question n° 1

SOLUTION

Pense toujours à vérifier les informations que tu trouves sur Internet avec plusieurs autres sites Internet pour éviter les erreurs

Le sport peut attendre, le plus important est de créer un devoir personnel en reprenant des informations de sources différentes, en les vérifiant et en les intégrant à sa manière dans son devoir.

Il est important d'avoir différentes sources d'information et ne pas se reposer uniquement sur une seule source d'information. Puisqu'une seule personne ne peut pas tout connaître, en demandant à plusieurs personnes on parvient à avoir une bonne idée d'un sujet et à faire un bon devoir en y mettant sa touche personnelle. En ne consultant qu'un seul site Internet pour faire ton devoir, tu risques de faire de grosses erreurs. N'oublie pas que l'auteur du site Internet a pu se tromper en écrivant ses pages web. Par exemple, la proposition de réponse #2 est totalement fausse puisqu'aucune vérification n'a été faite avec d'autres sources d'information. Tu peux te rendre compte qu'il y a de nombreuses erreurs (en gras).

question n° 2

SOLUTION

Ne publie jamais de photos de tes amis sur ton blog sans avoir leur autorisation. Ne donne jamais leur nom et leur adresse, ne te moque pas d'eux.

Internet est un lieu public où tout ce qui est écrit sera, pour toujours, accessible à tous les internautes. N'importe qui dans le monde peut accéder à ton blog et y lire ce que tu as écrit ou y voir les photos que tu déposes. Pour protéger tes amis, il ne faut pas publier leurs photos sans avoir eu leur autorisation. Rappelle-toi qu'Internet se souvient de tout, même des années après ! Aussi il n'est pas gentil de publier leurs photos en leur donnant des noms ridicules… Imagine la tête qu'ils feraient s'ils revoyaient ces photos et leurs surnoms quant ils auront des enfants.

Publier des informations comme leur nom et leur adresse est aussi très dangereux pour eux. Si quelqu'un veut leur faire du mal, cette personne saura comment ils s'appellent, où ils habitent et à quoi ils ressemblent.

question n° 3

SOLUTION

Ne publie sur ton blog que tes propres créations

Ton site perso est ton espace personnel sur Internet. Tant que tu respectes les personnes et la loi tu peux y mettre tout ce que tu veux.

Respecter les personnes veut dire qu'il ne faut pas écrire sur elles de mauvaises choses, ne pas mettre des photos ou des vidéos aggressives, humiliantes ou méchantes contre elles. Ainsi, demander l'autorisation de tes amis avant de mettre leurs photos sur ton blog c'est les respecter.

Respecter la loi veut dire qu'il ne faut pas mettre des jeux, de la musique ou des films sur Internet si tu n'as pas les droits d'auteur. Les droits d'auteur permettent de redonner de l'argent aux personnes qui ont créé quelque chose pour leur permettre de continuer à travailler et créer de nouvelles choses. Ainsi, les droits d'auteurs permettent à ton groupe de musique préféré de continuer à faire la musique que tu aimes. Aussi, lorsque tu fais de la musique avec ton groupe de musique, ce que tu as composé vous appartient, à toi et à ton groupe, tu peux donc les diffuser comme tu veux sur Internet. En revanche, tu n'as pas le droit de mettre sur Internet des MP3s de ton groupe préféré car tu ne possèdes pas le droit de diffuser la musique que tu n'as pas composée.

Rappelle-toi que ces deux règles s'appliquent tout le temps, pour tout ce que tu fais sur Internet.

Pour finir, il faut que tu saches que ce n'est pas parce que tu ouvres ton site perso sous un faux nom que tu échappes à ces deux règles. Garde en mémoire que personne sur Internet n'est vraiment anonyme et que la police pourra toujours te retrouver si tu ne respectes pas les règles.

question n° 4

SOLUTION

Protège ton intimité sur Internet

Des informations comme :

- ton nom,
- ton prénom,
- ta date de naissance,
- ton adresse,
- des détails sur ta vie, sur tes goûts ou sur tes parents,

sont des informations personnelles. Tu peux les considérer comme des informations intimes sur toi.

Tu dois tout le temps essayer de protéger ton intimité car si quelqu'un sur Internet arrive à obtenir ces informations, il pourra se faire passer pour toi auprès de tes amis. Il pourrait par exemple faire exprès de se fâcher avec eux pour te faire du mal.

Si tu te rends compte que des informations te concernant sont accessibles sur Internet, sur le blog d'un ami ou bien sur un site Internet que tu visites souvent, tu dois en parler très vite avec tes parents qui sauront quoi faire pour te protéger.

Pour finir, n'oublie pas que quand tu es sur Internet, tu ne dois jamais donner d'informations personnelles, même si en échange le site te propose des trucs cools. Rappelle-toi que certaines personnes peuvent rechercher cela pour te faire du mal à toi et à ta famille.

question n° 5

SOLUTION

N'envoie jamais de photos de toi, de ta famille ou de tes ami(e)s par MSN à des gens que tu ne connais pas dans la vraie vie.

MSN est un moyen simple pour dialoguer avec tes ami(e)s sur Internet, pour s'échanger des messages ou des photos, mais tu dois toujours penser à faire attention avec qui tu parles par MSN. Rappelle-toi que tu ne peux jamais savoir qui est vraiment derrière un écran d'ordinateur : un contact que tu ne connais pas peut être une personne très dangereuse pour toi. N'oublie pas : par MSN il est facile de mentir sur son âge, sur ses goûts et de s'inventer une fausse vie.

Lorsqu'une personne que tu ne connais pas dans la vraie vie te demande des choses personnelles, comme des photos de toi, de tes amis ou de ta famille ou même des détails intimes sur ta vie, tu dois en parler avec tes parents avant toute chose. De même, dès que tu te sens mal à l'aise, tu n'as pas à hésiter : coupe MSN et parle en très vite à tes parents.

Tu ne dois pas avoir honte d'être dans cette situation, tu ne dois pas non plus avoir peur de faire du mal à la personne avec qui tu parles. En premier, tu dois penser à te protéger pour éviter que l'on te fasse du mal.

question n° 6

SOLUTION

Sois toujours accompagné de tes parents lorsque tu rencontres des amis de MSN que tu n'as jamais rencontrés avant.

Tu ne peux jamais savoir qui est réellement derrière un écran d'ordinateur. Si tu n'as jamais rencontré la personne, tu ne peux pas savoir si elle est réellement gentille ou si elle fait seulement semblant pour pouvoir te faire du mal plus tard. Tu ne dois jamais considérer une personne que tu n'as jamais rencontrée comme un(e) vrai(e) ami(e) ! Lorsqu'un contact MSN demande à te rencontrer, tu dois immédiatement en parler avec tes parents pour qu'ils t'accompagnent pour faire connaissance avec ton contact MSN. Ne pars jamais tout seul, même si le rendez-vous n'est pas loin de chez toi. N'oublie pas : Il est très important d'éviter de faire de mauvaises rencontres qui pourraient te faire du mal.

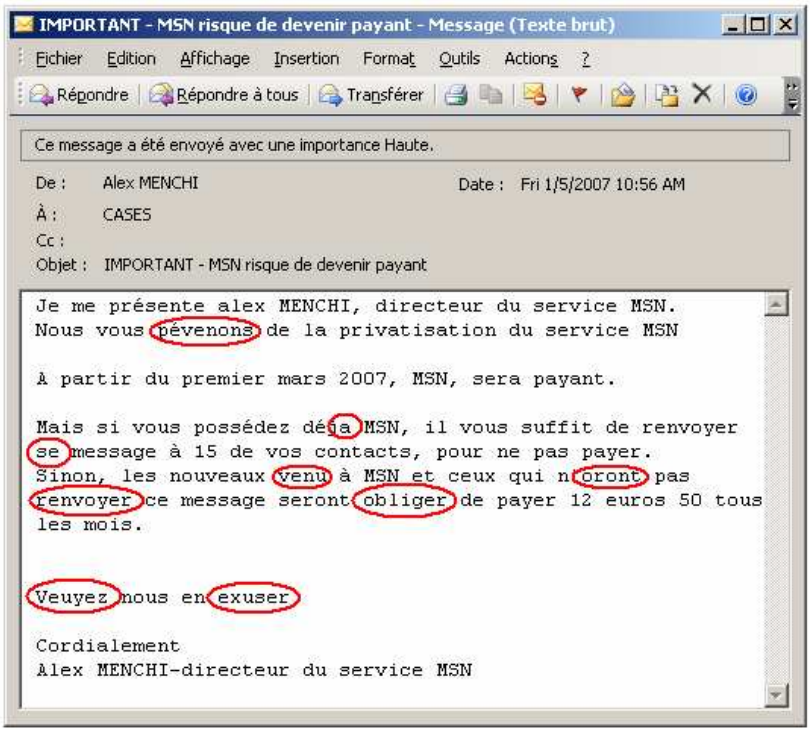
question n° 7

SOLUTION

Ne transmets jamais à tes amis les canulars que tu reçois par mail. Des mails qui se disent importants avec des fautes d'orthographe sont toujours des canulars.

Ce mail est un canular, ou plus précisément une chaîne de messages. Une chaîne de messages se caractérise toujours par le fait de devoir la renvoyer à plusieurs de tes contacts sinon une chose terrible risque de se passer. Tous ces types de messages sont des canulars : tu ne dois pas les prendre en compte et les ignorer. A l'avenir, quand tu recevras ce genre de message, tu dois le jeter à la poubelle sans le transmettre à tes amis.

Tu ne dois pas avoir peur et ne pas tenir compte des menaces du genre *« si tu ne transmets pas ce mail à 10 personnes tu auras les plus grands malheurs »*. Rappelle-toi que personne dans le monde ni sur Internet ne peut savoir si tu renvoies bien ce messages à 10 personnes, il ne peut donc rien t'arriver. De plus, regarde attentivement comment est écrit le message et compte le nombre de fautes d'orthographe. Un mail qui se dit être envoyé par le directeur du service MSN ne devrait comporter aucune faute d'orthographe !!



question n° 8

SOLUTION

N'ouvre jamais les pièces jointes des mails si quelque chose te semble bizarre.

C'est bizarre : ton ami(e) qui n'est pas doué(e) pour les langues, t'envoie un e-mail écrit en allemand avec un fichier attaché. Penses-tu que cela pourrait être possible ? Lorsque tu as ce genre de doute, tu ne dois pas hésiter, tu dois supprimer le message et contacter ton ami(e) pour savoir ce qu'il se passe et savoir quel était ce fichier, car il y a fort à parier que le fichier attaché au mail était un virus. Bien évidemment ne le transmets à aucun de tes contacts !

Il faut que tu saches que des virus informatiques sont capables de s'envoyer par e-mail à tous tes contacts sans que tu ne t'en rendes compte. C'est sûrement ce qui s'est passé, l'ordinateur de ton ami(e) est sûrement infecté par un virus qui cherche à contaminer d'autres ordinateurs… dont le tien.

Dans tous les cas, rappelle-toi que tous les mails que tu envoies sont conservés dans les *éléments envoyés* de ton programme de mail et que ton ami(e) pourra sans problème te renvoyer le message s'il n'y a aucun danger.

question n° 9

SOLUTION

Le phishing est une vraie menace, ne tombe pas dans le piège.

Le *phishing* est un piège pour voler des informations secrètes comme un numéro de carte bancaire ou ton mot de passe.

Dans le mail il est dit que tu dois très vite cliquer sur un lien pour ensuite taper ton mot de passe sur le site Internet. En fait, le site sur lequel tu taperas le mot de passe n'est pas le site officiel de eBay mais un site très ressemblant que les pirates d'informatique ont installé exprès sur Internet. Lorsque tu tapes ton mot de passe, en réalité tu le donnes aux pirates qui peuvent alors s'en servir pour faire des achats à ta place. Les ruses employées pour te piéger sont :

- Te faire croire que le mail provient du site officiel eBay, alors que ce n'est pas le cas, c'est un faux mail sur lequel on change l'adresse de l'auteur du mail,
- Te faire croire que c'est très grave,
- Te faire croire que tu dois agir vite pour éviter encore pire, comme la fermeture de ton compte.

Dans ce genre de cas, tu ne dois pas cliquer sur le lien et jeter tout de suite le mail à la poubelle.

question n° 10

SOLUTION

Fais attention aux programmes que tu downloades d'Internet.

Il faut faire attention aux programmes que tu trouves par hasard sur Internet. Ils peuvent être dangereux et risquent d'abîmer ton ordinateur. Si après avoir téléchargé d'Internet un programme ou un jeu, ton ordinateur a un comportement étrange : il affiche des pages de publicité, il est beaucoup plus lent, des programmes qui fonctionnaient avant ne fonctionnent plus, etc., il est possible que tu aies installé, sans le savoir un *spyware* ou un *adware* :

- Un *spyware* est un logiciel espion qui enregistre tout ce que tu fais sur Internet pour l'envoyer à des pirates.

Ainsi, les pirates peuvent connaître les sites que tu visites, les mails que tu reçois ou que tu écris ou même pire, le code de carte bancaire lorsque tes parents font des achats sur Internet ou bien ton mot de passe MSN.

- Un *adware* est un autre type de logiciel malicieux qui provoque l'affichage de publicité sur ton ordinateur,

allant jusqu'à te gêner très fort lorsque tu t'en sers.

Il est possible de télécharger en toute légalité et sans risque sur Internet, des démos de jeux ou d'applications pour te faire une idée avant de les acheter. Le download de ces programmes se faisant sur les sites Internet officiels des éditeurs de jeux ou de programmes, il n'y a pas de risques.

N'oublie pas, pour éviter les virus, d'utiliser un programme anti-virus pour scanner avant d'ouvrir, tout ce que tu reçois d'Internet ou que tu downloades.

question n° 11

SOLUTION

Ne partage sur Internet que les fichiers que tu as le droit de partager.

Les droits d'auteur permettent de rémunérer les artistes, chanteurs, acteurs, créateurs de jeux vidéos, de leurs créations. Il y a fort à parier que si tu downloades d'Internet des jeux vidéos, de la musique ou même des films avant leur sortie officielle, il est presque sûr qu'il s'agit de copies pirates. Tu ne dois pas télécharger illégalement ou mettre illégalement à disposition des programmes ou des fichiers.

Il faut que tu saches que la loi interdit et punit les personnes qui downloadent des programmes, de la musique ou des films piratés. De plus, le fait de les mettre à disposition est encore pire et tu risques d'être puni encore plus durement.

Deux autres choses sont importantes :

3. La loi punit même si tu downloades pour ton usage personnel.

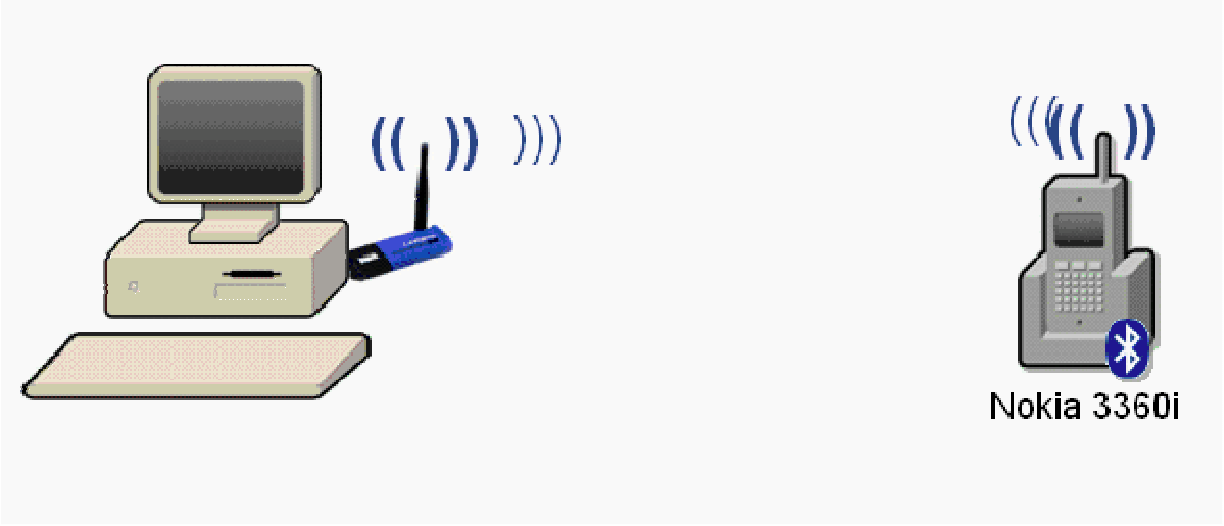
Si en plus tu renvends ce que tu as downloadé illégalement tu risques d'être puni(e) encore plus durement.

4. La loi punit dès le PREMIER download. Du point de vue de la loi, si tu downloades 1 programme tu es aussi responsable et tu risques les mêmes amendes et la même prison que celui qui downloade 1000 programmes.

5. **question n° 12**

SOLUTION

Désactive le Bluetooth dès que tu ne t'en sers plus



C'est vrai que le Bluetooth allumé en permanence risque de vider plus rapidemennt la batterie de ton GSM, mais le plus grave serait qu'un pirate puisse s'attaquer à ton téléphone. En effet, des pirates informatiques sont parvenus à écouter les conversations et à voler le carnet d'adresse de certains téléphones Bluetooth. Bien évidemment, les victimes de ces attaques ont été très embêtées. Comme tu ne peux pas savoir si un pirate informatique est à proximité de toi, le meilleur moyen pour se protéger est de désactiver le Bluetooth de ton téléphone quand tu as finis de t'en servir.

question n° 13

SOLUTION

Filmer une agression avec son téléphone portable est aussi grave que l'agression elle-même. Celui qui filme risque les mêmes ennuis que celui qui frappe.

Ce phénomène très grave consiste à filmer une agression avec son téléphone portable pour l'échanger entre amis ou la mettre sur Internet. L'humiliation de l'agression et d'être filmé est très durement ressentie pour la victime. On a vu au début du Permis Web qu'Internet a une grande mémoire, tout ce qui est déposé reste inscrit pour très longtemps. Frapper, filmer et diffuser ces images avec son handy a deux effets :

- Frapper est très douloureux pour la victime.
- Filmer et diffuser pour la victime c'est comme être une nouvelle fois agressée à chaque fois que la vidéo est regardée.

Rappelle-toi que la loi punit bien évidemment celui qui tape mais punit tout autant celui qui filme.
Il est important de lutter tous ensemble contre ce genre de comportements.

question n° 14

SOLUTION

Mets à jour les dernières versions de tes programmes et de tes jeux sur ordinateur pour te protèger contre les pirates informatiques.

La mise à jour de tes programmes et de tes jeux sur ordinateur est utile pour plusieurs raisons :

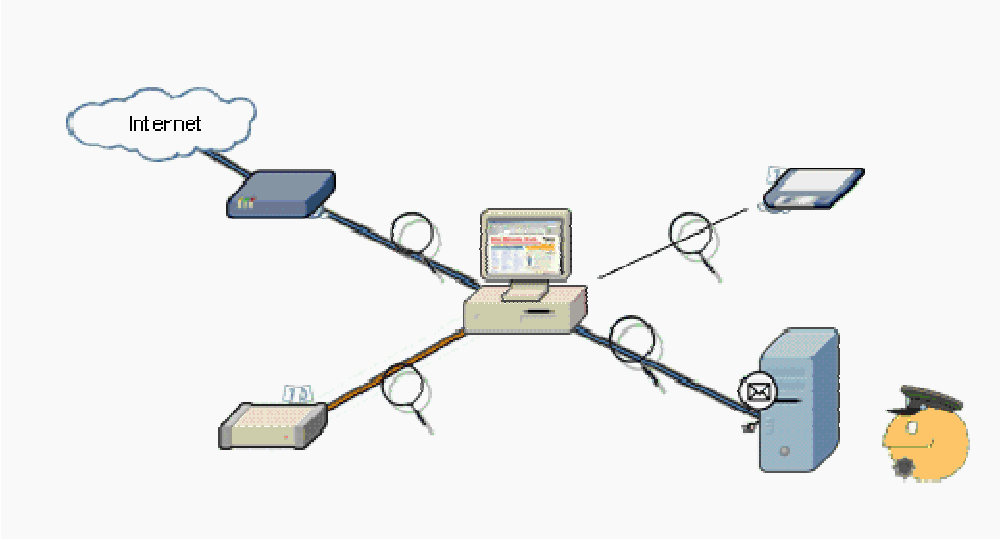
- Cela permet d'avoir les dernières options pour faciliter l'utilisation et le plaisir de les utiliser.
- Cela permet de corriger les erreurs dans les programmes, on appelle cela des bugs, qui pourraient te gêner quand tu utilises ces programmes.
- **Cela permet de corriger les problèmes de sécurité qui pourraient être exploités par les pirates pour attaquer ton ordinateur et te causer des problèmes.**

question n° 15

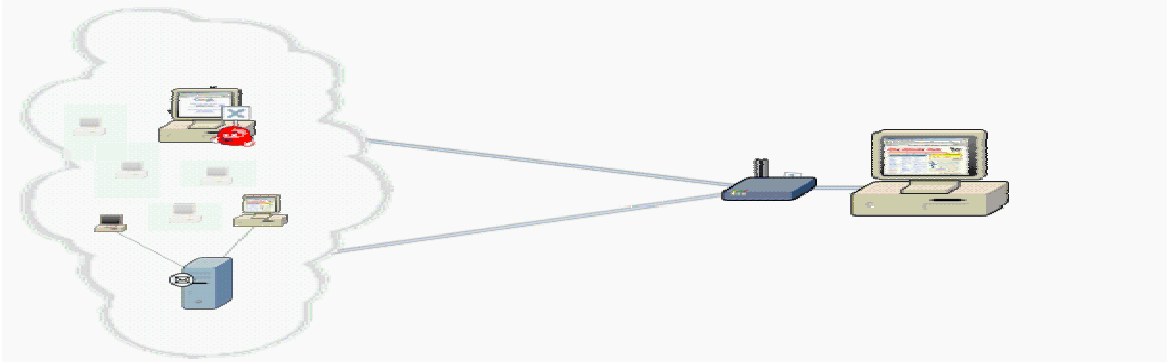
SOLUTION

Utilise en même temps un anti-virus et un firewall
L'anti-virus empêche qu'un virus infecte ton ordinateur Le firewall bloque les attaques des pirates

Pour assurer une sécurité maximale pour ton ordinateur, tu dois utiliser un firewall ET un anti-virus. Chacun est spécialisé dans son domaine et chacun fonctionne d'une manière différente pour protéger ton ordinateur contre différentes attaques.



Un **anti-virus** permet de protéger ton ordinateur contre les attaques de virus. Il agit comme un gardien qui inspecte chaque fichier de l'ordinateur pour essayer de savoir si un virus s'y cache. Si l'anti-virus détecte un virus caché dans un fichier, il essayera de l'enlever.



Un **firewall** permet de bloquer les attaques des pirates informatiques. Il agit comme une barrière autour de ton ordinateur qui bloque les attaques venant d'Internet.

question n° 16

SOLUTION

Un mot de passe c'est comme une brosse à dents :

- **On ne le prête pas**
- **On le choisit avec soin**
- **On le change régulièrement**

Le mot de passe est souvent le seul moyen pour protéger ton identité sur Internet. Plusieurs règles sont à suivre pour être sûr que personne ne pourra se faire passer pour toi :

- **On ne le prête pas.**

Ton mot de passe est personnel, c'est ton secret à toi

- Ne le donne à personne
- Ne l'écris pas sur un Post-It que tu pourrais coller sur ton écran d'ordinateur – c'est trop facile à lire
- Ne l'écris pas sur un papier que tu pourrais cacher sous ton clavier – c'est trop facile à trouver

- **On le choisit avec soin.**

- Choisis un mot de passe que personne ne pourra deviner
  - Ne le choisis pas à partir de ton nom
  - Ne le choisis pas à partir de ton prénom
  - Ne le choisis pas à partir de ta date de naissance
  - Ne le choisis pas à partir du nom de ton animal domestique
- Essaie de mélanger les lettres et les chiffres et si possible avec des signes de ponctuation
- Essaie de le faire le plus long possible. N'utilise pas de mots de passe de moins de 6 caractères

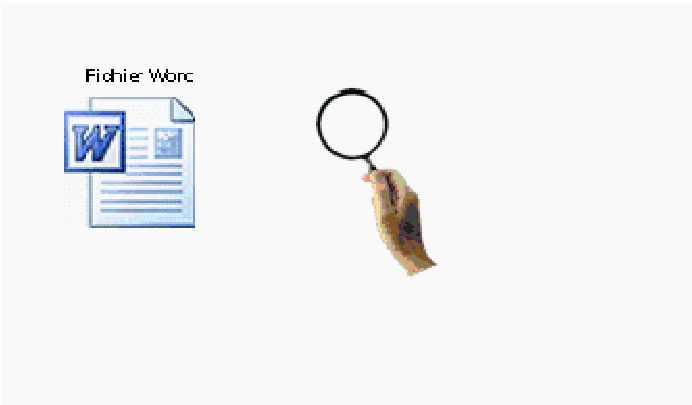
- **On le change régulièrement**

- Utilise un mot de passe différent pour chaque site sur lequel tu vas
- Essaie de changer tous tes mots de passe tous les 3 mois

question n° 17

SOLUTION

Un virus informatique est un programme qui peut se répandre d'ordinateur en ordinateur pour effacer des fichiers.

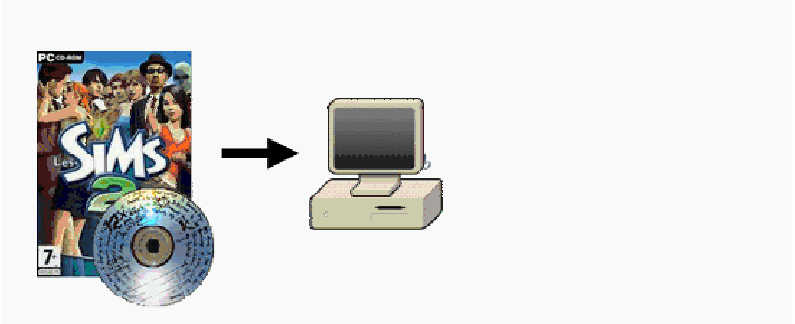


Un **virus informatique** est un programme qui s'attache sans que tu ne le saches à un fichier, comme un fichier Word, pour se répandre dans ton ordinateur. Dès que tu ouvres le fichier Word qui contient le virus, celui-ci se répand dans ton ordinateur et s'attache à d'autres fichiers Word.
Si à un moment tu envoies à un(e) ami(e) un fichier Word qui a été touché par le virus, l'ordinateur de ton ami(e) sera contaminé par le virus dès qu'il (elle) ouvrira le fichier.

question n° 18

SOLUTION

Installer un crack est interdit et en plus tu risques d'avoir encore d'autres problèmes ensuite.



Tout d'abord tu dois te souvenir qu'installer un crack pour un jeu est interdit par la loi. Rien que pour cela tu risques déjà de gros problèmes avec la police. Il faut de plus faire attention aux jeux vidéos gravés par un ami. Ils peuvent contenir des virus.

Le *crack* pouvait contenir un *cheval de Troie* qui aurait permis à un pirate informatique de prendre le contrôle à distance de ton ordinateur sans même que tu ne t'en rendes compte, on dit alors que ton ordinateur est devenu une *machine zombie*.
En prenant le contrôle de ton ordinateur, le pirate pouvait ensuite attaquer les sites Internet du Gouvernement en utilisant ton ordinateur. La police est venue chez toi car elle a vu que les attaques venaient de ton ordinateur.

C'est quoi la légende du cheval de Troie ?	*C'est quoi un cheval de Troie en informatique ?*
Dans la mythologie grecque, le cheval de Troie entre en scène lors de la guerre Troie. Après avoir vainement assiégé la ville de Troie, les Grecs ont l'idée d'une ruse pour prendre la ville : construire un cheval en bois géant. A l'intérieur de ce cheval se cachaient des soldats menés par Ulysse. S'étant laissée convaincre de laisser entrer ce cheval de bois dans l'enceinte de la ville en guise de cadeau, la cité de Troie organisa une grande fête, mais la nuit tombée, les Grecs sortirent de leur cachette pour prendre le contrôle de la cité.	A l'image de la légende avec le grand cheval de bois, un cheval de Troie en informatique est un programme qui semble à première vue inoffensif mais qui en réalité dissimule un programme malicieux qui s'installe en même temps que le programme inoffensif pour faire du mal à ton ordinateur.

Pour finir, rappelle-toi que tout le monde connecté à Internet est une cible intéressante pour les pirates. Les pirates ne sont pas seulement intéressés à attaquer les grandes entreprises, les banques ou les sites des gouvernements. Il y a plusieurs catégories de pirates informatiques :

- **Ceux qui s'attaquent à des sites Internet pour voler de l'argent, espionner ou simplement pour détruire** (on les nomme *crackers*).

Ces pirates cherchent par exemple à découvrir des numéros de cartes bancaires, d'installer des spywares pour espionner le comportement des internautes et en profiter pour voler des informations, comme leurs mots de passe ou bien font de la défiguration de sites web en modifiant les pages d'accueil ou effacent même des sites web entiers.
Ces pirates possèdent des réseaux de machines zombies et les utilisent pour lancer des attaques sans que l'on sache que c'est eux qui organisent tout cela.

- **Ceux qui s'attaquent à n'importe qui** (appeller *script-kiddies*).

Ce sont des gens, en général très jeunes, qui ne connaissent pas grand chose à l'informatique et qui utilisent des outils créés par des pirates expérimentés pour lancer des attaques au hasard.

- **Les pirates à chapeau blanc** (*white hat* ou *hackers*).

Ce sont les bons pirates, ils essaient de rentrer dans les ordinateurs ou trouver des failles dans les systèmes pour ensuite prévenir leur propriétaire et l'aider à sécuriser son ordinateur.

question n° 19

SOLUTION

N'ouvre jamais de fichiers douteux reçus par MSN.

Des virus utilisent MSN pour se propager d'ordinateur en ordinateur. Pour cela, ils envoient un fichier aux contacts MSN. Si tu cliques sur ce fichier, ton ordinateur sera infecté par ce virus. Bien souvent, le virus envoie le fichier sans que celui qui a l'ordinateur infecté ne s'en rende compte.
Il faut que tu agisses en te demandant pourquoi ton contact MSN t'envoit un tel fichier. Si tu penses qu'il n'aurait pas fait cela, alors tu dois ignorer ce fichier, surtout ne pas l'ouvrir et le supprimer si c'est possible.

question n° 20

SOLUTION

Pour aller sur Internet en toute tranquillité, demande à tes parents d'installer un contrôle parental.

Source :
http://lewebpedagogique.com/cdimatagots/tag/securite-sur-internet/