Contexte :

Réaliser une carte mental des Logiciel Malveillant

- Virus, Trojan, Phishing ...
- Spyware, Adware, RansomWare ...
- Spam, redirecteur de pages web ...
- KeyLogger
- Vol d'identité

Définir chaque type de logiciel malveillant et donner un exemple et expliquer comment s'en protéger.

-

Type de logiciel malveillant	Description	Exemple
Virus	Un virus est un agent infectieux nécessitant un hôte, souvent une cellule, dont il utilise le métabolisme et ses constituants pour se répliquer. On le considère de plus en plus comme faisant partie des acaryotes[1].	Cabir - Virus Cabir, développé en 2004, est le tout premier virus informatique *proof of concept* recensé se propageant par la téléphonie mobile grâce à la technologie Bluetooth et du système d'exploitation Symbian OS.
Trojan	Un cheval de Troie (*Trojan Horse* en anglais) est un type de logiciel malveillant, souvent confondu avec les virus ou autres parasites. Le cheval de Troie est un logiciel en apparence légitime, mais qui contient une fonctionnalité malveillante. Le rôle du cheval de Troie est de faire entrer ce parasite sur l'ordinateur et de l'y installer à l'insu de l'utilisateur 1.	Zeus - Trojan Zeus est un cheval de Troie destiné à voler des informations bancaires par récupération de formulaire, *keylogger* et attaques en *man-in-the-browser*.
Phishing	L'hameçonnage, *phishing* ou filoutage est une technique utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité.	Le *spear phishing*, qui vise une personne précise, par exemple sur des réseaux sociaux Exemple phishing page facebook
Spyware	Un logiciel espion (aussi appelé mouchard ou espiogiciel ; en anglais *spyware*) est un logiciel malveillant qui s'installe dans un ordinateur ou autre appareil mobile, dans le but de collecter et transférer des informations sur l'environnement dans lequel il s'est installé, très souvent sans que l'utilisateur en ait connaissance.	Cydoor est un spyware, utilisé par l'unité commerciale de l'entreprise du même nom. Il a pour but de recueillir des données sensibles sur les utilisateurs qui utilisent les logiciels infectés.

Ransomware	Un *ransomware*, rançongiciel ou logiciel de rançon est un logiciel malveillant qui prend en otage des données personnelles. Pour ce faire, un rançongiciel chiffre des données personnelles puis demande à leur propriétaire d'envoyer de l'argent en échange de la clé qui permettra de les déchiffrer.	« Reveton », ou encore « *the Police Trojan* ». Ce dernier se propageait par des publicités malicieuses (*malvertising*) qui visent à charger un Web Exploit sur l'ordinateur, sa charge active affiche un faux avertissement d'une autorité gouvernementale, signalant que l'ordinateur infecté serait utilisé à des fins illégales, comme du téléchargement de logiciels crackés[27].
Keylogger	En informatique, un enregistreur de frappe (en anglais, *keylogger*) est un logiciel espion ou un périphérique qui espionne électroniquement l'utilisateur d'un ordinateur. Le but de cet outil est varié, et peut se présenter sous des airs de légitimité[1], mais il ne peut être assuré qu'en espionnant l'intimité informatique de l'utilisateur.	