# Dealing with Flubot, an operator’s experience

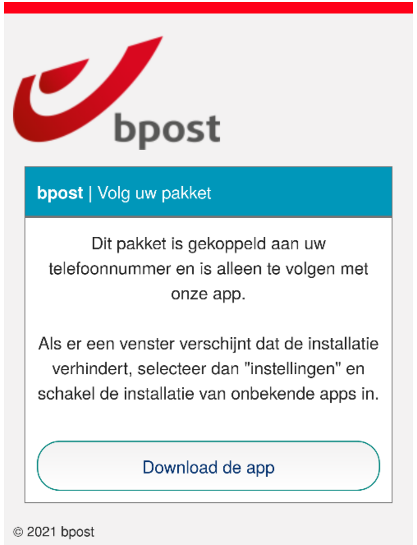
Steven Beerens – Investigations Specialist

proximus

# Flubot SMS

- Belgian regulator BIPT and National Center for Cyber Security (CCB) escalated on 09/05/2021
- International attack on android devices asking user to install a parcel tracking app DHL,  UPS, BPOST,…
- First wave 08/05/2021 till 24/07/2021 (including voicemail smishing)
- Wave 2: 06/09/2021 : Flubot started again
- Still ongoing : variabel content messages

# Flubot smishing



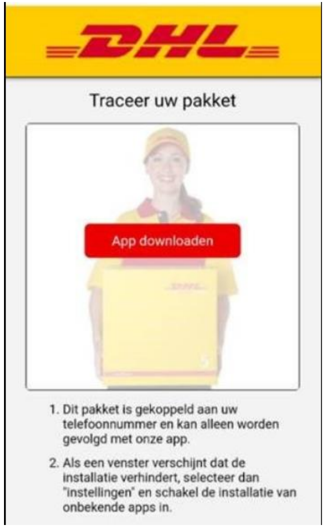
bpost

bpost | Volg uw pakket

Dit pakket is gekoppeld aan uw telefoonnummer en is alleen te volgen met onze app.

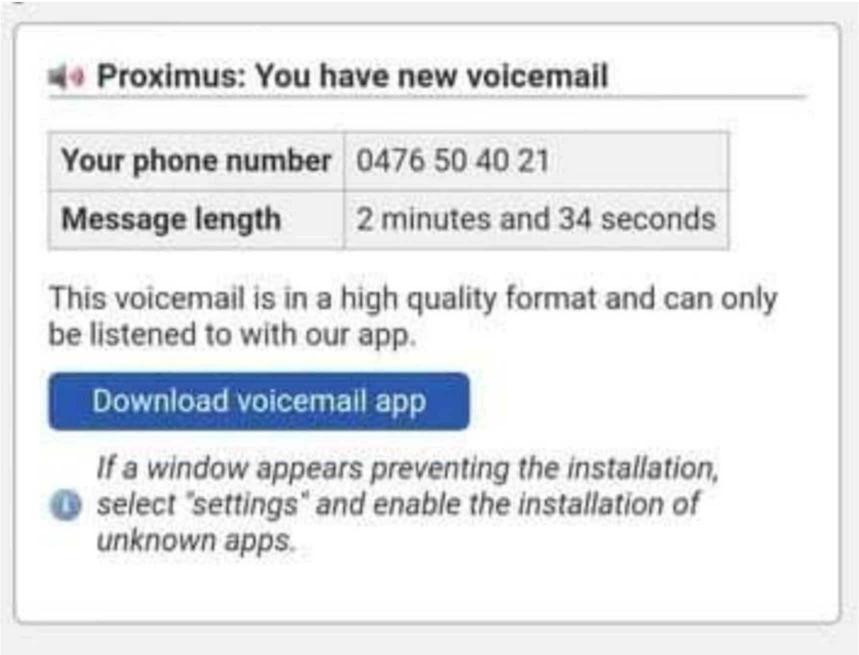
Als er een venster verschijnt dat de installatie verhindert, selecteer dan "instellingen" en schakel de installatie van onbekende apps in.

© 2021 bpost



Traceer uw pakket

1. Dit pakket is gekoppeld aan uw telefoonnummer en kan alleen worden gevolgd met onze app.
2. Als een venster verschijnt dat de installatie verhindert, selecteer dan "instellingen" en schakel de installatie van onbekende apps in.



Proximus: You have new voicemail

| | |
|---|---|
| Your phone number | 0476 50 40 21 |
| Message length | 2 minutes and 34 seconds |

This voicemail is in a high quality format and can only be listened to with our app.

*If a window appears preventing the installation, select "settings" and enable the installation of unknown apps.*

# Actions

- Wave 1
  - Align with BIPT, CCB and other olo's
  - Filtering Flubot( texts on SMSC )
  - Implement barring of outgoing SMS for infected customers during a week
  - Blocking on BICS level of international SMSes
  - Park bills of infected customers
  - Inform customers on barring, unbarring

- Wave 2
  - Blocking on SMSC firewall
  - IP and domain barring in agreement with CCB (to block traffic to command and control centers)

- BIPT is aware & approved mitigation actions taken by the different operators

# SMS content info customers

Barring SMS:

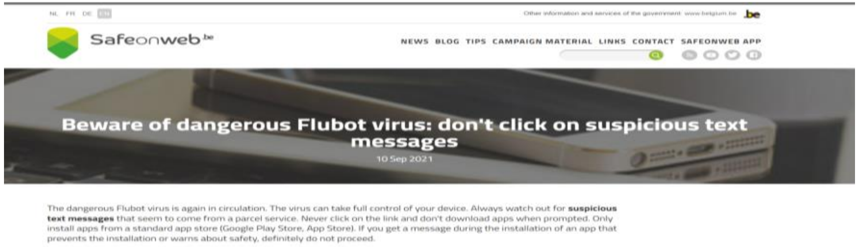
*Proximus-info: Dear customer, we have noticed an abnormal sending of SMS from your cell phone number. To protect you, the sending of SMS is temporarily suspended for a period of one week. To solve this situation, follow the instructions on safeonweb.be and read the article on fake SMS.*

Unbarring SMS:

*Dear customer, as previously announced, we enabled SMS-sending again for your mobile number.*
*As advised on safeonweb.be, you should have done a factory reset in the past week.*
*If you have not executed this step, your device remains infected. If abnormal usage is detected again, Proximus will block again SMS-sending.*

# Communication

- Proximus recommends  its customer to follow the rules defined by CCB (safeonweb.be)
  - Social Media
    - Proximus shares messages from CCB via Facebook and Twitter
    - Proximus informs customers via Facebook and Twitter
  - Support Pages of Proximus  - information published
  - WAP+ : banner on Proximus intranet page to inform collaborators


NL FR DE EN
Other information and services of the government: www.belgium.be
.be
Safeonweb.be
NEWS BLOG TIPS CAMPAIGN MATERIAL LINKS CONTACT SAFEONWEB APP

**Beware of dangerous Flubot virus: don't click on suspicious text messages**

10 Sep 2021

The dangerous Flubot virus is again in circulation. The virus can take full control of your device. Always watch out for **suspicious text messages** that seem to come from a parcel service. Never click on the link and don't download apps when prompted. Only install apps from a standard app store (Google Play Store, App Store). If you get a message during the installation of an app that prevents the installation or warns about safety, definitely do not proceed.

# What to do if you receive a suspicious message?

You can send a suspicious e-mail to **Safeonweb** via suspicious@safeonweb.be. Thanks to your report, the Centre for Cybersecurity Belgium (CCB) will block the suspicious links in collaboration with Proximus. This way you help others not to fall into the trap.

Furthermore, the CCB collects information on common suspicious messages and shares it through their new **Safeonweb app**. So you stay informed when suspicious messages are circulating.

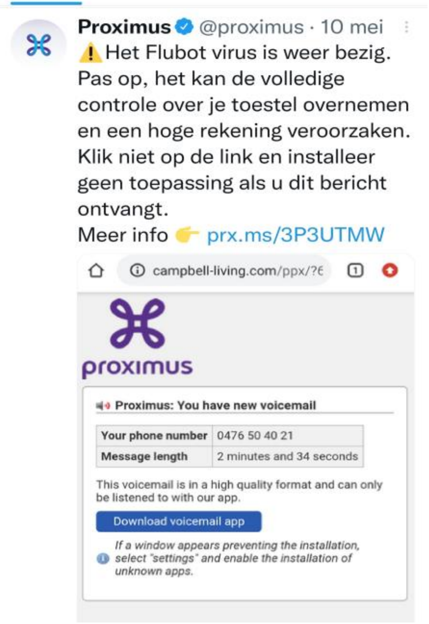
The app also warns you about cyber threats and new forms of online scams. You can download the Safeonweb app from your official app store (App Store and Google Play Store).

Did you know that you can send suspicious text messages on your smartphone for free to Proximus CSIRT (Cyber Security Incident Response Team) via the short number 8444? They will analyze the SMS and block the link.

Together we can outsmart cybercriminals!

Download the Safeonweb app for iOS ↗

Download the Safeonweb app for Android ↗



**Proximus** @proximus · 10 mei

⚠️Het Flubot virus is weer bezig. Pas op, het kan de volledige controle over je toestel overnemen en een hoge rekening veroorzaken. Klik niet op de link en installeer geen toepassing als u dit bericht ontvangt.

Meer info 👉 prx.ms/3P3UTMW

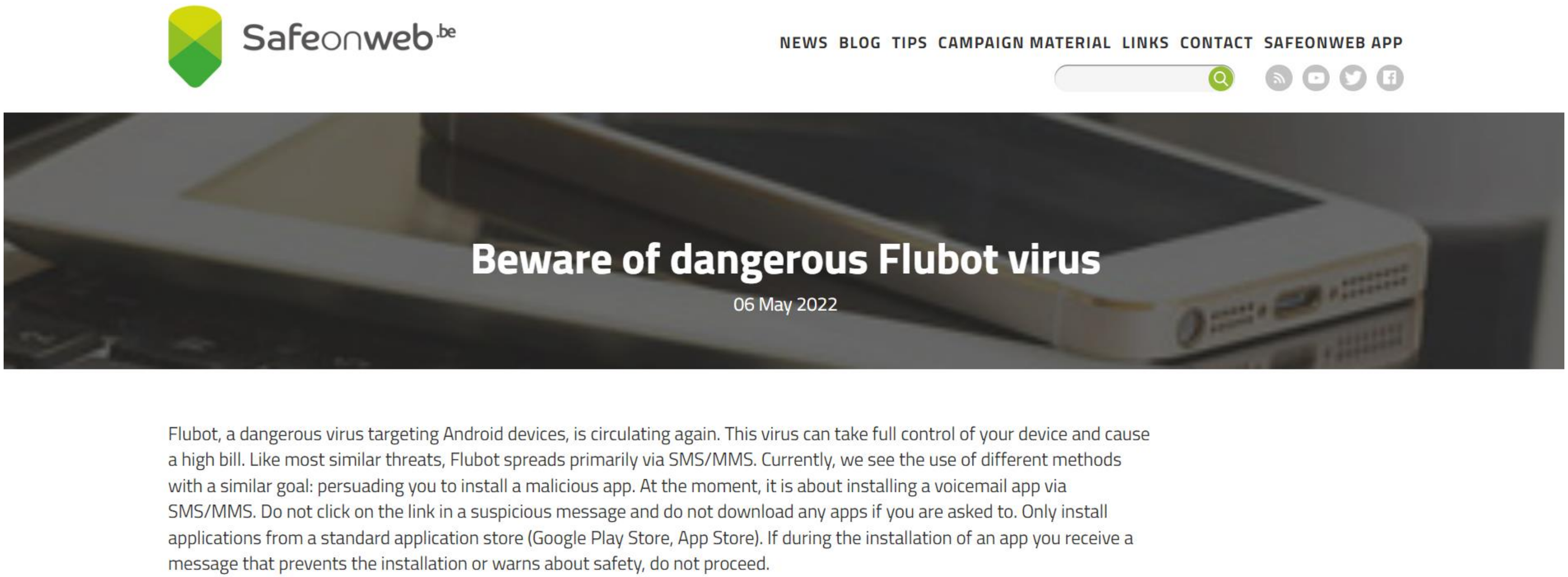
**Proximus: You have new voicemail**

| | |
|---|---|
| Your phone number | 0476 50 40 21 |
| Message length | 2 minutes and 34 seconds |

This voicemail is in a high quality format and can only be listened to with our app.

*If a window appears preventing the installation, select "settings" and enable the installation of unknown apps.*

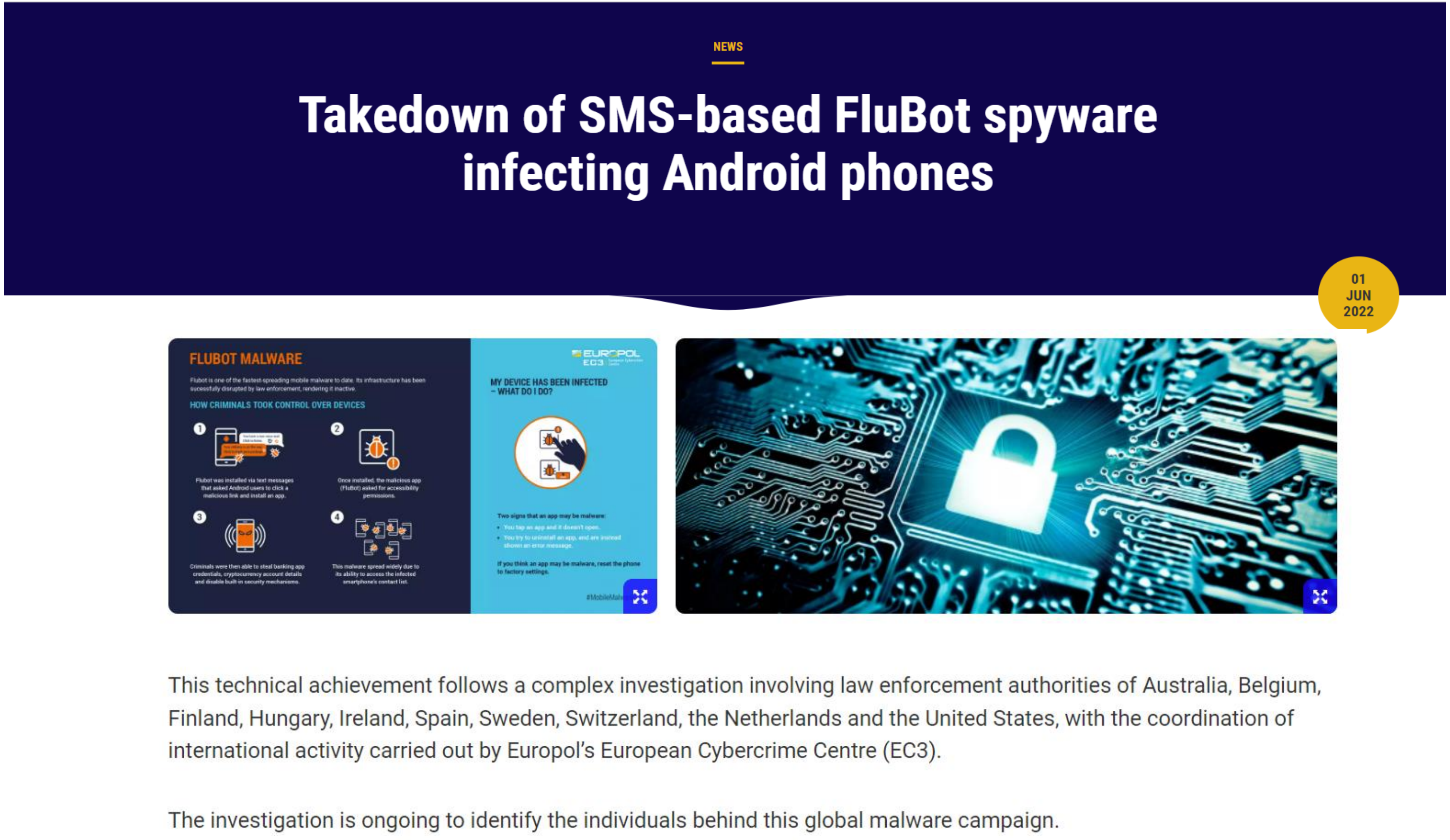
# Flubot MMS – May 2022



## Beware of dangerous Flubot virus

06 May 2022

Flubot, a dangerous virus targeting Android devices, is circulating again. This virus can take full control of your device and cause a high bill. Like most similar threats, Flubot spreads primarily via SMS/MMS. Currently, we see the use of different methods with a similar goal: persuading you to install a malicious app. At the moment, it is about installing a voicemail app via SMS/MMS. Do not click on the link in a suspicious message and do not download any apps if you are asked to. Only install applications from a standard application store (Google Play Store, App Store). If during the installation of an app you receive a message that prevents the installation or warns about safety, do not proceed.



NEWS

# Takedown of SMS-based FluBot spyware infecting Android phones

01 JUN 2022

FLUBOT MALWARE

Flubot is one of the fastest-spreading mobile malware to date. Its infrastructure has been sucessfully disrupted by law enforcement, rendering it inactive.

HOW CRIMINALS TOOK CONTROL OVER DEVICES

1 Flubot was installed via text messages that asked Android users to click a malicious link and install an app.

2 Once installed, the malicious app (FluBot) asked for accessibility permissions.

3 Criminals were then able to steal banking app credentials, cryptocurrency account details and disable built-in security mechanisms.

4 This malware spread widely due to its ability to access the infected smartphone's contact list.

MY DEVICE HAS BEEN INFECTED – WHAT DO I DO?

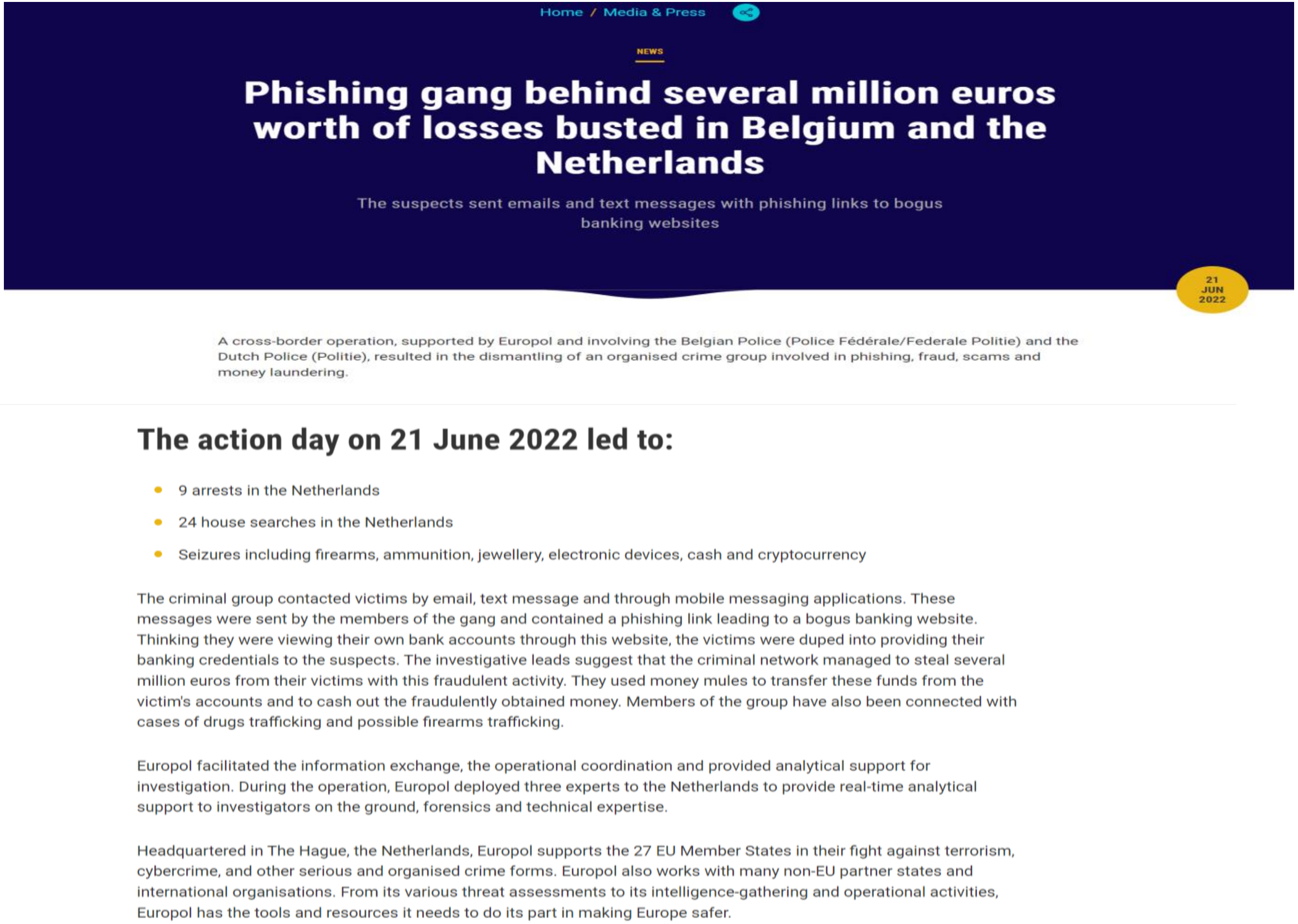
Two signs that an app may be malware:

- You tap an app and it doesn't open.
- You try to uninstall an app, and are instead shown an error message.

If you think an app may be malware, reset the phone to factory settings.

This technical achievement follows a complex investigation involving law enforcement authorities of Australia, Belgium, Finland, Hungary, Ireland, Spain, Sweden, Switzerland, the Netherlands and the United States, with the coordination of international activity carried out by Europol's European Cybercrime Centre (EC3).

The investigation is ongoing to identify the individuals behind this global malware campaign.



# Phishing gang behind several million euros worth of losses busted in Belgium and the Netherlands

The suspects sent emails and text messages with phishing links to bogus banking websites

21 JUN 2022

A cross-border operation, supported by Europol and involving the Belgian Police (Police Fédérale/Federale Politie) and the Dutch Police (Politie), resulted in the dismantling of an organised crime group involved in phishing, fraud, scams and money laundering.

## The action day on 21 June 2022 led to:

- 9 arrests in the Netherlands
- 24 house searches in the Netherlands
- Seizures including firearms, ammunition, jewellery, electronic devices, cash and cryptocurrency

The criminal group contacted victims by email, text message and through mobile messaging applications. These messages were sent by the members of the gang and contained a phishing link leading to a bogus banking website. Thinking they were viewing their own bank accounts through this website, the victims were duped into providing their banking credentials to the suspects. The investigative leads suggest that the criminal network managed to steal several million euros from their victims with this fraudulent activity. They used money mules to transfer these funds from the victim's accounts and to cash out the fraudulently obtained money. Members of the group have also been connected with cases of drugs trafficking and possible firearms trafficking.

Europol facilitated the information exchange, the operational coordination and provided analytical support for investigation. During the operation, Europol deployed three experts to the Netherlands to provide real-time analytical support to investigators on the ground, forensics and technical expertise.

Headquartered in The Hague, the Netherlands, Europol supports the 27 EU Member States in their fight against terrorism, cybercrime, and other serious and organised crime forms. Europol also works with many non-EU partner states and international organisations. From its various threat assessments to its intelligence-gathering and operational activities, Europol has the tools and resources it needs to do its part in making Europe safer.

# Belgian Legislation: Art. 125 §1, 7° Electronic Communication law:

- Allows the processing of **traffic data** and/or, **if necessary, message content for customers protection** against **fraud related to SMS/MMS/RCS.**

- No legal obligation for us to offer that protection.

- If content is processed, only by “mechanical means”.

- Processing only by Proximus’ employees fighting that type of fraud
  = No communication to third parties

- No prior customer’s consent needed but obligation to inform customer about the data we are collecting/processing, for which purposes, for how long, etc.

# Government’s Stop Phishing project - spamshield

Purpose:

- Improve national resilience to phishing in order to protect citizens, businesses and public actors.
- adapt the regulatory framework in line with European and national rules
- detect and block phishing attempts through the implementation of anti-phishing platforms at telecom operators operating in Belgium

- Proximus participation via implementing spamshield

# Thank you