# Qu’est que la Cyber Criminalité ?

AGIS
Allsure Global Insurance Solutions

Votre partenaire Courtage depuis 40 ans

www.agis-group.com

À mesure que l'utilisation de l'Internet augmente chaque jour, le monde rétrécit. Le World Wide Web ressemble à un phénomène vaste, mais étonnamment, l'une de ses spécificités est de nous rapprocher, ce qui en fait un lieu plus étroit à vivre pour les internautes. Le World Wide Web a également produit un phénomène de plus en plus présent, c'est la criminalité informatique et les personnes qui passent de longues heures à parcourir le Cyber World y sont de plus en plus exposées.

Bien que beaucoup d'Etats aient créé des organismes judiciaires de contrôle d'application de la loi, le risque d'exposition à la Cyber criminalité augmente sans cesse de façon constante et de nombreuses personnes sont à chaque instant victimes de piratage, de vol d'argent, de vol d'identité et de logiciels malveillants. L'une des meilleures façons d'éviter d'être victime de crimes cybernétiques et de protéger vos informations sensibles au moyen au moyen d'un système unifié de logiciels et de matériels authentifiant en temps réel toute information envoyée ou accessible via Internet.

Avant de choisir la protection qui convient, il est indispensable de prendre connaissance de tous les types de « cyber crimes » qui peuvent vous concerner.

**Tout crime commis sur Internet, est qualifié de cybercrime. Il existe de nombreux types de cybercrimes et les plus courants sont développés ci-dessous :**

## A - LA CYBERCRIMINALITE DE MASSE

1. **Hacking :** C'est un type de crime dans lequel l'ordinateur d'une personne est cassé afin que ses informations personnelles ou sensibles puissent être consultées. Aux États-Unis, le piratage est classé comme un crime et punissable en tant que tel. Ceci est différent du piratage éthique, que de nombreuses organisations utilisent pour vérifier leur protection de sécurité sur Internet. Dans le piratage, le criminel utilise une variété de logiciels pour entrer dans l'ordinateur d'une personne et la personne peut ne pas savoir que son ordinateur est accessible depuis un endroit éloigné.

2. **Vol :** Ce crime survient lorsqu'une personne enfreint les droits d'auteur et télécharge la musique, les films, les jeux et les logiciels. Il existe même des sites de partage partagés qui encouragent le piratage de logiciels et que beaucoup de ces sites Web sont actuellement visés par le FBI. Aujourd'hui, le système de justice s'attaque à ce cybercrime et il y a des lois qui empêchent les personnes de télécharger illégalement.

3. **Cyber Stalking :** Il s'agit d'une sorte de harcèlement en ligne dans lequel la victime est soumise à un vague de messages en ligne et de courriels. En règle générale, ces harceleurs connaissent leurs victimes et, au lieu de recourir à un harcèlement hors ligne, ils utilisent Internet pour réussir. Toutefois, s'ils remarquent que le « cyber harcèlement » ne provoque pas l'effet souhaité, ils commencent à traquer leurs victimes hors ligne et rajoutent en plus le « cyber harcèlement » ce qui rend la vie de leurs victimes difficile.

4. **Le vol d'identité :** Cela est devenu un problème majeur chez les personnes qui utilisent Internet pour les transactions en espèces et les services bancaires. Dans ce crime cybernétique, un criminel accède aux données sur le compte bancaire, les cartes de crédit, la sécurité sociale, la carte de débit et autres informations sensibles d'une personne pour siphonner ses comptes ou pour acheter en ligne au nom de la victime. Cela peut entraîner des pertes financières majeures pour la victime et même ruiner le crédit de la victime.

5. **Logiciel malveillant :** Ce sont des logiciels ou des programmes Internet utilisés pour perturber un réseau. Le logiciel permet d'accéder à un système pour voler des informations ou des données sensibles ou causer des dommages aux logiciels présents dans le système.

6. **Sollicitation et abus sur enfants :** C'est un type de cybercriminalité dans lequel les criminels sollicitent des mineurs dans des salles de discussion sur le thème de la pornographie juvénile. Les services spéciaux de toutes les grandes démocraties passent beaucoup de temps à surveiller les salles de discussion fréquentées par des enfants dans l'espoir de réduire et de prévenir les sévices et la sollicitation d'enfants.

## B - LA CYBERCRIMINALITE ET LES ENTREPRISES

*Chaque entreprise est désormais vulnérable sur internet, quelle que soit son ampleur ou son activité, de plus chaque entreprise peut s'avérer une cible intéressante, non pas en elle-même, mais parce qu'elle fait des affaires avec une autre entreprise*

1. **Les Botnets :** Partout dans le monde, des ordinateurs sont contaminés à l'insu de leurs utilisateurs. Bon nombre d'entre eux forment un botnet, c'est-à-dire un réseau pouvant être piloté à partir d'un point de commande central pour envoyer des spams, propager des virus, faire transiter des données en douce ou lancer des attaques sur des systèmes informatiques. Les ordinateurs d'un botnet nuisent également à l'entreprise contaminée car ils utilisent de la bande passante et peuvent ralentir un réseau. Vous pouvez en outre être considéré comme juridiquement responsable si vos ordinateurs sont impliqués dans un crime.

2. **Les attaques DDoS :** Les botnets sont souvent utilisés pour mener des attaques DDoS (Distributed Denial-of Service attacks, attaques distribuées par déni de service). Lors de DDoS, les ordinateurs du botnet se connectent en même temps à un serveur (web). Vu le nombre considérable de connexions simultanées, ce serveur plante ou devient inaccessible. De telles attaques peuvent paralyser des systèmes d'entreprises et d'institutions publiques.

3. **Le Phishing :** Le phishing est une forme de social engineering où des gens sont attirés vers un faux site (bancaire), souvent par e-mail. Les utilisateurs dupés sont alors invités à introduire leurs données de connexion, un numéro de carte de crédit ou d'autres données sensibles.

4. **Les Chevaux de Troie :** Un cheval de Troie ressemble à un programme ou fichier ordinaire, mais contient des fonctions cachées permettant l'accès à l'ordinateur infecté depuis l'extérieur. Souvent envoyés en pièce jointe à un e-mail, les chevaux de Troie sont utilisés pour collecter des adresses e-mail ou accéder à un compte bancaire. Il ne faut pas confondre un cheval de Troie avec un virus, qui endommage un ordinateur, ou un ver, qui se propage d'ordinateur en ordinateur.

## C - LES CAUSES DU CYBERCRIME

Lorsque le taux de rendement des investissements est élevé et le risque est faible, vous trouvez automatiquement des personnes désireuses de profiter de la situation. C'est exactement ce qui se passe dans le « cybercrime ». L'accès à des informations et à des données sensibles est facilité à un nombre important de spécialistes et l'utilisation des données ou leur revente génère une manne financière très importante.

La capture de ces criminels étant difficile, cela a entraîné une augmentation de la cybercriminalité à travers le monde.

## D - L'HISTOIRE DU CYBERCRIME

Lorsque les ordinateurs et les réseaux ont vu le jour dans les années 1990, le piratage a été effectué essentiellement pour obtenir plus d'informations sur les systèmes. Les pirates sont même entrés en compétition les uns contre les autres pour gagner le titre de meilleur hacker. De nombreux réseaux informatiques ont été touchés de l'armée aux organisations commerciales. Ces tentatives de piratage ne constituaient pas une menace à long terme. Cependant, les logiciels malveillants devenant omniprésents pendant la même période, le piratage a commencé à rendre les réseaux et les systèmes plus lents. Au fur et à mesure que les pirates devenaient plus habiles, ils ont commencé à utiliser leurs connaissances et leur expertise pour en tirer un profit financier basé sur l'exploitation des informations sensibles. De très nombreuses personnes ou organisation sont aujourd'hui victimes des pratiques de ces hackers.

## E - LA CYBER CRIMINALITE AUJOURD'HUI.

Aujourd'hui, les criminels qui se livrent aux crimes cybernétiques ne sont pas motivés par l'ego ou la démonstration de leur savoir-faire. Ils veulent utiliser leurs connaissances pour en retirer des profits immédiats. Ils utilisent leur expertise pour voler, tromper et exploiter les gens car ils trouvent qu'il est plus facile de gagner de l'argent sans avoir à faire une honnête journée de travail.

Les crimes cybernétiques sont devenus une menace réelle aujourd'hui et sont tout à fait différents des crimes des anciens, comme le vol, l'agression ou le vol.

Contrairement à ces crimes, les crimes cybernétiques peuvent être commis de manière ponctuelle, ils ne nécessitent pas la présence

physique des criminels. Les crimes peuvent être commis à partir d'un endroit éloigné et les criminels ne doivent pas s'inquiéter des organismes d'application de la loi dans le pays où ils commettent des crimes. Les mêmes systèmes qui ont facilité le développement du commerce électronique et des transactions en ligne sont désormais exploités par des cybercriminels.

**Les catégories de crimes relevant de la cybercriminalité sont généralement classées en trois catégories, à savoir**

**Visant les particuliers :** Ce type de cybercriminalité peut prendre des formes diverses « cyber harcèlement », distribution de pornographie, trafic et de «toilettage». Aujourd'hui, les organismes judiciaire de contrôle du web prennent très au sérieux cette catégorie de cybercriminalité et s'unissent à l'international pour atteindre et arrêter les auteurs.

**Visant la propriété des particuliers ou des entreprises :** Tout comme dans le monde réel où un criminel peut voler dans le monde cybernétique, il en est de même. Les criminels peuvent voler les données bancaires d'une personne et siphonner son argent; Abuser de sa carte de crédit pour faire de nombreux achats en ligne; Exécuter une arnaque pour amener les gens naïfs à se séparer de leur argent durement gagné; Utiliser un logiciel malveillant pour accéder au site Web d'une organisation ou perturber les systèmes de l'organisation. Le logiciel malveillant peut également endommager les logiciels et le matériel, tout comme les dommages causés par les vandales dans le monde hors ligne.

**Gouvernement :** Bien que pas moins fréquents que ceux des deux autres catégories, les crimes contre un gouvernement relèvent du cyber-terrorisme.

En cas de succès, cette catégorie peut causer des ravages et provoquer une panique parmi la population civile. Dans cette catégorie, les criminels piratent des sites Web gouvernementaux, des sites Web militaires ou diffusent une propagande.

Les auteurs peuvent être des groupes terroristes ou des gouvernements hostiles à d'autres nations.

## F - COMMENT LUTTER CONTRE LA CYBERCRIMINALITE?

On a vu que la plupart des cybercriminels ont des réseaux « souterrains » où ils collaborent et coopèrent les uns avec les autres. Contrairement au monde réel, ces criminels ne se battent pas pour la suprématie ou le contrôle. Ils travaillent ensemble pour améliorer leurs compétences et même s'entendent pour trouver de nouvelles opportunités.

Par conséquent, les méthodes habituelles de lutte contre la criminalité ne peuvent pas être utilisées contre ces cybercriminels. Alors que les organismes judiciaires de contrôle de la loi tentent de suivre le rythme des cybercriminels, mais n'y parviennent pas. C'est principalement parce que les méthodes utilisées par les cybercriminels et la technologie changent trop rapidement. C'est pourquoi les institutions commerciales et les organisations gouvernementales doivent se pencher sur d'autres méthodes de protection.

Les solutions de type Cross-Domain Solutions sont indispensables.

Lorsque les organisations utilisent des solutions de sécurité cybernétique, elles peuvent garantir que l'échange d'informations respecte les protocoles de sécurité.

La solution permet aux organisations d'utiliser un système unifié composé de logiciels et de matériel qui authentifie le transfert manuel et automatique et l'accès à l'information lorsqu'elle prend place entre différents niveaux de classification de sécurité.

Cela permet un partage sans interruption et l'accès à l'information dans un process de classification de sécurité spécifique, l'information ne peut pas alors être intercepté ou divulgué à l'utilisateur qui ne fait pas partie de la classification de sécurité. Cela permet de protéger les réseaux et les systèmes toute sécurité.

Les solutions « Cross Centre Domain » offrent un moyen de garder toutes les informations confidentielles en utilisant des domaines sûrs et sécurisés qui sont rendus inaccessibles.

Cette solution de sécurité peut être utilisée par une organisation commerciale et/ou gouvernementale pour rendre un réseau impénétrable tout en veillant à ce que les utilisateurs puissent facilement accéder à l'information requise.