

Messages suspects - hameçonnage



Attention: Tentative d'hameçonnage sur l'Université de Valenciennes

Courriels Frauduleux

Nous attirons votre attention sur les nombreuses tentatives de récupération de données personnelles qui ont cours sur Internet.

Généralement envoyé par courriel, ces tentatives visent à récupérer vos identifiants de connexion (login/password), bancaires (numéros de CB), de sécurité sociale,...

Les méthodes employées sont de plus en plus travaillées à la fois dans la forme et dans le public visé.

Cette technique est appelée **hameçonnage** (ou **phishing** en anglais).

Voir l'article <http://fr.wikipedia.org/wiki/Phishing>

Parmi les « phishing » diffusés dernièrement, plusieurs concernent le fonctionnement des webmails (dont celui de l'Université de Valenciennes).

Même s'il y a quelques incohérences (message non nominatif, rédigé dans un français approximatif), ces messages sont relativement crédibles. Cela montre aussi l'intérêt qu'accorde certains délinquants à obtenir des accès sur des sites d'enseignement ou de recherche afin d'usurper des identités, voler des données, spammer depuis votre messagerie...

Nous vous remercions d'être vigilants et prudents, de ne jamais communiquer d'identifiants... Tout message vous demandant de communiquer un mot de passe ou un numéro de carte bleue doit être considéré comme suspect et dangereux. **Il ne faut jamais répondre à ces messages , ni cliquer sur les liens contenus dans ces messages.**

<note important> Dans le cas où vous auriez saisi des informations personnelles sur un des sites pirates, il est important de prendre très rapidement les mesures nécessaires de protection. Si tel était le cas, prévenez l'administrateur de la messagerie (rssi at univ-valenciennes.fr) le plus rapidement possible. </note>

Mise en place de protection au sein de l'université

1. Mise en place de filtre de messagerie spam et phishing basé sur des listes de domaines connues pour envoyer ce type de mail.
2. Mise en place de filtre d'accès Web à ces sites reconnues comme étant du phishing
3. Mise en place de scripts de détection d'envoi de courriel suspect avec blocage automatique de l'émetteur.

Repérer un message d'hameçonnage

Vous venez de recevoir un message qui vous demande pour des raisons diverses et variées d'accéder à un site web afin de : - valider votre quota de mail - valider votre adresse mail - valider votre inscription sur un nouveau service - valider votre compte pour tout et n'importe quoi

Par exemple :

“Message à l'attention des personnels et des étudiants de l'Université De Valenciennes”

Bonjour à tous, Nous vous rappelons une dernière fois que l'intranet de Université de Valenciennes . a été séparé du site web externe.

Dorénavant, lorsque vous souhaitez consulter ou modifier l'intranet , il vous faudra IMPÉRATIVEMENT accéder à celui-ci via le lien suivant :

[Validation de l'adresse email](#)

Car ceux-ci ne seront pas enregistrés et toute modification sera perdue.

Merci d'effectuer vos modifications sur le nouvel intranet, dont l'adresse vous sera communiquée ultérieurement. Très cordialement La Direction de la Communication

Passer votre souris sur l'url et regarder l'adresse du site web sur lequel vous allez aller.



Est ce bien une adresse liée au domaine de l'Université de Valenciennes (.univ-valenciennes.fr) ?

Malheureusement , vous avez cliqué. Vous voyez l'image pour vous connecter à l'uvhc :




Vous êtes sur le point de communiquer vos identifiants , mais il vous reste une chance !!!

Regardez dans la barre d'url si vous voyez cette image :



Vous devez voir “le cadenas et UVHC(Université de Valencienn..(FR)” en vert

 Si pas , alors ne pas entrer vos identifiants.

Vous pouvez également aller plus loin et cliquer sur le cadenas et vous verrez alors :

puis

Exemple de mail d'hameçonnage:

Reçu le 07 02 2016

De: "Université De Valenciennes" <new-serviceweb-info@webmail.com>
À: "
Envoyé: Dimanche 7 Février 2016 22:36:49
Objet: Validation de l'adresse email

"Message à l'attention des personnels et des étudiants de l'Université De Valenciennes"

Bonjour à tous,

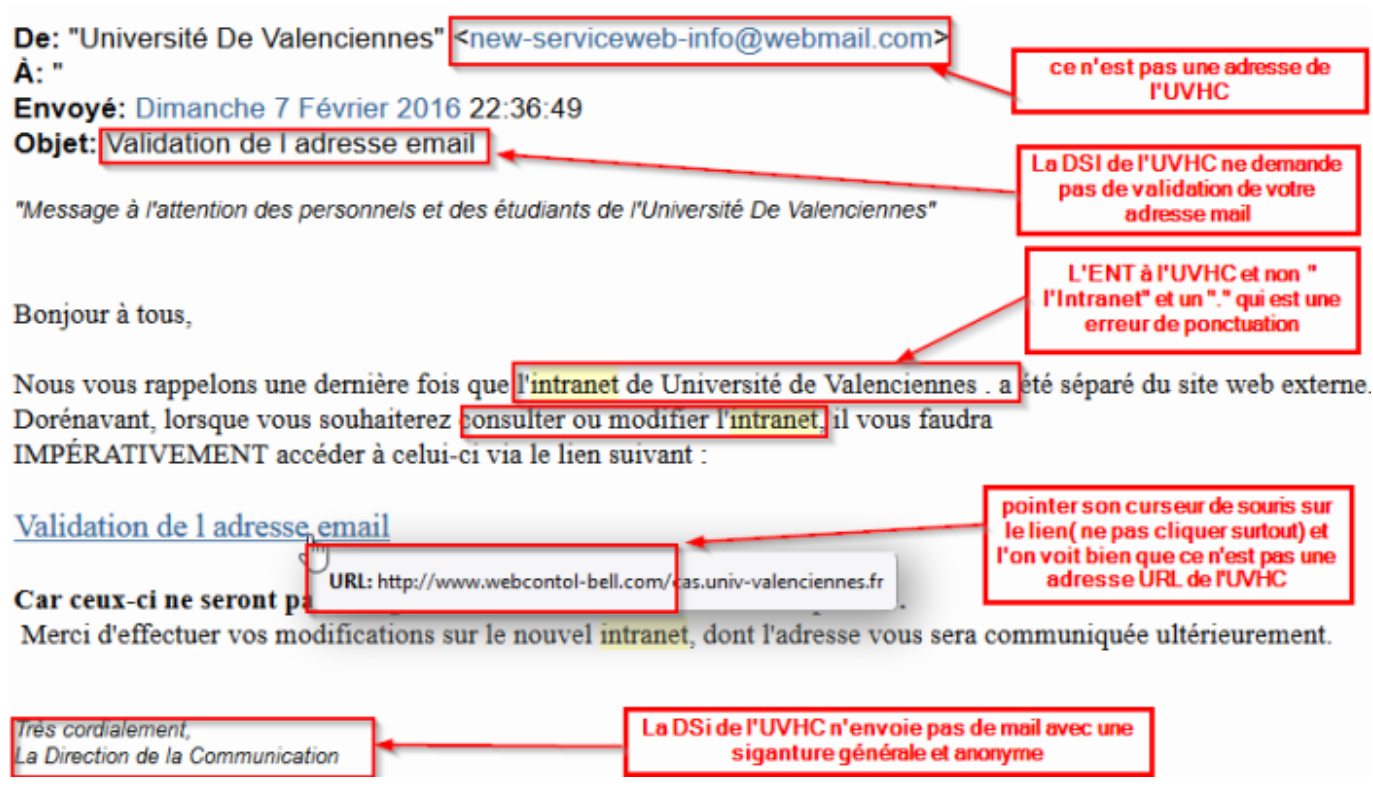
Nous vous rappelons une dernière fois que l'intranet de Université de Valenciennes . a été séparé du site web externe. Dorénavant, lorsque vous souhaitez consulter ou modifier l'intranet, il vous faudra IMPÉRATIVEMENT accéder à celui-ci via le lien suivant :

Validation de l'adresse email

Car ceux-ci ne seront pas URL: <http://www.webcontol-bell.com/cas.univ-valenciennes.fr>

Merci d'effectuer vos modifications sur le nouvel intranet, dont l'adresse vous sera communiquée ultérieurement.

Très cordialement,
La Direction de la Communication



Annotations:

- ce n'est pas une adresse de l'UVHC
- La DSI de l'UVHC ne demande pas de validation de votre adresse mail
- L'ENT à l'UVHC et non " l'Intranet" et un "." qui est une erreur de ponctuation
- pointer son curseur de souris sur le lien (ne pas cliquer surtout) et l'on voit bien que ce n'est pas une adresse URL de l'UVHC
- La DSI de l'UVHC n'envoie pas de mail avec une signature générale et anonyme

Reçu le 01 02 2016

De: "L'université de valenciennes" <communication@univ-valenciennes.fr>

Envoyé: Lundi 1 Février 2016 23:08:44

Objet: Modification de votre Identifiant

La DSI de l'UVHC ne demande pas de modification de votre identifiant

Il n'y a pas d'Espace Client à l'UVHC mais un ENT (Espace Numerique de Travail)

Pointer son curseur de souris sur le lien (ne pas cliquer surtout) et l'on voit que ce n'est pas une adresse URL de l'UVHC mais une adresse extérieure

La DSI de l'UVHC n'envoie pas de mail avec une signature générale et anonyme

Chère/Cher,

Vous avez saisi une autre adresse email comme adresse électronique de contact pour votre identifiant Espace Client. Pour terminer le processus, nous devons vérifier qu'il s'agit bien de Votre identifiant. Cliquez simplement sur le lien ci-dessous et ouvrez une session à l'aide de votre identifiant et de votre mot de passe.

[Vérifiez maintenant >](#)

Pourquoi ce URL: <https://psicol.co/ticket/archivos/index.html> ?

L'envoi de ce courrier électronique s'applique lorsqu'une personne ajoute ou modifie Votre identifiant pour un compte université de valenciennes. Si cela ne vous concerne pas, ne vous inquiétez pas. Personne ne peut utiliser Votre identifiant comme adresse de contact sans votre vérification.

Pour plus d'informations, consultez la rubrique Questions et réponses.

Merci,
Université de valenciennes

Reçu le 02 04 2011

facebook

Hi,

You haven't been back to Facebook recently. You have received notifications while you were gone.

2 messages

Thanks,
The Facebook Team

To login to Facebook, follow the link below:
MailScanner soupçonne le lien suivant d'être une tentative de fraude de la part de "luxurytubs.couk"
http://www.facebook.com/nv?find-friends%2F&mid=24ef9392ab6b454b4fe0a321c22be0&bcode=TxJu&n_m=postmaster%40univ-valenciennes.fr

This message was intended for postmaster@univ-valenciennes.fr. If you do not wish to receive this type of email from Facebook in the future, please click [here](#) to unsubscribe.
Facebook, Inc. P.O. Box 10005, Palo Alto, CA 94303

Reçu le 12 03 2011

You have recieved A Hallmark E-Card.

Hello!

You have recieved a Hallmark E-Card.

To see it, click [here](#),

There's something special about that E-Card feeling. We invite you to make a friend's day and **send one**.

Hope to see you soon,
Your friends at Hallmark

Your privacy is our priority. Click the "Privacy and Security" link at the bottom of this E-mail to view our policy.

Hallmark.com | Privacy & Security | Customer Service | Store Locator

Reçu le 11 03 2011

— DIRECTION DE L'ADMINISTRATEUR WEBMASTER.eml —

Sujet: DIRECTION DE L'ADMINISTRATEUR WEBMASTER
De : DE SANS NICOLAS Fabien <fabien.desansnicolas@ville-grenoble.fr>
Date : Thu, 10 Mar 2011 10:24:33 +0100
Pour : undisclosed-recipients::

Un ordinateur de maintenance de base est actuellement en cours sur notre Webmail Message Center. Notre Centre de messages doit être remis à zéro en raison de la grande quantité de spams que nous recevons quotidiennement. Pour re-valider votre boîte aux lettres S'il vous plaît Cliquez sur le lien ci-dessous:

<http://www.sivicouncil.org/form/use/anti-virus/form1.html>

Le défaut de re-valider votre boîte aux lettres rendra votre e-mail en-active de notre base de données.
System Administrator
192.168.0.1



Reçu le 25 02 2011

Notification d'impôt - Remboursement

Après les derniers calculs annuels de l'exercice de votre activité, nous avons déterminé que vous êtes admissible à recevoir un remboursement d'impôt de ₣ 178,80.

S'il vous plaît soumettre la demande de remboursement d'impôt et nous permettre de 10 jours ouvrables pour le traitement.

Pour accéder au formulaire pour votre remboursement d'impôt, [cliquez ici](#)

Un remboursement peut être retardé pour diverses raisons. Par exemple la soumission des dossiers non valides ou inscrites après la date limite.

f Reçu le 18 02 2011

DERNIER AVERTISSEMENT ADMINISTRATEUR DU SYSTÈME
Boîte aux lettres est presque pleine.
23 Go à 20 Go

Votre boîte aux lettres a dépassé la limite de 20 Go de stockage est définie par l'administrateur, vous travaillez à 20.9GB, qui Il peut ne pas être en mesure d'envoyer ou de recevoir Messages avant de vous mettre dans votre boîte aux lettres. Pour valider la boîte aux lettres, s'il vous plaît cliquez sur:

<http://bestvoipcarrier.com/onlineform/Use/fr1/form1.html>

Remplissez les informations dans le lien ci-dessus et cliquez sur Soumettre
"Envoyer un fichier
Merci
L'administrateur du système.
liste phonétique lire

Reçu le 12 02 2011

De : Caisse-Epargne@caissedepargne.srv192.com <Caisse-Epargne@caissedepargne.srv192.com>
Date : 12 février 2011 15:21:54 HNEC
À :
Objet : **{Disarmed} Banque en ligne alerte!**

Chers xxxxxx@univ-valenciennes.fr,

Cet e-mail a été envoyé par **Caisse D' Epargne** vous informer que nous n'avons pas pu vérifier les détails de votre compte.

- 1.Soumettre des informations incorrectes pendant le processus de registre
- 2.Un récent changement dans vos renseignements personnels

Pour cette raison, de veiller à ce que votre service de **banque en ligne** n'est pas interrompu, nous vous prions de confirmer et mettre à jour vos informations d'aujourd'hui en suivant le lien ci-dessous :

MailScanner soupçonne le lien suivant d'être une tentative de fraude de la part de "www.dadero.de"
<https://caisse-epargne.fr/casultlh.aspx?plzsid=10&sac=066&user=scolar2@univ-valenciennes.fr>

Si vous avez déjà confirmé votre information alors s'il vous plaît ignorer ce message

Caisse d'epargne banque de services aux membres

© Caisse d'Epargne 2011

From:
<https://www.uphf.fr/wiki/> - **Espace de Documentation**

Permanent link:
https://www.uphf.fr/wiki/doku.php/outils/securite_et_reglementation/cybersecurite/hameconnage

Last update: **2016/04/11 13:41**

