e-change
Plateforme d'échanges numériques

Sécurité informatique pour les associations

Comment se protéger.

Pourquoi se protéger ? • Contre qui ou quoi ? • Comment ?

Un support libre d'*e-change*

ritimo

1– Pourquoi se protéger ?

● Les piratages et fuites de données se multiplient.

Récemment, plusieurs groupes de pirates informatiques, dont Rex Mundi[i] (qui a attaqué Labio[ii] et Domino's Pizza), ont volé des bases de données et demandé une rançon en échange de leur non-publication.

● Des attaques ciblées contre des sites et serveurs français ont lieu continuellement depuis le massacre à *Charlie Hebdo*[iii] dans le cadre de l'opération de cyberattaque baptisée OPFrance[iv], et dans le contexte d'un affrontement en ligne entre pirates français et moyen-orientaux[v]. Le jeu ? Attaquer le plus de sites possible et laisser sa trace un peu partout. C'est ainsi que, en France, des sites sans aucun lien avec les conflits au Maghreb et au Moyen-Orient (campings, mairies, cabinets de conseil, syndicats…) ont été ciblés par le simple fait qu'ils n'avaient mis en œuvre aucune stratégie de sécurisation de leurs données.

● Mais ne pas avoir de sécurité informatique peut aussi signifier laisser traîner des données aux quatre vents, les rendant ainsi accessibles à n'importe quel revendeur, comme ce fut le cas pour la société nationale des chemins de fer belge, la SNCB, en 2013. Le fichier volé[vi], contenant les données personnelles de clients réguliers (adresse, numéro de téléphone, email personnel…), et notamment de députés européens, a été disponible pendant plusieurs mois sur la toile.

2– Bonnes pratiques

2.1 – Avoir un ordinateur propre

À quoi cela peut-il donc servir d'avoir un ordinateur « propre » ?
Cela permet d'éviter ce que l'on appelle aujourd'hui les « malwares » qui, il y a quelques années, étaient classés dans la grande famille fourre-tout des « virus ».

Aujourd'hui en informatique, le distingo est fait entre plusieurs types de virus, dont les *malwares* font partie. Les *malwares* sont des programmes, développés dans le but de nuire à un système d'exploitation, que l'on installe sans le savoir, donc sans le consentement de l'utilisateur dont l'ordinateur se trouve ainsi infecté.

On en trouve beaucoup, par exemple dans les logiciels gratuits que l'on télécharge sur des sites du type 01.net, ou dans des programmes récupérés sur des réseaux de *peer to peer*. Ainsi par exemple, le logiciel Photoshop coûte extrêmement cher ; mais ceux qui décident de le proposer en ligne gratuitement ne sont pas hélas ! le plus souvent, de sympathiques philanthropes : le logiciel « craqué » a été modifié et, lors de l'installation, le *malware* sort de sa cachette. *Idem* pour les jeux vidéos que l'on télécharge gratuitement.

• Procéder au grand nettoyage

Avant de procéder à l'installation de dispositifs de sécurité, essayons d'avoir un ordinateur propre, le mieux étant de tout réinstaller et reprendre de zéro lorsque l'on achète une machine d'occasion en rétablissant les paramètres d'usine ; idem pour un smartphone.

S'il s'agit de nettoyer son ordinateur personnel, le logiciel **Ccleaner**[vii] permettra de désinstaller les programmes corrompus et de supprimer des fichiers temporaires qui le seraient aussi.

Le temps du premier nettoyage est souvent très long, puisqu'il est conseillé de cocher alors le plus d'options possible (*cf.* dans la partie gauche de la fenêtre du logiciel).

Il est impossible de laisser tourner Ccleaner pendant la nuit, l'application sollicitant parfois l'utilisateur. Mieux vaut donc le lancer pendant le visionnage d'un film, par exemple, ou en tâche de fond, ce qui permet de garder un œil sur les messages tout en faisant autre chose.

• Mettre à jour ses applications

Seconde étape, mettre à jour ses applications. Bon nombre d'attaquants se glissent dans votre système grâce à une faille logicielle. Puisque les correctifs existent, puisqu'ils sont partagés et installés parfois automatiquement par les éditeurs, les pirates n'ont qu'à suivre ces mises à jour pour savoir où se trouvent les failles de la précédente édition, et attaquer.

2.2 – Éviter le « phishing »

Ne pas cliquer n'importe où est aussi plutôt une bonne idée ! C'est un bon moyen d'éviter le « harponnage » *(phishing)*.

Non ! votre ami coincé en Afrique qui a besoin d'un virement de 3 000 euros n'est pas en danger de mort ; et oui, votre fils qui vous envoie ses photos de vacances alors qu'il n'est pas en vacances – et qui vous demande de cliquer sur un lien au lieu de placer les photos en pièces jointes de son mail – n'est en définitive pas votre fils !

Au mieux, vous vous retrouverez sur des sites publicitaires. Au pire, on vous demandera d'entrer vos login et mot de passe Google (par exemple) pour vous connecter. La page de login ressemblera trait pour trait à celle que vous connaissez ; mais non ! il ne s'agira pas de la bonne. Un moyen de vérifier où vous êtes est de contrôler l'adresse de la page web qui s'affiche.

Cela est valable pour toute la navigation sur le Web : faux site des impôts, faux site Amazon, voire même site de votre banque, dont les attaquants aspirent et copient le code.

Mais, en y regardant de plus près, la simple lecture de ces mails destinés à nous harponner devrait nous mettre sur la voie…

De: Credit agricole <Securite@Credit-agricole.fr>
Objet: **Votre Facture: (FR- FR-TR-041-H0)**
À:
Date: Lundi 24 octobre 2011, 23h56

CRÉDIT AGRICOLE

Cher Client(e)
Nous avons remarquer un problème sur votre Carte de crédit.
Nous avons déterminer que quelqu'un a peut-être utiliser Votre Carte sans votre autorisation.
Pour votre protection, nous avons suspendue votre Carte de crédit.
Pour lever cette suspension, veuillez cliquer sur le lien ci-dessous et suivez la procédure indiquer pour Mettre à jour votre Carte Crédit.

Mettre à jour votre Carte Crédit

Nous nous excusons de la gêne occasionnée.

Bien Cordialement

Bob Parsons
Directeur Service Client
http://www.Credit-agricole.Fr

- Mon conseiller clientèle a un nom bien américain (Bob Parsons) par rapport à celui qui m'écrit habituellement ; d'ailleurs, pourquoi n'est-ce pas lui qui m'écrit ?
- Le titre du mail évoque une facture, mais son contenu parle lui de problèmes avec ma carte de crédit.
- Le mail n'est pas personnalisé : visiblement, Bob-mon-conseiller a des doutes sur mon genre et ne sait plus si je suis client ou cliente.
- Le mail comporte une palanquée de fautes d'orthographe.
- Et enfin, non ! une carte de crédit ne se remet pas à jour…

2.3 – Bien choisir les données déposées sur son « cloud* »

Mon fournisseur de *cloud* est propriétaire des données que j'y dépose. Si, si ! c'est écrit dans les conditions générales d'utilisation (CGU), ce texte que l'on ne lit pas et pour lesquelles on a cliqué trop rapidement sur : « oui oui, je suis d'accord, j'ai bien lu les conditions… ».

Mais tout dépend alors des fichiers que l'on y dépose. S'il s'agit de morceaux de musique ou de films que l'on affectionne, ce n'est pas bien grave. En revanche, s'il s'agit des données de mon association, avec ses activités, la liste de ses adhérents, la liste de ses amis, celle des participants à diverses activités, leurs contacts personnels, etc., cela peut devenir un vrai problème…

Alors, quand il s'agit d'une copie de sa carte d'identité ou de son RIB… attention à l'usurpation d'identité en cas de faille dans le système ! Accès aux serveurs du fournisseur de *cloud* par, au choix : un pirate informatique, un membre du personnel accrédité pour avoir accès à ces données et faisant n'importe quoi avec, un réparateur de clim' qui peut si facilement se brancher sur un serveur pour en récupérer les données, etc.

* espace de stockage en ligne.

2.4 – Se méfier des applications mobiles

Pourquoi une application mobile de fond d'écran ou de cuisine devrait-elle avoir accès à mes appels, à mes SMS, à ma géolocalisation ? Après tout, je veux juste une recette d'aubergines au four ou un fond d'écran avec la photo de mon chanteur préféré.

Encore une fois, ce n'est pas une question de technique mais de bon sens ! La vraie sécurité consiste à lire les différentes fonctionnalités et attributions de l'application avant de cliquer sur installer/accepter. Il s'agit donc d'être conscient des données que l'on partage

si l'on choisit d'installer tout de même l'application, données qui seront revendues, dans le « meilleur » des cas, à des publicitaires.

3– Surfer privé

3.1 – Le chiffrement des données

De plus en plus de sites orientent nos connexions, par défaut, vers du https au lieu de http.

Au-delà de passer par un port différent (80 pour le premier, et 443 pour l'autre), il s'agit de deux modes d'échange d'informations entre un serveur, sur lequel se trouve le site consulté, et notre ordinateur.

HTTP = Hypertext Transport Protocol
HTTPS = *idem,* mais avec un S pour « secure »[viii]

En http, il est possible, pour quiconque est sur le même réseau que vous au même moment, de voir vos connexions à un site web, y compris les informations échangées avec ce site ; par exemple, lors d'une commande sur Internet, les mots de passe, les données personnelles du type adresse de livraison et numéro de téléphone privé…

Les sites nécessitant des transactions bancaires sont aujourd'hui plutôt bien sécurisés grâce à différentes normes (PCI DSS notamment) encadrant les transactions en ligne en terme de sécurité. Toutefois, jeter un œil à la barre d'adresse avant de déposer une quelconque information est toujours une précaution utile.

L'autre moyen de se connecter en processus sécurisé https en permanence et sans trop y prêter attention est d'installer dans son navigateur le plugin « httpseverywhere ». Il suffit de se rendre dans le menu Modules de son navigateur (en général à droite de la barre d'adresse), de rechercher ce plugin et de cliquer sur installer.

Ainsi, la connexion aux sites visités sera automatiquement sécurisée.
Si un site ne permet pas cette connexion sécurisée, l'application le signale et demande si l'on souhaite néanmoins s'y connecter.

Il est très important que le plus de nos connexions possible se déroulent selon le protocole https et non http.

3.2 – Bloquer les « trackers »

Depuis quelques années, une multitude de petits boutons fleurissent sur les sites Internet, nous proposant de partager facilement nos lectures sur les réseaux sociaux ou de les envoyer par email.

Ces boutons ne sont pas là uniquement pour nous faciliter la vie, mais bien, comme certaines publicités, pour espionner notre activité en ligne : temps passé sur une page, liens cliqués, etc. Sur la page d'accueil du Monde. fr, par exemple, on note déjà 14 trackeurs *(cf. en haut à droite de l'illustration de la page suivante).*

La bonne nouvelle est que non seulement ces trackers sont identifiables, mais que l'on peut en outre les bloquer, grâce à l'application **Ghostery**[ix].

Cette application se télécharge et s'installe, quel que soit votre navigateur, de la même manière qu'httpseverywhere, en recherchant le module dans les paramètres du navigateur.

4– Se méfier des attaques physiques

4.1 – Périphériques amovibles

La simple introduction d'une clé USB dans une machine peut être à la source de graves problèmes de sécurité, il n'est que de se rappeler l'affaire du ver informatique Stuxnet, découvert en 2010, qui a attaqué 45 000 systèmes informatiques *via* des clés USB infectées[x].

Tout appareil « inconnu », qu'il s'agisse d'un téléphone mobile, d'une clé USB ou d'un disque dur que l'on ne maîtrise pas, doit susciter la méfiance, la solution la plus simple en cas de doute étant de ne pas le raccorder à son ordinateur.

A minima, il est indispensable de lancer à chaque branchement d'un périphérique une passe d'antivirus sur ce périphérique avant d'ouvrir un dossier ou de lancer un programme. Attention toutefois : les antivirus, même à jour, ne répertorient que les virus qu'ils connaissent, déjà identifiés par des chercheurs en sécurité (d'où l'importance d'avoir un antivirus à jour pour se protéger des virus les plus récents) ; l'on n'est donc pas pas à l'abri, même en procédant systématiquement ainsi, d'un virus nouvellement créé encore inconnu des chercheurs.

S'il s'agit juste de copier un document présent sur le périphérique, en plus du passage du périphérique à l'antivirus, il est préférable de transférer le fichier en question sur une application de type VirusTotal (dans la partie « fichier ») afin de vérifier que le fichier est sain avant de l'enregistrer sur votre son ordinateur.

4.2 – « Keyloggers », « malwares » et autres joyeusetés

Un bon virus, c'est comme une MST, on s'en aperçoit rarement tout de suite et ça fait des ravages. On a déjà évoqué des les *malwares* ; le *keylogger* est fort sympathique aussi, dans cette catégorie.

Le *keylogger*, qui nous infecte parce que l'on ne s'est pas protégé (*via* un fichier corrompu, un téléchargement irréfléchi, un clic sur un lien vérolé…), a pour mission d'enregistrer notre frappe sur le clavier et d'envoyer les informations ainsi récoltées vers le pirate. Ces informations que nous transmettons peuvent être des logins et ou des mots de passe, un numéro de carte bleue, des informations personnelles, etc., qui serviront de base à une usurpation d'identité, par exemple un achat en notre nom (d'ailleurs, quand un site comme celui de la Fnac nous propose de stocker notre numéro de carte bleue pour un prochain achat, répondons par la négative, puisque, dans ce cas précis, il suffit de se connecter à son compte pour effectuer des achats en son nom sans avoir besoin de sa carte de paiement).

Enfin, l'attaquant peut « juste » avoir besoin de votre ordinateur pour mener par exemple une attaque en intégrant votre ordinateur dans ce que l'on appelle un *Botnet*[xi]. De quoi s'agit-il ? Eh bien, une fois le fichier malveillant dans votre ordinateur, l'attaquant s'en sert pour ouvrir un chemin d'accès entre votre machine et un serveur qu'il gère, s'en servant notamment pour échanger des informations.

La machine étant corrompue, le pirate peut faire exactement ce qu'il veut avec, notamment l'utiliser pour mener des attaques DOS ou DDOS[xii], appelées en français « attaques par déni de service[xiii] ». Le but est de noyer un site sous les connexions afin que le son serveur soit submergé, pour :
– le mettre hors ligne ;
– « faire déborder » le serveur et en récupérer les bases de données ;
– corrompre le site et afficher un message politique, idéologique, etc.

Et vous, dans tout ça ? Eh bien, vous ne vous apercevez même pas que votre ordinateur a participé à une quelconque attaque. Vous ne vous apercevez pas non plus que, dans les traces laissées par l'attaque, c'est bien votre adresse IP, celle de votre ordinateur, qui est enregistrée, parmi tant d'autres, sur le serveur attaqué… pas l'adresse IP de l'attaquant. Et si des poursuites doivent avoir lieu, la victime peut notamment se retourner contre vous.

5– Applications de chiffrement

5.1 – Chiffrer ses dossiers

Chiffrer ses dossiers permet de rendre leur contenu illisible aux personnes ayant accès à votre ordinateur, que cet accès soit :
– physique (membre de la famille, ami à qui l'on prête sa machine, forces de police lors d'une saisie…) ;
– distant (attaquant qui aurait accès à l'ordinateur *via* un *malware*).

L'application **Veracrypt**[xiv] permet de créer des dossiers *(containers)* chiffrés dans lesquels déposer les documents que l'on souhaite protéger : données professionnelles, travaux divers, comptabilité, documents administratifs, etc.

Elle est téléchargeable gratuitement sur le site de l'éditeur et est accompagnée de différentes notices d'utilisation.

5.2 – Chiffrer une partition sur une clé USB

Veracrypt permet aussi de chiffrer entièrement une clé USB ou autre périphérique, puis divers dossiers présents sur ce périphérique. Soit donc de créer une partition chiffrée à l'intérieur d'une autre partition chiffrée, une sorte de double fond caché dans un tiroir. Ce chiffrement peut être utile lorsque l'on transporte des données relatives à son association sur un disque dur externe ou une clé USB et que ce support n'est pas totalement dédié à ces travaux. Si l'on prête ce support à un ami ou à un collègue de bureau le temps de déplacer un fichier ou de l'imprimer… celui-ci a alors également accès à nos documents privés stockés sur le support. Qui dit chiffrement des dossiers dit impossibilité d'y accéder.

6– Des mots de passe aux passphrases

Une étude très bien réalisée[xv] concernant la longueur et la diversité des caractères des mots de passe a prouvé la facilité avec laquelle un attaquant, en quelques secondes, accède à vos données.

Un bon mot de passe est un mot de passe long comportant des caractères variés. Quelques écueils sont également à éviter :
– générer un mot de passe sur un site spécialisé. Ce site détenant votre adresse IP, puisque vous vous y connectez et y avez même parfois laissé une adresse email pour vous y inscrire, il y sera très facile de retrouver un de vos comptes en ligne (profils sur les réseaux sociaux, par exemple) et d'essayer ce nouveau mot de passe que vous venez de générer. Un mot de passe est personnel, seul l'utilisateur doit le connaître ;
– lister vos mots de passe dans des dossiers, des fichiers Excel ou des espaces dédiés sur le *Cloud*. Pour les mêmes raisons qu'au paragraphe précédent, tout d'abord, mais aussi parce que, si tous vos mots de passe sont centralisés en un même endroit, il suffit d'accéder à cette application ou ce document pour avoir accès à l'ensemble de vos comptes. Keepass et LastPass[xvi], par exemple, programmes de stockage et de gestion de mots de passe, ont été piratés. Celui ou celle qui attaque de tels sites a accès à la totalité des données personnelles de leurs utilisateurs[xvii].

Comment avoir des mots de passe sécurisés et stockés en sécurité ? En se servant de sa tête !

Un exemple pour la création d'un mot de passe

Il nous faut quelque chose de long, avec des caractères variés, et facile à retenir. Pourquoi pas les paroles d'une de nos chansons préférée ou quelques vers d'un poème, pour commencer ?

Les sanglots longs des violons de l'automne

Ensuite, on peut s'amuser à remplacer quelques lettres par des chiffres ; de préférence, pour s'en souvenir, toujours le même chiffre pour une lettre donnée :

L3ss4ngl0tsl0ngsd3svi0l0nsd3l4ut0mne

Il nous faut aussi des caractères spéciaux. Pourquoi ne pas réintégrer l'apostrophe à sa place d'origine ? Ensuite, il suffira d'encadrer et de ponctuer.

L3ss4ngl0tsl0ngs, d3svi0l0nsd3l'4ut0mne !

Voilà comment une simple phrase, facile à retenir, se transforme en une phrase de passe sécurisée ! Mais attention, les attaquants utilisent des « dictionnaires » de mots de passe, soit des machines qui tournent et testent un nombre impressionnant de combinaisons créées à partir de mots de passe revenant souvent. Mieux vaut donc ne pas choisir les paroles d'une chanson des Beatles, par exemple, et préférer du folklore breton ou des chants basques, le poème d'un auteur inconnu…

7– Conclusion

Il n'y a pas *un* moyen de protéger ses données, il en existe beaucoup, dont certains, plus techniques, ne sont pas abordés dans ce texte.

Par ailleurs, tous les conseils présentés ici ne sont pas utiles à tous.

La base de la sécurité est avant tout la réflexion : que veut-on protéger ? de qui ? de quoi ?

Il suffit par exemple de ne pas prêter son ordinateur ou de créer des dossiers chiffrés (au cas où) si l'on souhaite juste protéger une poignée de documents en local.
On n'aura par ailleurs aucune hésitation à stocker ses données sur les *clouds* de Google ou de Windows si l'on souhaite rendre ces données accessibles largement et que l'on n'est pas regardant quant à la politique de ces groupes vis-à-vis de la vie privée de leurs utilisateurs et de la revente de données.

Chacun est libre de choisir les mesures de sécurité qui lui conviennent en fonction du contexte qui est le sien. Il suffit de réfléchir et d'être attentif au monde qui nous entoure.

Enfin, il est important, lorsque l'on se sépare d'un matériel informatique, même vieux, même défectueux, de détruire radicalement les documents qui y sont présents, faute de quoi quiconque aura récupéré ce matériel et saura le réparer pourra récupérer les données et utiliser nos documents.

Notes

i ▲ Rex Mundi sur Wikipédia

ii ▲ http://www.01net.com/actualites/rex-mundi-les-mysterieux-pirates-qui-extorquent-des-entreprises-francaises-649252.html

iii ▲ En janvier 2015.

iv ▲ OPFrance

v ▲ http://www.nextinpact.com/news/91728-opfrance-nous-ne-sommes-pas-terroristes-assure-groupe-meca.htm

vi ▲ Article SNCB en ligne sur le site de La Libre Belgique

vii ▲ Ccleaner

viii ▲ HTTP vs HTTPS (EN)

ix ▲ Ghostery sur Wikipédia

x ▲ Stuxnet sur Wikipédia

xi ▲ Botnet sur Wikipédia

xii ▲ https://www.nbs-system.com/blog/ddos-dos.html

xiii ▲ https://fr.wikipedia.org/wiki/Attaque_par_d%C3%A9ni_de_service

xiv ▲ Veracrypt

xv ▲ http://www.lockdown.co.uk/?pg=combi

xvi ▲ http://www.developpez.com/actu/86483/Le-gestionnaire-de-mots-de-passe-LastPass-pirate-l-entreprise-suggere-plusieurs-mesures-dont-le-changement-du-mot-de-passe-maitre/

xvii ▲ http://www.01net.com/actualites/comment-pirater-la-base-d-un-gestionnaire-de-mots-de-passe-927671.html

ritimo
Réseau des centres de documentation et d'information pour le développement et la solidarité internationale

e-change
Plateforme d'échanges numériques

E-change
plateforme-echange.org
e-change@ritimo.org

coredem

Avec le soutien de l'Agence française du développement et de la Fondation Charles Léopold Mayer.

Création maquette Claire Robert • Réalisation Claire Péraro