



Hellenic Police Headquarters Financial Police & Cyber Crime Agency

Cybercrime sub division [1]

- Established as a unit with the presidential order 100/2004.
- 06/2010: Recruitment of 25 police officers with special duties.
- Presidential order 9/2011: Establishment of the new **Economic Police and Cyber Crime Subdivision** as an independent Subdivision.
- The personnel of our Unit includes police officers and policemen.



Υποδιεύθυνση
Δίωξης Ηλεκτρονικού Εγκλήματος
Πεδίο Δράσης

Cybercrime sub division [2]

1

- Department of General Affairs & Personal Data Protection

2

- Department of Minor Protection

3

- Department of Software and Intellectual Property Rights Protection

4

- Department of Electronic Communication Security

Cooperation



Department of General Affairs & Personal Data Protection

- Prosecution of crimes committed with the use of the Internet and other electronic media and digital communication.
- Jurisdiction in entire Greece.
- Addressed Crimes
 - *Online fraud*
 - *Online gambling*
 - *Crimes committed through the social media*
 - *Personal data violation*
 - *Defamation, threats, blackmails with the use of electronic means*

Department of General Affairs & Personal Data Protection

- Techniques:
 - *Complaints from citizens*
 - *Facebook investigations*
 - *Online investigations*
 - *Interpol / Europol*
 - *Investigation in order to identify the electronic traces of the perpetrator*
 - *Contacting with internet service providers to provide us with the identity of the perpetrator*
 - *Field Investigation, arrestments, seizures*

Fraud

- 45% of the reports to our Unit concern frauds.
- Millions of euro every year from phishing attacks, credit card frauds, fraudulent sales and other frauds.
- Deliberate misinformation for online products.
- Excessive charges on credit cards for services that were never requested.
- Promises of jobs at home with increased profits.

Scam Emails

- Reception of an email informing you that you have won a great prize or legacy.
- Need for the provision of personal banking data or of a great amount of money in order to acquire the prize.
- Trying to identify the electronic traces of the email sender.



Phishing

- 'Phishing' of personal and banking data through fake websites.
- Worldwide profits for the perpetrators more than 1 billion annually.



Social Media [1]



4.300.000 USERS



465.400 USERS



963.000 USERS

- Variety of criminal activities with the use of social media accounts.

Social Media [2]

- 'Fake' or stolen social media accounts
- Offensive posts
- Publication of personal photos or videos
- Defamation of the victims
- Personal data violation
- Online threats
- Blackmailing of the victims
- Cyber bullying

Online Gambling

- Variety of webpages containing illegal online games.
- Law 4002/2011: established the criteria for the legal use of online games.
- Credit card frauds.
- Money laundering.



Department of Minor Protection [1]

- Prosecution of crimes committed against minors using the Internet and other electronic media and digital communication.
- Jurisdiction in entire Greece.
- Addressed Crimes
 - *Child pornography*
 - *Cyber Bulling*
 - *Suicides*
 - *Abduction / disappearance of minors*
 - *Sexual Exploitation / abuse*

Department of Minor Protection [2]

- Our unit was involved in many important operations against child pornography:
- 2004-2011: The investigations led to the arrestment of over 300 persons for child pornography.
- Suicides:
 - *Over 300 intentions to suicide during 2011 - 2013.*

Department of Minor Protection [3]

- Programs / techniques:
 - *T.L.O. (child pornography tool)*
 - *Complaints from parents / minors*
 - *Interpol / Europol*
 - *P2P investigations with known key words*
 - *Seminars to parents / minors*

Dept. of Software and Intellectual Property Protection

- Responsible for cases regarding:
 - *Hacking/cracking*
 - *Illegal sharing of copyright protected software*
 - *Illegal sharing of digital content (music/video)*
 - *Cable and Satellite TV key sharing*

Department of Electronic Communication Security

- Responsible for cases regarding:
 - *Internet Communications Security and Privacy*
 - *Auditing of Internet network infrastructures*
 - *Data protection*
 - *VoIP*
 - *Mobile Communication (Smartphone)*

Future Threats

- Cloud computing
- Wearable technology
- Crime as a Service
- Bring your own technology (BYOT), bring your own phone (BYOP)
- SPIT (SPam over Internet Telephony)
- Electronic money



Development Area

- Online educational platform.
- Creation of an educational center.
- Co-operation with the Academic Institutions and the Private sector in order to create innovative tools.
- Modern equipment in order to deal with ever changing cyber crime challenges.
- Secure system for the exchange of instant information between law enforcement agencies.

Thank you for your attention !