FINANCE PERSONNELLE 101 POUR ÉTUDIANTS

CIRANO

POLYFINANCES

LES BASES DE LA CYBERSÉCURITÉ

En collaboration

Autorité des marchés financiers

Table des matières

1. INTRODUCTION 1
2. LA CYBERSÉCURITÉ : DÉFINITION 2
2.1 Un sujet qui touche et impacte chacun 2
2.2 La présence des cyber risques 2
2.2.1 L'utilisation de technologies 2
2.2.2 Des efforts dans la protection des données 2
2.3 Les acteurs de la cybersécurité 3
2.4 Les cadres réglementaires et normes en cybersécurité 3
2.4.1 Les réglementations gouvernementales 3
2.4.2 Les normes en cybersécurité 4
3. LA SENSIBILISATION DES ÉTUDIANTS À LA CYBERSÉCURITÉ 5
3.1 Croissance des menaces dans les établissements d'enseignement 5
3.2 Finance personnelle des étudiants 5
3.3 Importance de la sensibilisation des étudiants 5
3.4 Rôle des établissements d'enseignement dans la formation à la cybersécurité 5
4. LES MENACES CYBERNETIQUES 7
4.1 Phishing ou hameçonnage 7
4.1.1 Hameçonnage 7
4.1.2 Spear-phishing 7
4.1.3 Fraude par carte de crédit : 8
4.2 Logiciels malveillants 8
4.3 Autres types de menaces 8
4.3.1 Menaces internes 8
4.3.2 Attaque de l'homme du milieu 9
4.3.3 Attaques par ingénierie sociale 9
5. L'OMNIPRESENCE DES CYBER RISQUES 10
5.1 La finance personnelle 10
5.2 L'investissement en ligne 10
5.2.1 L'infrastructure de la cryptomonnaie 11
5.3 Au-delà de la finance 11
5.3.1 Magasinage en ligne 11
5.3.2 Plateformes de divertissement 12
5.3.3 Réseaux sociaux 12
5.3.4 Plateformes de travail en équipe 13

6. MIEUX VAUT PRÉVENIR QUE GUÉRIR 15
6.1 Méthodes actuelles de protection 15
6.2 Bonnes pratiques 15
6.3 Outils disponibles pour contrer les risques cybernétiques 15
6.3.1 Prévention de la fraude 17
6.3.2 Détection de site sécurisé 18
6.4 Sensibilisation et formation continue en cybersécurité 19
7. CONCLUSION 20
References 21

1. INTRODUCTION

Dans l'ère numérique contemporaine où la population mondiale utilise énormément de technologies de l'information, celle-ci ne demeure pas à l'abri de vol, de perte de données ou encore de fraudes informatiques. En effet, un utilisateur de toute technologie de l'information, comme un téléphone, est exposé à des cyberrisques pouvant mettre en danger ses données. Ainsi, c'est pour cela que la cybersécurité émerge présentement comme une préoccupation majeure, touchant à la fois les individus et les organisations à l'échelle mondiale. Fondamentalement, la cybersécurité englobe les mesures et les pratiques visant à protéger les systèmes informatiques, les données sensibles et les réseaux contre les menaces en ligne, telles que les attaques malveillantes et les intrusions. Ainsi, pour un étudiant, comprendre la nature de la cybersécurité revêt une importance critique dans un monde où la connectivité est omniprésente. Cette compréhension s'avère essentielle alors que nous naviguons à travers divers aspects de notre vie quotidienne qui sont de plus en plus interconnectés et numérisés, allant de la gestion de nos finances personnelles au partage de contenu en ligne et à l'utilisation d'applications pour nos études et notre travail.

2. LA CYBERSÉCURITÉ : DÉFINITION

La cybersécurité se définit par l'action de veiller à la protection des systèmes en réseau afin d'empêcher toute attaque numérique de venir à l'encontre des activités de ces derniers. Par ailleurs, afin de veiller à maintenir la confiance de ses clients et l'intégrité de ses activités, il est de l'intérêt d'une entreprise de veiller à ce que les applications, l'infonuagique ou toute autre application du réseau soient protégées contre toute attaque numérique.

2.1 Un sujet qui touche et impacte chacun

En outre, que ce soit par téléphone, ordinateur personnel ou public, personne n'est à l'abri des dangers de vol de données. En effet, un exemple banal pourrait être un vol de données à travers un lien URL. Ainsi, un cybercriminel pourrait imiter les messages d'une compagnie de livraison et demander à l'utilisateur de suivre un lien qui parait anodin au premier abord. Ensuite, c'est à ce moment-là qu'à cause de diverses tactiques d'hameçonnage, l'utilisateur peut tomber dans le piège du cybercriminel et risquer de perdre ses données personnelles au profit de ce dernier.

Dans ce cas, la question sur l'utilisation des données personnelles volées par ces cybercriminels peut être posée. En effet, ces informations précieuses et confidentielles peuvent concerner toute donnée relative aux comptes bancaires, adresse ou encore des numéros d'identification nationaux (ex. Numéro d'assurance sociale). Ainsi, toute personne pourrait être impactée par des actions malveillantes, et si celles-ci se trouvent entre les mains d'une personne ayant des intérêts malsains, l'utilisateur pourrait risquer de perdre beaucoup de ces biens et des informations cruciales.

2.2 La présence des cyberrisques

2.2.1 L'utilisation de technologies

Aujourd'hui, la cybersécurité prend de plus en plus de place dans notre quotidien. L'essor des technologies de l'information a conduit à une augmentation exponentielle des cyberrisques. Que ce soit à travers l'utilisation d'ordinateurs, de téléphones intelligents, d'objets connectés ou encore de services en ligne, les menaces numériques sont omniprésentes. Les cyberattaques prennent diverses formes et avec la sophistication croissante des cybercriminels, une vigilance et une adaptation constantes des stratégies de protection sont nécessaires. Cette réalité pousse autant les particuliers que les entreprises à adopter des solutions de cybersécurité afin de se protéger des dangers en ligne.

2.2.2 Des efforts dans la protection des données

Les entreprises, conscientes de l'importance de sécuriser leurs informations sensibles, investissent massivement dans la cybersécurité. La protection des données est devenue une priorité stratégique, car une faille de sécurité peut engendrer des pertes financières considérables, ternir l'image de marque et nuire à la confiance des clients.

Par exemple, en 2022, les entreprises américaines ont dépensé en moyenne 9,44 millions de dollars pour réparer les dégâts causés par des violations de données (Montecuollo, 2022). Cette somme illustre l'ampleur des défis liés à la cybersécurité et la nécessité de renforcer les systèmes de protection. De nombreuses organisations adoptent ainsi des politiques strictes de gestion des accès, des protocoles de chiffrement des données et des audits réguliers afin d'anticiper les menaces.

Par ailleurs, les régulations gouvernementales, telles que le Règlement général sur la protection des données (RGPD) en Europe ou la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE) au Canada, imposent aux entreprises des normes élevées en matière de cybersécurité. Ces législations obligent les organisations à redoubler d'efforts pour sécuriser les informations personnelles de leurs clients et utilisateurs.

2.3 Les acteurs de la cybersécurité

La lutte contre les cybermenaces implique une diversité d'acteurs, chacun jouant un rôle essentiel dans la protection des données et des infrastructures numériques.

- **Les gouvernements et organismes de réglementation** : Ils établissent des lois et réglementations afin d'encadrer la cybersécurité. Par exemple, des entités comme l'Agence nationale de la sécurité des systèmes d'information (ANSSI) en France ou le Centre canadien pour la cybersécurité œuvrent pour protéger les infrastructures critiques et sensibiliser la population aux bonnes pratiques numériques.
- **Les entreprises spécialisées en cybersécurité** : De nombreuses sociétés développent des solutions avancées pour détecter, prévenir et contrer les cyberattaques. Elles fournissent des logiciels, des services de surveillance et des stratégies de réponse aux incidents.
- **Les entreprises et institutions** : Au-delà des firmes spécialisées, toutes les entreprises sont concernées par la cybersécurité. Elles doivent mettre en place des stratégies de protection des données et sensibiliser leurs employés aux risques liés aux cyberattaques.
- **Les utilisateurs** : Chaque internaute a un rôle à jouer dans la cybersécurité. En adoptant des pratiques sécuritaires, telles que la mise à jour régulière des logiciels, l'utilisation de mots de passe robustes et la vigilance face aux tentatives d'hameçonnage, les utilisateurs peuvent réduire les risques de compromission de leurs données personnelles.
- **Les pirates éthiques et chercheurs en cybersécurité** : Ces experts travaillent à identifier et corriger les vulnérabilités des systèmes avant qu'elles ne soient exploitées par des cybercriminels. Leurs recherches permettent d'améliorer continuellement les solutions de cybersécurité et de renforcer la résilience des infrastructures numériques.

L'évolution constante des menaces numériques requiert une collaboration accrue entre ces différents acteurs pour assurer un environnement numérique plus sécurisé et résilient face aux cyberattaques.

2.4 Les cadres réglementaires et normes en cybersécurité

Les cadres réglementaires et les normes en cybersécurité sont essentiels pour garantir la protection des données et des systèmes informatiques à l'échelle mondiale. Ils définissent les obligations des entreprises et des institutions afin de limiter les risques liés aux cyberattaques et aux violations de données.

2.4.1 Les réglementations gouvernementales

Plusieurs lois et règlements ont été mis en place pour encadrer la cybersécurité et protéger les données des utilisateurs :

- **Le Règlement général sur la protection des données (RGPD)** : Adopté par l'Union européenne en 2018, il impose des obligations strictes aux entreprises concernant la collecte, le stockage et l'utilisation des données personnelles des citoyens européens.
- **La Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE) – Canada** : Cette loi vise à protéger les informations personnelles des citoyens canadiens et à réguler la manière dont les entreprises les gèrent.
- **Le California Consumer Privacy Act (CCPA) – États-Unis** : Cette réglementation offre aux résidents de Californie un plus grand contrôle sur leurs données personnelles, notamment le droit de savoir quelles informations sont collectées et comment elles sont utilisées.
- **La Loi 25 (Québec)** : Anciennement connue sous le nom de projet de loi 64, cette loi modernise les règles en matière de protection des renseignements personnels au Québec et impose aux entreprises des obligations strictes, notamment en matière de consentement, de transparence et de gestion des incidents de sécurité.

2.4.2 Les normes en cybersécurité

En complément des réglementations nationales, plusieurs normes encadrent les pratiques en matière de cybersécurité :

- **Norme ISO/IEC 27001** : Cette norme internationale définit les exigences pour un système de management de la sécurité de l'information (SMSI), permettant aux organisations de gérer efficacement la protection de leurs données.
- **Norme ISO/IEC 27002** : Cette norme fournit un ensemble de bonnes pratiques pour la mise en œuvre de la gestion de la sécurité de l'information.
- **Norme NIST Cybersecurity Framework (États-Unis)** : Un cadre de référence développé par le National Institute of Standards and Technology qui aide les organisations à gérer et réduire les risques en cybersécurité.
- **Norme CAN/CIOSC 104** : Une norme canadienne qui établit des lignes directrices en matière de cybersécurité pour les petites et moyennes entreprises.
- **Cadre de cybersécurité du Centre canadien pour la cybersécurité** : Il fournit des recommandations aux organisations canadiennes pour améliorer leur posture en cybersécurité.
- **Norme CIS Controls** : Une liste de 20 contrôles de sécurité développée par le Center for Internet Security pour protéger les organisations contre les cyberattaques.

Ces réglementations et normes permettent aux organisations de renforcer leur posture en cybersécurité et de se conformer aux exigences légales pour éviter des sanctions et des pertes financières majeures.

3. LA SENSIBILISATION DES ÉTUDIANTS À LA CYBERSÉCURITÉ

3.1 Croissance des menaces dans les établissements d'enseignement

La sensibilisation à la cybersécurité est désormais indispensable pour les étudiants, en raison de la montée en puissance des menaces en ligne et de la dépendance croissante à l'égard des technologies numériques. Les écoles et les universités, qui ont été prises au dépourvu par le passage soudain aux cours en ligne, se trouvent souvent vulnérables et mal préparées aux cyberattaques. D'ailleurs, de nouvelles mesures et législations, telles que la *Loi sur la protection des cybersystèmes essentiels*, visent à souligner l'importance croissante de la cybersécurité dans les de nombreux secteurs (Gouvernement du Canada, 2023). L'objectif serait d'avoir les outils pour préparer et prévenir les incidents de cybersécurité qui pourraient subvenir.

Dans ce cas, en tant que membres de la société numérique, les étudiants ont la responsabilité de comprendre les risques en ligne et d'adopter de bonnes pratiques. Les cyberattaques, telles que l'hameçonnage, sont de plus en plus courantes dans le secteur de l'éducation, mettant en danger la sécurité des données des étudiants, du personnel et des parents. La mise en place de programmes de sensibilisation à la cybersécurité au sein des établissements d'enseignement est primordiale pour former leur personnel et leurs étudiants à détecter et à prévenir ces menaces. Ces programmes apparaissent notamment aux mois d'octobre, soit le mois de la sensibilisation à la cybersécurité. En 2023, la thématique du mois de la cybersécurité proposée au Canada a pu mettre en lumière différentes ressources variées afin d'inciter le public à « Penser cybersécurité » (Gouvernement du Canada, 2024).

3.2 Finance personnelle des étudiants

Sur le plan de la finance personnelle, la sensibilisation à la cybersécurité est tout aussi cruciale. Les étudiants gèrent souvent leurs finances en ligne, que ce soit pour le paiement des frais de scolarité, la gestion de leur budget ou les transactions bancaires. En étant conscients des risques de cyberattaques, ils peuvent protéger leurs informations financières et éviter les fraudes en ligne, ce qui peut avoir un impact significatif sur leur stabilité financière future.

3.3 Importance de la sensibilisation des étudiants

Plusieurs utilisateurs pourraient se poser la question suivante : en quoi est-il important pour un étudiant de se sensibiliser à la cybersécurité ?

La sensibilisation des étudiants à la cybersécurité est au cœur des enjeux de responsabilité individuelle. Cette sensibilisation nécessite l'éducation à la cybersécurité à la communauté étudiante, et pourrait se faire dans des formats variés qui encouragent l'interaction et la participation des étudiants. Des actions éducatives permettent de maximiser cette sensibilisation à la cybersécurité, et peuvent aller à l'hygiène des mots de passe, les simulations d'hameçonnage et la mise en place d'un plan de réponse aux incidents. Des études de cas démontrent même que les programmes de sensibilisation à la cybersécurité peuvent être efficaces et même ludiques, incitant les participants à mettre en pratique leurs connaissances nouvellement acquises.

La sensibilisation à la cybersécurité est alors primordiale dans l'éducation pour protéger les données, préparer les étudiants à leur vie professionnelle, renforcer la responsabilité sociale, sécuriser les finances personnelles et contribuer à la prévention des cyberattaques.

3.4 Rôle des établissements d'enseignement dans la formation à la cybersécurité

Avec la nécessité croissante à sensibiliser les étudiants aux risques et enjeux liés à la cybersécurité, il est important d'offrir des programmes attrayants pour tous les niveaux, afin d'en savoir davantage sur les mesures de sécurité qui sont utilisées lorsqu'on utilise nos appareils électroniques ou quand nous naviguons sur le web.

Voici des exemples d'universités à Montréal qui propose l'enseignement de la cybersécurité aux étudiants :

- Université de Montréal
- Polytechnique Montréal
- Université McGill

Pour les plus avancés, plusieurs types de compétitions de cybersécurité sont proposées, que ce soit sur une échelle internationale comme la compétition NorthSec CTF, ou même à travers des comités étudiants au sein d'établissements scolaires.

4. LES MENACES CYBERNÉTIQUES

Avec l'omniprésence de la cybersécurité, il est important de rester au courant des différentes formes d'attaques possibles réalisées par des malfaiteurs, etc.

4.1 « Phishing » ou hameçonnage

Par définition, le « phishing » ou hameçonnage est une technique de cyberattaque utilisée par des individus malveillants pour obtenir des renseignements personnels dans le but de commettre un vol d'identité.

Elle consiste essentiellement à faire croire à la victime qu'elle s'adresse à un tiers de confiance. Pour cela, l'individu malveillant n'hésite pas à se faire passer pour un organisme bien connu tel qu'un représentant d'une banque ou de toute autre entreprise afin de tromper sa victime. Il peut ainsi facilement soutirer des informations personnelles à son interlocuteur naïf (Wikipédia, 2024).

Ainsi, il existe plusieurs moyens utilisés par ces individus malveillants afin d'atteindre leur objectif. Ces différentes approches sont :

4.1.1 Hameçonnage

Par courriels et par SMS

Ce premier type d'hameçonnage est le plus courant de nos jours. En fait, il s'agit essentiellement d'envoyer un message à un individu, que ce soit un courriel ou un SMS. Le message envoyé viendrait d'une personne malveillante qui prétend être une personne occupant une certaine fonction dans une entreprise connue. Ainsi, il est difficile de douter de la crédibilité de l'information transmise. Dans la majorité des cas, il s'agit d'une demande d'informations personnelles telle que des identifiants de connexion, des mots de passe ou des informations de carte de crédit. Ces courriels contiennent généralement des liens Web et des pièces jointes malveillants. Par exemple, lors de la pandémie de COVID-19, de nombreux individus ont prétendu appartenir à des programmes d'aide du gouvernement canadien pour cibler les personnes vulnérables. Il est donc nécessaire d'être capable de détecter les signes d'une arnaque par message. De nombreux moyens de préventions et de détections sont disponibles en cliquant ici !

Par téléphone

En matière de fraude téléphonique, les individus malveillants utilisent divers stratagèmes pour piéger leurs victimes. L'une des méthodes courantes consiste en des appels automatisés, où un message préenregistré est diffusé à l'aide d'une voix robotisée ou, parfois, de la voix d'une vraie personne. Ces fraudeurs se font souvent passer pour des représentants d'organisations légitimes, telles que des banques ou des organismes gouvernementaux, afin d'amener les victimes à divulguer des informations personnelles sensibles, comme des numéros de compte bancaire ou des identifiants de connexion. Pour en apprendre plus sur les autres méthodes employées par ce type de fraude, cliquer ici !

Via les réseaux wifi

Cette forme d'hameçonnage est caractérisée par le vol d'informations personnelles via les réseaux wifi. Plusieurs méthodes peuvent être employées dans ce type de fraude. Un exemple de méthode employée pour frauder une victime est la création d'un réseau frauduleux portant le même nom que le réseau d'un aéroport, d'une bibliothèque ou d'un café. Ainsi, un cybercriminel réussit à tromper les utilisateurs qui s'y connectent et vole leurs données personnelles. Pour en apprendre plus, cliquer ici !

4.1.2 « Spear-phishing »

Le « spear-phishing » s'agit d'une attaque personnalisée. En d'autres termes, pour ce qui est de cette forme d'hameçonnage, les individus malveillants ciblent directement des personnes ou entreprises particulières. Il y a généralement plus de chance de tromper les individus de cette manière, car ces

messages personnalisés regorgent d'information touchant le récepteur. Dans ce cas, selon la victime, il lui est inconcevable que ces messages ne puissent pas provenir d'expéditeurs légitimes. Pour en savoir plus : cliquer ici.

4.1.3 Fraude par carte de crédit :

En ce qui concerne ce type d'hameçonnage, celui-ci s'agit du vol et de l'utilisation des informations d'une carte de crédit à l'insu de son véritable propriétaire (Gouvernement du Canada, 2019). Plusieurs moyens sont employés par les individus malveillants afin d'obtenir ces informations. Par exemple, il est possible de les récupérer en demandant à la victime d'utiliser sa carte de crédit pour l'achat d'un produit ou service à travers un faux site Web. En outre, une autre méthode consiste à installer des dispositifs sur les terminaux de paiement pouvant enregistrer l'information de la carte de crédit. D'ailleurs, cette dernière méthode est aujourd'hui une menace omniprésente dans le monde de la finance. Dans le cas où vos informations de carte de crédit sont compromises ou si vous avez perdu votre carte de crédit, voici des ressources pour connaître les mesures à prendre.

4.2 Logiciels malveillants

Les logiciels malveillants sont un type de menace qui survient souvent et qui entraine des conséquences importantes impactant l'utilisateur. Ce type de menace survient lorsque des logiciels tels que des virus ou bien des logiciels espions contournent les méthodes de détection pour accéder à l'ordinateur de l'utilisateur pour l'endommager.

Les logiciels malveillants désignent un large éventail de programmes informatiques qui sont conçus pour endommager, perturber ou effectuer des actions non autorisées sur le système informatique de l'utilisateur. Ils peuvent voler et supprimer des données, altérer ou prendre le contrôle des fonctions centrales de l'appareil et espionner l'activité de l'utilisateur sans consentement. Parmi les types les plus courants de logiciels malveillants, on trouve les virus, les rançongiciels ou « ransomwares » et les espiogiciels ou « spywares »

Les virus sont des types de logiciels malveillants qui, une fois exécutés, se répliquent en modifiant d'autres programmes informatiques. Les virus se propagent lorsque le logiciel infecté est exécuté sur un ordinateur, ce qui endommage le système, supprime des fichiers ou ralentit le dispositif. Les virus se propagent souvent via des pièces jointes de courrier électronique ou des téléchargements depuis Internet.

Le rançongiciel ou « ransomware » est un type de logiciel malveillant qui chiffre les fichiers de l'utilisateur, rendant toute donnée inaccessible, puis demande une rançon pour le déchiffrement des fichiers. Les attaques de rançongiciel ou « ransomware » ciblent aussi bien les individus que les entreprises, et peuvent entrainer la perte de données critiques ainsi que des coûts financiers importants.

L'espiogiciel ou « spyware » est conçu pour enregistrer l'activité d'un ordinateur ou d'un appareil mobile sans le consentement de l'utilisateur. Les informations recueillies peuvent inclure l'historique des sites Web, des données de formulaires, et même des identifiants et mots de passe.

4.3 Autres types de menaces

Plusieurs autres types de menaces sont possibles et les activités des nombreux utilisateurs peuvent être plus vulnérables aux risques des menaces (IBM, 2024).

4.3.1 Menaces internes

Les menaces internes en cybernétique sont possibles dans une organisation où un employé malveillant abuse de ses autorisations d'accès et les utilisent contre l'organisation, que ce soit en partageant des données, en les manipulant ou en les volant.

4.3.2 Attaque de l’homme du milieu

Les activités d’un utilisateur peuvent être surveillées pour ensuite avoir leurs données interceptées par des pirates informatiques. L'objectif de cette interception est de voler, d'écouter ou de modifier les données à des fins malveillantes, telles que l'extorsion de fonds.

4.3.3 Attaques par ingénierie sociale

L’ingénierie sociale est une méthode utilisée par les cybercriminels pour manipuler des individus et les inciter à divulguer des informations sensibles. Ces attaques prennent diverses formes, comme des appels téléphoniques frauduleux, des courriels trompeurs ou des interactions en personne visant à obtenir un accès non autorisé aux systèmes. Les attaquants exploitent la confiance, la peur ou l'urgence pour atteindre leurs objectifs.

5. L'OMNIPRÉSENCE DES CYBER RISQUES

De nos jours, la cybersécurité est devenue un aspect d'un extrême important au sein de notre vie quotidienne. Ainsi, nos modes de communication, d'éducation, de travail et de divertissement, la protection des informations personnelles et des données sensibles est devenue une priorité absolue. Que ce soit pour sécuriser nos transactions bancaires en ligne, protéger nos conversations privées des regards indiscrets, ou encore défendre l'intégrité de nos systèmes d'information contre les cyberattaques, la cybersécurité joue un rôle central dans notre quotidien.

5.1 La finance personnelle

Dans un paysage financier de plus en plus numérique, la protection des informations financières personnelles est non seulement essentielle pour éviter le vol d'identité et les fraudes bancaires, mais elle joue également un rôle crucial dans la préservation de la sécurité financière personnelle dans son ensemble. D'ailleurs, à la suite d'une étude menée par Equifax en 2023, près de 97% des Canadiens pensent être vulnérables face aux menaces frauduleuses (Global News WIre, 2023). De plus, Statistiques Canada a recensé près de 168 483 cas de fraude en 2021, comparé à 87 174 cas en 2011 (Statistique Canada, 2023).

Ainsi, afin de garantir la sécurité des comptes bancaires en ligne, il est impératif de mettre en place des mesures de sécurité rigoureuses, telles que l'utilisation de mots de passe robustes et la mise en œuvre d'un processus d'authentification à deux facteurs. Les mots de passe complexes, accompagnés de méthodes d'authentification supplémentaires telles que les codes SMS ou les applications d'authentification, renforcent considérablement la sécurité des comptes en limitant l'accès non autorisé.

De plus, l'utilisation de la technologie blockchain sous-jacente aux cryptomonnaies contribue à renforcer la sécurité financière personnelle. En effet, la nature décentralisée de la blockchain rend extrêmement difficiles la manipulation des transactions et la falsification des données, offrant ainsi une protection supplémentaire contre la fraude et la cybercriminalité.

5.2 L'investissement en ligne

Il existe de nos jours de nombreuses plateformes d'investissement en ligne. Ces plateformes permettent à leurs utilisateurs d'acheter, de vendre et de gérer en un seul endroit une large gamme d'actifs. Ce sont généralement des sites web ou des applications mobiles où il est possible d'acquérir des actions, de la cryptomonnaie, des ETF, des matières premières et même des fonds. D'ailleurs, chaque plateforme a ses propres avantages. Ainsi, en tant qu'utilisateur, il est important d'explorer ceux qui correspondent à ses besoins et à son profil d'investissement.

Voici un site qui vous permettra de vérifier si une personne ou une entreprise avec laquelle vous avez fait affaire est autorisée à exercer des activités liées au conseil ou à la vente de produits financiers : Registre des entreprises autorisées. Ce registre officiel vous aidera à confirmer la légitimité des conseillers et des entreprises dans le domaine financier.

En outre, les plateformes d'investissement constituent une réelle source de cybercriminalité en raison de leur grande attractivité. En effet, plusieurs fausses plateformes sont mises sur pieds par des individus malveillants. Ces dernières sont très élaborées et présentent une apparence très soignée, trompant facilement d'un coup d'œil les investisseurs.

Il devient donc important d'être capable de distinguer les faux sites ainsi que les faux courtiers. Pour ce faire, il faut constamment se tenir à jour des différentes stratégies développées. De nombreux moyens et stratégies pour détecter ce genre de sites sont évoqués et accessibles en cliquant ici .

5.2.1 L’infrastructure de la cryptomonnaie

Avec l’investissement en ligne vient également l’aspect particulier de l’investissement dans la cryptomonnaie.

La cybersécurité est un pilier fondamental pour les cryptomonnaies. Effectivement, la dépendance des cryptomonnaies envers la technologie digitale et les réseaux informatiques les exposent à des risques de cyberattaques. Par conséquent, une cybersécurité robuste est indispensable pour préserver l'intégrité des cryptomonnaies.

Au cœur des cryptomonnaies se trouve la blockchain, une technologie basée sur des principes cryptographiques rigoureux assurant sécurité et transparence des transactions. Effectivement, cette technologie empêche les risques de double dépense, de falsification des transactions ou de vols d'identité, qui pourraient autrement diminuer la confiance dans les cryptomonnaies. Par ailleurs, les contrats intelligents, qui automatisent les transactions et les accords sur la blockchain, doivent également être sécurisés contre les failles pouvant être exploitées pour détourner des fonds.

De même, face aux évolutions technologiques rapides, l'infrastructure des cryptomonnaies doit rester agile à travers l’adoption d’une démarche proactive en matière de cybersécurité. Cela inclut la recherche constante de nouvelles menaces ainsi que l'application régulière de mises à jour de sécurité.

Finalement, la réglementation joue un rôle clé, avec des normes de cybersécurité qui visent à protéger les consommateurs et prévenir le blanchiment d'argent. Ainsi, les acteurs de l'industrie doivent se conformer aux réglementations, renforçant l'importance d'une infrastructure de cybersécurité solide.

Voici les plateformes de négociation de cryptoactifs inscrites auprès de l’Autorité afin d'éviter les faux conseillers en finance ou les sites non réglementés : Plateformes inscrites auprès de l'Autorité

En conclusion, la cybersécurité n'est pas seulement une nécessité pour la protection des actifs dans l'univers des cryptomonnaies ; elle est également cruciale pour assurer l'intégrité de l'écosystème blockchain. Sans une attention aux défis de sécurité, la confiance dans les cryptomonnaies pourrait diminuer, freinant leur adoption et leur potentiel d'innovation.

5.3 Au-delà de la finance

La cybersécurité ne se limite pas au secteur financier ; elle concerne également de nombreux autres domaines. En 2018, 15 % des entreprises de dix salariés ou plus ont subi un incident de sécurité informatique, avec des disparités selon les secteurs : 21 % des sociétés spécialisées dans les activités scientifiques et techniques ont été touchées, contre 12 % dans la construction (INSEE, 2021).

5.3.1 Magasinage en ligne

Il est connu qu’aujourd’hui le magasinage en ligne est devenu une pratique courante pour de nombreux consommateurs. Cependant, cela présente également des risques pour la sécurité financière personnelle. Ainsi, il est important de reconnaître ces risques et de prendre des mesures pour les atténuer, tant du côté du client que du côté du commerçant.

Du côté du client, plusieurs risques peuvent survenir. Parmi ceux-ci, il existe la possibilité de recevoir des articles contrefaits ou de qualité inférieure par rapport à ce qui a été commandé. De plus, il existe des cas de fraudes où un client peut déclarer qu'un article n'a jamais été reçu ou tenter de retourner un article différent de celui initialement acheté, dans le but de récupérer un remboursement injustifié. Du côté du commerçant, les risques sont également présents. Certains commerçants peuvent se livrer à des pratiques frauduleuses telles que l’envoi de produits incorrects ou défectueux, dans le but de maximiser leurs profits. Il y a également le risque de vol d’informations personnelles des clients, comme les numéros de carte de crédit.

Par ailleurs, le magasinage en ligne offre alors de nombreux avantages, mais offre également des risques pour la sécurité financière personnelle. En prenant des précautions appropriées des deux côtés de la

transaction, les clients et commerçants peuvent minimiser ces risques et profiter des avantages du magasinage en ligne. Ainsi, afin d'atténuer ces risques, tant les clients que les commerçants doivent prendre des mesures de sécurité appropriées. Du côté du client, il est essentiel de vérifier la réputation du vendeur et de lire attentivement les avis et les politiques de retour avant de faire un achat en ligne. Il est également important d'utiliser des méthodes de paiement sécurisées et d'éviter de divulguer des informations personnelles sensibles à des sites non sécurisés. Du côté du commerçant, il est impératif de mettre en place des mesures de sécurité robustes pour protéger les informations des clients et éviter les fraudes. Cela peut inclure la surveillance régulière des transactions pour détecter toute activité suspecte ainsi que l'utilisation de protocoles de sécurité avancée.

5.3.2 Plateformes de divertissement

Dans les plateformes de divertissement en ligne, la sécurité est devenue une priorité incontournable pour garantir l'intégrité des données des utilisateurs et protéger contre les menaces telles que le piratage et les attaques de logiciels malveillants. Avec la montée en popularité des services de streaming et de téléchargement, la protection des informations personnelles des utilisateurs est devenue une préoccupation majeure.

Les sites de streaming gratuits, bien qu'attrayants pour les utilisateurs cherchant à économiser de l'argent, présentent souvent des risques en termes de sécurité. Ces sites peuvent être vulnérables aux attaques de logiciels malveillants et aux tentatives d'hameçonnage, où les utilisateurs sont incités à divulguer leurs informations personnelles sous prétexte de bénéficier d'un accès gratuit au contenu. De plus, certains de ces sites peuvent contenir des publicités malveillantes qui tentent de télécharger des logiciels malintentionnés sur les appareils des utilisateurs.

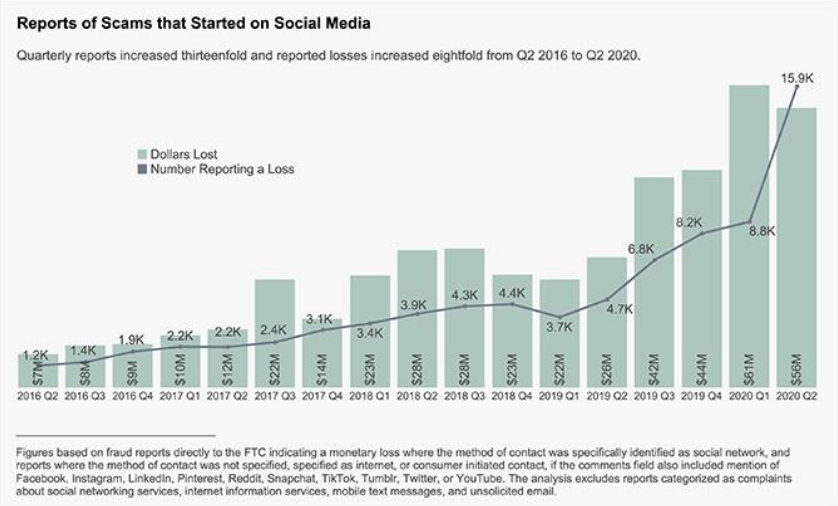
Face à ces défis, les plateformes de divertissement en ligne déploient des mesures de sécurité robustes pour protéger leurs utilisateurs. Cela comprend la mise en œuvre de protocoles de cryptage pour sécuriser les données des utilisateurs, la surveillance active des activités suspectes et la sensibilisation des utilisateurs aux pratiques de sécurité en ligne. De plus, les utilisateurs sont encouragés à utiliser des services de streaming légitimes et à éviter les sites douteux qui pourraient compromettre leur sécurité en ligne.

En résumé, la cybersécurité est une préoccupation importante même dans le domaine du divertissement en ligne, et les utilisateurs doivent être conscients des risques et prendre des mesures pour protéger leurs données personnelles lorsqu'ils accèdent à des plateformes de divertissement en ligne.

5.3.3 Réseaux sociaux

Les réseaux sociaux, autrefois considérés comme des espaces de partage informel, sont désormais soumis à des mesures strictes de protection des informations personnelles, afin de contrer la cybercriminalité et les abus en ligne. Avec des milliards d'utilisateurs actifs à travers le monde, les réseaux sociaux sont devenus des cibles attrayantes pour les cybercriminels cherchant à accéder à des informations sensibles et à mener des activités malveillantes. En effet, comme le présente la figure 1 ci-dessous, les attaques cybercriminelles, comme l'hameçonnage, n'ont cessé d'augmenter entre 2016 et 2020.

Figure 1. Augmentation des hameçonnages réalisés à partir des réseaux sociaux (TIME, 2020).



Ainsi, les plateformes de réseaux sociaux déploient des efforts considérables pour renforcer la sécurité de leurs utilisateurs, en mettant en œuvre des politiques de confidentialité strictes et en développant des outils de sécurité avancés. En effet, ces mesures comprennent la cryptographie de bout en bout pour les messages privés, la vérification en deux étapes pour sécuriser les comptes, et la détection automatique et la suppression de contenu inapproprié ou dangereux. De plus, les utilisateurs sont encouragés à être vigilants et à exercer un contrôle sur leur propre sécurité en paramétrant correctement leurs paramètres de confidentialité, en évitant de partager des informations sensibles en public, et en signalant tout comportement suspect ou toute activité malveillante. En définitive, les réseaux sociaux continuent d'évoluer pour répondre aux défis de la cybersécurité, mais la responsabilité de protéger les données personnelles des utilisateurs incombe également à ces derniers, qui doivent rester informés et engagés dans la sécurisation de leur présence en ligne. Par conséquent, il est crucial que les utilisateurs comprennent les risques associés à leur utilisation des réseaux sociaux et qu'ils prennent des mesures proactives pour protéger leur vie privée et leur sécurité en ligne.

Malgré ces efforts, les cybermenaces continuent d'évoluer, impactant la vie privée et la réputation en ligne des individus. Les traces numériques laissées sur ces plateformes peuvent être exploitées à des fins malveillantes, telles que le vol d'identité, le cyberharcèlement ou la diffusion de fausses informations. Par exemple, en Corée du Sud, des « deepfakes » pornographiques ont été utilisés pour cibler de jeunes femmes, illustrant les dangers de ces technologies (Le Monde, 2024).

Les avancées en intelligence artificielle ont également introduit de nouveaux risques, notamment avec la création de « deepfakes ». Ces vidéos truquées, générées par des algorithmes d'IA, peuvent représenter des individus tenant des propos ou commettant des actes qu'ils n'ont jamais réalisés, menaçant ainsi leur réputation et leur crédibilité. Par exemple, des « deepfakes » ont été utilisés pour diffuser de fausses informations lors d'élections, manipulant l'opinion publique et compromettant l'intégrité des processus démocratiques (Wikipédia, 2024).

Il est donc essentiel que les utilisateurs restent informés des risques associés à l'utilisation des réseaux sociaux et des technologies émergentes, et qu'ils adoptent des mesures proactives pour protéger leur vie privée et leur sécurité en ligne.

5.3.4 Plateformes de travail en équipe

En parallèle, la sécurité est également au cœur de la réalisation de travaux en équipe, où la confidentialité des données et la protection contre les fuites d'informations sensibles sont cruciales. Des outils de cryptage sophistiqués et des protocoles de sécurité avancés sont mis en place pour garantir que

les projets collaboratifs ne soient pas compromis par des accès non autorisés ou des atteintes à la vie privée. De plus, des fonctionnalités de suivi des modifications permettent de suivre l'historique des modifications apportées aux documents, ce qui renforce la transparence et la responsabilité au sein des équipes. En outre, les administrateurs de ces plateformes ont la possibilité de définir des politiques de sécurité personnalisées, de surveiller l'activité des utilisateurs et de détecter toute activité suspecte ou non autorisée. En adoptant ces mesures de sécurité avancées, les équipes peuvent collaborer de manière efficace tout en protégeant la confidentialité et l'intégrité de leurs données sensibles.

Ainsi, que ce soit dans notre divertissement en ligne, nos interactions sur les réseaux sociaux ou notre collaboration professionnelle, la sécurité se dresse comme un rempart essentiel, assurant la protection de nos informations et de nos échanges dans un monde de plus en plus connecté et exposé aux risques cybernétiques. En plus du domaine financier, il est important de noter la présence de la cybersécurité dans des parties essentielles de notre vie quotidienne. Notez que la présence importante des réseaux sociaux permet aux cyberattaquants d’utiliser ces mêmes plateformes de communication et de divertissement afin de réaliser des actes malveillants.

6. MIEUX VAUT PRÉVENIR QUE GUÉRIR

6.1 Méthodes actuelles de protection

La sécurité en ligne est devenue un enjeu majeur pour les internautes, qui sont de plus en plus conscients des risques liés à la navigation sur internet. Il est donc essentiel de savoir comment identifier un site sécurisé pour éviter les menaces telles que les virus, les logiciels malveillants ou le vol d'informations personnelles. Voici les principaux indicateurs de sécurité :

1. **Le cadenas :** L'un des premiers signes indiquant qu'un site est sécurisé est la présence d'un cadenas dans la barre d'adresse. Ce cadenas vert ou gris, selon le navigateur utilisé, signifie que le site utilise une connexion sécurisée (HTTPS) et que les données échangées entre votre ordinateur et le serveur sont chiffrées.
2. **Le protocole HTTPS :** Le protocole HTTPS (Hypertext Transfer Protocol Secure) est une version sécurisée du protocole HTTP. Il garantit que les informations transmises entre votre ordinateur et le serveur sont cryptées et donc protégées contre les interceptions ou les modifications non autorisées.
3. **Les certificats SSL :** Les certificats SSL (Secure Sockets Layer) sont des fichiers de données qui permettent d'établir une connexion sécurisée entre un serveur web et un navigateur. Ils sont émis par des autorités de certification reconnues et garantissent l'authenticité du site visité.
4. **Les avis et les commentaires :** Avant de fournir des informations personnelles ou financières sur un site, il est recommandé de consulter les avis et les commentaires d'autres utilisateurs. Les sites fiables et sécurisés ont généralement des évaluations positives et des commentaires élogieux de la part de leurs utilisateurs.

6.2 Bonnes pratiques

Voici de **bonnes pratiques** à avoir en naviguant à travers le web :

1. **Mettre à jour son navigateur et son système d'exploitation** : Les mises à jour régulières de votre navigateur et de votre système d'exploitation permettent de corriger les failles de sécurité connues et d'améliorer la protection contre les menaces en ligne.
2. **Utiliser un logiciel antivirus et un pare-feu :** Un logiciel antivirus et un pare-feu sont des outils essentiels pour protéger votre ordinateur contre les virus, les logiciels malveillants et les attaques en ligne. Assurez-vous de les maintenir à jour et de les configurer correctement.
3. **Éviter de cliquer sur des liens suspects ou des pièces jointes douteuses :** Les liens et les pièces jointes provenant d'expéditeurs inconnus ou de courriels suspects peuvent contenir des logiciels malveillants ou des virus. Il est important de ne pas cliquer sur ces liens ou de télécharger ces pièces jointes sans vérifier leur authenticité.
4. **Utiliser des mots de passe forts et uniques :** Les mots de passe forts et uniques sont essentiels pour protéger vos comptes en ligne contre les tentatives de piratage. Évitez d'utiliser des informations personnelles ou des mots de passe faciles à deviner, et changez-les régulièrement.

Il est crucial de savoir identifier les signes de sécurité sur un site web pour naviguer en toute sécurité et protéger vos informations personnelles. En appliquant les bonnes pratiques mentionnées ci-dessus, vous pouvez réduire considérablement les risques liés à la navigation en ligne.

6.3 Outils disponibles pour contrer les risques cybernétiques

Lorsqu'il s'agit de se protéger contre les attaques cybernétiques, plusieurs outils sont à la disposition des utilisateurs. Dans cette section, nous élaborerons sur chacun des outils les plus recommandés pour protéger ses données.

Antivirus/Anti-malware

Les antivirus ou anti-malware sont des programmes qui examinent les fichiers de votre ordinateur et les courriels à la recherche de virus dans le but de protéger votre système contre les logiciels malveillants, les virus et les programmes indésirables. Il est crucial de maintenir un tel logiciel à jour pour qu'il puisse détecter les nouveaux virus. Cet outil est essentiel pour protéger vos données, logiciels et système d'exploitation contre les menaces. Pour en savoir plus, consultez le site du gouvernement.

Coupe-feu : Un coupe-feu personnel ou plus connu sous le nom de "firewall" est un outil crucial pour la protection contre les attaques cybernétiques (Gouvernement du Canada, 2021). Il agit comme une barrière entre votre ordinateur et Internet, filtrant le trafic entrant et sortant pour détecter et bloquer les menaces. En surveillant le trafic, il peut identifier les activités suspectes, bloquer les tentatives d'intrusion et limiter l'accès des logiciels malveillants à Internet. Avec sa capacité à contrôler le trafic des applications et à générer des alertes en cas d'activité suspecte, un pare-feu personnel est un élément essentiel pour renforcer la sécurité de votre ordinateur contre les attaques en ligne. Pour en savoir plus, consultez le site du gouvernement.

RPV (Réseau Privé Virtuel) : Un RPV ou plus connu sous le nom de « VPN » crypte votre connexion Internet, ce qui rend difficile pour les pirates informatiques de surveiller vos activités en ligne (Gouvernement du Canada, 2022). Cet outil est particulièrement recommandé lorsque vous naviguez sur des réseaux Wi-Fi publics, par exemple dans un café. Il crée un tunnel sécurisé entre votre appareil et Internet, garantissant que toutes vos données sont sécurisées et cryptées avant d'atteindre leur destination. Alors que la plupart des applications sur votre appareil utilisent le cryptage pour sécuriser les données que vous envoyez, l'utilisation d'un RPV garantit que toutes les données envoyées sont protégées. Bien que plusieurs services de RPV soient à votre disposition, sachez que certains se concentrent sur simplement masquer votre adresse IP et non le cryptage de vos données. Choisissez un service qui protège vos données. Pour en savoir plus, consultez le site du gouvernement.

Bluetooth : La technologie Bluetooth vous permet de connecter vos appareils sans fil, mais elle ouvre également la porte aux cybercriminels (Gouvernement du Canada, 2021). De plus en plus de téléphones, ordinateurs portables et tablettes abandonnent les fils et encouragent l'utilisation de périphériques Bluetooth sans fil tels que les imprimantes, les écouteurs et les claviers. Cependant, l'utilisation du Bluetooth dans des lieux publics peut vous exposer à des risques de piratage. Pour vous protéger, désactivez le Bluetooth lorsque vous ne l'utilisez pas, évitez de vous connecter à des sources inconnues ou suspectes, et déconnecter immédiatement les appareils perdus ou volés de votre liste de périphériques Bluetooth. Pour en savoir plus, consultez le site du gouvernement.

Gestionnaire de mots de passe : Le gestionnaire de mot de passe est une manière simple de gérer vos mots de passe uniques pour différents comptes et appareils (Gouvernement du Canada, 2021). Ces outils vous aident à stocker en toute sécurité tous vos mots de passe et noms d'utilisateur pour divers sites Web, applications et appareils. Cependant, assurez-vous de choisir un gestionnaire de mots de passe avec des fonctionnalités de sécurité telles que l'authentification multifacteurs, les notifications pour les mots de passe faibles ou réutilisés, et l'intégration avec vos autres appareils. Gardez votre mot de passe principal en sécurité, activez l'authentification multifacteurs, et rappelez-vous de mémoriser vos mots de passe les plus sensibles, comme ceux de votre messagerie électronique et de votre banque. Pour en savoir plus, consultez le site du gouvernement.

Authentification à deux facteurs (2FA) : La validation en deux étapes, ou authentification à deux facteurs (2FA), ajoute une couche de sécurité supplémentaire à vos comptes et appareils en demandant une étape supplémentaire lors de la connexion (Gouvernement du Canada, 2021). Même si un pirate informatique obtient votre mot de passe, la 2FA peut empêcher leur accès. Utilisez-la autant que possible pour optimiser votre sécurité en ligne. Pour en savoir plus, consultez le site du gouvernement.

6.3.1 Prévention de la fraude

La fraude peut prendre plusieurs formes et toucher chacun d'entre nous. Pour mieux comprendre comment vous protéger et identifier les signes précurseurs, consultez ces ressources essentielles.

- **Prévention de la fraude** : Découvrez des conseils pratiques et des informations cruciales pour éviter les fraudes en tout genre. Cliquez ici pour en savoir plus.
- **Sécurité bancaire en ligne** : Apprenez comment vous protéger contre les fraudes bancaires en ligne et les cyberattaques. Cliquez ici pour en savoir plus.
- **Campagnes de prévention de la Sûreté du Québec** : Informez-vous sur les initiatives et conseils de prévention de la fraude. Cliquez ici pour en savoir plus.
- **Guide de formation sur la cybersécurité** : Accédez à un guide complet pour renforcer votre cybersécurité. Cliquez ici pour en savoir plus.

Que faire en cas de perte de carte de crédit ?

La perte d'une carte de crédit peut entraîner des risques de fraude. Voici quelques ressources pour savoir comment réagir rapidement.

- **Mesures immédiates à prendre** : Suivez ces étapes essentielles si vous perdez votre carte. Cliquez ici pour en savoir plus.

Et si vous avez déjà été victime de fraude ?

Si vous avez été victime de vol d'identité ou de fraude, ces ressources vous guideront sur les actions à entreprendre.

- **Assurance contre le vol d'identité** : Comprenez comment l'assurance habitation peut vous protéger. Cliquez ici pour en savoir plus.
- **Protection contre le vol d'identité avec l'ARC** : Informez-vous sur les mesures à prendre avec l'Agence du revenu du Canada. Cliquez ici pour en savoir plus.

Prévention sur les réseaux sociaux

Les réseaux sociaux sont un terrain fertile pour les fraudeurs. Protégez-vous grâce à ces conseils.

- **Bonnes pratiques en ligne** : Apprenez à sécuriser vos activités sur les réseaux sociaux. Cliquez ici pour en savoir plus.
- **Impact des réseaux sociaux sur la cybersécurité** : Découvrez les risques et comment les anticiper. Cliquez ici pour en savoir plus.

6.3.2 Détection de site sécurisé

La protection contre l'hameçonnage ainsi que d'autres formes de cyberattaques est essentielle pour maintenir une navigation sécurisée sur Internet. Heureusement, de nos jours, de nombreuses solutions sont disponibles pour aider à prévenir ces menaces.

Cependant, la sécurité en ligne ne repose pas uniquement sur les outils informatiques. Elle dépend également de la vigilance des utilisateurs. En effet, même avec les meilleures solutions de détection de site sécurisé, il est crucial que les utilisateurs restent attentifs aux signes de sites potentiellement dangereux. Cela inclut la vérification des URL, la prudence lors de l'ouverture de pièces jointes ou de liens provenant de sources inconnues ainsi que la mise à jour régulière des logiciels pour bénéficier des dernières protections contre les cybermenaces.

6.4 Sensibilisation et formation continue en cybersécurité

Rester à jour sur les avancées en cybersécurité est crucial dans un monde où les menaces évoluent constamment. L'AMF offre des ressources essentielles pour les professionnels et les entreprises qui cherchent à renforcer leurs connaissances et leurs défenses cybersécuritaires. Par exemple, l'AMF publie régulièrement des guides et des rapports sur les meilleures pratiques en cybersécurité dans un contexte financier. Elle organise également une multitude de formations et séminaires, permettant aux professionnels de rester à jour sur les avancées en cybersécurité.

Autre que les ressources offertes de l'AMF, assister à des conférences et des événements spécialisés en cybersécurité est un excellent moyen de se tenir au courant des dernières recherches et solutions. Également, de nombreuses institutions telles MIT et Stanford proposent des webinaires et des cours en ligne pour se former aux dernières techniques de défense contre les cyberattaques.

En tout, que ce soient des ressources fournies de l'AMF ou d'autres méthodes, se tenir informé sur la cybersécurité est fondamental. L'utilisation de ces ressources permet de renforcer la sécurité d'une organisation et donc de se prémunir efficacement contre les cybermenaces.

Voici des sites qui vous permettent d'en apprendre plus sur la cybersécurité :

- AMF
- Gouvernement du Canada – Cours pour les individus
- Gouvernement du Canada – Cours pour les petites et moyennes entreprises
- MIT Cybersécurité
- Stanford University – Cybersecurity Programs

7. CONCLUSION

En conclusion, la cybersécurité est devenue un élément indispensable de notre quotidien dans le monde digital actuel. À mesure que la connectivité devient omniprésente, la protection des données sensibles et des informations personnelles revêt une importance capitale, touchant à la fois les individus et les organisations à travers le monde. La sécurité en ligne ne se limite pas uniquement au domaine financier, mais s'étend également à d'autres aspects de nos vies, tels que les plateformes de divertissement en ligne, les réseaux sociaux et la réalisation de travaux en équipe. Dans chacun de ces domaines, la cybersécurité joue un rôle crucial pour prévenir les attaques malveillantes, garantir la confidentialité des données et protéger les utilisateurs contre les menaces en ligne.

La sensibilisation à la cybersécurité est essentielle pour les étudiants, qui doivent être préparés à naviguer dans un environnement numérique complexe et en constante évolution. En comprenant les risques en ligne et en adoptant des pratiques sécurisées, les étudiants peuvent protéger leurs données personnelles, sécuriser leurs finances et contribuer à la prévention des cyberattaques.

Il est donc impératif de rester informé des dernières menaces cybernétiques et des meilleures pratiques en matière de sécurité en ligne. En adoptant une approche proactive et en mettant en œuvre des mesures de sécurité appropriées, nous pouvons tous contribuer à créer un environnement numérique plus sûr et plus fiable pour tous.

Références

Global News WIre. (2023). *Les Canadiens se protègent contre la fraude et le vol d'identité selon un sondage d'Equifax Canada*. Récupéré sur https://www.globenewswire.com/news-release/2023/03/01/2617908/0/fr/Les-Canadiens-se-prot%C3%A8gent-contre-la-fraude-et-le-vol-d-identit%C3%A9-selon-un-sondage-d-Equifax-Canada.html

Gouvernement du Canada. (2019). *Fraude par carte de crédit*. Récupéré sur https://www.canada.ca/fr/agence-consommation-matiere-financiere/services/fraude-credit.html

Gouvernement du Canada. (2021). *Authentification multifactorielle*. Récupéré sur https://www.pensezcybersecurite.gc.ca/fr/securisez-vos-comptes/authentification-multifactorielle

Gouvernement du Canada. (2021). *Bluetooth*. Récupéré sur https://www.pensezcybersecurite.gc.ca/fr/securisez-vos-connexions/bluetooth

Gouvernement du Canada. (2021). *Coupe-feu*. Récupéré sur https://www.pensezcybersecurite.gc.ca/fr/securisez-vos-connexions/coupe-feu

Gouvernement du Canada. (2021). *Gestionnaires de mots de passe*. Récupéré sur https://www.pensezcybersecurite.gc.ca/fr/securisez-vos-comptes/gestionnaires-de-mots-de-passe

Gouvernement du Canada. (2022). *RPV*. Récupéré sur https://www.pensezcybersecurite.gc.ca/fr/securisez-vos-connexions/rpv

Gouvernement du Canada. (2023). *Projet de loi C-26 : Loi concernant la cybersécurité, modifiant la Loi sur les télécommunications et apportant des modifications corrélatives à d'autres lois*. Récupéré sur Gouvernement du Canada

Gouvernement du Canada. (2024). *Octobre est le Mois de la sensibilisation à la cybersécurité : voici comment l'Agence du revenu du Canada protège vos renseignements*. Récupéré sur https://www.canada.ca/fr/agence-revenu/nouvelles/salle-presse/conseils-fiscaux/conseils-fiscaux-2024/octobre-mois-sensibilisation-cybersecurite-comment-arc-protege-vos-renseignements.html

IBM. (2024). *Qu'est-ce que la cybersécurité ?* Récupéré sur https://www.ibm.com/fr-fr/topics/cybersecurity

INSEE. (2021). *Cyberdélinquance − Sécurité et société*. Récupéré sur https://www.insee.fr/fr/statistiques/5763599?sommaire=5763633

Le Monde. (2024). *En Corée du Sud, la jeunesse victime et bourreau des deepfakes pornographiques*. Récupéré sur https://www.lemonde.fr/pixels/article/2024/08/30/en-coree-du-sud-la-jeunesse-victime-et-bourreau-des-deepfakes-pornographiques_6299665_4408996.html

Montecuollo, L. (2022). *https://avasek.ca/fr/9-statistiques-sur-les-violations-de-donnees-que-votre-entreprise-doit-connaitre/*. Récupéré sur Avasek: https://avasek.ca/fr/9-statistiques-sur-les-violations-de-donnees-que-votre-entreprise-doit-connaitre/

Statistique Canada. (2023). *La fraude autodéclarée au Canada, 2019*. Récupéré sur https://www150.statcan.gc.ca/n1/pub/89-652-x/89-652-x2023001-fra.htm

TIME. (2020). *Here's How Shopping Scams on Facebook Are Ripping Off Thousands of Customers, With the Money Flowing Overseas*. Récupéré sur https://time.com/5921820/facebook-shopping-scams-holidays-covid-19/

Wikipédia. (2024). *Hameçonnage*. Récupéré sur https://fr.wikipedia.org/wiki/Hame%C3%A7onnage

Wikipédia. (2024). *Intelligence artificielle et élections*. Récupéré sur https://fr.wikipedia.org/wiki/Intelligence_artificielle_et_%C3%A9lections