INFINITY

IMMERSE. INTERACT. INVESTIGATE.

Policy Brief

Cybercrime Situation in Greece

DISSEMINATION LEVEL PUBLIC

PARTNER

Hellenic Police

AUTHORS

Nikolaos Georgiou

Apostolos Maspero

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No. 883293. The content of this document represents the view of the authors only and is their sole responsibility. The European Commission does not accept any responsibilty for any use that may be made of the information it contains.

Cybecrime situation in Greece[1]

1. Access to online services in Greece

The rapid evolution of information technology and the widespread use of Internet have led to revolutionary changes in all kinds of daily activities, such as work, socialization, education, entertainment, etc. This global phenomenon takes place also in Greece. The increasing usage of internet in Greece is evidenced by the statistics available, that show a continuous increase each year in all important indicators: internet access, online time, number of connected devices, participation in social media, e-commerce, use of mobile devices, etc.

In 2020, the Covid-19 pandemic accelerated this trend even more. More specifically, according to the report regarding the use of Information and Communication Technologies by households and individuals in Greece from the Hellenic Statistical Authority, in a representative nationwide sample of 5,111 people between 16-74 years old:[2]

» 8 out of 10 households had access to the internet from home (80.4 %)

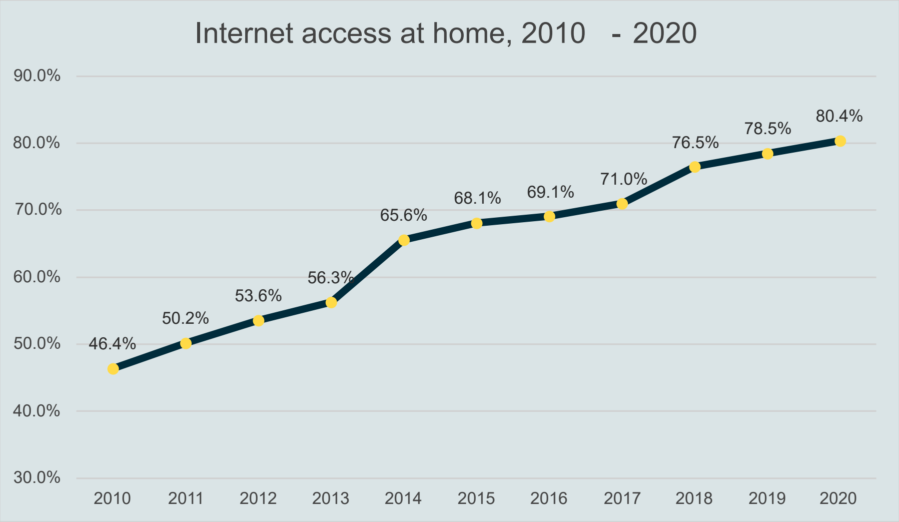


Figure 1: Access to the internet at home has steadily grown over the past 10 years.

» 1 out of 2 (47.8 %) persons having accessed the internet even once, in the first quarter of 2020, purchased or ordered goods or services over the internet for private purposes. Compared with the first quarter of 2019, the share of internet users who purchased or ordered goods or services online increased by 15.2 %.

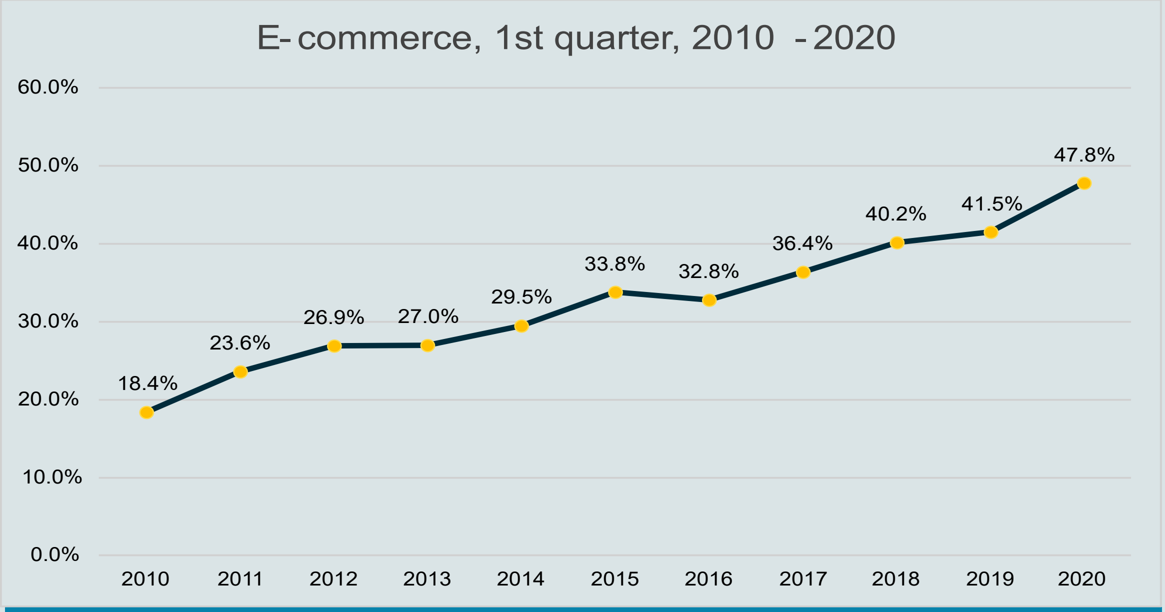


Figure 2: The number of people making online purchases has also grown

- 46.8% of population that have accessed the internet during the 1st quarter of 2020, used Internet Banking via website or app.
- 76% of population that have accessed the internet during the 1st quarter of 2020 are participating in social networks (Facebook, Twitter, Instagram, Snapchat etc.).
- According to the European E-Commerce Report for 2021, jointly published by the Hellenic E-Commerce Association, E-commerceEurope and EuroCommerce, Greece, in 2020, had the highest growth rate in e-commerce turnover in the EU with 77%.[3]
- According to the Financial Stability Report of the Bank of Greece, issued in June 2021, it appears that in the year 2020, there is an increase of 76% compared to the previous year in the number of fraudulent transactions with a corresponding increase of 18% of the value of fraudulent transactions, without, however, substantially changing the ratio of the number of fraud cases to the number of transactions.[4]

The widespread and ever-increasing use of the Internet and the information and communication technology (ICT), as evidenced by the above data, provides a large attack surface for cybercriminals. This phenomenon became even more intense during the Covid-19 pandemic era, where teleworking or hybrid work, shared between home and office, allowed cybercriminals to target employees that spend more time online.

2. Cybercrime Division - Hellenic Police

The Cybercrime Division of the Hellenic Police is the competent authority for the prevention, investigation and suppression of crime committed through the Internet or via ITC. The Cybercrime Division is an independent central service, which reports directly to the Chief of the Hellenic Police. It consists of five units that cover the whole range of cybercrimes against citizens:

- a. Unit of Administrative Support and Intelligence,
- b. Unit of Innovative Actions and Strategy,
- c. Unit of Electronic and Telephone Communication Security and Protection of Software and Intellectual Property Rights
- d. Unit of Minors Internet Protection and Digital Investigation
- e. Unit of Special Cases and Internet Economic Crimes Prosecution

Cybercrimes or cyber-dependent crimes can be defined as any crime that can only be committed using computers, computer networks or other forms of ICTs. Such types of crimes are: computer-related frauds, online child sexual exploitation and offences against the confidentiality, integrity and availability of computer data and systems (such as Illegal access, Illegal interception, etc).[5]

3. Cybercrime in Greece - statistics

Statistics from the Cybercrime Division regarding cybercrime show that the total number of new criminal cases handled during the year 2020 rose to 5,148.

As it is apparent from the chart below, there is a continuous increase in the number of cybercrimes throughout recent years. More specifically, the annual increase from 2019 to 2020 reached 14%.

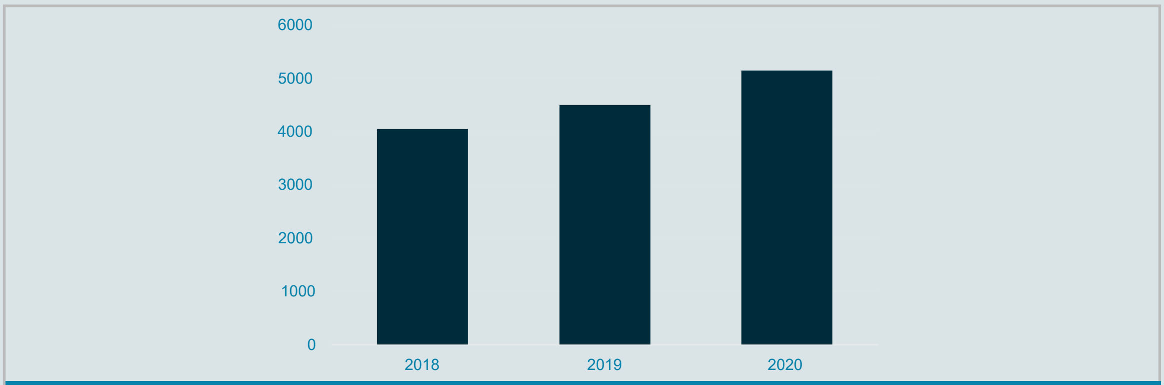


Figure 3: Year-on-year the number of cybercrimes reported to the Hellenic Police's Cybercrime division has also increased

The following chart differentiates the above mentioned 5,148 new cases for 2020 into different types of crime

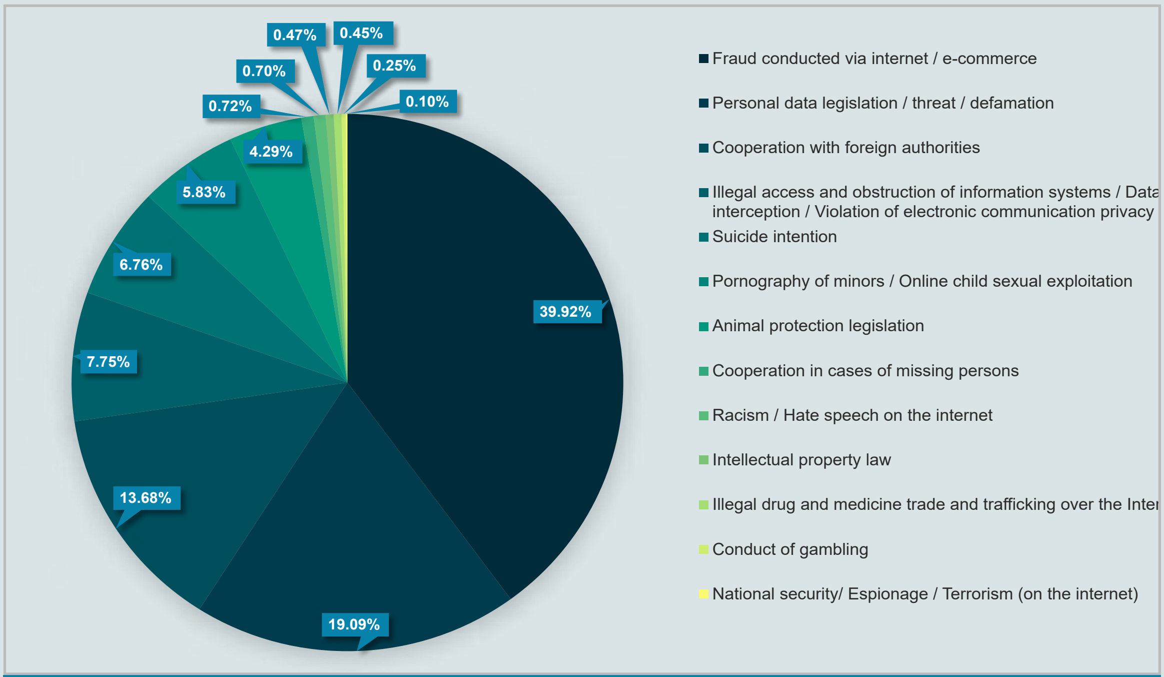


Figure 4: Percentage of the 5,148 reported cybercrimes in each category over 2020

4. Cybercrime trends in Greece

Cyber Attacks

Online Fraud Schemes

Online Child Sexual Exploitation

4.1 Online Fraud

A large amount, that reaches up to 40% of the total crimes, is related to online fraud. Online fraud increased by 13.66% from 2019 to 2020. Most of the cases were related to illegal money transfers through banking systems and fraud related to products purchase. New modus operandi also came up, such as scams committed through "sim swap", by replacement / change of mobile phone SIM cards and the scams with the promise of investment services.

Phishing is a well-known scam via e-mail, SMS or even messaging. In this message the scammer is presented as a reliable source, to deceive the recipients, to reveal sensitive information or to download malware. Phishing is often used with more diverse procedures, such as e.g. a user follows a link from an advertisement or an email and arrives at a page where they are asked to enter personal information and bank card details. Once they have this information, attackers can use it to steal money from a victim's account.

Investment-related messages did also appear online, promising extremely high returns, which can include lucrative investment opportunities such as stocks, bonds, cryptocurrencies, gemstones, offshore real estate investments and real estate.

The "Sim Swapping" model was also detected many times. The perpetrators in several cases gain illegal access to the victims' computers and steal their usernames and passwords on online banking platforms. Then, the perpetrators use "straw men" to issue new SIM cards on behalf of the victims.

In this way they manage to bypass the security procedures of e-banking (sending SMS or Viber text to customers with a unique code for each transaction) and remove large sums of money from the victims.

4.2 Cyber Attacks

The latest data show that cyber attacks in Europe are doubling. The number of serious cyber-attacks against critical targets in Europe in 2020 has risen and Covid-19 pandemic has contributed to this.

According to the EU Agency for Cyber Security (ENISA),[6] in 2020 there were 304 significant, malicious attacks against "critical targets", i.e. more than doubled from the 146 recorded in 2019. The agency also recorded a 47% increase in attacks on the critical sector of hospitals. This depicts the growing impact of cyber-attacks.

Europol also reported that criminals have used the Covid-19 scam to launch pandemic-themed social engineering attacks to distribute various malware packages.[7] Cybercriminals have also taken advantage of the growing number of businesses that offered the possibility of remote connection to their organizations' systems to assist remote working.

4.3 Child Sexual Exploitation Online

In 2020, Cyber Crime Division of Hellenic Police handled about 300 cases of Online Child Sexual Abuse.

During the Covid-19 lockdown, children turned into an online virtual life. They were mostly occupied with video calls with family and friends, social media, online gaming, remote education etc. According to Europol, sex offenders have found in this development a tempting opportunity to access a broader group of potential victims. there is also noticed an increase of distribution of child sexual exploitation material (CSAM) online, since offenders were unable to travel for sexual purposes.

Moreover, there has been an increase in detection and reporting of CSAM on the surface web, which indicates “the level of re-victimisation of children through the distribution of images and videos depicting them”.

4.4 Recent LEA cyber operations

On July 7, 2021, Greek and Romanian authorities arrested eight members of a Romanian criminal network involved in extensive online fraud against users of popular consumer sites such as Amazon and eBay, in a large operation coordinated by Eurojust.

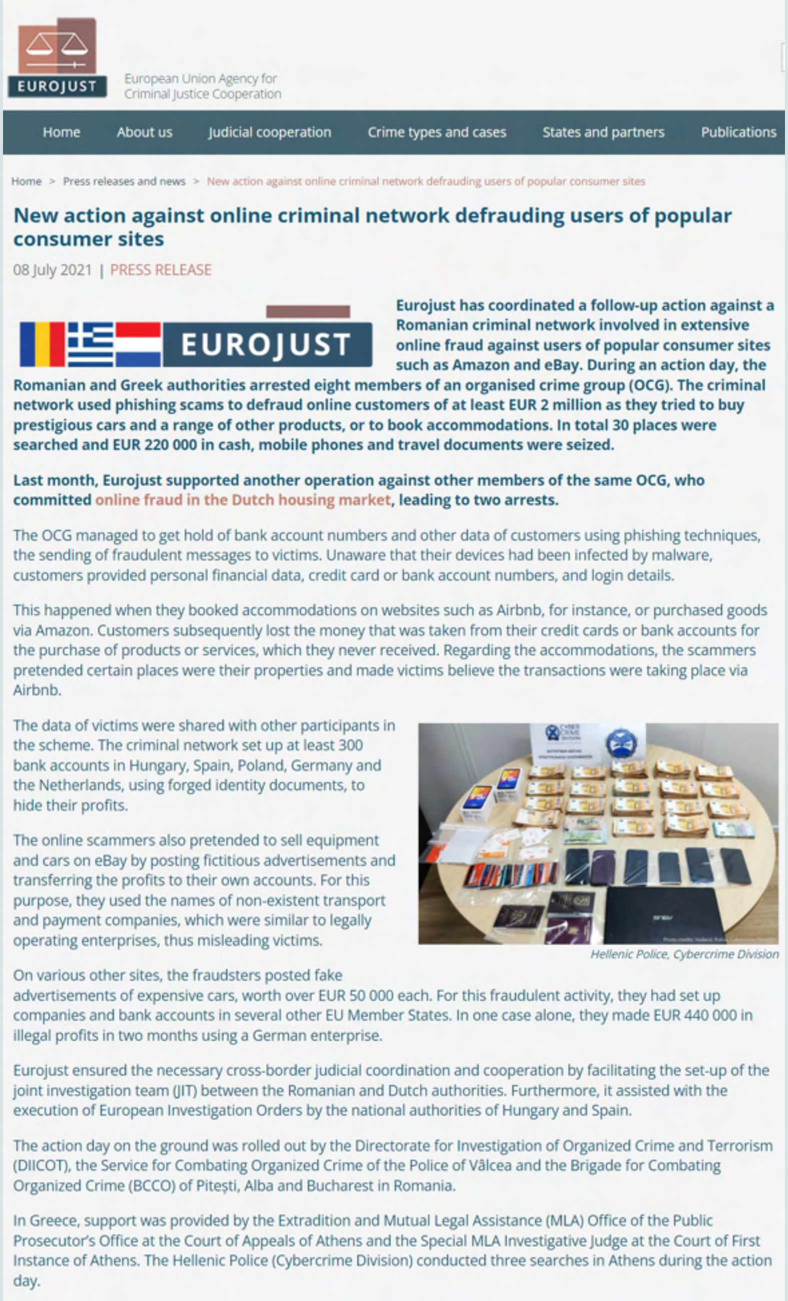
The gang used phishing scams to defraud online customers of at least 2 million euros as they tried to buy prestigious cars and a range of other products, or to book accommodations.

Police searched a total of 30 venues and seized 220.000 euros in cash, mobile phones and travel documents. The suspects managed to get hold of bank account numbers and other data of customers using phishing techniques, the sending of fraudulent messages to victims. Unaware that their devices had been infected by malware, customers provided personal financial data, credit card or bank account numbers, and login details when they booked accommodations on online platforms such as Airbnb or purchased goods via Amazon.

The scammers pretended certain houses were their properties and made victims believe the transactions were taking place via Airbnb.

Customers subsequently lost money for the purchase of products or services, which they never received.

The data of victims were shared with other participants in the scheme. The criminal network set up at least 300 bank accounts in Hungary, Spain, Poland, Germany and the Netherlands, using forged identity documents, to hide their profits.



EUROJUST
European Union Agency for
Criminal Justice Cooperation
Home
About us
Judicial cooperation
Crime types and cases
States and partners
Publications
Home > Press releases and news > New action against online criminal network defrauding users of popular consumer sites

New action against online criminal network defrauding users of popular consumer sites

08 July 2021 | PRESS RELEASE

Eurojust has coordinated a follow-up action against a Romanian criminal network involved in extensive online fraud against users of popular consumer sites such as Amazon and eBay. During an action day, the Romanian and Greek authorities arrested eight members of an organised crime group (OCG). The criminal network used phishing scams to defraud online customers of at least EUR 2 million as they tried to buy prestigious cars and a range of other products, or to book accommodations. In total 30 places were searched and EUR 220 000 in cash, mobile phones and travel documents were seized.

Last month, Eurojust supported another operation against other members of the same OCG, who committed online fraud in the Dutch housing market, leading to two arrests.

The OCG managed to get hold of bank account numbers and other data of customers using phishing techniques, the sending of fraudulent messages to victims. Unaware that their devices had been infected by malware, customers provided personal financial data, credit card or bank account numbers, and login details.

This happened when they booked accommodations on websites such as Airbnb, for instance, or purchased goods via Amazon. Customers subsequently lost the money that was taken from their credit cards or bank accounts for the purchase of products or services, which they never received. Regarding the accommodations, the scammers pretended certain places were their properties and made victims believe the transactions were taking place via Airbnb.

The data of victims were shared with other participants in the scheme. The criminal network set up at least 300 bank accounts in Hungary, Spain, Poland, Germany and the Netherlands, using forged identity documents, to hide their profits.

The online scammers also pretended to sell equipment and cars on eBay by posting fictitious advertisements and transferring the profits to their own accounts. For this purpose, they used the names of non-existent transport and payment companies, which were similar to legally operating enterprises, thus misleading victims.

Hellenic Police, Cybercrime Division

On various other sites, the fraudsters posted fake advertisements of expensive cars, worth over EUR 50 000 each. For this fraudulent activity, they had set up companies and bank accounts in several other EU Member States. In one case alone, they made EUR 440 000 in illegal profits in two months using a German enterprise.

Eurojust ensured the necessary cross-border judicial coordination and cooperation by facilitating the set-up of the joint investigation team (JIT) between the Romanian and Dutch authorities. Furthermore, it assisted with the execution of European Investigation Orders by the national authorities of Hungary and Spain.

The action day on the ground was rolled out by the Directorate for Investigation of Organized Crime and Terrorism (DIICOT), the Service for Combating Organized Crime of the Police of Vâlcea and the Brigade for Combating Organized Crime (BCCO) of Pitești, Alba and Bucharest in Romania.

In Greece, support was provided by the Extradition and Mutual Legal Assistance (MLA) Office of the Public Prosecutor's Office at the Court of Appeals of Athens and the Special MLA Investigative Judge at the Court of First Instance of Athens. The Hellenic Police (Cybercrime Division) conducted three searches in Athens during the action day.

Figure 5: Report from Eurojust from a Hellenic Police operation to disrupt a fraud network[8]

5. Conclusions

Cybercrime represents a new and fast-growing crime category in Greece within the last few years. From the data presented in detail, it is clear that the criminals took advantage of the Covid-19 pandemic by adapting the methods of their criminal action to the new situation.

Effective tackling of cybercrime requires a coordinated response by the competent authorities worldwide by taking advantage of an efficient and rapid judicial and law enforcement co-operation. On the other hand, in the direction of prevention, public awareness seems to be a way to minimize the effect of cybercriminals.

In the future, it is expected that cybercrime will become the dominant crime category, due to the various technological advancements and technological achievements should also be used in favor of the fight against cybercrime

References

1 This Policy Brief was prepared by the Cybercrime Division of the Hellenic Police, as part of INFINITY T10.5.

2 Survey on the Use of Information and Communication Technologies by Households and Individuals and Use of e-Commerce, Privacy and Protection of Personal Data and Internet Security, 10/11/2020, available at: https://www.statistics.gr/documents/20181/3149df81-e734-3655-329b-444674aaf9f9

3 European e-Commerce Report (2021) p.10, available at: https://ecommerce-europe.eu/wp-content/uploads/2021/09/2021-European-E-commerce-Report-LIGHT-VERSION.pdf

4 The Financial Stability Review p.59-60, Bank of Greece, June 2021, available at: https://www.bankofgreece.gr/ekdoseis-ereyna/ekdoseis/ekthesh-xrhmatopistwtikhs-statherothtas

5 Germanos,G. & Georgiou, N. (2021), Cybercrime: Prevention and Investigation (in Greek), p.71-73, ISBN 978-618-00-2651-1

6 EU Agency for Cyber Security (ENISA) (2021). ENISA Threat Landscape 2021, available at https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

7 Europol (2021), Internet Organised Crime Threat Assessment (IOCTA) 2021, available at https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2021

8 Eurojust (2021) New action against online criminal network defrauding users of popular consumer sites. European Union Agency for Criminal Justice Cooperation. 8 July 2021. https://www.eurojust.europa.eu/new-action-against-online-criminal-network-defrauding-users-popular-consumer-sites

Image Credits

p.6. Image by FotoRieth. https://pixabay.com/photos/bullying-hands-face-crawl-away-her-679274/