Le téléchargement, c’est quoi ? Ça marche comment ?

Le téléchargement, tout le monde en parle mais beaucoup oublient le véritable sens du terme. Que vous pensiez être incollable sur ce thème ou au contraire si le téléchargement est quelque chose de très vague pour vous et bien cette info vous est destiné !

Wikipédia est habituellement un outil redoutable, mais cette fois, sa réponse ne répond pas totalement aux attentes et laisse quelque peu perplexe.

En informatique, le téléchargement est l'opération de transmission d'informations, programmes, données, images, sons, vidéos d'un ordinateur à un autre par le biais d'un canal de transmission, en général l'internet ou un intranet.

En télécommunications, le téléchargement est l'opération d'échange de données numériques entre un client et un serveur.

De nos jours, la notion de téléchargement est très maladroitement associée, par abus de langage, uniquement aux téléchargements de fichiers stockés sur disque dur, après un passage par la mémoire vive des ordinateurs.

Le téléchargement c'est donc un échange de données entre plusieurs appareils par un canal de transmission, mais quel canal ?

Pour télécharger, on peut utiliser un canal **« physique »**, comme un câble USB, Ethernet, fibre optique ou autres. Les données vont circuler entre les appareils par les câbles qui les relient.

Ensuite, on retrouve le téléchargement **« dans l'air »,** on échange des données par des ondes tel que le **Bluetooth** ou encore **l'infrarouge**, mais aussi le **WiFi**.

Et concernant la radio dans la voiture peut-on parler de téléchargement ?

Oui, il y a échange de données par un canal de transmission donc on peut parler de téléchargement !

Et pour terminer le téléchargement **« par internet »,** c'est un cas un peu complexe, sachez que quand un internaute surf sur le web, le navigateur (Mozilla Firefox, safari, Google chrome, Edge, …) télécharge du texte et des images, pour les afficher sous forme de pages web depuis le serveur ou est hébergé le site web.

Donc finalement, le simple fait d'utiliser internet est apparenté à du téléchargement.

Sur Internet, il existe de nombreuses autres formes de téléchargements,

Le téléchargement direct ou en anglais, « **direct download** », qui est un téléchargement depuis un serveur vers vous, le client.

C'est le type de téléchargement le plus utilisé, la navigation sur internet est du téléchargement direct, car les pages affichées sont préalablement téléchargées sur le serveur.

Mais aussi la lecture en continu, en anglais **« streaming »**, qui est une application moderne du téléchargement. Toujours en passant par un serveur, visualiser une vidéo depuis un site internet est une forme de téléchargement.

Tout comme le pair à pair, en anglais « **peer-to-peer (P2P) »,** échange de données entre plusieurs ordinateurs qui ont un double rôle de clients et de serveurs.

Le concept, d'abord télécharger de l'information (**vous êtes alors le client**), puis dans un second temps la partager avec les autres membres connectés qui souhaitent la consulter (**vous devenez le serveur**).

Quels sont les deux sens de téléchargements ?

On trouve, le téléchargement en sens descendant (en anglais **download**), correspondant à la réception de données par le réseau, appelé par abus de langage **«téléchargement».** C'est le cas quand vous êtes client et que vous recevez des informations depuis un serveur.

Et le téléchargement en sens montant (en anglais **upload),** et en français, **téléversement**, correspondant à un envoi de données vers le serveur par le réseau.

Quand un site web est interactif, le fait de cliquer sur un bouton va générer une action et provoquer un **téléversement** de cette action vers le serveur.

Ce qu’il faut retenir

Le mot téléchargement est quotidiennement déformé de sa signification première, qui est, l’échange de données entre plusieurs appareils via un canal de communication.

Ce canal peut être l’air et donc les ondes, le cuivre ou le verre pour la fibre optique, mais aussi internet qui est aujourd’hui le canal le plus emprunté.

Il existe deux sens de circulation de l’échange, la réception appelée par abus de langage **téléchargement**, et l’envoie appelé **téléversement**.

Dans la pratique

Le Téléchargement ….est une opération à risques pour ne pas dire à hauts risques si vous êtes mal protégés.

Le Téléchargement

➢ d’un logiciel

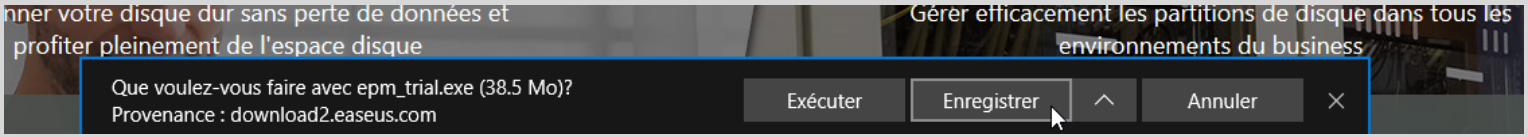
C’est transférer tous les composants d’un « outil » à un emplacement précis de votre ordinateur.

Avant de télécharger un logiciel (gratuit ou payant), vous assurer qu’il est compatible avec votre système d’exploitation.

Dans le cas de « gratuits », surveillez bien les fenêtres, les messages affichés, les boîtes à cocher/décocher et réagissez en conséquence.

Dans une moindre mesure, même chose dans le cas de logiciels « payants » pour lesquels un n° de licence vous sera demandé.

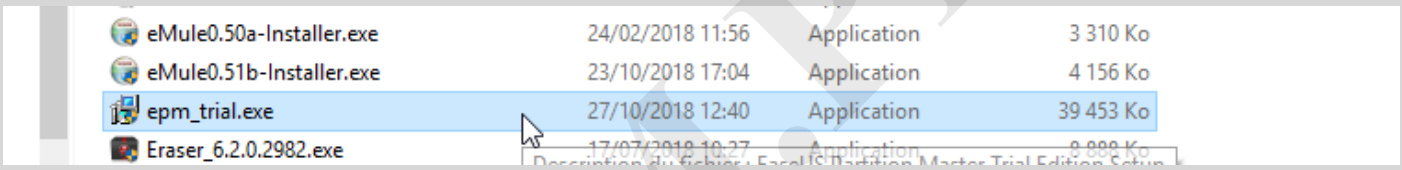
Au moment du téléchargement, c’est à vous de déterminer l’endroit où le logiciel doit être téléchargé –à défaut il ira dans la zone de téléchargement de windows.



ATTENTION ! télécharger ne veut pas dire « **installer** » ! par comparaison, télécharger c’est livrer mais ensuite il faut installer.

Un logiciel aura l'extension « .**exe** » même si il a été téléchargé compressé c'est-à-dire « .zip ». La décompression affichera le « .exe ».

Pour « **installer** » sur votre ordinateur un outil préalablement téléchargé, il faudra lancer l'exécutable « **.exe** » par un double clic dessus.



Pendant l'installation vous devrez répondre à un certain nombre de questions par oui ou non ou en cochant/décochant des cases.

L'installation terminée, vous pourrez utiliser le logiciel en cliquant sur son raccourci

➢ d'un document

C'est le transférer à un emplacement précis de votre ordinateur pour pouvoir être utilisé par la suite, dans la mesure où vous possédez les logiciels pour pouvoir les ouvrir.

Un document téléchargé prendra généralement l'extension « .pdf », « .jpg », « .gif », « .doc », « .docx », « .xls », « .xlsx », « .pptx », etc..

ATTENTION !

Méfiez-vous des virus dans les documents Word, Excel….

Vous le savez peut-être déjà : les virus informatiques ressemblent à de petits programmes logiciels.
Ils sont généralement téléchargés par inadvertance, cachés au sein de fichiers.
Lorsque vous ouvrez un fichier contaminé, le virus s'active.

Le virus peut endommager votre système, voler vos données d'identification, infecter les fichiers que vous envoyez ou même se propager à votre carnet d'adresses avec votre adresse comme adresse d'expédition.

Mais ce que vous ne savez peut-être pas, c'est que les virus s'introduisent par le biais de fichiers Microsoft Word, Excel, PowerPoint, Access, Outloock que vous recevez fréquemment par courrier électronique.

Les virus peuvent également **utiliser vos propres documents** pour causer des ravages sur votre ordinateur.

Les virus informatiques et les autres formes de logiciels malveillants occasionnent des milliards de dollars de dégâts chaque année et de terribles angoisses aux victimes de vol d'identité.

Il vous est déjà certainement arrivé d'entendre que de simples documents (comme Excel, Word ou autres**) ne pouvaient pas être infectés**.

C'est faux !

Il existe des virus que l'on appelle **macrovirus** et qui sont capables d'infecter un simple et banal document texte (comme Excel, Word, Word Pad).

La grande cible des macrovirus sont les produits de Microsoft comme Word, Excel, Access, PowerPoint et Outlook.

Q. Pourquoi ces fichiers sont-ils vulnérables ?

R. Les fichiers Microsoft faisant très souvent l'objet d'échanges, les virus sont devenus monnaie courante. Voici le principe de fonctionnement :

- Les fichiers Microsoft contiennent de petits programmes appelés "macros". Ce sont des raccourcis personnalisables qui automatisent certaines tâches, comme la mise en forme de texte ou l'insertion de listes à puces.
- Le langage de programmation des macros peut également être utilisé pour écrire des virus.
- Un virus peut être introduit dans un document.
- Il s'active automatiquement dès que vous ouvrez le fichier.

Q. Quelles en sont les conséquences ?

R. Les virus macros s'accrochent à tous les documents sauvegardés et passent d'un utilisateur à l'autre par e-mail ou selon la bonne vieille méthode : en passant par la clé USB !

Les logiciels de bureautique incluent des macros commandes dont le but est de simplifier les tâches des utilisateurs.

Les virus macros sont capables d'interrompre les actions d'enregistrement de fichiers, de contrôler le stockage des données, de manipuler des informations, de détruire des données et même d'effectuer des formatages de disque !

Imaginez les conséquences que cela peut avoir quand ces types de documents infectés circulent !

Il faut savoir qu'un document non infecté au départ peut le devenir au cours de son acheminement

Certains virus macros prennent le contrôle des logiciels de messagerie ou d'e-mail, piratant ainsi votre carnet d'adresses

Q. Comment les pirates nous incitent-ils à ouvrir un fichier Word contaminé ?

R. Les pirates utilisent de nombreuses ruses pour vous persuader d'ouvrir un fichier infecté par un virus. Leurs tactiques sont les suivantes :

- Usurper l'adresse d'un ami, d'une entreprise ou d'une ancienne connaissance.
- Prétendre qu'il s'agit d'un message important de votre banque, des impôts ou de la loterie nationale.
- Profiter de sujets d'actualité. Par exemple, demandes de soutien à une cause.

Q. Comment se protéger ?

R. Voici quelques conseils pour éviter les virus dans les documents Microsoft :

- Ouvrez uniquement les pièces jointes attendues et envoyées par un expéditeur de confiance *(et encore !).*
- Utilisez un logiciel de sécurité Internet qui analyse et détecte automatiquement les virus et autres programmes malveillants contenus dans les pièces jointes aux messages avant qu'elles ne soient ouvertes.
- Supprimez les messages suspects sans les ouvrir.
- Ne cliquez pas sur les liens Web et ne téléchargez pas les fichiers envoyés via des messages électroniques ou instantanés par des personnes que vous ne connaissez pas.

La règle de base :

Se méfier des fichiers joints aux messages, même s'il s'agit de fichiers Word, Excel, etc.., apparemment inoffensifs.

Ces fichiers peuvent contenir des virus ou d'autres programmes malveillants qui peuvent endommager votre système ou vous dérober des informations personnelles et se propager à la vitesse de l'éclair vers vos contacts.

Utilisez toujours des logiciels de sécurité Internet pour vous protéger contre les virus, les logiciels espions et le spam.

Tous les documents sont potentiellement dangereux car c'est à travers eux que peuvent circuler et se propager les virus.

Si vous n'êtes pas sûr de la provenance soyez prudent.

Soyez aussi prudent lors de vos envois (téléversement) notamment à travers les mails.

Par principe, ne transférez jamais de documents de type « .doc », « .docx », « .xls », « .xlsx », « .pptx » via des mails ou autres, sauf à être certain de leur origine et de leur destination.

Convertissez-les en « .PDF » et les transférer sous ce format.