Tip sheet

SPAM & PHISHING MESSAGES

As users have become increasingly active on the internet through social networks, emails and chats, a phenomenon has immediately set in: spam and phishing messages. Both types of messages have one common purpose: to access your personal data.

Main spam and phishing categories

Unsolicited message

Unwanted advertising message, frequently dubious origin, without any particular risk.

Its content mainly focuses on pharmaceutical (viagra, etc.)

SCAM

Spam promising a large profit or a large sum of money blocked in the bank account of a government employee, for example.

Such a spam is also known as nigerian spam or "spam 419", as in Nigeria, Criminal Code Section 419 deals with fraud.

Did you know?

The first unsolicited message was accidentally sent in 1978.

Gary Thuerk, a salesman, sent an advertising message to more than 400 of the 2,600 users of ARPAnet, the very first version of the Internet. Following numerous complaints to his company, this unsolicited message was called "spam".

Phishing

Spam, generally containing fraudulent email, misleading the user on its origin in order to obtain his private information (credit card, password, physical address, email, etc.) so to misuse it.

There are several classes of phishing.

Class 01 (Primitive Phishing)

A simple text prompts the user to complete, and then return, a form with its username, email and password.

Classe 02

A text, including a link to a website, prompts the user to type data into a form. A variant of these messages contains a link to a website, normally compromised, routing the request to a website that automatically downloads or asks to install (malicious) software on the computer.

With this software, the hacker can collect information about the user, such as passwords, bank details, etc.

Classe 03 (Malicious spam or Malspam)

The message often contains an attachment in *.zip, *.scr or *.flv format. This is normally malicious software that blocks access to the computer. The user is prompted to pay a ransom by prepaid card (e.g. safepaycard) or money transfer agency (e.g. Western Union).

In the worst-case scenario, the whole hard disk or file server is encrypted, and the ransom payment does not guarantee any decryption. In this scenario, victims are urged to contact an expert.

© Copyright Restena Foundation - November 2020 | www.restena.lu

restena
réseau · sécurité · .lu

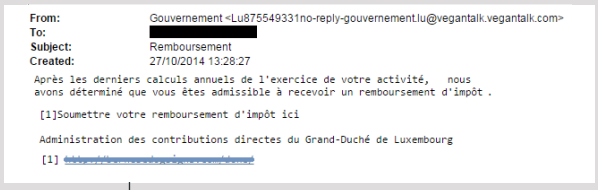
Examples of phishing

1. Phishing with malware and encryption software

After opening an email attachment containing malware hidden as an invoice or contract in *.zip/ *.flv/... format, all files on the hard disk are encrypted and a message is displayed. This message requires the user to pay a ransom of 0.2 to 5 Bitcoins within 72 to 96 hours, otherwise his disk will be definitively encrypted.

In this scenario, victims are urged to contact an expert or to download a software that can remove the virus.

2. Email with text and link to a phishing website with the appearance of the 'Administration des Contributions Directes'



The phishing website promises a credit card refund and collects the following information about the user:

- Credit card type
- Name on credit card
- Credit card number
- Expiry date
- Date of Birth
- Security Code (CVC)
- 3D secure password

How to recognize a spam?

Verify the origin / source of the email

If you don't know it or if it is a strange address, be careful!

Tips

- Do not open any attachment sent to you by a sender you do not know and be all the more vigilant if these attachments are, among others, in *.docx, *.pdf, *.zip, *.scr, *.png format.
- Configure your email client so that it does not open any attachment in the client itself. This will prevent malicious attachments from being automatically shown and thus the infection of your computer.

Read the content of the email carefully

If you find too many grammatical, spelling and stylistic errors, be suspicious!

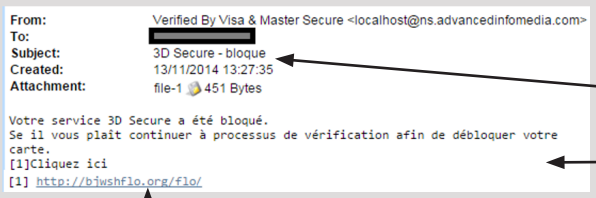
Check the recipient of the email

Is the email addressed to a list of people or is it personal? Depending on the content of the email, this information can alert you.

Compare the sender's name with the link(s) embedded in the email

Spam very often includes a link that has nothing to do with the email address of the sender or the institution for which he assumes the identity (bank, municipality, etc.) This is known as e-mail spoofing. Move your mouse over the link in the email to see what it really points to. Be careful, do not click on it!

Case study (real phishing)



Suspect source, unrelated to product

Grammatical error

Grammatical, spelling and stylistic errors

No relationship between the link and the subject ('Subject') or the email address ('From')

© Copyright Restena Foundation - November 2020 | www.restena.lu

restena
réseau · sécurité · .lu

Protecting privacy

Some recommendations to avoid a maximum of spam

- **Use a different username than your email address**.
- **Do not insert your primary email address on suspect websites**, such as websites that promise you winnings or vouchers/coupons with huge values.
- **Present your email address in a hidden form**, if you display it on a website: publish the email address in one of the following form: [name]@[education].lu or (name)[at](education)[dot]lu; or show it as an image. With this masking, primitive robots cannot recognize your address.
- **Check terms and conditions of online services you subscribe to**: when subscribing to online services, check boxes are often pre-selected in the terms and conditions so to allow further advertising to be sent.
- **Never reply to unsolicited messages.**

Filter your email with anti-spam solutions

To fight against spam, anti-spam solutions make it possible to filter unwanted email before it arrives in the mailbox. These specialized solutions can be either outsourced or directly installed on users' workstations or on mail servers.

To effectively identify spam, anti-spam solutions rely on a combination of anti-spam techniques:

- lexical analysis,
- blacklists,
- collaborative databases, etc.

Information

- Major email software programs include anti-spam solutions as a standard.
- If the filtering is too strict, there is a risk of false positives, while less strict filtering increases the amount of undetected spam. It is therefore important to find the right balance between the two.

Unfortunately, no anti-spam solution is perfect and spammers evolve and always find new ways to bypass anti-spam measures, making spam detection increasingly difficult.

The ideal anti-spam is a solution that detects 100% spam and leaves 100% of the good messages or in technical terms: 100% spam detected, 0% false negatives* and 0% false positives**. It is very difficult to reach 100% without generating a lot of false positives. This is a rather critical aspect, since these false positives can correspond to important legitimate messages.

→ Neither official organization (administrations, banks, municipalities, etc.) nor the Restena Foundation request sensitive information (credit card, password...) by email or phone!

Service Offer

The Restena Foundation offers anti-spam/anti-virus protection via its 'Anti-virus/anti-spam gateway' service to actors of research, education, culture, health and administration in Luxembourg, whether their emails are hosted or not on RESTENA servers.

For more information on this service, please visit restena.lu/en/service/gateway

** False Negative: undetected junk mail*

*** False-positive: legitimate email incorrectly classified as spam*

© Copyright Restena Foundation - November 2020 | www.restena.lu

restena
réseau · sécurité · .lu