CCN-CERT

BP/08

Meilleures pratiques en matière de Réseaux Sociaux

RAPPORT DE BONNES PRATIQUES

JUILLET **2021**

ccn-cert centro criptológico nacional

CCN centro criptológico nacional

Edition:

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA

CCN centro criptológico nacional

Date de sortie : julio de 2021

LIMITATION DE LA RESPONSABILITÉ

Ce document est fourni conformément aux conditions qu'il contient, rejetant expressément toute garantie implicite qui pourrait y être liée. En aucun cas, le Centre National de Cryptologie ne peut être tenu responsable des dommages directs, indirects, fortuits ou extraordinaires dérivés de l'utilisation des informations et du logiciel indiqués, même s'il a été averti de cette possibilité.

AVIS JURIDIQUE

Index

1. À propos du CCN-CERT

Le CCN-CERT est la capacité de réponse aux incidents de sécurité informatique du Centre national de cryptologie, CCN, rattaché au Centre national de renseignement, CNI. Ce service a été créé en 2006 en tant que **CERT gouvernemental national espagnol** et ses fonctions sont incluses dans la loi 11/2002 réglementant le CNI, le RD 421/2004 réglementant le CCN et dans le RD 3/2010, du 8 janvier, réglementant le schéma de sécurité nationale (ENS), modifié par le RD 951/2015 du 23 octobre.

Sa mission est donc de contribuer à l'amélioration de la cybersécurité espagnole, en étant le centre national d'alerte et de réponse qui coopère et aide à répondre rapidement et efficacement aux cyberattaques et à faire face activement aux cybermenaces, y compris la coordination au niveau public de l'État des différentes capacités de réponse aux incidents ou des centres opérationnels de cybersécurité existants.

F de la loi 11/2002) et des informations sensibles, défendre le patrimoine technologique de l'Espagne, former du personnel spécialisé, appliquer des politiques et des procédures de sécurité et utiliser et développer les technologies les plus appropriées à cette fin.

Conformément à ce règlement et à la loi 40/2015 sur le régime juridique du secteur public, le CCN-CERT est chargé de la gestion des cyber-incidents affectant tout organisme ou entreprise publique. Dans le cas des opérateurs critiques du secteur public, la gestion des cyber incidents sera assurée par le CCN-CERT en coordination avec le CNPIC.

CCN-CERT est la capacité de réponse aux incidents de sécurité de l'information du Centre national de cryptologie, CCN.

2. Introduction

2.1 Le cyberespace comme territoire habité

Les réseaux sociaux sont le lieu où se configure l'identité virtuelle. Il peut s'agir d'individus, de groupes, d'entreprises ou d'institutions. Il est composé de : un alias, une image personnelle et une déclaration biographique.

Le cyberespace est un domaine d'échanges sociaux qui connaît une croissance exponentielle chaque année et s'est imposé comme un territoire à part entière dans lequel les individus, les collectifs, les entreprises et les institutions exercent des activités.

Il s'agit d'un territoire essentiellement composé d'identités et d'objets connectés via l'internet. D'ici à 2020, on estime qu'il y aura 50 milliards d'objets connectés à l'internet des objets (IoT), interagissant avec les personnes grâce à leurs identités numériques.

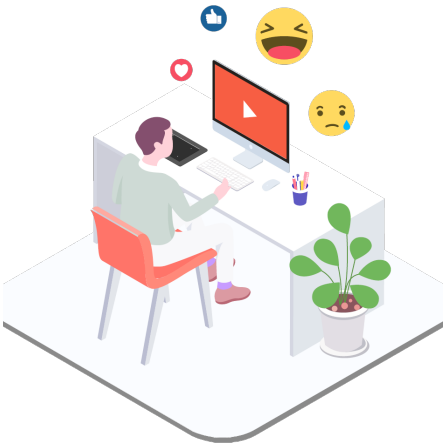
Toutefois, ce n'est pas seulement au niveau quantitatif que les êtres humains en sont venus à "habiter" le cyberespace, mais ce dernier est un territoire virtuel où les humains "vivent" : ils interagissent, communiquent, s'engagent dans des échanges sociaux, commerciaux, politiques ou religieux et, en somme, finissent par "être et être".

Au-delà de la présence générale sur le web, les réseaux sociaux sont le lieu où se configure l'identité virtuelle qu'une personne utilisera dans ses expériences, dans sa vie dans le cyberespace.

Cette identité numérique est composée d'un nom (un ou plusieurs pseudonymes) ; d'une image personnelle (type avatar), qui représente l'individu dans un ou plusieurs réseaux sociaux ; et d'une déclaration

biographique, basée sur une série de références personnelles ou professionnelles telles que la localisation géographique, les études ou le travail.

Plus important encore, à ces références est associé un volume important de contenu en texte, image, audio ou vidéo, où une personne montre son comportement, ses affinités, ses intérêts, bref, une trace plus ou moins détaillée de sa vie personnelle, sociale et, souvent, professionnelle.



2.2 Que sont les réseaux sociaux ?

Dès que se forment des groupes d'individus partageant des liens sociaux personnels ou des liens d'intérêt dans un domaine économique, religieux, politique, de loisirs ou autre, un réseau social est déjà configuré. Par conséquent, la relation sociale des êtres humains dans un réseau existe dès que les êtres humains communiquent et interagissent avec les autres.

Cependant, l'émergence des réseaux sociaux en tant que concept global et quotidien, associé à des millions d'êtres humains indépendamment de leur géographie de résidence ou de leur culture d'origine, est inhérente à l'émergence et à la croissance exponentielle des échanges sociaux à travers l'Internet, le web ou, finalement, le cyberespace.

On pourrait dire que les réseaux sociaux dans le cyberespace sont l'équivalent numérique ou virtuel de l'ensemble des relations personnelles, professionnelles ou sociales que les êtres humains entretiennent habituellement dans leur vie physique.

Dans les réseaux sociaux, dans le cyberespace, on maintient un agenda d'amis ou de connaissances, on converse avec eux et on partage des intérêts et des hobbies. Les réseaux sociaux finissent par être configurés pour partager des expériences numériques massives ; par exemple, il est possible d'assister virtuellement à un concert de musique ou de suivre un cours universitaire dispensé dans un autre pays que la résidence physique de l'utilisateur.

2.3 À quoi servent les personnes bien intentionnées qui utilisent les réseaux sociaux ?

La principale motivation pour rejoindre un réseau social, du moins ceux où il est nécessaire de créer un profil, est de rester en contact avec des amis et des connaissances ou d'accéder à un contenu qui intéresse l'utilisateur. En d'autres termes, la principale motivation des réseaux sociaux est l'interaction avec les autres membres de la communauté (famille, amitié, cercles professionnels, etc.).

Les réseaux sociaux, en tant qu'outil de communication de masse, permettent l'expansion des relations et la formation de l'identité. Après la création par Randy Conrads du site classmates.com en 1995 pour garder le contact avec ses anciens camarades de lycée, les réseaux sociaux ont connu une croissance rapide, aidés par le développement d'applications et de solutions de connectivité basées sur les appareils mobiles.

1. Source : "Informe de resultados Observatorio de Redes Sociales". L'analyse des cocktails. Quatrième vague, 2011. Avril 2012

2.3 À quoi servent les personnes bien intentionnées qui utilisent les réseaux sociaux ?

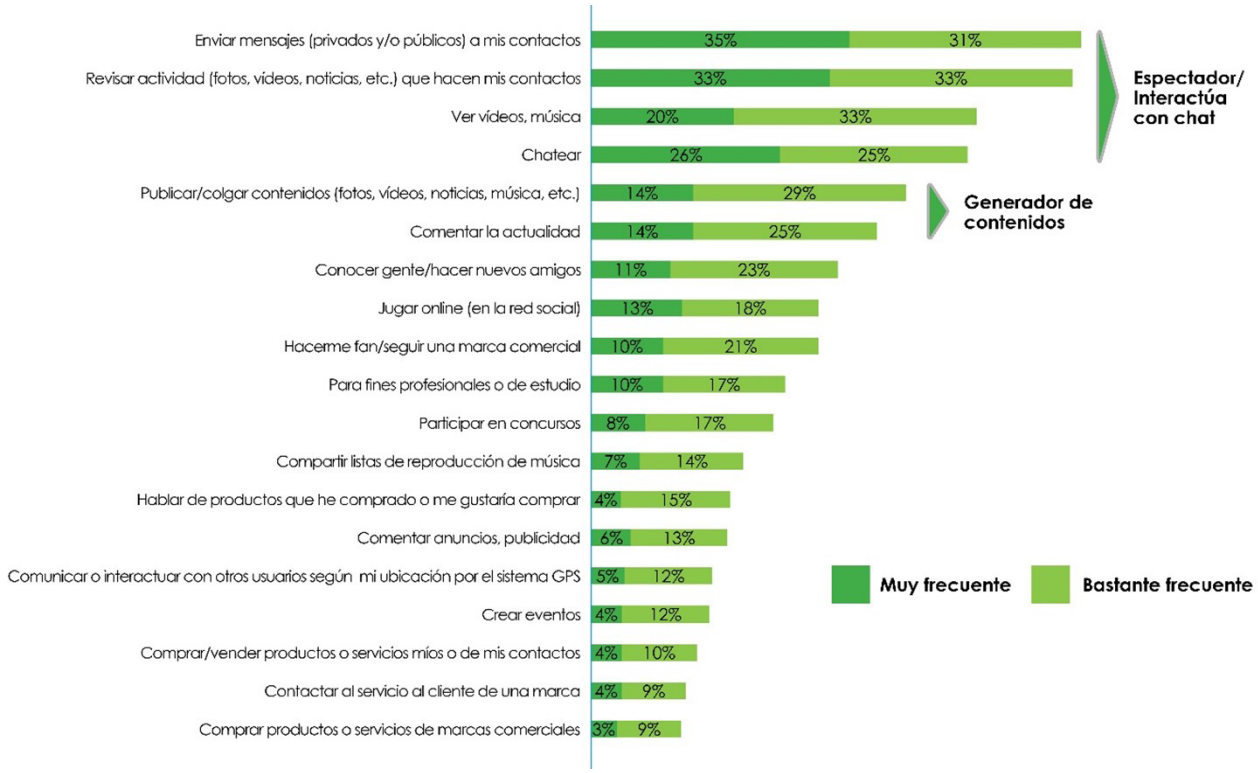


Figure 1.- Raisons de l'appartenance aux réseaux sociaux (étude iab Espagne)

2.4 À quoi servent les personnes malveillantes qui utilisent les réseaux sociaux ?

Les énormes possibilités offertes par les réseaux sociaux et leur utilisation massive entraînent une série de risques de différentes natures, tant dans la sphère privée et personnelle que dans la sphère professionnelle.

Compte tenu de la tendance croissante à utiliser ce type de réseaux comme moyen de développement de cyber-attaques, il est essentiel d'être protégé, de les utiliser correctement et d'utiliser un environnement sécurisé lors de leur utilisation.

En général, les acteurs qui utilisent les réseaux sociaux comme une passerelle pour mener des cyberattaques et compromettre la sécurité des utilisateurs exploitent trois (3) types de vulnérabilités implicites dans l'"architecture sociale" même des réseaux:

2.4 À quoi servent les personnes malveillantes qui utilisent les réseaux sociaux ?

La **surexposition d'informations personnelles.** La surabondance d'informations personnelles que les utilisateurs diffusent par l'intermédiaire de leurs profils sur les réseaux sociaux constitue une matière première attrayante pour les cybercriminels qui utilisent ces informations à des fins nuisibles.

Autoroutes de l'information. La fluidité et l'ouverture inhérentes à la communication font des réseaux sociaux d'authentiques autoroutes de l'information où circulent aussi bien des communications socialement inoffensives et légitimes que des contenus liés à divers types de codes malveillants. Ce malware n'est pas spécifique aux réseaux sociaux, mais il profite de la fluidité de la communication sur les réseaux sociaux pour se distribuer et propager son infection au plus grand nombre d'utilisateurs possible.

Utilisation massive. Avec un taux de pénétration de 42 % de la population mondiale (3 196 millions de personnes)[2], les réseaux sociaux sont le véhicule idéal pour accéder à un grand nombre de personnes, victimes potentielles d'une cyberattaque.

2. Global Digital Report 2018 (https://digitalreport.wearesocial.com)

2.4 À quoi servent les personnes malveillantes qui utilisent les réseaux sociaux ?

L'utilisation malveillante la plus courante des réseaux sociaux relève des catégories suivantes:

- **L'ingénierie sociale:** il s'agit de la conception de mécanismes ou de systèmes de tromperie, destinés à amener les utilisateurs à adopter certains comportements qui leur porteront préjudice, permettant ainsi aux cybercriminels d'obtenir un avantage illicite.

  L'ingénierie sociale utilise des modèles connus de comportement humain pour concevoir des processus comportementaux en ligne qui encouragent les utilisateurs à effectuer certaines actions, à accéder à certains contenus, à fournir des informations dans différents contextes ou à partager des données sensibles.

- **L'usurpation d'identité:** pour ce faire, ils profitent des informations personnelles diffusées par les utilisateurs sur les réseaux sociaux.

- **La cyberintimidation ou cyberbullying:** elle utilise la capacité d'une personne à harceler psychologiquement une autre, grâce aux informations obtenues de la victime par le biais de ses profils sur les réseaux sociaux, et est particulièrement grave lorsqu'elle concerne des mineurs et se produit dans le milieu scolaire . Certaines formes spécifiques de cyberintimidation sont:

  - Le **sexting**: il consiste à envoyer des photographies et des vidéos à contenu sexuel, filmées ou enregistrées par le protagoniste, sur internet, notamment via les *smartphones* (des applications comme WhatsApp facilitent cette pratique). Il s'agit d'une pratique de plus en plus courante chez les jeunes, qui peut conduire au harcèlement ou à l'extorsion si le destinataire des photos a des intentions malveillantes.

  - **Grooming**: méthode basée sur un ensemble de stratégies qu'un adulte développe pour gagner la confiance d'un mineur par le biais d'Internet, et ainsi gagner son contrôle émotionnel, dans le but ultime d'obtenir des concessions de nature sexuelle.

- **Atteinte à la réputation:** dans l'environnement personnel, social ou professionnel, découlant de contenus sur les réseaux sociaux susceptibles de nuire aux relations d'une personne dans ces domaines.

- **Publicité nuisible ou trompeuse:** diffusée et livrée par le biais des réseaux sociaux, souvent à des fins de fraude ou de diffusion de codes nuisibles.

3. https://www.anar.org/wp-content/uploads/2017/04/INFORME-II-ESTUDIO-CIBERBULLYING.pdf

2.4 À quoi servent les personnes malveillantes qui utilisent les réseaux sociaux ?

La **criminalité dans le monde physique:** utilise les informations obtenues sur les réseaux sociaux pour adopter un comportement criminel dans le monde physique, comme les vols de vacances, en profitant d'informations annoncées sur les réseaux sociaux, ou les enlèvements, dans le but d'obtenir une rançon en fonction du "niveau de vie" d'une personne observée dans ses réseaux sociaux.

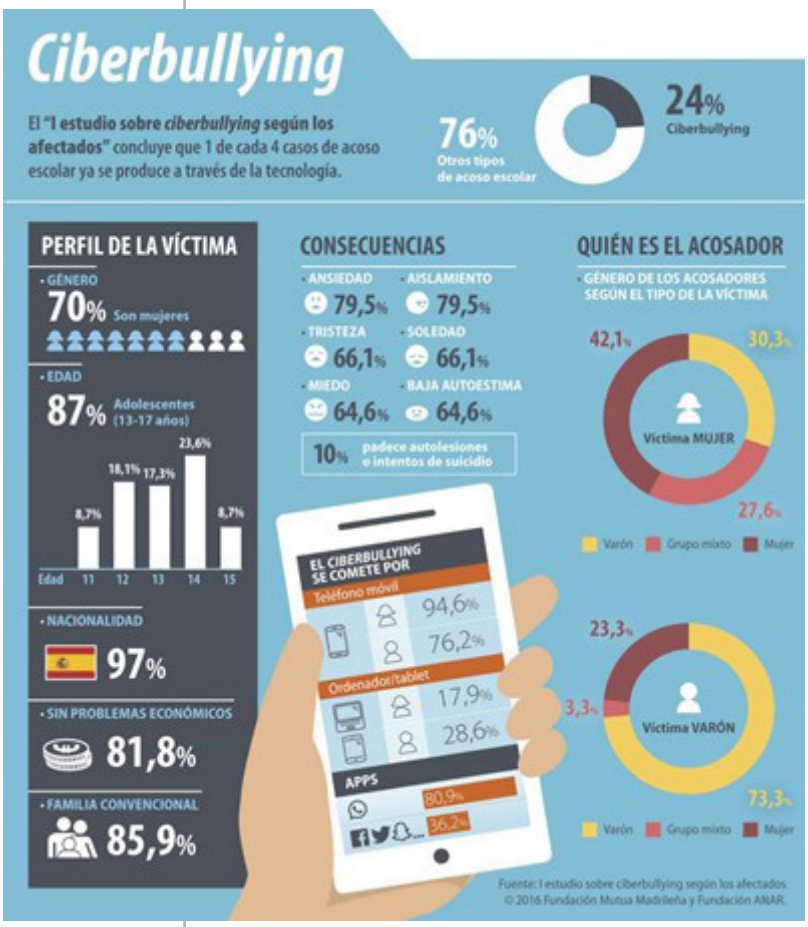


Figure 2 - Fondation de l'ANAR

Distribution de logiciels malveillants: pour ce faire, ils utilisent les autoroutes de l'information interpersonnelle représentées par les réseaux sociaux. Les groupes cybercriminels utilisent les réseaux sociaux comme simples canaux de distribution de toutes sortes de codes malveillants. Ils ne cherchent pas à exploiter les vulnérabilités de programmation ou de configuration des réseaux sociaux eux-mêmes, mais plutôt à se télécharger sur les appareils des utilisateurs (ordinateurs de bureau, téléphones mobiles, tablettes) et, une fois sur place, à agir en exploitant les vulnérabilités des applications et des logiciels installés sur cet appareil.

2.4 À quoi servent les personnes malveillantes qui utilisent les réseaux sociaux ?

Les méthodes les plus courantes de distribution de codes malveillants sur les réseaux sociaux sont les suivantes :

Phishing et Pharming. Le *phishing* est un type d'attaque dans lequel l'ingénierie sociale est utilisée pour obtenir des informations personnelles des utilisateurs, principalement l'accès à des services financiers. Pour atteindre le plus grand nombre de victimes possible et augmenter les chances de succès, ils utilisent le courrier indésirable ou "*spam*" pour se distribuer. Une fois que le courrier parvient au destinataire, il fournit des liens vers des sites web modifiés de banques et de sociétés financières, afin que des données personnelles telles que des numéros de compte bancaire, des mots de passe, des numéros de sécurité sociale, etc. puissent être saisies.

Le pharming consiste à rediriger les demandes de noms de domaine légitimes vers un site web faux ou frauduleux en exploitant le système DNS (détournement de DNS ou empoisonnement de DNS).

Des techniques de phishing sont également utilisées, en usurpant l'identité de pages d'accueil sur des plateformes de réseaux sociaux, pour collecter des informations et tenter d'accéder à d'autres services utilisés par la victime, car il est courant de partager le même nom d'utilisateur et le même mot de passe dans la plupart des services proposés sur Internet.

Liens malveillants. Ces types d'attaques apparaissent généralement sous la formule "message plus lien", le lien menant l'utilisateur au contenu malveillant. Dans le cas d'une attaque sur Facebook, par exemple, le mur de la victime est généralement utilisé, où est posté un message, une boîte de réception ou une photo dans laquelle l'utilisateur est tagué.
Dans le cas de Twitter, ce type d'attaque est réalisé par le biais d'une mention, d'un message privé ou de raccourcisseurs de liens, qui sont utilisés sur cette plateforme et sont exploités dans des campagnes de spam et de redirection.

Des vidéos prometteuses. L'une des "accroches" les plus courantes pour une attaque sur les médias sociaux, comme pour les e-mails, est la promesse d'une vidéo choquante, comme celle qui promettait de montrer la mort d'Oussama Ben Laden.

En cliquant sur ces vidéos, des informations sont affichées sur le profil du réseau social, publiant cette même vidéo ou une autre similaire, sans le consentement de la victime.

2.4 À quoi servent les personnes malveillantes qui utilisent les réseaux sociaux ?

Une étude de TrendMicro[4] suggère que les groupes cybercriminels préparent des arnaques (campagnes de phishing) sur des événements médiatiques entre deux (2) semaines avant et trois (3) heures après l'événement. En outre, jusqu'à 13% des utilisateurs ont été victimes d'une usurpation d'identité via les médias sociaux; 69 % des adultes et 88 % des adolescents sont exposés d'une manière ou d'une autre à l'intimidation ou à la cruauté sur les médias sociaux; et près de cinq (5) millions de personnes publient régulièrement des plans de voyage sur les médias sociaux.

Figure 3.- Informations partagées sur les réseaux sociaux (TrenMicro)

Sur l'internet, une grande partie des risques auxquels sont exposés les systèmes et leurs utilisateurs sont liés aux vulnérabilités des serveurs web, des systèmes de gestion de contenu, des configurations de bases de données ou des panneaux d'accès. Il est courant, par exemple, qu'une vulnérabilité dans la conception de la programmation d'un serveur web puisse être utilisée par un attaquant pour obtenir un accès illégitime à la base de données des utilisateurs de ce site web et voler toutes leurs données personnelles.

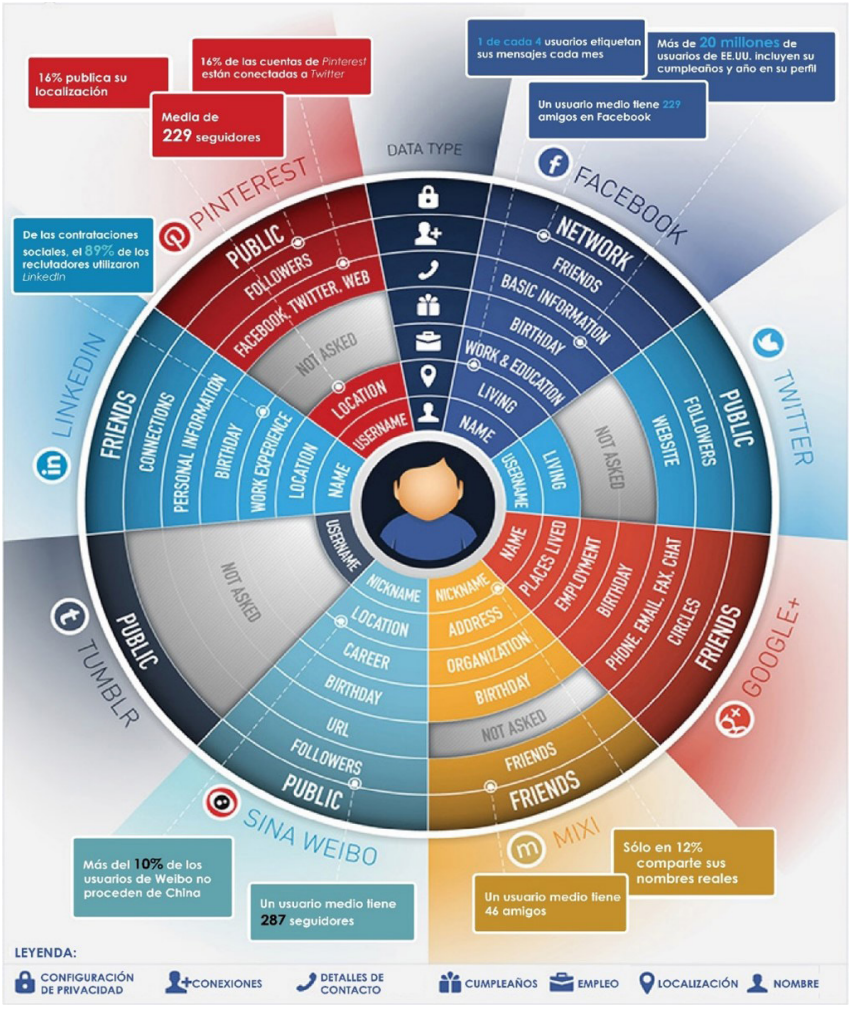
D'autre part, les **codes malveillants** peuvent être très variés dans leur conception et leurs fonctions (chevaux de Troie pour voler des informations personnelles, outils d'accès à distance pour prendre le contrôle des appareils, ransomware pour extorquer de l'argent, adware pour la fraude...), mais ils ont tous un élément commun, une sorte de code génétique que tous les malwares possèdent: ils seront conçus

4. http://blog.trendmicro.com/trendlabs-security-intelligence/the-risks-of-posting-in-social-networks/

2.4 À quoi servent les personnes malveillantes qui utilisent les réseaux sociaux ?

pour exploiter une ou plusieurs vulnérabilités, généralement dans les logiciels et, dans une moindre mesure, dans le matériel des appareils principalement connectés à un réseau, Internet étant le plus accessible.

Il existe une nette différence entre les vulnérabilités présentées par les réseaux sociaux et celles exposées par les appareils connectés à l'internet. Les réseaux sociaux constituent un canal privilégié, en raison de leur connectivité interpersonnelle, pour que les codes malveillants se propagent et infectent les appareils vulnérables des utilisateurs. En d'autres termes, la vulnérabilité que les créateurs de logiciels malveillants exploitent dans les réseaux sociaux est la *connectivité* même *intrinsèque* à la structure interpersonnelle du réseau.



Si les réseaux sociaux peuvent présenter des vulnérabilités liées à la programmation ou à la conception de leurs logiciels, qui permettent à un attaquant d'obtenir un accès illicite à des informations personnelles ou de compromettre la sécurité des utilisateurs, c'est rarement le cas.

2.4 À quoi servent les personnes malveillantes qui utilisent les réseaux sociaux ?

Parfois, une vulnérabilité dans un réseau social est rendue publique, qui permettrait à un attaquant, par exemple, d'accéder ou de modifier les informations privées des utilisateurs. Toutefois, ces vulnérabilités occasionnelles des réseaux sociaux ne constituent généralement pas leur talon d'Achille et n'attirent pas non plus l'attention des cybercriminels.

En général, les logiciels malveillants les plus répandus sont développés pour exploiter les vulnérabilités des logiciels des applications (programmes) ou des apps sur les appareils physiques des utilisateurs (téléphones, tablettes, etc.). Dans ce contexte, les réseaux sociaux sont principalement utilisés comme **vecteurs de diffusion et de transmission de codes malveillants dans** le but d'infecter les appareils des utilisateurs qui sont connectés à l'internet.

Dans cette utilisation malveillante des réseaux sociaux comme véhicules de propagation des menaces, les auteurs utilisent principalement deux (2) caractéristiques inhérentes aux réseaux sociaux: la surabondance d'informations personnelles et le grand volume de données. Dans les deux cas, le facteur clé est le comportement des utilisateurs dans les réseaux sociaux eux-mêmes, à travers leurs identités virtuelles et leur interaction avec d'autres utilisateurs.

3. Les meilleures pratiques en matière d'utilisation intelligente des réseaux sociaux

Le plus grand risque posé par les réseaux sociaux n'est pas lié à la façon dont leurs logiciels sont programmés, ni à la faiblesse ou à la force de leurs connexions cryptées avec les utilisateurs. Le plus grand risque des réseaux sociaux est principalement lié au comportement de leurs utilisateurs:

Extrêmement intelligent: l'utilisation intelligente des réseaux sociaux consiste à en tirer le meilleur parti pour interagir avec des amis et des contacts, partager des informations ou des intérêts, et exprimer des sentiments et des émotions dans le cyberespace ; mais, en même temps, il est nécessaire d'adopter des routines de protection qui ne sont pas très différentes, dans leur philosophie, de celles que toute personne adopterait dans l'espace physique.

En général, les gens ne laissent pas leur maison ouverte ou exposée aux intrus, ne racontent pas d'histoires intimes à des inconnus, ne laissent pas leur voiture ouverte dans la rue ou essaient de ne pas marcher isolés dans le noir dans une zone inconnue. Ces comportements, qui constituent une manière intelligente de prévenir les risques dans l'espace physique, ont également leur correspondance dans le cyberespace.

Extrêmement vulnérable: le comportement vulnérable implique une négligence et un manque de protection dans les informations personnelles et sensibles qui sont diffusées et partagées publiquement ; dans le pourcentage de vie privée qui est divulgué, accessible à la fois aux connaissances et aux étrangers ; et dans l'acceptation de contenus suspects qui peuvent conduire à différents types de logiciels malveillants.

En bref, un comportement vulnérable signifie que l'on s'aventure dans le cyberespace sans protection, comme si l'on marchait pieds nus sur un chemin plein de verre brisé.

Tout comme dans le monde analogique, vous ne devez pas partager des informations personnelles avec des inconnus dans le cyberespace. Vous devez également être très prudent quant aux données que des inconnus partagent avec vous.

L'utilisateur est le "*talon d'Achille*" car, même si les dispositifs logiciels et matériels peuvent être équipés des dernières mesures de cybersécurité, c'est finalement à l'utilisateur, à sa conscience de la sécurité et à sa propre protection de se protéger. **L'ingénierie sociale** vise à exploiter précisément cette faiblesse potentielle de la composante humaine dans les réseaux sociaux, plutôt que d'attaquer directement les logiciels ou le matériel pour violer la sécurité d'un système.

L'ingénierie sociale recourt à la tromperie et à la simulation pour présenter aux utilisateurs des scénarios qui ne sont pas vraiment ce qu'ils semblent être : des publicités sur les réseaux sociaux qui, lorsqu'on clique dessus, conduisent au téléchargement de logiciels malveillant; des publicités frauduleuses prétendant provenir de banques et conduisant à des formulaires conçus pour voler les informations d'identification des cartes de crédit ; ou des astuces publicitaires plus ou moins grossières pour abonner frauduleusement l'utilisateur à des services SMS surtaxés.

Figure 4.- Bonnes pratiques dans l'utilisation intelligente des réseaux sociaux

La réduction du risque dans les médias sociaux n'est pas sans rappeler la réduction du risque dans l'espace physique : le comportement des utilisateurs augmentera ou diminuera l'écosystème permettant aux menaces d'agir de manière malveillante. Les bonnes pratiques comportementales en matière de médias sociaux peuvent contribuer à réduire ou à annuler les intentions malveillantes.

Le comportement intelligent d'un utilisateur commence au moment où il définit sa propre identité dans le cyberespace, où il décide comment il veut se montrer, comment il veut être appelé, quel aspect il veut offrir ou quels intérêts il veut partager ; bref, où il décide qui il va être dans le cyberespace.

3.1 Étape 1 : Définition de l'identité dans le cyber-espace

3.1.1 Les constituants d'une identité virtuelle

L'identité dans les réseaux sociaux ne se compose pas seulement du nom ou du pseudonyme, du nom d'écran ou du nom d'utilisateur, qui est utilisé pour ouvrir un compte sur l'une des plateformes disponibles (Twitter, YouTube, Facebook, Instagram, Snapchat, WhatsApp, LinkedIn, etc.) L'identité est tout ce qui "identifie de manière stable" une personne, quelque chose comme les traits permanents qui font d'une personne ce qu'elle est (individualisation) et qui la distinguent des autres (différenciation) dans les réseaux sociaux.

En établissant un parallèle entre le cyberespace et l'espace analogique, l'identité analogique pourrait être composée d'un nom, éventuellement d'un surnom, d'un travail, d'études, d'un lieu de résidence et d'autres éléments qui sont pris comme référence sociale pour définir un individu de manière stable - sa famille, ses loisirs...-. Ces informations peuvent être transférées dans le domaine virtuel du cyberespace, où les utilisateurs des réseaux sociaux sont définis par le nom et le pseudonyme qu'ils adoptent, par l'image qu'ils placent comme profil, par la déclaration *biographique* qu'ils rédigent ou par les réseaux sociaux dans lesquels ils sont présents.

Il existe également d'autres paramètres, constitués par le contenu partagé à travers les profils qui définissent l'identité d'un individu dans les réseaux sociaux d'une manière plus dynamique, moins statique et, par conséquent, plus variable.

3.1.1 Les constituants d'une identité virtuelle

Contrairement à l'espace analogique, ce qui est défini dans les réseaux sociaux à propos d'un individu restera archivé dans les hyperliens de l'internet, dans la mémoire du cyberespace, probablement pour toujours.

Dans les réseaux sociaux, la personnalité d'un individu, c'est-à-dire **l'expression comportementale de son identité**, se traduit par le **contenu**, c'est-à-dire la manière dont la personne s'exprime à travers des messages qui communiquent des actions, des pensées ou des sentiments. Par conséquent, les contenus partagés communiquent les **traits de personnalité**, traduisent les essences de l'identité d'un individu en comportements par rapport aux autres personnes (**relations interpersonnelles**) et à l'environnement.

Contrairement à l'espace analogique, ce qui est défini sur les réseaux sociaux à propos d'un individu restera archivé dans les hyperliens de l'internet, dans la mémoire du cyberespace, probablement pour toujours. Même dans le cas des mineurs, on sait que 81% des bébés sont présents sur Internet par l'intermédiaire de leurs parents[5]. On l'appelle "*sharenting*", un anglicisme venant de *share* et *parenting*, qui désigne la pratique de plus en plus courante des parents qui partagent des photos, des vidéos et des informations sur leurs enfants sur les réseaux sociaux. Dans de nombreux cas, sans s'en rendre compte, des détails sur les enfants sont fournis qui favorisent l'usurpation d'identité ou ont un impact à terme sur l'honneur et la réputation de l'enfant.

En ce sens, une bonne pratique serait de se poser la question :

- **Quel est mon objectif social en créant un profil sur les réseaux sociaux ?**
- **Quelle image de moi-même est-ce que je veux montrer aux autres sur les réseaux sociaux pour atteindre le but que je vise ?**
- **Qui est-ce que je veux être ou comment est-ce que je veux que les autres me voient lorsqu'ils visitent mon profil sur les médias sociaux ?**
- **Le contenu que je télécharge sur mon profil peut-il me causer des problèmes maintenant ou à l'avenir ?**
- **Mon ami, mon collègue de travail ou le parent d'un autre enfant sera-t-il d'accord pour que je télécharge une photo ?**
- **Quand mes enfants seront plus grands, accepteront-ils que leur vie soit sur Internet dès leur plus jeune âge ?**

5. https://usolovedelatecnologia.com/sharenting/

3.1.2 Ce que je suis, ce que je semble être, ce que je pourrais être : les risques d'identité dans le cyberespace

Dans le monde analogique ou physique, l'identité individuelle est connue, dans une mesure plus ou moins grande, par soi-même et par les personnes avec lesquelles nous sommes le plus étroitement liés: famille, amis, collègues de travail, etc.

Dans le cyberespace, les profils personnels dans les réseaux sociaux sont basés sur des informations incomplètes et, surtout, sur l'absence de contact interpersonnel physique, et nos contacts peuvent avoir une impression erronée ou déformée de notre identité, davantage basée sur ce que **je semble être que sur ce que je suis vraiment**.

À de nombreuses reprises, **donner l'impression d'être quelque chose de différent** de ce que je suis est un effet qu'une personne recherche intentionnellement lorsqu'elle définit un profil sur les réseaux sociaux, en essayant peut-être d'offrir une image améliorée ou de mettre en avant un aspect spécifique à valoriser.

En d'autres occasions, les informations que l'on diffuse soi-même ou ses contacts font que l'on peut involontairement être une **autre identité différente de celle que l'on est ou de celle** que l'on veut volontairement paraître être, par manipulation ou utilisation illicite par des tiers.

Les informations descriptives d'une identité peuvent avoir une présence sur les réseaux sociaux qui n'est pas conforme aux souhaits de la personne. Les risques de ces **effets indésirables de la perte de contrôle d'une personne sur son identité dans le cyberespace** sont accrus dans les circonstances suivantes:

La quantité de données personnelles disponibles dans le cyberespace augmente le risque d'utilisation malveillante : plus les données sont disponibles, plus la probabilité d'une utilisation illicite à des fins malveillantes est grande.

3.1.2 Ce que je suis, ce que je semble être, ce que je pourrais être : les risques d'identité dans le cyberespace

Lorsque le **nom complet du sujet** (prénom et deux noms de famille) est publié sur un ou plusieurs profils sur les réseaux sociaux, plus le nom du sujet est statistiquement caractéristique, plus le potentiel d'utilisation illicite est élevé.

Tout d'abord, avec un nom comme "Epifanio Torreblanca Altaguardia", il est plus facile de trouver des informations supplémentaires sur un sujet sur Internet, ce qui n'est pas le cas si vous devez **chercher sur Google** "Juan Sánchez", où vous obtiendrez des milliers de résultats. Deuxièmement, lors d'une usurpation d'identité, un nom distinctif est plus utile qu'un nom commun, car le nom distinctif, s'il est accompagné d'informations de vérification supplémentaires, produit un effet psychologique de plus grande crédibilité.

Bien que cela puisse paraître contre-intuitif, il est plus intéressant de voler une identité très reconnaissable comme "Epifanio Torreblanca Altaguardia" que "Juan Sanchez".

Lorsque la **localisation exacte de l'adresse de la** personne est divulguée par les réseaux sociaux. Le nom et l'adresse d'un sujet sont deux caractéristiques principales de son identité administrative, qui, entre des mains malveillantes, peuvent constituer des informations très utiles pour la fraude par usurpation d'identité.

L'affichage d'un **numéro de carte d'identité ou de passeport,** associé au nom d'une personne, peut être utilisé pour la falsification d'identités en se faisant passer pour la personne qui a divulgué sa carte d'identité ou son passeport.

Lorsqu'un **numéro de compte bancaire ou de carte de crédit** est transmis ouvertement sur un réseau social. Les groupes cybercriminels ont conçu des procédures permettant de transférer immédiatement les numéros de cartes obtenus frauduleusement dans le cyberespace vers des cartes physiques.

Il est toujours conseillé de ne pas transmettre de numéros de comptes bancaires ou de cartes de crédit, car une fois que le message circule, il n'est plus sous contrôle, même si les réseaux sociaux comme Facebook ou Twitter, ou les systèmes de messagerie interne comme WhatsApp, ont leurs connexions cryptées.

Distribuer le **numéro de plaque d'immatriculation d'un véhicule** appartenant au sujet. Le numéro de la plaque d'immatriculation du véhicule, ainsi que le nom du sujet obtenu dans le cyberespace, pourraient être utilisés dans diverses procédures d'escroquerie. Parfois, en googlant un numéro de plaque d'immatriculation, on obtient l'adresse postale d'une

3.1.2 Ce que je suis, ce que je semble être, ce que je pourrais être : les risques d'identité dans le cyberespace

personne, ou du moins sa zone de résidence possible en raison d'une sanction administrative qui a été publiée.

- Diffusion de **l'adresse électronique ainsi que du** nom de la personne qui a attribué cette adresse. Sa diffusion incontrôlée peut faire en sorte que cette adresse soit utilisée comme source ou destination de spams ou de campagnes de phishing.

- Lorsque des amis ou des contacts d'une personne diffusent, sans intention malveillante, des **informations permettant d'identifier une autre personne** - telles que son adresse personnelle, le numéro d'immatriculation de sa voiture, son nom complet ou d'autres données sensibles. Cette diffusion peut se faire par le biais de textes, mais aussi d'images ou de balises. Par exemple, une personne qui n'a pas de profil sur les réseaux sociaux peut être étiquetée en son nom complet, par une autre qui en a un, dans une photo où les deux posent avec le véhicule de la première, laissant en vue la plaque d'immatriculation complète.

Les informations relatives à l'identité, qu'un utilisateur fournit dans les réseaux sociaux, peuvent créer des scénarios favorables à la perte de contrôle de celle-ci, étant exploitées par des individus ou des groupes aux intentions malveillantes pour usurper votre identité, la déformer ou lui donner une apparence différente de ce qu'elle est.

Afin de maximiser les possibilités de contrôle de ses propres informations dans le cyberespace, l'une des meilleures pratiques recommandées est de réfléchir avant de s'inscrire à un réseau social : pensez à ce que vous avez l'intention de faire de votre présence dans ce réseau social, à l'image que vous voulez donner et à la ou les parties de votre vie que vous avez l'intention de partager socialement, souvent avec des inconnus.

3.2 Étape 2: Réfléchissez avant de vous inscrire

3.2.1 Identité: Protéger notre image et notre réputation dans le cyberespace

La réputation numérique consiste à "googler" votre nom pour voir ce que les gens disent de vous sur l'internet ou dans les réseaux sociaux, les entreprises, les universités et autres groupes. Il est très difficile de supprimer ou de modifier un contenu sur les réseaux sociaux.

La réputation numérique, l'image positive ou négative dans le cyberespace, dépend très souvent du contenu que l'on (ou ses connaissances) place sur les réseaux sociaux. Et cette image, une fois constituée dans le cyberespace, est difficile à effacer ou à modifier car, comme on ne cesse de le répéter, lorsqu'un contenu entre sur Internet, il est très difficile de le faire disparaître de cet écosystème.

La réputation numérique, voire le profilage des traits de comportement ou de personnalité d'un sujet, sont des éléments qui sont de plus en plus pris en compte dans le cyberespace. Ce n'est pas seulement que pour se faire une idée d'une personne que nous venons de rencontrer dans le monde analogique, la première chose que nous faisons est de "googler" son nom pour voir ce qui se dit d'elle sur Internet ou ce qu'elle dit d'elle-même sur ses réseaux sociaux ; les entreprises, les universités et d'autres groupes ont de plus en plus recours à l'observation, voire à l'analyse professionnelle des réseaux sociaux comme élément de sélection ou d'acceptation.

Il ne faut pas oublier que ce sont les utilisateurs qui ont le premier contrôle sur les contenus divulgués dans les réseaux sociaux. Ainsi, en appliquant un minimum de réflexion sur ce que l'on fait avant de le faire, on peut éviter des conséquences indésirables sur l'identité publiée.

En règle générale, lorsqu'on fournit des informations d'identité de base lors de la création d'un profil sur les médias sociaux, il est conseillé de prendre en compte les aspects suivants:

3.2.1 Identité: Protéger notre image et notre réputation dans le cyberespace

Nom d'écran ou nom de profil. En ce qui concerne le nom d'écran, la première chose à laquelle un utilisateur doit penser est de savoir s'il va utiliser un alias numérique ou, au contraire, le même nom qu'il a dans le monde analogique. Si un alias est choisi, il faut tenir compte du fait qu'il sera lié à la personne et qu'il définira donc son identité numérique d'une certaine manière. Par conséquent, d'autres personnes pourront porter des jugements a priori, sans connaître la personne, en se basant uniquement sur le pseudonyme.

Si le nom de l'utilisateur est choisi, il est conseillé de ne pas fournir toutes les informations sur le nom, surtout si ce nom est très différenciant. Plus le nom complet d'une personne est distinctif, plus il sera facile pour les personnes mal intentionnées de se l'approprier. En général, il est conseillé d'utiliser le prénom et le premier nom de famille, sans exposer les seconds noms ou les noms de famille.

Il convient de noter que, même si un profil de réseau social est défini comme absolument privé par le sujet, au moins son nom d'écran, son nom d'utilisateur et son icône de profil seront entièrement publics.

Nom d'utilisateur. Il s'agit du nom court utilisé pour s'inscrire dans un réseau social. Il est généralement composé de caractères alphanumériques et ne peut coïncider avec celui d'un autre utilisateur enregistré.

Une bonne pratique pour éviter que notre nom d'utilisateur puisse être utilisé par des personnes ou des groupes ayant des intentions malveillantes est **d'éviter de le faire coïncider avec le nom d'utilisateur de notre adresse électronique habituelle.**

Bien qu'il soit courant pour une personne d'essayer de conserver le même nom d'utilisateur sur plusieurs réseaux sociaux - qui peut coïncider avec un alias comme s'il s'agissait d'un élément d'identification de cette personne dans le cyberespace - le fait de le faire en tant qu'utilisateur de notre adresse électronique habituelle permet à un individu ou à un groupe cybercriminel d'obtenir plus facilement notre adresse électronique.

Cette pratique est connue sous le nom de méthode de devinette et est courante dans les pratiques frauduleuses ou les cyberattaques, basées sur l'obtention massive d'adresses électroniques, comme le phishing ou la distribution massive de spam ou d'escroquerie.

Obtenir le nom de l'adresse électronique d'une personne est également une étape très utile pour usurper l'identité numérique d'une personne.

3.2.1 Identité: Protéger notre image et notre réputation dans le cyberespace

Figure 5.- Exemple d'un nom d'utilisateur déjà enregistré sur Twitter

Si une personne utilise l'utilisateur "poppy" dans ses comptes Skype, Facebook, Twitter et Instagram, même si elle n'a jamais communiqué publiquement son adresse électronique habituelle et la garde protégée dans sa vie privée, si cette adresse électronique est poppy@gmail, poppy@hotmail ou poppy@yahoo, un groupe ou un individu cybernétique malveillant la devinera en quelques secondes.

Icône ou image de profil. Il s'agit de la représentation visuelle de l'identité d'une personne sur les réseaux sociaux, secondairement accompagnée sur certaines plateformes de l'image dite "de couverture".

La meilleure pratique la plus évidente en matière de gestion des photos de profil sur les réseaux sociaux consiste à comprendre que les icônes de profil, tout comme les déclarations biographiques ou les pseudonymes que vous utilisez sur les réseaux sociaux, vont parler de vous dans le cyberespace.

Figure 6.- Exemple d'icône de profil et d'image de couverture dans Facebook

3.2.1 Identité: Protéger notre image et notre réputation dans le cyberespace

Par conséquent, la façon la plus intelligente d'utiliser les icônes de profil sur les réseaux sociaux, afin de protéger et de gérer votre réputation numérique, est de réfléchir très attentivement à ce que vous voulez transmettre à votre sujet par le biais d'images d'identification sur les réseaux sociaux.

La première chose à prendre en compte avant de placer une image représentative de manière stable dans les réseaux sociaux, comme l'icône de profil, est de penser qu'à partir du moment où elle est téléchargée, vous en aurez perdu le contrôle. Dans ce contexte, il est nécessaire de considérer que les images peuvent être téléchargées, manipulées et diffusées par d'autres personnes aux intentions inconnues.

Une recommandation générale supplémentaire consiste à ne pas placer comme icônes de profil des images à caractère administratif officiel, par exemple la photo de la carte d'identité nationale, du passeport ou d'une carte d'identification professionnelle, car ce type d'images facilite la tâche des personnes qui ont l'intention de falsifier des documents en usurpant notre identité.

Emplacement. La plupart des réseaux sociaux ont activé, au moment de l'enregistrement du profil, un champ permettant de localiser le lieu où se trouve le sujet. Dans ce cas, il ne s'agit pas de l'emplacement de l'utilisateur à un moment donné, mais de son emplacement habituel, par exemple, la ville où il vit, où il est né, la ville où il travaille ou à laquelle il se sent identifié pour une raison quelconque.

En outre, les réseaux sociaux tels que Facebook ou Instagram permettent d'ajouter individuellement une balise de localisation à chaque contenu diffusé par le profil.

La meilleure pratique la plus évidente pour les profils personnels sur les réseaux sociaux est de ne pas inclure d'adresses postales spécifiques comme lieu de résidence de l'utilisateur du profil. Les entreprises, les commerces ou les institutions ont généralement leur adresse postale localisée par une carte sur les réseaux sociaux, ce qui facilite leurs relations commerciales ou leurs contacts. En revanche, les profils personnels qui communiquent leur adresse postale sur les réseaux sociaux peuvent s'exposer à des risques et à des imprévus.

Une bande criminelle spécialisée dans la localisation et le vol de véhicules haut de gamme pourrait utiliser les informations obtenues sur les réseaux sociaux pour, avec un peu plus de recherche, localiser la position habituelle du véhicule et le voler. Il en va de même pour les lieux de résidence caractéristiques.

3.2.1 Identité: Protéger notre image et notre réputation dans le cyberespace

Notice biographique. Dans la plupart des réseaux sociaux, il est courant que dans la description générale du profil, un espace soit réservé à l'utilisateur pour qu'il puisse faire une déclaration, que la plupart des gens utilisent pour s'auto-décrire.

Il est assez courant d'indiquer la profession de l'utilisateur sur les réseaux sociaux destinés aux contacts personnels (comme Facebook ou Twitter), sans parler des réseaux sociaux spécifiquement conçus pour favoriser les contacts professionnels ou de travail, comme LinkedIn ou Viadeo.

Ce n'est pas parce qu'il s'agit d'une pratique courante qu'elle est dépourvue de risques, tant ceux liés au monde analogique et physique que ceux générés et développés dans le cyberespace. Outre les risques bien connus d'usurpation d'identité, qui sont d'autant plus faciles que les données spécifiques d'un sujet sont disponibles sur ses réseaux sociaux, il est possible que la déclaration de la profession d'un sujet dans les réseaux sociaux soit le vecteur d'attaque utilisé par un groupe cybercriminel pour en faire une cible pour la diffusion de logiciels malveillants.

Si un tel groupe sait quelles personnes occupent certains postes dans une entreprise et dispose de leur adresse électronique, les utilisateurs pourraient devenir la cible d'une opération de phishing ciblée visant à voler des informations sensibles de l'entreprise, à installer un outil logiciel pour infiltrer les systèmes d'information de l'entreprise, ou simplement à infecter le réseau de l'entreprise avec un code malveillant tel qu'un ransomware .

Numéro de téléphone ou adresse électronique. Bien que le téléphone et l'e-mail soient des coordonnées que l'utilisateur est obligé de fournir lorsqu'il crée un profil sur la plupart des réseaux sociaux, ces données restent privées, sans exposition publique, uniquement accessibles par le sujet et par l'entreprise à laquelle l'utilisateur les a attribuées dans les conditions de service que l'utilisateur accepte lors de son inscription.

Il est conseillé de **faire ce que presque personne ne fait :** lire les conditions de service de ce réseau social, où il sera établi si les données privées communiquées par l'utilisateur, lors de la création d'un profil sur le réseau, seront ou non partagées avec d'autres entreprises et dans quelles conditions.

Les organisations cybercriminelles fonctionnent en permanence avec des **traceurs** Internet **automatiques** (moissonneurs), dont le but est de détecter et de stocker les adresses électroniques et les numéros de téléphone dans des bases de données qui seront ensuite vendues au plus offrant sur le marché noir cybercriminel.

6. Un ransomware est un type de virus ou de logiciel malveillant dont le but est de bloquer l'accès d'un utilisateur à ses propres informations stockées sur un appareil, ordinateur, tablette ou téléphone, généralement en chiffrant ces informations et en exigeant une rançon financière de l'utilisateur pour les libérer.

3.2.2 Sécurité: Protection de l'accès à votre profil sur les réseaux sociaux

Le nom d'utilisateur, ou l'adresse électronique, et le mot de passe sont les identifiants de connexion de l'utilisateur à un réseau social. Plus précisément, le mot de passe est l'élément qui protège l'utilisateur contre les accès illégitimes et les tentatives d'accès à ses informations privées et à ses contacts sur le réseau social.

L'une des principales causes d'accès illégitime à des informations sensibles, qui devraient être protégées, est la **faiblesse des mots de passe** choisis par les utilisateurs pour protéger ces informations.

Parmi les mots de passe les plus courants pour accéder aux services web, y compris les réseaux sociaux, figurent "123456", "qwerty" ou le mot "password" lui-même. Ces mots de passe simples offrent une protection nulle contre un attaquant qui accéderait illégitimement à un service web, violant ainsi les droits de l'utilisateur.

Certains réseaux sociaux exigent que certains caractères alphanumériques soient saisis dans les mots de passe (combinaisons de majuscules et de minuscules, de chiffres et de lettres, ou caractères supplémentaires tels qu'un astérisque, un dièse ou un trait de soulignement), et la plupart d'entre eux informent par un code couleur (vert et rouge) de la force du mot de passe que l'utilisateur choisit pour créer un profil sur un réseau social.

Mais qu'est-ce qui est considéré comme un **mot de passe fort ou sûr** ? Dans l'idéal, les mots de passe forts sont ceux qui tendent à être générés de manière aléatoire, ce qui signifie que la probabilité qu'ils puissent être devinés ou prédits par quelqu'un qui ne les connaît pas est très faible. Un mot de passe fort sera long ; il combinera des chiffres, des lettres et des caractères spéciaux de manière à éviter tout schéma et aura l'inconvénient pour l'utilisateur d'être très difficile à mémoriser.

Les mots de passe les plus courants sont "123456", "qwerty" ou le mot "password" lui-même. Ces mots de passe simples offrent une protection nulle contre un attaquant qui accéderait illégitimement à un service web, violant ainsi les droits de l'utilisateur.

7. Par exemple, un rapport de janvier 2017: https://blog.keepersecurity.com/2017/01/13/most-common-passwords-of-2016-research-study/

3.2.2 Sécurité: Protection de l'accès à votre profil sur les réseaux sociaux

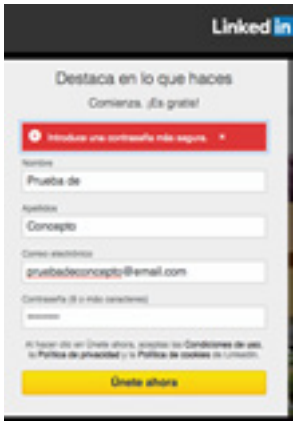


Figure 7.- Exemple de tentative d'inscription avec un mot de passe faible sur LinkedIn

En général, un mot de passe faible est prévisible car il suit un modèle (un ou plusieurs mots suivis ou non d'un chiffre, des séquences numériques, des dates significatives pour le sujet). Il arrive presque toujours qu'un mot de passe soit faible parce qu'il a été conçu pour être mémorisé par le sujet et non pour avoir une garantie minimale de solvabilité en termes de sécurité.

Les actions suivantes sont considérées comme de bonnes pratiques lors de l'accès à un profil personnel sur les réseaux sociaux:

1. **Adopter une conscience d'autoprotection personnelle.** L'entreprise est tenue de maintenir des normes de sécurité pour protéger le réseau, dans ses composantes matérielles, logicielles et humaines (ses propres employés), avec lequel elle fournit un service, mais elle va jusqu'à la limite où la protection de la sécurité de l'utilisateur incombe à l'utilisateur lui-même.

   Quel que soit le degré de sécurité d'un réseau dans le cyberespace, il sera aussi faible que son composant le moins sûr, généralement l'être humain. Si un réseau social fournit un cryptage, une authentification par mot de passe et prend soin de vérifier continuellement sa sécurité pour éviter d'avoir des failles exploitables par des attaquants, mais qu'un utilisateur laisse l'accès à son profil non protégé par un mot de passe faible, il sera facile pour un tiers non autorisé d'obtenir un accès illégitime à ce profil.

   Par conséquent, le premier facteur permettant à un utilisateur d'assurer la protection de ses propres profils sur les réseaux sociaux est qu'il soit conscient qu'il doit se préoccuper et prendre soin de sa propre sécurité en utilisant les mécanismes que le réseau met à sa disposition.

3.2.2 Sécurité: Protection de l'accès à votre profil sur les réseaux sociaux

2 **Utilisez des mots de passe pseudo-aléatoires.** En d'autres termes, composez des mots de passe à l'aide de chiffres, de lettres et de caractères spéciaux de manière à ce qu'ils ne suivent aucun modèle et soient suffisamment longs (six caractères ou plus ; plus un mot de passe est long, moins il a de chances d'être cassé). Par exemple, un mot de passe fort serait "89Jy$+_'1VwqÇ#", en mélangeant toutes sortes de caractères sans suivre aucun modèle.

De toute évidence, un tel mot de passe est difficile non seulement à retenir, mais aussi à taper en continu par l'utilisateur moyen. Il faudra donc adopter d'autres tactiques pour éviter d'avoir à se souvenir et à taper des mots de passe complexes qui sont sûrs, mais "rendent la vie impossible".

Un moyen est d'avoir écrit les mots de passe pour accéder aux différents réseaux sociaux dans un fichier texte, à son tour protégé par un mot de passe, stocké sur l'appareil à utiliser (ordinateur, téléphone, tablette), avec un accès également protégé par un mot de passe.

Une autre solution consiste à activer la fonction **"se souvenir du mot de passe"** dans le navigateur Web pour les accès authentifiés les plus courants. Cette option n'est raisonnablement sûre que si l'accès au dispositif est protégé par un mot de passe.

Un troisième moyen consiste à utiliser des "gestionnaires de mots de passe" qui sont des applications ou des programmes que nous installons sur nos appareils et qui sont chargés non seulement de stocker les mots de passe pour nos services de réseau, mais aussi de les générer avec des garanties de sécurité, et de s'intégrer aux navigateurs web pour nous authentifier dans nos services. Si le "gestionnaire de mots de passe" est un logiciel dont la sécurité est vérifiée et mise à jour par son fabricant et que nous avons accès au gestionnaire protégé par un mot de passe fort, ce sera une méthode raisonnablement sûre.

Ces trois (3) options de stockage de mots de passe obligeront l'utilisateur à mémoriser au moins un mot de passe difficile (**mot de passe principal**) : celui qui permet d'accéder à l'appareil, au fichier de mots de passe ou au gestionnaire de mots de passe.

3 **N'utilisez pas le même mot de passe pour plusieurs réseaux sociaux.** Ainsi, si le mot de passe de l'utilisateur pour accéder à un réseau est compromis, les autres réseaux resteront sécurisés (à moins que le mot de passe compromis ne soit le mot de passe principal).

4 **N'utilisez pas de mots de passe formatés en leet sur[8] des mots courants.** Le monde des pirates informatiques a commencé dès ses débuts à communiquer à l'aide de ce langage, et les dictionnaires de logiciels

8. Leet : remplacement des lettres par des chiffres ou des caractères spéciaux

pour les attaques par force brute peuvent donc incorporer des variations léonines de mots courants.

Si vous ajoutez des majuscules et des caractères spéciaux au début et à la fin, comme le dollar ou la barre oblique, vous disposez d'un mot de passe fort, facile à mémoriser par mnémotechnie en ayant une couleur et un chiffre favoris enchaînés en leet par un hash : "$R0j0#s13T3/".

5 **N'utilisez pas de mots de passe contenant des informations personnelles**, telles que des dates de naissance ou des anniversaires, des lieux importants, des surnoms ou des seconds prénoms. Un attaquant essaiera toutes les informations personnelles qu'il connaît sur un utilisateur s'il tente de deviner son mot de passe.

6 **Vous pouvez également utiliser l'authentification en deux étapes.** Les réseaux sociaux tels que Twitter, Facebook ou Google ont mis en place l'option de vérification en deux étapes pour que les utilisateurs puissent accéder à leur profil depuis leurs appareils.

En plus du mot de passe (première étape), il vous sera demandé de saisir un code numérique (deuxième étape) généralement envoyé par SMS au numéro de téléphone que l'utilisateur a enregistré dans son profil de réseau social. Dans tous les cas d'authentification en deux étapes, il sera essentiel que l'utilisateur ait enregistré son numéro de téléphone dans son profil de réseau social.

Figure 8 - Menu de configuration de l'authentification en deux étapes de Facebook

3.2.3 Vie privée: Ce qui est montré et ce qui est caché

Dans les réseaux sociaux, la confidentialité est le paramètre qui régit ce que l'utilisateur montre et cache publiquement dans les réseaux sociaux. La confidentialité est généralement associée, dans la plupart des réseaux sociaux, à deux types d'informations:

- Les informations descriptives propres au profil, par exemple l'adresse électronique de contact, le nombre et l'identité des amis et des contacts.
- Le contenu individuel que l'utilisateur divulgue par le biais de messages, d'images, d'audios, de likes ou de commentaires sur le réseau social.

Lors de la création d'un profil, chaque entreprise qui gère un réseau social présente à l'utilisateur des "conditions de service" sous la forme de plusieurs dizaines de pages que l'utilisateur est invité à "lire" avant de poursuivre et enfin à "accepter" s'il est d'accord avec ces conditions. Aucun utilisateur ne peut ouvrir un profil sur un réseau social sans accepter les conditions de service qui lui sont présentées par l'entreprise qui gère le réseau social.

Les conditions de service permettant à un utilisateur d'adhérer à un réseau social ont la nature d'un contrat juridiquement contraignant entre les parties (entre l'utilisateur et l'exploitant du réseau social, par exemple Facebook Inc. ou Twitter Inc.), et ce contrat régit la relation entre l'exploitant et l'utilisateur.

Toutes les entreprises qui gèrent les réseaux sociaux ont publié leurs conditions de confidentialité, c'est-à-dire la manière dont elles gèrent et traitent les données que les utilisateurs hébergent sur les serveurs web de ces entreprises lorsqu'ils créent un profil sur le réseau social[9]. Ces conditions de confidentialité établissent non seulement la manière dont les sociétés exploitant les réseaux sociaux partagent les informations fournies volontairement par les utilisateurs, mais aussi les données supplémentaires que les sociétés collectent automatiquement, après acceptation de l'utilisateur, sans que celui-ci en soit conscient.

9. Par exemple, Facebook [https://www.facebook.com/about/privacy/], Twitter [https://twitter.com/privacy?lang=es], Instagram [https://www.instagram.com/about/legal/privacy/?hl=es], Snapchat [https://www.snap.com/es/privacy/privacy-policy/]

3.2.3 Vie privée: Ce qui est montré et ce qui est caché

Figure 9 - Sociétés avec lesquelles Facebook affirme partager les données de ses utilisateurs

Par exemple, parmi les informations que Snapchat déclare recueillir auprès de ses utilisateurs, outre le contenu que chaque utilisateur divulgue et contribue dans son interaction quotidienne avec le réseau social, on trouve des métadonnées sur le contenu divulgué, des informations sur l'activité, des informations sur la localisation du sujet (si le sujet l'a activée), ou l'accès à l'appareil photo du sujet et aux photos stockées sur son appareil, sur demande d'autorisation de Snapchat.

Le contrat de service comprend aussi généralement des clauses dans lesquelles l'entreprise indique quelles autres entreprises l'utilisateur autorise à recevoir des données, non plus par lui-même, mais par l'entreprise exploitant le réseau social lui-même. Chacune des sociétés tierces avec lesquelles une société d'exploitation de réseau social déclare partager des données possède ses propres conditions de confidentialité et de prestation de services (on suppose que l'utilisateur a connaissance de ce scénario de partage des données lorsqu'il accepte de signer le contrat d'inscription à un réseau social).

En ce qui concerne la confidentialité des contenus divulgués par chaque utilisateur dans les réseaux sociaux, chaque réseau a établi les possibilités de protéger totalement ou individuellement les contenus afin qu'ils ne soient accessibles que par le sujet lui-même et ses contacts/amis.

Par exemple, Facebook permet de protéger avec un filtre de confidentialité chaque contenu individuel diffusé sur le réseau social, en cliquant sur une liste déroulante associée à chaque contenu individuel ; en revanche,

3.2.3 Vie privée: Ce qui est montré et ce qui est caché

Instagram ou Twitter permettent de définir la confidentialité dans le menu des paramètres de chaque profil en protégeant l'ensemble du contenu des messages envoyés par l'utilisateur, afin qu'ils ne soient visibles que par les followers du profil, mais ils n'ont pas la possibilité de définir chaque message individuellement comme privé.

Figure 10.- Menu déroulant sur chaque contenu individuel de Facebook pour votre confidentialité

Figure 11.- Option permettant de protéger tous les messages sur Twitter avec un filtre de confidentialité.

En ce qui concerne la confidentialité des informations descriptives du profil d'un utilisateur sur les réseaux sociaux, certains ont la possibilité de **configurer la visibilité du profil**. L'option permettant à d'autres personnes de localiser un profil, en effectuant une recherche par e-mail ou par numéro de téléphone, est généralement activée par défaut sur Facebook et Twitter dans le menu des paramètres du profil.

Figure 12 - Paramètres de visibilité du profil Facebook

3.2.3 Vie privée: Ce qui est montré et ce qui est caché

Une autre question pertinente que les utilisateurs de réseaux sociaux doivent prendre en compte lorsqu'ils **réfléchissent et agissent sur** la confidentialité de leur profil est la géolocalisation du profil et de son contenu.

Figure 13.- Configuration de la géolocalisation du contenu dans Twitter

Sur Snapchat, par exemple, l'option de géolocalisation par défaut n'est pas disponible pour le moment, mais il existe une fonctionnalité appelée "géofiltres", qui permet aux utilisateurs d'utiliser des balises graphiques de lieux pour montrer où (la ville) ils se trouvent ou à quel endroit le contenu partagé s'identifie.

Figure 14.- Exemples de géofiltres sur Snapchat

Le cryptage des messages et des contenus partagés sur le réseau social est une autre caractéristique que les réseaux sociaux ont intégrée ces derniers temps, en relation avec la vie privée des utilisateurs.

Cependant, le cryptage est une propriété qui n'empêche pas quiconque de pouvoir lire ou visualiser le contenu que nous partageons dans l'intention de le rendre public ; le cryptage n'est pas destiné à le faire dans le cas des réseaux sociaux. Le cryptage offre une protection pour éviter que, si un attaquant mal intentionné parvient à intercepter le

trafic de données entre l'appareil d'un utilisateur et son réseau social, le contenu de ces données interceptées ne soit pas révélé.

Certains réseaux sociaux de messagerie privée, comme WhatsApp, disposent par défaut d'un système de cryptage entre les utilisateurs, de sorte que la communication entre les utilisateurs est automatiquement cryptée. D'autres réseaux sociaux, tels que Facebook, offrent la possibilité de configurer, dans l'onglet sécurité, l'utilisation par l'utilisateur de sa propre clé de cryptage PGP pour ses communications avec d'autres utilisateurs.

Figure 15 - L'onglet Paramètres de cryptage dans les paramètres de Facebook

Un autre chapitre lié à la confidentialité des informations personnelles d'un utilisateur sur les réseaux sociaux concerne le partage du carnet de contacts que l'utilisateur possède sur l'appareil mobile avec lequel il se connecte à ce réseau social, ou la liste de contacts que l'utilisateur possède sur un autre réseau social.

Dans la plupart des cas, il est obligatoire d'autoriser le réseau social à accéder au carnet d'adresses du téléphone mobile si vous souhaitez installer *l'application* Android ou iOS et vous connecter à un réseau social. Dans certains cas, comme pour Facebook ou WhatsApp, les autorisations incluent même la possibilité pour l'application de "modifier" les contacts de l'utilisateur dans le carnet d'adresses du téléphone, par exemple en ajoutant certaines données dans un champ spécifique.

Figure 16 - Autorisations que les applications mobiles Snapchat, Facebook et WhatsApp demandent concernant les contacts.

Les contacts auxquels l'application d'un réseau social accède dans le carnet d'adresses ne sont pas insérés dans le profil du sujet, à moins que le sujet ne les "importe" et ne les ajoute, et ils ne sont pas non plus divulgués, à moins que le sujet n'effectue expressément cette action dans ses paramètres de confidentialité. Cependant, tous ces contacts font partie de la base de données des liens des utilisateurs maintenue par la société qui gère le réseau social, légitimement autorisée par les utilisateurs à travers les termes du contrat de service.

3.2.4 Risques pour la sécurité et la vie privée

La confidentialité et la sécurité d'un profil sur les réseaux sociaux régissent le contrôle du sujet sur les informations partagées et le canal par lequel elles le sont. Les risques potentiellement associés à la sécurité et à la vie privée seront ceux qui compromettent ou diminuent le niveau de contrôle que l'utilisateur a sur son canal (son profil) ou la visibilité de son contenu.

3.2.4 Risques pour la sécurité et la vie privée

La sécurité régit la capacité du sujet à empêcher d'autres utilisateurs d'accéder et, par conséquent, de contrôler les informations et le canal de communication lui-même (le profil sur le réseau social).

La protection de la vie privée intervient dans la régulation des contenus partagés par le sujet lui-même dans le réseau social qui sont montrés, sont visibles par d'autres personnes dans le cyberespace, qu'ils soient utilisateurs ou non (internautes généraux) du réseau social.

Parmi les menaces et les vulnérabilités, c'est-à-dire les risques, les plus directement associés aux problèmes de sécurité ou de respect de la vie privée dans les réseaux sociaux, on trouve:

- **Utilisez des mots de passe faibles ou des mots de passe basés sur des informations personnelles** connues de l'utilisateur, comme son anniversaire, le nom de son animal de compagnie, son groupe de musique ou son film préféré.

- **Partager les mots de passe avec d'autres personnes,** même si elles sont de confiance. Par définition, le partage d'un secret augmente la probabilité que ce secret soit révélé, car il augmente les sources par lesquelles il peut être divulgué.

- **Manque de sensibilisation à l'identité dans le cyberespace**. Lorsqu'un sujet possède plusieurs profils sur différents réseaux sociaux, les caractéristiques de son identité dans le cyberespace ne sont pas fonction de chacun des profils isolés, mais de l'ensemble des profils. Autrement dit, un utilisateur peut éviter de déclarer sa localisation ou sa profession sur son profil Facebook, mais le faire sur son compte Twitter ou Instagram.

  Il convient donc d'être conscient que toutes les informations sur soi diffusées par n'importe quel média sur Internet seront une pièce pour composer le puzzle dans lequel le visage de soi apparaîtra finalement. Un individu ayant l'intention de "résoudre le puzzle" n'aura qu'à rassembler pièce par pièce jusqu'à ce qu'il puisse composer une image plus ou moins claire de l'utilisateur.

- **Des images qui exposent des informations non désirées.** Par exemple, il est courant de prendre des portraits personnels ou des selfies dans lesquels un sujet apparaît sur le fond de son bureau, de son domicile ou de tout autre lieu personnel. Parfois, l'arrière-plan de ces images, qui n'est pas le centre d'intérêt de la photographie à partager, révèle des informations d'identification sur le sujet ou son entreprise que l'utilisateur lui-même ne souhaite peut-être pas divulguer.

Dans ces cas, il est recommandé de revoir les contenus identifiants (nom de notre société, plaque d'immatriculation de notre véhicule ou du véhicule d'un ami ou d'un parent) que l'utilisateur a l'intention de garder protégés pour des raisons de confidentialité.

Le marquage des tiers. La vie privée des personnes peut être violée, même celles qui n'ont pas de profil sur les réseaux sociaux, en marquant leur nom sur des photographies ou des images.

En d'autres termes, grâce au marquage, une personne qui n'est pas présente volontairement sur les réseaux sociaux peut finir par l'être involontairement, en exposant sa vie privée, son nom, son visage, ses contacts et ses amis. Pour prévenir ces risques, il est recommandé d'être prudent avec le marquage des personnes sur les photographies, en demandant le consentement préalable de cette personne avant de marquer son nom sur une image qui va être diffusée sur les réseaux sociaux.

Révéler les trajectoires géographiques. La géolocalisation du contenu, ou géopositionnement, pourrait permettre de connaître un pourcentage significatif de trajectoires géographiques et, par conséquent, d'effectuer un contrôle des itinéraires (carte des temps et des lieux) d'un utilisateur dans les réseaux sociaux, qui pourrait être utilisé de manière malveillante.

Il est recommandé de désactiver par défaut les géolocalisations des profils et des contenus dans les réseaux sociaux, en les activant individuellement et uniquement pour des contenus spécifiques.

Configuration inadéquate du profil lors de l'inscription sur le réseau social, dans la mesure où le niveau de confidentialité offert par la plateforme elle-même n'est pas correctement configuré. Il est conseillé, en effet, de ne pas choisir les options par défaut mais d'analyser attentivement chacun des paramètres proposés pour afficher certains contenus.

Obtenir des données personnelles avec une intention malveillante. Plus la quantité d'informations d'identification publiées est importante, plus la probabilité est grande que ces données soient utilisées pour, par exemple, tenter de répondre à des questions de sécurité et s'authentifier de manière illégitime afin d'accéder au profil.

Vol d'identité. Si l'on considère que pour s'inscrire dans un réseau social, il suffit d'avoir un compte de courrier électronique, n'importe qui peut s'inscrire sous son vrai nom ou celui d'une autre personne.

De même, si notre téléphone portable est perdu ou volé et qu'il n'est pas protégé, toute personne qui y a accès peut se faire passer pour nous sur nos réseaux sociaux (notamment ceux dans lesquels nous n'avons pas à

nous authentifier, comme WhatsApp). Il est donc nécessaire d'utiliser le verrouillage du terminal et, si nous détectons que quelqu'un a usurpé notre identité, de le signaler.

3.3 Étape 3: Réfléchir avant d'écrire

La nature et l'objectif des réseaux sociaux ne consistent pas simplement à créer un profil avec des données d'identification à la manière d'un annuaire téléphonique moderne. Le principe fondateur d'un réseau social est de créer un réseau en partageant du contenu.

Le contenu partagé est ce qui donne sa nature à un réseau social et ce qui façonne ses caractéristiques. Certains réseaux sont plus axés sur la diffusion de contenus multimédias, comme Instagram ; d'autres sont polyvalents, comme Facebook ; d'autres sont plus axés sur le message rapide et bref, comme Twitter ; et d'autres encore sur la composition d'un curriculum vitae professionnel, qui nous permet d'établir des relations à caractère essentiellement professionnel, comme LinkedIn. Ces différentes orientations sont déterminées par le contenu que les utilisateurs partagent via un réseau social.

La pertinence des contenus partagés sur les réseaux sociaux réside essentiellement dans le fait qu'ils définissent et caractérisent l'utilisateur qui les partage personnellement et professionnellement. Dans une telle mesure, le contenu partagé et les utilisateurs qui le partagent peuvent être considérés comme s'identifiant mutuellement, puisque le public mondial qui habite le cyberespace se tourne généralement vers le profil de réseau social d'une personne pour se faire une première impression de cette personne, en regardant comment elle s'est décrite dans les identifiants personnels, mais surtout en observant quel type de contenu elle partage.

C'est pourquoi, précisément en raison de sa pertinence, comme cela a été suggéré pour la description des identifiants personnels lors de

La pertinence des contenus partagés sur les réseaux sociaux réside dans le fait qu'ils définissent et caractérisent l'utilisateur qui les partage sur le plan personnel et professionnel. Nous devrons réfléchir avant d'écrire un contenu qui peut être préjudiciable via les réseaux sociaux.

la création d'un compte sur un réseau social, il convient de développer un instinct minimal de cyberconservation, une culture minimale de réflexion avant de rédiger un contenu à diffuser sur les réseaux sociaux.

3.3.1 Partage de contenu: Ce qui est partagé sur le réseau

La meilleure pratique qu'un utilisateur puisse adopter lorsqu'il s'agit de diffuser du contenu sur les médias sociaux est de réaliser qu'une fois le contenu transmis, l'utilisateur a déjà perdu le contrôle de ce contenu.

Indépendamment de la façon dont l'utilisateur a défini la confidentialité de son profil sur un réseau social, il doit être conscient qu'une fois le contenu transmis, en général, il aura donné à l'entreprise qui gère ce réseau social des droits d'utilisation importants de ce contenu.

Un élément général de confusion concernant les droits juridiques sur le contenu transmis par un utilisateur sur un réseau social découle de la distinction (ou de l'absence de distinction en termes de perception par l'utilisateur) entre la propriété du contenu et l'utilisation de ce même contenu:

- La **propriété intellectuelle du contenu** diffusé par un réseau social est détenue par l'utilisateur qui le partage, à moins que ce contenu ne soit affecté par des droits de propriété intellectuelle antérieurs : par exemple, l'utilisateur partage un contenu dont la propriété intellectuelle est déjà légitimement attribuée à un tiers.
- Le **droit d'utiliser le contenu** dont un utilisateur est le propriétaire légal peut être cédé avec des droits d'utilisation étendus pour la partie à laquelle les droits sont cédés.

En substance, quel que soit le degré de propriété d'un utilisateur sur un contenu, la signature d'un contrat juridiquement contraignant avec une société qui gère un réseau social implique nécessairement le transfert des droits d'utilisation du contenu dont l'utilisateur est propriétaire.

3.3.1 Partage de contenu: Ce qui est partagé sur le réseau

L'utilisateur reste le propriétaire, mais l'entreprise qui gère le réseau social en est l'usufruitier, utilisant le contenu avec une large marge de manœuvre, légalement et légitimement accordée par l'utilisateur.

Fondamentalement, l'enregistrement d'un profil sur un réseau social signifie qu'un individu accorde à une entreprise, en vertu d'un contrat juridiquement contraignant entre les parties, une licence de transfert de droits pour un large éventail de comportements pour l'utilisation du contenu et des informations personnelles de l'utilisateur. Dans ce contexte, l'utilisateur peut être propriétaire du contenu, mais n'a plus le contrôle de sa diffusion.

En ce qui concerne la cession des droits d'utilisation des contenus hébergés sur un réseau social, cette cession à la société qui gère le réseau social s'effectue dans le cadre d'un contrat dont la clause doit être remplie par les deux parties.

Cependant, lorsqu'un contenu est diffusé par un réseau social définissant sa confidentialité comme publique (c'est-à-dire visible par tous les utilisateurs de ce réseau social et, dans la plupart des cas, par tout habitant du cyberespace), **l'utilisateur cède implicitement le contrôle de la circulation et de la diffusion de ce contenu à tout habitant du cyberespace.**

Il est vrai que lorsque les utilisateurs s'inscrivent sur un réseau social, ils s'engagent, par le contrat que représentent les conditions de service signées, à "respecter les règles du jeu" et, par conséquent, à être respectueux des droits de diffusion limités sur les contenus des autres utilisateurs.

Même si un utilisateur a marqué un contenu comme devant être diffusé de manière privée parmi ses contacts, suiveurs ou amis, une fois que ce contenu est diffusé, il fait déjà partie des informations accessibles à d'autres personnes, principalement la liste privée des contacts, suiveurs ou amis de la personne qui a diffusé le contenu.

Ainsi, chacun d'entre eux peut refondre en public un contenu initialement marqué comme privé par son diffuseur d'origine, ce qui donne lieu à une "déprivatisation" de la vie privée d'origine. Dans les réseaux sociaux, la confidentialité du contenu n'est pas un paramètre absolu qui est fixé lorsqu'une personne définit un contenu comme privé, mais la c**onfidentialité du contenu est un paramètre relatif et interactif**, qui dépend du fait que les autres utilisateurs, qui reçoivent un contenu privé, continuent à le garder privé.

Par conséquent, **avant de diffuser du** contenu par le biais d'un profil de médias sociaux, vous devez vous poser les questions suivantes :

3.3.1 Partage de contenu: Ce qui est partagé sur le réseau

Est-ce que je révèle des informations personnelles que je voudrais garder privées, uniquement parmi ma famille et mes amis? Si la réponse à cette question est oui, il est préférable de ne pas diffuser le contenu sur les réseaux sociaux car, même s'il est marqué comme privé, il peut être redistribué volontairement ou involontairement par un contact qui a accédé à ce contenu.

En ce sens, il convient de garder à l'esprit qu'il existe des informations personnelles, qui pourraient mettre en danger l'utilisateur ou ses proches, car en les révélant publiquement, elles pourraient être utilisées de manière malveillante par des individus ou des groupes cybercriminels à des fins d'usurpation d'identité ou d'ingénierie sociale, entre autres.

Quelqu'un qui verrait ce contenu penserait-il qu'il représente mon opinion ou ma façon d'être, de penser ou de me comporter? Si la réponse à la question est oui, vous devez vous demander si le contenu représente l'utilisateur et ce qu'il dira de lui, non seulement sur le plan personnel, mais aussi sur le lieu de travail. Et pas seulement maintenant, mais aussi à l'avenir, car quelqu'un pourrait se faire une opinion sur la base du contenu des réseaux sociaux, et peut-être que cette opinion compte.

Y a-t-il un risque que je regrette d'avoir publié le contenu et que je veuille le supprimer immédiatement après l'avoir publié parce qu'il est offensant ou inapproprié? Si la réponse à cette question est oui, il est préférable de ne pas envoyer le contenu. Une fois qu'il a été diffusé sur un réseau social, il peut s'écouler quelques secondes avant que le contenu n'apparaisse sur le profil d'un contact, qui met une seconde de plus pour le renvoyer, de sorte qu'au moment où vous voulez le supprimer, le contenu a atteint la vitesse de la lumière dans le cyberespace et ne peut plus être supprimé.

Le contenu que je m'apprête à publier contient-il une image de moi ou de mes proches qui, par une simple manipulation, pourrait se transformer d'une image inoffensive en une image offensante ou inappropriée? Si la réponse à cette question est oui, il vaut mieux ne pas la diffuser, car elle pourrait se retrouver dans un forum d'échange indésirable, après avoir été soumise à de légères retouches avec un programme d'édition d'images.

Ceci est particulièrement sensible dans le cas des mineurs, dont la diffusion d'images sur les réseaux sociaux doit toujours être supervisée par des adultes ayant la responsabilité du mineur.

Le contenu que je vais diffuser contient-il des images d'autres personnes qui n'ont pas de profil sur les réseaux sociaux ou dont le profil est entièrement protégé par la confidentialité? Parmi les amis proches, il peut y avoir des personnes qui, pour des raisons légitimes de mode de pensée ou de compréhension de la vie, n'ont pas de profil sur les réseaux sociaux, mais

apparaissent sur des photos représentant des moments familiaux, sociaux ou professionnels. Il se peut également que ces personnes occupent des positions sociales ou professionnelles dans lesquelles un certain contrôle de leur image publique est approprié.

Dans ce cas, avant de diffuser une image qui met en jeu la vie privée protégée d'autrui, il est conseillé de les consulter pour savoir s'il faut ou non diffuser le contenu.

Si je redirige mes contacts vers le contenu de quelqu'un d'autre que je viens de recevoir, vais-je contribuer à la diffusion d'un contenu offensant, inapproprié ou nuisible, voire d'un contenu illégal? L'ingénierie sociale est un procédé par lequel ils tentent de camoufler un contenu nuisible par un contenu apparemment inoffensif, voire attrayant ou nécessaire pour les utilisateurs (notes informatives, factures, vidéos choquantes...).

Le succès de la diffusion de ces contenus nuisibles ou inappropriés réside essentiellement dans la chaîne de rediffusion. C'est-à-dire qu'un utilisateur qui le reçoit le transmet à nouveau. Par conséquent, lorsque vous recevez du contenu d'autres contacts, qu'ils soient connus ou non, il est conseillé de réfléchir un instant et d'analyser le contenu de manière minimale.

Suis-je sûr de pouvoir utiliser le contenu que je vais diffuser via mon profil? Certains contenus diffusés contiennent des images ou des documents de marque protégés par des droits. Parfois, la différence entre le contenu qui est protégé et celui qui ne l'est pas est subtile.

Par exemple, la diffusion d'un selfie pris par un utilisateur montrant le logo du bâtiment d'une entreprise en arrière-plan ne serait pas, en principe et à moins que d'autres circonstances ne se présentent, limitée par des droits, ou du moins il est douteux que l'entreprise revendique ces droits. Toutefois, l'utilisation du logo d'une entreprise ou de l'identité d'une personne ayant une image publique sans le consentement d'un tiers pour diffuser un produit que l'on souhaite promouvoir par le biais des réseaux sociaux pourrait entraîner une revendication du droit à l'image par l'entreprise ou la personne publique dont l'image est utilisée.

Suis-je sûr de vouloir que le contenu que je vais diffuser soit à jamais sur Google et que n'importe qui puisse le trouver avec une recherche? Face à cette question, nous devons penser de manière préventive que tout contenu que nous diffusons sera à jamais dans le cyberespace. Dès que nous diffusons un contenu par le biais d'un réseau social, que ce soit publiquement ou en privé, nous avons perdu le contrôle du contenu et, par conséquent, ce contenu peut se retrouver indexé dans Google, pour toujours.

3.3.2 Utilisations malveillantes ou involontaires du contenu divulgué

Tant le contenu diffusé que celui reçu peuvent faire l'objet d'utilisations non désirées ou malveillantes:

Il y a **utilisation non désirée** lorsqu'une autre identité dans le cyberespace utilise un contenu pour le diffuser à des personnes qui ne sont pas intéressées, fait circuler un contenu à une fréquence élevée ("no message flooding"), transmet un contenu jugé inapproprié ou utilise le contenu de l'utilisateur pour un usage qui n'est pas souhaitable pour l'utilisateur, pour quelque raison que ce soit.

Dans ce cas, l'expéditeur du contenu ne se livre pas à une activité qui implique une intention malveillante ou une volonté de nuire, mais finit par être gênant ou inapproprié par son comportement sur les réseaux sociaux.

L'utilisation malveillante implique l'utilisation de tout type de contenu divulgué sur les réseaux sociaux pour obtenir un bénéfice illicite et/ou illégal, généralement au détriment de tiers, ou pour produire directement un préjudice à ces tiers.

Des exemples d'utilisation malveillante sont la transmission de virus informatiques (codes malveillants) via les réseaux sociaux ou l'utilisation de contenus frauduleux dans le but de tromper l'utilisateur pour qu'il s'abonne à des services payants.

L'un des premiers domaines d'utilisation indésirable que des identités tierces pourraient faire du contenu que nous transmettons via les réseaux sociaux est encadré par **la réputation virtuelle.** Le contenu que nous transmettons sur les réseaux sociaux, en quelque sorte, définit les utilisateurs, dit quelque chose sur lui, ses goûts, ses pensées, ses idéologies et son comportement.

Cependant, il est moins intuitif de voir l'utilisation que des tiers intéressés pourraient faire du contenu diffusé dans les réseaux sociaux pour **élaborer des profils psychologiques ou comportementaux** d'un utilisateur, profils qui seront ensuite utilisés à des fins d'emploi ou pour prédire et influencer leur comportement.

3.3.2 Utilisations malveillantes ou involontaires du contenu divulgué

Une autre utilisation non désirée des contenus diffusés sur les réseaux sociaux, qui en plus d'être non désirée peut impliquer une utilisation malveillante de ces contenus par d'autres identités, est **l'utilisation des contenus intimes d'un utilisateur pour porter atteinte à son image ou pour en faire une victime de cyberchantage.** Le sexting est l'échange d'images érotiques qu'un utilisateur effectue, initialement, dans l'intimité de la communication avec un autre par le biais des réseaux sociaux -généralement, par le biais d'applications telles que Messenger sur Facebook, les messages directs sur Instagram ou Twitter, ou par WhatsApp-.

La procédure la plus couramment utilisée pour diffuser du contenu malveillant via les réseaux sociaux est **l'ingénierie sociale.** C'est-à-dire l'utilisation de la tromperie dans les messages afin que l'utilisateur télécharge un fichier au contenu malveillant (un virus, par exemple) ou clique sur un lien qui le conduira vers un site web où il sera exposé à une escroquerie, entre autres.

Comme son nom l'indique, l'ingénierie sociale consiste à manipuler les leviers des relations sociales pour atteindre un objectif, ou à construire un contexte spécifique pour produire un effet. Dans le cyberespace, les procédures d'ingénierie sociale sont couramment utilisées pour conduire les utilisateurs vers l'une des trois (3) destinations suivantes:

1. Le téléchargement d'un **virus** sur votre appareil.
2. Action d'une **fraude** par laquelle vous allez prétendre vous abonner à un service payant, par exemple, l'abonnement à des services SMS premium.
3. Obtenir les données personnelles (téléphone ou courriel) et financières (informations sur les cartes de crédit) de l'utilisateur à des fins de vol d'argent, d'usurpation d'identité, de fraude ou à d'autres fins illégales.

Figure 17 - Objectifs les plus courants de l'ingénierie sociale

3.3.2 Utilisations malveillantes ou involontaires du contenu divulgué

Les **escroqueries les plus couramment utilisées en matière d'ingénierie sociale** et de réseaux sociaux peuvent être classées dans les catégories suivantes:

- **Contenu accrocheur ou attractif,** tel que des vidéos choquantes dont le visionnage est recommandé, ou des liens vers du contenu sur des curiosités, des célébrités, des nouvelles alarmantes, ou tout autre contenu similaire. L'ingénierie sociale, dans ce cas, utilise la curiosité naturelle de l'homme pour les contenus choquants ou nouveaux afin d'augmenter la probabilité que les utilisateurs cliquent sur le contenu et, de là, les dirigent vers le virus ou la fraude.

- Les **enquêtes**, qui circulent quotidiennement sur les réseaux sociaux, notamment par le biais des appareils mobiles, dans le but apparent de demander l'avis de l'utilisateur sur différents comportements d'achat pour masquer le but réel de l'enquête.

  Leur but, en général, est d'inciter l'utilisateur à s'inscrire à un service payant, à des tarifs spéciaux pour les SMS ou, dans le moindre des cas, de lui demander son adresse électronique de contact, qui fera immédiatement partie d'une base de données qui sera vendue et utilisée pour convertir le sujet en destinataire d'énormes quantités de spam.

- **Publicité pour des applications nouvelles ou très demandées,** qui dans la plupart des cas sont des applications frauduleuses que l'utilisateur télécharge par le biais d'un message sur les réseaux sociaux pour découvrir que l'application n'était pas ce qui avait été promis -dernière version du jeu vidéo préféré, optimiseur d'espace sur le téléphone portable, antivirus gratuit, utilitaire pour voir les nouveaux contacts sur les réseaux sociaux, mais plutôt des applications qui contiennent une sorte de code malveillant dans le but de prendre le contrôle de l'appareil mobile, de voler des informations sensibles telles que des mots de passe ou des cartes de crédit, de détourner le contenu pour obtenir une rançon ou, si vous êtes bienveillant, d'afficher des publicités indésirables.

- **Offres de bons ou de coupons de réduction** dans des établissements commerciaux connus dans lesquels, derrière la tromperie du faux coupon de réduction qui peut arriver par les réseaux sociaux ou par email parfois masqué dans un tirage au sort, le but caché est d'obtenir les données personnelles de l'utilisateur pour faire du commerce avec eux ou pour les abonner, par des astuces, à des services de paiement de tarifs spéciaux.

- **Les revendications de contacts sexuels ou de pornographie gratuite** qui, sous couvert d'identités proposant des relations intimes, suggèrent à l'utilisateur

10. Pour un exemple de faux coupons de réduction: https://www.osi.es/es/actualidad/avisos/2016/05/de-nuevo-vales-descuento-de-lidl-que-te-vacian-la-cartera

de cliquer sur des liens ou des contenus multimédias qui finiront par le diriger vers des sites web où il lui sera demandé de fournir des données personnelles pour les échanger avec eux, où il tentera de s'abonner, par la manipulation et la tromperie, à des services payants, ou encore où il téléchargera un code malveillant ayant divers effets néfastes pour le dispositif que le sujet utilise.

Le dépannage de problèmes technologiques ou de comptes d'utilisateurs, dans lequel des messages d'avertissement prétendant provenir des services techniques de fournisseurs connus auxquels l'utilisateur peut ou non s'abonner (PayPal, Google, Facebook, Netflix ou autres) sont utilisés pour informer le sujet de problèmes avec son appareil ou son compte d'utilisateur, en lui suggérant de cliquer sur des liens ou de télécharger des contenus qui entraîneront une fraude, un virus ou le vol de données, de mots de passe ou d'argent. Une procédure identique à celle du *phishing* traditionnel est utilisée, mais dans ce cas, l'escroquerie est diffusée par le biais de messages sur les réseaux sociaux au lieu d'utiliser le courrier électronique.

3.4 Étape 4: Soigner les relations personnelles

Bien que la création d'un profil dans un réseau social soit déterminée par la définition de traits d'identité - qui nous sommes ou à qui nous aimerions ressembler -, et qu'ensuite les contenus diffusés déterminent le comportement des personnes, ce sont les contacts et les amis qui donnent un sens à la signification même de "réseau social".

Le réseau social est déterminé par la définition des traits d'identité et le contenu diffusé déterminera le comportement des personnes; contacts et amis.

En effet, un réseau social est un instrument, un **outil de socialisation dans le cyberespace;** socialisation qui se matérialise par des contacts, des amis ou des suiveurs, c'est-à-dire les autres identités avec lesquelles nous sommes en relation avec le réseau à travers le plan *cybersocial*.

3.4.1 Gestion des relations, des contacts et des amis

En matière de gestion des contacts, les utilisateurs de réseaux sociaux devront principalement prendre deux (2) types de décisions;

- **Choix des contacts:** principalement lors de la création du profil sur le réseau social, mais aussi tout au long de la vie du profil, où de nouveaux contacts seront établis et certains des contacts existants seront perdus. Dans certains réseaux sociaux, pour établir de nouveaux contacts, il faut demander à d'autres identités de devenir amis et être accepté comme tel.

- **Protéger avec le voile de la vie privée,** en gardant la liste des contacts ouverte, de sorte que tout le cyberespace sache avec qui vous êtes en relation (ou avez l'intention d'être en relation), ou en gardant cachée la liste des amis et des followers, de sorte qu'elle ne soit visible que pour vous-même et vos contacts.

Avant de décider si vous voulez que votre liste de followers, de contacts ou d'amis ne soit pas visible grâce aux options de confidentialité définies par les différents réseaux sociaux, la première étape consiste à les choisir, c'est-à-dire à commencer à cliquer sur "suivre" ou à faire des demandes d'amis à d'autres identités.

Certains réseaux sociaux demandent à l'utilisateur d'accéder à son carnet de contacts existant pour créer une première liste d'amis à partir de laquelle il pourra commencer à construire le profil qu'il vient de créer. Cette demande d'accès est courante dans les applications de réseaux sociaux pour les appareils mobiles où les utilisateurs ont généralement enregistré leurs contacts dans le répertoire téléphonique. Dans la demande d'une application au carnet de contacts d'un utilisateur, il faut distinguer deux (2) concepts:

- **Demander des autorisations à l'application.** Certains réseaux sociaux, pour que leurs *applications soient* obligatoirement installées par l'utilisateur, demandent la permission d'effectuer certaines actions dans le carnet de contacts (lecture et modification, principalement). Cette autorisation *n'implique pas* que les contacts de l'utilisateur dans votre répertoire téléphonique seront incorporés en tant qu'amis ou suiveurs au profil du réseau social qui a été formé.

3.4.1 Gestion des relations, des contacts et des amis

Demande d'importation de contacts. Certains réseaux sociaux, lorsqu'un utilisateur est en train de créer un nouveau profil, demandent la permission d'importer des contacts d'autres réseaux sociaux où le sujet a déjà des amis, ou de son carnet d'adresses. En important des contacts, le réseau social tente d'absorber la liste complète des amis d'un profil que le sujet possède déjà sur un autre réseau social ou sur son téléphone.

Les demandes initiales d'accès au carnet d'adresses ou d'importation de contacts ne présentent pas en soi de menaces pour la sécurité (à moins qu'il n'y ait d'autres circonstances à risque, par exemple l'infection de l'appareil par un logiciel malveillant), mais elles constituent des exemples **pertinents de la vie privée du sujet dans le cyberespace.**

Dans les deux cas, de riches informations sur les contacts de l'utilisateur sur plusieurs réseaux sociaux sont transférées à l'opérateur du réseau social. Cette réalité ne représente pas un problème a priori, mais il est bon d'être conscient de l'implication de la cession d'informations à plusieurs réseaux sociaux, qui sont gérés par le même groupe d'entreprises, comme Facebook, Instagram et WhatsApp, tous sous le groupe Facebook ; ou Skype, LinkedIn ou Yammer, propriété de Microsoft.

D'autre part, dans la plupart des réseaux sociaux, la structure de contact d'un utilisateur est composée des autres identités que le sujet suit dans les réseaux sociaux, en plus des utilisateurs qui suivent le profil du sujet. Dans certains réseaux, tels que Facebook, l'ajout de nouveaux contacts implique d'être "ami" avec ce contact afin d'être accepté dans son réseau de relations.

Dans les deux cas, que ce soit par l'ajout direct d'un contact ou par une demande d'ami, ce contact fait partie des informations auxquelles d'autres identités ont accès sur les réseaux sociaux. Si le profil diffuse des informations au grand jour sans protection de la vie privée, grâce à lui, d'autres personnes sauront non seulement qui nous sommes (les déclarations biographiques consignées), quels sont nos intérêts, nos goûts et, dans une certaine mesure, nos comportements (le contenu que nous publions), mais aussi avec quelles autres personnes nous sommes en relation ou aimerions l'être.

La structure relationnelle d'un sujet est une source d'information primordiale pour déduire son idéologie, ses études, son domaine de performance professionnelle, son lieu de résidence probable et d'autres facteurs qui, bien que l'utilisateur ne les ait pas expressément indiqués, peuvent être déduits. Ces informations que l'on pourrait déduire sur un

sujet à partir de ses contacts dans les réseaux sociaux peuvent être cachées en restreignant, par des contrôles de confidentialité, la visibilité de la liste des contacts, amis ou suiveurs du profil de l'utilisateur.

Les paramètres de confidentialité pour les contacts d'un profil sont disponibles dans le menu des paramètres de tous les réseaux sociaux, de la même manière que la confidentialité est activée et désactivée pour les contenus. À cet égard, Facebook permet de masquer la liste des amis tout en gardant le contenu du profil ouvert, tandis que Twitter ou Instagram exigent du sujet qu'il protège la confidentialité de l'ensemble du profil (contenu et amis) afin de ne pas rendre la liste de contacts du sujet visible par d'autres identités qui ne sont pas des amis ou des followers de l'utilisateur.

Un dérivé de la protection de la vie privée de la liste de contacts est lié aux demandes d'amis. Cette intention de créer de nouvelles amitiés fait partie de la nature même des réseaux sociaux: rencontrer de nouvelles personnes pour établir de nouvelles relations. Il s'agit donc d'une contribution positive des réseaux sociaux en tant qu'outils de communication.

Cependant, il existe des risques dont l'utilisateur doit être conscient et qu'il doit gérer. Le risque le plus évident de donner accès (en acceptant une demande d'ami) à une nouvelle identité à la liste de contacts, si celle-ci est protégée par la confidentialité, est que le nouveau venu aura accès aux informations sur les contacts de l'utilisateur et à la structure du réseau de relations de l'utilisateur dans ce réseau social.

3.4.2 Ingénierie sociale et risques des relations en réseau

La visibilité de la structure des amis et des contacts dans un réseau social comporte des risques potentiels. La plus évidente d'entre elles est liée à l'entrée dans le cercle des contacts d'identités inconnues, ce qui constitue une opportunité d'élargir et d'enrichir l'univers des relations personnelles, sociales et professionnelles, mais qui implique une phase initiale de risque au cours de laquelle une personne peut en aborder une autre avec des intentions cachées.

El personaje que se construye como un "yo virtual" para que represente a una persona en redes sociales puede hacer creer que son "amigos".

Un concept préliminaire à prendre en compte en ce qui concerne les contacts qui sont acquis dans un réseau social est le **cadrage de la relation d'amitié.** Étant donné que les gens ont des relations virtuelles, le manque de proximité physique est compensé par une tendance à surévaluer le lien virtuel, en lui donnant plus de poids sentimental qu'il n'en aurait dans un processus normal de connaissance mutuelle entre personnes dans le monde analogique.

Un autre élément qui contribue au fait que, dans les réseaux sociaux, la nature des relations interpersonnelles est surdimensionnée, en **considérant des amis qui ne sont pas plus que des contacts**, est le masque ou le personnage que le profil dans un réseau social représente pour chaque utilisateur. Dans les réseaux sociaux, les vertus peuvent être exagérées ou même représenter un rôle avec des qualités que l'utilisateur aimerait posséder, en plus du fait qu'il est plus facile de cacher ce qui est considéré comme des défauts; de cette façon, lors d'une nouvelle rencontre, lors d'un nouveau contact et en interagissant avec lui, on essaie d'auto-affirmer autant que possible le **personnage qui** a été construit dans le réseau social.

La structure psychologique et perceptive particulière qui est générée lorsqu'un utilisateur a de nombreux contacts dans un réseau social peut conduire à la fausse sensation que ces contacts sont des amis, au même

sens que les amis dans le monde analogique. Ce phénomène peut conduire à un abaissement de la garde, à une **diminution de la perception du risque dans les relations interpersonnelles** avec des inconnus et, par conséquent, à une confiance plus grande que celle qui est due dans un délai plus court qu'elle ne devrait l'être.

En ayant accès au réseau d'amis, une identité malveillante peut non seulement déduire des informations sur une personne qui ne sont pas initialement destinées à être explicitement énoncées, mais elle pourrait utiliser ces informations pour se livrer à des comportements de cyberintimidation de toutes sortes.

Parmi l'éventail des comportements de cyberintimidation, le *sexting* de contenu intime a déjà été mentionné. La distorsion de la perception de l'amitié virtuelle est plus fréquente chez les enfants et les jeunes, devant lesquels des personnes aux intentions malveillantes et illégales peuvent développer des comportements de harcèlement sexuel, qui sur Internet et les réseaux sociaux sont appelés *grooming*. Le *grooming* est "l'ensemble des stratégies qu'un adulte développe pour gagner la confiance d'un mineur par le biais d'Internet afin d'obtenir des concessions sexuelles"[11].

Une autre forme d'intimidation via les réseaux sociaux, qui touche particulièrement les enfants et les mineurs, est la *cyberintimidation*, par laquelle un agresseur tente de saper la stabilité émotionnelle d'une victime en utilisant les canaux des médias sociaux, mais aussi les SMS, les courriels ou les messages WhatsApp, faisant de la victime l'objet de menaces, d'insultes ou de messages d'intimidation (pouvant aller jusqu'au chantage).

En termes de contrôle des risques liés au maintien d'une liste de contacts "sains" sur les médias sociaux, un élément supplémentaire de prévention consiste à surveiller les demandes d'adhésion et d'amitié afin de supprimer, au fur et à mesure, à la fois les adeptes et les **bots** suspects.

Les *bots*, dont le nom est l'abréviation de *robots*, sont des profils automatisés créés sur les réseaux sociaux pour effectuer des comportements répétitifs qui ne nécessitent pas l'intervention d'un humain pour être exécutés. Par exemple, un *bot* sur Twitter ou Instagram peut être programmé pour émettre des *likes* ou faire des commentaires (toujours les mêmes, comme "bravo", "génial" ou "peut être amélioré") à un contenu spécifique; par exemple, lorsqu'on parle d'un film, d'un livre, d'une exposition ou d'un gouvernement ou d'un dirigeant politique.

Il existe d'autres *bots* programmés pour suivre automatiquement les profils qui parlent de certains sujets. Les *bots* sont des outils utiles dans le cyberespace lorsqu'il s'agit d'automatiser des tâches. Ils sont de plus en plus utilisés dans les campagnes de marketing en ligne, les sondages d'opinion,

11. http://www.pantallasamigas.net/proteccion-infancia-consejos-articulos/grooming-acoso-a-menores-en-la-red.shtm

pour tester le comportement de nouvelles solutions logicielles ou pour augmenter le trafic sur les réseaux sociaux ou les sites web.

Toutefois, les *robots de médias* sociaux peuvent également être utilisés pour générer un trafic indésirable, gênant ou carrément malveillant. Voici des exemples de scénarios à éviter dans lesquels les *bots* peuvent être impliqués:

- **Créer une image négative d'une personne ou d'une marque.** Ces bots sont programmés pour diffuser des messages négatifs et, pour ce faire, ils diffusent des contenus préconçus, en cherchant à ce que les adeptes reproduisent et rediffusent ces contenus.
- **Harceler ou faire pression sur certaines personnes ou groupes,** ce que l'on appelle le trolling dans l'argot des réseaux sociaux (les *trolls* sont les bots qui trollent), comportement qui peut être réalisé avec des *bots* préprogrammés pour insulter, disqualifier ou reprocher certains contenus ou personnes répondant à certaines caractéristiques (par exemple, une certaine idéologie, orientation personnelle ou hobby).
- **Diffuser du spam, de la publicité ou des services non désirés.** Il s'agit de l'écosystème d'action le plus courant des *bots*, qui sont capables de transmettre un ensemble programmé de messages publicitaires et de les diffuser sans relâche. Parfois, les robots sont conçus avec des publicités trompeuses pour capter les clics des utilisateurs et les rediriger vers des sites de téléchargement de logiciels malveillants. En d'autres termes, différents types de virus qui vont infecter l'appareil de l'utilisateur avec des intentions cybercriminelles.
- **Augmenter artificiellement le volume de followers des utilisateurs.** Ce type de bots est créé en masse, de l'ordre de plusieurs centaines de milliers, pour s'accumuler dans la liste des followers ou des amis de certains utilisateurs afin de générer un faux sentiment de popularité dans le profil de cet utilisateur - généralement lié à la vente de followers sur les réseaux sociaux, lorsqu'un utilisateur vient de créer un profil sur les réseaux sociaux et a besoin "d'avoir des amis et des followers"-. Il est courant de vendre des paquets de followers (5 000, 10 000, 100 000).

Dans ces cas, les **bonnes pratiques recommandées** sont les suivantes:

- **Gardez les** informations considérées comme plus personnelles sur les profils et qui pourraient exposer une personne si elles étaient connues publiquement, **protégées par la confidentialité**. D'une manière générale, il

serait judicieux de ne pas insérer d'informations personnelles sur un profil de médias sociaux qui pourraient être considérées comme sensibles.

- **Soyez plus prudent lorsqu'il s'agit de demandes d'amis provenant d'identités inconnues.** Avant de les accepter, il est préférable d'examiner le profil de cette personne sur ce réseau social, pour s'assurer que vous avez des intérêts communs, ou du moins que ce qu'elle dit d'elle-même ne déclenche pas de signaux d'alarme. Si le profil est caché ou restreint ou s'il présente une caractéristique qui, a priori, "ne convient pas", il est recommandé de ne pas accepter la demande d'ami.

- **Bloquez les identités ayant des intentions malveillantes ou gênantes.** Les situations de blocage sont celles dans lesquelles une autre identité insulte ou partage des contenus inappropriés ou inconfortables avec l'utilisateur, comme les identités ayant pour but d'administrer en permanence des publicités ou des services non désirés, les profils qui suivent l'utilisateur ou demandent son amitié afin d'"obtenir plus de followers" ou d'augmenter artificiellement les leurs.

- **Signalez les identités non désirées au fournisseur de services.** Si vous recevez des contenus inappropriés, si vous êtes harcelé ou si vous avez le sentiment qu'une identité se comporte de manière inappropriée, il est conseillé, par principe, de signaler cette identité au fournisseur de services du réseau social. Tous les réseaux sociaux ont mis en place une procédure de "dénonciation"[12].

- **Enregistrez et signalez tout contenu jugé inapproprié ou harcelant.** Si vous commencez à recevoir des contenus qui vous sont spécifiquement destinés et qui sont considérés comme suspects parce qu'ils ressemblent à des insultes, des propositions inappropriées, des menaces ou d'autres types d'expressions qui causent de l'ennui, vous devriez sauvegarder une copie de ces contenus, car elle pourrait être utile si vous devez déposer un rapport sur l'identité ennuyeuse ou malveillante.

- **Activez systématiquement la protection de la vie privée dans les profils des mineurs.** Il est conseillé de s'assurer que les mineurs qui créent un profil sur les réseaux sociaux activent les contrôles de confidentialité, tant pour les contenus que pour les listes d'amis, en les réduisant au minimum et sans fournir de données personnelles, comme les informations visibles par le grand public dans le cyberespace.
  Si les contrôles de confidentialité sont combinés avec la supervision du profil par les adultes en charge du mineur et une éducation minimale sur l'utilisation des réseaux sociaux, un standard acceptable de bonnes pratiques dans la gestion des réseaux sociaux pour les mineurs sera maintenu.

12. https://support.twitter.com/articles/108038

3.5 Étape 5: Adopter une culture de cyberprotection personnelle

La prévention et la gestion des risques dans les réseaux sociaux ne se fait pas de manière isolée, en intensifiant et en renforçant la sécurité des sites web ou des applications à partir desquels le service est fourni dans chaque réseau social; ni seulement en réduisant de plus en plus les vulnérabilités des appareils utilisés pour se connecter au cyberespace, tels que les téléphones, les ordinateurs, les montres et progressivement tout objet d'usage quotidien comme la voiture ou la télévision.

La meilleure prévention des risques est obtenue lorsque, dans un écosystème où plusieurs facteurs convergent, comme c'est le cas du cyberespace avec les sites web, les dispositifs, les objets et les personnes, **la sécurité du maillon le plus faible est considérablement accrue;** et, dans le cyberespace, le maillon le plus faible en termes de sécurité est l'être humain, qui, contrairement aux machines, ne peut être programmé.

La cybersécurité humaine dans le cyberespace peut être partiellement réalisée en "forçant" les humains à effectuer certaines tâches qui impliquent des comportements de sécurité. Par exemple, en les empêchant de choisir des mots de passe qui ne sont pas alphanumériques et qui comportent plus de huit caractères, ou en limitant l'utilisation de certains types de fichiers dans les navigateurs web qui sont considérés comme potentiellement vulnérables. Cependant, tant le libre arbitre du comportement humain lui-même que les techniques malveillantes utilisées par l'ingénierie sociale prouvent à l'envi que **la cybersécurité la plus efficace commence par l'autoprotection de l'internaute dans le cyberespace.**

Les humains doivent se protéger des menaces du cyberespace. Par exemple: des mots de passe alphanumériques de plus de huit caractères ou en diminuant les vulnérabilités des appareils.

3.5.1 Définir le cybernaute intelligent

L'autoprotection dans le cyberespace exige que l'internaute, l'utilisateur des réseaux sociaux, adopte un comportement personnel en matière de cybersécurité:

Conscience situationnelle du risque. L'autoprotection dans le cyberespace exige de comprendre que, comme dans le monde analogique, il existe également des espaces dans les réseaux sociaux où des identités malveillantes tenteront d'obtenir un avantage illicite en causant du tort à autrui.

S'informer sur les menaces et les vulnérabilités. Soyez généralement conscient des dangers potentiels qui peuvent se cacher sur les réseaux sociaux. Le meilleur moyen de rester informé est de s'abonner, sur les réseaux sociaux eux-mêmes, à une chaîne d'information proposant des mises à jour quotidiennes avec des conseils et des avertissements sur la sécurité sur Internet. En Espagne, l'Institut national de la cybersécurité a créé le Bureau de la sécurité Internet précisément à cette fin, avec des canaux d'information sur le web et les réseaux sociaux[13].

Internaliser et appliquer les bonnes pratiques de cyberprotection, en étant conscient des comportements qui mettent les utilisateurs en danger sur les réseaux sociaux et de ceux qui les empêchent d'être exposés aux cybermenaces. Ces comportements préventifs doivent être mis en pratique et progressivement intériorisés comme faisant partie d'une **manière sûre de naviguer dans** le cyberespace.

13. www.osi.es, www.facebook.com/osiseguridad, www.twitter.com/osiseguridad, www.youtube.com/user/OSIseguridad.

3.5.1 Définir le cybernaute intelligent

Par conséquent, le **cybernaute intelligent** est une personne consciente et informée, qui profite du contenu qui circule quotidiennement sur ses réseaux sociaux pour y inclure des alertes ou des notifications sur les nouveaux risques et les meilleures pratiques; qui est au courant des dernières formes de *phishing*, des derniers contenus préjudiciables ou des publicités indésirables qui peuvent l'affecter, des derniers schémas de fraude ou des derniers codes nuisibles qui sont transmis par les réseaux sociaux dans l'intention de voler des données personnelles ou de l'argent.

En d'autres termes, le cybernaute intelligent tire parti de ce que les réseaux sociaux représentent comme canaux d'information immédiats et continus pour se doter d'une **culture personnelle de la cyberprotection et de la cybersécurité;** une culture qui fait de lui un habitant moins vulnérable du cyberespace, réduisant la surface d'exposition et lui permettant d'extraire toute la valeur personnelle, sociale et professionnelle que les réseaux sociaux pourraient lui apporter. Ainsi, en intégrant des directives de protection simples et de bonnes pratiques dans leur routine quotidienne de navigation sur Internet, les risques qui peuvent être évités sont mis de côté.

4. Décalogue de recommandations

Voici dix (10) recommandations de sécurité pour l'utilisation des sites de réseautage social

Décalogue de la sécurité dans les réseaux sociaux

1. Un site permanent alimenté par des photographies, des données personnelles et des informations sur les études, la profession, les goûts, les intérêts, les amis et la famille fournit beaucoup plus d'informations sur la personne que sa carte d'identité ou son passeport. En outre, elle serait visible par tous. Il est essentiel de prêter attention à la manière dont vous définissez votre profil sur les réseaux sociaux, car il sera la lettre d'introduction de votre identité dans le cyberespace.

2. Réfléchissez au contenu qui est partagé sur les réseaux sociaux. De plus en plus de personnes et d'entreprises observent et analysent les réseaux sociaux pour porter un jugement sur d'autres personnes. Si vous voulez un jugement équitable, vous devez contrôler votre propre contenu.

3. Ne partagez pas de contenus sensibles concernant votre vie personnelle ou celle des autres sur les réseaux sociaux : documents d'identité, numéros de téléphone, adresses postales, localisation exacte, identifiants de véhicules, etc. Plus vous partagez ce type de contenu, plus vous risquez d'être victime d'une usurpation d'identité, de cyberintimidation ou de toute autre conduite illégale qui utilise vos propres informations pour vous nuire.

4. Dans le cyberespace, le principe de "se méfier de l'inconnu" s'applique. Ne cliquez pas sur un contenu dont l'origine ou le but n'est pas clair et redoublez de prudence face à des messages provenant d'identités inconnues. En bref, évitez la tentation de tout ce qui paraît d'autant plus attrayant qu'il est inconnu.

5. Protégez l'accès aux profils de médias sociaux avec des mots de passe forts en utilisant une authentification à deux facteurs lorsque cela est possible.

6. Contrôlez la géolocalisation des profils et des contenus sur les réseaux sociaux. Désactivez la géolocalisation par défaut dans le menu de configuration des profils et faites-en un usage intelligent, en réfléchissant dans chaque cas si vous voulez que les autres aient une carte de votre vie ou d'une partie de celle-ci.

7. Vérifiez les paramètres de confidentialité à la fois sur votre profil et sur le contenu que vous partagez. Sachez que le cyberespace est rempli d'yeux numériques et que vous ne devez montrer que ce que vous êtes sûr que tout le monde peut voir. Dans le doute, gardez les informations privées pour les amis et les contacts.

8. Ne pas diffuser d'informations privées sur d'autres personnes sans leur consentement et ne pas étiqueter nommément d'autres personnes qui n'ont pas de profil sur les réseaux sociaux sans leur demander au préalable l'autorisation de le faire.

9. Prenez soin et protégez vos relations dans le cyberespace. Gardez votre liste de contacts privée et examinez attentivement les demandes d'amis émanant d'inconnus.

10. Adopter la conscience que la première ligne de défense pour la protection dans le cyberespace est soi-même. De cette manière, l'aide fournie par les institutions et organisations de cybersécurité sera beaucoup plus efficace et vous serez vous-même d'une aide précieuse pour assurer la sécurité des réseaux sociaux.

centro criptológico nacional

centro criptológico nacional

www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es