Olivier Bogaert

Conseils + Anti-arnaques

LE WEB SANS RISQUE !

Racine

« À Nina, Suzy, Manoé et Charline,
la génération qui grandit avec le numérique.
Et pour leurs parents qui doivent les guider. »

SOMMAIRE

PRÉFACE

Olivier Bogaert, c'est la conjugaison d'un immense vécu sur le terrain et de remarquables qualités pédagogiques.

Sa fonction de policier spécialisé au sein de la Computer Crime Unit le met quotidiennement aux prises avec la criminalité informatique et ses victimes. Il examine les modus operandi des criminels, rassemble les éléments de preuve permettant de les identifier et de les poursuivre en justice.

Cette position privilégiée lui confère une expérience hors du commun. Celle-ci serait largement perdue si Olivier Bogaert ne veillait à la partager au travers de ses innombrables interviews à la radio et à la télévision, de même que par les ouvrages qu'il a écrits.

Vous aurez pu admirer avec quelle aisance et limpidité il parvient à expliquer aux non-spécialistes des sujets, qui ne sont jamais éloignés de la technologie complexe.

Olivier Bogaert consacre un temps important à diffuser la bonne parole sécuritaire au sein des établissements d'enseignement. Peut-être est-ce le secret de son approche ? Cela relève du grand art que de parvenir à expliquer aux adolescents, en des termes simples et compréhensibles, des sujets arides et souvent compliqués.

Le présent ouvrage est le reflet de son savoir-faire et surtout de son faire savoir. À partir de multiples cas qu'il a eu à traiter au sein de la Computer Crime Unit, Olivier Bogaert est parvenu à distiller l'essentiel de ce que tout utilisateur d'un ordinateur et de l'Internet devrait connaître. Il a rassemblé en un seul ouvrage une mine de conseils qui devraient éviter bien des désagréments aux internautes, ainsi que la réponse aux questions que nombre d'entre nous se posent… ou, à tort, ne se posent pas.

Confucius disait : « L'expérience est une lanterne que nous portons dans le dos et qui éclaire le chemin parcouru. »

En matière de sécurité informatique, nous devons en effet avoir l'humilité de reconnaître que quels que soient les efforts que nous déployons pour nous protéger, nous risquons toujours d'être victime d'attaques inconnues jusqu'alors. Toutefois, cela ne peut aucunement être une excuse pour ne pas savoir les risques connus. À cet égard, la lecture de cet ouvrage est un « must » incontournable pour jeunes et vieux, pour internautes débutants et chevronnés. Olivier Bogaert fait, en effet, un tour d'horizon particulièrement exhaustif des risques identifiés à ce jour et des moyens pour s'en prémunir.

Il vous reste à mettre en œuvre les bonnes pratiques qui y sont exposées. Tout le monde sait qu'il est dangereux de ne pas mettre sa ceinture de sécurité ou de téléphoner au volant… Et pourtant, combien ne voyons-nous, autour de nous, de gens qui ne respectent pas ces règles, mettant non seulement leur personne mais aussi les autres en danger ?

Alors, lisez ce livre avec l'attention qu'il mérite, mettez les conseils en pratique… et surfez tranquille !

ir. Luc Golvers
Président du Club de la Sécurité Informatique Belge (CLUSIB)
Consultant et expert en informatique auprès des Tribunaux

1

LA SÉCURITÉ

LES TRUCS & ASTUCES POUR BIEN COMMENCER

Le choix d'un bon mot de passe

Les mots de passe sont les clés de votre maison virtuelle, qui peuvent mener jusqu'à la salle des coffres. Mieux vaut donc réfléchir à deux fois avant de les choisir. Voici quelques mauvais exemples et quelques bons conseils.

D'abord un constat: nous sommes encore trop nombreux à choisir la facilité. Plus d'un quart d'entre nous prennent l'option d'un prénom. Certains utilisent leur numéro de téléphone ou une combinaison autour de leur date de naissance. Viennent ensuite les simples suites de caractères: azerty, 1234 ou 12345678. Chez les plus jeunes, ce seront les héros du moment ou la star à la mode. Et puis, il y a les réactifs qui préfèrent «jenaimarre», «jemenfiche» ou encore «n'importequoi», et les romantiques qui se protègent avec un «jetaime». Ces mots de passe sans imagination ni particularité sont évidemment du pain bénit pour les pirates informatiques. En effet, ils se font aider par des logiciels qui s'appuient sur des dictionnaires. Et, grâce à ces outils, il leur est facile de tester toutes les possibilités.

Alors, quelques conseils… Si vous devez composer un mot de passe, utilisez des lettres en minuscule et en majuscule. Ajoutez-y un chiffre de votre choix et terminez par un symbole, celui de l'euro

par exemple, ou encore par un point d'exclamation. Veillez également à ce que ce mot de passe comporte un minimum de dix caractères.

Vous pouvez aussi choisir une phrase que vous pourrez mémoriser sans difficulté et dont vous prenez la première lettre de chaque mot. Un exemple ? Un extrait d'une fable de La Fontaine : « Maître Corbeau sur un arbre perché tenait en son bec un fromage. » Ceci nous donnera : MCs1aptesb1f ! Autre exemple ? « Ma sœur Christine est née en 1963 ! » Ce qui nous donnera : MsCene1963 ! Vous pouvez également utiliser ces phrases en collant les mots les uns aux autres, cette méthode garantissant aussi une très grande sécurité.

Si vous souhaitez faire un test afin de vérifier la qualité de votre mot de passe, vous pouvez taper dans Google les mots-clés ci-dessous. Vous arriverez sur le site BeeSecure, qui permet de vérifier la solidité de votre clé numérique.

MOTS-CLÉS

Test
Mot de passe
Luxembourg

Un deuxième cadenas sur votre compte

Depuis plusieurs mois, les grands acteurs du Net nous invitent à accroître le niveau de sécurité en nous proposant notamment d'adopter la validation en deux étapes.

Souvent, le piratage d'un compte est rendu possible soit parce que l'utilisateur tombe dans le piège du *phishing*, dont nous parlons dans une des rubriques de ce livre, soit parce que le pirate a réussi à trouver la réponse à la question secrète, générée par le processus « J'ai oublié mon mot de passe », en se basant sur les très nombreuses informations que nous diffusons notamment sur les réseaux sociaux.

À titre d'exemple, expliquons la validation en deux étapes de Google. Si vous disposez d'une adresse Gmail, connectez-vous et, après avoir accédé à la page d'accueil, cliquez sur la petite bulle en haut à droite. La mention « Compte » apparaît, cliquez également. Dans la rubrique « Se connecter à Google », arrêtez-vous sur « Validation en deux étapes ».

Google vous demande ensuite de lui fournir un numéro de GSM sur lequel il pourra vous envoyer un SMS contenant un premier code. Vous pourrez alors associer l'application Authenticator que vous trouverez dans le magasin lié au système de votre smartphone.

À partir de l'activation, à chaque connexion, une fenêtre apparaît après l'introduction de vos identifiant et mot de passe ; dans le champ qui se présente,

vous devrez entrer le code généré par l'application ou celui qui vous a été envoyé par SMS. Si donc un pirate trouve votre mot de passe, il sera bloqué car il n'aura pas accès au téléphone qui est dans votre sac ou votre poche.

Pour éviter les soucis en cas de perte, vous pouvez, au moment de la configuration ou même ultérieurement, imprimer ou sauver un document qui contient des codes de secours, ce qui vous permettra de garder toujours le contrôle.

Facebook vous propose, lui aussi, cette solution. Vous pourrez l'activer en vous rendant dans la rubrique « Sécurité et connexions » de vos paramètres.

Pourquoi un antivirus ? Infection de votre ordinateur : petit mode d'emploi

Les logiciels malveillants ont évolué. Il y a quelques années, ils étaient souvent destructeurs. Aujourd'hui, ils sont surtout devenus des voleurs d'informations ou cherchent à faciliter l'accès à votre ordinateur.

Là aussi, il importe de les distinguer en fonction de leur mode de propagation. C'est ainsi que vous pourrez rencontrer des logiciels malveillants orientés sur les programmes, sur le courrier électronique, les documents ou encore les sites web.

La plupart du temps, les cybercriminels vont faire appel à des langages de programmation de type Java et Active X (voir Lexique) pour rendre possible l'installation du logiciel malveillant. Ces technologies apportent des fonctionnalités supplémentaires à votre navigateur internet. Elles vous permettent de télécharger automatiquement (et, souvent, de façon invisible) du code exécutable à partir d'Internet. Une fois téléchargé, ce code s'exécute lui aussi automatiquement sur votre ordinateur. C'est ainsi que vous pouvez par exemple visionner une vidéo en ligne ou encore jouer avec des applications sur Facebook.

Par l'intermédiaire de ces applications, les cybercriminels donnent pour instruction d'installer un logiciel malveillant en générant des messages qui vous inviteront à procéder à une mise à jour.

D'où l'intérêt de disposer d'un programme antivirus mis à jour, et donc capable de détecter la signature du logiciel malveillant que l'application essaye d'exécuter sur votre machine, même si celui-ci est récent.

Deux exemples concrets pour comprendre ce qu'est un virus…

1. LES CHEVAUX DE TROIE

Le « cheval de Troie » s'installe sur votre ordinateur sans que vous le sachiez lors de la visite d'un site, de l'ouverture d'un fichier attaché à un e-mail ou encore suite à un clic malheureux sur un lien proposé par un réseau social. Les développeurs de ces outils cherchent à exploiter la négligence, l'insouciance ou la naïveté des utilisateurs.

Un cheval de Troie peut, par exemple, ouvrir un accès à votre ordinateur pour en utiliser les ressources, ou encore permettre l'installation d'un autre logiciel malveillant comme un spyware (logiciel espion) chargé de récupérer vos données sensibles.

Mais ces logiciels malicieux sont également diffusés lors d'infections par simple visite d'un site web, sans interaction de l'utilisateur : en visitant le site, votre ordinateur se voit infecté.

Certains pirates ont ainsi tenté de capturer, parmi la clientèle du « e-banking », les identifiants et mots de passe lors de la connexion au service bancaire.

Heureusement, grâce à la diffusion massive du Digipass par les institutions bancaires, en Belgique, le risque est extrêmement faible.

Le cheval de Troie peut également menacer votre ordinateur en étant programmé pour donner accès au PC l'ayant téléchargé à l'insu de son propriétaire, permettant ainsi au pirate d'en prendre le contrôle à distance. Ce dernier peut alors utiliser les ressources de cet ordinateur afin de l'intégrer dans un vaste réseau de machines infectées : on parle alors de botnet et les ordinateurs qui en font partie sont appelés « pc zombies ».

2. LES « *BOTNETS* »

Il s'agit de réseaux de machines infectées à l'insu de leurs propriétaires et dont les cybercriminels ont pris le contrôle. Ils peuvent ainsi donner l'ordre à leurs armées de *bots* (*pc zombies*) d'installer des logiciels espions, comme nous l'avons évoqué dans l'exemple précédent.

Ces informations, qui ont pris beaucoup de valeur, peuvent ensuite être directement utilisées par le ou les hackers, ou encore être vendues à bon prix à d'autres pirates, qui les utiliseront, par exemple, pour initier des opérations financières frauduleuses. Une autre possibilité est de donner l'ordre à toutes les machines de lancer des requêtes vers un serveur ou un groupe de serveurs déterminé. Ceux-ci, alors saturés par ces demandes, se bloquent et cessent de fonctionner.

Le problème réside dans le fait que, derrière chacun des ordinateurs d'une armée de bots, se trouve un ou une propriétaire qui n'a pas conscience que son ordinateur a été piraté, l'installation du logiciel ayant permis de capturer l'ordinateur dans un botnet étant liée à un clic sur un mauvais lien. Par exemple, celui qui vous propose de regarder une photo de vous et qui, lorsque vous arrivez sur la page correspondante, vous invite à mettre à jour votre lecteur ; sans le savoir, vous installez alors le logiciel malveillant. Il se peut aussi que votre ordinateur soit infecté par la simple visite d'un site web : profitant d'une faille, les pirates installent par exemple un petit module complémentaire sur la

page d'accueil du site qui, lorsque vous visitez la page, a pour but d'introduire le logiciel malveillant dans votre ordinateur.

Mais la technique la plus vicieuse, c'est l'invitation à télécharger un logiciel antivirus installant un outil que le pirate pourra ainsi utiliser à sa guise. Concrètement, vous visitez un site peu regardant sur l'origine des bannières publicitaires qui l'agrémentent, et vous voyez s'ouvrir des messages vous informant d'un problème de sécurité détecté sur votre machine. Bien entendu, il n'y a aucun problème sur votre PC mais vous vous voyez proposer d'acheter un antivirus afin de tout réparer. Après un petit paiement par SMS, le téléchargement commence et installe le logiciel malveillant. C'est le comble de l'ironie : vous avez payé l'infection de votre ordinateur !

Pour vous prémunir contre ce risque, le moteur de recherche de Google est désormais équipé d'une fonctionnalité qui vous informe que le site dont vous allez ouvrir la page est potentiellement piraté. Ce système d'alerte vous avertit qu'un tiers a modifié le site web sur lequel vous allez vous connecter et qu'il est donc potentiellement dangereux. Si, malgré tout, vous souhaitez accéder à la page, Google vous le permettra.

Pour que votre ordinateur soit correctement protégé, il importe que vous procédiez à une analyse régulière de son disque dur avec un logiciel antivirus performant. Le scan régulier de votre machine permettra de découvrir ceux des virus qui auraient franchi les barrières protectrices automatiques.

Antivirus
Quelle solution choisir ?

Vous souhaitez installer un logiciel antivirus car c'est devenu une nécessité absolue, y compris si vous faites usage d'une machine Apple. Mais vous vous demandez lequel choisir.

Dans ce domaine, la concurrence est vive et l'évolution, permanente. Un conseil dès lors : mieux vaut faire confiance aux laboratoires professionnels qui testent régulièrement la fiabilité et les performances des antivirus. Pour vous permettre de retrouver l'usage de votre système en cas d'incidents, il existe également une solution intéressante. Elle se nomme *FixMeStick* et se présente sous la forme d'une clé USB qui contient tous les logiciels nécessaires pour faire redémarrer votre ordinateur dans un environnement où les virus qui ont pu s'y installer n'auront aucune prise, les rendant ainsi plus faciles à éradiquer. La clé, qui fonctionne avec le système d'exploitation Linux, contient trois antivirus. Il suffit de l'insérer, d'allumer l'ordinateur et de la laisser travailler. Elle se met à jour automatiquement via Internet à chaque utilisation.

MOTS-CLÉS
Av-test
FixMeStick

Dans votre moteur de recherche, tapez les mots-clés « comparatif » et « antivirus ». Vous trouverez plusieurs sites pour vous faire une opinion. Vous pourrez prendre connaissance des choix de plusieurs laboratoires ainsi que de la méthodologie utilisée.
En effet, en fonction de celle-ci et de l'usage de votre ordinateur, vous pourrez notamment décider de la solution qui convient le mieux à vos habitudes de navigation.

Les supports externes Quelques conseils pour bien les utiliser

Les supports de données que sont les clés USB sont devenus incontournables, aussi bien dans le cadre personnel que professionnel. Très mobiles, elles vous suivent partout et se branchent sur tous les ordinateurs auxquels vous avez accès.

Toutefois, comme tous les supports de données, ces clés USB sont vulnérables.

Nous allons examiner les risques provenant du contenu de la clé et les illustrer à l'aide d'un exemple parlant.

Un des responsables de la sécurité chez Google a mené une expérience : il a disposé 297 clés en différents endroits de l'Université de l'Illinois. Il a pu constater que 98 % d'entre elles avaient été ramassées et, grâce au logiciel envoyant un signal qu'il y avait dissimulé, que 45 % avaient été connectées à un ordinateur. Si ce logiciel avait été malveillant, il aurait pu infecter les machines et voler des données ou permettre l'accès à ces ordinateurs.

Mais il y a également les dangers visant le contenu, qui sont, eux, plus classiques. Si vous venez à perdre votre clé ou qu'elle vous est volée, vos données sont évidemment disponibles comme le serait le contenu d'un porte-documents. Ne perdez donc pas de vue que la clé abandonnée sur votre bureau peut être empruntée, et son contenu copié à votre insu.

Pour vous aider à garder les bons réflexes, voici quelques conseils de sécurité.

Pour vous aider à garder les bons réflexes, voici quelques conseils de sécurité.

- Considérez comme suspecte toute clé que l'on vous prête.
- Placez les données sensibles dans une archive (*zip*, par exemple) protégée par un mot de passe. Pour rendre la tâche plus difficile à celui qui tenterait de l'ouvrir, utilisez un mot de passe solide, comme expliqué dans la rubrique qui y est consacrée.
- Utilisez de préférence sur votre machine un compte utilisateur et non un compte administrateur, cela pourra limiter l'infection à cette session et permettra parfois de ne pas compromettre toute la machine.
- Veillez à la mise à jour de votre antivirus.