Sujet : [Information Sécurité SI] Risques d'usurpation d'identité électronique par courriel.
De : Responsable Sécurité des Systèmes d'Information <rssi@ac-lille.fr>
Date : 05/02/2018 17:01
Pour : rssi@ac-lille.fr

A l'attention de l'ensemble des personnels de l'Académie de Lille,

Mesdames, Messieurs,

N'importe quelle personne malveillante (appelée pirate dans la suite du message) peut vous envoyer un courriel en se faisant passer pour quelqu'un d'autre.

Cette ruse peu compliquée à réaliser s'apparente à mettre un faux nom d'expéditeur au verso d'une enveloppe postale.

Elle s'est multipliée ces dernières semaines sous la forme d'un courriel malveillant dont l'adresse électronique d'expédition ne correspond pas au nom d'expéditeur (exemple: Pierre Barrial <peu.probable@nonaclille.fr>).

De manière plus générale, la prudence s'impose et si vous vous posez une des questions ci-dessous, vous pourrez consulter sa réponse en bas de ce message.

1) Pourquoi un pirate tente ou tenterait d'usurper mon identité ?

2) Quel est l'objectif du pirate en usurpant mon identité ?

3) Comment savoir que l'identité de l'expéditeur d'un courriel que j'ai reçu est la bonne ?

4) Comment connaître la réelle identité de l'expéditeur d'un courriel que j'ai reçu ?

5) Comment savoir qu'un courriel est malveillant ?

6) J'ai reçu un courriel avec du contenu inapproprié/malveillant. Que dois-je faire ?

7) On m'a indiqué que j'avais envoyé un courriel avec du contenu inapproprié/malveillant. Que dois-je faire ?

Cordialement,

--

Région académique
HAUTS-DE-FRANCE

Pierre BARRIAL
*Equipe SSI > **R**esponsable **S**écurité des **S**ystèmes d'**I**nformation*

Adresse fonctionnelle rssi@ac-lille.fr

1) Pourquoi un pirate tente ou tenterait d'usurper mon identité ?

Le souhait du pirate est d'obtenir la confiance des personnes qui vous connaissent.

Elles se méfieront moins et elles seront ainsi plus facilement manipulables par le pirate.

2) Quel est l'objectif du pirate en usurpant mon identité ?

L'objectif du pirate est en général de vous amener à :

- lui confier vos informations personnelles (mots de passe, informations bancaires),

- installer un logiciel malveillant,

- consulter de la publicité, ...

Il pourra ainsi se rémunérer par la revente de vos informations personnelles, par votre consultation de la publicité, par le vol d'argent sur votre compte, ...

3) Comment savoir que l'identité de l'expéditeur d'un courriel que j'ai reçu est la bonne ?

L'identité de l'expéditeur d'un courriel ne peut pas être garantie.

En effet, il est possible techniquement pour un pirate de remplacer le nom de l'expéditeur et l'adresse électronique d'expédition.

Il est fréquent de ne voir que le nom remplacé.

Il peut également envoyer un courriel à la place d'une personne s'il connaît l'identifiant et le mot de passe de sa messagerie.

4) Comment connaître la réelle identité de l'expéditeur d'un courriel que j'ai reçu ?

Si une usurpation est bien faite, il est presque impossible de connaître la réelle identité de l'expéditeur. C'est le cas notamment lorsque le pirate possède l'identifiant et le mot de passe de l'expéditeur usurpé.

Cependant, s'il n'est pas toujours possible de connaître le réel expéditeur, il est en revanche possible d'identifier si le message est malveillant. Si le message est malveillant, l'identité de l'expéditeur n'a plus d'importance.

5) Comment savoir qu'un courriel est malveillant ?

Pour identifier un courriel malveillant, il faut être capable de reconnaître ses caractéristiques.

Une précaution élémentaire consiste à comparer le nom de l'expéditeur avec l'adresse électronique d'expédition (exemple: Pierre Barrial <peu.probable@nonaclille.fr>). S'il n'y a pas de correspondance entre les deux, vous pouvez déjà commencer à avoir des doutes sur l'origine du message.

L'académie d'Aix-Marseille met à disposition sur son site internet "Observatoire Académique de la Sécurité de l'Information" (https://www.pedagogie.ac-aix-marseille.fr/jcms/c_10472767/fr/accueil) une liste commentée de messages piégés.

En les étudiant, vous apprendrez à reconnaître facilement les futurs courriels malveillants que vous recevrez.

Voici un exemple classique de courriel où le pirate a tenté d'usurper l'identité de l'expéditeur :

https://www.pedagogie.ac-aix-marseille.fr/upload/docs/image/png/2017-10/spam171015.png

Si vous souhaitez apprendre à vous protéger contre ce type de malveillance ou sur les autres menaces d'internet, vous pouvez suivre le MOOC dédié à ce sujet sur le site https://www.secnumacademie.gouv.fr/

6) J'ai reçu un courriel avec du contenu inapproprié/malveillant. Que dois-je faire ?

Si vous avez le moindre doute à la lecture d'un courriel, ne prenez surtout pas le risque de cliquer sur un éventuel lien présent dans le courriel ou de cliquer sur une éventuelle pièce jointe.
Si vous connaissez l'expéditeur, vous pouvez lui demander par téléphone de confirmer l'envoi de ce courriel.

Si vous êtes certain-e du caractère malveillant du courriel, vous pouvez le supprimer.

7) On m'a indiqué que j'avais envoyé un courriel avec du contenu inapproprié/malveillant. Que dois-je faire ?

Un pirate tente sûrement d'usurper votre identité.

Même s'il n'est pas garanti que le pirate connaisse votre mot de passe de messagerie, par mesure de précaution, il est préférable de le changer au plus vite.

Cependant, votre nom et votre adresse de messagerie sont maintenant connus par les pirates. Ils pourront les utiliser pour tenter de tromper la méfiance de vos connaissances.

Il ne vous reste plus qu'à informer les personnes qui vous ont prévenu-e que vous n'êtes pas à l'origine de ces messages.