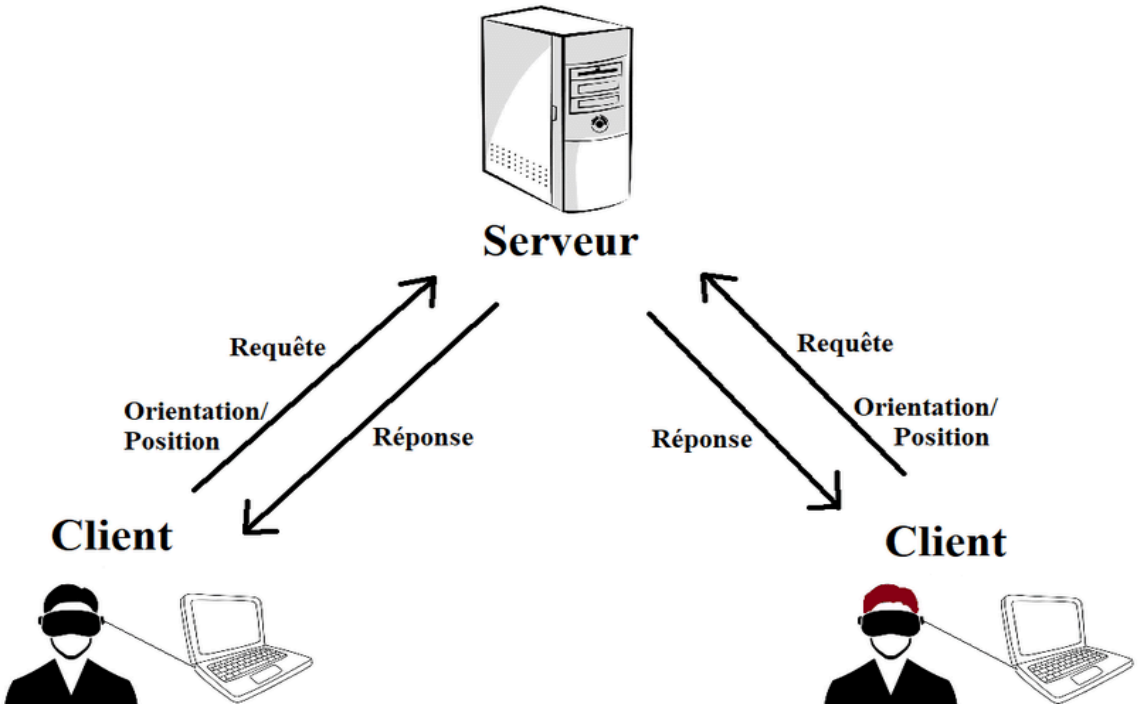
Erine
Mvouama
BTS SIO.1B

Synthèse Mission 7:
Module 3 - Sécurité sur Internet

- ## Internet:

  Réseau qui est moyen pour des machines de communiquer dans tous les domaines aujourd'hui via le téléphone, la télévision, ou les réseaux sociaux c'est le protocole TCP/IP qui permet d'établir facilement des communications entre les machines. Internet apparaît de plus en plus dans les objets du quotidien.



La navigation sur internet repose sur une architecture appelée client/serveur c'est à dire que les clients envoient leurs demandes au serveur qui envoie à son tour une réponse à ses demandes.

- **Le client** : C'est l'utilisateur final qui interagit avec les applications via son appareil (navigateur, application mobile).

- **Le serveur** : C'est l'entité qui héberge des ressources (sites web, bases de données, etc.) et répond aux requêtes des clients. Un serveur peut être dédié à l'hébergement d'un site web, d'une application, ou d'un service.

C’est un des modes les plus courants en informatique de nos jours.

● Cybermalveillance

Bien qu’Internet nous soit utile et avantageuse au quotidien, cela comporte a contrario des risques j’entend dire que des grandes attaques informatique sont de plus en plus fréquente, c’est ce que l’on pourrait appeler de la Cyber Malveillance qui a pour but d'exploiter des vulnérabilités des systèmes informatiques et des réseaux dans le but de nuire, voler, extorquer, ou perturber des individus, des entreprises ou des institutions de manière générale.

Voici quelques exemples de types d'attaques courantes en cybermalveillance:

- Rançongiciel: Pirates demandant une rançon en contrepartie d’un arrêt de l’attaque.
- Défiguration de site: Consiste à modifier une partie d’un site web affichant alors des éléments choisis par le pirate cherchant à faire passer un message à caractère politique.
- Malvertising: Le pirate intégre du contenu malveillant sur des fausses publicités en ligne pour essayer de piéger les visiteurs de sites web sans passer par le propriétaire du site en question.
- Spyware: Un programme enregistre les conversations à travers le micro de l’ordinateur de l’utilisateur.

● L’Ingénierie sociale

Les attaques par ingénierie sociale reposent souvent sur la ruse. Le pirate joue avec vos émotions (peur, confiance, envie d'aider etc…) et vos habitudes, pour vous mettre en confiance, vous inquiéter ou encore endormir votre vigilance.

Voici les techniques généralement utilisées par les pirates:

- Déjouer une authentification faible
- Utiliser l'hameçonnage
- Faire diversion
- Recourir à une situation de pression
- Donner confiance
- Utiliser la fuite d’informations

Cependant, il existe des contre-mesures possibles pour lutter efficacement contre l'ingénierie sociale en suivant quelques règles de bonnes pratiques comme demander des preuves de l'identité de vos interlocuteurs et si l'on a des doutes alerter le responsables qui aura le choix d'avoir recours à l'ANSSI ou le CNIL. 2 services et organismes étatiques pour nous accompagner en cas d'incident cybercriminel, illicite ou fraude.

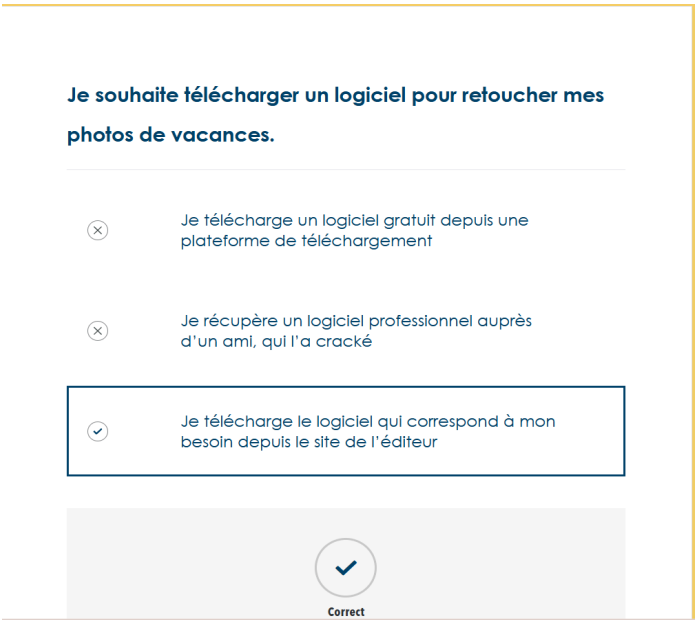
- ## Réseaux Sociaux

Bien que les réseaux sociaux soient de bons outils pour rester en contact avec ses connaissances et amis, permet d'exprimer ses idées et opinions etc.. Cela est tout de même un terrain propice à la cyber malveillance en raison de la quantité d'informations personnelles partagées et de l'interconnexion des plateformes. Les risques incluent le phishing, les escroqueries, la collecte de données personnelles et la manipulation psychologique. Il est essentiel que les utilisateurs soient conscients de ces dangers et adoptent des comportements sécuritaires pour se protéger.

- ## Fichier en provenance d'internet

De même, les fichiers que nous téléchargeons et partageons sur Internet sont à l'origine de nombreuses cyberattaques notamment le type rançongiciel. Il est possible que quelqu'un de malveillant tente d'exploiter des formats et des extensions courants pour inciter l'utilisateur à double-cliquer innocemment pour ouvrir un fichier.

Maintenir ses logiciels à jour serait une première solution pour s'assurer que toutes les vulnérabilités récentes qu'un pirate tenterait d'exploiter sont corrigées grâce aux mises à jour de sécurité. Deuxièmement, disposer d'un antivirus à jour et lancer une analyse sur les fichiers et pour finir ne pas ouvrir des fichiers qui proviennent de sources non fiables (expéditeur inconnu, courriel suspect, site Web peu fiable, etc.).



- Les sites des éditeurs sont les seules sources fiables. Un logiciel récupéré sur une plateforme de téléchargement pourrait être une version remodelée contenant un code malveillant.
Et au-delà de son caractère illégal, l'installation d'un logiciel cracké récupéré auprès d'un ami ou depuis un site de téléchargement illégal, vous expose à des cyberattaques.

- ## Navigation web

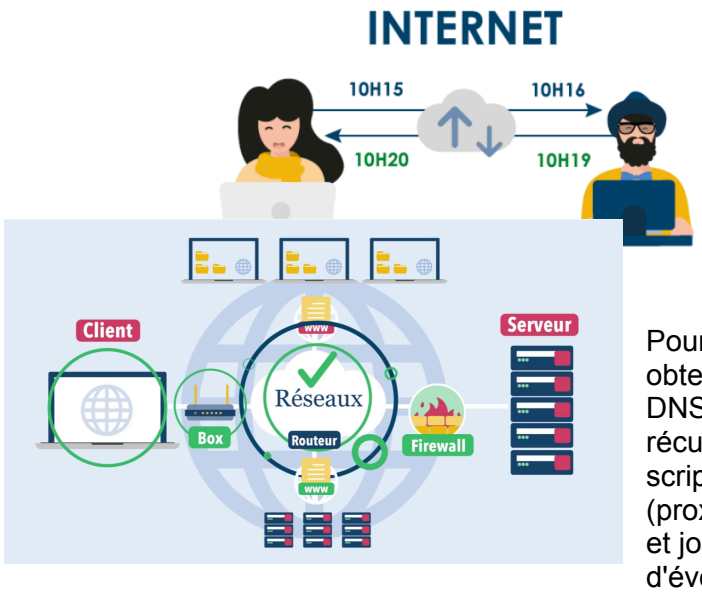
Un navigateur web est un logiciel qui sert d'interface entre l'utilisateur et le contenu d'Internet en interprétant le code HTML, CSS et JavaScript des sites web pour afficher des pages de manière visuelle et interactive. Il fonctionne en se connectant à un serveur web via le protocole HTTP ou HTTPS, en envoyant des requêtes pour récupérer des ressources (textes, images, vidéos, etc.) que le serveur héberge. Les principaux navigateurs web actuels incluent Google Chrome, Mozilla Firefox, Microsoft Edge, et Safari.

Le navigateur web peut être victime d’attaques comme le typosquatting, où des sites aux noms similaires aux sites légitimes piègent les utilisateurs pour voler leurs informations ou installer des malwares ; pour se protéger, il est important de vérifier l’URL et de sauvegarder les sites fréquents dans ses favoris. Les cookies, quant à eux, sont des fichiers stockés par les sites web pour mémoriser les informations des utilisateurs, mais lorsqu’ils sont partagés avec des régies publicitaires, ils permettent de suivre les activités en ligne et de proposer des publicités ciblées en fonction des recherches récentes.

- ## Courrier électronique

L'échange de courriels, bien que courant, comporte des risques tels que phishing, virus et usurpation d'identité, nécessitant une vigilance constante. Un courriel est un message électronique envoyé via le protocole SMTP, mais l'adresse de l'expéditeur peut être falsifiée, ce qui impose de se méfier des demandes d'informations sensibles. Pour sécuriser sa messagerie, il est recommandé d'utiliser un mot de passe robuste, de limiter la diffusion de son adresse et de créer des adresses dédiées pour les usages personnels, professionnels et commerciaux.

La messagerie instantanée, rapide mais parfois peu sécurisée, expose les utilisateurs à des risques d'interception. Pour garantir la confidentialité, privilégiez des services offrant un chiffrement de bout en bout et consultez leur charte de confidentialité pour connaître le niveau de protection des données.



- **L'envers du décor d'une connexion web**

Pour accéder à une page web, le navigateur doit d'abord obtenir l'adresse IP du serveur web via la résolution DNS. Ensuite, il envoie une requête HTTP pour récupérer la page et ses ressources (images, styles, scripts) nécessaires à l'affichage. Un serveur mandataire (proxy) peut améliorer la rapidité et la sécurité en filtrant et journalisant les requêtes, utile pour détecter d'éventuelles menaces. Enfin, le HTTPS garantit une connexion sécurisée entre l'utilisateur et le serveur, symbolisée par le cadenas dans la barre d'adresse.