« La meilleure protection...
...c'est la connaissance »

Le mini guide de la sécurité Internet

Comment vous protéger des menaces d'Internet

http://formation-informatique-avec-cedric.fr

DATE DE MISE A JOUR DE CET EBOOK : **09 NOVEMBRE 2017** – VERSION : **4.0**

Les logiciels malveillants

Pourquoi est-ce la nouvelle plaie d'Internet ?

Les logiciels malveillants sont aujourd'hui très présents sur internet.
La plupart d'entre eux ne sont pas trop virulents mais ils envahissent votre système et pénalisent énormément l'utilisation de votre ordinateur. L'inconvenient majeur de ces nuisibles est qu'ils sont souvent nombreux et difficiles à supprimer.

Quels sont les symptômes

- Pages de publicités intempestives en permanence
- Faux logiciels ou solutions miracles où l'on vous demande de payer
- Modifications des différentes pages d'accueil de vos navigateurs Internet
- Présence de nombreuses barres d'outils
- Ralentissement important de l'ordinateur
- Bloquage de votre accès à Internet

Comment on les attrape

- En installant toutes sortes de logiciels : ils s'immiscent sournoisement
- En fréquentant des sites "dangereux" avec un ordinateur non à jour
- En regardant des films illégaux en streaming sur Internet
- En effectuant de fausses mises à jour qui semblent légitimes
- En téléchargeant de la musique, des films... sur les réseaux de partage
- En laissant vos enfants installer les logiciels eux-mêmes
- En installant des emoticons pour Facebook, Windows live etc.

Comment s'en protéger

La vigilance est la base de votre défense contre ces intrusions. En effet, ces logiciels malveillants s'infiltrent dans votre ordinateur car vous les avez souvent invités, même si vous n'en êtes pas conscient.

Attention, lorsque vous téléchargez un logiciel gratuit, vous pensez qu'il va s'installer seul, mais souvent plusieurs programmes parasites additionnels (et subventionnés) viennent polluer votre système si vous ne faites pas attention. Nous pouvons citer en exemple la barre d'outils "Ask" qui s'installe si vous ne décochez pas la case adéquate lors de la mise à jour de "Java".

Evitez également de réaliser des téléchargements sur les réseaux de partage, vous vous exposez fortement aux ennuis. Les programmes que vous utilisez sont autant de portes d'entrées pour les logiciels malveillants. Alors : Soyez vigilants !

Quelle est la solution de Cédric

Si malgré les conseils que je vous ai donné sur cette page, vous avez quand même été infectés et présentez les symptômes décrits ici : n'hesitez pas à utiliser notre guide pratique au format PDF (Ebook) pour Windows XP, Vista, 7 et 8. Il vous permettra en 1 heure de retrouver un PC rapide et sain. Fini les publicités intempestives et les logiciels inutiles, parasites, malveillants...

Pour en savoir plus sur ce guide indispensable visitez mon site

Les virus et chevaux de Troie

Qu'en est-il vraiment de cette menace ?

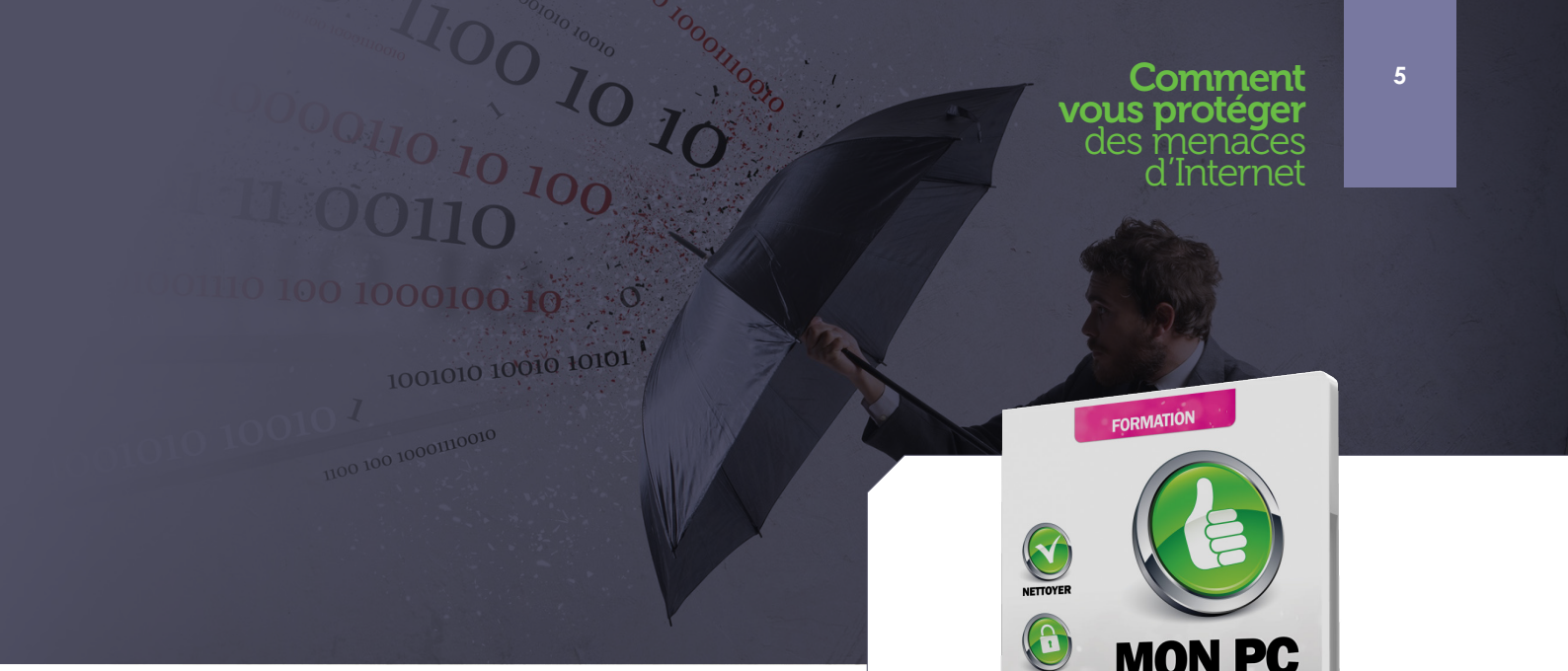
Les virus ne sont plus ce qu'ils étaient, tant en nombre qu'en agressivité.
Il serait faux de dire qu'ils n'existent plus, mais ils sont quand même rares. Les antivirus gratuits font du très bon travail. Ils permettent aujourd'hui pour un particulier de se passer de versions payantes malgré ce que l'on veut vous faire croire.

Quels sont les symptômes

- Votre système est lent et cesse de répondre
- Votre ordinateur redémarre intempestivement
- Vos logiciels ne fonctionnent pas normalement
- Il vous est impossible d'accéder à votre disque dur ou clés usb
- Votre logiciel antivirus ne veut plus s'exécuter ou est introuvable
- Des boîtes de dialogue apparaissent à l'écran de façon inhabituelle

Comment on les attrape

- Par l'intermédiaire d'une clé usb ou tout autre support infecté
- Par l'intermédiaire d'un lien ou d'une pièce jointe dans un email
- En ouvrant une photo ou tout autre fichier contaminé
- Par le biais de votre navigateur et de ses extensions
- En naviguant sur des sites Internet infectés
- En téléchargeant des logiciels parasités
- En accédant à une ressource partagée sur un réseau



Comment s'en protéger

La première chose à faire est d'installer un antivirus, gratuit ! En effet les performances des logiciels distribués aujourd'hui sont suffisantes pour assurer une protection de qualité et bloquer la majorité des contaminations.

La seconde étape est l'application systématique des mises à jour de votre système et de vos applications, particulièrement de Java et Flash Player. Ceci est indispensable afin de colmater les failles de sécurité connues.

Si des amis vous prêtent des clés usb, analysez en premier lieu le contenu avec votre antivirus pour être sûr qu'elles ne soient pas infectées.

Enfin, téléchargez uniquement ce qui vous est utile et seulement si vous êtes sûr de l'origine. Evidemment, évitez les logiciels contrefaits qui sont sources de problèmes.

Quelle est la solution de Cédric

Une bonne protection passe avant tout par la connaissance et la prévention. Avec les conseils que je vous prodigue dans ce mini guide vous avez déjà une bonne idée de comment vous protéger des virus. Si vous voulez allez plus loin nous avons mis au point une formation qui vous explique en vidéos quel antivirus gratuit choisir et beaucoup, beaucoup d'autre choses.

Apprenez les gestes essentiels pour protéger votre ordinateur et bien plus

L'hameçonnage (ou «Phishing»)

Ne prenez pas cette menace à la légère.

De nombreuses personnes succombent bien malgré elles à ce fléau.
L'hameconnage est la menace sournoise de l'Internet et du mail. Elle n'a pas forcément de conséquences directes et visibles sur votre ordinateur, mais elle peut se révéler catastrophique en donnant accès à vos données personnelles aux pirates.

Quels sont les symptômes

- L'hameçonnage est une forme de piratage par mail ou par le biais d'une page Internet qui consiste à tenter de récupérer vos informations personnelles par l'intermédiaire d'un formulaire à remplir ou d'un lien à cliquer.

  Les conséquences ne sont pas forcement immédiates et vous pouvez vous aperçevoir de l'escroquerie des semaines voire des mois plus tard.

Comment on l'attrape

- Par l'intermédiaire d'un lien dans un email frauduleux
- En naviguant sur un site internet illégitime usurpant le site officiel
- En répondant à une petite annonce trop alléchante (Le Bon Coin, Vivastreet...)
- Au travers d'une fausse mise à jour qui vous demande vos informations
- Sur les sites de rencontres où l'on vous promet monts et merveilles

Comment s'en protéger

La première chose à savoir, c'est qu'aucun organisme, ne vous demandera directement vos informations confidentielles par mail (nom d'utilisateur, mot de passe, numéro de carte bancaire).

Ne cliquez jamais sur un lien suspect dans un mail, si vous avez le moindre doute. C'est justement le principe du Phishing, vous faire croire qu'il s'agit d'un courriel légitime et officiel.

Rendez-vous toujours directement sur le site internet de l'organisme vous demandant des informations personnelles. En cas de doute, privilégiez un contact téléphonique. D'une manière générale ne communiquez pas vos coordonnées à des personnes tierces qui ne sont pas de confiance.

Ne succombez pas aux annonces trop attractives car les bonnes affaires existent, mais les miracles rarement.

Conseils supplémentaires

Que dois-je savoir de plus sur la sécurité ?

La sécurité informatique implique bon nombre de domaines.
Mots de passe, paiements sur Internet, Wi-Fi des box, réseaux sociaux... Découvrez ci-dessous nos conseils sur la conduite à tenir pour éviter les principaux pièges auxquels vous pouvez être confrontés.

Les mots de passe

Les mots de passe sont omniprésents sur Internet. Que vous souhaitiez souscrire un service de messagerie, le consulter, regarder vos comptes ou encore interagir avec d'autres personnes sur des forums de discussion, vous allez être obligé de vous identifier.

Vous aurez donc besoin de ce que l'on appelle un "nom d'utilisateur" ou "identifiant" et d'un mot de passe.

Nous vous conseillons de choisir des mots de passe différents pour chaque service que vous allez souscrire afin de cloisonner les risques. Il peut être également judicieux de stocker ces derniers en lieu sûr.

Un bon mot de passe est composé de chiffres, de lettres, de majuscules, de minuscules, de caracères spéciaux (+,-, @,#...) et comporte au minimum 8 caractères.

Payer sur Internet

Payer sur Internet est un choix que certains ne feront jamais. C'est effectivement le meilleur moyen d'éviter les nombreuses escroqueries qui sévissent sur la toile.

Même si les sites marchands se sont beaucoup améliorés ces dernières années, si vous devez acheter sur Internet, respectez les règles suivantes afin de vous assurer un minimum de sécurité :

- N'achetez que sur des sites de confiance ou de grandes enseignes.
- Assurez-vous de la présence d'un cadenas ou de "https://" dans la barre d'adresse de votre navigateur avant de saisir vos diverses coordonnées.
- Profitez du service e-carte bleue fourni par votre banque qui garanti une sécurité élevée.
- Utilisez Paypal qui est un partenaire reconnu et fiable.

Le Wi-fi des Box

Toutes les Box sont aujourd'hui équipées du Wi-fi. Cela permet à vos appareils de se connetcter à Internet sans fil (mobiles, ordinateurs, tablettes, ou encore imprimantes Wi-fi).

Pourquoi cela peut-il être problématique ? Tout d'abord car aux yeux de la justice, vous êtes responsable de votre connexion Internet et de votre réseau Wi-Fi. De ce fait, si une personne pirate votre connexion et télécharge des contenus illégaux, c'est vous qui serez responsable, même si vous n'étiez pas au courant.

Attention également si quelqu'un de mal intentionné accède à votre réseau sans fil, celle-ci pourrait être en mesure de pirater vos données.

Nous vous conseillons donc sur votre Box de mettre un mot de passe solide ou de désactiver le Wi-Fi, si vous ne l'utilisez pas.

Les réseaux sociaux

Les réseaux sociaux sont aujourd'hui incontournables : Facebook, Twitter, Pinterest etc... Attention, une utilisation non maîtrisée peut se révéler préjudiciable.

Loin de nous l'idée de diaboliser ces mêmes réseaux, mais vous devez être vigilant quant aux informations que vous diffusées car votre avenir professionnel ou celui de vos enfants peut en dépendre.

Une critique, une photo, tout cela se partage et se propage à la vitesse de l'éclair sur la toile et peut très facilement entâcher votre e-réputation.

Un conseil supplémentaire : ne transmettez jamais vos mots de passe et données personnelles sur les réseaux sociaux.

Soyez très vigilant pour vous et vos proches.

Dernières recommandations

Lorsque vous êtes loin de votre ordinateur

Vous devez également faire attention lorsque vous n'êtes pas devant votre clavier. Que ce soit pour une utilisation ponctuelle d'Internet chez des amis, dans un cyber café, avec votre téléphone ou que vous laissiez vos proches accéder à votre ordinateur, mettez en pratique nos conseils.

Internet à l'extérieur

Lors d'une utilisation d'Internet à l'extérieur de votre domicile, vous êtes beaucoup plus exposé aux dangers du piratage ou à une erreur d'inattention qui peut être fatale.

En effet, bien que la majorité des réseaux Wi-Fi sur lesquels vous vous connectés soient cryptés, il n'est pas forcément difficile de récupérer vos données lorsque vous "surfez" sur ceux-ci.

Utilisez donc au minimum ces réseaux pour accéder à vos données sensibles : messageries, shopping sur internet, accès à vos comptes bancaires.

Si vous devez naviguez dans des cybercafés, au bureau ou chez des amis, pensez à supprimer l'historique des navigateurs, effacer les cookies et les mots de passe enregistrés et déconnectez-vous des différents services que vous avez utilisés.

Le contrôle parental

Le contrôle parental devrait être surtout utilisé pour les plus jeunes. En effet sur Internet, on peut rapidement être confronté à des contenus violents, voire choquants mais également récupérer bon nombres de logiciels malveillants.

L'installation d'un logiciel de contrôle parental va vous permettre de :

- Maîtriser les sites pouvant être visités.
- Empêcher l'installation de logiciels.
- Spécifier des plages horaires d'utilisation.
- Interdire l'execution de jeux, programmes ou messagerie instantannée.
- Bloquer certains mots clés par l'intermédiaire de listes noires.
- Historiser les sites visités

Nous vous conseillons donc de mettre en place ce type de logiciel afin de vous garantir une protection supplémentaire.

La fin de Windows XP

Depuis le 8 avril 2014 : C'est fini

Voici quelques règles pour tenter de survivre avec XP

Nous ne pouvions pas faire ce guide sur la sécurité Internet sans parler du cas de Windows XP. En effet, depuis le 8 avril 2014, Microsoft ne prend plus en charge les mises à jour de ce système d'exploitation.

Cet événement peut avoir de très fâcheuses répercutions sur le fonctionnement de votre ordinateur si vous utilisez encore Windows XP.

Votre système est vulnérable, vos données risquent de ne plus être sécurisées, les virus et logiciels malveillants vous infecteront plus facilement....

N'hésitez pas à appliquer les 8 règles suivantes :

- **Règle #1** : Sauvegardez vos données
- **Règle #2** : Installez un antivirus gratuit. (Inutile d'engager des frais supplémentaires).
- **Règle #3** : Utilisez un navigateur moderne (Google Chrome ou Mozilla Firefox).
- **Règle #4** : Mettez vos programmes à jour (Java, Flashplayer, Acrobat reader...).
- **Règle #5** : Soyez encore plus prudent quant aux sites que vous visitez.
- **Règle #6** : Evitez d'installer des logiciels.
- **Règle #7** : Désinstallez toutes les versions de Java (Si vous ne l'utilisez pas).
- **Règle #8** : Déconnectez vous d'Internet et préparez-vous au changement de votre système.

Envie d'aller plus loin ?

Comment me joindre et me rejoindre

Partager c'est aider

N'hésitez pas un seul instant à partager ce guide et son contenu autour de vous, car **«la meilleure protection...c'est la connaissance»**

Grâce à ce mini guide vous connaîssez les bons gestes à adopter sur Internet et vous savez comment vous comporter face aux menaces et aux arnaques diverses.

Joindre ou rejoindre

- **Sur mon site internet**
  http://formation-informatique-avec-cedric.fr/
- **Sur ma page Google+**
  https://plus.google.com/+cchabrely/
- **Sur ma page Facebook**
  https://www.facebook.com/fiaced/
- **Sur Twitter**
  https://twitter.com/fiacedric

Ce mini guide de la sécurité Internet
A ETE REALISEE PAR : **BENOIT CLAIR ET CEDRIC CHABRELY -** CREDIT PHOTO : **FOTOLIA**