24 novembre 2016
Attention !

Quelques conseils pour éviter l'usurpation d'identité

Les usurpations d'identité peuvent survenir très rapidement si nous ne faisons pas attention à nos données personnelles sur Internet. Pour éviter tous problèmes, il faut adopter quelques réflexes qui peuvent paraître du bon sens, mais auxquels on ne pense pas assez souvent.

Avec Thomas Léger

Atlantico : Les particuliers sont de plus en plus connectés sur Internet. Chaque site exige de créer des identifiants de connexion, sites de commerce, banques, administrations, services de streaming, opérateurs téléphoniques, voyages, alimentation... Pour la plupart d'entre eux, une adresse mail et un mot de passe en plus de l'adresse physique et des données de facturation suffisent pour activer un compte. D'autres sites comme Pôle emploi ou les Caisses d'Allocations Familiales exigent de remplir des champs avec des données personnelles très précises (revenus, avis d'imposition, médecin traitant, questions sur la santé, allergies, régimes de retraites...). Quels sont les conseils à retenir pour protéger ses données personnelles sur Internet en fonction de ces deux types de sites ?

Thomas Léger : Notre environnement collecte de plus en plus d'informations sur notre vie personnelle, parfois de manière insidieuse, mais dans la majorité des cas de manière volontaire pour accéder à un service organisationnel, marketing ou de loisirs.

Dans le premier cas que vous citez, celui des inscriptions autres qu'institutionnelles, je recommande tout simplement de créer une adresse secondaire avec un mot de passe différent. Cela va permettre de cloisonner facilement un problème de piratage. De plus cette adresse mail remplira la fonction secondaire de stockage des spams, préservant aussi le confort d'utilisation sur votre adresse mail principale. L'usage d'une ou de plusieurs adresses mail secondaires est à mon sens la meilleure alternative et facile à mettre en œuvre. De plus il est alors possible de mettre en place un processus de récupération du compte A par le compte B en cas de piratage de celui-ci. Il faut bien comprendre que la sécurité de votre boîte mail est un des éléments clefs, si le pirate atteint celle-ci il sera alors très aisé pour lui d'obtenir non seulement des informations sur vous, mais en plus d'avoir une action sur votre environnement. À ce titre je recommande la mise en place de la double authentification et d'associer un numéro de téléphone au compte. Cela peut devenir très utile comme contre mesure face à un piratage et fluidifier la récupération de votre boîte mail.

Saisir ses données sur un site institutionnel ne pose pas de problème directement, du moment qu'il s'agit du site officiel. À ce titre, la principale menace pour l'utilisateur est le phishing. Cela consiste pour le pirate à venir intercaler entre l'utilisateur et le site officiel une fausse page clone du site. Celle-ci vous demande alors tout simplement votre identifiant et votre mot de passe avant de vous renvoyer vers le site officiel. Le pirate récupère ensuite les informations saisies et peut accéder à votre compte sur le site en question. L'opération est relativement transparente pour l'utilisateur non averti. La principale précaution pour éviter ce genre de situation consiste à vérifier l'authenticité du site sur lequel vous allez vous identifier. Pour cela, un site en HTTPS est un facteur rassurant. Je conseille également de ne pas accéder à un site par le biais d'un lien obtenu par mail. À titre d'exemple, un contact vous envoie un lien sur Facebook, vous accédez à ce lien qui semble être Facebook, pourtant il vous redemande une authentification, c'est sans doute du

phishing. Assurez-vous alors que votre contact est sûr, voire qu'il n'est pas victime lui-même d'un piratage. De plus une banque, ou un organise quel qu'il soit, ne vous demandera jamais par mail de saisir vos identifiants ou votre numéro de carte bleue pour vérifier votre identité, en cas de doute appelez directement l'organisme en rapport.

Un élément important qui facilite trop souvent le piratage est le type du mot de passe utilisé, il n'est pas rare de voir des 1234 ou encore le nom de votre animal de compagnie, l'année de naissance. Tous ces éléments sont souvent faciles à trouver pour un pirate. Une phase de recherche sur vos réseaux sociaux lui apportera souvent les éléments dont il a besoin et dans l'hypothèse où il ne trouve pas directement sur votre profil, il élargira son cercle de recherche à vos contacts moins prudents. Pour contrer cela, la solution la plus simple est de filtrer vos informations. Rendre publiques votre date de naissance, vos photos de vacances ou celles de vos enfants, vos loisirs ou encore votre géolocalisation vous expose considérablement. Il faut être conscient que chaque élément que vous injectez sur le net peut devenir un indice pour une personne malintentionnée. Facebook a revu et amélioré ses paramètres de confidentialité, il est impératif pour les utilisateurs d'en prendre connaissance et de régler au plus juste ceux-ci. Il en est de même avec tous les réseaux sociaux que vous êtes amené à utiliser.

Avez-vous des chiffres sur les cas d'usurpations d'identités en France ? Les Français sont-ils conscients des risques encourus sur Internet ? Protègent-ils efficacement leurs données ?

C'est alarmant et très peu pris en considération par les internautes. Bien que les comportements s'améliorent progressivement, mais lentement, les techniques de piratage et notamment la qualité des phishings s'améliore très rapidement. Le site phising-initiative.fr a annoncé au Forum International de la Cyberdéfense 2016 que le piratage par cette technique a fait plus de 2 millions de victimes dans l'année 2015. Ce chiffre a, malheureusement, sans nul doute évolué à la hausse depuis.

La prise de conscience des dangers par les français est encore relativement faible, elle n'impacte pas une classe sociale en particulier. Je vois régulièrement des dirigeants de sociétés poster en public une quantité impressionnante d'informations personnelles. Dans une optique malveillante elles pourraient aider le piratage du compte privé de cette personne, mais de manière encore plus insidieuse à atteindre la société elle-même. C'est un cas courant qu'il ne faut pas sous-estimer. Quel que soit votre travail, votre localité, vous pouvez à un moment devenir la proie d'un cybercriminel, s'exposer c'est augmenter les risques.

Il est clair que dans cette continuité les internautes protègent mal leurs données, je pense, à titre d'exemple aux photos d'enfants. Quoi de plus simple et mignon que de les montrer à la terre entière, les premiers pas, la rentrée des classes, etc. Mais c'est oublier que derrière il peut y avoir une récupération pédophile, un détournement de l'image. La gendarmerie déconseille vivement la publication des photos d'enfants, cela fait écho à des cas concrets de problèmes.

Les achats sur Internet sont de plus en plus fréquents. Comment être sûr que le site possède bien les garanties pour se prémunir du vol de données bancaires ? Comment faire pour déceler des prélèvements ou des retraits parfois sous forme de petites sommes anodines dont nous n'aurions plus le souvenir ? Que faut-il faire auprès de sa banque une fois que l'on constate des achats potentiellement frauduleux ?

Les paiements en ligne sont devenus indispensables, mais il faut être prudent. Donner ses informations bancaires n'est jamais anodin, au contraire. Tout d'abord il faut si possible concentrer son périmètre d'achat en ligne sur les sites les plus populaires. Ils sont de par leur taille, garants d'une meilleure sécurité. Idéalement il faut prendre connaissance des CGU (Conditions Générales d'Utilisation) et identifier les points de contact possibles avec l'administration du site en cas de litiges. Un site sans possibilité de contact et sans CGU a sûrement des choses à cacher. Les sites doivent être en HTTPS et non en HTTP, prouvant ainsi la sécurisation de la page.

En complément, il existe des moyens alternatifs efficaces comme le paiement par un compte tampon de type PayPal, ou l'usage d'une carte jetable. Les banques françaises développent le système 3D Secure qui en complément de votre paiement nécessite des informations complémentaires comme la saisie d'un code unique reçu par SMS. Et enfin, surveillez vos comptes. Il n'est pas rare qu'une carte bancaire piratée soit débitée plusieurs fois. Un achat à l'étranger, une somme importante débitée, il est alors urgent de faire opposition et de contacter votre banque. Les forces de l'ordre seront à même de vous accompagner lors de votre dépôt de plainte. Légalement vos relevés de comptes font preuve et si vous êtes reconnu comme étant victime d'un piratage votre banque est tenue de vous rembourser.

Les services bancaires, postaux, institutionnels ont-ils besoin de demander des justificatifs par mail aux particuliers ? Quels sont les différents mails que nous pouvons recevoir ? Certains demandent de cliquer sur un lien explicite alors que d'autres sont plus sournois, leur ouverture peut déclencher un cheval de Troie. Pouvez-vous nous expliquer ces différences ? Par conséquent, quelle est l'attitude à adopter face à des emails que l'on recevrait qui imiteraient les logos des opérateurs téléphoniques, des banques, des institutions comme le service des impôts qui demanderaient des informations confidentielles ?

Les pirates rivalisent d'ingéniosité c'est indéniable, ils s'adaptent en permanence pour maintenir un niveau de performance élevé. Tout d'abord il faut savoir que tous ces services ne vous demanderont jamais d'informations confidentielles par mail, particulièrement vos coordonnées bancaires et vos mots de passe. Dans un tel cas, cela doit attirer votre attention et votre refus. Les pirates détournent souvent votre prudence grâce un mail à l'apparence officielle, avec des logos du service des impôts ou encore de la gendarmerie. Ne vous laissez pas avoir par une belle présentation graphique et un aspect légitime. D'autres attaques par mail vous renvoient sur un lien, les possibilités sont alors multiples, téléchargement d'un virus ou d'un ransomware ou encore l'ouverture d'une page en apparence sûre mais qui vous demande des informations confidentielles. La meilleure règle est la confirmation téléphonique. Vous recevez un mail de votre centre des impôts, pas d'hésitation à avoir, un appel sur le numéro officiel permettra de confirmer la légitimité de celui-ci.

Dans le cas d'un mail avec une pièce jointe, les possibilités techniques sont tellement multiples que je déconseille tout simplement de l'ouvrir sans être sûr de l'identité de l'expéditeur. Dans l'hypothèse où vous n'avez pas d'autre choix que de l'ouvrir, il existe plusieurs

logiciels permettant d’effectuer un scan de votre pièce jointe, ou idéalement de l’ouvrir dans une "Safe zone" isolée du reste de l’ordinateur.

En parallèle, votre ordinateur et votre smartphone ont besoin de maintenance, maintenez-les à jour. Faites régulièrement des scanners antivirus mais aussi anti-malware. Une fois par semaine est un idéal, cela doit être en rapport avec l’usage. N’oubliez pas de faire des sauvegardes et de les isoler physiquement de votre ordinateur. En cas de doutes, de suspicions de piratage, renouvelez l’opération et effectuez un changement de tous vos mots de passe. Il vaut mieux perdre 30 minutes à faire preuve de prudence, que de perdre le contrôle de sa vie numérique pendant des jours.