



Déceler un mail de filoutage

Objet :

Voici le scénario : vous recevez un mail, vous demandant de remplir un formulaire et de ressaisir votre mot de passe pour différentes raisons :

vous avez dépassé votre quota de messagerie
votre compte a été piraté
etc

Si vous ne le faites pas, le mail vous informe que votre compte va être supprimé.

Certains mails de filoutage vous demandent également de répondre en indiquant votre mot de passe.

Comment savoir si ce mail a été émis par un collègue de votre DSI, ou si c'est une tentative de récupération de votre mot de passe ?

Tout d'abord, pourquoi un pirate veut récupérer votre mot de passe ?

Si une personne ou une organisation "criminelle" possède votre mot de passe de l'ENT UBO, elle peut envoyer des dizaines de milliers de mail en votre nom (publicité - spam, autre filoutage, etc). De ce fait, l'UBO est considéré comme spammeuse et est bloquée pour l'envoi de mails. En conséquence, tous les collègues ne peuvent plus envoyer de mails à l'extérieur, votre DSI doit contacter les différents organisation de contrôle anti-spam, qui peuvent bloquer les mails de l'UBO plusieurs jours ou semaines.

Voici quelques indices pour déceler un mail de filoutage :

Tout d'abord, la DSI ne vous demande jamais votre mot de passe par mail !

Aucun membre de DSI ne vous envoie de mail en anglais

Le français est approximatif (en tout cas, encore plus approximatif que nos mails ;-)). Gros soucis avec l'orthographe ou avec la grammaire.

La signature des mails est autre que 'La Direction des Systèmes d'Information' ou la DSI.

L'adresse d'expédition n'est pas un mail du genre informations.dsi@univ-brest.fr ou service.dsi@univ-brest.fr

Si on vous indique de saisir vos données sur un formulaire, le lien indiqué (l'URL) n'est pas de type xxx.univ-brest.fr

Illustrations :

De : Université de Bretagne Occidentale (UBO) [redacted@univ-brest.fr]  **message semblant provenir d'un collègue**
 Date d'envoi : jeudi 19 décembre 2013 02:41
 À : [redacted@univ-brest.fr]
 Objet : [j [redacted@univ-brest.fr] : We Are So Sorry For The Inconveniece {5:41:42 PM}

Hello [redacted@univ-brest.fr],

We recently updated our service and your access has been limited To re-confirm your details please login from the link below :

univ-brest.fr

signature fantaisiste et en anglais

Copyright ©2014 University of Western Brittany. All rights reserved. 

Sujet:Attention!
Date :Sun, 23 Oct 2011 23:31:33 -0700
De :Helpdesk Support Webmail Centre <webmailupgrade05@gmail.com>
Répondre à :webmailupgrade05@gmail.com  **mail hors univ-brest.fr**
Pour :undisclosed-recipients;

Il a été remarqué que vous avez dépassé votre quota Email de 450 Mo et vous avez besoin d'élargir votre quota. En moins de 48 heures si vous n'avez pas mettre à jour votre limite de quota email, votre compte e-mail sera désactiver.

Pour élargir votre quota mail à 5Go, utiliser l'un des ci-dessous
 Liens Web:

<http://tinyurl.com/administratorform11>  **lien différent de xxx.univ-brest.fr**

Nous vous remercions de votre compréhension.
 Copyright © 2011 Helpdesk Soutien Webmail Centre.

Sujet:Revalider votre boîte mail
Date :Mon, 30 Dec 2013 09:59:32 +0100 (CET)
De :Francois Maerten <francois.maerten@etu.univ-tours.fr>
Répondre à :Francois Maerten <francois.maerten@etu.univ-tours.fr>
Pour :undisclosed-recipients;  **adresses mails de univ-tours !**

Votre boîte aux lettres a dépassé la limite de stockage qui est de 20 Go que définie par votre administrateur, vous utilisez actuellement sur 20,9 Go, vous ne pouvez pas être en mesure d'envoyer ou de recevoir de nouveaux messages jusqu'à ce que vous re-valider votre boîte aux lettres.

<http://free.allforms.mailjol.net/u/6a118c41.php>  **l'URL ne se contient pas univ-brest**

Pour re-valider votre boîte aux lettres s'il vous plaît cliquer ou copier-coller le lien ci-dessus et de remplir les données demandées de

Merci,
 © Webmail Inc. Tous droits réservés  **signature non DSI**

Plus d'Infos :

<http://fr.wikipedia.org/wiki/Hameçonnage>

<http://www.eila.univ-paris-diderot.fr/sysadmin/securite/virus/phishing>

<http://sosconso.blog.lemonde.fr/2014/01/12/mail-ou-spam-phishing-initiative-vous-permet-de-le-savoir/>

<http://www.lefigaro.fr/secteur/high-tech/2014/02/03/01007-20140203ARTFIG00111-donnees-personnelles-qu-e-st-ce-que-le-phishing.php>

contributeurs :

Nom	Date	type modifications	version
AM JGA	28/3/2014	Première version	1.0.0

