

01/10/2018

LES DANGERS SUR INTERNET

Ou comment se protéger dans la jungle du Web

SOMMAIRE



Web et Internet ?

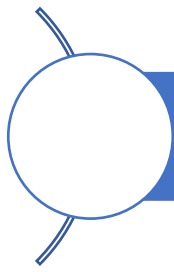
Règles fondamentales

Navigation et achats

Les mails

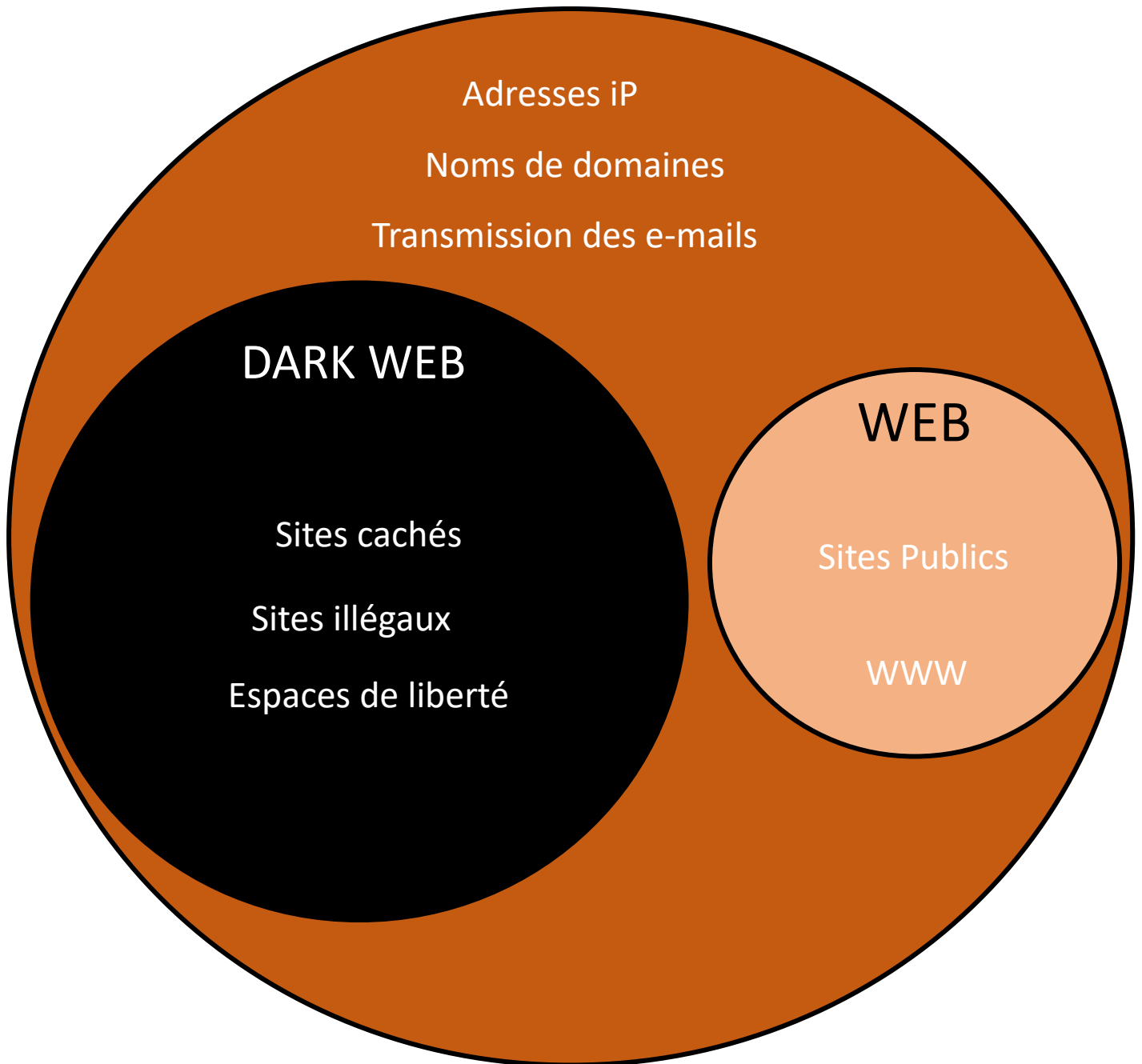
Les Smartphones

Et l'écologie ?

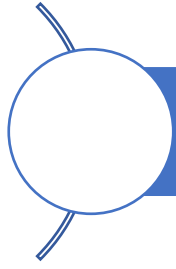


Web et Internet ?

INTERNET



195.14.0.198 *TRADUCTION* → <https://www.ville-monnaie.fr>



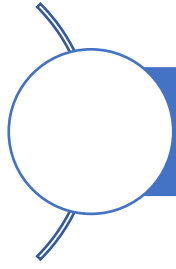
Règles fondamentales

MISES à JOUR

- Navigateur
- Antivirus
- Système d'exploitation

LA CONNEXION

- Sécuriser votre accès WiFi(WPA2 avec 20 caractères minimum)
- Attention aux Hotspot
- Compte standard plutôt qu'administrateur



Navigation et Achats

- La problématique des mots de passe
 - Eviter les mots de passe simples (Date de naissance, prénoms, villes, départements etc...)
 - Alternier chiffres et caractères spéciaux
 - Une longueur de 10 à 12 caractères minimum
 - Changez régulièrement de mot de passe : environ 90 jours
 - Ne revenez JAMAIS à un ancien mot de passe.
 - « G1MO2PASCQRIZÉ »
 - Passez aux phrases de passe : par exemple, « Lareine@presque100Ans! »
 - N'utilisez jamais le même mot de passe pour différents services : Prenez par exemple les 3 premières lettres d'un site puis les 3 dernières.
 - Ne pas les enregistrer dans votre navigateur
 - Utilisez un gestionnaire sécurisé de mots de passe comme Keepass ou EnPass.
- Le piège des cases à cocher
 - Décochez la case « Se souvenir de moi », prenez un peu plus de temps pour ressaisir votre mot de passe.
 - Décochez les cases de newsletters, abonnements divers et surtout offres promotionnelles des fameux sites tiers.
 - Lisez bien TOUT ce qui est écrit sur la page.
- Avoir le bon « clic »
 - Toujours vérifier où un lien vous amène avant de cliquer dessus.
 - Vérifier que vous êtes sur le site souhaité grâce à son adresse.
 -

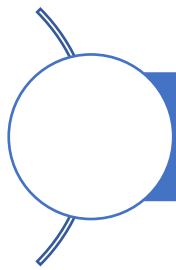
- Vérifiez régulièrement le HTTPS
- Pas de clic sur les pubs, elles sont vectrices de maladies informatiques et ne respectent pas votre vie privée.
- TOUJOURS se déconnecter !

- Achats sécurisés ?
 - Toujours en HTTPS avec le cadenas
 - Se connecter à votre compte toujours en HTTPS aussi
 - Lire les conditions de vente et surtout les conditions en cas de problème (défaut, distribution...)
 - Trouver où se trouve le siège social (généralement dans les CGV)
 - Conserver une copie de votre transaction (copie d'écran, PDF, mail...)
 - Pas d'achats ou de connexion à votre banque à partir d'un ordinateur public ou d'une connexion Wifi publique.

- Bonnes affaires et e-réputation
 - Attention aux ventes à prix très bas -> Arnaques ?
 - Si le site comporte trop de fautes d'orthographe, méfiance.
 - Vérifier les avis sur le site, avec Google Maps par exemple.

- Vie privée
 - Ne partager pas votre localisation.
 - Attention aux réseaux sociaux : tout est enregistré et gardé, même ce qui est supprimé et les saisies effacées.
 - Les GAFAM vivent de vos données.
 - Soyez conscient des interactions et des partenariats entre sites.
 - Changer de Moteur de recherche : abandonner Google pour Qwant par exemple (ou DuckDuckGo).
 - Changer de navigateur : abandonner Chrome pour Firefox par exemple ou Brave.

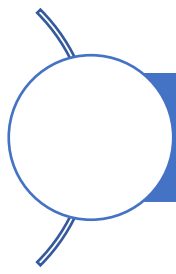
- Vider le cache de son navigateur (fichiers temporaires, historique, cookies)
- Attention aux documents scannés laissés sur le Web (Usurpation d'identité).
- Restreindre la collecte de données sous Windows 10
- Ransomwares : attention au cryptage et au kidnapping de vos données contre une rançon.



Les mails

- Bien écrire et créer les mails
 - Utiliser la zone Cci si plusieurs destinataires (même s'ils se connaissent).
 - Ne négligez pas les formules de politesse.
 - N'hésitez pas à mettre en place des signatures automatiques (avec formule de politesse au besoin).
 - Ne négligez pas l'objet du mail sans pour autant tomber dans l'excès.
 - Munissez-vous, créez, plusieurs adresses mails en fonction de vos besoins.
- Bien recevoir les mails
 - Attention aux SPAMS, aux courriers indésirables, vecteurs de perte de temps et soucis de sécurité.
 - Attention au Phishing -> Vérifiez bien la destination du lien !
 - Lorsque vous recevez un email contenant une pièce jointe que vous n'attendiez pas, ne la téléchargez pas. Surtout si vous ne connaissez pas l'expéditeur. Et si vous connaissez l'expéditeur, demandez-vous s'il est susceptible de vous l'avoir envoyé volontairement ou si sa boîte mail n'a pas été piratée.
 - Ne relayez pas les chaînes de mails. Sous couvert de solidarité ou d'information choc à diffuser au plus grand nombre, vous risquez de propager un hoax, une fake news.
 - Attention aux mails d'amis ou de la famille demandant de l'aide car en vacances et ayant perdu leur argent.
- Les pièces jointes

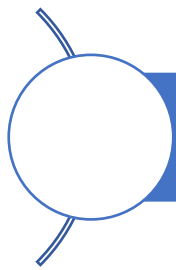
- Ne dépassez pas 5Mo de pièce jointe : cela vous assure quasiment la délivrance de vos messages et n'encombre pas la bande passante de vos destinataires, ni leur disque dur ou le serveur (voir chapitre écologie).
- Comprimez vos pièces jointes.
- PEBCAK ?
 - « *Problem exists between chair and keyboard* » (littéralement « le problème est situé entre la chaise et le clavier »)



Les Smartphones

- La problématique du Wifi
 - Le Wifi sert à être pisté : exemple des magasins
 - Déconnecter le Wifi dès que vous n'en avez plus besoin.
- La problématique de la Géolocalisation
 - Comme le Wifi, ça sert à vous suivre, comme un GPS.
 - A désactiver si vous ne souhaitez pas utiliser de cartes ou faire des recherches des restaurants par exemple autour de vous.
- Le verrouillage : ne laissez pas le paramétrage par défaut avec le glissement, passez par le schéma ou le code PIN
- Les Applications et la vie privée
 - Les droits des applications sont souvent excessifs : une application de lampe torche (pour transformer votre flash en lampe) a-t-elle besoin d'accéder à vos contacts ou aux informations de votre Wifi ?
 - La hausse des malwares sur plateforme Android est de 300 % en 2017 et a pour but de vous espionner principalement.
 - Téléchargements exclusivement sur le Play Store ou l'Apple Store.
- Les effets néfastes
 - Addiction
 - Etat de manque
 - Troubles du sommeil
 - Lumière bleue
 - Radiofréquences
 - Accidents
 - 25 millions de smartphones
 - 1/3 l'utilise en conduisant soit 8 millions

- < 35 ans : ½ l'utilise en conduisant.
- Risque d'accident X 23
- Troubles musculosquelettiques
- Perte de données et vol
- Nomophobie : peur de sortir sans téléphone
- Autisme : écrans > 2 heures/ jours



L'écologie

Internet représente environ 10% des émissions de Co2

Internet en France équivaut à la conso électrique de Bordeaux en 2016.

Le réseau Internet consomme chaque année l'équivalent de l'énergie produite par 40 centrales nucléaires ;

Le visionnage des vidéos sur YouTube représente 1,2 % de la consommation électrique mondiale

Les quelques 500 millions de tweets envoyés chaque jour génèrent 10 tonnes de CO2, soit environ ce qu'émet un Français pour se chauffer, se déplacer, s'équiper et manger chaque année.

- Les mails
 - Nettoyer vos messages afin d'alléger la charge de stockage des serveurs et donc leur conso électrique.
 - Désabonnez-vous des newsletters qui ne vous intéressent plus.
 - Opter pour une signature sobre de bas de mail.
 - Evitez d'utiliser le Répondre à tous quand pas nécessaire.
 - Transférez les documents lourds par clé USB.
- Le Cloud
 - Ne pas trop recourir au stockage sur le cloud, ça consomme de l'électricité
 - Vider le cloud régulièrement.
- Les moteurs de recherche
 - Saisissez directement l'adresse du site dans la barre en haut de la fenêtre de votre navigateur.
- Autres astuces
 - Bloquez les pubs sur le Net
 - Prenez soin de votre matériel (en le nettoyant avec CCleaner par exemple) afin de prolonger sa durée de vie.
 - Nettoyer les poussières dans votre ordinateur : ça évite qu'il chauffe et consomme de trop.

- Sauvegardes régulières
- Partition de Disque Dur entre l'OS et les données.
- Eteignez les box le soir : besoin de Wifi en dormant ?
- Eteignez votre ordinateur si vous ne l'utilisez pas pendant plus de deux heures.
- Débrancher l'alimentation de votre ordinateur portable en cas de non utilisation : cela consomme toujours de l'électricité, même si la batterie est en pleine charge.



Conclusion

Chacun est légalement responsable de sa connexion internet et, le cas échéant, de son mauvais usage : voir loi HADOPI

Bonnes pratiques Internet pour les enfants.

<https://play.google.com/store/apps/details?id=com.qwant.games.incollables.maif&hl=fr>