Pour en finir avec Facebook.

Remarque préliminaire : dans ce qui suit, on parle souvent de « ta machine ». Qui donc, peut être un PC, une tablette, un téléphone portable, etc. (Je ne situe pas bien ce que pourrait comprendre l'etc. en question, mais tout évolue à une telle vitesse désormais que je n'ai pas envie de voir mon texte se démoder dans les quinze jours).

1. Les virus

Il n'y a pas de virus sur Facebook : il est techniquement impossible qu'un virus puisse se propager via Facebook sans que tu y mettes toi-même, de la bonne volonté.

Une liste non-exhaustive de ce qu'il ne faut pas faire :

- UTILISER UN MOT DE PASSE FACILE. On est encombré de mots de passe, à un point tel que ta machine te propose de les stocker pour toi. Libre à toi d'utiliser cette facilité, mais je te rappelle qu'il n'y a pas d'algorithme de cryptage infaillible. Pour ma part, je considère que les systèmes mnémotechniques sont les meilleurs, pour autant qu'ils comprennent au moins 4 lettres dont au moins une est une

majuscule et les 3 autres des minuscules, ou n'importe quelle autre combinaison, ainsi que 4 chiffres et au moins un *caractère spécial* si autorisé. Par exemple, cette fiesta que tu as faite à Houte Si Plout en 2016, te fournit un bon mot de passe : « HsiP2016! » Ou la naissance de ton premier enfant à Bruxelles en 2013 : « Brxs_2013 ». Attention : pas « Bruxelles_2013 » : sur base d'un début de mot, les systèmes de cryptages *intelligents*, construisent eux-mêmes la fin. Il est sain de changer de mot de passe au moins une fois par an, mais on sait que personne ne fait ça.

Si on te craque ton mot de passe, on en profitera pour faire passer sur ton compte, des messages douteux, le plus souvent avec des tentatives d'arnaque à la clé et en espérant que ta bonne renommée permette de pêcher l'un ou l'autre poisson. Pour récupérer la situation, ce sera la croix et la bannière : il ne te restera plus qu'à clôturer ton compte, à en ouvrir un nouveau et à essayer de retrouver tous les « amis » que tu auras perdus.

- ACCEPTER N'IMPORTE QUI COMME « AMI ». Il y a des tonnes de faux comptes sur Facebook. Ces comptes sont créés au moyen de noms inventés avec une intelligence et un souci de vraisemblance variables ; une adresse e-mail bidon sur GMail ou autres, quelques photos chipées à un utilisateur quelconque, et le tour est joué. Les fausses pages ainsi créées se repèrent facilement : historique très court, aucun chichi comme une photo de couverture, et très souvent, des études universitaires – histoire de faire joli dans le décor. Si tu acceptes comme « ami », l'un de ses comptes, on essaiera d'entrer en contact avec toi, le plus souvent via Messenger : si tu es une, ce sera un mec – de préférence plutôt bien de sa personne –, si tu es un, ce sera une nana dans le genre mignonne et sérieuse mais pas l'air trop farouche. L'objectif principal est de créer une certaine intimité, de manière à te soutirer du fric : pleurnicheries,

échange de photos *très personnelles* grâce auxquelles on tentera de te faire chanter, etc. Il peut y avoir un objectif annexe – voir « les vidéos », ci-après.

- PARTICIPER À LA PROPAGATION DE CHAINES. Très souvent, accolée aux messages de chaine que tu reçois, il y a une petite vidéo, de préférence bien innocente, du style d'un bouquet de fleurs qui s'épanouissent sous ton regard émerveillé, etc. Techniquement, ces vidéos renvoient très discrètement à des sites qui enregistrent ton nom d'utilisateur quand tu les regardes. Il y a dès lors toutes les chances pour que, dans un avenir plus ou moins proche, tu feras partie de celles et ceux dont on utilisera – au moins – les photos ou une partie du nom afin de créer de faux profils comme expliqué ci-dessus.
- CLIQUER SUR UN FICHIER EXÉCUTABLE. C'est le top évidemment : c'est le meilleur moyen d'installer toi-même un virus sur ta machine. La plupart du temps, ces fichiers portent une extension « .com » ou « .exe » et seront analysés puis refusés par ton antivirus. Toutefois, ils peuvent aussi se présenter sous la forme de scripts, plus compliqués à filtrer. La règle de base est donc simple : on ne clique pas sur n'importe quoi, même s'il s'agit de choses expédiées par une connaissance au-dessus de tout soupçon – car son compte peut avoir été piraté. Et sûrement pas avant d'avoir demandé à cette personne si c'est bien elle qui a envoyé la pièce jointe.
- CLIQUER « OUI » SANS AVOIR LU ce qui se trouve au-dessus. Le plus connu des systèmes qui permettent la propagation de virus consiste en l'envoi d'une vidéo qui... ne fonctionne pas sur ta machine car soi-disant, « Flash n'est pas à jour ».

  Flash – appelé parfois Shockwave Flash – est un logiciel multimédia créé en 1996 par Future Wave, qui fut par la

suite racheté par Macromedia avant d'atterrir dans le giron d'Adobe Software, éditeur entre autres de PhotoShop et d'Acrobat. C'est Flash qui te permet entre autres, de voir les vidéos et les photos diffusées sur Facebook. D'une façon générale, les versions relativement récentes de Flash sont stables, et on n'en édite donc pas de nouvelles à tout bout de champ.

Le procédé utilisé par les pirates te renvoie en arrière-plan sur un site où un logiciel prend le contrôle de ta machine « avec ton consentement, puisque tu as cliqué Oui » et installe dessus ce qu'il a envie. Donc, si tu cliques sur une vidéo qui ne fonctionne pas et qu'on te propose de mettre quoi que ce soit à jour, envoie tout au diable, et ne traine pas : certains vicieux te laissent une dizaine de secondes pour dire non, et passé ce délai, le processus s'enclenche automatiquement. Dans le cas où tu voudrais vraiment voir la vidéo en question, clique sur « Non », puis va vérifier sur le site de Flash (ou en version anglaise) si ta version est réellement obsolète.

Si malgré ce qui précède, tu t'es fait rouler dans la farine, ta machine servira probablement un jour ou l'autre, à une attaque portée sur un site quelconque, à moins que plus prosaïquement, on n'essaie de te pirater ton accès bancaire, tes e-mails professionnels, tes mots de passe, etc. Il existe des antivirus et anti-malware gratuits, tels qu'Avast et Malwarebytes, et ne crois surtout pas ceux qui prétendent que ce qui est gratuit fonctionne moins bien ou est moins efficace que le reste. Toutefois, en les installant a posteriori, ils sont susceptibles – tout comme les payants – d'éliminer ou de corrompre des fichiers systèmes *vérolés* mais essentiels à la bonne marche de ta machine. Auquel cas, tu seras malgré tout obligé de sortir ton portefeuille de ta poche et de contacter un réparateur.

2. Les hoax

On appelle « hoax » une fausse information destinée, la plupart du temps, à te faire peur. Le but du jeu peut être double : nuire à une personne, à une association ou à une société ; te pousser à faire une démarche qui te mènerait à installer un virus sur ta machine.

Il existe un site régulièrement tenu à jour sur lequel sont répertoriés la plupart des hoax que l'on t'envoie. Va jeter un coup d'œil dessus : tu y retrouveras certainement l'un ou l'autre attrape-nigaud auquel tu t'es laissé prendre.

En passant, coupons les ailes à un canard qui commence à devenir de plus en plus dodu. Dans les préfixes de sites, on trouve pour l'heure, deux versions. La première et la plus ancienne, est « http ». L'autre est « https », où on a ajouté un « s » pour indiquer que ce site est sécurisé.

D'une manière trompeuse, si tu vas sur un site dont le préfixe est « http », comme http://www.chilou.net, Chrome par exemple, te balance un « not secure » devant le nom du site. En vérité, ces sites ne sont pas moins sûrs que les autres : c'est seulement qu'ils ne collectent pas d'informations personnelles et qu'ils ne te proposent pas de payer quoi que ce soit pour des choses dont tu n'as éventuellement rien à faire. Et que donc, le webmaster ne voit aucune utilité à faire les démarches administratives en vue de l'obtention d'un certificat de sécurité.

Si en revanche, on te demande d'entrer ton nom, ton e-mail ou ton numéro de carte bancaire sur un site dont le préfixe n'est pas « https », on essaie de t'arnaquer.

3. Les foutages de gueule

Facebook a changé depuis quelques mois, la façon de laquelle les avis te sont présentés. On a jugé pour toi, que sur

les 500 « amis » que tu as, tu corresponds en moyenne avec 25 – en vérité, c'est nettement plus compliqué et sophistiqué que ça comme calcul, mais pour notre santé mentale, schématisons.

Dès lors – schématisons encore –, Facebook ne te propose plus les avis diffusés par les autres, ce qui présente un côté frustrant pour certains.

Comme expliqué sur hoax-slayer, ne t'imagine pas que tu vas régler ce problème en copiant un message sur ta page : déjà, et d'abord, Facebook ne limite rien du tout. C'est juste qu'il considère que dans le tas, tu corresponds le plus régulièrement avec un nombre limité de personnes. Mais de plus, comment imaginer que le simple fait de copier un message de texte sans aucune particularité notable, puisse changer quoi que ce soit ?

En fait, si tu désires voir les avis laissés par d'autres « amis » que ces fameux « 25 », ce n'est pas très compliqué :

1. Clique sur les trois points bien connus, donnant accès au menu « Fil d'actualité »
2. Choisis « le plus récent », car en vérité, « à la une » te remballe les messages auxquels d'autres ont le plus répondu, même s'ils datent d'il y a une semaine.
3. Clique ensuite sur « Modifier les préférences », ce qui ouvre une fenêtre spéciale.
4. Clique sur « Choisir qui afficher en premier » : « Tout », « Amis uniquement », prends ce qui t'inspire – tu pourras de toute façon, modifier ta sélection ultérieurement.
5. Clique sur « Terminer », puis ferme la fenêtre à moins que d'autres options ne t'intéressent.

Tu vois ? Ça ne prend pas plus de temps que copier un message sur ta page et c'est plus efficace.