Newsletter N°5/2015

RESTENA
Réseau Téléinformatique de l'Education Nationale et de la Recherche

"Spam, spam, spam, lovely spam, wonderful spam, lovely spam, wonderful spam..." - the "spam" song from the "Monty Python's Flying Circus" play

SPAM & PHISHING MESSAGES

Users are more and more active in the Internet nowadays by means of social media, email, video chat,... A phenomenon in direct relation to these activities is unwanted messages of all kind.

Do you know that the first spam ever was accidentally sent in.1978? Gary Thuerk - a salesman, transmitted an advertisement to more than 400 of 2600 ARPAnet* users. After major complaints from the users next to his company, this unsolicited message was called "spam".

Source: www.spam.com

This edition of the newsletter presents the most common categories of spam and gives advice about the protection of sensitive data.

*ARPANET: a first version of the Internet founded by DARPA

Different ways, one common purpose: your private data!

- **Spam message**

It is an unwanted advertisements of doubtful origin, but without major risks. Often the content is related to the pharmaceutical domain (Viagra, ...).

- **Nigerian spam**

This spam is called "spam 419" and often has an African origin. In Nigeria, "article 419" of the penal code treats fraud. The content of such a message often promises a large gain or other amount of money blocked on a bank account of an governmental employee.

- **Phishing spam**

Phishing is fraud, where users are deceived about the origin of the message, such as the recent phishing wave about the tax administration of Luxembourg (administration des contributions directes).

This message clearly aims to collect sensitive information about users, such as credit card numbers, passwords, home address, email address, in order to reuse these for criminal purpose.

Fondation RESTENA

6, rue Richard
Coudenhove-Kalergi

L-1359 Luxembourg

Tél: +352 42 44 09-1

Fax: +352 42 24 73

Phishing (cont'd)

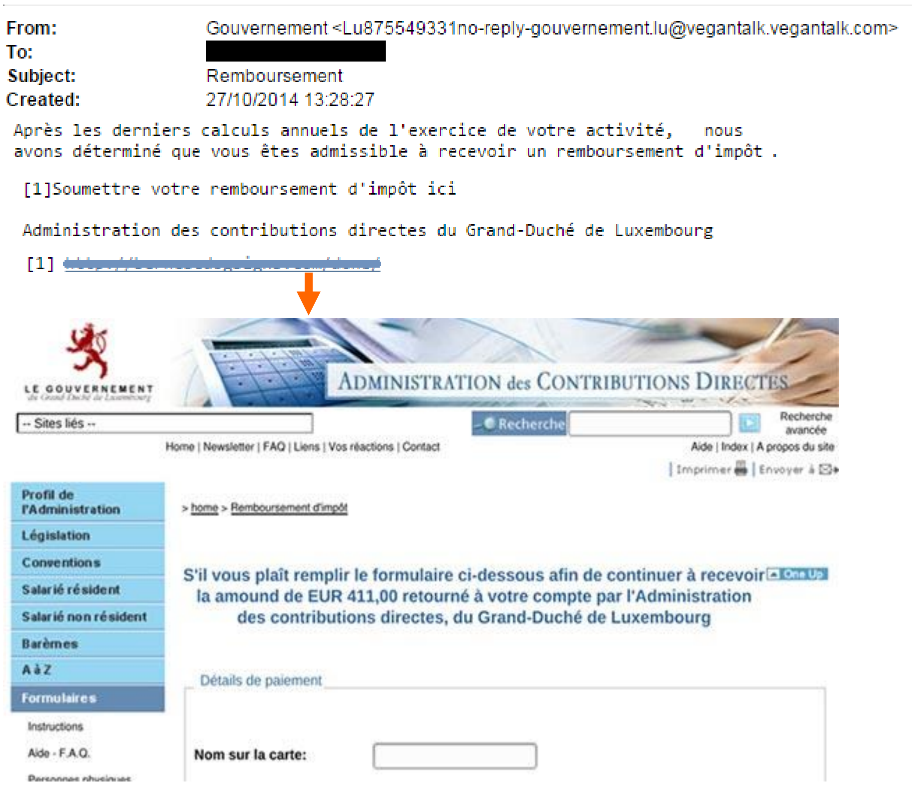
The most simple phishing message only includes a text with a form to be submitted, that asks private user information, such as the user name, email address, password...

Another phishing class includes text with a link to website, asking to fill the online form and to submit it. A similar category of phishing includes a link to a website, that is often compromised, and that redirects to another website with malware or that immediately asks to download and install malware. By this piece of software, the attacker can collect all information about a user, as for example all keystrokes, passwords, banking information, ...

The most severe phishing class is «ransomware». The phishing message has an attachment with an extension class like *.zip, *.scr or *.flv. It contains malware that blocks access to the computer, encrypts all files and asks the user to pay a certain amount of money, also called a ransom, either by prepaid card (ex. safepaycard) or by a money transfer agency (ex. Western Union). In the worst case, the hard drive or file server will stay encrypted even if the ransom is paid. In this case, it is recommended to contact an expert.

Phishing example

This spam includes a text and a link to a phishing site that has a copied design of the "administration des contributions directes" website.



From: Gouvernement <Lu875549331no-reply-gouvernement.lu@vegantalk.vegantalk.com>
To: [redacted]
Subject: Remboursement
Created: 27/10/2014 13:28:27

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

 [1]Soumettre votre remboursement d'impôt ici

 Administration des contributions directes du Grand-Duché de Luxembourg

 [1] [redacted]
```

LE GOUVERNEMENT
du Grand-Duché de Luxembourg
ADMINISTRATION des CONTRIBUTIONS DIRECTES
-- Sites liés --
Recherche
Recherche avancée
Home | Newsletter | FAQ | Liens | Vos réactions | Contact
Aide | Index | A propos du site
Imprimer | Envoyer à
Profil de l'Administration
Législation
Conventions
Salarié résident
Salarié non résident
Barèmes
A à Z
Formulaires
Instructions
Aide - F.A.Q.
Personnes physiques
> home > Remboursement d'impôt
One Up

S'il vous plaît remplir le formulaire ci-dessous afin de continuer à recevoir la amound de EUR 411,00 retourné à votre compte par l'Administration des contributions directes, du Grand-Duché de Luxembourg

Détails de paiement

Nom sur la carte:

The phishing website claims to reimburse fees by using the credit card and by this collect senstivie information about a user, such as:

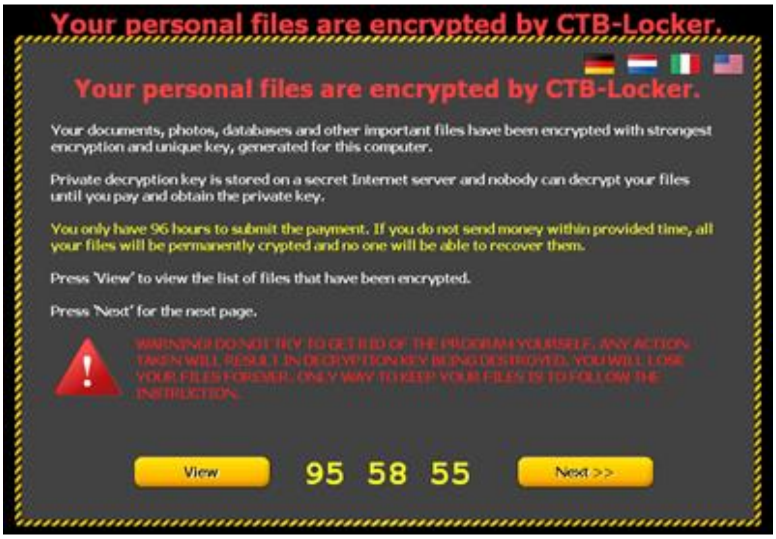
- Type of credit card
- Name on credit card
- Number of credit card
- Expiration date

- Date of birth
- Security code (CVC)
- Password including 3D secure code

- **Ransomware example with malware and encryption (active phishing wave)**

This spam has an attachment with consequently a malicious software masked as a bill or contract with extension *.zip/*.flv/…

Once the attachment was opened, all files on the hard drive are encrypted and a message pops up, asking to pay a ransom to 0.2 up to 5 Bitcoin in a time period of 72 to 96 hours. Otherwise, the hard drive will remain encrypted and all the files lost (see screenshot). In this case, it is recommended to contact an expert or to download a specific malware remover.



Your personal files are encrypted by CTB-Locker.

Your personal files are encrypted by CTB-Locker.

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer.

Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.

You only have 96 hours to submit the payment. If you do not send money within provided time, all your files will be permanently crypted and no one will be able to recover them.

Press 'View' to view the list of files that have been encrypted.

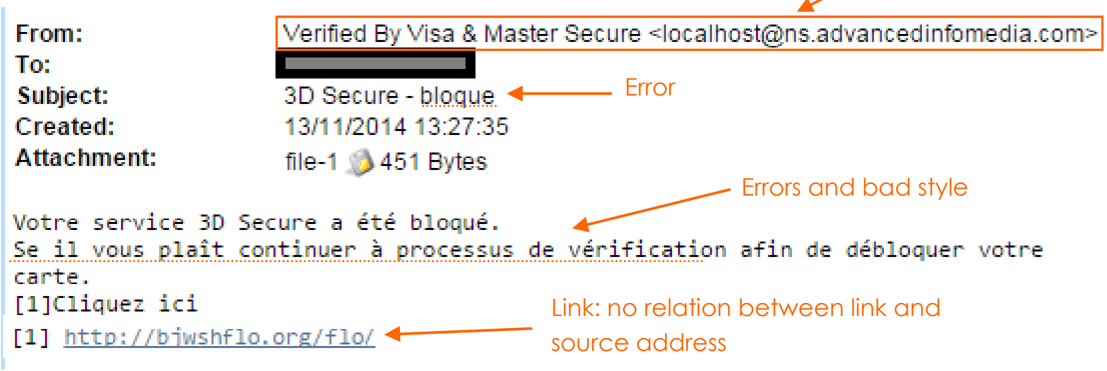
Press 'Next' for the next page.

WARNING! DO NOT TRY TO GET RID OF THE PROGRAM YOURSELF. ANY ACTION TAKEN WILL RESULT IN DECRYPTION KEY BEING DESTROYED. YOU WILL LOSE YOUR FILES FOREVER. ONLY WAY TO KEEP YOUR FILES IS TO FOLLOW THE INSTRUCTION.

Some hints to recognise a spam

- Verify the **origin**/source of the email — if you do not know the sender or if it is a strange address, take care!
- The **receiver** — check if the email is sent to a list or to your private address!
- **Content** — read the content carefully! Pay attention to **spelling**, **grammar** or **style errors** (often machine translation)
- **Link** to a web page — often the link text has no relation to the sender or the organism (bank, administration,...). Compare the sender name to the link and the subject line! Slide the cursor over the link to see the complete link resolution, BUT without clicking!
- Do not open attachments having an unknown sender address! Pay attention to attachments with extensions such as *.docx, *.pdf, *.zip, *.scr, *.png.

Example: a real phishing message



From:	Verified By Visa & Master Secure <localhost@ns.advancedinfomedia.com>
To:	[redacted]
Subject:	3D Secure - bloque
Created:	13/11/2014 13:27:35
Attachment:	file-1 451 Bytes

```
Votre service 3D Secure a été bloqué.
Se il vous plaît continuer à processus de vérification afin de débloquer votre
carte.
[1]Cliquez ici
[1] http://bjwshflo.org/flo/
```

Strange source address, no link between source and product

Error

Errors and bad style

Link: no relation between link and source address

All official institutions, such as administrations, banks, communes, etc., the same as the RESTENA Foundation, will never ask users for sensitive data (credit card, password,...) by email or telephone!

How to avoid too much spam!

- Use a user name that is different to your email address!

- Do not submit your primary email address on strange websites, such as websites promising large gains, vouchers or lotteries, etc.

- If you publish your email address on a web site, refer to masking techniques, as for example:

  [name]@[education].lu / (name) [at] (education) [dot] lu

  or represent it as an image:

name@education.lu

⇒ By using these masking techniques, the email address cannot be recognized by primitive robots.

- When you subscribe to an online service, always check the general conditions. Often checkboxes are enabled which permit to send you other advertisements.

- If you get an unwanted message, do not reply!

Anti-Spam solutions

To fight spam, a lot of «anti-spam» solutions exist to filter unwanted message before they even arrive in a mailbox. These specialised solutions can be installed directly on the user equipment, on the mail servers or externally. The best known mail clients also integrate anti-spam solutions.

Most anti-spam solutions use a combination of different anti-spam techniques (such as lexical analysis, blacklists, collaborative-based,…) to more efficiently identify spam. Unfortunately no solution is perfect!

In the meantime, spammers also evolve and always show up with newer methods to circumvent anti-spam solutions in place and by consequence, make spam detection even more complex.

An ideal anti-spam solution detects 100% of spam and additionally achieves to detect 100% of legitimate messages. Technically this means, it detects 100% of spam, has 0% of false negatives[*] and 0% of false positives[+].

In practice it is difficult to achieve these 100% without generating too much false positives. This is a very critical aspect, since false positives can be legitimate mail messages.

Strict filtering induces a risk for false positives, weak filtering increases the amount of unwanted messages. Therefore it is important to elaborated a balanced filtering ratio.

[*] **False negative**: an undetected spam message

[+] **False positive**: a legitimate message detected as spam

Anti-spam/anti-virus protection— at the RESTENA Foundation

The anti-spam/anti-virus protection uses a filtering system that actively protects user mailboxes against spam. This system allows the detection and tagging of spam messages.

Emails detected as spam normally include information in the header field that indicates that it is a ******SPAM****** .

By default, all tagged messages are delivered in the user mailbox and can be processed locally by additional tools in the email client.

If a user opts for an immediate deletion of tagged messages, the mailbox blocks spam and infected messages before downloading them in the user mailbox. By this, the user does not see any spam in his mailbox anymore and no additional filtering is necessary.

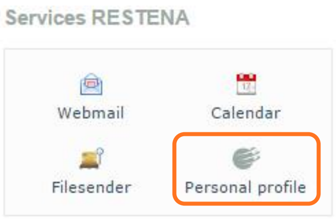
All products may have faulty results, therefore it is possible that some messages may be wrongly tagged as ******SPAM******. These are called false positives. The immediate deletion of these risks the loss of important messages. **This is why the email protection configuration is considered as the responsibility of each user.**

Another challenge is to find the right balance between false negatives and false positives! A good approach is to filter less, admitting a few false negatives instead of a severe filtering , where legitimate emails, false positives, may be deleted. Our engineers try to keep the false positive level as low as possible by regularly adjusting the spam detection.

• How to change the email protection configuration

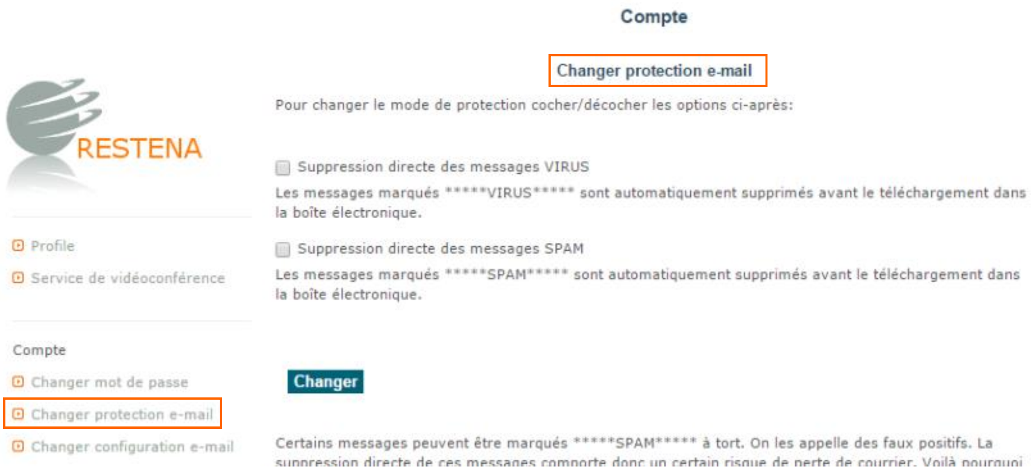
You can de/activate your spam filter settings by using the User profile tool on our website:

RESTENA Services→ User Profile



In your profile, select: **change e-mail protection**

Here you can choose between different suppression modes for tagged emails, such as
******SPAM*******
and
******VIRUS*******.


Compte
RESTENA
Profile
Service de vidéoconférence
Compte
Changer mot de passe
Changer protection e-mail
Changer configuration e-mail
Changer protection e-mail
Changer

Pour changer le mode de protection cocher/décocher les options ci-après:

☐ Suppression directe des messages VIRUS

Les messages marqués *****VIRUS***** sont automatiquement supprimés avant le téléchargement dans la boîte électronique.

☐ Suppression directe des messages SPAM

Les messages marqués *****SPAM***** sont automatiquement supprimés avant le téléchargement dans la boîte électronique.

Certains messages peuvent être marqués *****SPAM***** à tort. On les appelle des faux positifs. La suppression directe de ces messages comporte donc un certain risque de perte de courrier. Voilà pourquoi

Other articles about phishing, spam and online fraud

Bee-Secure:

https://www.bee-secure.lu/fr/clever-klicken

Cases:

https://www.cases.lu/les-phish-a-laffiche-ne-mordez-pas-a-lhamecon.html

“Guichet public”:

http://www.guichet.public.lu/entreprises/fr/gestion-juridique-comptabilite/contentieux/litiges/arnaques/index.html

Contact us

If you encounter any problems or have further questions, feel free to contact us:

helpdesk@restena.lu or by phone +352 42 44 09 - 1

NEWS

Discover the new edition of the **CONNECT** magazine from the research and education community in Europe. Follow this link:

http://www.geant.net/MediaCentreEvents/news/Pages/CONNECT_issue_18_is_now_available.aspx

GÉANT PROJECT
CONNECT
THE MAGAZINE FROM THE GÉANT COMMUNITY | ISSUE 18 2015
SPECIAL EDITION
INNOVATION WITH IMPACT
AN IN-DEPTH LOOK AT GÉANT'S FIRST OPEN CALL
idea

TNC15
THE LARGEST NETWORKING CONFERENCE FOR RESEARCH AND EDUCATION
15 - 18 June 2015, Porto, Portugal
Theme: Connected Communities

The 2015 edition of the prestigious «**Terena Networking Conference**» for actors of the research and education domain takes place in Porto, Portugal, from the 15th to 18th June 2015. For more details, visit its official website:

https://tnc15.terena.org/

eduroam, the secure wireless network dedicated to the research and education community registers a new record of more than 17 million connections in Luxembourg in 2014 . To read the press release: http://www.restena.lu/restena/Pdfs/CP_eduroam_en.pdf