Passerelles numériques
Un passeport pour la vie

SECURITÉ EN LIGNE

SEHENOARISOA ADELAÏDE

TABLE DES MATIÈRES :

INTRODUCTION

Un réseau social, ou média social, est tout simplement un site internet (ou une application mobile) qui consiste et permet aux utilisateurs d'échanger entre eux, de partager des contenus, de découvrir des photos, vidéos, sons, ou de s'informer sur des sujets. Facebook, Twitter, LinkedIn, Instagram… Les médias sociaux sont un formidable réservoir de clients potentiels. Partir à la conquête de nouveaux prospects grâce à la publicité, fidéliser ses clientèles existantes ou animer votre communauté, les réseaux sociaux sont de véritables atouts pour les entreprises. Avec une page professionnelle créée sur le réseau social, le plus adapte aux contenus (article professionnel, photos de vos créations…), vous pourriez inviter vos clients à vous suivre pour garder le lien avec eux.

En étant présent sur une plateforme d'échange de contenus, on peut facilement communiquer par rapport à notre marque, produit, entreprise ou encore pour des événements. Comme exemple, LinkedIn est le leader des réseaux sociaux dédié aux relations professionnelles. Permettant de se créer un CV en ligne et de se connecter avec d'autres professionnels, le réseau social est également mondialement connu pour être très utile lors de la recherche d'emploi ou d'employés.

Pour les particuliers, il permet de partager des photos, des vidéos, des messages, mais également de suivre les actualités de ses amis. Les entreprises, quant à elles, peuvent compter sur Facebook pour communiquer avec leurs clients (partage de photos, vidéos, Live…), faire des publicités ciblées, vendre leurs produits ou encore servir de plateforme de service client.

Chap1. LA SÉCURITÉ EN LIGNE

La sécurité en ligne, c'est la sécurité Internet qui est une expression qui décrit la sécurité des activités et des transactions exécutés sur Internet. Cela implique la cybersécurité, la sécurité informatique, la sécurité du navigateur, les comportements en ligne et la sécurité du réseau.

I. Le rôle de la sécurité en ligne

La sécurité informatique protège les technologies de l'information comme les systèmes, les réseaux et les données informatiques contre les attaques, les dommages et les accès non autorises.

1. La sécurité des réseaux wifi public

a. Qu'est-ce que le wifi public ?

Le Wi-Fi public est accessible dans des lieux publics fréquentés (aéroports, cafés, centres commerciaux, restaurants et hôtels). Il vous permet d'accéder gratuitement à Internet. Ces points d'accès sont si répandus et font tellement partie du quotidien que les gens s'y connectent sans y réfléchir.
Quels sont les risques ?

Quand une personne se connecte à un Wifi public à l'aide de sa machine, elle peut ouvrir l'accès à un malware un logiciel malveillant sur son appareil et le pirate pourra ainsi avoir accès à toutes ses données même à distance.

b. Quels sont les risques du wifi publics ?

Quand une personne se connecte à un wifi public à l'aide de sa machine, elle peut ouvrir l'accès à un malware un logiciel malveillant sur son appareil et le pirate pourra ainsi avoir accès à toutes ses données, même à distance.
L'utilisation du WIFI public est dangereuse. Les pirates informatiques adorent le partage des données.

Pour se connecter au WIFI public, il est très rare qu'une authentification soit demandée et donc, les pirates sont en mesure d'intégrer les réseaux sociaux et de piocher dans les données personnelles qui transitent. L'un des risques les plus importants concerne l'interception des informations.

Les inconvénients du WIFI c'est les fuites d'informations ou la présence d'utilisation non autorises ne sont pas à exclure sur ce réseau sans fil, lorsqu'il est mal sécurisé. Les pirates informatiques ont également la possibilité d'utiliser une connexion WIFI non sécurisée pour diffuser des programmes

malveillants. Si vous autorisez le partage de fichiers sur un réseau, le pirate peut facilement installer des logiciels infectés sur votre ordinateur

c. Comment sécuriser les réseaux WIFI publics

Il existe quelques bonnes habitudes à prendre pour minimiser le niveau de risque, c'est-à-dire de désactivés la connexion automatique aux réseaux WIFI disponibles et vérifier que vous vous connectez bien au bon SSID ou le nom du réseau.
Le moyen le plus sûr de se connecter à un réseau WI-FI public est d'utiliser un VPN.

Les appareils numériques et les logiciels que nous utilisons au quotidien sont exposés à **des failles de sécurité**. Ces failles peuvent être utilisées par des cybercriminels pour prendre le contrôle d'un ordinateur, d'un équipement mobile ou encore d'une montre connectée. Face à ces risques, les éditeurs et les fabricants proposent des mises à jour (patch en anglais) visant à corriger ces failles. Si l'opération de mise à jour est souvent ressentie comme une contrainte, il s'agit pourtant d'un acte essentiel pour se protéger.

Il faut penser à mettre à jour l'ensemble de vos appareils et logiciels

Ordinateurs, téléphones, systèmes d'exploitation, logiciels de traitement de texte, objets connectés… Nous utilisons un grand nombre d'appareils et de logiciels. Il suffit qu'un seul ne soit pas à jour et soit exposé à une faille de sécurité pour ouvrir une brèche dans votre environnement numérique.
Afin d'empêcher les cybercriminels d'utiliser ces failles de sécurité pour vous pirater et vous dérober des informations personnelles sensibles, il est primordial de réaliser les mises à jour de vos équipements dès qu'elles sont disponibles.

Il faut se méfier des fausses mises à jour sur internet

En naviguant sur Internet, il arrive que des messages prenant l'apparence d'alertes de mises à jour apparaissent à l'écran : fausses publicités sur des sites Internet ou fenêtres malveillantes. Restez extrêmement vigilant, car il peut s'agir d'une technique pour vous inciter à installer une prétendue mise à jour qui serait en réalité un virus.

2. Le mot de passe

Un mot de passe, c'est un code alphanumérique ou phrase, moyen d'authentification, qu'il faut donner pour accéder dans un endroit protégé ou pour utiliser une ressource ou un service dont l'accès est limité et protégé.

Quels sont les mots de passe ?

Dans les Boites mail, sites d'e-commerce, services administratifs… De nombreux sites demandent de créer un compte et de le protéger avec un mot de passe et de nombreux internautes utilisent le même mot de passe sur tous les sites afin de ne pas l'oublier. Attention ! Cette pratique est risquée et peut permettre à des pirates d'avoir accès à toutes vos informations pour utiliser votre identité, ou votre compte bancaire. Voici tous nos conseils pour créer un mot de passe sécurisé

- **La protection des données personnelles :** les mots de passe forts et uniques sont essentiels pour protéger les comptes en ligne et les données personnelles qu'ils contiennent. En outre, les logiciels de sécurité tels que les antivirus peuvent aider à prévenir les atteintes à la vie privée et les fuites de données en détectant les programmes malveillants qui tentent d'accéder aux données personnelles stockées sur l'ordinateur ou l'appareil mobile.

- **Les mots de passe :** les mots de passe sont les uns des éléments clé de la sécurité en ligne. En utilisant des mots de passe forts et uniques pour chaque compte, les utilisateurs peuvent se protéger contre les attaques de phishing et les violations de la vie privée. Les gestionnaires de mots de passe peuvent aider à stocker les mots de passe en toute sécurité et à les gérer facilement. Dans les Boites mail, sites d'e-commerce, services administratifs… De nombreux sites demandent de créer un compte et de le protéger avec un mot de passe et de nombreux internautes utilisent le même mot de passe sur tous les sites afin de ne pas l'oublier.

- **La protection contre les logiciels malveillants :** Les logiciels malveillants peuvent être transmis via des e-mails de phishing, des sites web infectés ou des périphériques USB infectés. Les logiciels de sécurité, tels que les antivirus et les pares-feux, peuvent aider à détecter et à prévenir l'infection par des logiciels malveillants. En outre, la sensibilisation aux attaques de phishing et l'adoption de pratiques de navigation en ligne sûres peuvent aider à prévenir les infections.

3. La sécurité des appareils mobiles : les appareils mobiles sont souvent utilisés pour effectuer des transactions en ligne, stocker des informations sensibles et se connecter à des réseaux Wi-Fi publics. En utilisant des mots de passe forts pour verrouiller les appareils mobiles et

en installant des logiciels de sécurité tels que les antivirus, les utilisateurs peuvent se protéger contre les attaques de logiciels malveillants. En outre, l'utilisation de réseaux Wi-Fi sécurisés et la prudence lors de la navigation en ligne peuvent aider à prévenir les violations de la vie privée.

4. LES RÈGLES DE BASE DE LA SÉCURITÉ EN LIGNE :

• Gérez les mots de passe.

• Faites des sauvegardes

• Faites vos mises à jour

• Protégez-vous des virus.

• Évitez les réseaux wifi public.

• Séparez vos usages pro-perso.

• Contrôlez les permissions des comptes utilisateurs.

• Contrôlez les permissions des comptes utilisateurs.

• Faire attention aux informations personnelles ou professionnelles que l'on diffuse sur Internet

• Sécurité numérique : être vigilant sur les liens ou les pièces jointes contenus dans des messages électroniques

II. L'authentification a double facteur.

L'authentification à double facteur est un processus de sécurité par lequel l'utilisateur fournit deux modes d'identification à partir de catégories de données distinctes : l'une se présente généralement sous la forme d'un jeton physique, comme une carte, et l'autre sous forme d'informations mémorisées, par exemple un code de sécurité.

Qu'est-ce qu'un facteur d'authentification ?

Ces deux facteurs représentent une chose *possédée* et une chose *sue*.

Une carte bancaire est un bon exemple d'authentification à double facteur : la carte elle-même constitue l'élément physique, tandis que le code secret (ou PIN) représente les données qui y sont associées. La combinaison de ces deux éléments rend plus difficile l'accès à un compte bancaire par une personne non autorisée, celle-ci devant posséder à la fois l'élément physique (la carte) et le code secret.

Ce type d'authentification permet de réduire l'incidence de fraudes en ligne, telles que l'usurpation d'identité et l'hameçonnage, étant donné que le mot de passe de la victime ne suffit pas à accéder aux informations.

La double authentification ajoute une seconde couche de protection lorsque vous vous connectez à un site. Après avoir saisi un mot de passe, il vous faut prouver que c'est bien vous.

L'authentification à deux facteurs ajoute un second niveau de sécurité, pour sécuriser votre compte même si votre mot de passe a été pirate. Avec Duo Push, vous recevez immédiatement une alerte (sur votre téléphone) si un autre utilisateur tente de se connecter en utilisant votre compte.

La double authentification, qu'est-ce que c'est ? Depuis plusieurs années, les mots de passe ne suffisent plus. Faciles à détourner (il suffit que quelqu'un connaisse votre mot de passe pour se connecter à votre compte), ces vestiges du web sont amenés à évoluer, en attendant leur disparition annoncée avec **les passkeys**, qui identifient automatiquement un utilisateur sur une page grâce à un identifiant unique stocké sur leur appareil. En attendant, la double authentification (ou 2FA) s'est imposée comme la meilleure alternative.

Au moment où vous insérez votre mot de passe, un site qui propose l'authentification à double facteurs procèdera à une seconde vérification pour prouver votre identité. Cela peut-être un code généré par une application,, un SMS, un scan de votre empreinte digitale sur un lecteur spécial… La double authentification se repose en fait sur une logique de sécurisation connue : s'identifier avec l'aide de ce que vous savez (votre mot de passe) et de ce que vous avez (un code, une empreinte, etc.). Mais il existe plein de manières de mettre cet outil en place, et toutes ne se valent pas.

De nombreux sites proposent la double authentification. Google, Apple, Facebook, Instagram, Snapchat, Microsoft, PlayStation, Slack, Amazon

1. L’application d’authentification

Une application d’authentification est sûrement la meilleure solution aujourd’hui. Simple à utiliser, ces logiciels offrent un niveau de sécurité élevé. L’idée est la suivante : on télécharge sur son smartphone un logiciel comme *Google Authenticator* ou *Microsoft Authenticator*. Ensuite, depuis le site que l’on utilise (Twitter ou Facebook par exemple), on choisit l’option application de connexion dans les réglages de sécurité. Un QR Code apparaît à l’écran, il suffit de le scanner avec l’application.

À chaque fois que l’on se connectera à ces sites, un code de vérification sera demandé. Il faut alors ouvrir son application et renseigner le code à 6 chiffres qui apparaît. Ces codes expirent toutes les minutes, mais se renouvellent automatiquement.

Plutôt sécurisée, cette méthode présente par contre un inconvénient : vous ne pourrez pas vous identifier sur une machine inconnue si vous n’avez pas votre téléphone sous la main. La plupart des sites proposent sinon des codes de « secours » pour les moments où vous n’avez justement pas votre téléphone sur vous (un SMS par exemple, ce qui abaisse la sécurité). Depuis peu, il existe aussi des systèmes 2FA intégrés aux systèmes d’exploitation. Un iPhone peut par exemple stocker et générer ses propres codes, pour que l’utilisateur n’ait rien à faire.

2. Comment activer l’authentificateur a double facteur ?

- Allez sur la page COMPTE.
- Cliquez sur l’onglet MOT DE PASSE et SECURITE.
- Sous l’intitule « AUTHENTIFICATION A DEUX FACTEURS », cliquez sur l’option d’authentification à deux facteurs que vous souhaitez activer
- Vérifier que l’authentification à deux facteurs est **activée.**

Comme nous avons pu le voir, il existe de nombreuses manières de s’identifier avec la double authentification. Toutes ont des qualités et des défauts qu’il faut prendre en compte au moment de choisir la solution qui convient le mieux. Tous les sites ne proposeront pas forcément toutes ces méthodes, donc il faudra potentiellement composer avec ces limites aussi.

Chap2. ANTIVIRUS

I. Définition :

Un antivirus est un logiciel informatique destine à identifier et à effacer des logiciels malveillants (malwares en anglais et virus en français). Son but principal est de détecter, neutraliser ou éradiquer les logiciels malveillants des ordinateurs et autres appareils informatiques qui sont infectés. Il joue également un rôle préventif en empêchant les virus d'infecter les systèmes informatiques et de leur nuire.

L'antivirus est le **cadenas** qui verrouille la porte d'entrée d'un appareil.

Ce logiciel élimine ou réduit le risque de **cyberattaques** sur l'ordinateur, le téléphone ou la tablette qui disposent d'un accès à internet.

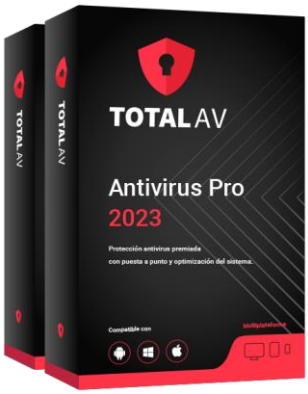
II. Le fonctionnement d'un antivirus

Un logiciel antivirus vérifie les fichiers et courriers électroniques, les secteurs de démarrage (afin de détecter les virus de boot), mais aussi la mémoire vive d'ordinateur, les médias amovibles (clefs USB, CD, DVD, etc.), les donnees qui transitent sur les éventuels réseaux.

La détection et suppression des logiciels malveillants, protège contre le piratage informatique et le vol de donnees, la protection (par le pare-feu) contre l'exploitation des vulnérabilités, la protection contre les attaques de phishing.

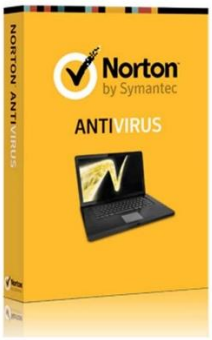
III.Les meilleurs antivirus

Total AV : est un programme antivirus gratuit avec un excellent taux de détection de malware et une gosse gamme de fonctionnalités de sécurité, une fois installé sur votre ordinateur, se chargera de l'analyser, et détecter les éventuelles menaces.



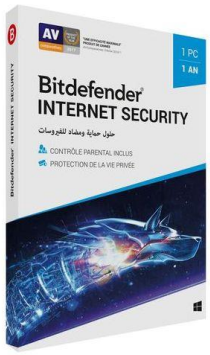
Source : Safety Detectives Total AV Antivirus Review 2023

Norton Antivirus fait partie des antivirus parmi les plus utilises dans le monde, protégeant des millions d'utilisateurs depuis des décennies contre les programmes malveillants qui peuvent menacer votre cybersécurité et la confidentialité des services Windows.



Source: Swifter Mall |Norton Security Software

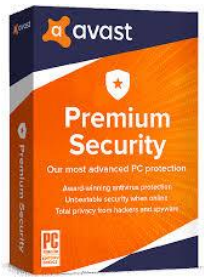
Bitdefender : est une suite de sécurité complète qui offre une protection en temps réel en surveillant les fichiers, les connexions réseau et les activités systèmes pour détecter les comportements suspects.



Source : Bitdefender Antivirus Internet Security |Jumia Tunisie

AVG Antivirus : protège le navigateur Web de l'utilisateur contre les sites Web malveillants, le phishing et les attaques d'hameçonnage en avertissant l'utilisateur des pages potentiellement dangereuse et en bloquant les tentatives d'escroquerie en ligne.

Source: AVG Antivirus for Mac Antivirus Software Review – Consumer Reports



Avast

Source : Walmart.ca

McAfee

Source : monlogiciel.fr

IV. SÉCURITÉ DES DONNÉES PAR RAPPORT AU PHISHING ANTIVIRUS

1. Base de données de signature de virus :

L'une des méthodes pour identifier et classifier un code informatique, au sens de son innocuité ou de sa nocivité, est l'usage de « **bases de signatures** ».

Les **bases des signatures** sont des fichiers (des bases de donnees), mis à jour en continue par les éditeurs de solutions de sécurité, contenant des éléments remarquables des malveillances, permettant de reconnaître la « signature » d'une malveillance (un ou des bouts de codes particuliers, une méthode ou habitude de programmation d'un cybercriminel, un ensemble de comportements).

2. Blocage des sites de phishing:

C'est la référence à la capacité d'un programme antivirus ou d'un logiciel de sécurité à détecter et à empêcher l'accès a des sites web qui sont identifiés comme étant des sites de phishing.

Le phishing est une technique utilisée par les cybercriminels pour tromper les utilisateurs et les inciter à divulguer des informations sensibles telles que des identifiants de connexion, des mots de passe, des numéros de carte de crédit.

3. Analyse comportementale:

Une analyse comportementale utilise l'autoapprentissage, l'intelligence artificielle, le Big Data et les donnees chiffrées pour identifier les comportements malveillants en analysant les différences dans les activités quotidiennes normales.

La protection comportementale observe l'activité du système (Windows, Android, MacOs…) et reconnait des actions qui paraissent malveillantes, tels que des requêtes vers un serveur inconnu, des modifications de fichiers, ou des demandes d'accès à des emplacements de la mémoire.

4. Protection en temps réel:

La protection en temps réel fournit une protection antivirus. Le composant détecte et neutralise les menaces, applications publicitaires et applications que les individus malintentionnés utilisent pour nuire à votre appareil ou exploiter vos données personnelles.

Avec la protection temps réel, l'antivirus analyse tous les fichiers qui vont entrer dans votre ordinateur ou qui peuvent être exécutés par l'utilisateur ou le système.

5. Mise à jour de l'antivirus

Il est important de s'assurer que l'antivirus est toujours a jour pour une protection optimale.

La mise a jour est un processus consistant à apporter des modifications ou des améliorations à un logiciel, un système d'exploitation, une application ou tout autre élément informatique. Elle vise à corriger des erreurs ou à améliorer les performances globales du logiciel ou du système.

Les mises à jour importantes ou critiques corrigent des failles de sécurité qui peuvent etre utilisées pour pirater votre équipement. Les mises à jour de version apportent en général de nouvelles fonctionnalités et corrigent également des failles de sécurité.

Chap3. ARNAQUE

I. Définition :

Les arnaques sur les réseaux sociaux sont des pratiques frauduleuses où des individus malveillants exploitent les plateformes de médias sociaux pour tromper les utilisateurs et les soutirer de l'argent, des informations personnelles sensibles ou d'autres formes de valeur. Ces arnaques ressemblent à des offres, des opportunités d'investissement, des loteries, des cadeaux ou des demandes d'aide, afin de piéger les utilisateurs et de les inciter à prendre des mesures qui profitent aux fraudeurs.

Par défaut, les paramètres de visibilité de vos informations personnelles (numéro de téléphone, adresse email…) et de vos publications sont souvent très ouverts. Vos donnees peuvent ainsi etre partagées à tous les abonnés du réseau social.

❖ Comment éviter de se faire arnaquer

S'informer sur les différentes formes d'arnaques sur les réseaux sociaux et le partager avec votre entourage. Soyez vigilant face aux offres belles pour etre vraies, se méfier des demandes d'argent, des demandes d'informations personnelles sensibles ou des demandes de connexion a des liens suspects. Ne croyez pas tout ce que vous voyez ou lisez sur les réseaux sociaux.

Avant de partager es informations, de répondre à des messages ou de cliquer sur des liens, vérifiez soigneusement la source et de s'assurer de son authenticité. Prendre le temps de paramétrer les options de confidentialité et de sécurité de votre compte sur les réseaux sociaux. Limitez la visibilité de vos informations personnelles et de vos publications aux personnes de confiance.

Installez et maintenez à jour un logiciel de sécurité fiable sur vos appareils, y compris des programmes antivirus et antimalwares. Ces outils peuvent aider à détecter et à bloquer les menaces potentielles sur les réseaux sociaux.

Si vous rencontrez des arnaques sur les réseaux sociaux, signalez-la immédiatement a la plateforme concernée. La plupart des réseaux sociaux disposent de mécanismes de signalement pour lutter contre les activités frauduleuses.

Eviter de partager des informations personnelles telles que votre numéro de carte de crédit, votre numéro de sécurité sociale, ou des photos de documents officiels sur les réseaux sociaux.

Soyez prudent lorsque vous recevez des demandes d'amis ou de connexions de personnes que vous ne connaissez pas car ils utilisent souvent des faux profils pour approcher leurs victimes. Si vous rencontrez une publication, un message ou un commentaire suspect, évitez d'interagir avec eux, ne pas cliquer sur les liens suspects et ne pas répondre aux demandes d'informations personnelles.

II. GESTION DE MOT DE PASSE ET CRYPTAGE DE DONNÉE

- **Un gestionnaire de mot de passe** est une solution numérique avec laquelle l'utilisateur peut gérer ses mots de passe en centralisant l'ensemble de ses identifiants et mots de passe dans une base de donnees.

Le gestionnaire de mots de passe sert à mémoriser pour vous vos codes d'accès, dans un environnement protégé, c'est comme une sorte de coffre-fort par un type de logiciel ou de service en ligne qui permet à un utilisateur de gérer ses mots de passe.

- **Le cryptage de données** se résume à chiffrer des documents ou informations par le biais d'algorithmes et de clefs de chiffrement. Il sert ainsi à assurer à la fois leur intégrité et leur confidentialité. Il permet de rendre les informations totalement incompréhensibles afin d'en garder leur confidentialité. Le chiffrement est un processus réversible qui ne fait que masquer les donnees. Il est donc toujours possible de retrouver leur valeur initiale grâce a une clé.

III.VPN ??

VPN vient en réalité de l'anglais ***Virtual Private Network*** qui signifie **Réseau Privé Virtuel** en français.

Le VPN est donc un logiciel qui s'installe sous plusieurs appareils reliés à Internet. Une fois le VPN active, un tunnel sécurisé se créer entre vous et le réseau Internet. De cette manière, les informations qui y transitent seront chiffrées.

La définition de VPN est la même, peu importe l'appareil sur lequel vous comptez l'installer. En effet, ce logiciel n'est pas uniquement compatible sur votre ordinateur mais peut également s'installer sur un smartphone (que vous soyez sous iOS ou Android) ou sur une tablette. On parle d'application VPN.

À quoi sert un VPN ?

- **A protéger ses donnees sur Internet :** les VPN sont connus pour leur capacité à sécuriser la connexion des internautes. Les VPN rendent l'accès a vos donnees web plus difficile, même si une personne malintentionnée venait à s'emparer d'informations vous concernant, elle ne pourrait les exploiter car les logiciels VPN ont recours à des algorithmes de chiffrement très puissants.

Les VPN protègent donc l'ensemble de vos donnees personnelles (mots de passe, coordonnées bancaires, sites web consultés…)

- **A naviguer de manière anonyme :**la connexion a un serveur VPN va avoir pour conséquence de masquer votre adresse IP réelle. Et rappelons que l'IP est un numéro attribué à votre appareil qui permet de vous identifier. En échange, c'est l'adresse IP du serveur VPN qui sera visible sur le net.

Ainsi, lorsque vous naviguer sur un réseau non sécurisé, comme dans le lieu public par exemple, l'activation du VPN va écarter les risques d'usurpation d'identité et de tracking en ligne.

A changer son adresse IP

Un VPN, ça sert également à changer son adresse IP afin, notamment, de contourner de nombreux blocages géographiques. Le VPN vous permet de récupérer l'adresse IP de serveurs partout dans le monde.

Ainsi, même si vous vous trouvez en France, vous pourrez récupérer une IP australienne, américaine, allemande. Le choix dépend simplement de la localisation des serveurs de votre fournisseur VPN. Dans votre sélection, essayez-donc de vous assurer que le fournisseur de VPN dispose bien de serveur dans le pays de votre choix.

IV. Phishing malware et ransomware

1. Le phishing

L'hameçonnage ou phishing est une forme d'escroquerie sur internet.

Le fraudeur se fait passer pour un organisme que vous connaissez (banque, service des impôts, CAF, etc.), en utilisant le logo et le nom de cet organisme. Il vous envoie un mail vous demandant généralement de « mettre à jour » ou de « confirmer vos informations suite à un incident technique », notamment vos coordonnées bancaires (numéro de compte, codes personnels, etc.) afin de vous soutirer des renseignements personnels : mots de passe, numéro de carte de crédit, numéro ou photocopie de la carte d'identité, date de naissance, etc.

En effet, le plus souvent, une copie exacte d'un site internet est réalisée dans l'optique de faire croire à la victime qu'elle se trouve sur le site internet officiel ou elle pensait se connecter. La victime va ainsi saisir ses codes personnels qui seront récupérés par celui qui a créé le faux site, il aura ainsi accès aux donnees personnelles de la victime et pourra dérober tout ce que la victime possède sur ce site.

Attention ! Ne répondez jamais à ces messages, ne cliquez pas sur les liens, n'ouvrez pas les pièces jointes.

Que faire ?

Signalez les escroqueries auprès du site www.internet-signalement.gouv.fr

Supprimez les messages puis videz la corbeille.

S'il s'agit de votre messagerie professionnelle, transférez courriels au service informatique de votre employeur pour vérification. Attendre leur réponse avant de supprimer le courrier électronique.

Déposez plainte auprès du commissariat de police ou de la gendarmerie dont vous dépendez en fournissant tous les éléments de preuve en votre possession. Vous pouvez déposer une pré-plainte en ligne pour faciliter les démarches.

2. Malware

Un malware est un logiciel malveillant qui intervient dans le but de nuire à l'utilisateur de l'ordinateur. C'est une forme de cyberattaque et l'objectif est de voler des données personnelles, financières ou commerciales.

Le logiciel malveillant peut aussi :

Chiffrer ou supprimer des donnees sensibles

Modifier ou détourner des fonctions IT de base

Espionner l'activité IT des utilisateurs.

Les malwares sont utilisés par les cybercriminels pour gagner de l'argent mais peuvent aussi être utilisés à des fins de sabotage, pour des motivations politiques.

a. Comment un malware infecte votre appareil

Lorsque vous téléchargez des fichiers sur des sites douteux, des malwares peuvent être téléchargés sur votre appareil a votre insu. De même, des malwares peuvent s'introduire sur vos appareils si vous cliquez sur des liens dans des e-mails suspects envoyés depuis des adresses électroniques inconnues.

b. Un malware peut se propager à partir de :

Les Wi-Fi non sécurisés, les clés USB, les fausses applis mobiles, les sites internet frauduleux, les scarewares, les programmes logiciels gratuits, les logiciels publicitaires…

3. Le ransomware

Les ransomwares est un élément de la famille des applications malveillantes.

a. *Comment détecter les ransomwares et s'en protéger :*

Lorsqu'il s'agit de se protéger contre les ransomwares, il vaut mieux prévenir que guérir. Pour y parvenir, il est essentiel de faire preuve de vigilance et d'utiliser **le bon logiciel de sécurité**. Tout d'abord, il est important de s'assurer que votre appareil n'est pas une cible idéale pour les ransomwares. Les logiciels des appareils doivent toujours etre mis à jour afin de bénéficier des derniers correctifs de sécurité. Il est essentiel d'agir avec prudence, notamment en ce qui concerne les sites web malveillants et les pièces jointes des emails. Cependant, même les meilleures mesures préventives peuvent échouer, ce qui rend plus indispensable l'existence d'un plan d'urgence. Dans le cas des ransomwares, un plan d'urgence consiste à disposer d'une sauvegarde de vos donnees.

Les ransomwares présentent une menace importante pour les utilisateurs prives et les entreprises. Il est donc plus important de garder un œil sur la menace qu'ils représentent et d'etre aussi préparé que possible a toute éventualité. Il est donc essentiel de se renseigner sur les ransomwares, d'adopter une approche très consciente de l'utilisation des appareils et de disposer des meilleurs logiciels de sécurité disponibles.

b. *Comment les éviter ?*

Ne jamais cliquer sur un lien dans un email ou un message instantané qui semble suspect ou peu fiable.

Ne jamais ouvrir des pièces jointes ou des fichiers qui viennent d'une source inconnue ou suspecte.

Ne pas répondre aux emails qui vous demandent des informations personnelles ou financières sensibles.

CONCLUSION

L'importance du soin apporte à la gestion des données et à la manière dont chacun traite les informations qui s'échangent à travers les différentes plateformes et outils technologiques, paramétrant ce qu'on appelle l'hygiène numérique. Une hygiène numérique fait référence au soin que les utilisateurs de la technologie accordent aux systèmes. En leur accordant la maintenance dont ils ont besoin. En les configurant de manière à ce qu'ils ne soient pas vulnérables et en les mettant à jour en temps opportun pour maintenir un environnement numérique propre.

Le nombre d'intentions d'attaques et de fraudes numériques a augmenté. C'est pourquoi une bonne hygiène numérique personnelle est importante. Une meilleure hygiène numérique permet d'éviter d'être victime de certaines attaques numériques. Certaines habitudes qui devraient être adoptées pour ne pas être une proie facile pour les cybercrimes et les données qui ne sont pas fonctionnels. Avec un accent particulier sur les virus, les pirates malveillants tentent de nouvelles attaques. Les développeurs d'antivirus ajoutent de nouvelles méthodes et pour les détecter, vous devez donc rechercher la version la plus récente. Certaines habitudes qui devraient être adoptées pour ne pas être une proie facile pour les cybercrimes et les données qui ne sont pas fonctionnels. Parfois, des liens contenant des virus se propagent, ce qui peut affecter les appareils. Il faut s'assurer que les appels que l'on partage provienne d'une source fiable avant de les ouvrir.

Passerelles numériques
Un passeport pour la vie

Écrit par:

SEHENOARISOA Adelaïde

Encadré par:

Sitraka RANDRIAKOTO