Table des matières

[Introduction 2](#_Toc118314251)

[I. Définition de la cybercriminalité 2](#_Toc118314252)

[II. Historique de la cybercriminalité 4](#_Toc118314253)

[1. Comment la cybercriminalité est apparue : 4](#_Toc118314254)

[2. Grandes étapes historique de la cybercriminalité 4](#_Toc118314255)

[III. Les différents types de cybercriminalité 6](#_Toc118314256)

[IV. Causes de la cybercriminalité 9](#_Toc118314257)

[1. Les causes de la criminalité au niveau individuel 9](#_Toc118314258)

[2. Les causes de la criminalité au niveau communautaire 9](#_Toc118314259)

[3. Les causes de la cybercriminalité au niveau mondial 10](#_Toc118314260)

[4. Conséquence sur la société 11](#_Toc118314261)

[5. Conséquences sur l’économie. 12](#_Toc118314262)

[6. Les différentes sanctions prévues par la loi 13](#_Toc118314263)

[V. Mise en pratique (voir la présentation pour plus de détail) 14](#_Toc118314264)

[VI. Moyens de protection contre la cyber criminalité 15](#_Toc118314265)

[Conclusion générale 17](#_Toc118314266)

# Introduction

L’essor croissant de la technologie d’information et de communication donne lieu au développement des activités de médias, des banques et des services gouvernementaux numérisées, De plus dans notre quotidien a créé de profondes transformations dans la société. La numérisation des communications et des activités humains s’est manifestée par des nombreux avantages ; accès directs à l’information, disparition des frontières géographiques multiplication des capacités des stockage…

Cette forte puissance technologique constitue également au développement de nouvelles formes infractionnelles, soit la cybercriminalité. Associer au développement de l’ordinateur, le délit informatiques a vu le jour à la fin des années cinquante. La délinquance informatique est un phénomène récent liée au développement technologique et à l’utilisation de l’ordinateur. L’avènement de réseaux informatique transnationaux a mené à la naissance des pirates informatiques. Ce développement de technologie de télécommunication a substitué la délinquance informatique à la délinquance informationnelle, ou la criminalité informatique à la cybercriminalité. Cela a permis au délinquant de sortir du champ d’incrimination des infractions liées au cyberespace, notamment liées au réseau informatique soit le réseau internet.

# Définition de la cybercriminalité

Pour mieux comprendre et appréhender le concept de la cybercriminalité, il faut tout d’abord connaitre la définition étymologique de ces deux mots à savoir le cyber et le crime ou criminalité.

* Le terme cyber

Le mot cyber n’a fait son apparition que dans les années 1950, et provient de mot cybernétique qui signifie étymologiquement « science de gouverner », inventé par André-Marie dans l’étude des moyens des gouvernements en 1834. Ainsi repris par Norbert Wiener dans son texte en 1948. Alors cyber désigne un préfixe tiré de cybernétique et son usage en général consécutif à l’avènement de l’internet ou en sens large cyberespace.

* Le terme crime (criminalité)

Etymologiquement le mot crime est dérivé du mot latin « crime (-Inis) » qui signifie à l’origine « décision judiciaire ». Ce latin vient à son tour du grec « Krimein », c’est-à-dire « juger », « choisir », « séparer ». Dans le latin classique, le mot « crimen » a pris le sens « accusation ».

Selon juriste Italien Francesco Carra qui a dit « le crime comme une action, mais comme une infraction », car il n’est pas « un fait matériel, mais plutôt un être juridique »

Après avoir définir les termes qui constitue la cybercriminalité, elle peut être définit comme ensemble des infractions graves liées à cyberespace ou des infractions qui sont commis en utilisant les ordinateurs.

La cybercriminalité n’a pas une définition standard c’est-à-dire conventionnelle ce qui fait l’objet d’une confusion entre les différents états. En effet chaque état définisse la cybercriminalité selon sa législation.

En Europe, pas de texte universel législative qui se définit la cybercriminalité mais il y’a des tentatives :

-Selon le ministère de l’intérieur français, la cybercriminalité recouvre « l’ensemble des infractions pénales susceptibles de se commettre sur les réseaux de communications en général et de plus particulièrement sur l’internet »

-Selon l’office de la fédération de la police suisse la cybercriminalité signifie « des nouvelles formes des criminalités spécifiquement liées aux technologies modernes de l’information et des délits connus qui sont commis à l’aide de l’informatique plutôt qu’avec les moyens des communications »

Aux Etats-Unis aussi, il y a absence d’une définition commune.

# Historique de la cybercriminalité

## Comment la cybercriminalité est apparue :

La cybercriminalité est un phénomène qui est apparu avant même l’existence de l’internet, c’est-à-dire les premiers actes de la cybercriminalité étaient liés au vol des données à travers ce qu’on appelle « la cassation de code » ou en Anglais « code Breaking » et ces actes ou plutôt ces attaques premières étaient connues sous le nom de phreaking et hacking.

La première attaques cybercriminels est née en 1960-1970 par John Draper qui était l’inventeur de technique de système de « Blue box » qu’il permet de communiquer gratuitement par téléphone via le sifflet d’un son sur la même fréquence que le signal téléphonique.

## Grandes étapes historique de la cybercriminalité

* En 1960-1970 : origine de la cybercriminalité

John Draper alias « Cap’n Crunch » découvre que le siThet gadget présent dans les boites de céréales de la marque Cap’n Crunch émet un son, lorsque l’on s’en sert exactement à la même fréquence que le réseau téléphonique l’opérateur AT&T.

Grace à Draper et au siThet, des milliers des personnes peuvent utiliser AT&T pour passer des appels nationaux ou internationaux.

* En 1981 :

Lan Murphy alias « captain zéro » est officiellement la première personne inculpée pour un crime informatique suite à son intrusion dans le système informatique d’AT&T, et à la modification du programme de facturation, étendant les heures creuses à toute la journée.

Les « exploits » de Murphy inspire le film SNEAKERS avec Robert Redford, Dan Aykroyd, River Phenix, où une bande des hackers repentis ayant créé une société testant la sécurité des systèmes informatiques se trouve confrontés à des agents corrompus du FBI.

* En 1983

Le film War Games popularise les hackers et le phénome du cybercrime.

* En 1985

Le premier numéro du journal Phrack voit le jour. C’est le premier magazine « underground » concernant le piratage et les hackers.

* En 1986

Le premier virus informatique voit le jour au Pakistan, il se nomme Brain et infecte les ordinateurs IBM.

La même année, la première loi contre la fraude informatique est votée par le congrès américain. Elle rend punissable par la loi, accès non autorisé aux ordinateurs du gouvernement. L’année suivante, le virus Jérusalem est détecté. Il est conçu pour supprimer les fichiers infectés les vendredi 13, c’est un des premiers virus capables d’infecter et de détruire des fichiers.

* En 1988

Robert Morris « lâche » dans la nature le premier ver internet qui va se répandre sur 6000 machines connectées. Il tentera d’expliquer après un coup qu’il s’agissait d’une erreur de programmation, il sera néanmoins condamné à trois mois de prison avec sursis et à 10000 dollars d’amende.

* En 1994

Le mathématicien russe Vladimir Levin Subtilise électroniquement dix millions de dollars à la Citybank ; s’introduisant sur le réseau bancaire international SWIFT. Interpellé à Londres en 1995, il fut condamné à trois ans de prison par un Tribunal américain.

La fin des années 90 a été marquée par la multiplication des virus informatique et les guerres déclarées entre les groupes de hackers rivaux.

La décennie 2000 a été marquée par la prise en compte des cyber délits. En 2000, David Dufresne et Florent Latrive, sont auteurs de livre Pirates et flics du Net, qui traduit le développement nécessaire de la régulation face à la montée de la cyberdélinquance.

Depuis 2003, les actes des cyberdélinquance se multiplient, les techniques se spécialisent en prenant des formes très variées.

# III. Les différents types de cybercriminalité

**La cybercriminalité** (ou le cybercrime) peut prendre de nombreuses formes, dont certaines pourraient sembler ne rien avoir à faire avec cette activité. Par exemple, même le vol d’un ordinateur physique peut être considéré comme une activité cybercriminalité si l’auteur a l’intention d’utiliser les informations qu’il contient pour son gain personnel. Si quelqu’un vole une clé USB contenant des données sensibles qu’ils prévoient de vendre sur le <<dark web>>, il s’agit aussi d’un cybercrime.

Voici quelques types de cybercrimes courants :

* **Attaques DDos** (attaques par déni de service distribue)

Celles-ci servent à rendre un service en ligne indispensable et à détruire le réseau en submergeant le site de trafic provenant de diverses sources. Les grands réseaux de périphériques infectes, appelés botnets, sont créés en déposant des logiciels malveillants sur les ordinateurs des utilisateurs.

* **Le vol d’identité**

Ce cybercrime se produit lorsqu’un criminel obtient l’accès aux informations personnelles d’un utilisateur pour lui voler de l’argent, accéder à ses informations confidentielles ou participer à une fraude fiscale ou une fraude à l’assurance maladie. Ils peuvent aussi ouvrir un compte téléphonique ou internet a votre nom, utiliser votre nom pour planifier une activité criminelle et réclamer les aides que vous donne le gouvernement. Pour ce faire, ils piratent les mots de passe de l’utilisateur et récupèrent des informations personnelles sur les réseaux sociaux ou en envoyant des emails de phishing.

Exemple : Yahoo a été pirate en 2013. Cette attaque a touché plus d’un milliard de compte dont le compte du directeur de campagne d’HILARY CLINGTON

* **Le phishing de mots de passe sur les réseaux** **publics**

Technique : nous le savons tous, les ordinateurs publics sont vulnérables et peuvent stocker des informations sur des milliers de personnes. Les pirates peuvent installer des applications sur des ordinateurs publics (sur place ou à distance) pour récupérer ces informations.

* **Les Malwares**

Le terme malware est compose des équivalents anglais de <<malveillant>> et <<logiciel>> ; vous savez donc qu’il est nuisible. Avec un malware, un pirate peut lancer un virus sur votre appareil. Ce malware peut être installe via un site web ou une App et peut voler des informations personnelles, financières ou commerciales. Il peut également être utilise pour rendre votre appareil complètement inutilisable parfois pour vous faire chanter.

* **Les faux réseaux publics**

Oui, se connecter au WIFI est toujours tentant, mais, comme chacun le sait, un réseau WIFI est très facile à créer. Quelqu’un peut parfaitement créer un faux réseau WIFI au nom du café ou de la place publique, où vous vous trouvez. Ensuite, il suffit que vous vous connectiez au réseau pour que cette personne surveille toutes vos activités numériques.

# Causes de la cybercriminalité

## Les causes de la criminalité au niveau individuel

Au niveau individuel, les causes sont multiples dont entre autres les fuites de données, les usurpations d’identité, les problèmes de fonctionnement des appareils : la cybercriminalité peut peser lourd dans vie des particuliers. Tout utilisateur peut se trouver confronté à des frais inattendus sur une carte bancaire à la suite d’un vol d’identité, ou victime d’une attaque au ransomware exigeant le paiement de plusieurs certaines ou milliers de dollars pour récupérer ses fichiers ou encore à des facteurs élevées de données mobiles ou d’électricité en raison d’activités de cryptojacking ou botnets. Pour les victimes de cyber harcèlement, nomment de harcèlement sexuel, le prix psychologique à payer est encore plus difficile à supporter.

## Les causes de la criminalité au niveau communautaire

Les entreprises, les institutions sanitaires et les gouvernements peuvent également être victimes de pertes de données sensibles, de charges financières énormes et de dommages à leur image de marque. En moyenne les attaques au ransomware visant les petites et moyennes entreprises en 2019 exigeant le paiement d’une rançon de 5900 dollars pour récupérer leurs fichiers ou leurs systèmes. Pire encore, le temps d’arrêt directement lié à ces attaques a couté en moyenne 141000 dollars aux entreprises concernées. Mais cela n’est en comparaison des attaques au ransomware adressées aux gouvernements, comme l’attaque dont a été victime le comité de Jackson, dans l’Etat de la Géorgie, contraint de payes 400 000 dollars pour récupérer ses systèmes et son infrastructure informatiques.

Les fuites de données peuvent également avoir des effets importants sur les entreprises et leurs clients, par exemple le piratage massif à équifax, la fuite Yahoo! ou les nombreuses failles de Facebook.

## Les causes de la cybercriminalité au niveau mondial

La cybercriminalité présente souvent une dimension internationale. Il faut noter que par exemple que les contenus illicites transmis par courrier qui transitent souvent par plusieurs pays avant d’atteindre leur destinataire. Parfois, ils ne sont pas stockés dans le pays mais à l’étranger. Ils est donc essentiel que les Etats concernés par un cyber délit collaborent étroitement aux enquêtes diligentées, ce que les accords en vigueur en matière d’entraide judiciaire ne favorisent pas, car ils disposent sur des procédures formelles et complexes, qui prennent souvent beaucoup de temps, et ne couvrent généralement pas des enquêtes spécifiques aux infractions informatiques.il est donc crucial de réviser les procédures afin de pouvoir rapidement réagir aux incident et répondre aux demandes de coopération internationale.

Dans de nombreux pays, le régime d’entraide repose sur de principe de la << double criminalité >> c’est pourquoi une enquête internationale n’est également ordonnée qui si l’infraction est sanctionnée dans tous les pays impliqués. Il existe certes des infractions, telle que la distribution de matériel pornographique impliquant des enfants, qui peuvent faire l’objet de poursuites n’importe où dans le monde. Malgré tout, les différences régionales jouent un rôle important. C’est cas notamment des infractions pour contenu illicite, par exemple les discours haineux, qui sont sanctionnés différemment selon les pays. Il n’est pas rare que certains contenus légalement autorisés par certains soient jugé par d’autre.

Partout dans le monde l’informatique repose fondamentalement sur la même technologie. Ainsi, à l’exception des différences linguistiques et du format des prises de courant, les ordinateurs et téléphones portables vendus en Asie ressemblent de très près a ceux vendus en Europe le cas d’internet n’est pas différent : du fait de la normalisation des réseaux, les pays africains utilisent les même protocoles que les Etats-Unis. C’est aussi pour cette raison que les internautes du monde entier peuvent avoir accès aux mêmes services. Il se pose la question des effets de l’harmonisation des normes techniques au niveau mondial sur l’évolution du droit pénal au niveau de chaque pays. En effet, s’agissant des contenus illicites, les internautes peuvent avoir accès à des informations venant du monde entier, et donc à certains disponibles légalement à l’étranger mais considérés comme illicites dans leur pays.

# Conséquence sur la société

La cybercriminalité est en l’espace de quelques années un véritable problème de la société. En effet l’usage des nouvelles technologies de l’informatique connaît assurément des dérivations dangereuses. Les entreprises sont plus concernées par la cybercriminalité car la plupart des cyberattaques sont dirigés vers elles. Surtout les PME (petites moyennes entreprises) car plus vulnérables, et notamment les e-commerces qui détiennent des données sensibles. Une cyberattaque peut entraîner une cyber crise, que ce soit au niveau IT (blocage du site), financier ou de réputation (les données utilisateurs risquent d’être exposées).

Les cyberattaques peuvent avoir les conséquences suivantes :

• Vol d'identité, fraude, extorsion,

• Matériel volé, comme les ordinateurs portables ou les appareils mobiles

• Violation de l'accès

• Sniffing du mot de passe

• Infiltration du système

• Dégradation du site Web

• Exploitation des navigateurs Web privés et publics

• Abus de messagerie instantanée

• Vol de propriété intellectuelle ou accès non autorisé

## Conséquences sur l’économie.

Ces attaques ont une incidence désastreuse sur l’économie. À cet effet selon une enquête réalisée par une entreprise de conseil en cyber sécurité (SERIANU), la criminalité informatique a fait perdre à l’Afrique près de 3,5 milliards de dollars en 2017. Un site spécialisé nous informe en ce sens que l’Afrique enregistre des centaines de millions de cyberattaques par an. Les banques et les administrations sont les plus ciblées par les hackeurs; L’Afrique paie un lourd tribu au fléau. Selon une estimation de la même source généralement acceptée, la cybercriminalité coûte à l’économie mondiale la somme de 500 milliards de dollars US.

# Les différentes sanctions prévues par la loi

Selon la loi nº2019-33, du 03 Juillet 2019, portant répression de la cybercriminalité, il existe en matière de cybercriminalité

Des infractions aussi bien dans le code pénal que dans la loi de

Cybercriminalité au Niger.

Voici quelques dispositions prévues par celle-ci :

-Article 29 : Diffamation par un moyen communication

Est puni d'une peine d'emprisonnement de six (6) mois à trois

(3) ans et d'une amende de un million (1.000.000) à cinq millions (5.000.000) de francs CFA, quiconque commet une diffamation par le biais d'un moyen de communication électronique.

-Article 30 : Injure par un moyen de communication électronique

Est puni d’une peine d’emprisonnement de six (6) mois à trois

(3) ans et d'une amende de un million(1.000.000) à cinq millions (5.000.000) de franc CFA, quiconque profère ou émet toute expression outrageante, tout terme de mépris ou toute invective qui ne renferme l'imputation d'aucun fait, par le biais d'un moyen de communication électronique»

-Article 31 : Diffusion de fausses nouvelles

Est puni d'une peine d'emprisonnement de six (6) mois à trois (3) ans et d’un million (1 000 000) à cinq millions (5 000 000) de francs CFA d'amende, le fait pour une personne de produire, de mettre à la disposition d'autrui ou de diffuser des données de nature à troubler l'ordre public ou à porter atteinte à la dignité humaine par le biais d'un système d'information.>>

-Article 32 : Propos à caractère raciste, régionaliste, ethnique, religieux ou xénophobe.

Est puni d'une peine d'emprisonnement d'un (1) à cinq (5) ans et de un million (1.000.000) à cinq millions (5.000.000) de francs

CFA d'amende, quiconque crée, diffuse ou met à disposition, sous quelque forme que ce soit, des écrits, messages, photos, sons, vidéos, dessins ou toute autre représentation d'idées ou de théories, de nature raciste, régionaliste, ethnique, religieux ou xénophobe, par le biais d'un système d’information ».

-Article 28 : Chantage par un moyen de communication électronique

« Est puni d'une peine d'emprisonnement de deux (2) à sept (7) ans et d'une amende de cinq millions (5.000.000) à vingt

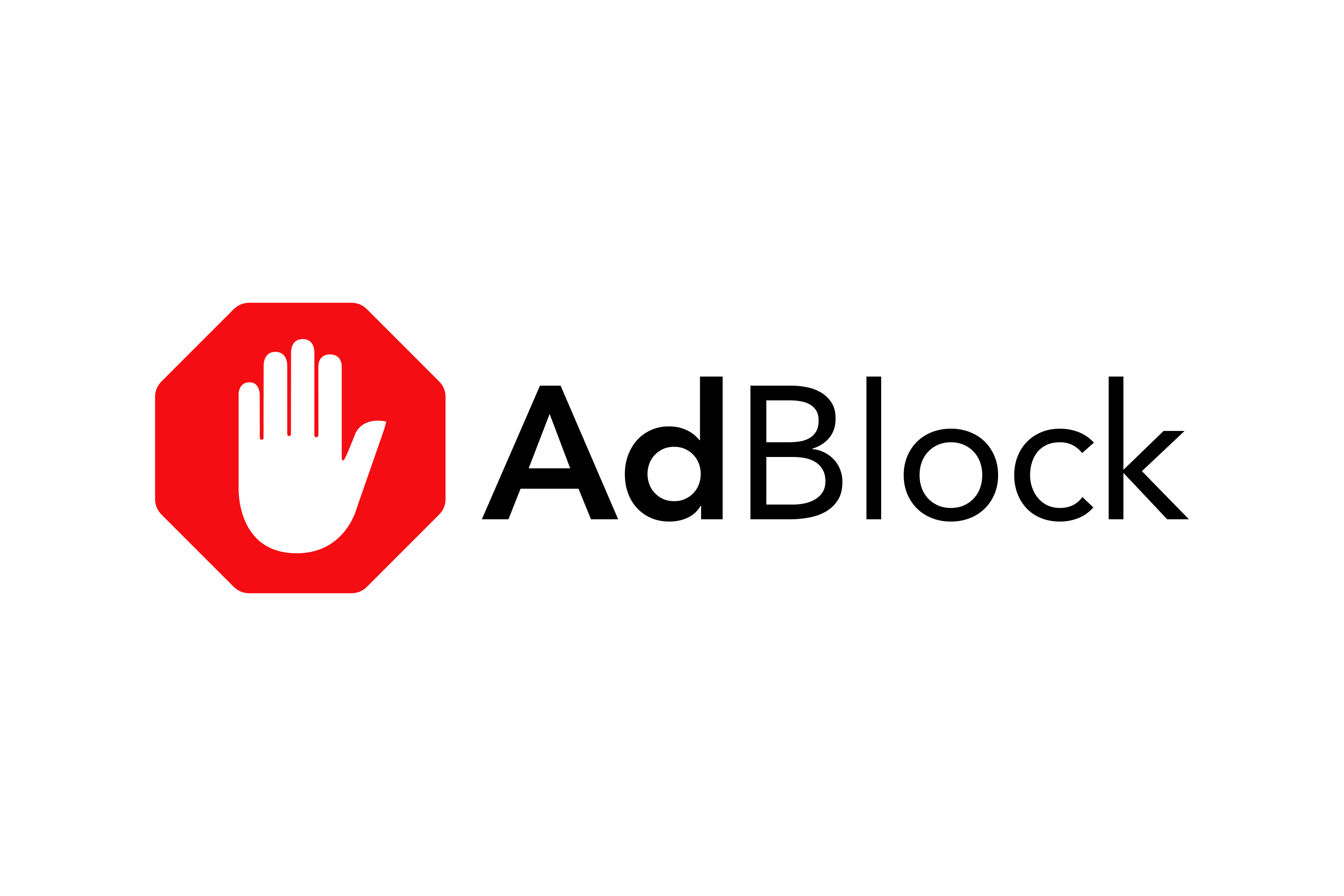
(20.000.000) de francs CFA, quiconque, au moyen de la menace d'atteintes à la confidentialité, à l'intégrité des données informatiques ou par toute forme d'atteintes à la confidentialité ou au fonctionnement du système informatique, extorque ou tente d'extorquer, soit la remise de fonds ou valeurs, soit la signature »

# Mise en pratique (voir la présentation pour plus de détail)

Ici pour mettre en pratique ce que nous venons d’exposer, nous avons décidé de créer **trois virus** selon les différentes époques dont la cyber criminalité a parcouru.

* Nous avons dans un premier point les attaques qui se faisaient avec les matériels informatiques (**clé USB, carte mémoire SSD, disc dure ...**) : pour ce type de crime nous avons créé un virus que nous appelons **FileThief** (voleur des fichiers). En effet, une fois mettre ce programme dans une **clé USB**, tant que vous la (USB) branchez à un ordinateur, celui-ci(**FileThief**) attaque automatiquement vos fichiers et les copie dans **la clé USB** en question.
* Nous avons codé et nommé le deuxième **autoreboot** pour qu’il soit un cas pratique des virus qui affectent les ordinateurs et qui causes par finir un dysfonctionne total du votre PC attaqué.
* Et enfin, le dernier sous le nom de **Fishing** qui démontre un des exemples de crimes qui se font de nos jours à travers l’internet(donc les HAKER créent des sites pour les arnaques et tant que vous inscrives dans ces sites, ils auront votre contrôle total n’importe quand et n’importe où).

# Moyens de protection contre la cyber criminalité



**Adblock** est une extension gratuite qui vous permet de personnaliser votre expérience sur le web. Vous pouvez bloquer les pubs agaçantes, désactiver le suivi et bien d’autres choses. Il est disponible pour tous les principaux navigateurs de bureau et pour vos appareils mobiles.



**KeePass : retenez un seul mot de passe et chiffrez tous les autres**

**KeePass** est sans conteste le **gestionnaire de mot de passe** le plus apprécié du moment et cela grâce à une myriade d’options qui apportent une fiabilité en sécurité hors du commun.

Sous licence GPL v2, KeePassKeePass est gratuit et le restera. Son code source est disponible pour tous les codeurs et développeurs du monde entier ce qui assure à KeePass des mises à jours et évolutions majeures au fil de ses versions

Son principe est très simple : **KeePass sauvegarde tous vos mots de passe** dans une base de données qui lui est propre et qui est en réalité un fichier chiffré (« crypté »).

Cette base de données n’est alors accessible que grâce à votre mot de passe principal, le seul que vous avez à retenir et que vous aurez préalablement judicieusement choisi.

La sécurité de l’accès à cette base de données peut être alors encore renforcée très simplement en joignant « une clé » (à l’aide d’un fichier .key)

Antivirus Microsoft Defender est un composant majeur de votre protection nouvelle génération dans Microsoft Defender pour point de terminaison. Cette protection regroupe le Machine Learning, l’analyse big data, la recherche approfondie sur la résistance aux menaces et l’infrastructure cloud Microsoft pour protéger les appareils (ou les points de terminaison) de votre organisation. Antivirus Microsoft Defender est intégré à Windows et fonctionne avec Microsoft Defender pour point de terminaison pour fournir une protection sur votre appareil et dans le cloud.

# Conclusion générale

Le monde depuis ses origines a connu des multiples évolutions, la révolution numérique est équivalent de bouleversement apporté au 15eme siècle par l’invention de l’imprimerie. Aujourd’hui nos vies sont digitalisées et internet est devenu un moyen de communication ultrapuissant, la délinquance numérique accompagnée du développement web constituent un nouveau fléau, chose qui a créé une grande ouverture pour les passionnés le l’informatique. Ainsi le domaine de la cyber criminalité est devenu une chose qui n’a pas de limite, car évolue en fonction du progrès de la technologie.