Karunanayake Dinura / Torres Matteo / Doppia Calvin / Mukunayi Dan

12 règles essentielles pour sécuriser vos équipements informatiques.

1) Choisir avec soin ses mots de passe

Règle de sécurité est nécessaire dans un premier temps de protéger ses données , pour ne pas que les autres utilisateurs puissent accéder à votre session pour faire ce qu'ils ont à faire ou encore de se munir de vos informations personnelles comme par exemple votre compte bancaire.
Pour cela, il est important de choisir un mot de passe à la fois facile à retenir pour vous, mais à la fois très difficile de trouver pour les autres. Il faut choisir un mot de passe qui contient au moins 8 caractères, des majuscules, des chiffres et des caractères spéciaux afin de sécuriser au maximum votre mot de passe (**ET SURTOUT FACILE A RETENIR POUR VOUS**) .
On peut prendre exemple des utilisateurs qui doivent accéder à leur facture à la M2L, on peut leur demander un mot de passe qui sera leur numéro de facture afin de pouvoir y accéder en toute sécurité sans que personne d'autres puissent le consulter.

2) Mettre à jour régulièrement vos logiciels

Règle de sécurité est nécessaire dans un premier temps pour éviter d'avoir une mauvaise version d'un de leurs logiciels et donc ne pouvoir plus l'utiliser correctement avec la version la plus récente du logiciel , mais aussi pour sécuriser le logiciel afin de ne pas se faire infecter par les différents virus que vous pouvez rencontrer dans vos machines

Pour cela, il est important de faire les mises a jour le plus vite possible dès que l'occasion s'offre à vous (sauf si vous ne voulez pas le faire volontairement) , et de pouvoir bloquer les virus qui veulent pirater votre logiciel grâce à une application d'antivirus que vous pourrez trouver facilement dans votre appareil.

3) Bien connaître ses utilisateurs et ses prestataires

Règle de sécurité est nécessaire pour pas que des personnes mal intentionné et suspect ne puisse pas venir intégrer votre groupe social pour pirater votre compte ou encore de prendre vos informations personnelles.

Pour cela , nous vous conseillons dans un premier temps de mettre votre compte en privée pour éviter d'obtenir des demandes d'amis de la part d'autres utilisateurs , cela vous permettra de mieux contrôler votre compte , et dans un 2eme temps d'accepter uniquement les demandes des utilisateurs d'extremes confiances.

4) Effectuer des sauvegardes régulières

Règle de sécurité est nécessaire pour pas que vous perdiez votre travail de documents que vous êtes en train de faire depuis plusieurs heures et que vous devez tout recommencer depuis le début , et donc la perte de vos données.

Pour cela , je vous conseille de ne pas oublier de sauvegarder votre travail de manière régulière (environ toute les 20 minutes) afin de conserver au mieux votre travail ou sinon de mettre un logiciel de sauvegarde automatique pour ne plus en prendre en compte de ce problème là.

5) Sécuriser l'accès Wi-Fi de votre entreprise

Règle de sécurité est nécessaire pour pas que différentes personnes hors de votre entreprise puisse dans un premier temps accéder à votre connexion Wi-Fi mais surtout pour pas que les hackers et les personnes frauduleuses piratent votre Wi-Fi pour récolter toutes les données de toute les personnes connectés à ce Wi-Fi

Pour cela , il faut sécuriser votre accès Wi-Fi en mettant un mot de passe pour accéder à votre Wi-Fi, et pour la sécurisation de votre mot de passe Wi-Fi, vous pouvez prendre les mêmes conseils que je vous ait donné dans le numéro 1 (Choisir avec soins ses mots de passe).

6) Etre aussi prudent avec son smartphone ou sa tablette qu'avec son ordinateur

Règle de sécurité est nécessaire car il existe autant de cas de piratage des hackers avec leurs Smartphones ou bien leurs ordinateurs . Il permet aux hackers de pouvoir dans un premier temps d'accéder à tout vos logiciels que vous disposez dans votre téléphone mais surtout , il aura accès à vos réseaux sociaux et ceci est très dangereux car ils peuvent faire du mal à votre entourage et beaucoup d'autres choses.

Pour cela , vous pouvez dans un premier temps sécuriser votre téléphone avec des mots de passe sur chaque applications que vous utilisez au quotidien (si possible des mots de passe tous différents des uns des autres) , afin que votre hacker puissent accèder à moins d'applications possibles. Nous vous conseillons aussi si c'est un cas de vol de téléphone , d'installer une application de localiseur de votre téléphone depuis un autre appareil comme par exemple l'application « Localiser » de chez iPhone.

7) Protéger ses données lors de ses déplacements

Cette règle de sécurité est nécessaire car protéger ses données sur internet est primordial afin de ne pas être tracé. Ne pas être tracer permet divulguée des données privées. Les données téléphonique représente l'ensemble de notre vie avec vos photos, vos fichier, votre carte bleu, vos vaccins etc.

Nous pouvons d'abord y remédié en faisant attention sur les liens cliquable d'où vous êtes sur de sa provenance, sur les applications que vous téléchargeons, des fichiers à télécharger sur internet ou branché une clé USB inconnue sur votre pc.

Pour cela il y différente manière d'y échapper comme par exemple :

- Installer un anti virus afin d'être prévenue si il y a une infraction dans le système
- Activer le Windows defender afin d'être signaler si un logiciel malveillant ou un virus se trouve dans un fichier.
- Effectuer des sauvegardes de son téléphone afin de ne pas tout perdre dans le cas d'un vol, d'une casse, ou d'une infraction dans votre système.

8) Etre prudent lors de l'utilisation de sa messagerie

Règle de sécurité nécessaire car l'utilisation de messageries instantanées expose à des risques en matière de sécurité et de confidentialité des données échangées, donc la possibilité de transmettre la mauvaise donnée à la mauvaise personne et aussi de la divulgation des données.
Pour cela, vous devez bénéficier d'une protection intégrale lors de l'utilisation de la messagerie, vous devez utiliser des **certificats SSL/TLS (SSL = Secure Socket Layer , TLS = Transport Layer Security)** pour sécuriser l'intégralité de la chaîne de transmission, c'est-à-dire : La connexion entre le navigateur de l'utilisateur et la messagerie Web exécutée sur un serveur Web.

9) Télécharger ses programmes sur les sites officiels des éditeurs

Cette règle de sécurité est nécessaire afin de ne pas avoir un ordinateur contaminé par un virus ou logiciel malveillant. Le virus ce situe dans les fichiers télécharger par l'ordinateur.

Pour y remédier il faut faire attention sur les pages internet ou allons. Nous regarder sur internet si le site est sure d'utilisation ou non.

Il faut faire attention au niveau du Protocol HTTPS si il y a un s alors le site est sécuriser alors que sans le s le site n'est pas sécuriser il peut donc posséder un virus.

Les outils :

-Avec un anti virus nous pouvons être informés de la possibilité qu'il y est un virus.

-Pour la sécurité de l'ordinateur il est indispensable de télécharger son programme sur le site officiel des éditeurs.

-Effectuer des sauvegardes sur votre pc et mobile afin d'être assurer de ne pas tout perdre lors d'un casse, d'un vol ou d'une infraction dans le système.

10) Etre vigilant lors d'un paiement sur Internet

Cette règle de sécurité est primordial car si nous ne faisions pas attention il serrait possible d'avoir accès au donnée bancaire de la victime.

Pour y remédier

Il ne faut enregistrer ces données bancaires sur les sites. (Amazon, LeBoncoin)

- Il ne faut pas rentrez sa carte dans les liens qui sont envoyer par message
- Prévenir assez rapidement sa banque si nous recevons des commandes sans votre accord personnel.
- Ne pas mettre le même mot de passe sur le site que son adresse email.

Outils

- Il faut faire attention au niveau du Protocol HTTPS si il y a un s alors le site est sécuriser alors que sans le s le site n'est pas sécuriser il peut donc posséder un virus.
- Double identification pour avoir accès à votre carte bleu en recevant un code pour confirmer l'accès.

11) Séparer les usages personnels des usages professionnels

La règle de sécurité est que le fait de réunir l'usage personnels et professionnels créent un bordel au niveau de votre compte et donc potentiellement surchargé les données et aussi de louper les informations importantes qui doivent se situer dans le usager professionnel

Pour cela , séparer les 2 comptes personnels et professionnels comme ça si uns des comptes est piraté , l'autre reste sain et sauf.

12) Prendre soin de ses informations personnelles, professionnelles et de son identité numérique

La règle de sécurité est nécessaire car sont identité nous permet de nous identifier. Perdre son identité signifierait qu'une personne pourrait prendre votre identité et parler a votre place.

Différencier les informations personnelles et professionnelles permettras de ne pas divulgué toutes les données si un seul est contaminé.

Nous pouvons y remédier

- Faire attention a vos données et ne pas divulgué des informations importantes sur vous (pièce d'identité, carte bancaire, compte de ses réseaux sociaux).
- S'informer sur le site avec le quel nous souhaitons communiquer et ne rien envoyé par message a cause du nombre d'arnaque très important.

Outil

- Nous pouvons utiliser une double identification afin que se soit sure et que l'accès a votre compte soit plus complexe.
- Stocker les données de travail dans un autre ordi avec des mots de passe différents.