« Cookie : Anciennement : petit gâteau sucré, qu'on acceptait avec plaisir. Aujourd'hui : petit fichier informatique drôlement salé, qu'il faut refuser avec véhémence. » Luc Fayard

DOMAINE 4 du pix : Protection et sécurité

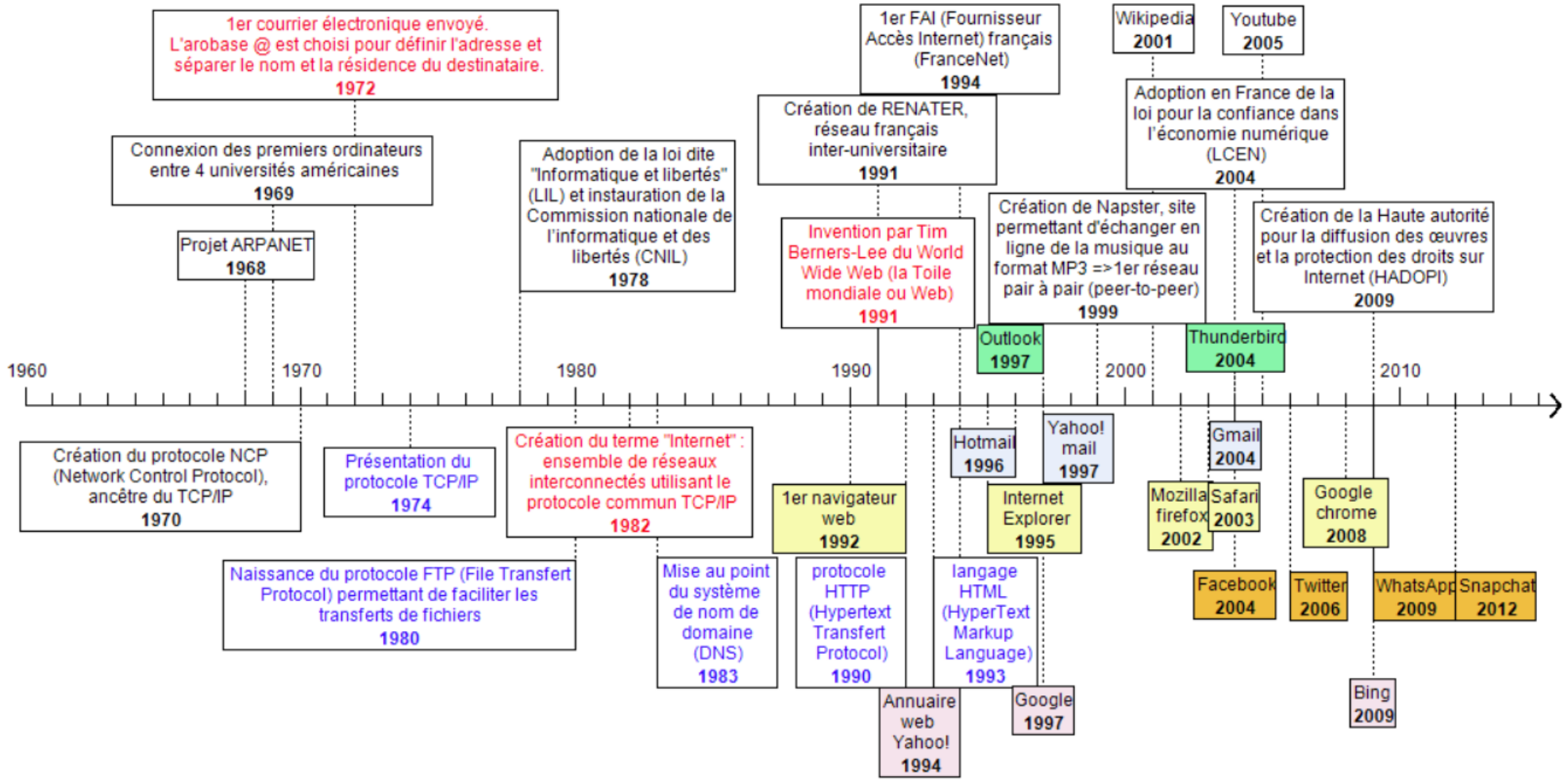
Table des matières :

Partie 1 : Internet et protocoles 2
I / Un petit historique 2
II / Réseaux et Internet 3
III / Les protocoles 4
Partie 2 : Compétence 4.1, Sécuriser l'environnement numérique 8
I / Qui peut attaquer mon ordinateur ? 9
II / Quels sont les principaux types d'attaque informatique ? 9
III / Quels sont les différents types de logiciels malveillants ? 11
IV / Les sites sécurisés 11
V / Le chiffrement de bout en bout, c'est quoi ? 12
VI / Le certificat SSL, c'est quoi ? 12
VII / Vérifier l'intégralité d'un fichier : 12
VIII / Quel site permet de savoir si mes données ont été rendues publiques ? 13
IX / Comment éviter les comportements à risque : les bonnes pratiques 13
Partie 3 : Compétence 4.2, Protéger les données personnelles et la vie privée 14
I / Quels textes règlementaires protègent la confidentialité des données des citoyens ? 14
II / Guide des autorisations des applications d'Android 15
III / Internet et données personnelles 17
Partie 4 : Compétence 4.3, Protéger la santé au travail, le bien-être et l'environnement 18
I / Santé 18
II / Cyberharcèlement 19
III / Environnement et électricité : 20
IV / Environnement et métaux rares 21

Partie 1 : Internet et protocoles

I / Un petit historique

Saviez-vous que Mark Zuckerberg a créé Facebook dans sa chambre d'étudiant à Harvard en 2004 ?



II / Réseaux et Internet

Le **réseau informatique** est un ensemble d'équipements reliés entre eux pour échanger des informations, stocker des données… Par exemple, celui de l'IUT est composé de tous les ordinateurs ou périphériques qui sont reliés entre eux. Vous aurez accès au réseau par connexion filaire (par un fil relié au port Ethernet).

Internet (aussi appelé **Net**) est un réseau informatique mondial. Il résulte d'une interconnexion d'une multitude de réseaux informatiques privés et publiques à travers la planète.

Comment fonctionne les ordinateurs pour communiquer en réseau ?

Pour communiquer entre eux, les ordinateurs d'un réseau échangent très rapidement des données binaires (que des 0 ou des 1).
Le principe de fonctionnement est simple, c'est le même que pour envoyer des cartes postales (ou des colis).
Le seul élément différent (enfin presque) est l'adresse utilisée.

- Pour une carte postale on utilise l'adresse du destinataire (nom+ rue + code postale)
- Pour un ordinateur, on utilise son adresse IP.

La gestion des ressources techniques d'internet est centralisée par les Etats-Unis.

Neutralité du Net :

La neutralité du Net, **c'est ce principe qui régit Internet depuis ses débuts**, et qui garantit un traitement technique identique à tous les fournisseurs de contenus, petits ou grands, consensuels ou dérangeants.
En fait, il s'agit **d'un principe de non-discrimination** : tout le monde doit avoir un égal accès à Internet et aucun contenu (vidéo, site Web…) ne doit bénéficier d'un traitement préférentiel et s'afficher plus vite que les autres. Cette règle empêche le fournisseur d'accès à Internet d'influer sur ce que fait l'internaute ou sur la vitesse à laquelle sont transmis les paquets de données sur le réseau.
En réalité, **la neutralité du Net est très importante**. Elle intervient à chaque connexion à Internet, que vous vouliez regarder une vidéo sur YouTube, envoyer un mail… En clair, toutes les données doivent être traitées de la même manière, qu'elles proviennent de monsieur Tout-le-monde, du gouvernement ou des grosses entreprises. C'est comme ça que Google, YouTube, ou Facebook ont réussi à naître et à grandir, pour supplanter certaines compagnies.
Le principe de neutralité garantit donc la libre circulation des informations sur le réseau.
Il permet le droit d'accès à tous les sites internet sans restriction.
Il assure que le contenu des pages consultées ne soit pas modifié.

Le World Wide Web

Le **World Wide Web** (appelé Web ou toile), inventé par Tim Berners-Lee, est une technologie permettant de consulter, via des **navigateurs** (logiciels de navigation comme internet explorer, safari, chrome, firefox…) des pages regroupées sur des sites.
L'image de la toile (d'araignée) découle des liens hypertextes qui relient les pages entre elles et qui peuvent donc faire penser à une toile d'araignée.
Il ne faut pas confondre internet et le web ! Le web est une application d'internet comme le courrier électronique, le partage de fichiers (avec le protocole FTP ou en peer to peer), la messagerie instantanée, etc…
Le 1er site web, créé par Tim Berners-Lee, est toujours disponible: http://info.cern.ch

III / Les protocoles

Qu'est-ce qu'un protocole ?

Un protocole est un ensemble de règles définissant le mode de communication (c'est-à-dire l'échange de données) entre deux ordinateurs.

1. L'adresse IP (Internet Protocol)

Qu'est-ce l'adresse IP ?

L'adresse IP est une « adresse » (un code) internet qui permet d'identifier de manière unique mon ordinateur sur le réseau ou sur internet en utilisant le protocole IP. Elle géolocalise mon ordinateur, permet la transmission de données sur un réseau et sert d'identifiant personnel pour toute autorité. Elle peut être statique (elle ne change pas) ou dynamique (elle change en fonction de certaines conditions).

Il existe deux types d'adresse IP :

- Adresse IPv4 (Version 4) : Ce sont les anciennes adresses, les plus couramment utilisées. Elles tendent à disparaitre.
  - Notation avec 4 valeurs comprises entre 0 et 255, séparées par des points.
    Par exemple : 192.168.1.10
  - Longueur de 32 bits, c'est-à-dire 4 octets
- Adresse IPv6 (Version 6) : Ce sont les nouvelles adresses.
  - Notation hexadécimale avec 8 valeurs séparées par des « : »
    Par exemple : 1987:0c02:0000:0000:cf2a:9077
  - Longueur de 128 bits, c'est-à-dire 16 octets

Adresse IP privée ou publique

- L'adresse IP privée est celle que l'on peut utiliser pour les équipements sur un réseau local (maison, réseau de l'IUT, réseau d'entreprise, …) Elle ne peut pas être directement utilisée sur internet car elles ne sont pas reconnues sur Internet.
- L'adresse IP publique est unique au monde. C'est ce qui provoque la pénurie des adresses IPv4. L'adresse IPv6 est celle utilisée par votre Box, un site internet, …

Utilisateur, client Adresse IP privée	⇒	Box de la maison Adresse IP fixe	⇒	Serveur internet Adresse IP fixe

Où trouver l'adresse IP ?

- Dans les données associées à un commentaire d'un réseau social
- Dans l'en-tête d'un courrier électronique (Dans les 3 … à droite, chercher l'original)
- Dans l'historique d'un article modifié de Wikipédia
- Sur la page HTML

Localiser l'adresse IP ?

Pour connaitre l'endroit où se situe une personne, trouver son adresse IP sur la page HTML et entrer cette adresse dans un site dédié. Vous obtiendrez sa localisation.
Sur Google, on peut demander « Quelle est la localisation de l'adresse IP … ? »

Serveur de noms Internet (DNS : Domain Name Server) :

Lorsque qu'un client désire une ressource, il doit d'abord localiser où se trouve cette ressource. Pour cela il fait appel à son DNS qui localisera la ressource pour lui. Le serveur DNS permet de traduire le nom complet d'une ressource disponible sur le réseau (en général Internet mais cela est aussi vrai pour un réseau local) en une adresse IP et un chemin d'accès à cette ressource. La réciprocité est vraie. Le serveur DNS sert en quelque sorte d'annuaire de site web.

2. Protocole pour le transfert de données sur internet : TCP (Transmission Control Protocol) ou TCP/IP

Le protocole TCP est un protocole de **transfert de données fiable** (mais pas forcément sécurisé).
Lors d'une communication à travers le protocole TCP, les deux machines doivent établir une connexion.
La machine émettrice (celle qui demande la connexion) est appelée **client**, tandis que la machine réceptrice est appelée **serveur**. On dit qu'on est alors dans un environnement **Client-Serveur**.
Les machines dans un tel environnement communiquent en mode connecté, c'est-à-dire que la communication se fait dans les deux sens.
Les données (messages) sont fractionnées et encapsulées dans un **paquet de données** ou segment (1 paquet = 1500 octets). L'acheminement des données sur le réseau est appelé **routage.**
La taille des paquets (1500 octets) de données circulant sur un réseau comme Internet est limitée. La fragmentation permet de transmettre des paquets de données en plusieurs morceaux.
Pour assurer la fiabilité des transferts de données (aussi appelés segments), chaque transfert est associé à un numéro d'ordre. A réception de ce segment de données, la machine réceptrice retourne un accusé réception. La machine émettrice sait alors que les données sont bien arrivées. **On assure ainsi le contrôle des erreurs de transmission de données.**
Le protocole TCP détermine et fixe les règles inhérentes à l'émission et à la réception de données sur un réseau.

Le tableau ci-dessous montre une partie de l'en-tête d'un paquet de données :

<table>
<tr><td>Version d'IP</td><td></td><td></td><td colspan="2"></td></tr>
<tr><td colspan="3">Identification</td><td>Indicateur</td><td>Fragment offset :</td></tr>
<tr><td colspan="2"></td><td>Protocole :</td><td colspan="2"></td></tr>
<tr><td colspan="5">Adresse IP du commanditaire</td></tr>
<tr><td colspan="5">Adresse IP du destinataire</td></tr>
</table>

Version d'IP :	Version du protocole réseau de l'adresse IP de ce paquet
Identification :	N° permettant d'identifier les fragments d'un même paquet
Indicateur :	010 : Le paquet ne peut pas être fragmenté. 001 : Ce paquet est un fragment de données, d'autres paquets doivent suivre. 000 : Soit c'est le dernier paquet (dans ce cas fragment offset est différent de 0) Soit le paquet n'est pas fragmenté
Fragment offset :	Position du fragment par rapport au paquet de départ, en nombre de mots de 8 octets. Lorsque la valeur est 0, il s'agit du premier fragment
Protocole :	n° du protocole : TCP = 6 ; UDP = 17 ; ICMP = 1

Protocole TCP/IP

Le protocole TCP/IP a été créé, à l'origine, dans un but militaire pour répondre à certains critères :

- Le fractionnement des messages en paquets (par exemple, 1 paquet = 1500 octets)
- L'utilisation d'un système d'adresses pour identifier les ordinateurs du réseau
- L'acheminement des données sur le réseau (routage)
- Le contrôle des erreurs de transmission des données

Les raisons principales de son succès sont :

- Adresse unique (IP) attribuée à chaque ordinateur (appelé hôte) par le protocole IP
- Simplicité du protocole de communication TCP/IP
- Services de base universels (courrier électronique, transfert de fichiers, chat, …)
- Faibles couts de communication

3. Protocole FTP

File Transfer Protocol (protocole de transfert de fichier), ou **FTP**, est un protocole de communication destiné au partage de fichiers sur un réseau TCP/IP. Il permet, depuis un ordinateur, de copier des fichiers vers un autre ordinateur du réseau, ou encore de supprimer ou de modifier des fichiers sur cet ordinateur. Ce mécanisme de copie est souvent utilisé pour alimenter un site web hébergé chez un tiers.

4. Protocole SNMP (gestion de réseau)

Simple Network Management Protocol, en français « protocole simple de gestion de réseau », est un protocole de communication qui permet aux administrateurs réseau de gérer les équipements du réseau, de superviser et de diagnostiquer des problèmes réseaux et matériels à distance.

5. Protocole pour les applications sur internet : HTTP (Hypertext Transfer Protocol)

Le protocole HTPP ou protocole de transfert hypertexte permet à un client (le navigateur) de communiquer avec un serveur web en lui envoyant des requêtes pour obtenir des documents (comme des pages HTML) qui peuvent contenir des liens vers d'autres documents.

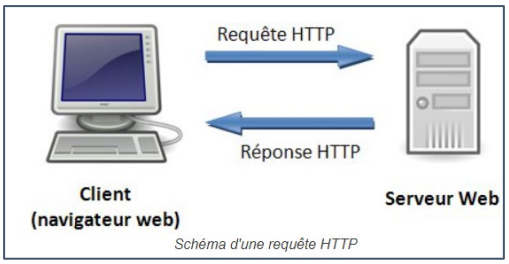


Schéma d'une requête HTTP

Site sécurisé :

Lors d'un achat, vérifier que le site est sécurisé (https)

En effet, il existe 2 types de sites internet.

- ✓ Ceux dont l'adresse commence par « http:// ». (Site non sécurisé)
  Les données transmises en http transitent en clair.
  Évitez de faire vos achats sur les sites en « http:// » et ne créez par un compte sur un site lorsque l'url commence par « http:// » car les informations (mot de passe, informations personnelles, informations bancaires, etc.) peuvent être interceptées par des tiers (cette condition est nécessaire, mais pas suffisante).

- ✓ Ceux dont l'adresse commence par « https:// ». (Site sécurisé)
  Le protocole https est une variante du protocole http incluant l'utilisation de canal de communication sécurisé. En effet, les informations seront cryptées (chiffrées).
  En général, au moment du paiement, un petit cadenas est visible dans l'adresse de votre navigateur.
  Pour le paiement, on utilisera en plus le protocole TLS.
  

FQDN (Full Qualified Domain Name)

Le terme « Fully Qualified Domain Name », abrégé en FQDN, désigne l'adresse complète et unique (adresse absolue) d'un site Internet.

Il se compose : Exemple www.

- du nom d'hôte (Ici www désigne une page Web)
- du nom du domaine (Ici google.fr : .fr désigne le suffixe ou l'extension d'un site français).

Il est utilisé pour localiser des hôtes spécifiques sur Internet et les interroger à l'aide de la résolution de nom.

Les FDQN sont une forme littérale d'écriture des adresses IP. Par exemple www.google.fr est associé à l'adresse IP 209.85.147.94.

Les protocoles HTTP et FQDN sont séparés par //.

Fonctionnement du protocole HTTP : Les requêtes et les réponses :

Il existe deux types de messages HTTP, les requêtes et les réponses, chacun ayant son propre format.

Exemple :

```
GET / HTTP/1.1
Host : Sitefictif.net
User-Agent : Mozilla/5.0 …
Accept : image/webp,*/*
Accept-Language : fr-FR….
Accept-Encoding : gzip, deflate, br
Connection : keep-alive
[…]
```

```
http/1.1  200 OK
Date : Tue, 19 oct 2021 12 :09 :32 GMT
Server : Apache
X-Powered-By : PHP/7.4.6
Connection : Close
Content-Length : 5265
Content-Type : text/html ; Charset=UTF-8
[…]
```

```
GET  / images/logo.png HTTP/1.1
Host : Sitefictif.net
User-Agent : Mozilla/5.0 …
Accept: image/webp, */*
```

Une requête comprend les éléments suivants :

- ✓ Une **méthode** HTTP : généralement un verbe tel que GET, POST ou un nom comme OPTIONS ou HEAD qui définit l'opération que le client souhaite effectuer.
  Par exemple, un client souhaite accéder à une ressource (en utilisant GET) ou téléverser le résultat d'un formulaire HTML (en utilisant POST).
- ✓ La version du protocole HTTP.
  Les messages HTTP/1.1 et ceux des versions précédentes d'HTTP sont lisibles par des humains.
- ✓ Le chemin de la ressource à extraire : l'URL de la ressource.
- ✓ Les en-têtes optionnels qui transmettent des informations supplémentaires pour les serveurs.
  L'en-tête HTTP **`Accept-Encoding`** permet de définir quel sera l'encodage du contenu. Il s'agit généralement de l'algorithme de compression utilisé par le serveur. Le serveur choisit l'une des propositions d'encodage que le client prend en charge. Le serveur l'utilise et le notifie au client à l'aide de l'en-tête de réponse **`Content-Encoding`**.
  L'en-tête général **`Connection`** contrôle la façon dont la connexion reste ouverte ou non après que la transaction courante soit terminée. Si la valeur envoyée est **`keep-alive`**, la connexion est persistante et n'est pas fermée, permettant aux requêtes qui suivent et s'adressent au même serveur d'être envoyées.
- ✓ Ou un corps, pour certaines méthodes comme POST, semblable à ceux dans les réponses, qui contiennent la ressource envoyée.

Une réponse comprend les éléments suivants :

- ✓ La version du protocole HTTP qu'elle suit
- ✓ Un code de statut, qui indique si la requête a réussi ou non. (http/1.1 200 OK)

Code statut	200	La requête a abouti	200 OK = Validé
	403	Erreur de la part du client	Accès interdit
	404	Erreur de la part du client	Not found (Non trouvé)

- ✓ Les en-têtes HTTP, comme pour les requêtes.

Partie 2 : Compétence 4.1, Sécuriser l'environnement numérique

Pour lutter contre les intrusions malveillantes, il faut sécuriser son espace de travail. Ainsi, il faut éviter les comportements à risques et avoir un logiciel de protection installé sur sa machine.

Pourquoi faut-il sécuriser son espace de travail ?

- Pour pouvoir accéder à nos ressources **quand on en éprouve le besoin** et **pour le temps nécessaire**.
- Pour pouvoir accéder à nos ressources **sans que celles-ci aient été modifiées**.
- Pour que mes données restent **confidentielles** (mot de passe, n° de carte, fichier, …).

Quels sont les risques ?

- La récupération de mes données personnelles,
- La prise de contrôle de mon ordinateur, ainsi que son exploitation pour lancer des attaques,
- Le détournement de mon IP personnelle (l'adresse internet permet d'identifier de manière unique mon ordinateur sur le réseau), l'usurpation d'identité,
- La perte de mes données, …

Qu'est-ce l'adresse IP ?

L'adresse IP est une « adresse » (un code) internet qui permet d'identifier de manière unique mon ordinateur sur le réseau ou sur internet. Elle géolocalise mon ordinateur et sert d'identifiant personnel pour toute autorité. Elle peut être statique (elle ne change pas) ou dynamique (elle change en fonction de certaines conditions).

Qu'est-ce qu'un logiciel ?

Un logiciel est un ensemble de fichiers permettant d'exécuter un programme informatique.
Parmi les logiciels, on distingue :

- les applications : logiciels destinés aux utilisateurs comme le traitement de texte, le navigateur, etc. ;
- les logiciels systèmes : logiciels proches de la machine qui permettent aux applications de communiquer avec le matériel.

Le système d'exploitation (Windows, MAC OS, Linux, Unix) est un logiciel système de base.
Chaque application est développée pour fonctionner avec un système d'exploitation spécifique.

Quels sont les logiciels qui protègent votre ordinateur ?

- Windows Defender
- Kasperky
- Bitdefender
- Norton security
- Avast premier
- McAfee Total Protection…

Quelles sont les principales fonctionnalités d'un anti-virus ?

- Mettre en quarantaine un fichier infecté pour empêcher sa propagation.
- Assurer une protection résidente qui analyse tout fichier entrant.
- Réparer un fichier infecté quand c'est possible.

I / Qui peut attaquer mon ordinateur ?

Un « hacker » informatique désigne un virtuose en informatique qui utilise ses compétences dans le but de résoudre un problème lié à la programmation, l'architecture matérielle d'un ordinateur, l'administration système, l'administration réseau, la sécurité informatique ou tout autre domaine de l'informatique.
Les médias associent souvent les hackers aux pirates, personne qui utilise ses compétences de façon nuisible, illégale.

En général, on distingue plusieurs types de hackers :

- Les « **White hat hackers** » sont des professionnels de la sécurité informatique.
- Les « **Black hat hackers** » ou **pirates** informatiques sont des cybers escrocs (ou cyber criminel). leurs buts est de gagner de l'argent en :
  - créant des virus (en détruisant ou contournant les protections des logiciels),
  - vendant des informations piratées,
  - extorquant de l'argent.
- Les **chapeaux gris ou Grey hat** n'ont pas de mauvaises intentions et sont souvent motivés par l'exploit informatique.
- Les **hacktivistes** agissent afin de défendre une cause, ils peuvent transgresser la loi pour attaquer des organisations afin de les paralyser ou d'obtenir des informations

II / Quels sont les principaux types d'attaque informatique ?

Une **cyberattaque** est tout type d'action offensive qui vise des systèmes, des infrastructures ou des réseaux informatiques, ou encore des ordinateurs personnels, en s'appuyant sur diverses méthodes pour voler, modifier ou détruire des données ou des systèmes informatiques.

- **Le "spam"** ou pourriels est un simple courrier publicitaire non sollicité.

- Le **"spam" téléphonique** existe aussi. Il est généralement adressé à des fins de prospection commerciale mais peut également revêtir un caractère malveillant (incitation à appeler un numéro surtaxé, …).

- **L'arnaque au faux support technique** consiste à effrayer la victime, par SMS, téléphone, chat, courriel, ou par l'apparition d'un message qui bloque son ordinateur, lui indiquant un problème technique grave et un risque de perte de ses données ou de l'usage de son équipement afin de la pousser à contacter un prétendu support technique officiel (Microsoft, Apple, Google…), pour ensuite la convaincre de payer un pseudo-dépannage informatique et/ ou à acheter des logiciels inutiles, voire nuisibles. Si la victime refuse de payer, les criminels peuvent la menacer de détruire ses fichiers ou de divulguer ses informations personnelles.

- **L'arnaque aux faux ordres de virement** consiste pour le fraudeur à se faire passer pour un directeur en **usurpant son identité** et à vous demander de réaliser un virement à l'international.

- Le «**typosquatting**» : quand les pirates informatiques exploitent les fautes de frappe

- Le **"smishing"** (mot composé de SMS et phishing) consiste à transmettre des messages type SMS pour tromper des victimes en les incitants à agir immédiatement. En effet, nous avons plus confiance en nos SMS qu'en nos mails.

- Le **"phishing" ou hameçonnage** consiste pour le fraudeur à se faire passer pour un organisme qui vous est familier (banque, administration fiscale, caisse de sécurité sociale…), en utilisant son logo et son nom. Vous recevez un courriel dans lequel il vous est demandé de "mettre à jour" ou de "confirmer suite à un incident technique" vos données.
  Leur but est de soutirer des informations confidentielles comme :
  - Des données personnelles : nom, prénom, adresse postale ou de messagerie, numéro de téléphone…
  - Des identifiants de connexion : nom d'utilisateur, mot de passe…
  - Des informations bancaires : RIB, numéro de carte bancaire…

  Autrefois facilement identifiables, ces arnaques par message électronique apparaissent de mieux en mieux réalisées et même les internautes les plus avertis peuvent parfois s'y méprendre.
  Voici quelques éléments que vous devez observer avec attention :
  - **Le corps du texte. Attention aux** éventuelles fautes d'orthographe, de grammaire…
  - **L'adresse de messagerie de l'expéditeur.**
  - **Le lien.**

- **Chantage à l'ordinateur ou à la webcam piratés** (dit « **cryptoporno** ») désigne un type d'escroquerie qui vise à vous faire croire que vos équipements ont été piratés afin de vous soutirer de l'argent.
  Il prend généralement la forme d'un message reçu (souvent par courriel). Le cybercriminel annonce avoir des vidéos compromettantes qu'il menace de publier si la victime ne lui verse pas une rançon.

- Un **défacement** exploite la faille de sécurité d'un système d'exploitation d'un serveur web de manière à modifier la présentation d'un site internet. Les défaceurs attaquent les sites web principalement pour exprimer leur revendication. Ainsi les principales cibles sont des organisations gouvernementales ou des sites religieux.
  Lorsqu'un site web est défiguré, il doit se mettre hors ligne. Sa maintenance entraîne une grande perte de temps et d'énergie. L'image de l'organisation est endommagée puisqu'il ne paraît pas sécurisé.

- Une **attaque par l'homme du milieu** représente un pirate qui s'insère dans les communications entre un client et un serveur réseau :
  1. Le client se connecte à un serveur.
  2. Le pirate s'insère entre le client et le serveur. Il déconnecte le client et prend sa place. Il usurpe ainsi l'identité du client et continue le dialogue avec le serveur.

- Une **injection SQL** est devenue un problème courant qui affecte les sites Web exploitant des bases de données. Elle se produit lorsqu'un malfaiteur exécute une requête SQL sur la base de données via les données entrantes du client au serveur. Des commandes SQL sont insérées dans la saisie du plan de données (par exemple, à la place du nom d'utilisateur ou du mot de passe) afin d'exécuter des commandes SQL prédéfinies. Un exploit d'injection SQL réussi peut lire les données sensibles de la base de données, modifier (insérer, mettre à jour ou supprimer) les données de la base de données, exécuter des opérations d'administration de la base de données (par exemple la fermer), récupérer le contenu d'un fichier spécifique, et, dans certains cas, envoyer des commandes au système d'exploitation.

- **Une attaque par force brute :** Il s'agit de tester une à une, toutes les combinaisons possibles des mots de passe.

- **Une attaque par DNS** : L'objectif de cette attaque est de rediriger, à leur insu, des internautes vers des sites pirates.

III / Quels sont les différents types de logiciels malveillants ?

Un **logiciel malveillant** ou **malware** est un ensemble de programmes conçu par un pirate pour être implanté dans un système afin d'y déclencher une opération non autorisée ou d'en perturber le fonctionnement. Les logiciels malveillants peuvent être transmis via l'Internet, un réseau local ou par des supports tels que les clés USB, les disques durs externes, ...
Parmi les logiciels malveillants, on distingue :

- le virus : logiciel, généralement de petite taille, qui se transmet par les réseaux ou les supports d'information amovibles, **s'implante au sein des programmes en les parasitant**, **se duplique** à l'insu des utilisateurs et **produit ses effets dommageables** quand le programme infecté est exécuté ou quand survient un événement donné.
- le ver : **logiciel indépendant** (il ne s'implante pas au sein d'un autre programme) qui se transmet d'ordinateur à ordinateur par l'Internet ou tout autre réseau et perturbe le fonctionnement des systèmes concernés en s'exécutant à l'insu des utilisateurs. **Les vers sont souvent conçus pour saturer les ressources disponibles ou allonger la durée des traitements**. Ils peuvent aussi **détruire les données d'un ordinateur, perturber le fonctionnement du réseau ou transférer frauduleusement des informations.** Une bombe programmée est un **logiciel malveillant** qui se déclenche lorsque certaines conditions sont réunies.
- Un cheval de Troie (ou Troyen) est un logiciel au sein duquel a été dissimulé un programme malveillant qui peut par exemple **permettre la collecte frauduleuse, la falsification ou la destruction de données.** Le cheval de Troie ne se reproduit pas.
- Un logiciel publicitaire (ou adware) est un logiciel qui affiche des annonces publicitaires sur l'écran d'un ordinateur et qui transmet à son éditeur des renseignements permettant d'adapter ces annonces au profil de l'utilisateur.
- *Les rançongiciels* sont une catégorie particulière de logiciels malveillants qui bloquent l'ordinateur des victimes et réclament le paiement d'une rançon.

IV / Les sites sécurisés

Lors d'un achat, vérifier que le site est sécurisé (http**s**)
En effet, il existe 2 types de sites internet.

- ✓ Ceux dont l'adresse commence par « http:// ». (Site non sécurisé)
  Les données transmises en http transitent en clair.
  Évitez de faire vos achats sur les sites en « http:// » et ne créez par un compte sur un site lorsque l'url commence par « http:// » car les informations (mot de passe, informations personnelles, informations bancaires, etc.) peuvent être interceptées par des tiers (cette condition est nécessaire, mais pas suffisante).

- ✓ Ceux dont l'adresse commence par « https:// ». (Site sécurisé)
  Le protocole https est une variante du protocole http incluant l'utilisation de canal de communication sécurisé. En effet, les informations seront cryptées (chiffrées).
  En général, au moment du paiement, un petit cadenas est visible dans l'adresse de votre navigateur.
  

V / Le chiffrement de bout en bout, c'est quoi ?

Le récepteur du message (Alice) génère une clé privée (A) et une clé publique (B).
Le récepteur du message (Alice) envoie sa clé publique (B) à un émetteur (Bob).
L'émetteur (Bob) chiffre son message avec la clé publique (B) du récepteur (Alice).
Le récepteur (Alice) déchiffre le message de l'émetteur (Bob) grâce à sa clé privée (A).
Seul le récepteur (Alice) pourra prendre connaissance des messages de l'émetteur (Bob).
Il suffit que l'émetteur (Bob) applique le même procédé que le récepteur (Alice) et cet échange de clés publiques leur permet une communication bidirectionnelle sécurisée.
La clé privée (A) est générée aléatoirement et la clé publique (B) est générée à partir de la clé privée.
On appelle cette méthode le chiffrement asymétrique.

Le chiffrement permet d'assurer la confidentialité des données, de certifier les échanges numériques et d'apporter une preuve numérique qu'un document n'a pas été modifié.

VI / Le certificat SSL, c'est quoi ?

Le certificat SSL sécurise le transport des données entre un serveur web et le navigateur des internautes.

Souvent, vous pouvez trouver des informations sur ce certificat dans votre navigateur en cliquant sur le cadenas qui indique la présence du protocole HTTPS.

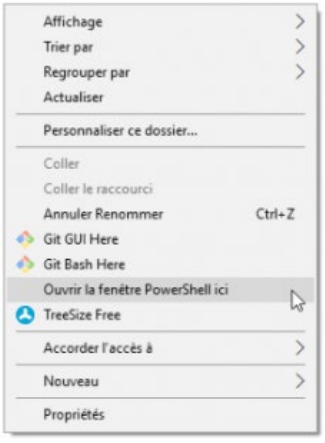
VII / Vérifier l'intégralité d'un fichier :

SHA-256, qui signifie Secure Hash Algorithm (algorithme de hachage sécurisé) 256 bits, est utilisé dans les applications de sécurité cryptographique. Les algorithmes de hachage cryptographique génèrent des hachages irréversibles et uniques.

Pour vérifier l'intégrité d'un fichier téléchargé et être certain qu'il est identique à l'original, il faut calculer la somme SHA-256 et vérifier qu'elle est identique au fichier original.

Trouver la somme SHA-256

1. Télécharger le fichier
2. Aller dans les téléchargements
3. Faire un clic droit dans une zone non vide tout en restant appuyé sur la touche `Maj (⇧)`
4. Cliquer sur : « Ouvrir la fenetre PowerShell ici »



5. Entrez ensuite la commande Get-FileHash .\NomDuFichier.iso -Algorithm SHA256
(Pensez à l'auto-complétion avec la touche `TAB (⇄)`).

VIII / Quel site permet de savoir si mes données ont été rendues publiques ?

Il existe un célèbre site anglophone qui permet de savoir si vos mots de passe, ou d'autres informations personnelles, ont fuité : haveibeenpwned.com

Aller tout en bas de la page et vous trouverez de qui cela provient

IX / Comment éviter les comportements à risque : les bonnes pratiques

Une bonne pratique est l'ensemble de nos actions qui contribue à sécuriser l'ordinateur :

- Installer des logiciels de protection :
  - Antivirus : logiciel possédant une base de données de signatures virales qui scanne les fichiers à la recherche de ces signatures dans leur code. Il les répare les fichiers infectés quand c'est possible ou les met en quarantaine pour empêcher la propagation du virus. (Kaspersky, bit defender). Il est nécessaire quand la connexion passe par un réseau WIFI public.
  - Pare-feu (firewall) est un système permettant de protéger l'ordinateur des intrusions extérieures par le réseau. Il agit comme un filtre entre le réseau et l'ordinateur.
  - Logiciel anti-espion (antispyware) pour éradiquer les logiciels espions (spywares).

- Sécuriser ses mots de passe
  - Avoir des mots de passe de 8 à 12 caractères minimum.
  - Caractères de type différent (majuscules, minuscules, chiffres, caractères spéciaux).
  - Ne pas utiliser de mot de passe ayant un lien avec soi (noms, dates de naissance…).
  - Le même mot de passe ne doit pas être utilisé pour des accès différents.
  - Changer de mot de passe régulièrement (72 jours recommandé !)
  - Ne pas configurer les logiciels pour qu'ils retiennent les mots de passe.
  - Ne pas utiliser des mots de passe avec des mots trouvés dans les dictionnaires.
  - Ne pas noter le mot de passe dans un post-it ou un document à côté.
  - Éviter de stocker ses mots de passe dans un fichier en local.
  - Utiliser des logiciels comme keepass pour les gérer

- Lors d'un achat :
  - Vérifier que le site est sécurisé (http**s**)
  - Ne pas sauvegarder ses données bancaires
  - Eviter de payer sur les réseaux Wi-Fi publics.
  -

- Dans la vie de tous les jours :
  - Mettre à jour son navigateur et les logiciels présents sur votre ordinateur.
  - Se méfier des sites douteux, des pop-ups ou des redirections étranges.
  - Ne pas cliquer sur des liens transmis par messagerie instantanée
  - Ne pas ouvrir les pièces jointes douteuses.
  - Ne pas brancher une clé USB inconnue, cadeau…
  - Ne pas télécharger un film de pair à pair

Partie 3 : Compétence 4.2, Protéger les données personnelles et la vie privée

I / Quels textes règlementaires protègent la confidentialité des données des citoyens ?

Le **Règlement Général sur la Protection des Données (RGPD)** est une **directive européenne** qui a pour but de fixer les conditions dans lesquelles sont collectées, conservées et exploitées des données à caractère personnel au sein de l'Union européenne. Il a été adopté en 2016 et trouve son application en France depuis 2018.
Son but est de protéger la vie privée.
Il s'applique :

- au traitement des données à caractère personnel pour des activités d'un établissement de l'Union Européenne (que le traitement ait lieu ou non dans l'Union ;
- au traitement des données à caractère personnel de personnes se trouvant sur le territoire de l'Union même si l'établissement n'est pas dans l'Union ;
- au traitement des données à caractère personnel pour des activités d'un établissement régi par le droit RGPD.

Les droits du Règlement général sur la protection des données :

- **Droit à l'information :** Rester informé
- **Droit d'opposition :** Vous pouvez vous opposer à tout moment à ce qu'un organisme utilise vos données à des fins commerciales ou idéologiques
- **Droit d'accès :** Vous avez le **droit** de savoir quelles informations les administrations, les organismes publics ou privés et les sociétés commerciales détiennent sur vous dans leurs fichiers.
- **Droit de rectification ou modification :** Rectifier vos données personnelles
- **Droit au déréférencement :** vous avez le droit de déréférencer un contenu, c'est-à-dire ne plus associer votre nom/prénom à un contenu visible dans un moteur de recherche (photo, orientation sexuelle, …). Ce droit est valable sur tout le territoire de l'Union Européenne et partout où la norme RGPD est appliquée. Par exemple, on peut sortir de google.pt (Portugal) ou de google.be (Belgique)
- **Droit à la portabilité :** Possibilité de récupérer une partie de vos données dans un format lisible par une machine. Libre à vous de stocker ailleurs ces données portables ou les transmettre facilement d'un système à un autre, en vue d'une réutilisation à d'autres fins. (Par exemple une play-list)
- **Droit à l'effacement ou à l'oubli :** Effacer vos données si la conservation de celles-ci n'est plus justifiée.
- **Droit lié au profilage :** Le profilage est une technique de traitement automatisé des données personnelles. Elle permet notamment l'analyse et la prédiction de comportements, de performances, etc. Lorsque le profilage est lié à une prise de décision, les personnes physiques peuvent s'y opposer.
  L'article 22 du RGPD énumère **trois situations** dans lesquelles le profilage engendrant une décision automatisée peut être autorisé. En effet, cela est possible dans les cas où la décision est :
  - **nécessaire à l'exécution ou à la conclusion d'un contrat** entre la personne concernée et le responsable du traitement des données ;
  - **autorisée par le droit de l'Union Européenne ou le droit national ;**
  - fondée sur le consentement explicite de la personne.
- **Droit d'accès FICOBA :** Le FICOBA sert à recenser les comptes de toute nature (bancaires, postaux, d'épargne, etc.) et à fournir aux personnes habilitées des informations sur les comptes détenus par une personne ou une société. Selon votre situation, vous pouvez bénéficier d'un droit d'accès à ce fichier si :
  - Vous êtes titulaire du compte.
  - Vous êtes un héritier.
  - Vous êtes un professionnel agissant pour le compte d'un particulier.
  - Vous êtes un tiers autorisé.
- **Droit d'accès au fichier de la police/gendarmerie :**

En France, l'autorité qui assure la protection des données est la CNIL (Commission Nationale Informatique & libertés).

La loi HADOPI (Haute Autorité pour la diffusion des œuvres et la protection des droits sur Internet), créée en 2009. Elle permet notamment de combattre les téléchargements illégaux et d'interdire les sites web immoraux.

II / Guide des autorisations des applications d'Android

Les autorisations système peuvent être divisées en deux groupes : les normales et les autorisations à risque. Les groupes des autorisations normales sont autorisés par défaut, parce qu'ils ne posent pas de risque pour votre confidentialité. (Par exemple, Android permet aux applications d'accéder à Internet sans votre permission). Les groupes des autorisations à risque, cependant, peuvent donner aux applications l'accès à des éléments comme l'historique des appels, les messages privés, l'emplacement, l'appareil photo, le microphone, et plus encore. Par conséquent, Android vous demandera toujours d'approuver les autorisations à risque.

Autorisations potentiellement à risque à surveiller
Toute personne soucieuse de la protection de sa vie privée et de sa sécurité devrait surveiller les applications qui demandent l'accès aux neuf groupes d'autorisations suivants. Chaque groupe contient plusieurs autorisations et l'approbation d'une seule autorisation de n'importe quel groupe approuve automatiquement toutes les autres autorisations au sein de ce même groupe. (Par exemple, si vous autorisez une application à voir qui vous appelle, vous lui permettrez aussi de passer des appels téléphoniques.)

- **Capteurs corporels**
  Autorise l'accès à vos données de santé à partir des cardio fréquence mètres, de trackers de fitness et d'autres capteurs externes.
  Avantage : les applications de fitness ont besoin de cette autorisation pour surveiller votre fréquence cardiaque pendant que vous faites de l'exercice, fournir des conseils de santé, etc.
  Inconvénient : une application malveillante pourrait espionner votre santé.

- **Calendrier**
  Permet aux applications de lire, créer, modifier ou supprimer les événements de votre calendrier.
  Avantage : les applications de calendrier ont évidemment besoin de cette autorisation pour créer des événements de calendrier, mais il en va de même pour les applications de réseautage social qui vous permettent d'ajouter des événements et des invitations à votre calendrier.
  Inconvénient : une application malveillante peut espionner vos routines personnelles, l'heure des réunions, etc. et même les supprimer de votre calendrier.

- **Appareil photo**
  Permet aux applications d'utiliser votre appareil photo pour prendre des photos et enregistrer des vidéos.
  Avantage : les applications de photographie ont besoin de cette autorisation pour que vous puissiez prendre des photos.
  Inconvénient : une application malveillante peut secrètement allumer votre appareil photo et enregistrer ce qui se passe autour de vous.

- **Contacts**
  Permet aux applications de lire, créer ou modifier votre liste de contacts, ainsi que d'accéder à la liste de tous les comptes (Facebook, Instagram, Twitter, etc.) utilisés sur votre appareil.
  Avantage : une application de communication peut l'utiliser pour vous permettre d'envoyer des SMS ou d'appeler d'autres personnes de votre liste de contacts.
  Inconvénient : une application malveillante peut voler tout le contenu de votre carnet d'adresses, puis cibler vos amis et votre famille avec du spam, des arnaques par hameçonnage, etc.

- **Emplacement**
  Permet aux applications d'accéder à votre position approximative (à l'aide de stations de base cellulaires et de points d'accès Wi-Fi) et à votre position exacte (à l'aide du GPS).
  Avantage : les applications de navigation peuvent vous aider à vous déplacer, les applications de photographie peuvent géolocaliser vos photos pour que vous sachiez où elles ont été prises et les applications de shopping peuvent estimer votre adresse de livraison.
  Inconvénient : une application malveillante peut secrètement suivre votre position pour établir un profil sur vos habitudes quotidiennes ou même faire savoir aux voleurs quand vous n'êtes pas chez vous.

- **Microphone**
  Permet aux applications d'utiliser votre microphone pour enregistrer du son.
  Avantage : une application de reconnaissance musicale comme Shazam l'utilise pour écouter n'importe quelle musique que vous voulez identifier ; une application de communication peut l'utiliser pour vous permettre d'envoyer des messages vocaux à vos amis.
  Inconvénient : une application malveillante peut enregistrer secrètement ce qui se passe autour de vous, y compris les conversations privées avec votre famille, les conversations avec votre médecin et les réunions d'affaires confidentielles.

- **Téléphone**
  Permet aux applications de connaître votre numéro de téléphone, les informations actuelles sur le réseau cellulaire et l'état des appels en cours. Les applications peuvent également passer et terminer des appels, voir qui vous appelle, lire et modifier vos journaux d'appels, ajouter des messages vocaux, utiliser la VoIP et même rediriger les appels vers d'autres numéros.
  Avantage : les applications de communication peuvent l'utiliser pour vous permettre d'appeler vos amis.
  Inconvénient : une application malveillante peut espionner vos habitudes téléphoniques et passer des appels sans votre consentement (y compris des appels payants).

- **SMS**
  Permet aux applications de lire, recevoir et envoyer des messages SMS, ainsi que de recevoir des messages WAP push et MMS.
  Avantage : les applications de communication peuvent l'utiliser pour vous permettre d'envoyer des messages à vos amis.
  Inconvénient : une application malveillante peut espionner vos messages, utiliser votre téléphone pour spammer d'autres personnes et même vous abonner à des services payants non désirés.

- **Stockage**
  Permet aux applications de lire et d'écrire sur votre stockage interne ou externe.
  Avantage : une application musicale peut enregistrer les chansons téléchargées sur votre carte SD ou une application de réseautage social peut enregistrer les photos de vos amis sur votre téléphone.
  Inconvénient : une application malveillante peut secrètement lire, modifier et supprimer n'importe lequel de vos documents, musiques, photos et autres fichiers enregistrés.

III / Internet et données personnelles

Les sites Web auxquels vous vous connectez peuvent avoir accès à :

- Votre adresse IP
- Votre nom d'hôte (hostname) ainsi que le nom de votre fournisseur d'accès
- Votre système d'exploitation
- la page qui vous a conduit jusqu'à lui (c'est-à-dire le navigateur utilisé)
- la résolution de votre écran
- Ils peuvent avec votre autorisation déposer des cookies

Cnil protection des données dans le monde : https://www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde

1. Qu'est-ce qu'un cookie ?

Un cookie est un fichier qui est déposé par le navigateur sur votre ordinateur lorsque vous surfez sur internet.

- Il est stocké sur le disque dur de l'internaute.
- Il est déposé par un site Web lors de la consultation d'une de ses pages
- Il permet à un internaute de naviguer entre les différentes pages d'un site en restant identifié.
- Il permet aux sites de vente en ligne de pouvoir conserver le panier d'achat de l'internaute.
- Il retrace votre historique de navigation.
- Il permet aux annonceurs de proposer de la publicité ciblée.

Comment s'en prémunir ? La navigation privée ?

Les sites Web peuvent garder la trace de votre navigation en déposant des cookies. La navigation privée est un mode spécial de navigation proposé par son navigateur qui permet de naviguer sur le web avec plus de confidentialité. En effet, certaines données de navigation ne sont pas conservées comme :

- l'historique de navigation
- le cache navigateur
- les fichiers temporaires comme les cookies de votre navigateur
- les téléchargements
- le remplissage automatique des formulaires
- les mots de passe enregistrés dans votre navigateur (saviez-vous au passage qu'il était possible de récupérer un mot de passe enregistré dans votre navigateur ?)

2. Comment les emails sont-ils suivis ?

En théorie, le courrier électronique est un support de communication très simple. Mais en réalité, vous n'envoyez pas seulement un message texte à quelqu'un – les emails peuvent contenir du code HTML, comme sur les pages web. Ils peuvent également charger des images, c'est ainsi que fonctionne le suivi.
Lorsque vous ouvrez un email, votre client de messagerie charge les images présentes dans cet email depuis le serveur distant et les affiche, de la même manière que lorsque vous ouvrez une page web. Vous pouvez spécifier à votre client de messagerie de **ne jamais charger d'images** si vous le souhaitez, mais en général, il les charge par défaut.
Les entreprises qui envoient des newsletters par email ou d'autres emails automatisés incluent presque toujours une image de suivi spécifique. Il s'agit d'un minuscule fichier image invisible qui ne mesure qu'un seul pixel, aussi appelé **pixel invisible** ou **pixel espion**. Chaque destinataire de la newsletter se voit attribuer un code de suivi unique au sein de cette image. Ces images sont aussi connues sous le nom de " balises web ". Lorsque vous ouvrez la newsletter, et qu'elle charge des images (même si vous ne pouvez pas les voir), elle charge donc également une balise web. Lorsque cette image spécifique est chargée à partir des serveurs de l'entreprise ou d'un service tiers, l'expéditeur peut dès lors savoir que l'email envoyé à votre adresse vient d'être ouvert.

Partie 4 : Compétence 4.3, Protéger la santé au travail, le bien-être et l'environnement

I / Santé

DAS ?

Dans les caractéristiques techniques de votre téléphone, vous devriez trouver son débit d'absorption spécifique (DAS), exprimé en watts par kilogramme (W/kg).
Les experts du Centre de recherche et d'informations indépendantes sur les rayonnements électromagnétiques (Criirem) jugent préférable d'utiliser des appareils dont l'indice est inférieur à 0,7 W/kg.
Trois types de DAS sont prévus pour mesurer l'exposition due aux téléphones portables :

- La « DAS tête » reflète l'usage du téléphone à l'oreille. Sa valeur limite est de 2 W/kg.
- La « DAS tronc » reflète l'usage du téléphone quand il est porté sur le tronc (poche de veste, sac, …) à l'oreille. Sa valeur limite est de 2 W/kg.
- La « DAS membre » reflète l'usage du téléphone quand il est porté près d'un membre (main, bras avec brassard, …). Sa valeur limite est de 4 W/kg.

Quelles pratiques diminuent l'exposition aux ondes radio émises par un téléphone portable ?

- Bien choisir son téléphone notamment la DAS
- Utiliser un « kit mains-libres » afin d'éloigner le mobile de votre cerveau.
- Ne pas téléphoner dans les transports car lorsque nous nous déplaçons à grande vitesse, notre mobile élève sa puissance pour faire le lien avec les différentes antennes.
- De plus, dans un habitacle en métal, les ondes électromagnétiques sont moyenne deux fois plus élevées.
- Pas de téléphone dans la poche. En effet, les téléphones mobiles affecteraient la qualité du sperme et accentueraient les risques d'infertilité.
- Préférer les échanges par SMS
- Mettre le téléphone portable en mode avion pour la nuit et/ou l'éloigner de son oreiller.

Aménagement du poste de travail d'un ordinateur :

La posture idéale n'existe pas. En revanche, il existe une posture de moindre inconfort dont les caractéristiques sont les suivantes :

- Les pieds reposent à plat sur le sol de préférence ou sur un repose-pied permettant de maintenir les pieds à plat lorsque le plan de travail n'est pas réglable en hauteur,
- Les yeux sont au niveau du haut de l'écran
- L'angle du coude est droit ou légèrement obtus,
- Les avant-bras sont proches du corps,
- La main est dans le prolongement de l'avant-bras,
- Le dos est droit ou légèrement en arrière, et soutenu par le dossier.
- Jambes formant un angle droit

Posture de moindre inconfort pour le travail sur écran

Le poste de travail :

- Fauteuils avec accoudoirs et dossier
- La lumière perpendiculairement à l'écran
- Ecran à distance d'un bras de la tête
- Clavier à 10-15cm du bord
- Souris à droite (ou gauche) du clavier

La cyberaddiction

Qu'est-ce que c'est ?

La cyberdépendance ou Trouble de Dépendance à Internet (TDI)) désigne une dépendance qui s'instaure chez une personne faisant un usage compulsif de l'ordinateur et principalement des moyens de communication liés à Internet (addiction aux jeux vidéo, réseaux sociaux, …).

Quelles en sont les conséquences ?

- Trouble du sommeil
- Manque de concentration
- Fatigue visuelle
- Perte de la notion de temps
- Isolement

II / Cyberharcèlement

Le **harcèlement via internet** (mails, réseaux sociaux...) est appelé **cyberharcèlement**. Il s'agit d'un délit: Acte interdit par la loi et puni d'une amende et/ou d'une peine d'emprisonnement inférieure à 10 ans. Si vous êtes victime de ce type de harcèlement, vous pouvez demander le retrait des publications à leur auteur ou au responsable du support électronique. Vous pouvez aussi faire un signalement en ligne à la police ou à la gendarmerie ou porter plainte. Ce délit est sanctionné par des peines d'amendes et/ou de prison. Les sanctions sont plus graves si la victime a moins de 15 ans.

Le cyberharcèlement en meute ?

Il s'agit d'une attaque de meute sur une cible isolée : souvent rapide, toujours agressive pour blâmer dans les propos

C'est quoi, un compte « fisha » ?

Il s'agit d'un compte créé et utilisé pour publier des photos dénudées de jeunes femmes, y compris mineures, sans leur consentement (ce qui est bien sûr interdit). Il s'agit le plus souvent de photos volées. Le ou les propriétaires d'un compte fisha (ou ficha) veulent « afficher » leurs victimes, parce qu'ils jugent leur comportement (slut shaming), par vengeance (revenge porn, par exemple) ou simplement pour se divertir.

L'outing consiste à divulguer des informations intimes et /ou confidentielles sur une personne, par exemple révéler, sans qu'elle le sache ou ne le veuille, son homosexualité.

L'usurpation d'identité est l'utilisation des données (de l'identité numérique) d'une personne afin de poster de fausses informations.

III / Environnement et électricité :

Consommation des appareils électriques : Du plus énergivore au plus économe

- Ordinateur fixe de 120 à 250 kWh/an
- Ordinateur portable de 30 à 100 kWh/an
- Ecran d'ordinateur de 20 à 100 kWh/an
- Tablette tactile de 5 à 15 kWh/an

- Imprimante laser 200 à 300 W Attention aux cartouches d'encre
- Imprimantes à jet d'encre 5 à 10 W

Réduire sa facture d'électricité :

- Privilégier les modèles l'Ecolabel Européen.
- Eteignez votre ordinateur le plus souvent possible (il consomme plus qu'en mode veille.)
- Débrancher les ordinateurs fixes sinon ils continuent à consommer
- Diminuer la luminosité des écrans.
- Débrancher les portables une fois chargé.
- Une imprimante à jet d'encre est à éteindre entre deux impressions.
- Une imprimante laser est à mettre en veille.

Ce logo indique que l'équipement informatique est économe en énergie aussi bien en fonctionnement qu'en veille. On le trouve sur des ordinateurs, des écrans, des imprimantes, des scanners, des photocopieurs, des fax et des appareils qui cumulent plusieurs fonctions.

Un **économiseur d'écran** sert à augmenter la durée de vie des écrans cathodiques.
Un **économiseur d'énergie** assure une importante économie d'énergie en mode veille.

Internet, courriels : Réduire les impacts : Limiter nos consommations d'énergie et de matières premières

- Envoyer un lien hypertexte plutôt qu'une pièce jointe.
- Compresser les fichiers volumineux en pièces jointes.
- Limiter le nombre de destinataires.
- Supprimer les messages dont on n'a plus besoin de sa messagerie.
- Installer un logiciel anti-spam et/ou supprimer immédiatement les spams.

Datacenter ou centre de données

Un data center ou centre de données est un site physique regroupant des installations informatiques (serveurs, routeurs, commutateurs, disques durs...) chargées de stocker et de distribuer des données (*data* en anglais) à travers un réseau interne ou *via* un accès Internet.
Les entreprises possédant des bases de données (tous les sites Internet, les services clouds, …) hébergent leurs activités dans des Datacenters. Il peut s'agir d'installations privées à usage exclusif ou bien de centres de données administrés par des prestataires qui regroupent plusieurs clients.
Les transferts de données mettent en activité les serveurs qui consomment de l'énergie. Cette dernière produit entre **2 et 10 % des émissions mondiales de gaz à effet de serre.**
De plus, de telles installations dégagent énormément de chaleur et doivent être refroidies par des **climatiseurs** pour éviter toute panne, ce qui induit une consommation électrique très élevée et don des problèmes environnementaux.
Le recours aux énergies renouvelables et la mise en place de systèmes de récupération d'énergie font partie des solutions privilégiées pour répondre à ces enjeux. Ainsi, certains Datacenters sont entièrement alimentés par des énergies non fossiles et la chaleur qu'ils dégagent est réutilisée pour chauffer des bâtiments ou produire de l'eau chaude.

IV / Environnement et métaux rares

Quel est l'impact environnemental des ressources d'un smartphone ?

- Utilisation de plus de 50 métaux différents dont
- 15 métaux sont critiques car
    - ils sont exploités par des milices (Congo : cobalt)
    - ce sont des métaux rares