

# STAYING SAFE DURING COVID-19: WHAT YOU NEED TO KNOW

Last update: 12 November 2020



## COVID-19 – QUICK LINKS

Been a victim of a COVID-19 scam? Report it to your national police.

Want to know more about COVID-19?

Always check official channels like the World Health Organization or your national health authority.



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.

## EUROPOL AND COVID-19

### Reports

Europol works around the clock to collect information from EU Member States and publishes regular reports on how criminals are adapting their crimes to exploit the COVID-19 pandemic. Read the reports below.

The illicit sales of false negative COVID-19 test certificates

*1 February 2021*

How COVID-19-related crime infected Europe during 2020

*11 November 2020*

EXPLOITING ISOLATION: Offenders and victims of online child sexual abuse during the COVID-19 pandemic

*19 June 2020*

EU Drug Markets: Impact of COVID-19

*29 May 2020*

Beyond the pandemic - How COVID-19 will shape the serious and organised crime landscape in the EU

*30 April 2020*

Viral marketing: Counterfeits in the time of pandemic

*17 April 2020*

Catching the virus cybercrime, disinformation and the COVID-19 pandemic

*3 April 2020*

How criminals profit from the COVID-19 pandemic report

## NEWS

COVID-19 chiefs of police working group meets to talk pandemic and fighting crime threats

15 February 2021

Europol warning on the illicit sale of false negative COVID-19 test certificates

1 February 2021

Crime against the elderly: four arrests in Germany and Poland

20 January 2021

Medicines and doping substances worth €73 million seized in Europe-wide operation

10 December 2020

Europol predictions correct for fake COVID-19 vaccines

4 December 2020

COVID-19 waste crime: Europe-wide operation to tackle unlawful sanitary waste disposal

30 November 2020

Exploiting isolation: sexual predators increasingly targeting children during COVID pandemic

19 June 2020

EU Drug Markets: Impact of COVID-19

29 May 2020

Beyond the pandemic - What will the criminal landscape look like after COVID-19?

30 April 2020

Viral marketing: counterfeits in the time of pandemic

17 April 2020

Corona crimes: multi-million face mask scam foiled by police across Europe

14 April 2020

Corona crimes: suspect behind €6 million face masks and hand sanitisers scam arrested thanks to international police cooperation

6 April 2020

Catching the virus

27 March 2020

How criminals profit from the COVID-19 pandemic

27 March 2020

Rise of fake 'corona cures' revealed in global counterfeit medicine operation

21 March 2020

COVID-19 joint statement

20 March 2020

COVID - 19 update

17 March 2020

### 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?

FIND OUT  
MORE

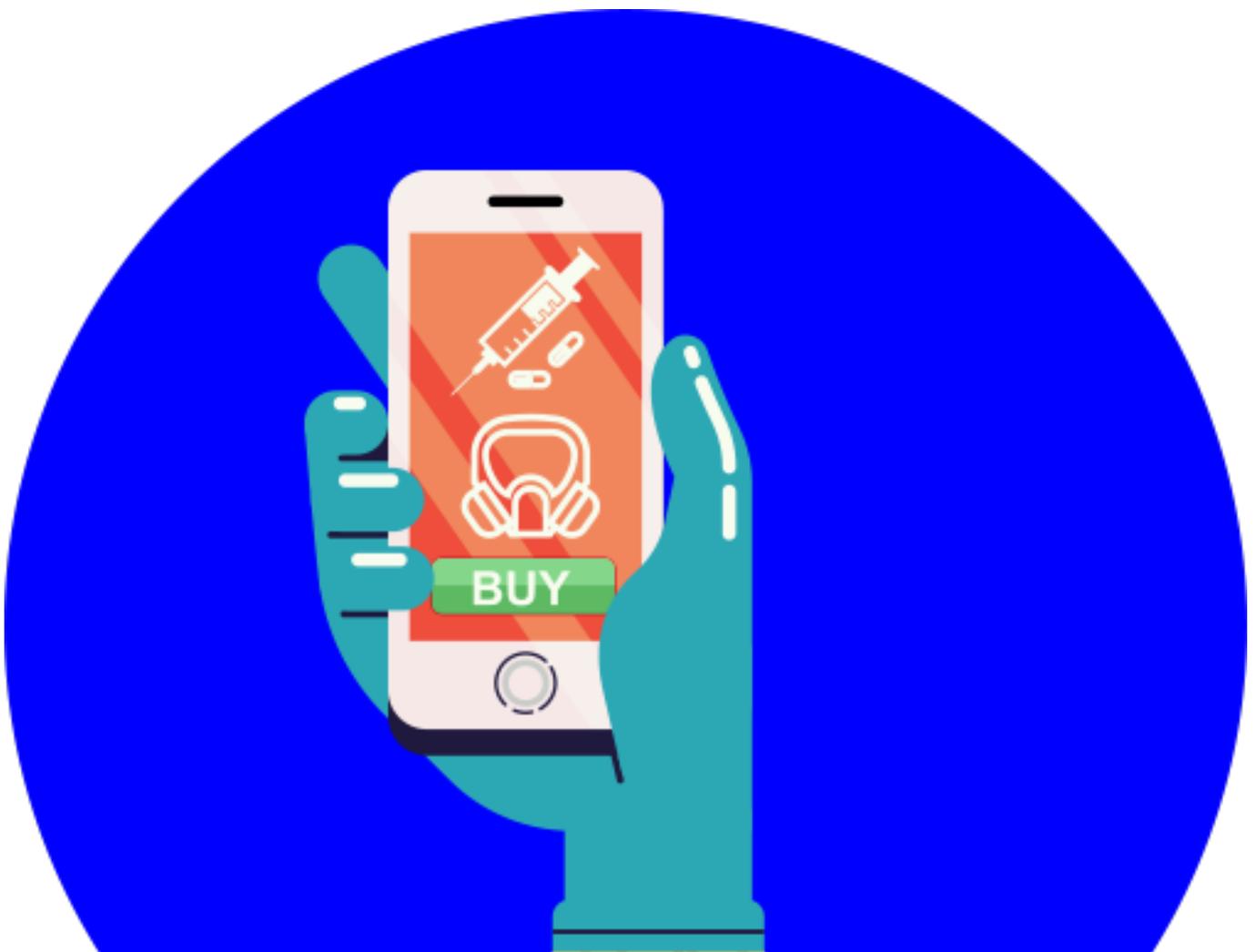


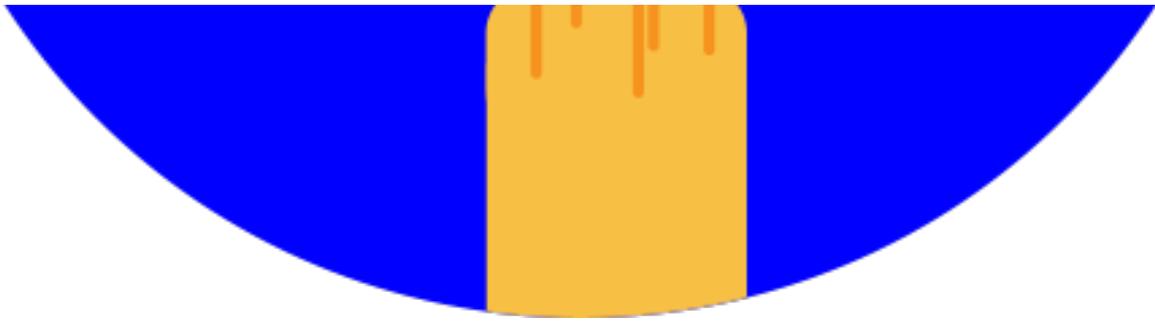


### A safety guide for the 'new normal' after COVID-19

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

FIND OUT  
MORE





### 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.

FIND OUT  
MORE



## 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?

FIND OUT  
MORE



## 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.

FIND OUT  
MORE



### 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.

FIND OUT  
MORE



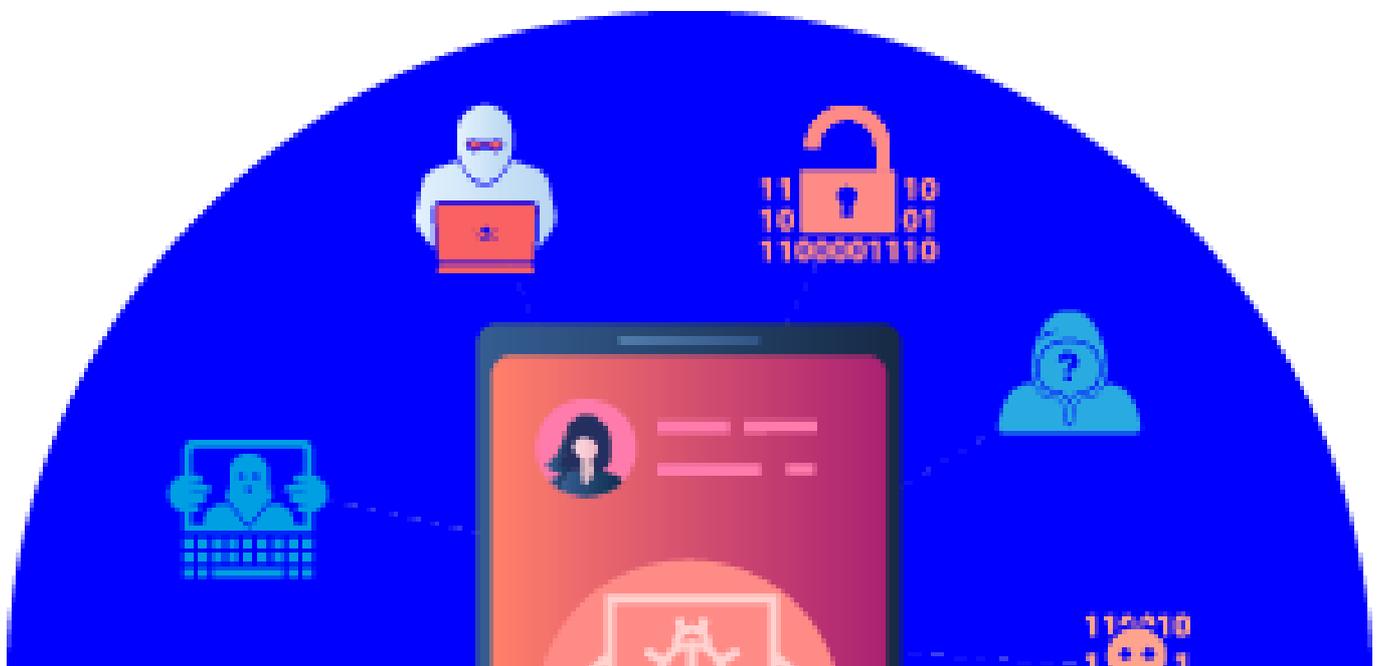


## Fraud

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.

FIND OUT  
MORE



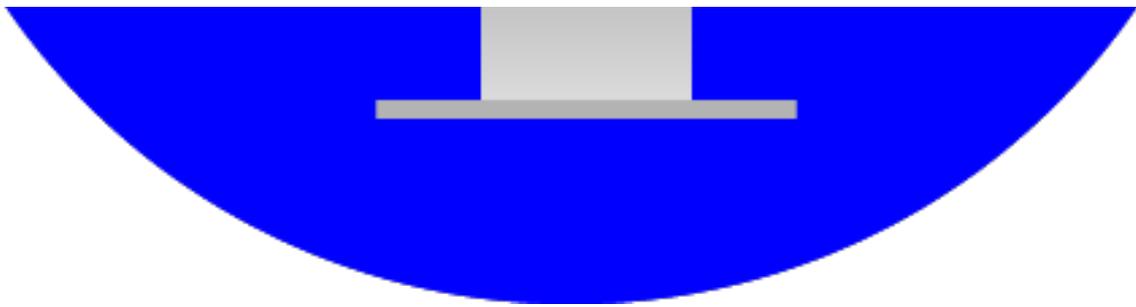


### Mobile threats

Criminal activities appropriating the COVID-19 outbreak have also gone mobile, with some instances of malware targeting Android devices.

FIND OUT  
MORE





### 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.

FIND OUT  
MORE



The global impact of COVID-19 means people will be spending more time online. This includes both children and adults.

FIND OUT  
MORE



### Spreading misinformation and disinformation

Get to know what to do to avoid becoming a part of the fake news distribution chain.

FIND OUT  
MORE



### 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!

FIND OUT  
MORE





### Get the kids involved

Download the PDF file, print it on an A4 or A3 paper and let your children colour it!

DOWNLOAD  
DRAWING

GENERAL TERMS:

[COVID-19](#)

CRIME AREAS:

[Trafficking in Human Beings](#) · [Facilitation of Illegal Immigration](#) · [Drug Trafficking](#) · [Cybercrime](#) · [Child Sexual Exploitation](#) · [Forgery of money and means of payment](#) ·

[Economic Crime](#) · [Organised property crime](#) · [Forgery of Administrative Documents and Trafficking therein](#) · [Intellectual property crime](#)

TARGET GROUPS:

[General Public](#) · [Law Enforcement](#) · [Academia](#) · [Professor](#) · [Students](#) · [Researcher](#) · [Press/Journalists](#) · [Other](#)

Source URL: <https://www.europol.europa.eu/activities-services/staying-safe-during-covid-19-what-you-need-to-know#comment-0>