

Identifier un mail frauduleux

Pour vous aider à identifier des messages frauduleux que vous pourriez recevoir dans votre boite de messagerie, voici les derniers mails recensés à l'Université de Nantes.

Ne jamais répondre à ces messages Delete!

février 2019

1 - Message frauduleux

De : "Service Support Utilisateurs - Université de Nantes" supporte.gpi-servicescentraux@univ-nantes.fr

Sujet : [SPAM] Notification en attente: Télécharger pour voir votre fichier

message :

De Service Support Utilisateurs - Université de Nantes <supporte.gpi-servicescentraux@univ-nantes.fr> ☆

Sujet: [SPAM] Notification en attente: Télécharger pour voir votre fichier

20/02/2019 à 09:33

Attention:

Votre document a été mis en attente. Veuillez télécharger et vous connecter pour publier les documents

Université de Nantes.htm

 **Webmail**
Étudiant - Université de Nantes

Votre identifiant est **votre** numéro d'étudiant précédé de la lettre e.
Par exemple: **e44719**

Identifiant
Mot de passe

Ma communication universitaire

1 pièce jointe : Université de Nantes.htm 7,3 Ko

Répondre Transférer Archiver Indésirable Supprimer Autres

Non lu x 0 Total : 105 Panneau d'aujourd'hui

2 - Message frauduleux

De : adresse mail de l'usager

Sujet : Votre compte a été piraté

message :

Last update: 2019/03/04 securite:actualites:mails_frauduleux https://wiki.univ-nantes.fr/doku.php?id=securite:actualites:mails_frauduleux&rev=1551705647
14:20

De : [utilisateur](#) @univ-nantes.fr ☆
Sujet [SPAM] Votre compte a été piraté!
Pour : [utilisateur](#) @univ-nantes.fr ☆
Répondre Transférer Archiver Indésirable Supprimer Auc
15/02/2019

Je vous value!

J'ai de mauvaises nouvelles pour vous.
10/11/2018 - ce jour-là, j'ai piraté votre système d'exploitation et obtenu un accès complet à votre compte à partir [utilisateur](#) @univ-nantes.fr

Pas la peine de changer le mot de passe, mon logiciel malveillant l'intercepte à chaque fois.

Comment c'était:
Le logiciel du routeur auquel vous êtes connecté ce jour-là comportait une vulnérabilité.
J'ai d'abord piraté ce routeur et y ai placé mon code malveillant.
Lorsque vous êtes entré sur Internet, mon cheval de Troie était installé sur le système d'exploitation de votre appareil.

Après cela, j'ai effectué une sauvegarde complète de votre disque (j'ai tout votre carnet d'adresses, l'historique des sites de visionnage, tous les fichiers, les numéros de téléphone et les adresses de tous vos contacts).

Il y a un mois, je voulais verrouiller votre appareil et demander un peu d'argent pour le déverrouiller.
Mais j'ai jeté un œil sur les sites que vous visitez régulièrement, et j'ai eu grand plaisir à voir vos ressources préférées.
Je parle de sites pour adultes.

Je veux dire - tu es un grand pervers. Vous avez une fantaisie débridée!

Après cela, une idée m'est venue à l'esprit.
J'ai fait une capture d'écran du site Web Intimeo vous contentez-vous (Comprends-tu ce que je veux dire?).
Après cela, j'ai fait une vidéo de votre plaisir (en utilisant la caméra de votre appareil). Il s'est avéré magnifique!

Je suis fermement convaincu que vous ne voudriez pas montrer ces photos à vos parents, amis ou collègues.
Je pense que 334€ est une très petite somme pour mon silence.
En plus, j'ai passé beaucoup de temps sur!

J'accepte de l'argent uniquement en Bitcoin.
Mon portefeuille BTC: 16xg78KbzSR2TrcY3hR7ViMtJecyyZEoQJ

Vous ne savez pas comment reconstruire un portefeuille Bitcoin?
Dans n'importe quel moteur de recherche, écrivez "comment envoyer de l'argent à un portefeuille de la BTC".
C'est plus facile que d'envoyer de l'argent à une carte de crédit!

Pour le paiement, vous avez un peu plus de deux jours (exactement 50 heures).
Ne vous inquiétez pas, la minuterie commencera au moment où vous ouvrez cette lettre. Oui, oui .. cela a déjà commencé!

3 - Message frauduleux

Sujet : Vérifier le compte

Date : Mon, 4 Mar 2019 12:29:18 +0000

De : Kurt D Jansen Kurt.D.Jansen@rexnord.com

Chers utilisateurs de boîtes aux lettres,

Vous avez reçu cet e-mail, car nous migrons tous les comptes de messagerie vers la fonctionnalité anti-spam Outlook Web-mail 2019. Par conséquent, tous les utilisateurs actifs doivent vérifier et se connecter pour que la mise à niveau et la migration prennent effet maintenant. Ceci est fait pour améliorer la sécurité et l'efficacité en raison des récents spams reçus.

Tous les utilisateurs sont invités à CLIQUER ICI pour passer à l'anti-spam Outlook Web-mail 2019.

Si vous ne pouvez pas exécuter cette tâche dans les 3 prochains jours à partir de votre session de connexion actuelle, votre compte cessera de recevoir des courriers électroniques et le contenu de votre boîte aux lettres, y compris tous les courriers électroniques, les paramètres et les dossiers, sera définitivement supprimé.

Cordialement,

Support technique

Copyright 2019

Bonnes pratiques pour la sécurité

A consulter

1. [Donner l'alerte sur un mail frauduleux !! !](#)
2. [Les bonnes pratiques pour la sécurité](#)
3. [Comment éviter le vol d'identité](#)

From:

<https://wiki.univ-nantes.fr/> - Wiki

Permanent link:

https://wiki.univ-nantes.fr/doku.php?id=securite:actualites-mails_frauduleux&rev=1551705647

Last update: **2019/03/04 14:20**

