2-LES PIRATES

DIAPO 1 : LES CIBLES

- les hôpitaux : ransomware
- les agences gouvernementales, institutions, les banques...
- l’administration
- l’entreprise : PMEs...
- les militants
- Les hommes politiques, VIPs
- Tout le monde

DIAPO 2 : QUI SONT-ILS (ELLES) ?

- Les agences de renseignement : I-s-r*, les Chinois, les Russes, Corées (2), U-S...
- Pegasus
- I-s-r* : campagne d'influence massive pour des élections
- les mafias, les trafiquants
- Les anonymous, les hackers (white/grey/black hats)
- les 'brouteurs' d'Abidjan, 'arnaque au sentiment' (cyber-arnaqueurs)
- Les étudiants en cybersécurité
- Ceux qui 'surveillent' l'Internet : la gendarmerie, la police, le Fisc...

DIAPO 3 : Les diverses formes d’arnaque

- Les malwares : virus, vers, chevaux de Troie, Trojan, logiciels espions, ransomwares...
- Spam, Phishing et Spoofing, quishing
- arnaques e-commerce
- ’hacking social’ # hacking informatique
- deepfake : deep learning + fake (=fausse profondeur).
  Modifications de vidéos et de fichiers audio par l’IA
- ’sextorsion’ : extorsion de fonds suite à video (webcam)
- fraude : proposition de support informatique
- cyberattaques massives et simultanées (U-S)

DIAPO 3.1 : Les diverses formes d’arnaque (FIN)

- vol de temps machine, d’espace sur des ordis
- arnaque à la carte bleue : par téléphone => avoir une seconde carte pour les achats internet et une assurance avec sa banque
- vols de fichiers d’usagers
- ransomwares (rançongiciels) <=> iloveyou (destruction ‘gratuite’!)
- fraudes liées à la cryptomonnaie et aux investissements
  - !! attention : aux faux sites, si rendements mirobolants, si offres limitées
  - !! attention : si règlements d’achats uniquement en crypto
  - substitution d’identifiant, mot de passe, clé de portefeuille numérique
  - ‘SIM Swap’ usurpation de carte SIM, évite l’authentification à 2 facteurs

DIAPO 4 : Le Hacking ‘Ethique’ (Ethical Hacking)

- Tester les vulnérabilités
- Participe à des cyberguerres : ex Ukraine/Russie
- Veille et signalement : pédocriminalité...
- Les ‘Anonymous’ : hacktivistes
  - lutte contre la discrimination et la racisme
  - campagne contre la S-c-i-e-n-t-o
  - contre des gouvernements : I-r-a-n, A-u-s-t*l-i-e...les anti LGBT

DIAPO 5 : Se former/s'informer

- zataz.com reportages sur les attaques connues
- ZDNet Security : articles, analyses et conseils…
- threatpost.com : vulnérabilités…
- krebsonsecurity.com : reportages approfondis
- nombreuses videos YT poussant à suivre ensuite les cours d'une « cybersecurity academy » ($)
- offensive-security.com : cybersecurity training
  - $$$
  - certifications
  - cours approfondis : réseaux, windows, linux, langages de programmation...
  - labs : machines « attaquables » pour s'entraîner

DIAPO 6 : MES DONNÉES ONT-ELLES ÉTÉ VOLÉES ?

- haveibeenpwned.com
- cybernews data leak checker : mes données ont-elle fait partie d’une fuite de données

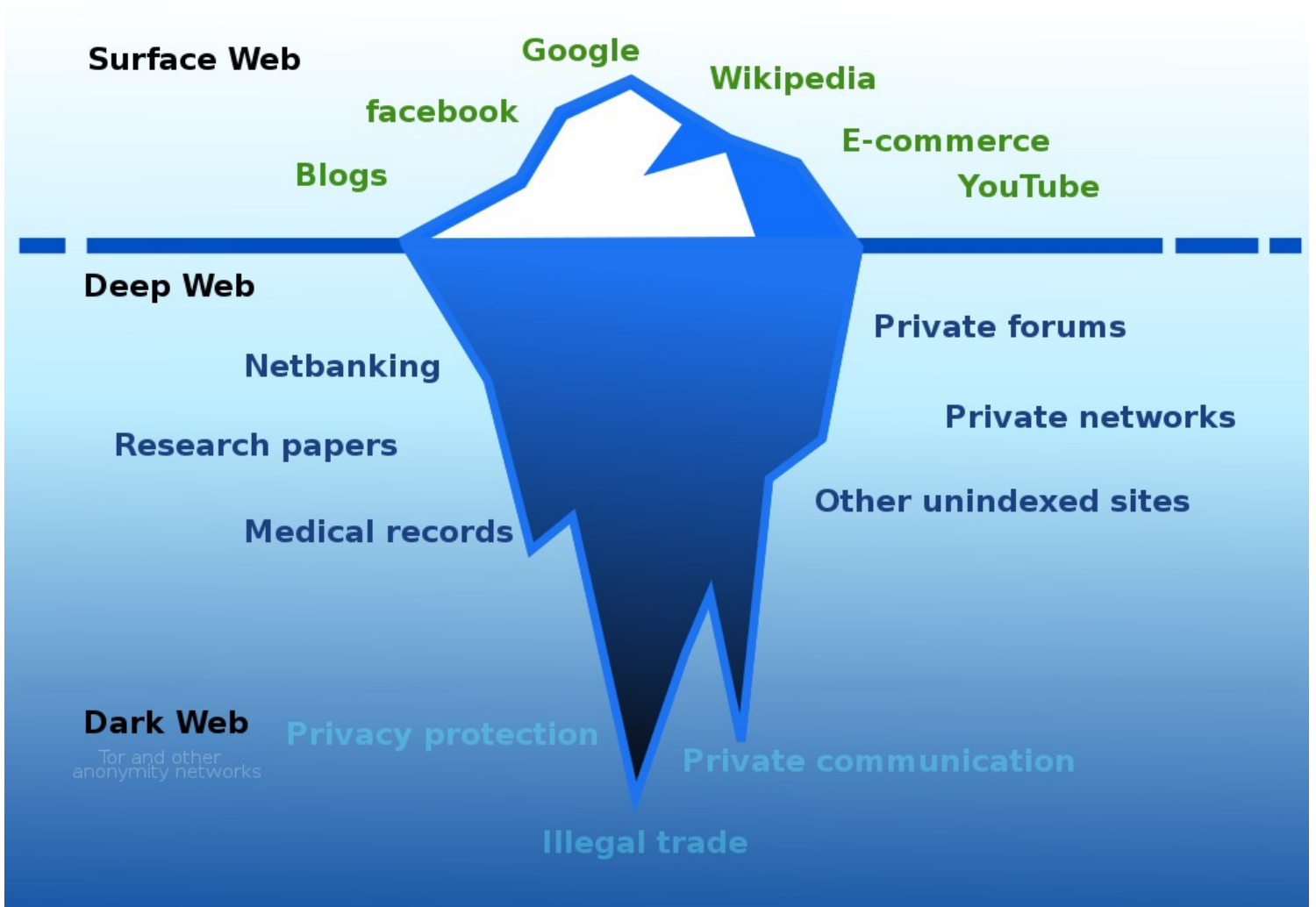
https://cybernews.com/personal-data-leak-check/

- la CNIL : cnil.fr, possibilité de signalement

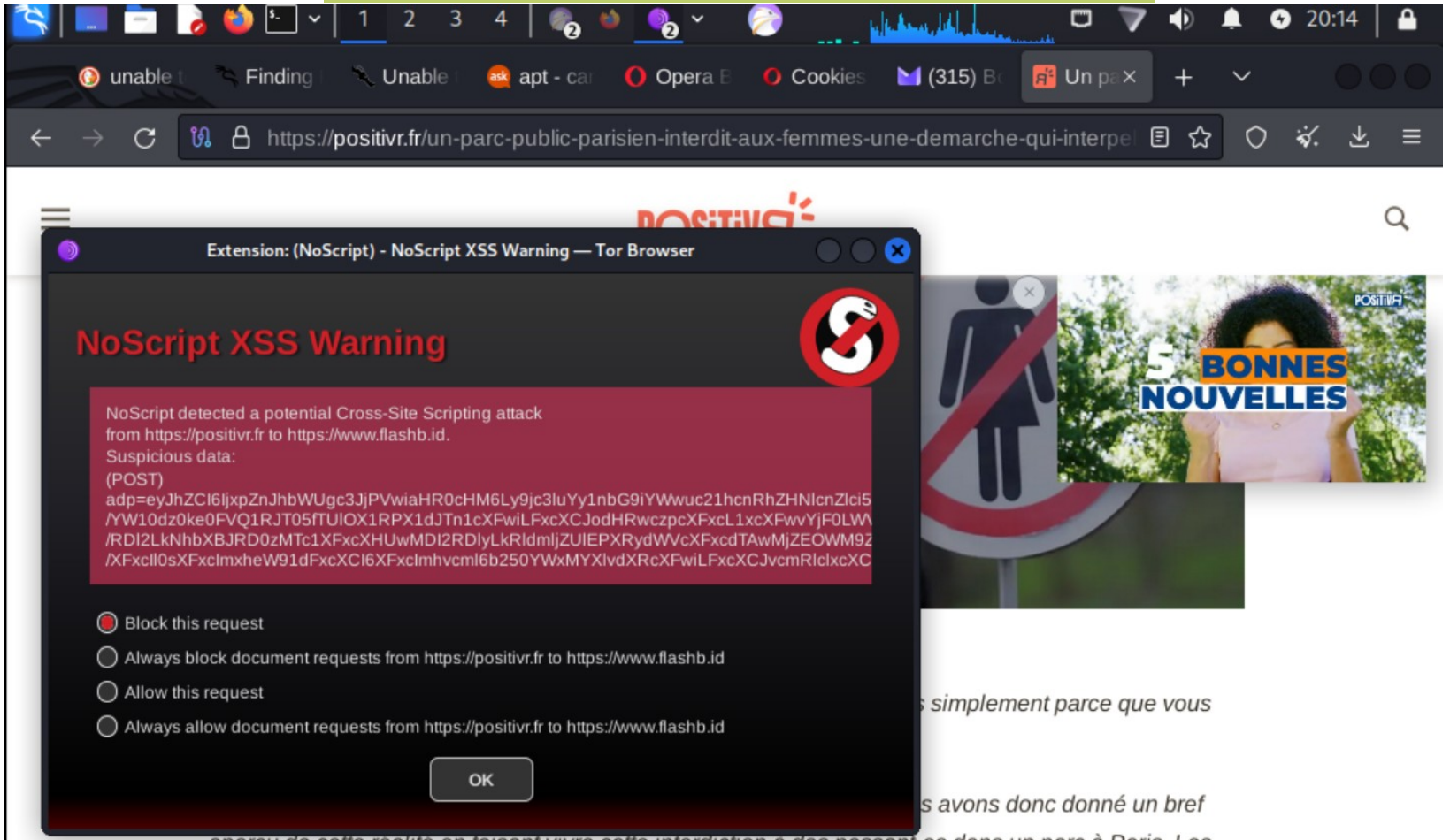
DIAPO 7 : le DARKNET

- Surface <=> Deep <=> Dark
  - Open web (=visible web) 4 % : **public** web sites (indexables par Google, Bing…)
  - Deep web : **privé** 90 % du contenu en ligne (non indexés, identifiant/mot de passe...)
  - Dark web : **secret** 6 % du contenu en ligne
- précautions à prendre : VPN, proxy, parefeu, Tails, TOR over VPN…
  - Si TOR désactiver Javascript
  - Si TOR, langue anglais + ne pas agrandir les fenêtres
- Un ‘mythe’ : le darknet c’est risqué, oui mais PAS QUE
- Attention aux écrans d’alerte (diapo suivante)
- Qui va sur le darknet : journalistes, commerce illégal, whistleblowers, traffics illégaux...
- Nos premiers pas dans le Darknet : The hidden wiki

DIAPO 7.1 : Les 3 parties du web



DIAPO 7.2 : TOR : écran d'alerte



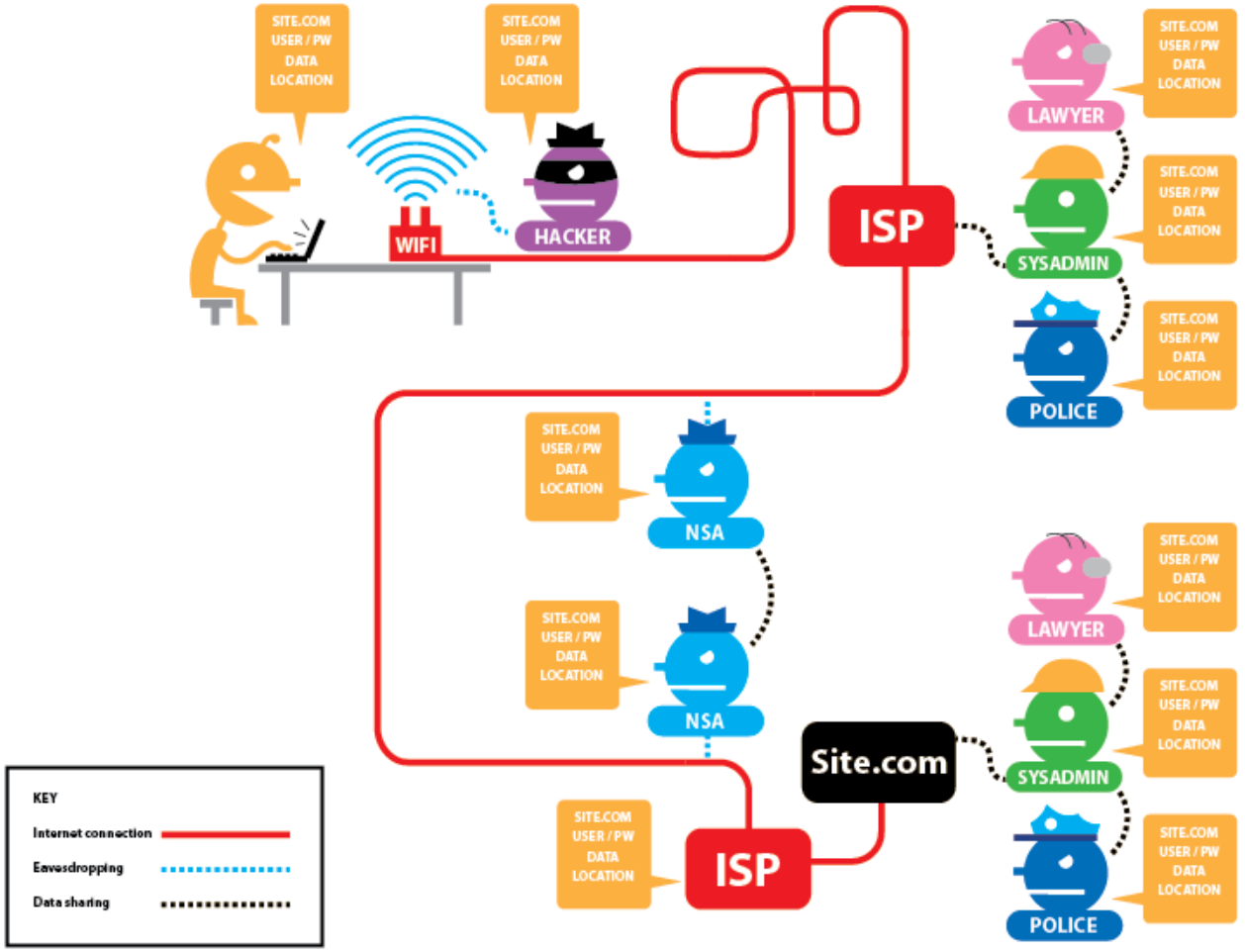
DIAPO 8 : The hidden wiki

- https://thehiddenwiki.com/ le vrai, sans risque!
  - Nombreux secteurs : financiers, general knowledge, commercial services, drugs...
  - Darknet version of popular sites :
    - c-i-a !!
    - B-B-C news
    - The Guardian
    - books/archives, TVs& radios on TOR…
- https://vpnoverview.com/privacy/anonymous-browsing/dark-web-websites-worth-visiting/ 26 sites not listed on Google
- https://thehiddenwiki.org/ !! Warning
- https://fr.wikipedia.org/wiki/The_Hidden_Wiki court article en français

DIAPO 9 : Devenir un Ethical Hacker ?

- Au début : on étudie les méthodes des ‘black hat hackers’
  - MAIS comment les hackers pénètrent-ils dans une machine ?
  - TOUS les systèmes d’exploitation ont des failles !!!
  - Davantage de tentatives contre les systèmes les plus répandus : Windows, IOS (MacOS), Android
- Pour aider les entreprises, les associations...
- Ce qui semble plus ‘facile’ : s’introduire dans un réseau wifi

DIAPO 10 : Un usager/Un réseau/ Beaucoup d’oreilles



DIAPO 11 : Les attaques selon les couches du réseau

Activités Visionneur de documents 11 avril 23:17

30 sur 270 20240410_Network-basic-for-hackers_archive.org-pdf 100%

The OSI Model from a Cybersecurity Perspective

The attacks against the protocols in this model can be categorized as follows;