Fiche-conseils

LES MESSAGES SPAM & PHISHING

À mesure que les utilisateurs sont devenus de plus en plus actifs sur Internet par le biais, notamment, des réseaux sociaux, e-mails et *chats*, un phénomène s'est aussitôt installé : les messages spams et *phishing* (hameçonnage). Ces deux types de messages poursuivent un seul objectif commun : accéder à vos données personnelles.

Principales catégories de spams et hameçonnage

Le message non-sollicité

Message de publicité non-désiré, souvent d'origine douteuse, mais sans risque particulier.

Son contenu est principalement axé sur les pharmaceutiques (viagra, etc.)

Le saviez-vous ?

Le premier message non-sollicité a été envoyé par hasard en 1978.

Gary Thuerk, un commercial, avait transmis un message de publicité à plus de 400 des 2600 utilisateurs de l'ARPAnet, la toute première version de l'Internet. Suite à de nombreuses plaintes auprès de son entreprise, ce message non-sollicité fut appelé « spam » .

Le SCAM

Spam promettant un gros bénéfice ou une large somme d'argent bloquée sur le compte en banque d'un employé gouvernemental, par exemple.

Ce spam est également appelé spam nigérien ou « spam 419 », car au Nigéria l'article 419 du code pénal traite la fraude.

L'hameçonnage ou *phishing*

Message généralement frauduleux trompant l'utilisateur sur son origine afin de récupérer ses informations privées (carte de crédit, mot de passe, adresse physique, email, etc.) pour en abuser.

Il existe plusieurs classes d'hameçonnage.

Classe 01 (*Phishing* primitif)

Texte simple invitant l'utilisateur à compléter, puis à renvoyer, un formulaire avec son nom d'utilisateur, e-mail et mot de passe.

Classe 02

Texte comprenant un lien vers un site web invitant l'utilisateur à saisir des données dans un formulaire. Une variante de ces messages contient un lien vers un site web, normalement compromis, acheminant la requête vers un site téléchargeant automatiquement ou demandant d'installer un logiciel (malveillant) sur l'ordinateur.

Grâce à ce logiciel, l'attaquant peut recueillir des informations sur l'utilisateur (mots de passe, données bancaires, etc.)

Classe 03 (Spam malveillant ou Malspam)

Message contenant souvent une pièce jointe en format *.zip, *.scr ou *.flv. Il s'agit normalement d'un logiciel malveillant bloquant l'accès à l'ordinateur. L'utilisateur est invité à payer une rançon (*ransom*) par carte prépayée (p. ex. safepaycard) ou par agence de transfert d'argent (p. ex. Western Union).

Dans le cas extrême, tout le disque dur ou le serveur de fichiers est encrypté et un paiement de la rançon ne garantit pas le décryptage. Dans un tel cas, il est conseillé de contacter un expert.

restena
réseau · sécurité · .lu

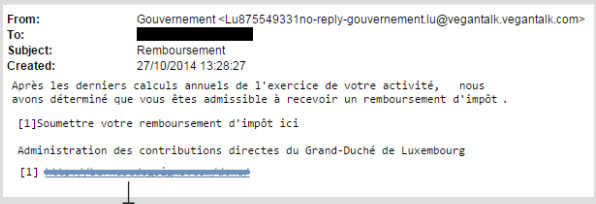
Exemples d'hameconnage

1. Hameçonnage avec logiciel malveillant et de cryptage

Après avoir ouvert la pièce jointe d'un e-mail contenant un logiciel malveillant masqué comme facture ou contrat en format *.zip/ *.flv/..., tous les fichiers sur le disque dur sont cryptés et un message s'affiche. Ce message exige de l'utilisateur de payer une rançon de 0.2 à 5 Bitcoins dans un délai de 72 à 96 heures, sous peine de voir son disque définitivement crypté.

Dans ce cas, il est conseillé de contacter un expert ou de télécharger un logiciel qui peut supprimer le virus.

2. E-mail avec texte et lien vers un site *phishing* à l'apparence de l'Administration des Contributions Directes



Le site *phishing* promet un remboursement par carte de crédit et collecte de nombreuses informations sur l'utilisateur :

- Type de carte de crédit
- Nom sur la carte de crédit
- Numéro de la carte de crédit
- Date d'expiration
- Date de naissance
- Code de sécurité (CVC)
- Mot de passe 3D secure

Comment reconnaître un spam ?

Vérifiez l'origine / la source de l'e-mail

Si vous ne la connaissez pas ou s'il s'agit d'une adresse étrange, soyez prudent !

Conseils

- N'ouvrez pas les pièces jointes envoyées par un expéditeur que vous ne connaissez pas. Soyez d'autant plus vigilant si elles sont en format *.docx, *.pdf, *.zip, *.scr, *.png...
- Configurez votre client de messagerie de sorte qu'il n'ouvre pas les pièces jointes dans le client même. Cela évitera la visualisation automatique des pièces jointes malicieuses et donc l'infection de votre ordinateur.

Contrôler le destinataire de l'e-mail

L'e-mail est-il adressé à une liste de personne ou est-il personnel ? Selon le contenu de l'e-mail, cette information peut vous mettre la puce à l'oreille.

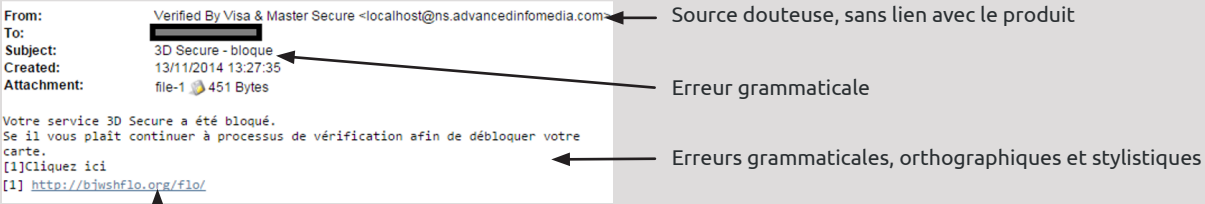
Lisez attentivement le contenu de l'e-mail

Si vous y repérez de trop nombreuses erreurs grammaticales, orthographiques et stylistiques, méfiez-vous !

Comparez le nom de l'expéditeur avec le(s) lien(s) intégré(s) dans l'e-mail

Les spams présentent très souvent un lien qui n'a rien à voir avec l'adresse e-mail de l'expéditeur ou de l'institution pour laquelle il usurpe l'identité (banque, commune, etc.) On parle alors d'*email spoofing.* Passez la souris sur le lien présent dans l'e-mail pour voir vers quoi il pointe réellement. Attention, surtout, à ne pas cliquer dessus !

Cas pratique (*phishing* réel)



Aucune relation entre le lien ni avec le sujet ('Subject') ni avec l'adresse e-mail ('From')

restena
réseau · sécurité · .lu

Protéger sa vie privée

Recommandations pour éviter un maximum de spams

- **Utilisez un nom d'utilisateur différent de votre adresse email**.
- **N'insérez pas votre adresse e-mail primaire sur des sites web douteux**, comme par exemple des sites qui vous promettent des gains ou des bons/coupons à valeur colossale.
- **Présentez votre adresse e-mail sous forme masquée**, si vous l'affichez sur un site web : intégrez l'adresse e-mail, par exemple, sous la forme [nom]@[education].lu ou (nom)[at](education)[dot]lu, ou représentez la sous forme d'image. Grâce à ce masquage, les robots primitifs ne peuvent pas reconnaître votre adresse.
- **Vérifiez les conditions générales des services en ligne auxquels vous vous abonnés** : lors de la souscription de services en ligne, il arrive souvent que des boîtes de contrôle ('*check box*') soient présélectionnées dans les conditions générales pour autoriser l'envoi d'autres publicités.
- **Ne répondez jamais à des messages non-sollicités.**

Filtrer son courrier grâce à des solutions anti-spam

Pour lutter contre le spam, des solutions anti-spam permettent de filtrer le courriel indésirable avant son arrivée dans la messagerie. Ces solutions spécialisées, peuvent être soit externalisées soit directement installées sur les postes de travail des utilisateurs ou sur les serveurs de messagerie.

Pour identifier efficacement les spams, les solutions anti-spam s'appuient sur une combinaison de techniques :

- analyse lexicale,
- listes noires,
- bases collaboratives, etc.

Information

- Les logiciels de messagerie les plus courants intègrent par défaut des solutions anti-spam.
- Un filtrage trop strict entraîne un risque de faux-positifs, un filtrage moins sévère augmente par contre la quantité de pourriels (spams) non détectés. Il convient donc de trouver le bon équilibre entre les deux.

Malheureusement, aucune solution n'est parfaite et les spammeurs évoluent et trouvent toujours de nouvelles méthodes pour contourner les mesures anti-spam mises en place, rendant la détection des spams de plus en plus difficile.

L'anti-spam idéal est une solution qui détecte 100% de spams et laisse 100% des bons messages, ou, en termes techniques : 100% de spams détectés, 0% de faux-négatifs* et 0% de faux-positifs**. Il est très difficile d'atteindre les 100% sans générer beaucoup de faux-positifs. C'est un aspect assez critique, puisque ces faux-positifs peuvent correspondre à des messages légitimes importants.

→ Ni les organismes officiels (administrations, banques, communes, etc.) ni la Fondation Restena ne demandent d'informations sensibles (carte de crédit, mot de passe...) par e-mail ou téléphone !

Offre de services

La Fondation Restena propose une protection anti-spam/anti-virus via son service 'Passerelle anti-virus/anti-spam' aux acteurs de la recherche, de l'éducation, de la culture, de la santé et de l'administration au Luxembourg, que leur messagerie soit hébergée ou non sur les serveurs RESTENA.

Pour plus d'informations sur ce service, rendez-vous sur restena.lu/services/passerelle

** Faux-négatif: un courriel indésirable non détecté*

*** Faux-positif : un courriel légitime classé par erreur en spam*

restena
réseau · sécurité · .lu