Risques :		Conséquences :
1.Virus	Un virus se compose d'instructions programmées qui prescrivent à l'ordinateur les actions à exécuter. Afin de se propager, le virus s'installe dans un "programme hôte" qui peut être une application (p. ex. un logiciel téléchargé) ou un document (p. ex. un fichier Word ou Excel). En exécutant l'application ou en ouvrant le document, le virus est activé et exécute des actions . Les virus sont souvent transmis par des documents attachés aux courriels ou via des fichiers infectés téléchargés à partir d'Internet. Une fois activés, ils peuvent aussi se propager par courriel aux contacts répertoriés dans le carnet d'adresse. D'autres moyens de propagation sont des supports de données externes, p. ex. des CD-ROM, des clés mémoire USB (USB memory sticks), etc. ex :"Blaster" et "Slammer" ont causé la panne de millions d'ordinateurs à travers le monde.	• Modification et effacement de données • Changement affectant les contenus affichés à l'écran et apparition de messages inattendus.
2.Vers	Même fonctionnement que pour les virus mais n'ont pas besoin d'un programme hôte pour se propager d'eux mêmes dans des réseaux	• Mêmes effets que les virus .
3.Chevaux de Troie	Programmes qui exécutent des actions préjudiciables tout en se présentant à l'utilisateur comme des applications ou des fichiers utiles. Il s'agit souvent de programmes téléchargés depuis l'Internet. Mais des chevaux de Troie peuvent aussi prendre la forme de morceaux de musique ou de films (p. ex. dans les formats MP3 ou MPEG). Ils utilisent les lacunes de sécurité dans différents programmes de lecture (p. ex. Media Player), afin de s'installer dans le système.Ils se répandent également via les fichiers attachés aux courriels.	• Accès illicites aux données confidentielles (p. ex. mots de passe pour les services en ligne, codes d'accès pour le ***e-banking**** en enregistrant les touches activées et transmettant ces données aux hackers. • Accès non autorisé à l'ordinateur (p. ex. en installant ou en utilisant une **porte dérobée***) • Envoi de pourriels c'est à dire des spam qui sont des publicités envoyé par mail sans demander a l'utilisateur depuis votre ordinateur . **banque electronique qui permet d'avoir accés a tout les compte*) ** La personne connaissant la **porte***

		dérobée *peut l'utiliser pour surveiller les activités du logiciel, voir en prendre le contrôle.*
3.Phishing	Le phishing est une technique dans laquelle des bandes organisées de cybercriminels se font passer pour des organismes financiers ou grandes sociétés en envoyant des emails frauduleux.	• Récupération des mots de passe de comptes bancaires ou numéros de cartes de crédit pour détourner des fonds.
4.Cookies	Les cookies (témoins de connexion) sont des petits fichiers texte qui s'installent sur l'ordinateur du visiteur lorsque ce dernier consulte une page Internet, ceci dans le but de lui simplifier la tâche. A titre d'exemple, il faut parfois dans certains services en ligne s'annoncer à l'aide d'un nom d'utilisateur et du mot de passe correspondant. Afin d'éviter de devoir répéter l'opération à chaque fois, ces informations sont stockées après sélection de l'option correspondante sur un témoin de connexion sur le disque dur local et réutilisées automatiquement à chaque visite du site. Les boutiques en ligne les utilisent également afin de procéder à l'enregistrement intermédiaire de la corbeille d'achat ou pour présenter des produits qui sont venus s'y ajouter depuis la dernière visite.	• Mise en danger de la sphère privée. Les exploitants de sites Internet peuvent à l'aide des cookies enregistrer le comportement de la personne qui visite le site pour établir son profil client.
5. Hoax / Canulard	Les courriels vous annonçant de nouveaux virus sont presque toujours de fausses annonces. Les canulars sont toujours conçus sur le même modèle. Ils signalent l'apparition d'un nouveau virus dangereux résistant même à un logiciel anti-virus récent. De plus, la source indiquée par l'annonce est une entreprise informatique renommée et il est demandé de transmettre l'annonce à autant de monde que possible. Outre de fausses informations concernant les virus, on trouve également des annonces très diverses nous faisant compatir au triste destin de personnes malades ou proposant des offres discutables. On parle également dans ce cas de chaînes de courriels.	• Suivre les mesures proposées dans le canular peut entraîner la perte de données ou la mise hors usage de l'ordinateur.

6.Logiciel d'espion «mouchard»:	Logiciel malveillants qui s'installe dans un ordinateur 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. L'essor de ce type de logiciel est associé à celui d'Internet qui lui sert de moyen de transmission de données .	• Espionnage de données confidentielles (p. ex. des mots de passe) • Mise en danger des données privées • Publicité non sollicitée
7.Wireless LAN (Local Area Network)	C'est un réseau local sans fil. Dans un tel réseau, les terminaux (p. ex. ordinateurs portables, agendas électroniques ..) communiquent sans fil avec un point d'accès WLAN (WLAN Access Point), relié à Internet ou à un réseau local. L'avantage du WLAN est que ses utilisateurs sont davantage mobiles étant donné que leurs terminaux ne sont pas câblés.	• Entraîne un accès total au réseau local. Il devient alors possible d'accéder aux ordinateurs et aux données ainsi que de pirater les raccordements à Internet.
8.Chat et messagerie instantanée	Le "chat" (bavardage en ligne) désigne un moyen de communiquer sur Internet en temps réel avec d'autres utilisateurs. Un mode de communication analogue est offert par les services de messagerie instantanée (p. ex. AOL, MSN, ICQ et Yahoo), auprès desquels des millions d'internautes sont enregistrés.	• Les services de bavardage en ligne sont utilisés en raison de leur apparent anonymat également pour agir de manière illégale (p. ex. par des pédophiles à la recherche de victimes) . • Introduction de virus, vers et chevaux de Troie sur votre propre ordinateur. • Les participants au bavardage en ligne sont régulièrement tentés à cliquer sur des liens ou à entrer des commandes inconnues.
9.L'addiction	Dépendance d'une personne à une activité qui donne du plaisir ici Internet . C'est l'usage intensif qui est devenu un besoin chez la personne. Elle ne peut plus s'en passez en dépit de sa propre volonté .	• L'isolement • L'exclusion • Vivre dans le mensonge • Plus d'activité le soir donc il y a des décalages au niveau du sommeil, de l'alimentation.