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 :

---

2 - Message frauduleux

De : *adresse mail de l'usager*

Sujet : Votre compte a été piraté

message :

4 - Message frauduleux

Ce message semble être envoyé depuis votre propre adresse. Bien évidemment, il n'en est rien en réalité.

Sujet : This account has been hacked! Change your password right

```
now!\\
```

Date : Sat, 12 Jan 2019 17:59:31 -0000
De : votre propre adresse mail

<note>You may not know me and you are probably wondering why you are getting this e mail, right?

I'm a hacker who cracked your devices a few months ago.

I sent you an email from YOUR hacked account.

I setup a malware on the adult vids (porno) web-site and guess what, you visited this site to have fun (you know what I mean).

While you were watching videos, your internet browser started out functioning as a RDP (Remote Control) having a keylogger which gave me accessibility to your screen and web cam.

After that, my software program obtained all of your contacts and files.

You entered a passwords on the websites you visited, and I intercepted it.

Of course you can will change it, or already changed it.

But it doesn't matter, my malware updated it every time. What did I do?

I created a double-screen video. 1st part shows the video you were watching (you've got a good taste haha . . .), and 2nd part shows the recording of your web cam.

Do not try to find and destroy my virus! (All your data is already uploaded to a remote server)

– Do not try to contact with me – Various security services will not help you; formatting a disk or destroying a device will not help either, since your data is already on a remote server.

I guarantee you that I will not disturb you again after payment, as you are not my single victim. This is a hacker code of honor.

Don’t be mad at me, everyone has their own work.

Exactly what should you do?

Well, in my opinion, $1000 (USD) is a fair price for our little secret. You'll make the payment by Bitcoin (if you do not know this, search “how to buy bitcoin” in Google).

My Bitcoin wallet Address:

1AyRZviUxoBaCU1pJM5m7C1V2LdhPYiRcB

(It is cAsE sensitive, so copy and paste it)

Important:

You have 48 hour in order to make the payment. (I've a facebook pixel in this mail, and at this moment I know that you have read through this email message).

To track the reading of a message and the actions in it, I use the facebook pixel.

Thanks to them. (Everything that is used for the authorities can help us.)

If I do not get the BitCoins, I will certainly send out your video recording to all of your contacts including relatives, coworkers, and so on. Having said that, if I receive the payment, I'll destroy the

video immidiately.

If you need evidence, reply with “Yes!” and I will certainly send out your video recording to your 6 contacts. It is a non-negotiable offer, that being said don't waste my personal time and yours by responding to this message. </note>

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