Association Loisirs et culture

Les risques d'Internet
Et les solutions aux préjudices

Jean Marie Herbaux

Vous utilisez Internet de façon intensive et malgré toutes les précautions que vous avez prises, vos données ont été subtilisées ou pire. Il est temps de réagir et d'appliquer quelques principes et solutions simples pour limiter la portée du préjudice subi.

Table des matières

I. Quelques risque brièvement évoqués !

Pour naviguer sans risque sur Internet, il est bien sur absolument nécessaire de posséder un antivirus *à jour*. Mais c'est loin d'être suffisant car l'un des pièges les plus courants sur Internet est le Fishing.

1. le Fishing.

Le phishing (contraction des mots anglais « fishing », en français *pêche*, et « *phreaking* », désignant le piratage de lignes téléphoniques), traduit parfois en « *hameçonnage* », est une technique frauduleuse utilisée par les pirates informatiques pour récupérer des informations (généralement bancaires) auprès d'internautes. Et vous êtes le seul rempart contre le fishing.
La technique du phishing est une technique d'« ingénierie sociale » c'est-à-dire consistant à exploiter non pas une faille informatique mais la « **faille humaine** » en dupant les internautes par le biais d'un courrier électronique semblant provenir d'une entreprise de confiance, typiquement une banque ou un site de e-commerce.
Le ***mail*** envoyé par ces pirates usurpe l'identité d'une entreprise (banque, site de commerce électronique, etc.) et vous invite à vous connecter en ligne par le biais d'un lien hypertexte et de mettre à jour des informations vous concernant dans un formulaire d'une page web factice, copie conforme du site original, en prétextant par exemple une mise à jour du service, une intervention du support technique, etc.
Dans la mesure où les adresses électroniques sont collectées au hasard sur Internet, le message a généralement peu de sens puisque l'internaute n'est pas client de la banque de laquelle le courrier semble provenir. Mais sur la quantité des messages envoyés il arrive que le destinataire soit effectivement client de la banque.
Ainsi, par le biais du formulaire, les pirates réussissent à obtenir les identifiants et mots de passe des internautes ou bien des données personnelles ou bancaires (numéro de client, numéro de compte en banque, etc.).
Grâce à ces données les pirates sont capables de transférer directement l'argent sur un autre compte ou bien d'obtenir ultérieurement les données nécessaires en utilisant intelligemment les données personnelles ainsi collectées.
Lorsque vous recevez un message provenant a priori d'un établissement bancaire ou d'un site de commerce électronique il est nécessaire de vous poser les questions suivantes :

- Ai-je communiqué à cet établissement mon adresse de messagerie ?
- Le courrier reçu possède-t-il des éléments personnalisés permettant d'identifier sa véracité (numéro de client, nom de l'agence, etc.) ?
- Le message est-il en français correct et sans faute d'orthographe ?

Par ailleurs il est conseillé de suivre les conseils suivants :

- Ne cliquez pas directement sur le lien contenu dans le mail, mais ouvrez votre navigateur et saisissez vous-même l'URL d'accès au service.
- Méfiez-vous des formulaires demandant des informations bancaires. Il est en effet rare (voire impossible) qu'une banque vous demande des renseignements aussi importants par un simple courrier électronique. Dans le doute contactez directement votre agence par téléphone !
- Assurez-vous, lorsque vous saisissez des informations sensibles, que le navigateur est en mode sécurisé, c'est-à-dire que l'adresse dans la barre du navigateur commence par **https** et qu'un petit **cadenas** est affiché dans la barre d'état au bas de votre navigateur, et que le domaine du site dans l'adresse de la barre d'adresse du navigateur correspond bien à celui annoncé (gare à l'orthographe du domaine) !
- Dans le moindre doute supprimez le message et videz les messages supprimés !

2. Les Téléchargements sont une autre source d'ennuis !

L'autre risque vient des téléchargements qui peuvent contenir des malveillants qu'on appelle malware. En anglais, le terme **malware** est la contraction de " **malicious software** ". En français, on emploie donc le terme de " **maliciel** ", contraction de " **logiciel malveillant** ". Ce terme désigne tous les codes ou programmes informatiques malicieux qui peuvent être dangereux pour les systèmes informatiques.
Les malwares sont hostiles, intrusifs, et conçus pour envahir, endommager ou désactiver les ordinateurs, les réseaux, les appareils mobiles et autres serveurs. En règle générale, ils permettent

aux cybercriminels qui les déploient de prendre contrôle de la machine à distance et d'interférer sur son fonctionnement. Bien souvent, un malware a pour but d'extorquer de l'argent à la victime. Il est capable de voler, de chiffrer, ou de supprimer des données. Il peut aussi altérer ou désactiver les principales fonctions de l'ordinateur, et permettre d'espionner secrètement l'activité d'un ordinateur par les frappes au clavier par exemple.
Les chevaux de Troie comptent parmi les malwares les plus renommés. Déguisés en logiciels légitimes, ou dissimulés dans un logiciel légitime, ils agissent discrètement et créent des portes dérobées dans la sécurité d'un système pour permettre à d'autres malwares d'y entrer.
Les " Spywares ", quant à eux, sont des malwares conçus pour espionner la victime. Dissimulés en arrière-plan, ils surveillent ce que vous faites en ligne. Ils peuvent notamment permettre de dérober les mots de passe, les coordonnées bancaires, par vos saisies au clavier ou d'épier vos habitudes de navigation.
Depuis quelques années, les malwares les plus répandus sont les " *Ransomwares* " ou *rançongiciels*. Ils sont capables de verrouiller un ordinateur et menacent de supprimer tout son contenu, à moins que la victime accepte de payer une rançon.
Conseils :

- Quand vous téléchargez un logiciel (ou même un fichier PDF), ne vous contentez pas de le rechercher par son nom ! Dans la ou les pages de résultats de votre recherche, privilégiez le lien vers le site du propriétaire du produit plutôt qu'un autre lien dont vous ne connaissez pas l'origine !
- à la fin du téléchargement, contrôlez le avec votre antivirus avant de l'installer !
- La meilleure façon de rester protégé contre les malwares est d'utiliser un logiciel anti-malware ou antivirus.

3. Les Réseaux sociaux sont également une autre source de risques !

- suivre soudainement une personne que vous n'aimez pas.
- désabonnement à des comptes que vous adorez.
- blocage de certains individus.
- …

II. Repérer un piratage !

Malgré toutes les précautions que vous avez prises, vos données ont été subtilisées ou pire. Il est temps de réagir et d'appliquer quelques principes simples pour limiter la portée du préjudice subi.

1. Mot de passe incorrect !

Pour repérer un piratage, il y a quelques pistes à étudier. Par exemple, si vous êtes certain de votre **mot de passe**, mais qu'il ne vous permet pas de vous identifier sur votre compte. Il a certainement été piraté et changé par une autre personne.
Vous devez également vous méfier lorsque des **tweets** ou plus généralement des **billets** qui ont été publiés depuis votre compte alors que vous n'en êtes pas à l'origine.
Idem pour des messages privés.

2. Des activités inhabituelles

Un moyen d'identifier un piratage est aussi le fait d'observer des activités inhabituelles sur votre compte de réseaux sociaux, par exemple, comme de suivre soudainement une personne que vous n'aimez pas, le désabonnement à des comptes que vous adorez, le blocage de certains individus, etc.

III. Comment agir et vers qui se tourner en cas de problème?

1. Les obligations des sites

Qu'il s'agisse de la destruction, la perte, l'altération ou la divulgation non autorisée de données à caractère personnel transmises, sauvegardées ou l'accès à de telles informations, ces actes sont considérés comme un incident de sécurité. Malveillant ou non, il a pour conséquence de

compromettre l'intégrité, la confidentialité voire la disponibilité des données personnelles. Le *Règlement Général sur la Protection des Données*, le fameux *RGPD* oblige maintenant les responsables des sites à notifier à la CNIL toute violation ou perte de données personnelles. Outre la CNIL, l'entreprise peut également communiquer plus directement, auprès de ses clients ou via la presse, par exemple pour informer d'un incident.

2. Vos actions personnelles

- S'il y a une cyberattaque, il est très fortement conseillé de déposer une ***plainte*** au commissariat de police ou à la gendarmerie la plus proche de votre domicile. Tenez-vous également à la disposition des services concernés et réunissez tous les éléments de preuve technique que vous pouvez afin de constituer le dossier le plus solide possible. N'hésitez pas à réaliser des captures d'écran et à sauvegarder les éléments qui peuvent l'être pour apporter des informations les plus précises possibles aux autorités.
- Pour réagir, signalez le compte piraté auprès du ***réseau social*** concerné et demandez immédiatement la réinitialisation de votre mot de passe.
- Pour des éléments plus spécifiques, rendez-vous sur le site https://www.cnil.fr/fr/plaintes/internet afin de réaliser le signalement de contenus ou de comportements illicites auxquels vous vous trouvez confrontés.
- Le site http://www.netecoute.fr permet également de signaler des problèmes et de faire valoir vos droits informatiques et libertés. Étant donné que chaque service propose une procédure spécifique, il est important de se rendre au bon endroit et c'est notamment pour cette raison que le site propose des liens directs vers les services concernés qu'il s'agisse de Facebook, Instagram, Twitter, YouTube, Discord ou d'autres.

IV. Les principaux sites de signalement aux autorités

- Déclarez une plainte auprès de la CNIL, la Commission Nationale Informatique et Libertés, directement sur son site Internet, sur la page Plaintes en ligne | CNIL
- Sur la plateforme nationale d'assistance aux victimes d'actes de cybermalveillance
- Assistance aux victimes de cybermalveillance
- vous pouvez trouver des conseils et des vidéos pour sensibiliser votre entourage personnel, voire professionnel. Il y a également des services de proximité disponibles en cas de dommages causés par une attaque informatique.
- La page Prévenir, repérer et réagir face au piratage de ses comptes sociaux | CNIL
- est particulièrement prolixe en matière de conseils. Elle donne aussi des instructions très claires et très concrètes sur la meilleure manière de réagir en cas de problème, selon le réseau social utilisé.
- Enfin, notez que le site www.netecoute.fr est une plateforme qui permet aux plus jeunes de trouver une oreille attentive à leurs potentiels problèmes sur les usages numériques.