Criminals have quickly adapted their techniques to exploit our fears around the COVID-19 pandemic. Their main aim is profit by any means necessary.

Our desire for COVID-19 news is the perfect opportunity for criminals to dupe more victims looking for information and in-demand products and services.
How are criminals abusing the COVID-19 crisis?

Police from across the EU have reported an increase in:

Shopping scams
Criminals post fake adverts for products we want and need, like medicines, hygiene products and test kits.

Organised property crime
We expect more criminals will become involved in organised property crime during the pandemic. Criminals try to cash in on COVID-19 by targeting society's most vulnerable groups, such as senior citizens.

Teleworking vulnerabilities
If not done properly, teleworking can expose a company's vulnerabilities and lead to data leaks.
Phishing and smishing

Received a strange email or text about COVID-19?
Think twice before clicking on any links and attachments.

Fraud

Fraudsters adapt well-known fraud schemes to target citizens, businesses and public organisations.

Mobile malware

Criminal activities appropriating the COVID-19 outbreak have also gone mobile.

Ransomware

The types of criminals exploiting the COVID-19 pandemic online were also active in the area of cybercrime before. However, some have intensified their activities and are actively recruiting collaborators to maximise the impact of their attacks or schemes.

Child sexual exploitation

While children are allowed greater unsupervised internet access, offenders are likely to attempt to take advantage of those emotionally vulnerable and isolated through grooming and sexual coercion and extortion.

Spreading misinformation and disinformation

Spreading fake information about COVID-19, though not always a criminal offense, has very serious repercussions, endangering public health and directly affecting people’s lives.

Illegal streaming

Criminals are trying to take advantage of the current situation by expanding their activities in the area of intellectual property (IP) crime. This is particularly apparent in the form of IP infringements related to the illegal use of Internet Protocol Television (IPTV).

BE SMART, STAY SAFE!
Make your home a cyber safe stronghold

Lots of EU citizens have been asked to stay at home, taking their personal and work lives online. From smarthomes to smartphones, are you sure your devices are cyber safe?
A safety guide for the ‘new normal’ after COVID-19

Protect your children, house, finances and data now that confinement measures are starting to relax. Criminals are still looking for victims.
Shopping scams

Criminals post fake adverts for products we want and need, like medicines, hygiene products and test kits.

If an offer sounds too good to be true, then it probably is. Only buy from trusted sources and use safe payment options.
Faking and entering
Criminals try to cash in on COVID-19 by targeting society's most vulnerable groups, such as senior citizens. How can we keep them safe?

Teleworking vulnerabilities
Encouraging staff to work from home can have positive effects on businesses – it can provide flexibility and solve office space issues. But if not done properly, teleworking can expose a company's vulnerabilities and lead to data leaks.

Make your online office as safe as can be with our tips.
Phishing and smishing scams

Received a strange email or text about COVID-19? Think twice before clicking on any links and attachments. They could be phish or smish you, which is how criminals use social engineering to access your personal information.
Fraud

Fraudsters have been very quick to adapt well-known fraud schemes to target citizens, businesses and public organisations.

Know how they operate and stay one step ahead in the pandemic.
Mobile threats
Criminal activities appropriating the COVID-19 outbreak have also gone mobile, with some instances of malware targeting Android devices.
Ransomware
Ransomware prevents or limits users from accessing their system or devices. Criminals ask their victims to pay a ransom through certain online payment methods (and by a deadline) to regain control of their data.
The global impact of COVID-19 means people will be spending more time online. This includes both children and adults.

Spreading misinformation and disinformation
Get to know what to do to avoid becoming a part of the fake news distribution chain.
Illegal streaming

People locked down at home are looking for different types of digital entertainment to cope with social isolation. Several services illegally delivering streamed content have emerged during the COVID-19 pandemic. Know the risks!
Get the kids involved
Download the PDF file, print it on an A4 or A3 paper and let your children colour it!