Sécurité informatique

A. Définitions :

1. Les logiciels malveillants **(Les malwares)** sont des programmes informatiques qui ont le but d'accéder à l'ordinateur ou le smartphone d'un utilisateur. Exemple : les virus, les chevaux de Troie (**Trojan horse**), les vers (**Worm**), les logiciels espions (**Spyware**), les logiciels publicitaires (**Adware**), les logiciels de rançon (**Ransomware**), **spam**...
2. **Un virus informatique** est un programme ou un code qui est chargé dans votre ordinateur sans votre autorisation ou que vous n'en ayez connaissance. Un virus peut détruire vos fichiers ou empêche l'ordinateur de fonctionner correctement.
3. **Un cheval de Troie** (**trojan horse**) est un type de virus qui prétend être quelque chose d'utile, d'agréable ou d'amusant alors qu'en réalité il provoque des dommages ou vole des données.
4. **Les vers** (**Worm**): sont des types de virus capables de se propager à travers un réseau informatique.
5. **Un logiciel espion** (**Spyware**) recueille des informations sur vos habitudes, votre historique de navigation, ou des informations personnelles (comme des numéros de carte de crédit), et utilise souvent Internet pour transmettre ces informations à des tiers sans que vous ne le sachiez. Les enregistreurs de frappe sont un type de spyware qui surveille vos frappes sur le clavier.
6. **Les logiciels publicitaire (Adware)** est un type de logiciel gratuit financé par des publicités qui s'affichent dans des fenêtres indépendantes ou dans une barre d'outils sur votre ordinateur ou dans votre navigateur. La plupart des adwares sont utilisés pour recueillir vos informations personnelles, suivre les sites web que vous fréquentez ou même enregistrer les touches sur lesquelles vous appuyez.
7. **Les logiciels de rançon** (**ransomwares**) restreignent l'accès à votre système informatique et exigent le paiement d'une rançon pour que la restriction soit levée.
8. **Le spam** est un message non sollicité qui fait la publicité d'un service ou d'un produit : la version électronique d'un courrier publicitaire.
9. **Les faux sites internet** : sont des sites internet qui récupèrent les données de paiement ou les mots de passe. Attention, les faux sites internet sont des copies parfaites des sites originaux.
10. **HOAX** : Il s'agit des messages de fausse alerte («canular») sur des virus soit disant très dangereux (ou toute autre forme de fausse rumeur). Son objectif est de provoquer la panique et t'inciter à envoyer des e-mails à tes amis, provoquant ainsi la saturation des serveurs de messagerie et des réseaux.
    Exemple : امانة برقبتك أرسلها لـ 122 شخص حتى ولو أنا منهم ستسمع خبر سار الليلة وحق الله مجربة وأذا نسيت راح تفقد شيء.....
11. **Une faille (on dit aussi vulnérabilité)** est une faiblesse, qui résulte d'une erreur de programmation d'un des logiciels utilisés sur l'ordinateur.
12. **Patch** : C'est un correctif de sécurité est un petit programme qui corrige les erreurs failles.
13. **Le piratage informatique** représente la manipulation d'un ordinateur et des systèmes qui lui sont connectés. Il est généralement effectué en utilisant des scripts ou des programmes qui manipulent les données en passant pas une connexion réseau afin d'accéder aux informations du système. Les techniques de piratage incluent virus, chevaux de Troie, rançongiciels, détournements de navigateur,...
14. **Hacker** : Les hackers sont des programmateurs intelligents qui cherchent à manipuler ou modifier un système ou un réseau informatique. Certains d'entre eux veulent s'emparer de vos données sensibles comme vos informations de carte bancaire, vos photos personnelles etc.
15. **Un antivirus** : c'est un logiciel de sécurité capable de rechercher, d'identifier et de supprimer les virus et les vers (et autres codes malicieux) connus dans la base de ses signatures de virus.
16. **Un pare-feu** (**firewall**) est un logiciel de sécurité qui protège le PC contre les tentatives d'attaques:
    - celles basées sur l'utilisation de chevaux de Troie,
    - celles (attaques directes), qui essayent d'exploiter les failles du PC, qu'elles soient l'œuvre d'un attaquant ou celles des vers.

B. Les risques provenant des communautés virtuelles

1. Voler ton d'identité ou l'identité des autres utilisateurs,
2. Publier ou partager du contenu violent (images choquantes, insultes,)
3. Diffuser des données sur votre vie privée,
4. Installer des chevaux de Troie, des virus, des programmes espion,… sur votre appareil.

C. Procédures de protection des données personnelles et de l'environnement de travail

I. Sur votre ordinateur :

1. Protéger ton PC par un mot de passe (Bios) et un mot de passe de compte sur le système d'exploitation.
2. Installer **un seul** antivirus et le mettre à jour périodiquement. Exemple : Avast, Avira, AVG, Kaspersky, Nod32, bitdefender, (le système d'exploitation Windows 10 a son propre antivirus Windows defender).
3. Installer un parefeu et le mettre à jour. Exemple : Comodo, agnitium outpost firewall, Armor, … (Le système d'exploitation Windows a un pare-feu.
4. Installer un utilitaire de protection contre les virus venant des flashs disque. Exemple : USB Disk Security, USBFix, smadav,…
5. Mettre à jour votre système d'exploitation (Windows update) et les logiciels installés si nécessaire.
6. Sauvegardez régulièrement vos données sur un DVD (une fois par an).
7. Eteindre le modem ou déconnecte du réseau wifi si vous n'avez pas besoin d'Internet.

II. Sur votre SmartPhone :

1. Protéger ton Smartphone par un mot de passe (Reconnaissance faciale, empreint digital).
2. Notez les informations d'identification de votre Smartphone (IMEI, Adresse MAC, Certification FCC)
3. N'installer des applications que depuis les boutiques connues (Play store, App store, Galaxy Store).

III. En navigant sur Internet :

1. Lorsque vous vous apprêtez à régler un achat sur internet ou se connecter à votre compte Facebook ou autre, vérifiez bien le nom du site et qu'il est bien sécurisé. L'adresse doit commencer par : « https ».
2. Si vous avez un doute sur un email, n'ouvrez pas la pièce jointe ou le lien qu'il contient.
3. Apprenez à identifier les extensions douteuses des fichiers. Si vous avez un doute ne les ouvrez pas surtout les fichiers exécutables (.exe / .vbs / .js)
4. N'ouvrez pas les mails dont la forme ou la provenance vous paraît douteuse.
5. Installez uniquement les logiciels provenant de sources fiables. Les sites www.ansi.tn et www.telecharger.com sont des références ou depuis les sites des développeurs ou constructeurs.
6. Si vous avez reçu un HOAX : n'appliquez pas les consignes et ne répondez pas l'expéditeur.
7. Ne partagez jamais des données personnelles sur Internet (Date naissance, Adresse, photos, vos avis, vos sentiments, vos favoris,…)
8. Si vous utilisez un ordinateur à usage publique : utilisez le mode navigation privé et supprimez l'historique de votre navigation.
9. Méfiez-vous : Le compte de ton père, d'un ami, ton professeur, ton entraineur, … peut être piraté.

IV. Les mots de passe

1. Créez un mot de passe complexe : lettres minuscules et majuscules, caractères spéciaux et chiffres.
2. Utilisez un mot de passe long et mémorisable (8 caractères ou plus). **Exemple** : la Tunisie mon beau pays 20 mars 1956. **le mot de passe peut être : LTmbP!20/3+1011**
3. Changez votre mot de passe périodiquement. (Deux mois au minimum)
4. Evitez d'utiliser les dates de naissance, noms d'une ville, numéros de téléphone… ou d'autres éléments figurant sur les réseaux sociaux.
5. Ayez un mot de passe différent pour chaque compte.
6. N'enregistrer jamais votre mot de passe même sur votre ordinateur personnel.
7. Ne communiquez jamais votre mot de passe. D'ailleurs, aucun site fiable ne vous le redemandera.
8. Toujours déconnectez de vos différents comptes avez de quitter.