

LE GUIDE DE SURVIE SUR INTERNET



QUELQUES CHIFFRES POUR 2021

Infos générales (<https://www.blogdumoderateur.com/30-chiffres-internet-reseaux-sociaux-mobile-2021>)

66,6 % de la population mondiale utilise mobile,
4,66 milliards d'internautes (sur 7,9 Milliards d'humains),
4,32 milliards d'utilisateurs d'Internet à partir d'un mobile,
316 millions d'internautes supplémentaires en 2020 (+7,3 %),
4,2 milliards d'utilisateurs actifs des réseaux sociaux (53,6 %),
6h54 passées en moyenne sur Internet (+4 %),
63,4 % des internautes utilisent le navigateur Chrome (-0,4 %),
2,6 milliards de personnes disposent d'une adresse mail (chiffres 2015).

Infos Cyber sécurité (<https://www.websiterating.com/fr/research/cybersecurity-statistics-facts/>)

85 % des violations de la cybersécurité sont causées par **une erreur humaine**.

94 % de tous les logiciels malveillants **est livré par e-mail**.

Les attaques de ransomware se produisent toutes les **10 secondes**.

71 % de toutes les cyberattaques sont motivées financièrement (suivi par le vol de propriété intellectuelle, puis l'espionnage).

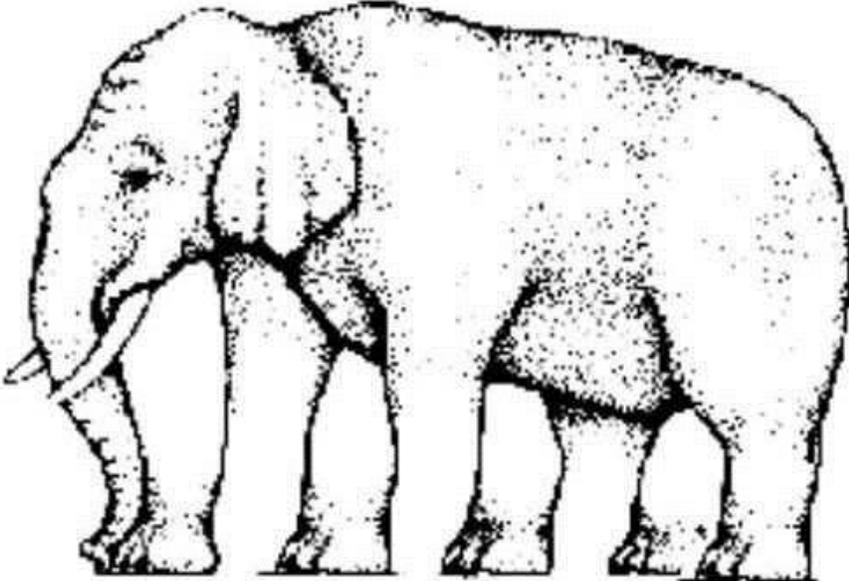
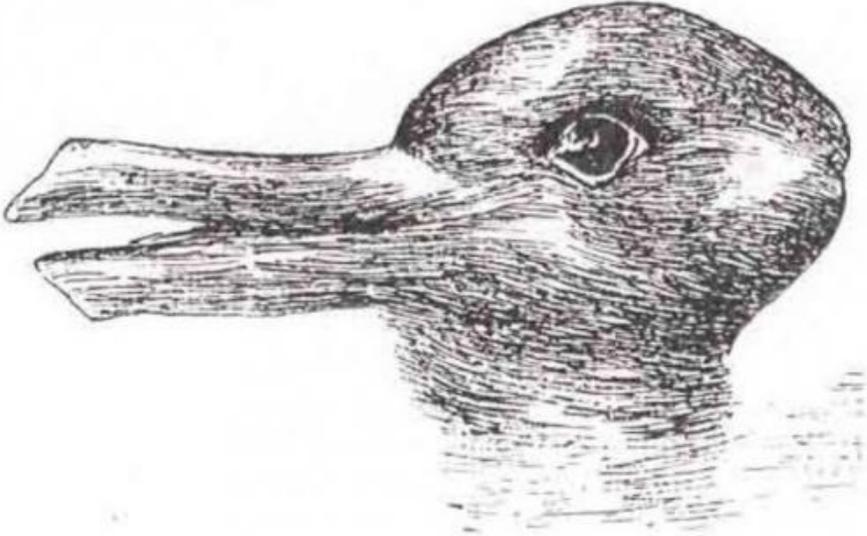
Le coût mondial annuel de la cybercriminalité est estimé en **6000 Milliards \$** en 2021.

1 L'ORACLE ET LE TEST



- Les biais cognitifs
- Etat émotionnel
- Missclic Don't Panic

LES BIAIS COGNITIFS (def: « Un *biais cognitif* est une distorsion dans le traitement cognitif d'une information »)



ETAT EMOTIONNEL ET EXEMPLE D'UTILISATION DARK PATTERN

- FATIGUE (par ex: liée à manque de sommeil, actions répétitives etc..)
- STRESS (par ex: lié à pression de sa direction/clients, situation familiale, etc..)
- TROP DE CURIOSITE SANS REELLE REFLEXION

} Combo Perdant

Exemple Dark Pattern

Moyens:

- Pop-up intrusif
- Divers boutons validation
- Case cochée par défaut
- Vidéo lancée automatiquement
- Article qui intrigue etc...

But:

- Collecter données perso
- Augmenter tarif
- Augmenter trafic
- Améliorer Taux clic
- Force souscriptions
- Etc..

The screenshot shows a website interface with several elements illustrating dark patterns:

- Top Bar:** A notification banner for Opera Browser with a 'Download' button.
- Navigation:** 'softonic' logo and menu items: APPS, GAMES, ARTICLES, SOLUTIONS. A search bar is on the right.
- Main Content:** A large green 'Télécharger' button with a download icon. Below it, a section for 'CCleaner for Mac' with a 'Free Download' button and a 'Buy now' button. A 'Rate it!' button shows 6 votes and 267 votes.
- Pop-ups:** A 'Votre Mac est lent ?' pop-up with a 'Visit Website' button. A 'softonic.com Newsletter' pop-up with a 'Discover new apps, games, and software!' headline and an 'ACCEPT' button.
- Footer:** A cookie consent banner with 'Customize privacy settings' and 'ACCEPT' buttons.

Annotations with blue arrows point from the 'Moyens' and 'But' text to specific elements on the page:

- 'Pop-up intrusif' points to the newsletter pop-up.
- 'Divers boutons validation' points to the 'Télécharger', 'Free Download', 'Buy now', and 'ACCEPT' buttons.
- 'Case cochée par défaut' points to the 'ObtenezEmail' text area.
- 'Vidéo lancée automatiquement' points to the 'Rate it!' button.
- 'Article qui intrigue etc...' points to the 'CCleaner for Mac' article.

J'AI CLIQUE AU MAUVAIS ENDROIT: DON'T PANIC > ARRET DES CONNEXIONS > DEMANDER DE L'AIDE ENTOURAGE



Ooops, 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 AMT from Monday to Friday.

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

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

Send \$300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw Copy

Check Payment Decrypt

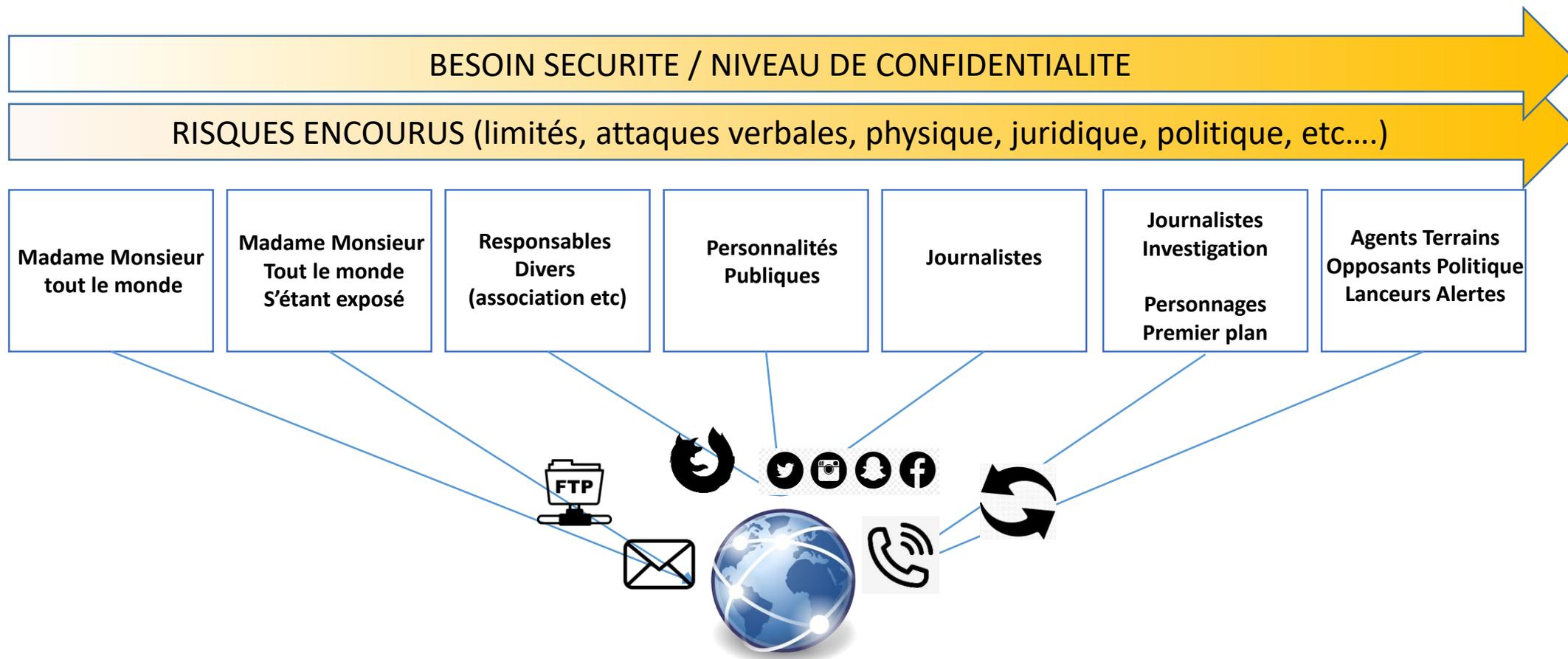


DON'T PANIC!

2 SE CONNAITRE DEFINIR SES BESOINS

- Juger son niveau de risque
- Contexte géopolitique
- Connaitre son niveau

JUGER SON ECHELLE DE RISQUES A S'EXPOSER SUR INTERNET



Exemple de menaces:

Enquete (Rh, assurances etc...)



Curieux malsains Nuisance Image



Nuire €



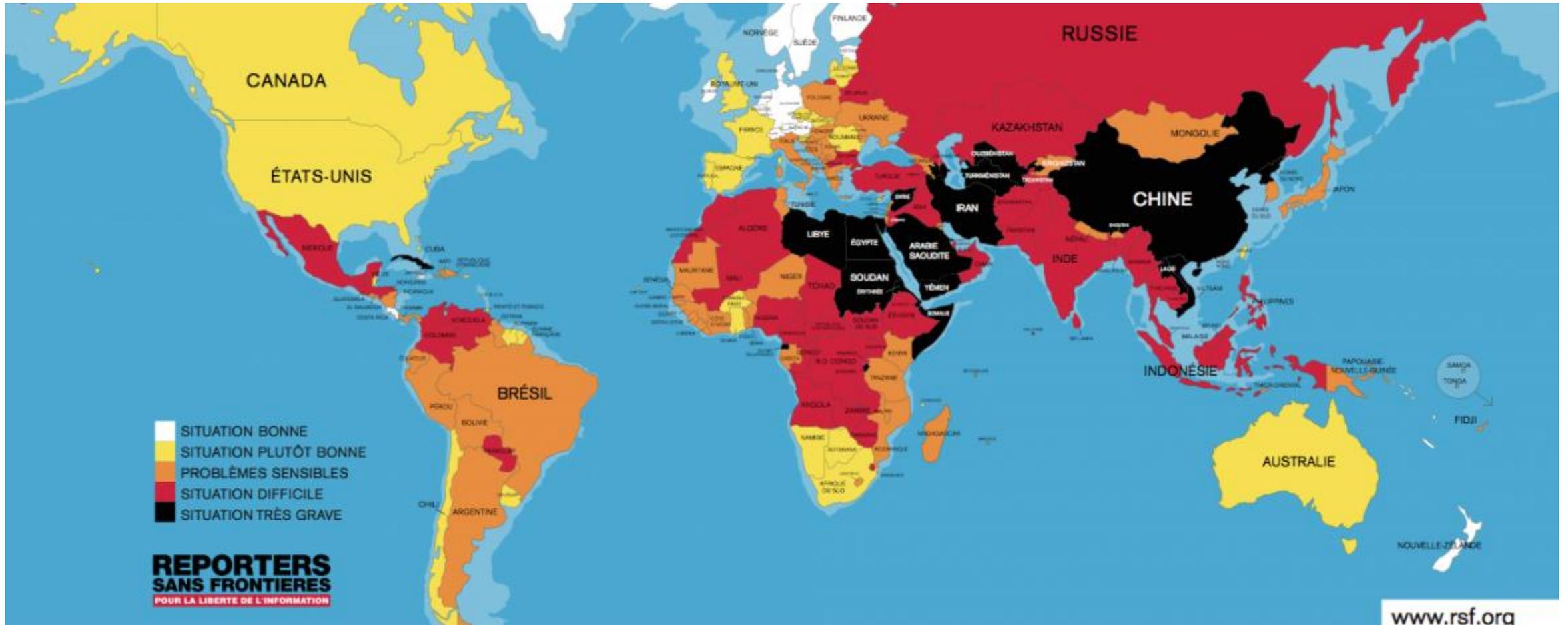
Groupes Interets



Etat Censure



LE CONTEXTE GEO POLITIQUE IMPLIQUE DE S'ADAPTER



DEFINIR CONNAITRE SON NIVEAU



EXEMPLE CONCRET
AVEC LA RANDONNEE

BESOIN EQUIPEMENT / NIVEAU DE LA PERSONNE



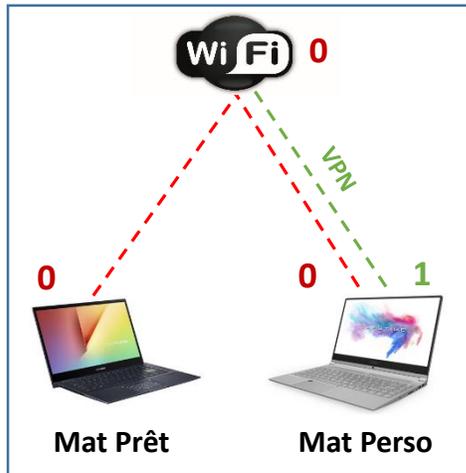
EXEMPLE CONCRET
AVEC L'INFORMATIQUE

3 LES VERIFICATIONS DE BASES / LE MATERIEL

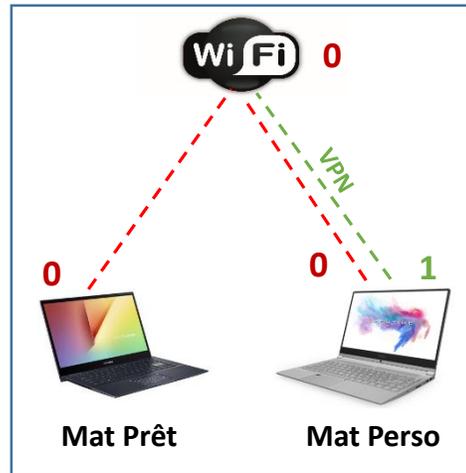
- Les lieux de connexion
- Le cas de la maison
- Les bases d'une bonne protection

LES LIEUX DE CONNEXION (OU? AVEC QUEL MATERIEL? QUAND & QUELLE DUREE?):

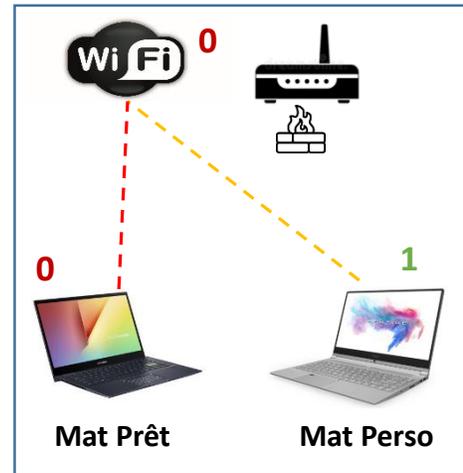
LIEU PUBLIC
OUVERT
(ex: GARE)



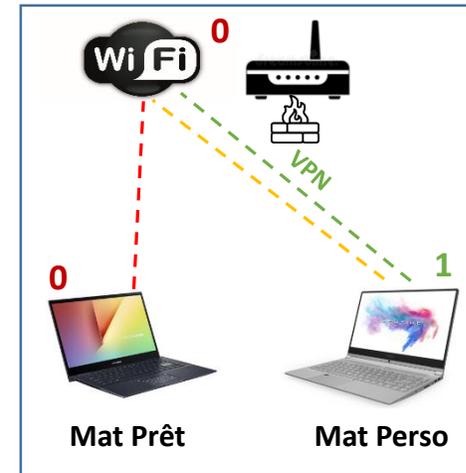
LIEU PUBLIC
« FERME »
(ex: HOTEL)



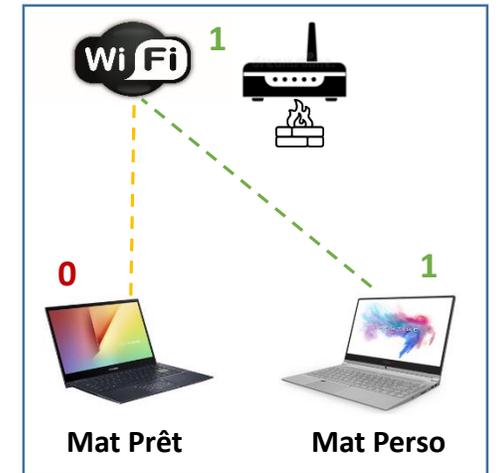
LIEU PRIVE
(ex: TRAVAIL)



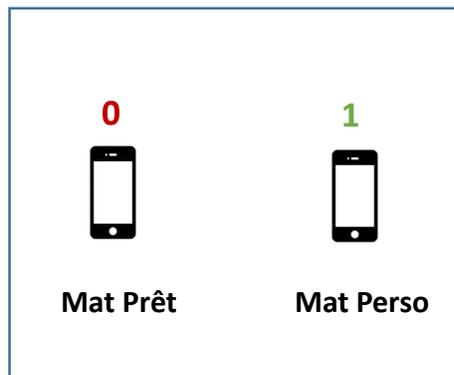
LIEU PERSONNEL
ex: AMIS



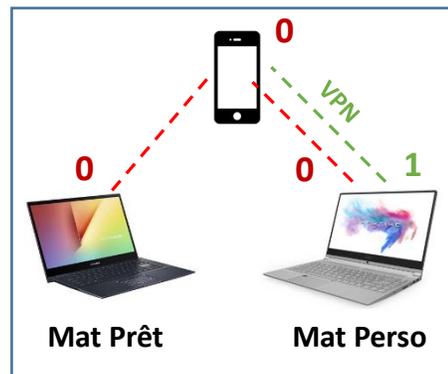
LIEU PERSONNEL
ex: MAISON



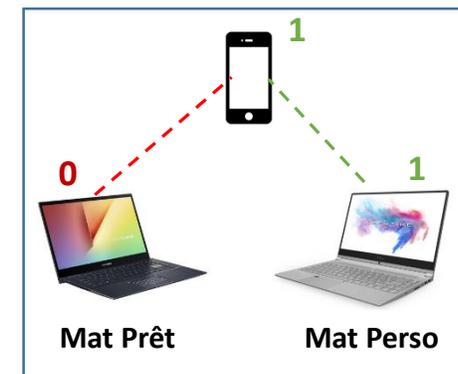
SMARTPHONE SEUL



SMARTPHONE PRET



SMARTPHONE PERSO

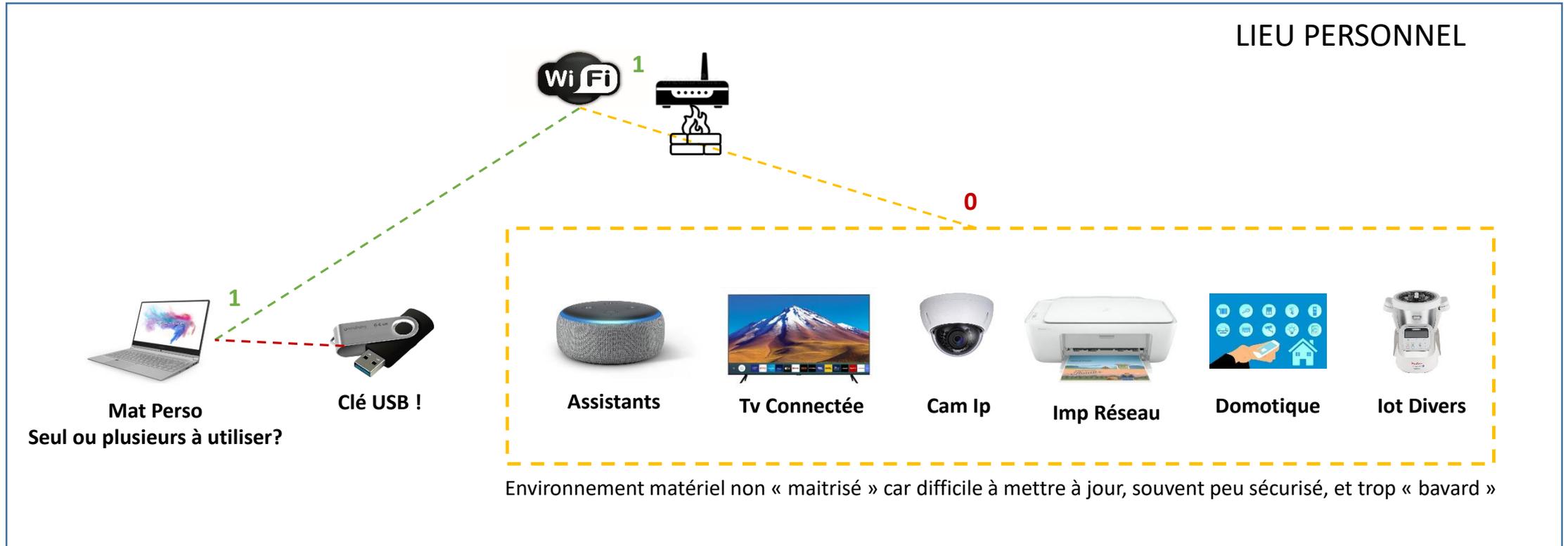


LE CAS PRECIS DU LIEU PERSONNEL (MATERIELS MAITRISES ET NON MAITRISES):



INTERNET

LIEU PERSONNEL



LES BASES D'UNE BONNE PROTECTION: LA PORTE D'ENTREE



FAI INCONNU

?



FAI CONNUS
(BOUYGUES/FREE/ORANGE/SFR)



FAI ALTERNATIF
ATTENTIF VIE PRIVE



Nb serveur DNS:

Régler ses propres DNS est conseillé (à discuter avec la communauté pour les adresses + voir DNS over TLS)

Nb Wifi:

Clé de sécurité de longueur suffisante en protocole mini **WPA2-PSK**

On limite son utilisation, sa portée (voir on l'utilise pas et on préfère le bon vieux câble)

Filtrage des appareils par adresse mac

On ne partage/donne pas sa clé wifi même à un voisin > c'est vous qu'on viendra voir si problème

([article L.335-7-1 du Code de la propriété intellectuelle](#))

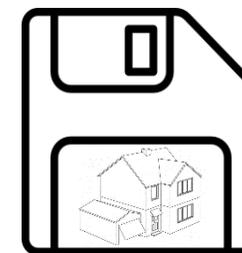
LES BASES D'UNE BONNE PROTECTION: DERRIERE LA PORTE ENTREE



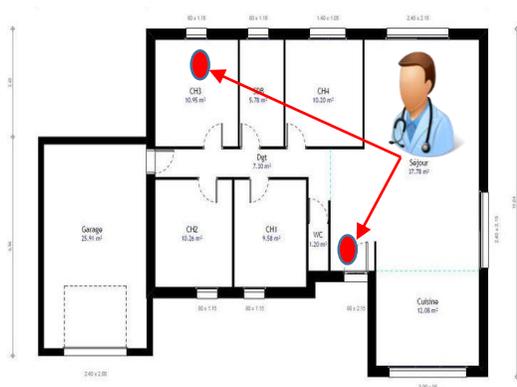
FIREWALL ACTIF



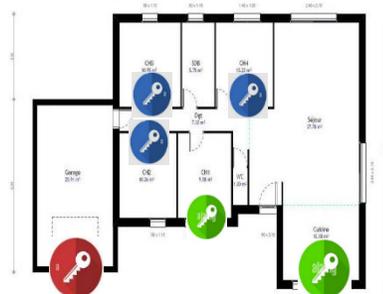
MISES A JOUR OK



JEU DE SAUVEGARDES



**ANTIVIRUS
A JOUR**



**PASSWORD
SPECIFIQUES
+
GESTION
DROITS ACCES**



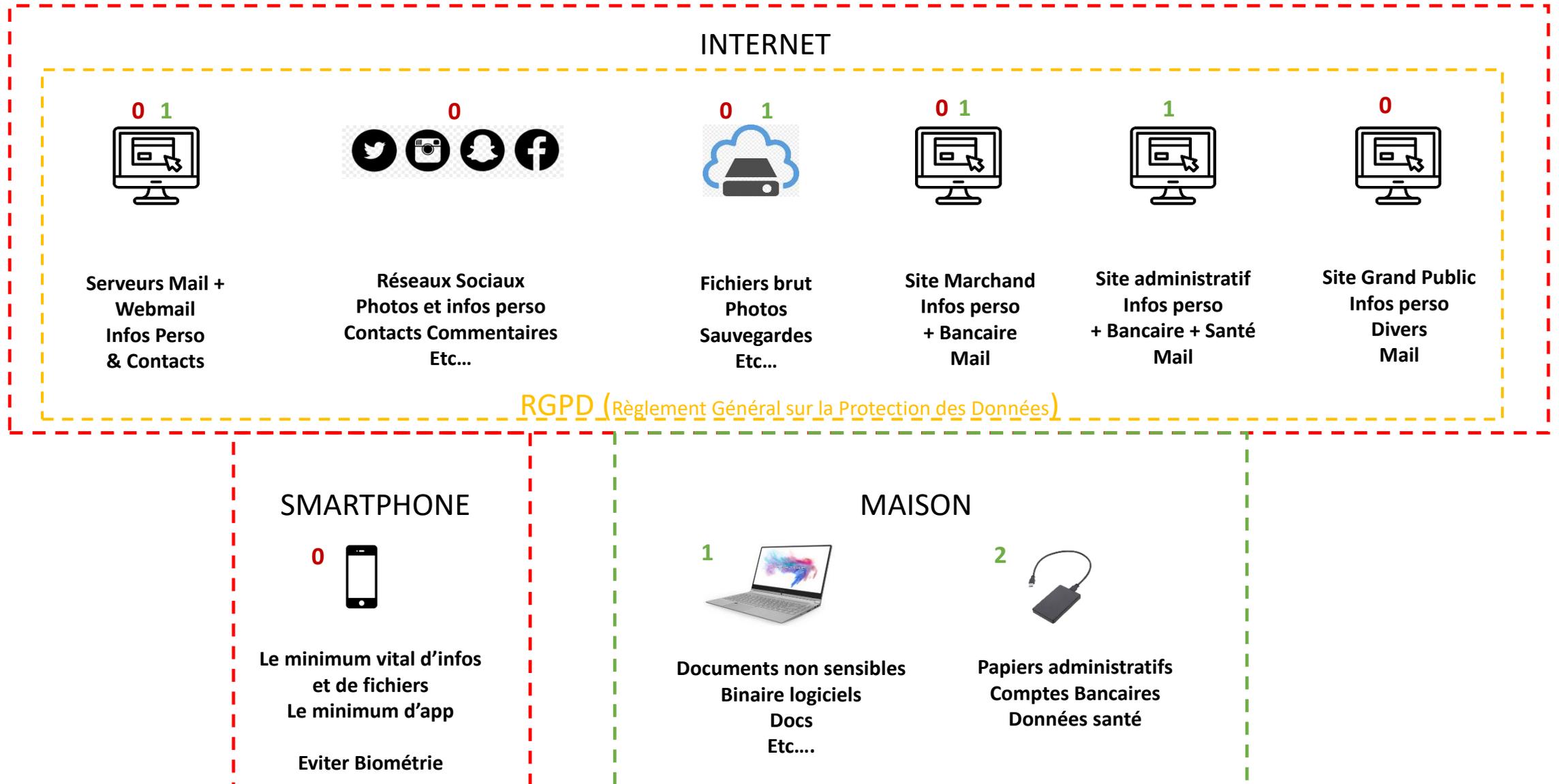
**CONTRÔLE ORIGINE
(SITE EDITEUR)**

4 CIBLER LE NIVEAU DE SES DONNEES

- COMMUNES (binaires app, pdf doc, etc...)
- PERSONNELLES (photos, documents perso, etc...)
- TRAVAIL (documents travail, etc...)
- PUBLIQUES (photos, commentaires, informations perso, etc...)
- SENSIBLES (photos, doc santé, bancaires, etc...)
- BIOMETRIQUES (digitales, facial, rétine, etc.....)

- VIE PRIVE = DOIT ETRE PROTEGEE (article 9 du Code civil)

SAVOIR SITUER ET MAITRISER OU SE TROUVENT VOS DONNEES / NIVEAU DE CONFIANCE / RGPD



5 LA COMMUNICATION: LES OUTILS / RISQUES

- Messagerie classique (client lourd avec connexion Ssl / Webmail)
- Messagerie temps réel directe (ex: Whatsapp, Teams, Discord etc...)
- Messagerie temps réel additionnelle (ex: Facebook, Steam, Site etc...)

- Quelques Types d'attaques
- Comment Se prémunir

QUELQUES TYPES D'ATTAQUES (CIBLEES OU NON CIBLEES)

Le spam

Les malwares

Phishing par url

Arnaques

Usurpation nom domaine

Usurpation de marque

Chantage

Piratage compte/serveur

Mail publicitaire non désiré pour forcer à acheter un produit

Mail contenant une pièce jointe infectieuse laissant la curiosité faire le reste

Mail imitant un organisme avec un lien web infectieux (demande clic)

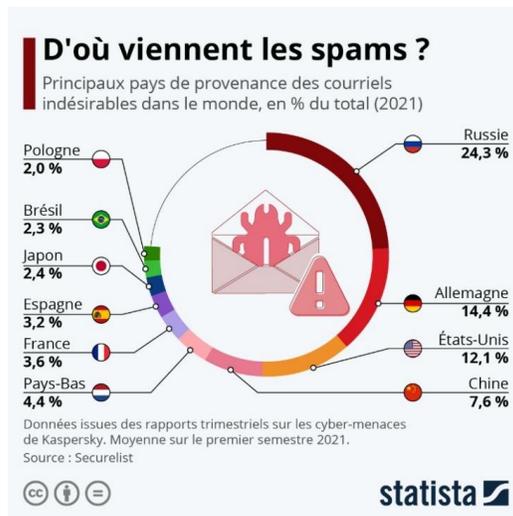
Mail trompant la vigilance sur un sujet (ex fausse livraison UPS)

Mail avec expéditeur imitant le nom d'un domaine connu (ex IMPOTS, EDF etc..)

Mail imitant une marque connue (ex Ovh fausse alerte expiration domaine sous 3j)

Mail tentant d'intimider sur un sujet (ex fausse ou vraies photos nude) demande rançon

Vrai Mail venant d'un contact infecté et demandant à ouvrir une url infectée



Bonjour,

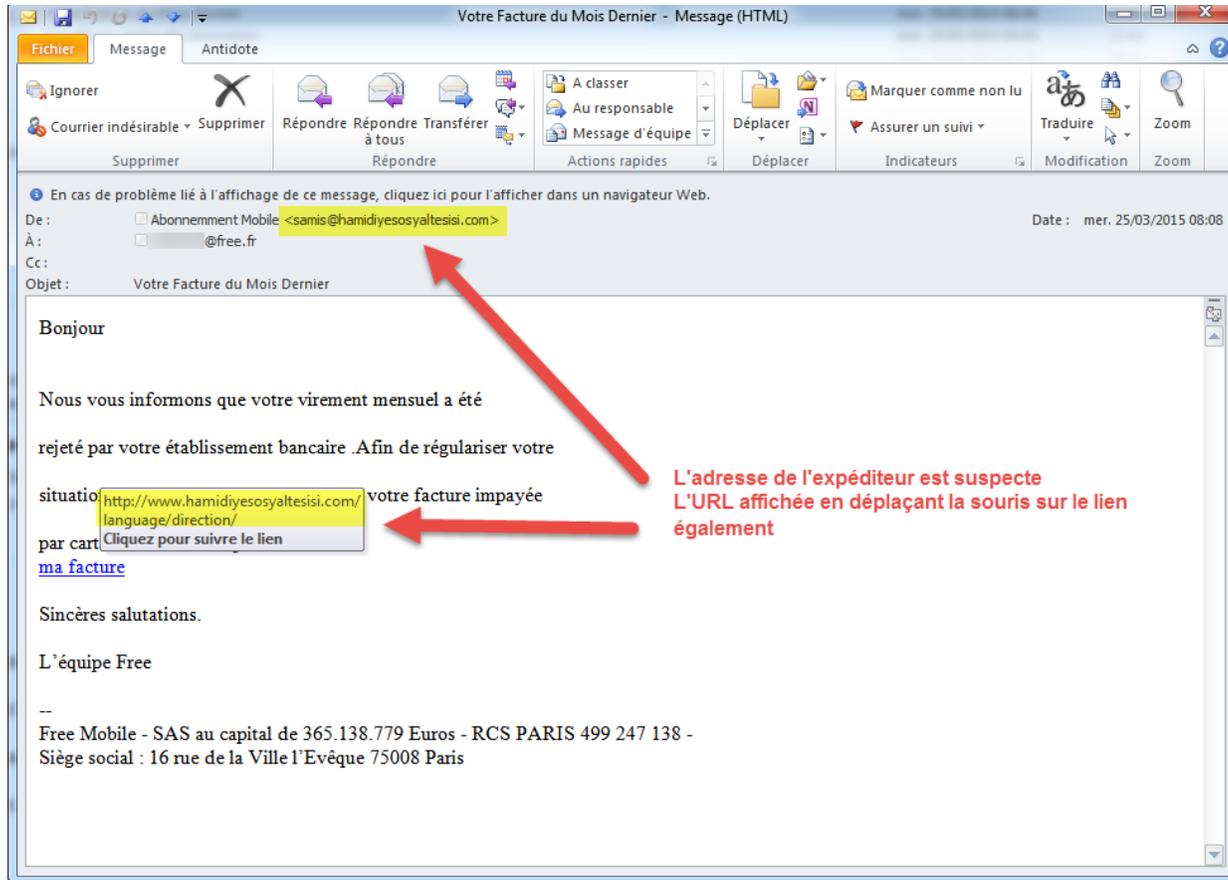
Après les derniers calculs annuels de l'exercice de votre activité, nous avons déterminé que vous êtes admissible à recevoir un remboursement de 50.80 €.

Veillez nous soumettre s'il vous plaît la demande de remboursement d'impôt pour nous permettre de la traiter dans un plus bref délai.

>> Pour accéder au formulaire , cliquez ici .

Un remboursement peut être retardé pour diverses raisons. Par exemple, une soumission de dossiers non valides ou une inscription après une certaine limite.

2 EXEMPLES



Source: <https://vleclerc.files.wordpress.com/2015/03/snaghtmlc705004.png>



Source: https://clairejanssens.fr/wp-content/uploads/2015/04/mail_dangers_phishing.jpg

COMMENT SE PREMUNIR

LOGICIEL MAIL / NAVIGATEUR / ANTIVIRUS A JOUR

FILTRE ANTISPAM ACTIF (SOIT LOCAL GERE PAR ANTIVIRUS / SOIT GERE PAR SERVICE TIERS)

AVOIR PLUSIEURS MAILS (OU ALIAS) AFIN DE CONTENIR LES MENACES

SI POSSIBLE AVOIR SON PROPRE NOM DE DOMAINE AFIN DE POUVOIR GERER L'ENSEMBLE

UTILISER LES BOITES MAILS TEMPORAIRES PROPOSEES PAR DIFFERENT SERVICES WEB

GESTION DES CONTACTS: SURVEILLANCE ACCRUE

LIMITER LES CC POUR NE PAS IMPACTER LATERALEMENT

ACTIVER L'OUVERTURE EN MODE TEXT SEUL (CONTRAIGNANT MAIS BLOQUE LES SCRIPTS)

LIMITER CURIOSITE D'OUVRIR OU TESTER UN LIEN, EST CE REELLEMENT NECESSAIRE?

LE MAIL:

VERIFIER ADRESSE MAIL DE L'EMETTEUR (EN PARTICULIER LE NOM DE DOMAINE)

VERIFIER LE CORPS ET LA DEMANDE GENERALE (FAUTES ORTHOGRAPHES ETC..)

URL NE PAS CLIQUER / AVEC UN CLIC DROIT VERIFIER LE TEXTE DE SON URL

PIECE JOINTE, ENREGISTRER SOUS ET SCANNER AVEC L'ANTIVIRUS

MAIL SUSPECT: NE SURTOUT PAS REpondre ET AVERTIR VOTRE CONTACT TECHNIQUE PROCHE

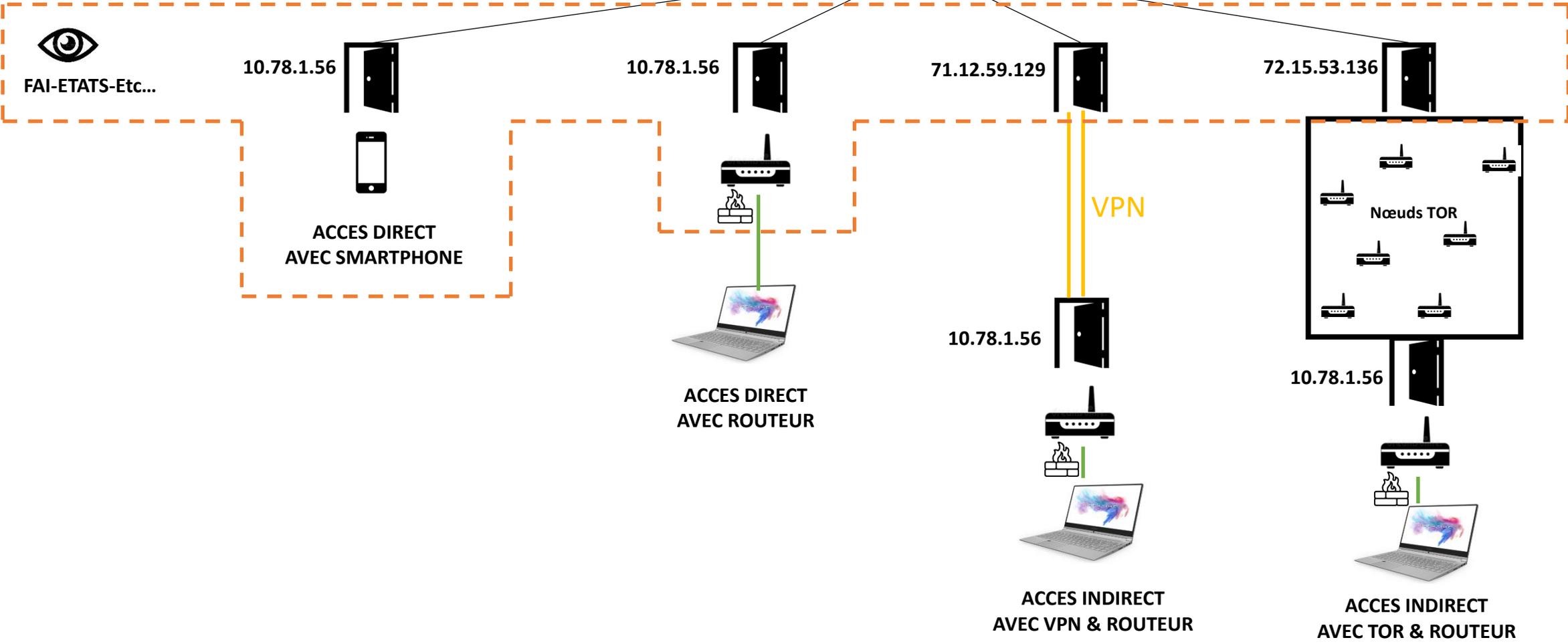
6 LA NAVIGATION: LES OUTILS / LES RISQUES

- ACCES DIRECT? VPN? TOR?
- GESTIONNAIRE DE MOT DE PASSE
- QUELQUES REGLES DE NAVIGATIONS
- QUELQUES MOTS SUR LES RESEAUX SOCIAUX

ACCES DIRECT? VPN? TOR?



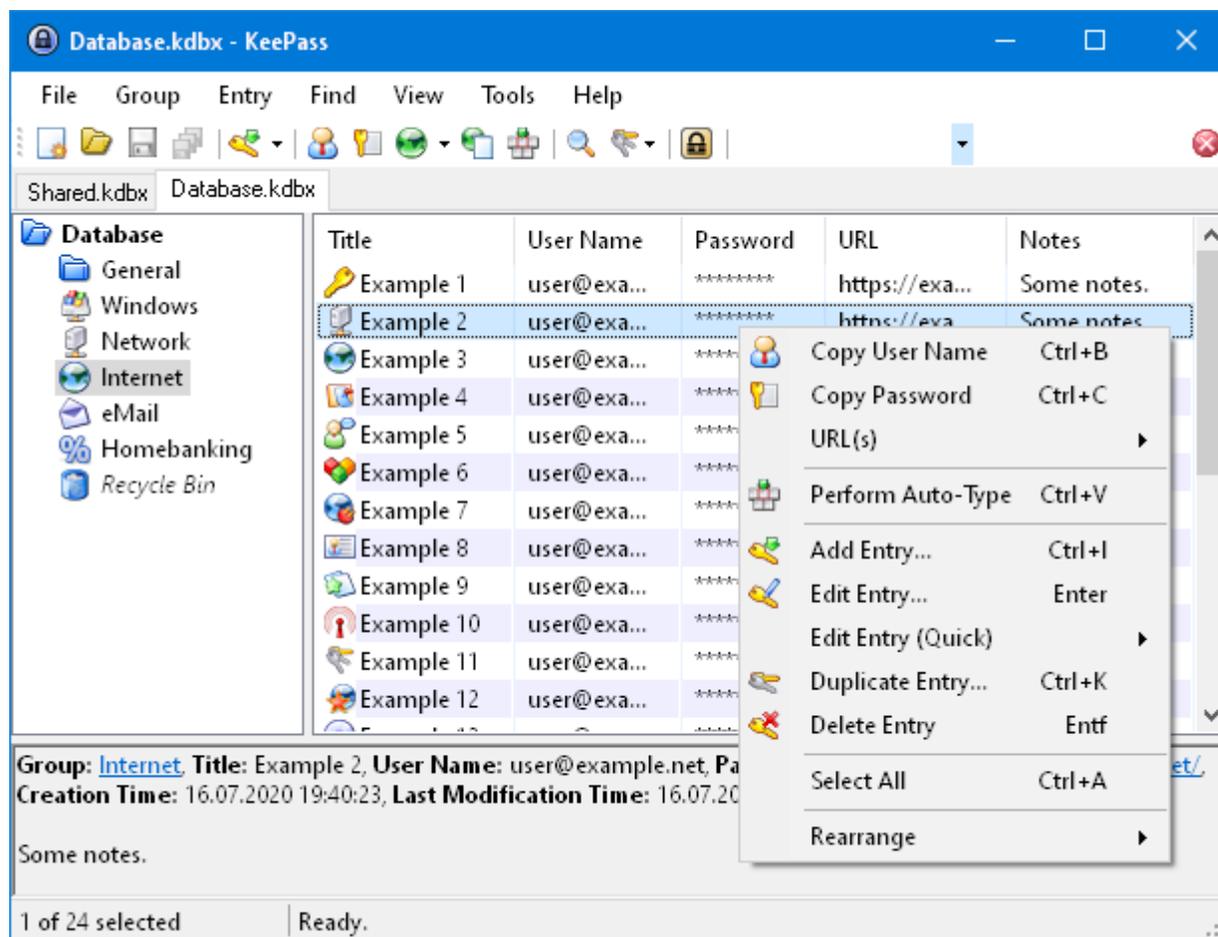
INTERNET



GESTIONNAIRE DE MOT DE PASSE

Rappel de Base:

Un mot de passe différent
Pour chaque site
Et de longueur suffisante



QUELQUES REGLES DE NAVIGATION

POUR TOUS SITES WEB

SI C'EST GRATUIT C'EST TOI LE PRODUIT ! (A CONSOMMER AVEC MODERATION + LIRE CHARTE)
EXCEPTION FAITE POUR LE MONDE « OPEN SOURCE » (MAIS MEFIANCE TOUT DE MEME)

NE PAS HESITER A UTILISER UN SERVICE DE VPN (EXTENSION POSSIBLE POUR LES NAVIGATEURS)

HTTPS TOUT LE TEMPS (OU LE PLUS POSSIBLE)

OPTION ISOLATION ONGLET ACTIVE

NAVIGATION EN MODE PRIVE / SINON VIDER LE CACHE REGULIEREMENT

POUR CHERCHER/DOWNLOAD LES SOURCES, TOUJOURS SE REFERER AU SITE EDITEUR/CONSTRUCTEUR
BIEN VERIFIER LE DOMAINE DANS L'URL ET ETRE VIGILANT SUR LES DOMAINES INCONNUS

UTILISER LE PLUS POSSIBLE LA DOUBLE AUTHENTIFICATION

LIMITER LE PLUS POSSIBLE LES INFORMATIONS PERSONNELLES SUR N'IMPORTE QUEL SITE

PENSER AUX BOITES MAILS TEMPORAIRES POUR CERTAINS FORMULAIRES

UTILISATION DES FAVORIS + SYNCHRO / EVITER DE STOCKER LES MOTS DE PASSE DANS NAVIGATEUR

EXTENSIONS NECESSAIRES : BLOQUEURS DE PUBS/COOKIE & BLOQUEUR SCRIPT

LIMITER LE NOMBRE D'EXTENSIONS POUR ALLEGER LE NAVIGATEUR

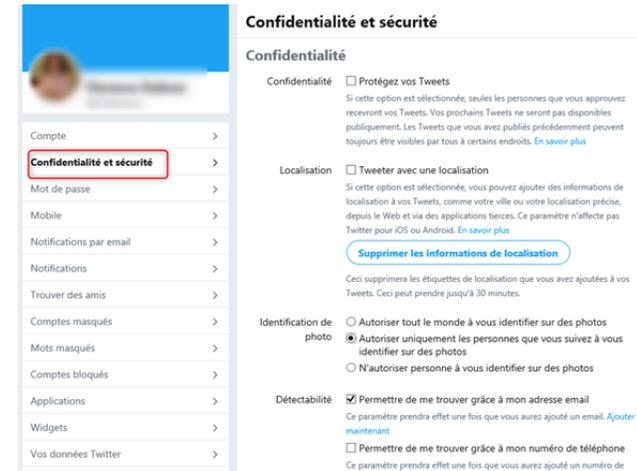
QUELQUES MOTS SUR LES RESEAUX SOCIAUX

SI C'EST GRATUIT C'EST TOI LE PRODUIT ! (A CONSOMMER AVEC MODERATION + LIRE CHARTE)

BIEN PRENDRE CONSCIENCE QUE PLUS VOUS ABREUVEZ DE DONNEES CES RESEAUX PLUS ON A LA CAPACITE DE VOUS CIBLER POUR LA PUBLICITE, MARKETING, ETC.....

MIEUX VOUS CONNAITRE, C'EST MIEUX VOUS MANIPULER (ex campagne 2016 USA: CAMBRIDGE ANALYTICA)

PENSER A DE SUITE ALLER DANS LES PREFERENCES ET LIMITER LA DIFFUSION D'INFO
BIEN DEFINIR CE QUI EST PUBLIC ET AUTORISE EN DIFFUSION DE CE QUI EST « PRIVE »
AVEC RGPD NE PAS HESITER A DEMANDER UN RAPPORT DE VOS DONNEES



7 L'AUTOHEBERGEMENT: LES + LES -

- VOUS MAITRISEZ ENTIEREMENT VOTRE SOLUTION
 - VOUS CONTROLER SES ACCES DE A à Z
 - VOUS LE FAITES EVOLUER/OPTIMISER COMME VOUS SOUHAITER
-
- DEMANDE DU MATERIEL ET UN SAVOIR FAIRE TECHNIQUE
 - ATTENTION FORTE A LA SECURITE / RISQUES A VOTRE CHARGE
 - DEMANDE UN ENTRETIEN ET UN SUIVI CONSEQUENT

