruites, anonymisées ou archivées. Il existe des règles spécifiques applicables en matière de conservation des archives publiques.

**5 SÉCURISÉZ LES DONNÉES ET IDENTIFIEZ LES RISQUES**

Vous devez prendre toutes les mesures utiles pour protéger les données contre toute atteinte ou sécurité informatique, sécurisation des lieux, des bâtiments et des installations, sécurité des personnes, des habitations et droit d'accès à l'information. Les personnes doivent être informées de l'existence et de l'autorité de ces risques et accès aux données. Les personnes doivent être informées de la sensibilité des données ou des risques qui peuvent peser sur les personnes en cas d'incident de sécurité.

**6 INSCRIVEZ LA MISE EN CONFORMITÉ DANS UNE DÉMARCHE CONTINUE**

La conformité n'est pas prévue dans le cadre réglementaire. Elle dépend du bon respect au quotidien des règles de protection des données. Des procédures et mesures mis en œuvre. Vérifiez régulièrement la mise en œuvre de ces procédures et mesures. Les procédures et les mesures de sécurité mises en place sont bien respectées et adaptées si besoin.

**CNIL**  
COMMISSION NATIONALE  
INFORMATION & LIBERTÉS

[www.cnil.fr](http://www.cnil.fr)

# Des liens



## La Brigade Numérique

Signaler un contenu illicite : <https://www.internet-signalement.gouv.fr/PharosS1>  
Contacter la Gendarmerie : <https://magendarmerie.fr>



<https://www.cybermalveillance.gouv.fr>



<https://ssi.gouv.fr>

