Newsletter N°5/2015

RESTENA
Réseau Téléinformatique de l'Education Nationale et de la Recherche

"Spam, spam, spam, lovely spam, wonderful spam, lovely spam, wonderful spam..." - la chanson "spam" de "Monty Python's Flying Circus"

LES MESSAGES SPAM & PHISHING

Les utilisateurs deviennent de plus en plus actifs sur le net par les réseaux sociaux, emails, chats, etc. Un phénomène qui s'est aussitôt installé est le message non-sollicité dans tous ses variétés.

Saviez-vous que 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 du ARPAnet*. Suite à des plaintes auprès de son entreprise, ce message non-sollicité fut appelé «spam» .

Cette édition de la newsletter présente différentes catégories de spam et d'hameçonnage, ainsi que des astuces pour la protection de la vie privée.

*ARPANET: la première version de l'Internet fondée par DARPA

Différentes catégories, un seul objectif commun: accéder à vos données personnelles!

- **Le message non-sollicité**

Il s'agit d'un message de publicité non-désiré, souvent d'origine douteuse, mais sans risque particulier. Souvent le contenu est d'origine pharmaceutique (viagra, ...).

- **Le spam nigérien**

Ce spam est appelé «spam 419» et très souvent d'origine africaine. Au Nigéria, l'article 419 du code pénal traite la fraude, d'où le nom. Le contenu du message promet un gros bénéfice, ou une large somme d'argent bloquée sur un compte en banque d'un employé gouvernemental.

- **L'hameçonnage ou « phishing »**

Le message de phishing est en général frauduleux, dans le but de tromper l'utilisateur sur son origine, comme par exemple la vague de phishing récente des emails masqués comme messages de l'Administration des contributions directes.

Un tel message a comme tentative de récupérer des informations privées sur l'utilisateur, comme par exemple, carte de crédit, mot de passe, adresse physique, email, etc., afin d'abuser de ces informations.

Fondation RESTENA
6, rue Richard Coudenhove-Kalergi
L-1359 Luxembourg
Tél: +352 42 44 09-1
Fax: +352 42 24 73

- **L'hameçonnage ou « phishing » (suite)**

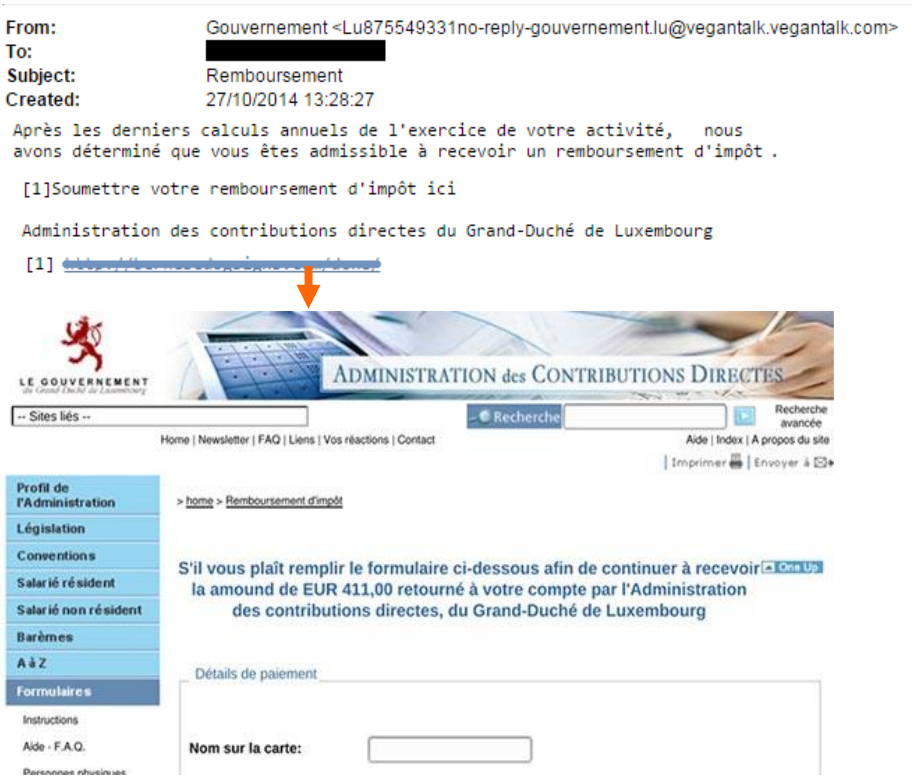
Le message phishing le plus primitif contient un texte simple avec un formulaire qui demande à l'utilisateur son nom d'utilisateur, email et mot de passe et de le renvoyer.

Une autre classe de messages phishing inclut un texte avec un lien vers un site web qui fait une saisie des données sur un formulaire. Une variante de ces messages contient un lien vers un site web, normalement compromis, qui achemine la requête vers un site qui télécharge automatiquement ou demande d'installer un logiciel (malveillant) sur l'ordinateur. Par ce logiciel, l'attaqueur peut recueillir des informations sur l'utilisateur, comme les mots de passe, les données bancaires, etc.

La classe de messages de phishing la plus sévère traite le «ransomware». Le message contient souvent un attachement en format *.zip, *.scr ou *.flv. Il s'agit normalement d'un logiciel malveillant qui bloque l'accès à l'ordinateur et l'utilisateur est invité de 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 sera encrypté et un paiement de la rançon ne garantira pas le décryptage. Dans un tel cas, il est conseillé de contacter un expert.

- **Exemple d'hameçonnage**

Courriel avec texte et lien vers un site phishing à l'apparence de l'administration des contributions directes par exemple.



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

- Type 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

- **Exemple d'hameçonnage avec logiciel malveillant et de cryptage (vague de phishing actuelle)**

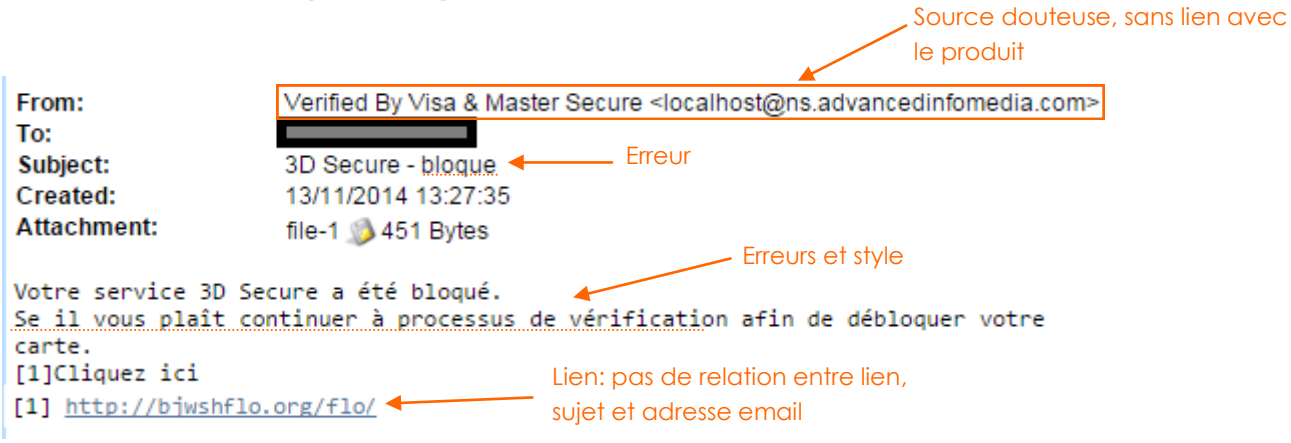
Le courriel avec un attachement, contient normalement un logiciel malveillant masqué comme facture ou contrat en format *.zip/ *.flv/…

Après avoir ouvert cet attachement, tous les fichiers sur le disque dur sont cryptés et un message s'affiche avec la demande de payer une rançon de 0.2 à 5 Bitcoins dans un délai de 72 à 96 heures, sinon le disque restera crypté (voir la capture d'écran). Dans ce cas, il est conseillé de contacter un expert ou de télécharger un logiciel qui peut supprimer le virus.

Quelques astuces pour reconnaître un spam

- Vérifiez l'**origine**/source de l'email — si vous ne la connaissez pas ou qu'il s'agit d'une adresse étrange, soyez prudent!
- Le **destinataire** — est-ce que l'email est adressé à une liste ou est-il personnel?
- **Contenu** — lisez le contenu de l'email! Soyez attentifs aux erreurs de **grammaire**, d'**orthographie** et de **style** (souvent traduit automatiquement)!
- **Lien** vers une page web — très souvent il s'agit d'un lien qui n'a rien à voir avec l'adresse email de l'expéditeur ou l'institution concernée (banque, commune,...). Comparez les noms de l'expéditeur avec le lien! Passez la souris sur le lien, pour voir le réel lien, sans cliquer!
- N'ouvrez pas des attachements dont l'expéditeur n'est pas connu! Soyez prudents avec des annexes en format *.docx, *.pdf, *.zip, *.scr, *.png!

Exemple réel d'un message phishing:



Tous les organismes officiels, comme les administrations, banques, communes, etc., ainsi que la Fondation RESTENA, ne demandent jamais des informations sensibles (carte de crédit, mot de passe,...) aux utilisateurs par email ou téléphone!

Comment éviter trop de spam?

- Utilisez un nom d'utilisateur différent de votre adresse email.

- N'insérez pas votre adresse email primaire sur des sites web douteux, comme par exemple des sites qui vous promettent des gains ou des bons/coupons à valeurs énormes.

- Si vous affichez votre adresse email sur un site web, présentez la sous forme masquée, comme par exemple:

  [nom]@[education].lu / (nom) [at] (education) [dot] lu

  ou bien représentez la sous forme d'image: 

  Par ce masquage, les robots primitifs ne peuvent pas reconnaître votre adresse.

- Lorsque vous vous abonnez à un service en ligne, vérifiez les conditions générales de celui-ci. Souvent des boîtes de contrôle («check box») sont sélectionnées qui permettent de vous envoyer d'autres publicités.

- Si vous recevez un message non-sollicité, ne répondez jamais!

Solutions Anti-Spam

Pour lutter contre le spam, il existe des solutions «anti-spam» qui permettent de filtrer le courriel indésirable avant son arrivée dans la messagerie. Ces solutions spécialisées, peuvent être installées directement sur les postes de travail des utilisateurs, sur les serveurs de messagerie, ou bien être externalisées. Les logiciels de messagerie les plus courants intègrent également en standard des solutions anti-spam.

Les solutions anti-spam proposées s'appuient sur une combinaison de techniques anti-spam (tels que l'analyse lexicale, listes noires, bases collaboratives, etc.) permettant d'identifier efficacement les spams. Malheureusement, aucune solution anti-spam n'est parfaite.

Les spammeurs évoluent et trouvent toujours de nouvelles méthodes pour contourner les mesures anti-spam mises en place et par conséquent, rendent la détection des spams de plus en plus difficile.

L'anti-spam idéal est une solution qui détecte 100% 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.

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.

*__Faux-négatif__: un courriel indésirable non détecté +__Faux-positif__: un courriel légitime classé par erreur en spam

La protection anti-spam/anti-virus dans notre service email

La protection anti-spam/anti-virus comporte un système de filtrage qui protège les boîtes aux lettres des utilisateurs contre les spams. Le système permet la détection et le marquage des messages spam.

Chaque email détecté comme spam contient dans son en-tête («header») une information indiquant qu'il s'agit d'un *******SPAM******* .

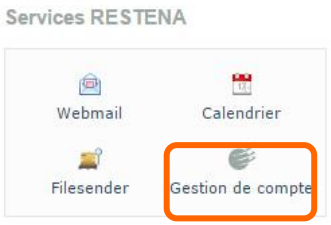
Par défaut, tous les messages ainsi marqués sont délivrés dans la boîte aux lettres de l'usager et peuvent, après téléchargement, être traités localement selon les préférences avec des outils intégrés dans les logiciels de messagerie les plus courants.

Si l'utilisateur opte pour une suppression directe des messages marqués, alors la messagerie bloque les spams et les messages infectés détectés avant le téléchargement dans sa boîte aux lettres. L'utilisateur ne reçoit donc plus les messages détectés. Aucune mesure locale de filtrage n'est nécessaire.

Cependant, des erreurs d'analyse peuvent se produire dans tous les produits. Donc, il est probable que certains messages peuvent être marqués *******SPAM******* à tort. On les appelle des faux-positifs. La suppression directe de ces messages comporte donc un certain risque de perte de courrier important. **Voilà pourquoi le choix du traitement de ces messages est à considérer comme étant entièrement sous la responsabilité de l'usager.**

Le défi: Trouver un bon équilibre entre les faux-négatifs et les faux-positifs! Il vaut mieux avoir un filtre moins strict avec des faux-négatifs, qu'un filtre trop sévère qui entraîne une suppression des faux-positifs, donc des emails légitimes supprimés. Nos ingénieurs essaient de réduire au maximum le taux de faux-positifs tout en essayant de conserver un bon niveau de détection de spam par une supervision constante et vigilante.

- **Comment changer la configuration de la protection email**

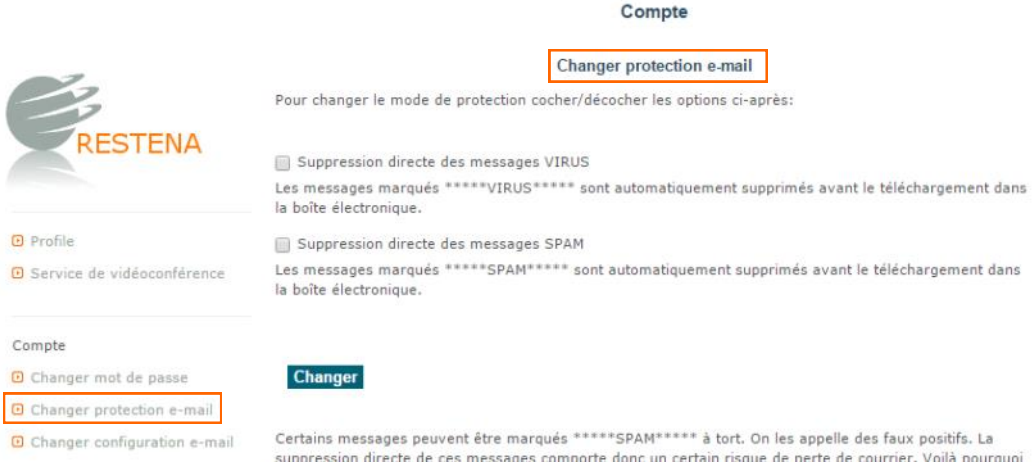


Vous pouvez activer et désactiver les filtres spam en utilisant l'outil de gestion de compte sur notre site web, sous:

Services RESTENA → Gestion de compte

Dans votre profile, sélectionnez la rubrique: **changer protection e-mail**

Ici vous pouvez choisir le mode de suppression des emails marqués comme *******SPAM******** et *******VIRUS********.



Autres articles sur l'hameçonnage, spam et d'autres arnaques en ligne

Bee-Secure:

https://www.bee-secure.lu/fr/clever-klicken

Cases:

https://www.cases.lu/les-phish-a-laffiche-ne-mordez-pas-a-lhamecon.html

Guichet public:

http://www.guichet.public.lu/entreprises/fr/gestion-juridique-comptabilite/contentieux/litiges/arnaques/index.html

En cas de problèmes ou questions

Si vous rencontrez des problèmes ou si vous avez des questions, contactez nous:

helpdesk@restena.lu ou par téléphone au +352 42 44 09 - 1

NEWS

Découvrez la nouvelle édition du magazine **CONNECT en** suivant ce lien: http://www.geant.net/MediaCentreEvents/news/Pages/CONNECT_issue_18_is_now_available.aspx

L'édition 2015 de la «**Terena Networking Conference**», la prestigieuse conférence des acteurs du domaine de l'éducation et de la recherche se déroulera à Porto, Portugal, du 15 au 18 juin 2015. Pour plus de détails, visitez la page web de la conférence:

https://tnc15.terena.org/

eduroam, le service sécurisé de réseau sans fil dédié à la communauté de l'Éducation et de la Recherche annonce plus de 17 millions de connexions au Luxembourg en 2014 . Lire le communiqué de presse entier: http://www.restena.lu/restena/Pdfs/CP_eduroam_fr.pdf