http://www.cite-sciences.fr/carrefour-numerique/ressources/tutoriel/virus/virus_home.swf

**Dia 01** **Meilleur Antivirus : Entre la chaise et le clavier, les mains !!!!!!!!!**

**Un virus** (dans un contexte médical) **est *un agent responsable d'une maladie infectieuse***, *de nature particulaire. Il a besoin d'infecter **une cellule hôte** pour utiliser sa machinerie : un virus est un **parasite**.*

**Dia 2** *Tout être vivant peut être infecté par un virus. Il existe **plusieurs types de virus** : Le virus de la grippe est un des plus connus…. Le virion pénètre une cellule hôte plus ou moins spécifique où il libère son contenu qui en s'activant **prend le pas sur les fonctions cellulaires normales**. Les virus peuvent entraîner plusieurs **effets néfastes**.*

**Dia 3** *Étant donné que les virus utilisent la machinerie cellulaire de l'hôte pour se reproduire à l'intérieur même de la cellule, il est **difficile de les éliminer sans tuer la cellule hôte**. Des médicaments antiviraux permettent cependant de perturber la réplication du virus.*

*Une autre approche est la vaccination qui permet de résister à l'infection.*

Dia 4 Et si **on a choisi ce terme en informatique**, c'est parce que c'est la même chose. Nous allons voir par la suite.

Dia 5 Un **virus informatique** est un **automate auto réplicatif** additionné de **code malveillant** (donc classifié comme logiciel malveillant), **conçu pour se propager** à d'autres ordinateurs **en s'insérant** dans des logiciels légitimes, appelés « **hôtes** ». Il existe des programmes capables de se copier tous seuls d'ordinateurs en ordinateurs, et dont la fonction est d'être nocifs. Il peut **perturber** plus ou moins gravement le fonctionnement de l'ordinateur infecté. Il peut **se répandre** à travers tout moyen d'échange de données numériques comme les réseaux informatiques (Internet) et les cédéroms, les clefs USB, etc.

Dia 6 On attribue **le terme** de « **virus informatique** » à l'informaticien et spécialiste en biologie moléculaire Leonard Adleman (1984).

Les virus informatiques ne doivent pas être confondus avec les vers informatiques, qui sont des programmes capables de se propager et de se dupliquer par leurs propres moyens sans contaminer de programme hôte. Au sens large, on utilise souvent et abusivement le mot *virus* pour désigner toute forme de logiciel malveillant.

Le nombre total de programmes malveillants connus est énorme, il en sorte tous les mois des milliers (tous types confondus). Cependant, le nombre de virus réellement en circulation serait inférieur à ce que les éditeurs de programmes

antivirus disent, **chaque éditeur** ayant intérêt à « **gonfler » (surestimer)** le nombre de virus qu'il détecte afin de stimuler la vente de son produit. La très grande majorité des virus **touche la plate-forme Windows**. Pourquoi Windows est plus touché que les autres ? Parce que c'est le système d'exploitation le plus vendu au monde entier, donc plus intéressant pour les malfaiteurs.

**Historique** **Dia 7** **Saviez-vous que le premier virus informatique a 40 ans? Il a été créé en 1971.**

Son nom était Creeper, en français liane grimpant, capable de se mettre partout !
A l'heure actuelle, des millions de virus différents seraient en circulation et ce nombre ne fait qu'augmenter.

**Différents types de virus** **Dia 8** **:**

**Concrètement, les virus informatique sont écrits par des informaticiens mal intentionnés.** Il y a donc au départ une volonté de **nuire** de la part d'un individu…**Un virus est programmé pour d'une part se reproduire, et d'autre part agir**

Le **virus classique** **est un morceau de programme, qui s'intègre dans un programme normal**. Chaque fois que **l'utilisateur exécute ce programme** « infecté », il active le virus qui en profite pour aller **s'intégrer dans d'autres programmes exécutables**. Il peut exécuter une action **prédéterminée**. Cette action peut aller d'un simple message anodin à la détérioration de certaines fonctions du système d'exploitation ou la détérioration de certains fichiers ou même la destruction complète de toutes les données de l'ordinateur. Vous comprenez maintenant pourquoi il faut faire des **sauvegardes** de votre système et de vos données sur un support externe, comme une clé USB, des DVD au un disque dur externe.

- Un **virus de boot** **s'installe dans un des secteurs de boot d'un périphérique de démarrage, disque dur. Il remplace un programme de démarrage** existant en copiant l'original ailleurs. **Quand il remplace un programme de démarrage existant, il agit comme un virus.**
  COMMENTAIRE (la cartouche)
- Les **macrovirus** **s'attaquent aux macros de logiciels de la suite Microsoft Office (Word, Excel, etc.) Les macrovirus utilisent un langage de**

**programmation d'un logiciel pour en altérer le fonctionnement**. Ils **s'attaquent principalement aux fichiers des utilisateurs.** Un virus peut être activé à chaque fois que l'utilisateur lance ce programme. Ces virus se propagent actuellement dans de fortes proportions et peuvent malheureusement causer de grands dégâts (formatage du disque dur par exemple, donc effacement de toutes les données). COMMENTAIRE (la barre en haut)

- **Les virus-vers sont des virus classiques car ils ont un programme hôte. Mais s'apparentent aux vers car :**
  - Leur mode de **propagation** est lié au **réseau**, comme des vers, en général via l'exploitation de failles de sécurité.
  - Comme des vers, leur action se veut **discrète**, et non-destructrice pour les utilisateurs de la machine infectée.

D'autres menaces existent en informatique, s'en distinguant souvent par l'absence de système de reproduction qui caractérise les virus et les vers ; le terme de « **logiciel malveillant » (« *malware* » en anglais)** est dans ce cas plus approprié. Un **logiciel malveillant est un programme développé dans le but de nuire à un système informatique, sans le consentement de l'utilisateur infecté. De nos jours, le terme *virus* est souvent employé, à tort, pour désigner toutes sortes de logiciels malveillants. En effet, les malwares englobent les virus, les vers, les chevaux de Troie, ainsi que d'autres menaces.**
Le terme *Logiciel malveillant*, dont l'usage est préconisé par la commission générale de terminologie et de néologie en France, est donc une traduction du mot anglais ***malware*, qui est une contraction de *malicious* (qui signifie *malveillant*, et non *malicieux*) et *software* (*logiciel*).** Dans les pays francophones, l'utilisation de l'anglicisme *malware* est le plus répandu.
COMMENTAIRE (« Gendarmerie »)
**Glossaire Dia 8**

**Malware Il désigne tout type de programme nocif introduit sur un ordinateur à l'insu de l'utilisateur. Il regroupe les virus, vers, spywares, keyloggers, chevaux de Troie, backdoors... on en parlera toute à l'heure.**

**Spyware Contraction de spy et software. Logiciel espion qui collecte des données personnelles avant de les envoyer à un tiers, comme transmettre les données saisies grâce au clavier par exemple.**

**Backdoor (porte dérobée) Point (port) d'accès confidentiel à un système d'exploitation, à un programme ou à un service en ligne. Ces passages secrets sont ménagés par les concepteurs des logiciels pour fournir des accès privilégiés pour les tests ou la maintenance de l'ordinateur comme les mises à jour. Mais les pirates qui les découvrent peuvent déjouer tous les mécanismes de sécurité et rentrer dans le système.**
**Backdoor désigne également des petits programmes installés dans l'ordinateur à l'insu de l'utilisateur (généralement par des vers), et qui donnent accès au contrôle de l'ordinateur par des pirates.**

**Keylogger (key : touche) Un keylogger est un type de spyware spécialisé pour espionner les frappes sur les touches du clavier sur l'ordinateur qui l'héberge, et pour les transmettre via internet à une adresse où un pirate pourra les exploiter.**

**Un keylogger peut donc recueillir et transmettre vos mots de passe, code de carte bancaire, identifiant sous lequel vous ouvrez une session...**

**Cheval de Troie** Initialement un cheval de Troie désignait un programme se présentant comme un programme normal destiné à remplir une tâche donnée, voire ayant parfois un nom connu , mais qui une fois installé exerçait une action nocive totalement différente de sa fonction "officielle", **en quelque sorte "déguisé" sous une fausse apparence**, comme dans ce petit rappel de la **mythologie grecque** :La guerre de Troie est un conflit légendaire provoqué par l'enlèvement d'Hélène, reine de Sparte, par le prince troyen Pâris.
Après avoir vainement assiégé Troie pendant dix ans, les Grecs ont l'idée d'une ruse pour prendre la ville : Ils construisent un cheval géant en bois creux pour donner en cadeau aux Troyens, mais dans lequel **se cachent** des soldats menés par Ulysse. Un **espion** grec, appelé Sinon, réussit à convaincre les Troyens **d'accepter** l'offrande, **malgré les avertissements** de Laocoon et de Cassandre. Le cheval est tiré dans l'enceinte de la cité qui fait alors une grande fête. Lorsque les habitants sont pris par la torpeur de l'alcool, la nuit, **les Grecs sortent du cheval et ouvrent alors les portes, permettant au reste de l'armée d'entrer** et de piller la ville. Tous les hommes sont tués, les femmes et les filles sont emmenées comme esclaves. Les enfants mâles sont tués eux aussi pour éviter une éventuelle vengeance.

**Actuellement le terme Cheval de Troie désigne à peu près tout programme qui s'installe de façon frauduleuse.**
**La distinction entre cheval de Troie, spyware, keylogger, porte dérobée n'est donc souvent qu'une question de mot ou de contexte.**

**autres définitions :**

**Ver**

**Programmes souvent confondus avec les virus. Mais, à la différence de ceux-ci, ils sont autonomes sur le disque dur au lieu de parasiter les fichiers existants. Ils n'ont pas besoin de cellule hôte.**
**En informatique un ver est un programme nocif qui diffère des virus par plusieurs points.**
**Tout d'abord le ver est donc un programme autonome.**
**Un ver peut arriver directement par le réseau en profitant d'un port ouvert, ou sous la forme d'une pièce jointe attachée à un mail.**
**Un ver ne se multiplie pas localement, contrairement aux virus.**
**Les vers installent généralement sur l'ordinateur d'autres programmes nocifs.**

**Dia 9 petit résumé Virologie**

**Le terme virus informatique a été créé par analogie avec le virus en biologie** : un virus informatique utilise son hôte (l'ordinateur qu'il infecte) pour se reproduire et se transmettre à d'autres ordinateurs.

Comme pour les virus biologiques, pour lesquels ce sont les hôtes les plus en contact avec d'autres hôtes qui augmentent les chances de développement d'un virus, en informatique ce sont les systèmes et logiciels les plus répandus qui sont **les plus atteints par les virus :** Microsoft **Windows**, Microsoft **Office**, Microsoft **Outlook**, Microsoft **Internet Explorer**, ….

**La banalisation de l'accès à Internet a été un facteur majeur dans la rapidité de propagation à grande échelle des virus les plus récents. Ceci est notamment dû à la faculté des virus de s'approprier des adresses des emails présentes sur la machine infectée (dans le carnet d'adresses mais aussi dans les messages reçus ou dans les archives de pages web visitées ou de messages de groupes de discussions).**

**De même, l'interconnexion des ordinateurs en réseaux locaux a amplifié la faculté de propagation des virus qui trouvent de cette manière plus de cibles potentielles. Et de nouveau, j'insiste, le meilleur antivirus c'est vous-même en faisant très attention sur certains sites internet comme Kazaa, Bittorrent, E-mule, PTP, Shareaza, Skype, Facebook, Messenger etc. …**

**Et de nouveau : Le meilleur antivirus c'est vous-même. COMMENTAIRE**

**Comment mon ordinateur peut-il contracter un virus?**

**Les virus se propagent dans votre ordinateur quand vous lancez des logiciels infectés. Étant donné que les virus se reproduisent sur le code des autres programmes, ils sont inoffensifs jusqu'à ce que vous lanciez le programme infecté. En d'autres mots, télécharger un programme infecté d'un site Web ou insérer un CD ou clé USB dans votre ordinateur est inoffensif, jusqu'à ce que vous démarriez un logiciel ou que vous ouvriez un fichier infecté.**

**Vous pouvez contracter un virus à partir d'un fichier joint à un message électronique, si ce document est un logiciel ou un type de fichier susceptible d'être infecté, comme c'est le cas pour les fichiers Word ou Excel. Mais pour que votre ordinateur soit infecté, vous devez au préalable lancer le logiciel ou le fichier joint.**

**Dia 10 Analysez les fichiers téléchargés avant de les ouvrir, surtout les fichiers xxxx.exe. On en reparlera toute à l'heure. Déjà votre FAI et votre programme Antivirus font des analyses.**

**Dia 11 Ordinateur infiltré** : **et effets :** aller sur dia 12 :

**Dia 12 lien pour animation Flash** clic sur Animation Flash dans la diapositive

http://www.cite-sciences.fr/carrefour-numerique/ressources/tutoriel/virus/virus_home.swf

**Dia 13 Autres ennuis Hoax :**

**Les Hoax sont des canulars de toutes sortes que vous recevez par e-mail et qui parfois vous demande de supprimer certaines choses sur votre ordinateur qui soi-disant serais infectées, ne le fait pas : Renseignez-vous auprès de nous et ne les transférez jamais à vos contact. COMMENTAIRE** (torche brulante etc.)

**Logiciels antivirus** **Dia 14** **Comment se protéger des virus : Le meilleur antivirus, mieux que Norton, Kaspersky, Avast se trouve** ***Entre la chaise et le clavier***

**Les logiciels antivirus sont des logiciels capables de détecter des virus, détruire, mettre en quarantaine et parfois de réparer les fichiers infectés sans les endommager.**

**Dia 15 Logiciel antivirus Payant ou Gratuit et En ligne, comme MalwareByte**

**Dia 16 Différences entre un antivirus gratuit ou payant (exemple d'Avast)**

**Dia 17 Les logos des mises à jour Windows de Microsoft. Adobe. Java. (Icônes)**

**Dia 18 Décochez le toolbar (barre d'outils) Ask de Java. Ne remplacez pas Google par Ask.**

**Dia 19 Exemple Interface Avast Gratuit. Différence entre mettre à niveau et mise à jour.**

**Dia 20 Scanner**

**Faites travailler votre antivirus en effectuant régulièrement des scans approfondis, que vous pourriez programmer dans votre programme antivirus.**

**Et n'oubliez jamais, que le meilleur antivirus c'est vous-même, en évitant les pièges, en freinant vos clics, en se méfiant de tout ce qui est (parfois piraté) sur les CD et les clés USB des copains, qu'il faut toujours analyser avant de faire des copies sur votre ordinateur et avant de les ouvrir.**

**Dia 21 Comment analyser un fichier téléchargé ? En faisant un clic droit dessus et dans le menu contextuel qui s'ouvre faire un clic gauche sur Analyser**

**Dia 22 Conclusion :**

- **Ayez un antivirus (gratuit ou payant)**
- **Vérifiez qu'il soit à jour**
- **Scannez régulièrement de manière approfondie**
- **Surveillez de près votre index (c'est souvent lui le responsable de tous vos ennuis)**