



Cyber ... “*”

février 2022

Liminaire



« 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

[chiffres avril 2021]

↗ 53,8 millions d'internautes en France

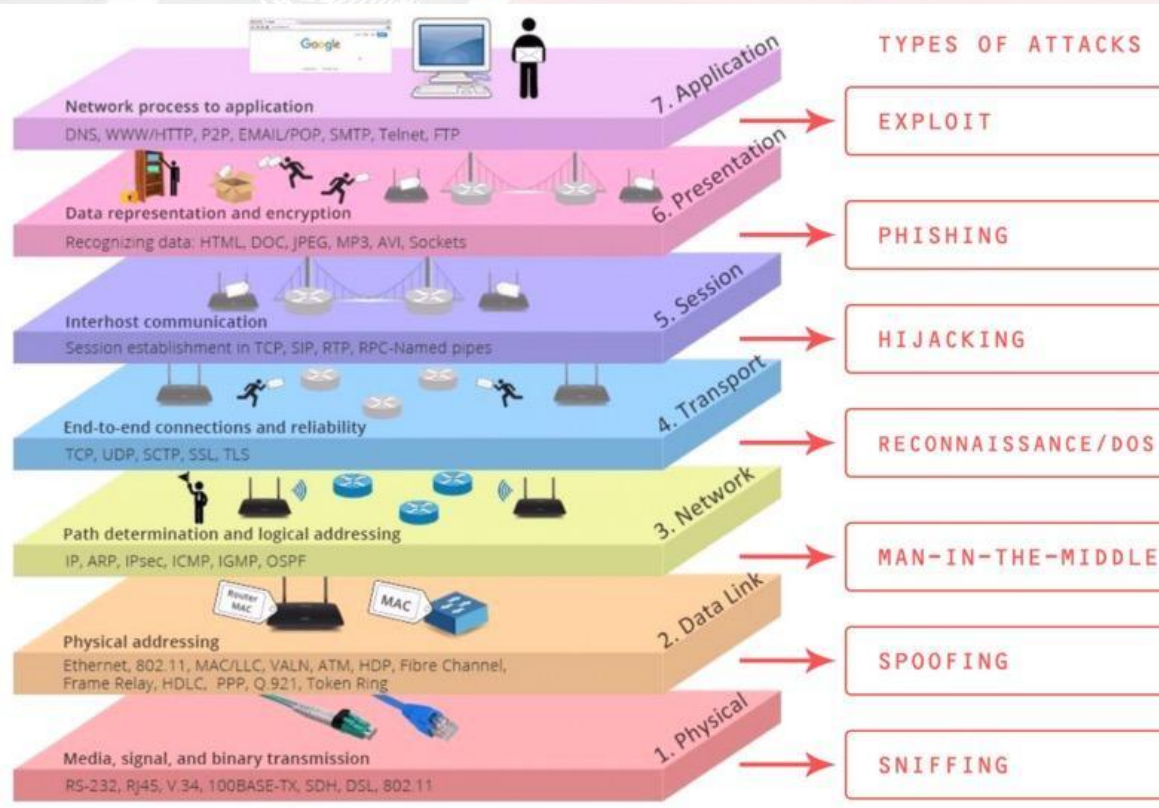
↗ Temps passé sur le web : **2h39 par jour**

↗ 1,4 milliard d'emails envoyés en France par jour [306,4 milliards d'emails dans le monde] et 85% sont des spams !

↗ 1 site internet sur 500 est infecté par un virus ou un malware

↗ Google bloque 10 000 sites /jour

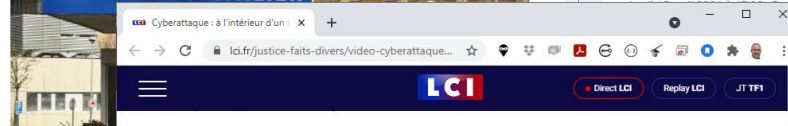
Internet



Partager



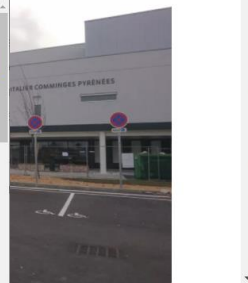
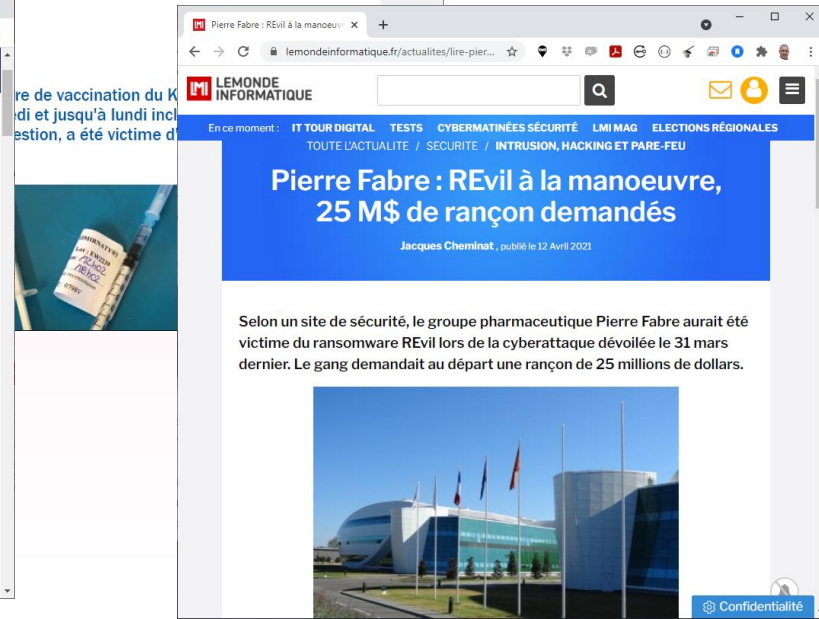
Depuis le début de la crise du Covid, on observe une recrudescence des cyberattaques contre des hôpitaux. Pourquoi ces établissements sont-ils spécialement pris pour cible par les hackers ? Entretien avec Jean-Marc Bourguignon de l'ONG Nothing to hide.



Cyberattaque : à l'intérieur d'un hôpital paralysé



CYBERCRIMINALITÉ – Victime d'une cyberattaque, le centre hospitalier de Dax fonctionne au ralenti. Des soins ont été reportés





Des faits [récents] en France

- ↔ Institut Pasteur [janvier 2021] : vol de données ?
- ↔ Hôpital de Dax [février 2021] : demande de rançon [*ransomware*]
- ↔ Hôpital de Villefranche-sur-Saône [février 2021] : demande de rançon [*ransomware* RYUK]
- ↔ Pierre Fabre [mars 2021] : demande de rançon [*ransomware*]
- ↔ Centre hospitalier de Saint-Gaudens [avril 2021] : demande de rançon [*ransomware*]
- ↔ Centre de vaccination de Berck/Mer [avril 2021] : « intrusion et propagation » [*ransomware* ?]



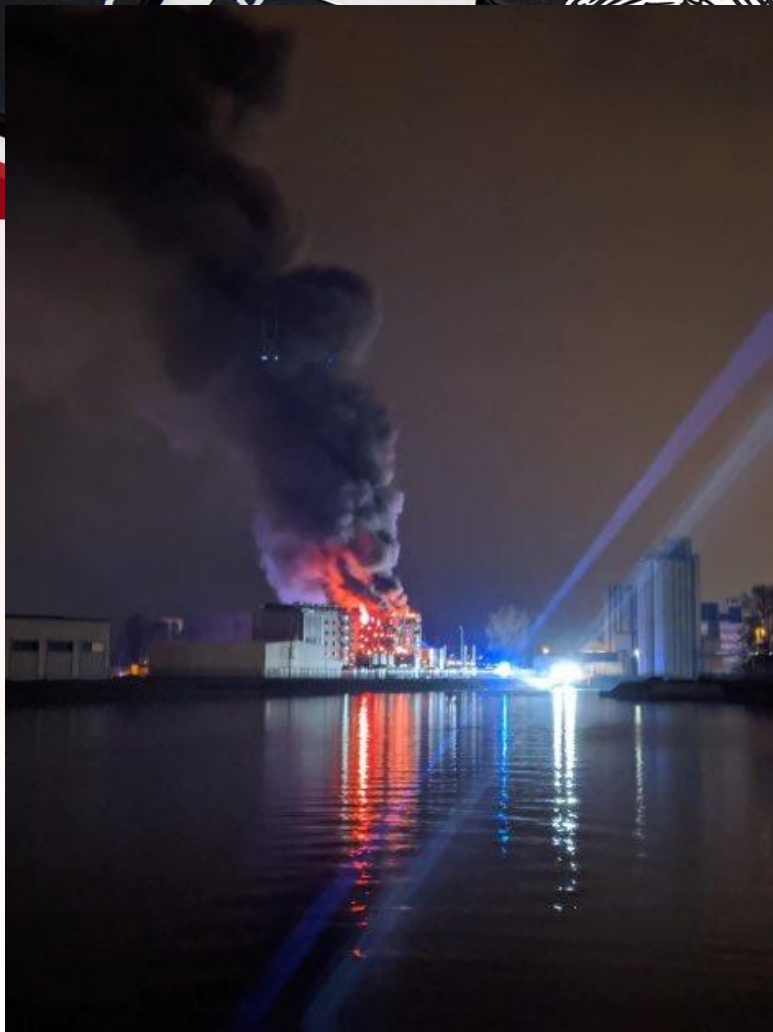
Un constat

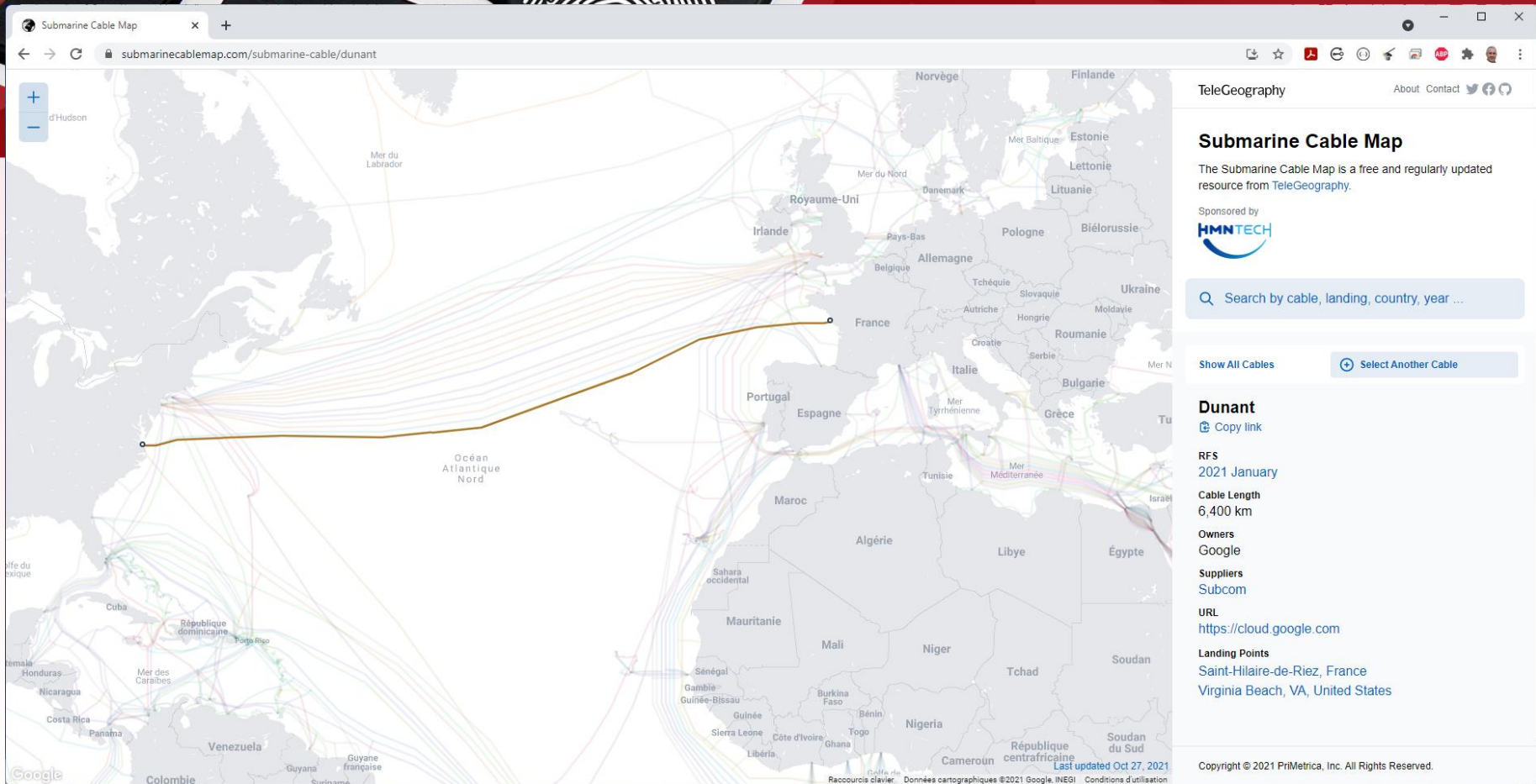
- Une motivation primordiale : **l'argent**
- Un levier majeur : **la mise en confiance**

Un constat



• **Confiance** dans les **réseaux** utilisés [infrastructure]





<https://www.submarinecablemap.com>

Un constat



- ↗ **Confiance** dans les **réseaux** utilisés [infrastructure]
- ↗ **Confiance** dans les **machines** [PC, smartphones, ...]

Types of malware



Un constat



- **Confiance** dans les **réseaux** utilisés [infrastructure]
- **Confiance** dans les **machines** [PC, smartphones, ...]
- **Confiance** dans les **personnes** derrière les machines

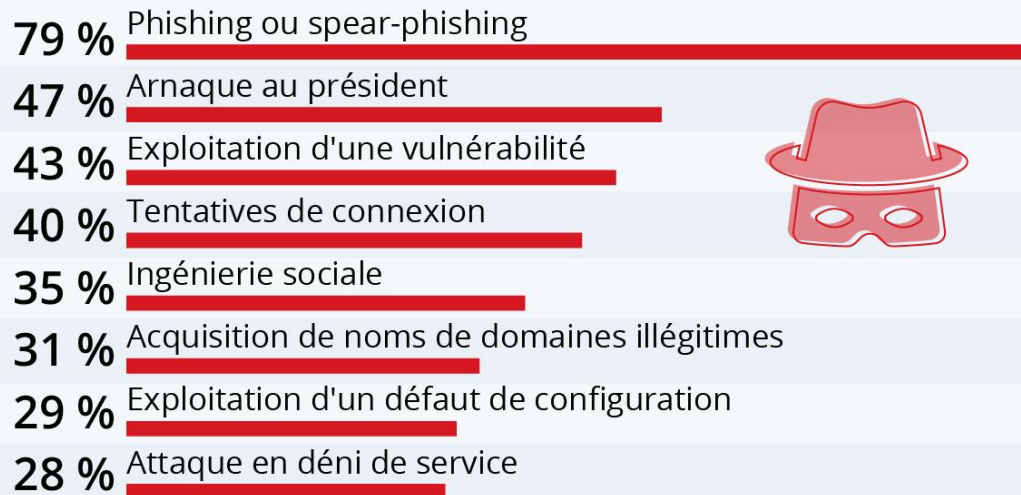


"On the Internet, nobody knows you're a dog."

Peter Steiner, New Yorker, 05/07/1993

Les cyberattaques les plus courantes contre les entreprises

Types d'attaques les plus constatés par les entreprises françaises en 2019 *



* Plusieurs réponses possibles, sélection des résultats supérieurs à 20 %.
En moyenne : 3,9 types d'attaques constatés parmi les entreprises ayant subi au moins une attaque.

Sources : CESIN, OpinionWay

Un constat



En résumé ...

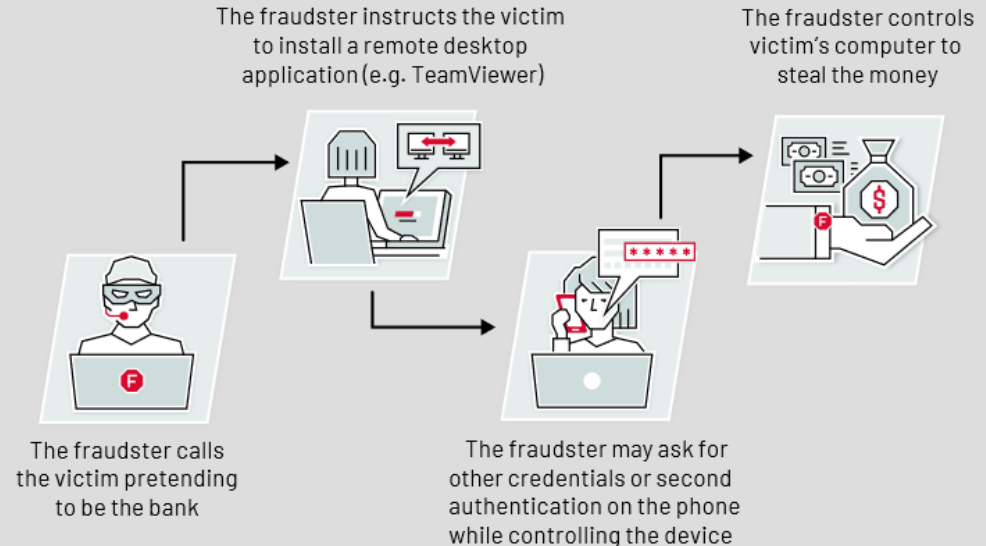
- Comment se protéger en tant qu'individu ou professionnel ?
- Souvent, grâce au « **GBS** » !
- Et en respectant quelques règles ...

En résumé ...

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



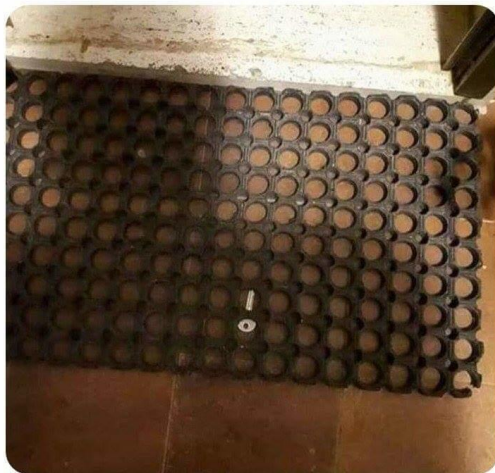
SOPHISTICATED (RAT) VISHING



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 SPÉCIAUX
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)

- **Menace 2 : on clique beaucoup [trop] ...**

Rançongiciel une prise d'otage informatique

1 Envoi d'e-mails infectés

Exploitant une faille du système informatique, des pirates envoient des millions d'e-mails avec, en pièce jointe, un virus de type rançongiciel.

2 Contamination de l'ordinateur

L'internaute visé ouvre le fichier infecté qu'il a reçu en pièce jointe sans se douter de sa dangerosité.



3 Cryptage des fichiers

Le logiciel malveillant chiffre tous les fichiers (disques durs externes, clés USB...) pour les rendre inutilisables.

4 Demande de rançon

Un message apparaît sur l'écran avec une demande de rançon.



5 Paiement de la rançon

Si l'utilisateur accepte le chantage, il paie en bitcoin, une monnaie virtuelle et anonyme, et peut espérer récupérer ses fichiers.



5 Refus du paiement

Si l'utilisateur ne paie pas, ses données restent inutilisables. Il peut toutefois réinitialiser son ordinateur au prix de la perte de toutes ses données.





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/9Yqnl2



+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

Fichier Edition Affichage Aller à Messages Événements et tâches Outils Aide

Courrier entrant - Philippe.Truillet [MESSAGE MARQUE SPAM : X]

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

De Cdiscount <anniversaire@cdiscout.com> ☆

Sujet [MESSAGE MARQUE SPAM : MOYEN]Félicitations ! Vous avez été choisi pour gagner un smartphone . 06:39

Pour philippe.truillet@irit.fr ☆

Répondre Transférer Archiver Indésirable Supprimer Autres



Félicitations !

Aujourd'hui, **28-10-2021**, nous célébrons donc le 22e anniversaire de notre activité en ligne, Cette journée auelles 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 !](#)

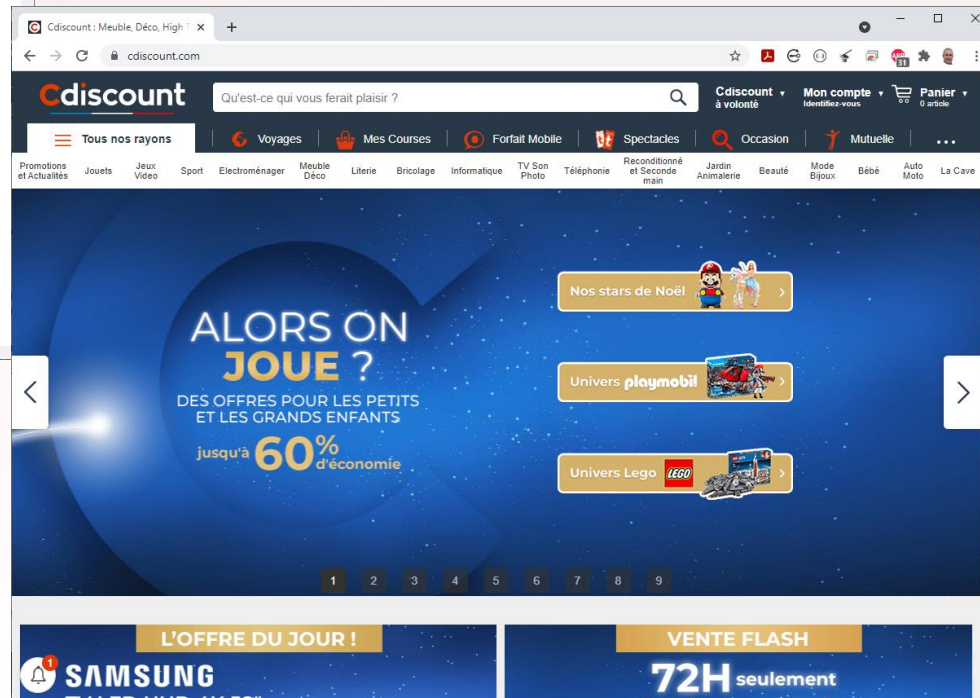
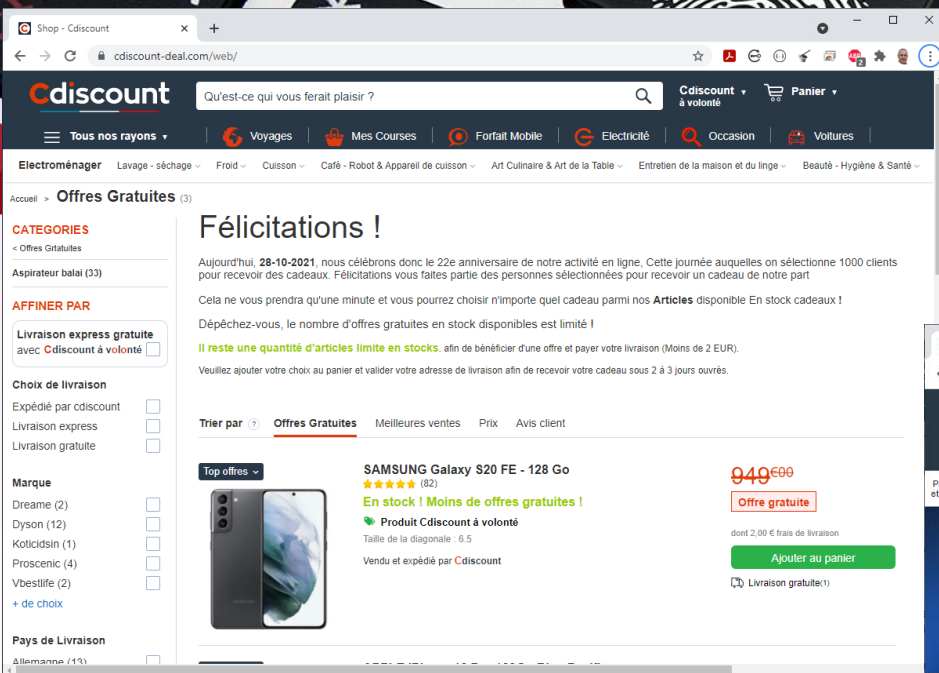
Il reste une quantité d'articles limite en stocks.

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.

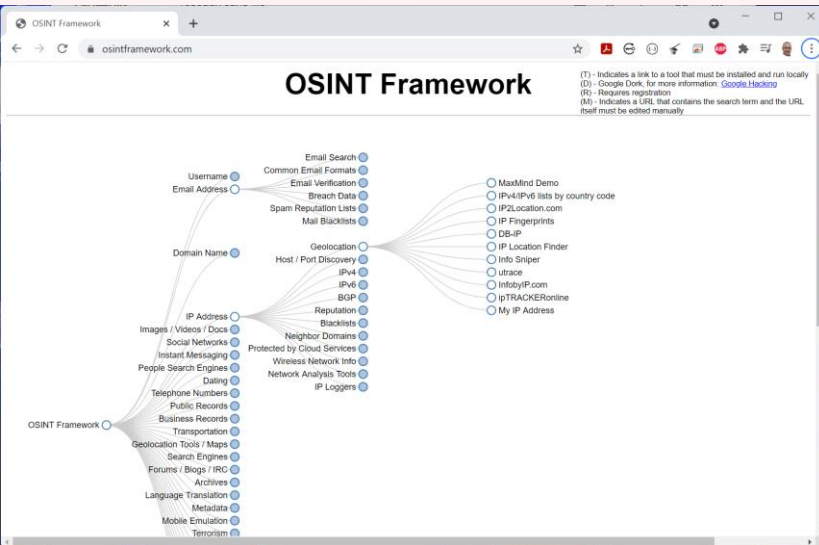
phishing

phishing



En résumé ...

- **Menace 3** : on laisse beaucoup (*trop*) de traces (→ **OSINT**)




- Données EXIF
- QR-Code
- Réseaux sociaux,
- ...

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
[Agrandir le plan](#)

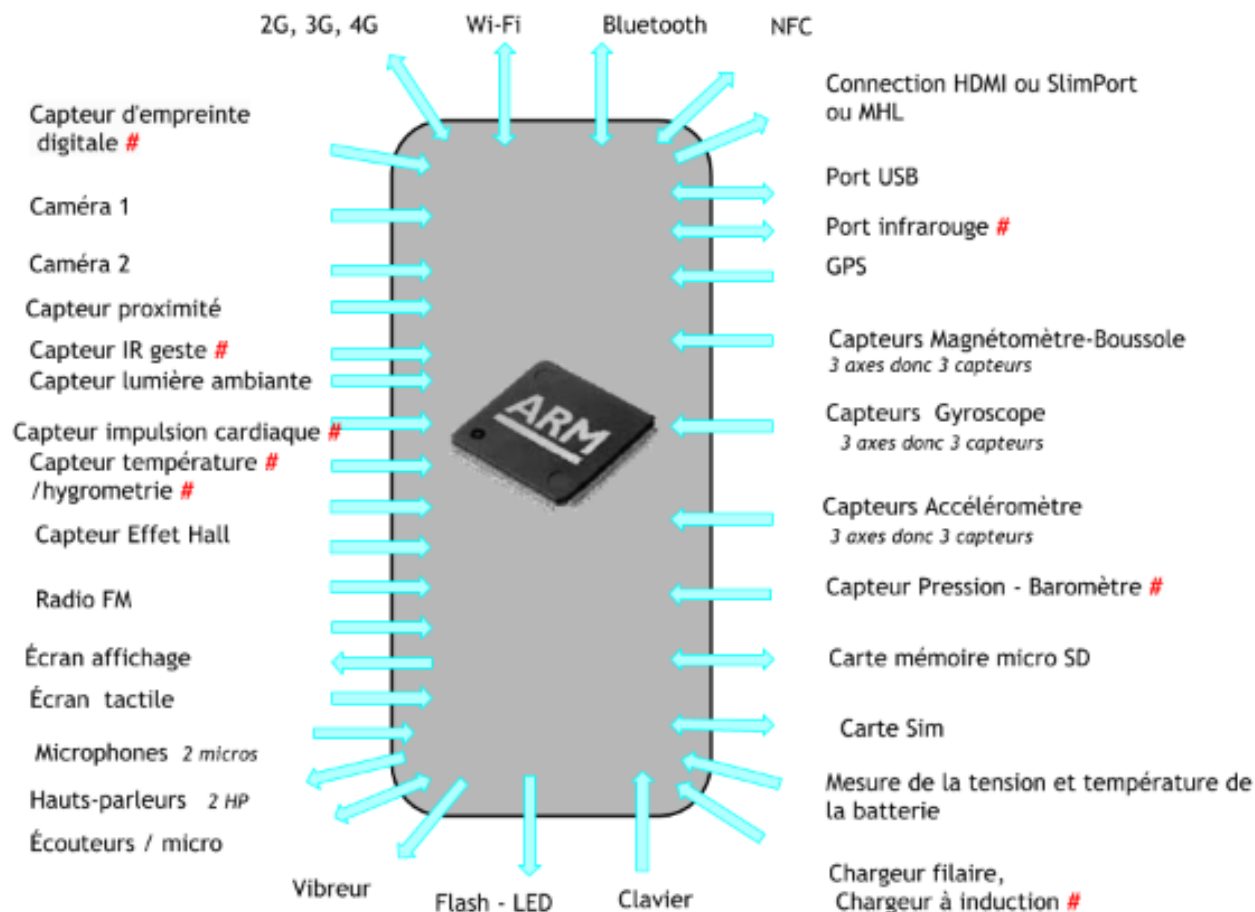


61 [Recommander](#)

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



Un SmartPhone = Un SuperOrdinateur

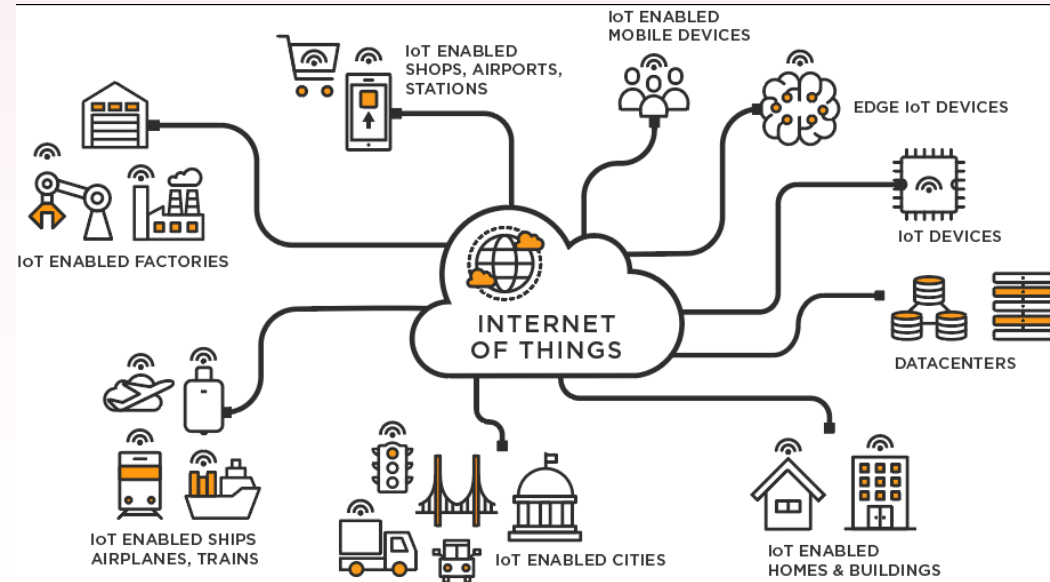


Les composants du Smartphone

= dans smartphone ou tablette haut de gamme

En résumé ...

- Et au delà ... **Menace 5 : l'IoT**
 - des milliards de capteurs disséminés
 - des problèmes de sécurité



STRAVA

Mobile

Fonctionnalités

Inscription

Blog

S'inscrire

Se connecter

Carte mondiale des activités

Couleur de la carte des activités

Vif

Bleu

Purple

Gris

Rouge

Type d'activité

Tous



Opacité

0%

40%

60%

80%

100%

Couches

Carte

Étiquettes

Styles de carte

Sombre

Lumineuse

Standard

Chercher



En résumé ...

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





CNIL.

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

→ 3 niveaux



Des liens



La Brigade Numérique

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



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



<https://ssi.gouv.fr>

