

Le meilleur Antivirus est-il suffisant pour votre protection?

La sécurité informatique n'est plus une option. Elle est devenue un besoin vital pour tout utilisateur. Le choix d'une solution efficace est crucial pour assurer une protection intégrale face aux menaces actuelles et futures.

Il a été prouvé qu'une approche traditionnelle est insuffisante dans l'environnement actuel, notamment en raison de sa nature réactive, et de son manque certain de protection face aux virus inconnus.

La société ESET est spécialisée dans la conception et le développement de logiciels de sécurité offrant une protection globale contre les menaces évolutives qui sévissent dans les environnements informatiques. Pionnier en matière de détection proactive des menaces, la technologie ThreatSense® d'ESET offre le plus haut degré de protection du marché. Sur les neuf dernières années, elle est la seule technologie antivirus à n'avoir manqué aucun virus „In-the-Wild“ („dans la nature“) lors des tests VB100 du Virus Bulletin et détient le record absolu de 50 récompenses à ces mêmes tests. ESET NOD32 Antivirus a aussi été sacré « Meilleure solution antivirus » pour les années 2006 et 2007 par AV-Comparatives (www.av-comparatives.org).

Cependant, les experts s'accordent à dire que le plus grand risque est d'origine humaine. En effet, aussi fiable que puisse être une solution, elle ne peut empêcher l'utilisateur de compromettre, volontairement ou non, la sécurité de son système en accédant à certains sites, en autorisant la réception des fichiers de contacts inconnus ou en exécutant des fichiers compromis. Il est impératif « d'éduquer » l'utilisateur, de l'informer des risques qu'il encourt au travers d'Internet.

Dans ce but, le portail de la sécurité informatique, géré par la Direction Centrale de la Sécurité des Systèmes d'Information (DCSSI), a publié une liste de dix commandements : dix recommandations et conseils à l'attention des usagers. Nous vous les rappelons, afin de vous sensibiliser et d'accroître encore plus votre protection.

ESET Smart Security ESET NOD32 Antivirus



we protect your digital worlds



Les 10 commandements de la sécurité sur l'Internet préconisés par la Direction Centrale de la Sécurité des Systèmes d'Information

I. Utiliser des mots de passe de qualité.

Le dictionnaire définit un mot de passe «comme une formule convenue destinée à se faire reconnaître comme ami, à se faire ouvrir un passage gardé». Le mot de passe informatique permet d'accéder à l'ordinateur et aux données qu'il contient. Il est donc essentiel de savoir choisir des mots de passe de qualité, c'est-à-dire difficiles à retrouver à l'aide d'outils automatisés, et difficiles à deviner par une tierce personne.

II. Avoir un système d'exploitation et des logiciels à jour : navigateur, antivirus, bureautique, pare-feu personnel, etc.

La plupart des attaques tentent d'utiliser les failles d'un ordinateur (failles du système d'exploitation ou des logiciels). En général, les agresseurs recherchent les ordinateurs dont les logiciels n'ont pas été mis à jour afin d'utiliser la faille non corrigée et ainsi parviennent à s'y introduire. C'est pourquoi il est fondamental de mettre à jour tous ses logiciels afin de corriger ces failles.

III. Effectuer des sauvegardes régulières

Un des premiers principes de défense est de conserver une copie de ses données afin de pouvoir réagir à une attaque ou un dysfonctionnement. La sauvegarde de vos données est une condition de la continuité de votre activité.

IV. Désactiver par défaut les composants ActiveX et JavaScript

Les composants ActiveX ou JavaScript permettent des fonctionnalités intéressantes mais ils présentent aussi des risques de sécurité pouvant aller jusqu'à la prise de contrôle par un intrus d'une machine vulnérable. En dépit de la gêne que cela peut occasionner, il est conseillé de désactiver leur interprétation par défaut et de choisir de ne les activer que lorsque cela est nécessaire et si l'on estime être sur un site de confiance.

V. Ne pas cliquer trop vite sur des liens

Une des attaques classiques visant à tromper l'internaute pour lui voler des informations personnelles, consiste à l'inciter à cliquer sur un lien placé dans un message. Ce lien peut-être trompeur et malveillant. Plutôt que de cliquer sur celui-ci, il vaut mieux saisir soi-même l'adresse du site dans la barre d'adresse du navigateur. De nombreux problèmes seront ainsi évités.

VI. Ne jamais utiliser un compte administrateur pour naviguer

L'utilisateur d'un ordinateur dispose de privilèges ou de droits sur celui-ci. Ces droits permettent ou non de conduire certaines actions et d'accéder à certains fichiers d'un ordinateur. On distingue généralement les droits dits d'administrateur et les droits dits de simple utilisateur. Dans la majorité des cas, les droits d'un simple utilisateur sont suffisants pour envoyer des messages ou surfer sur l'internet. En limitant les droits d'un utilisateur on limite aussi les risques d'infection ou de compromission de l'ordinateur.

VII. Contrôler la diffusion d'informations personnelles

L'internet n'est pas le lieu de l'anonymat et les informations que l'on y laisse échappent instantanément ! Dans ce contexte, une bonne pratique consiste à ne jamais laisser de données personnelles dans des forums, à ne jamais saisir de coordonnées personnelles et sensibles (comme des coordonnées bancaires) sur des sites qui n'offrent pas toutes les garanties requises. Dans le doute, mieux vaut s'abstenir...

VIII. Ne jamais relayer des canulars

Ne jamais relayer des messages de type chaînes de lettres, porte-bonheur ou pyramides financières, appel à solidarité, alertes virales, etc. Quel que soit l'expéditeur, rediffuser ces messages risque d'induire des confusions et de saturer les réseaux.

IX. Soyez prudent : l'internet est une rue peuplée d'inconnus !

Il faut rester vigilant ! Si par exemple un correspondant bien connu et avec qui l'on échange régulièrement du courrier en français, fait parvenir un message avec un titre en anglais (ou tout autre langue) il convient de ne pas l'ouvrir. En cas de doute, il est toujours possible de confirmer le message en téléphonant. D'une façon générale, il ne faut pas faire confiance machinalement au nom de l'expéditeur qui apparaît dans le message et ne jamais répondre à un inconnu sans un minimum de précaution.

X. Soyez vigilant avant d'ouvrir des pièces jointes à un courriel : elles colportent souvent des codes malveillants

Une des méthodes les plus efficaces pour diffuser des codes malveillants est d'utiliser des fichiers joints aux courriels. Pour se protéger, ne jamais ouvrir les pièces jointes dont les extensions sont les suivantes : .pif (comme par exemple une pièce jointe appelée «photos.pif») ; .com ; .bat ; .exe ; .vbs ; .lnk. A l'inverse quand vous envoyez des fichiers en pièces jointes à des courriels privilégiez l'envoi de pièces jointes au format le plus «inerte» possible, comme RTF ou PDF par exemple. Cela limite les risques de fuites d'informations.

ESET NOD32 Antivirus
ESET Smart Security

Protégez vos ordinateurs et serveurs avec les solutions ESET et respectez les 10 commandements de la sécurité sur l'Internet pour vous garantir une sécurité maximale.

Extrait du Portail gouvernemental de la sécurité informatique:

www.securite-informatique.gouv.fr.

Ces dix commandements sont publiés avec l'aimable autorisation de la Direction Centrale de la Sécurité des Systèmes d'Information, service du Premier ministre relevant du Secrétariat général de la défense nationale.

