

Avril 2020

ANSI - CSIRT

TECHNIQUE DE PHISHING: Display Name Impersonation

LES PRINCIPES DE CETTE TECHNIQUE

LES CONSEILS POUR ÉVITER D'EN ÊTRE VICTIME



الوكالة الوطنية للأمن المعلوماتية
Agence Nationale de la Sécurité Informatique

C'EST QUOI LE « DISPLAY NAME IMPERSONATION »

L'usurpation du nom au niveau de l'entête de l'e-mail consiste à définir des noms trompeurs sur leurs comptes de messagerie afin d'induire en erreur les destinataires. Ce nom ne fait pas partie de l'adresse e-mail elle-même: c'est le nom affilié au compte qui apparaît généralement avant l'adresse e-mail dans les boîtes de réception.

to: unspecified recipient
from: **HSBC BANK <ricardoahumada@alfresco.net.co>**
date: 01/24/2018 08:42 PM

Dear Sir/Madam,

The attached payment advice is issued at the reference only.

Yours faithfully,
Global Payments and Cash Management
HSBC

HSBC 
Commercial Bankina

Display Name : HSBC BANK

L'adresse email d'envoi :

ricardoahumada@alfresco.net.co



L'adresse e-mail de l'émetteur ne fait pas partie du nom du domaine de cette banque



COMMENT LES PIRATES MANIPULENT-ILS LE « DISPLAY NAME »

Même pour les personnes ayant peu, ou pas de connaissances, techniques approfondies, la manipulation du « display Name » reste très facile à réaliser : l'opération peut être effectuée dans presque tous les principaux clients de messagerie, l'exemple suivant est celui de Gmail :

Accueil

Informations personnelles

Données et personnalisation

Sécurité

Contacts et partage

Paielements et abonnements

Informations personnelles

Informations de base utilisées sur les services Google (nom, photo, etc.)

Profil

Certaines de ces informations peuvent être vues par les autres utilisateurs des services Google.
[En savoir plus](#)

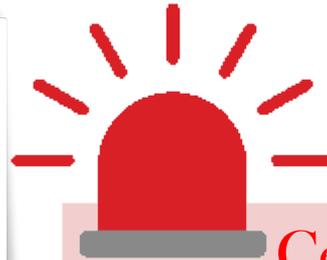
PHOTO Personnalisez votre compte en ajoutant une photo

| | | |
|--------------|-----------------|---|
| NOM | Sofien Masmoudi | > |
| ALIAS | sofien007 | > |
| ANNIVERSAIRE | 3 mai 1982 | > |
| SEXE | Homme | > |

Display Name



SMARTPHONE & « DISPLAY NAME IMPERSONATION »



Cette approche est particulièrement efficace sur les appareils mobiles, car le champ « de » est masqué par défaut sur les écrans mobiles.



CONSEILS DE PRÉVENTION DU PHISHING (1/3)



Vérifiez l'authenticité de l'adresse e-mail :

Vérifier le nom de l'expéditeur n'est pas suffisant car les escrocs peuvent usurper l'identité de votre banque ou de l'un de vos collègues. Il faut, donc, vérifier toutes les conversations précédentes pour vérifier la véracité du mail reçu.



Recherchez d'éventuelles fautes :

L'existence d'éventuelles fautes d'orthographe ou de grammaire dans un e-mail peuvent être un signe d'une activité frauduleuse.



Il ne faut jamais communiquer des informations sensibles:

La plupart des entreprises évitent de demander les informations personnelles de leurs clients par e-mail.

CONSEILS DE PRÉVENTION DU PHISHING (2/3)



Méfiez-vous des messages urgents:

Les utilisateurs sont plus susceptibles de communiquer des informations sensibles lorsqu'ils sont stimulés par un sentiment d'urgence.



Vérifiez la véracité des informations !

Si vous êtes perplexe quant à toute demande faite par e-mail, appelez la source directement pour vérifier la véracité de la demande.

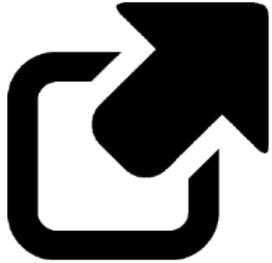


Evitez d'ouvrir des pièces jointes non sollicitées :

Les pièces jointes peuvent contenir des programmes malveillants.



CONSEILS DE PRÉVENTION DU PHISHING (3/3)



Vérifiez les liens externes :

Avant d'ouvrir les liens , survoler le texte du lien pour vérifier le site Web qu'il cible.



Contactez l'ANSI :

Si vous n'êtes pas sûr de la validité de l'e-mail, signalez-le sur:
incident@ansi.tn
assistance@ansi.tn
www.ansi.tn



الوكالة الوطنية للسلامة المعلوماتية

Agence Nationale de la Sécurité Informatique



الوكالة الوطنية للسلامة المعلوماتية
Agence Nationale de la Sécurité Informatique



**49, AVENUE JEAN
JAURÈS, 1000 TUNIS**



ansi@ansi.tn



**(+216) 71 846 020
(+216) 71 848 575**



(+216) 71 846 363



www.ansi.tn



<https://www.linkedin.com/in/ansi-tuncert-80bb4b172/>



/ansitn



<https://twitter.com/ATuncert>