Background
Safeonweb campaign, October 2022
OK is not always OK!

The Centre for Cybersecurity Belgium and the Cybersecurity Coalition are joining forces again this year with more than 500 partners. The aim? To combat scammers with the slogan: OK is not always OK! During the campaign we will shout this from the rooftops via radio ads, videos on social media, banners and other campaign materials.

Everyone, from the very young to very old, has a smartphone in their pocket these days. We use one for more and more things: to stay in touch with friends, to make purchases, to watch movies, to play games or to do homework.

Criminals and scammers see this as a great opportunity. They develop viruses that are specially developed to hit mobile devices and go on full attack.

The cyberattack that worried us the most in 2021 and that affected ordinary internet users was undoubtedly the spread of the FluBot virus. More than 11,000 smartphones were infected with this virus in no time because users carelessly downloaded an application. This allowed the virus to spread unnoticed to all of the victims' contacts .

It's not that hard to keep your smartphone secure. The main way devices get infected is by downloading untrustworthy apps, so be careful if you receive an email or text message asking you to do so. The chances are that you will install a dangerous app or even a virus from an unsafe app store.

The slogan of this year's campaign is therefore: **OK is not always OK!** After all, clicking OK to download an app can have very unpleasant consequences.

Summary

- More people are using a smartphone – almost the entire population over the age of 16
- Increasingly intensive use of smartphones: for more different applications, for longer periods and from an increasingly young age
- Criminals and scammers see this as a great opportunity
- The number of viruses specially developed to infect smartphones is increasing
- The user is not aware of the problem
- Prevention is possible and easy: **download apps from official app stores**
- You can also keep your smartphone safe by following these tips:
  - Always be very careful if you receive an email or text message asking you to download an app. The chances are that you will install a dangerous app or even a virus via a less secure app store.
  - Got a warning that you are trying to install an untrustworthy app? Then stop the installation straight away.
  - When you install an app, you are often asked for access to other data, e.g. your photos, contacts or location. Only give permission if this is necessary and useful for the use of the app.
  - Being asked to make updates? Do so as soon as possible.

1. Increasing use of mobile devices (smartphones and tablets)

93% of Flemish people (16+) have a smartphone in their pocket and 59% also have a tablet available (IMEC, Digimeter 2021, p. 24 onwards).

96% of Walloon families have at least one mobile device at their disposal. This is 4% more than in 2019. (BAROMÈTRE 2021 de maturité numérique des citoyens wallons, pp.4-6)

Not only does almost everyone have a smartphone at their disposal, but the devices are also very frequently used for various applications.

Users can no longer do without a smartphone, but are worried about the safety of certain actions they perform with it. *(IMEC, Digimeter 2021, p.114, 124)*

Children get their first smartphone at an increasingly young age. According to a research report by Apestaartjaren (2022), this is now at the age of 8. From the age of 13, every young person seems to be the proud owner of a smartphone. (https://www.apestaartjaren.be/, 2022, p.9)

2. Increase in mobile malware

As we increasingly rely on mobile devices, cybercriminals see them as an excellent opportunity to get their hands on our information and money, or to simply do harm. With this in mind, they are developing a number of threats specifically designed to work on mobile platforms, namely **mobile malware.**

https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/mobile-malware

Mobile malware (or viruses for mobile devices) is malicious software designed specifically for mobile devices, such as smartphones and tablets, for the purpose of accessing private data. (ENISA Threat Landscape 2021, p. 47)

3. Recent case: the FluBot virus

The cyberattack that worried the CCB in 2021 and that affected ordinary internet users was undoubtedly the spread of the FluBot virus. 11,000 smartphones were infected with this virus in no time because users carelessly downloaded an application. This allowed the virus to spread unnoticed to all the victims' contacts. An infected device sometimes sent out more than 10,000 messages. Between 6 and 13 September 2021, an average of 2 million messages per day were detected and blocked by the operators (BIPT figures, 2021).

FluBot's infrastructure was dismantled in 2022 by a large-scale police action. Flubot may have disappeared from the radar, but there are dozens of other viruses ready to launch an attack.

https://www.europol.europa.eu/media-press/newsroom/news/takedown-of-sms-based-flubot-spyware-infecting-android-phones