# Qu’est-ce que la cybersécurité

Cette un ensemble de pratiques, de processus, conçus pour protéger le système d’informations (les ordinateurs, les réseaux, les données,), contre les attaques, dommages et accès non autorisés.

## Les différentes formes de cybersécurité

* **La sécurité des applications**, qui se focalise sur les applications et logiciels.
* **La sécurité des réseaux,** qui se focalise sur les ordinateurs et infrastructure réseau.
* **La sécurité de l’information**, qui se concentre sur l’intégrité et la confidentialité des données.
* **La sécurité opérationnelle**, processus globaux de la sécurité.

## Pourquoi la cybersécurité

Le nombre de **cyberattaques** augmente chaque jour, la cybersécurité et donc là, pour assurer la confidentialité, l’intégrité et la disponibilités des informations stockées dans le SI.

**Concepts de la cybersécurité :**

Pour mieux ce protégé, il est important de savoir quel sont **les diffèrent types de cyberattaques qui existe**.

* **Les malwares**, et la combinaison des mots **MALICIOUS SOFTWARE** (Logiciels malveillants).  
    
  Sont objectif principal est de **nuire**, il a pour cible tout **types de systèmes informatiques**.

Une image contenant logo

Description générée automatiquementIl existe diffèrent types de malware.  
  
**Virus :** C’est un programme qui est créé pour **s’auto-reproduire en infectant des programmes**, et ainsi de se propager d’appareils en appareils.

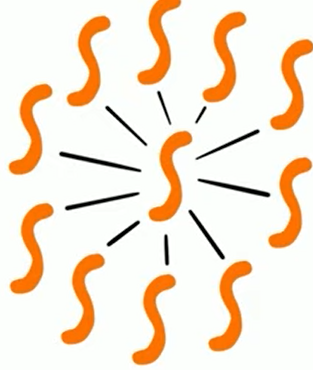
  
Une fois infecté le virus va chercher à **endommager, altérées ou supprimer** des fichiers ou des données de vos appareils.

Une image contenant texte, reine, signe, graphique vectoriel

Description générée automatiquement

**VER :** Les vers sont une catégorie de virus, car eux aussi il se duplique, en revanche il n’infecte pas vos fichiers et vos données.

  
  
Leurs Objectifs, est en premier de se **reproduire via l’exploitation de vulnérabilité**, ensuite **ils se réplique eux même**, que ça soit sur un disque dur, des partages réseaux.

  
  
Cela va **surcharger** l’espace des disque durs, et consomme beaucoup de ressources du processeur.

**Trojan** (**Cheval de Troie) :** Programme malveillant, qui se font passer pour des **programmes légitimes**, ils vont embarquer **à l’insu** de l’utilisateur des programmes malveillants, ainsi quand l’utilisateur exécute le programme légitime, **le sous-programme malveillant et lancer**.  
  
Il peut héberger **une porte dérobée**, ce qui permet au cybercriminel de prendre **à distance la machines**.  
  
Il pourra par la suite par exemple, **installer des spyware (logiciel espion)**.

**SPYWARE (Logiciel Espion) :** Ces logiciel vont collectées des informations à votre insu, que ça soit des mots de passes, des informations de paiements, etc.  
  
On a le **keyloger**, qui permet **d’enregistrer toutes les touches frapper** sur votre clavier, toutes ses données sont enregistrées ensuite **envoyer au cybercriminel.**

Une image contenant diagramme

Description générée automatiquement

**RAMSOMWARE (Rançongiciel) :** Malware qui **chiffre les données** de l’équipement infecté, et il va demander **une forte rançon pour déchiffrer** vos données.

**Les méthodes de propagations :**

Documents piégés : La plupart du temps un malware a besoin de **l’action de l’utilisateur, pour s’infiltré sur l’appareil**, bien évidement les cybercriminels vont ruser pour que les utilisateurs téléchargent ce malware (mails).  
  
Bien souvent cela est à **travers un mail** **que le malware est transmis**, sous forme de pièce jointe, le malware peux être **contenu dans un document, qui peux être contenue sous la forme.exe,zip,. word, .excel, .pdf**.  
  
Cela peut être **un sms, via support amovible**.

Sites WEB piégé : Les malwares peuvent aussi affecter vos appareils, **pendant votre navigation WEB**.   
  
Paracerque vous suivez un **lien piégé dans un mail**, ou parce que vous avez trainer sur des **sites non fiables**.

Par exemple votre page WEB peut héberger un **fichier affecté par un malware**, est un **script exploitant la vulnérabilité** de votre navigateur Internet.   
Quand un utilisateurs Viste la page WEB affecté, le script **télécharge le fichier affecté** sur l’ordinateur de l’utilisateur, **via la vulnérabilité et le lance.**

Une image contenant diagramme

Description générée automatiquement

**Symptômes d’infections :**

Comportement anormal de l’appareil, ouverture de fenêtre non désiré, notamment des pops publicitaires, des demandes de mot de passe sans raison, messages d’alerte régulier sur votre ordinateur.

Ralentissement sur vos appareils, les malwares peuvent **utiliser beaucoup de ressources** en arrière-plan, et par conséquent on va avoir **un processeur qui chauf continuellement** et le ventilateur qui tourne à fond, redémarre sans arrêt, document supprimer, mot de passe changer.

**Bonnes pratiques :**

Être vigilant :

* Ne fait pas confiance aux mails d’inconnu
* Messages
* Demande étrange

Mettre à jour vos équipent et applications.

Sauvegarde régulière de vos données, permet de remplacer les données chiffrer ou supprimer par des malwares.

Utiliser des logiciels de sécurité

* **La sécurité des réseaux,** qui se focalise sur les ordinateurs et infrastructure réseau.
* **La sécurité de l’information**, qui se concentre sur l’intégrité et la confidentialité des données.
* **La sécurité opérationnelle**, processus globaux de la sécurité.

Avec la croissance rapide des technologies de l'information et de la communication, les cyberattaques sont devenues de plus en plus sophistiquées et de plus en plus fréquentes.   
  
Les entreprises doivent donc faire face à un environnement de menace en constante évolution qui met leurs actifs numériques et leur réputation en danger. Les cyberattaques peuvent prendre de nombreuses formes, notamment les attaques par phishing, les attaques par ransomware, les attaques par déni de service (DoS) et les attaques par virus.

Les enjeux sont élevés, car une cyberattaque peut causer des pertes financières importantes, ainsi que des dommages à la réputation et à la confiance des clients. Par conséquent, il est crucial pour les entreprises de mettre en place des mesures de cybersécurité efficaces pour protéger leurs actifs numériques et garantir la continuité de leurs opérations.