

# APAV in the Support to victims of Cybercrime

ROAR Workshop

***Gaps, Challenges and Best Practices in Preventing and Combatting Cybercrime***



ROAR  
empowering  
victims of  
cybercrime

Co-funded by the  
European Union's Internal  
Security Fund - Police



APAV®

Apoio à Vítima



APAV®

Victim Support

# The Portuguese Association for Victim Support

- **social charity** organization, founded in 1990;
- its goal is to **inform, protect** and **support** victims of crime;
- supported by **volunteers**;
- giving **free** and **confidential** support in a **personal, sensitive** and **professional** way;
- is governed by the principles of **equal opportunities, treatment** and **non-discrimination**.



# The Portuguese Association for Victim Support

## Victim Support Offices®

Network of 20 Victim Support Offices® in Portugal

31 Itinerant Support Offices



## Specialised Sub-networks

Specialised Support Network to Families and Friends Victims of Homicide and Terrorism



Specialized Support Network to Children and Youth Victims of Sexual Violence



Support Network to Migrant Victims



## Safer Internet Helpline

LIS | Safer Internet Helpline



## System of Integrated Support at a Distance

LAV | Victim Support Helpline



## Shelters

Network of Shelters



SUL Centre for Shelter and Protection



70 community-based services



# Safer Internet Helpline



Safer  
Internet  
Helpline

800 219 090



A vertical banner on the right side of the page. The top section is orange and contains the ROAR logo (a geometric shape) and the text "ROAR empowering victims of cybercrime", along with a small European Union logo and the text "Co-funded by the European Union's Internet Security Fund - Police". The middle section is red and contains the APAV logo (silhouettes of people) and the text "Apoio à Vítima". The bottom section is white and contains the APAV logo and the text "Victim Support".

# Safer Internet Helpline – 2 types of support

- A platform for reporting online contents: **child pornography, incentive to racism and incentive to violence**
- A Helpline for Cybercrime Victims, available from **09h00 to 21h00** on **working days**



# Safer Internet Helpline

Helpline for Cybercrime Victims, available from **09h00 to 21h00** on **working days**

With this helpline we aim to assure free and confidential support on the following situations:

- **Cybercrime victims** – e.g. Cyber–bullying, Grooming, Identity Theft
- **Technical Help in promoting the safe use of the Internet**
- **Online Addictions** (Social Media, Videogames)



# Safer Internet Helpline

The platform for reporting online contents of **child pornography, incentive to racism and incentive to violence** works in the following way:

1. The content's link is shared through a complaint form available on Centro Internet Segura's website.
2. The content is reviewed and classified by the expert.
3. If the above mentioned content is involved, it will be denounced to the competent authorities, namely the Judiciary Police (PJ)
4. After notifying the police, the content is signalled to the **Internet Service Providers** (if the content is lodged in Portugal).
5. The content is removed within **three working days** (preferably).



# Awareness raising and changing attitudes

AT LUNCH TIME,  
ANTHONY ENTERED AT

WWW.DATING-WEBSITE.COM

AFTER DESERT HE LEFT WITH

WWW.HACKED-COMPANY.COM

WHAT HAPPENS ONLINE DOESN'T STAY ONLY ONLINE.  
A LINK MAY DESTROY YOUR LIFE AND GO FROM DIGITAL TO REAL.  
REPORT 800 219 090

APAV<sup>®</sup>  
Apoio à Vítima

Safer Internet Helpline  
800 219 090

WHEN SHE BOOKED HER VACATIONS ONLINE,  
MARIA THOUGHT THAT SHE WAS GOING TO A

WWW.LUXURY-COVERED-HOTEL.COM

AND SHE ENDED UP WITH A

WWW.OVERDRAFT-BANK-ACCOUNT-AT-NET.COM

WHAT HAPPENS ONLINE DOESN'T STAY ONLY ONLINE.  
A LINK MAY DESTROY YOUR LIFE AND GO FROM DIGITAL TO REAL.  
REPORT 800 219 090

APAV<sup>®</sup>  
Apoio à Vítima

Safer Internet Helpline  
800 219 090



**ROAR**  
empowering victims of cybercrime

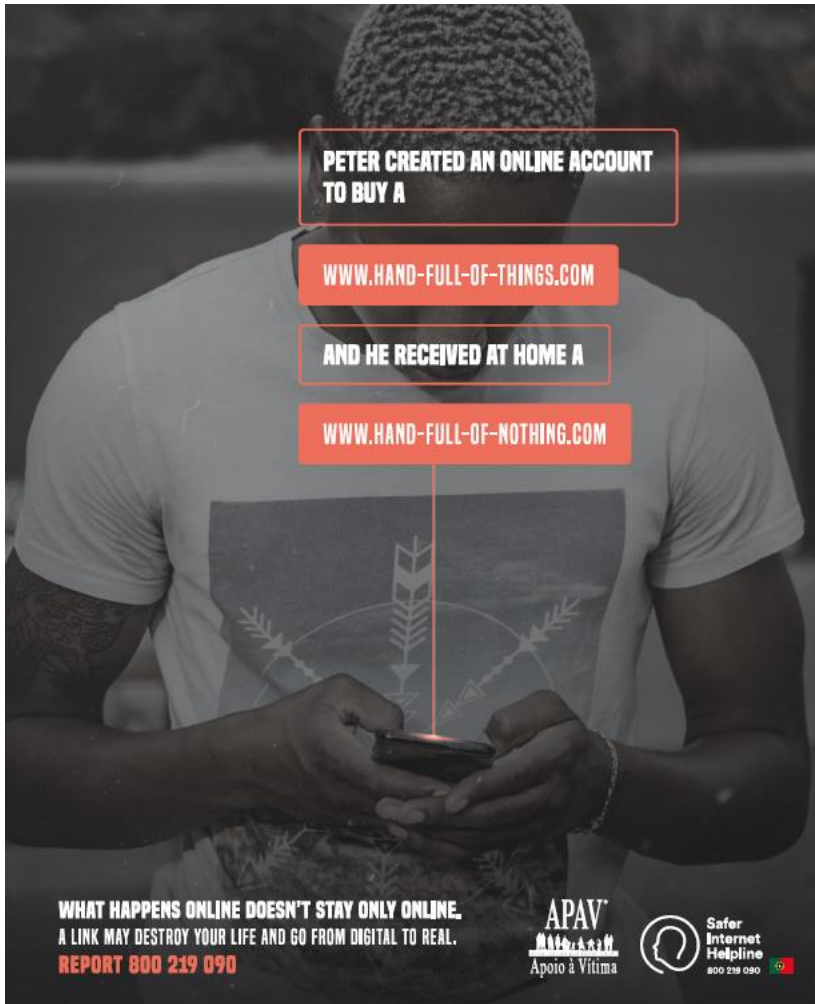
Co-funded by the European Union's Internal Security Fund - Police

**APAV<sup>®</sup>**  
Apoio à Vítima

**APAV<sup>®</sup>**  
Victim Support



# Awareness raising and changing attitudes



PETER CREATED AN ONLINE ACCOUNT TO BUY A

WWW.HAND-FULL-OF-THINGS.COM

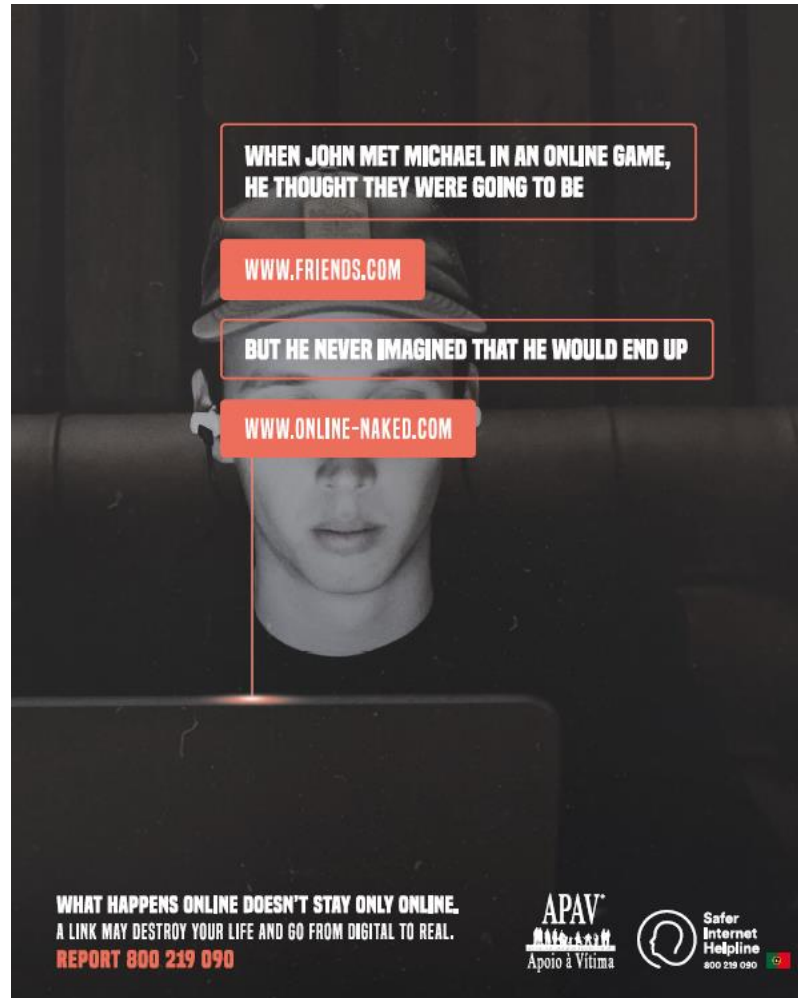
AND HE RECEIVED AT HOME A

WWW.HAND-FULL-OF-NOTHING.COM

WHAT HAPPENS ONLINE DOESN'T STAY ONLY ONLINE. A LINK MAY DESTROY YOUR LIFE AND GO FROM DIGITAL TO REAL. REPORT 800 219 090

APAV<sup>®</sup> Apoio à Vítima

Safer Internet Helpline 800 219 090



WHEN JOHN MET MICHAEL IN AN ONLINE GAME, HE THOUGHT THEY WERE GOING TO BE

WWW.FRIENDS.COM

BUT HE NEVER IMAGINED THAT HE WOULD END UP

WWW.ONLINE-NAKED.COM

WHAT HAPPENS ONLINE DOESN'T STAY ONLY ONLINE. A LINK MAY DESTROY YOUR LIFE AND GO FROM DIGITAL TO REAL. REPORT 800 219 090

APAV<sup>®</sup> Apoio à Vítima

Safer Internet Helpline 800 219 090

# Awareness raising and changing attitudes

**WHEN SHE MARRIED GEORGE,  
KATE THOUGHT THEY WERE GOING TO BE**

[WWW.HAPPILY-EVER-AFTER.COM](http://WWW.HAPPILY-EVER-AFTER.COM)

**AND SHE ENDED UP**

[WWW.ONLINE-NAKED-EVER-AFTER.COM](http://WWW.ONLINE-NAKED-EVER-AFTER.COM)

**WHAT HAPPENS ONLINE DOESN'T STAY ONLY ONLINE.  
A LINK MAY DESTROY YOUR LIFE AND GO FROM DIGITAL TO REAL.**  
**REPORT 800 219 090**

**APAV**  
Apoio à Vítima

Co-funded by the European Union's Internal Security Fund - Police

Ministério Público

WESSER RING

ACTEDO

altice

SAFER INTERNET HELPLINE  
800 219 090

**MARINNA TOLD PAULA HER BIGGEST  
SECRET BECAUSE THEY WERE**

[WWW.BEST-FRIEND.COM](http://WWW.BEST-FRIEND.COM)

**AND SHE ENDED UP**

[WWW.EXPOSED-AND-WITHOUT-FRIEND.COM](http://WWW.EXPOSED-AND-WITHOUT-FRIEND.COM)

**WHAT HAPPENS ONLINE DOESN'T STAY ONLY ONLINE.  
A LINK MAY DESTROY YOUR LIFE AND GO FROM DIGITAL TO REAL.**  
**REPORT 800 219 090**

**APAV**  
Apoio à Vítima

Co-funded by the European Union's Internal Security Fund - Police

Ministério Público

WESSER RING

ACTEDO

altice

SAFER INTERNET HELPLINE  
800 219 090

**ROAR**  
empowering victims of cybercrime

Co-funded by the European Union's Internal Security Fund - Police

**APAV**  
Apoio à Vítima

**APAV**  
Victim Support



# Awareness raising and changing attitudes

WHEN JOANNA ASSUMED HERSELF IN  
[WWW.GROUP-OF-FRIENDS.COM](http://WWW.GROUP-OF-FRIENDS.COM)  
SHE NEVER IMAGINED SHE WOULD BE  
[WWW.VICTIM-OF-HATE.COM](http://WWW.VICTIM-OF-HATE.COM)

WHAT HAPPENS ONLINE DOESN'T STAY ONLY ONLINE.  
A LINK MAY DESTROY YOUR LIFE AND GO FROM DIGITAL TO REAL.  
**REPORT 800 219 090**

APAV<sup>®</sup>  
Apoio à Vítima

Safer Internet Helpline  
800 219 090



ROAR  
empowering victims of cybercrime

Co-funded by the European Union's Internal Security Fund - Police

APAV<sup>®</sup>  
Apoio à Vítima

APAV<sup>®</sup>  
Victim Support



# Support to victims of cybercrime

# ROAR

## Manual de Formação:

Apoio Especializado a Vítimas de Cibercrime

## Training Manual:

Specialised Support to Victims of Cybercrime

## Manual de Formare:

Asistență Specializată pentru Victimele  
Criminalității Informatice



**ROAR**  
empowering  
victims of  
cybercrime

**APAV**  
Apoie à Vitima



This Manual was funded by the  
European Union's Internal  
Security Fund – Police

PART 1 - UNDERSTANDING CYBERCRIME	37
MODULE 1 - UNDERSTANDING CYBERCRIME PHENOMENA	37
Typologies of cybercrime	37
Concepts and definitions	37
Risk factors and related behavioural vulnerabilities related to cyber-victimisation	40
MODULE 2 - LEGAL FRAMEWORK OF CYBERCRIME	45
Cybercrime in International Law and in the European Union acquis	45
National legal framework of cybercrime	45
Investigation and law enforcement main challenges	46
MODULE 3 - VICTIMOLOGY AND IMPACT OF CYBERCRIME	53
Prevalence of cybercrime	53
Impact on individual victims	53
<ul style="list-style-type: none"><li>Physical, psychological and emotional health consequences</li><li>Financial impact</li><li>Fear of cybercrime and perceptions of cybersecurity</li></ul>	54 54 54
PART 2 - SPECIALISED SUPPORT TO VICTIMS OF CYBERCRIME	61
MODULE 4 - KEY ASPECTS OF SPECIALISED SUPPORT TO VICTIMS OF CYBERCRIME	61
Structuring specialised support to victims of cybercrime	61
<ul style="list-style-type: none"><li>Empathy, communication techniques and emotional support</li><li>Collection of information</li><li>Risk assessment and development of protection plans</li><li>Identification of support needs</li><li>Crisis intervention</li></ul>	61 62 62 63 64
MODULE 5 - SPECIALISED SUPPORT TO VICTIMS OF CYBER-DEPENDENT CRIMES	71
Modi operandi and nature of the crime	71
Prevention strategies	72
Intervention strategies	73
<ul style="list-style-type: none"><li>Strategies for preserving digital evidence</li><li>To whom and how to report</li><li>Strategies to overcome victimisation and its impacts</li></ul>	73 73 73
MODULE 6 - SPECIALISED SUPPORT TO VICTIMS OF ONLINE FRAUD	81
Types, modi operandi and nature of the crimes	81
<ul style="list-style-type: none"><li>Online shopping (ecommerce) fraud</li><li>Bank fraud</li><li>Scams in intimate relationships (romance and dating scams)</li></ul>	81 81 82
Prevention strategies	83
Intervention strategies	83
<ul style="list-style-type: none"><li>Strategies for preserving digital evidence</li><li>To whom and how to report</li><li>Strategies to overcome victimisation and its impacts</li></ul>	83 84 84



**ROAR**  
empowering  
victims of  
cybercrime



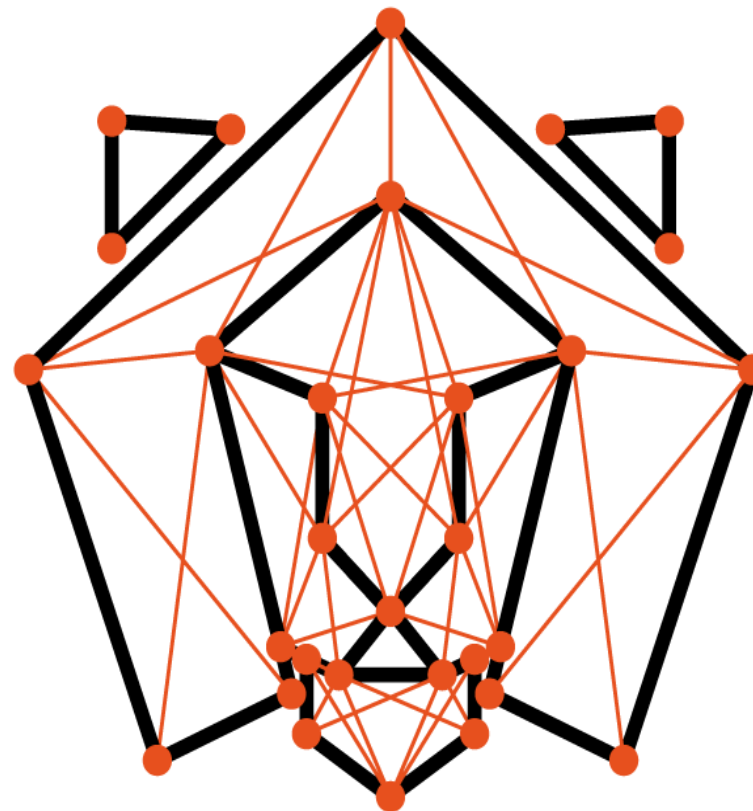
Co-funded by the  
European Union's Internal  
Security Fund - Police

**APAV**  
Apoie à Vitima

**APAV**  
Victim Support

# Support to victims of cybercrime

MODULE 7 - SPECIALISED SUPPORT TO VICTIMS OF ONLINE IDENTITY THEFT	97
Modi operandi and nature of the crime	97
Prevention strategies	99
Intervention strategies	99
<ul style="list-style-type: none"> <li>• Strategies for preserving digital evidence</li> <li>• To whom and how to report</li> <li>• Strategies to overcome victimisation and its impacts</li> </ul>	99 99 100
MODULE 8 - SPECIALISED SUPPORT TO CHILDREN AND YOUNG PEOPLE VICTIMS OF ONLINE SEXUAL ABUSE	109
Types, modi operandi and nature of the crimes	109
<ul style="list-style-type: none"> <li>• Dissemination of child sexual abuse material (CSAM)</li> <li>• Child sexual abuse material generated online</li> <li>• Self-generated content</li> <li>• Live streaming of child sexual abuse</li> <li>• Online grooming</li> <li>• Grooming via social networks and online video games</li> </ul>	109 109 110 110 110 110
Prevention strategies	111
Intervention strategies	111
<ul style="list-style-type: none"> <li>• Strategies for preserving digital evidence</li> <li>• To whom and how to report</li> <li>• Strategies to overcome victimisation and its impacts</li> </ul>	111 112 112
MODULE 9 - SPECIALISED SUPPORT TO VICTIMS OF CYBERBULLYING	123
Modi operandi and nature of the crime	123
Prevention strategies	124
Intervention strategies	124
<ul style="list-style-type: none"> <li>• Strategies for preserving digital evidence</li> <li>• To whom and how to report</li> <li>• Strategies to overcome victimisation and its impacts</li> </ul>	124 124 125
MODULE 10 - SPECIALISED SUPPORT TO VICTIMS OF ONLINE VIOLENCE IN INTERPERSONAL RELATIONSHIPS: CYBERSTALKING AND NON-CONSENSUAL SHARING OF IMAGES	135
Types, modi operandi and nature of the crime	135
<ul style="list-style-type: none"> <li>• Cyberstalking</li> <li>• Non-consensual image sharing</li> </ul>	135 135
Prevention strategies	136
Intervention strategies	136
<ul style="list-style-type: none"> <li>• Strategies for preserving digital evidence</li> <li>• To whom and how to report</li> <li>• Strategies to overcome victimisation and its impacts</li> </ul>	136 137 137



# Support to victims of cybercrime

## Typologies of cybercrime

### Typologies of cybercrime

This Module presents definitions for the concept of cybercrime. We use different typologies and categorisations to demonstrate this phenomenon's complexity and the range of forms or types of acts included.

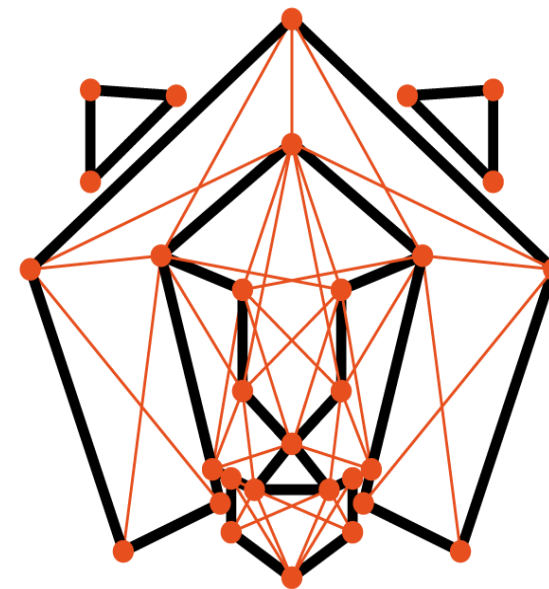
As these definitions and typologies are developed in Chapter 1 - Part I of the *ROAR Handbook - from understanding and preventing cybercrime to supporting and empowering victims*, this Manual will only present a summary of this content, with emphasis on key concepts.

The trainer should point out that cybercrime can be categorised into:

- **Cyber-dependent crimes** – these are associated with new forms of crime, whose occurrence depends on the existence and use of ICT, computers and computer networks (Leukfeldt, Notté & Malsch, 2020; Maimon & Louderback, 2019). They are designated cybercrimes *stricto sensu* as their practice depends on a computer system and their aim is to attack the availability, access, integrity, authenticity, confidentiality, conservation and security of information.
- **Cyber-enabled crimes** - traditional forms of crime in which ICT plays an important role, and which include not only financially motivated crime, but also forms of interpersonal violence and sex crimes. Examples are cyberstalking or Internet scams (Leukfeldt et al., 2020).

In the latter case, the different forms of cybercrime that are made possible or enabled by the Internet and ICT can be further subdivided into:

- Financially motivated cybercrimes (e.g. phishing<sup>9</sup> and romance and dating scams<sup>10</sup>);
- Cybercrimes in interpersonal relationships (e.g. cyberstalking<sup>11</sup>);
- Sexual cybercrimes (e.g., revenge porn<sup>12</sup>).



# Support to victims of cybercrime

## Concepts and definitions

### Introduction and overview:

Introductions and survey of expectations

Introduction of the trainer

Introductions of the participants

Presentation of the objectives and content of the training course

### Typologies of cybercrime:

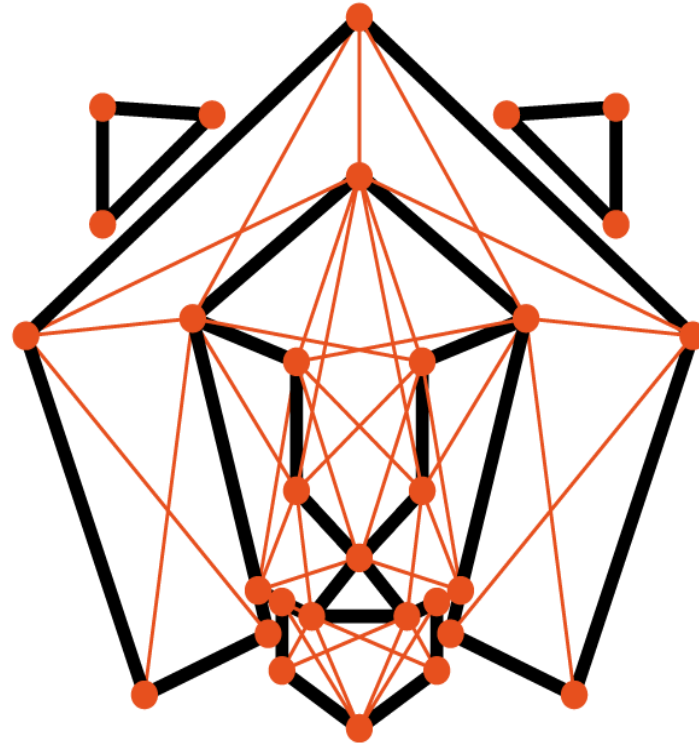
- Cyber-dependent crimes vs. cyber-enabled crimes

### Concepts and definitions:

- Concepts and definitions:
- Hacking, spamming, malware, phishing and DDoS (distributed denial of service) attack
- Online fraud: online shopping (e-commerce) fraud, bank fraud and intimate relationship scams (online romance and dating scams)
- Online identity theft
- Online child sexual abuse and exploitation: online live child sexual abuse, online grooming and child sexual abuse material
- Cyberbullying
- Cyberstalking and non-consensual image sharing

### Risk factors and behavioural vulnerabilities related to cyber-victimisation:

- Risk factors associated with socio-demographic characteristics
- Risk factors associated with the use of the Internet and ICT





# Support to victims of cybercrime

## Legal framework

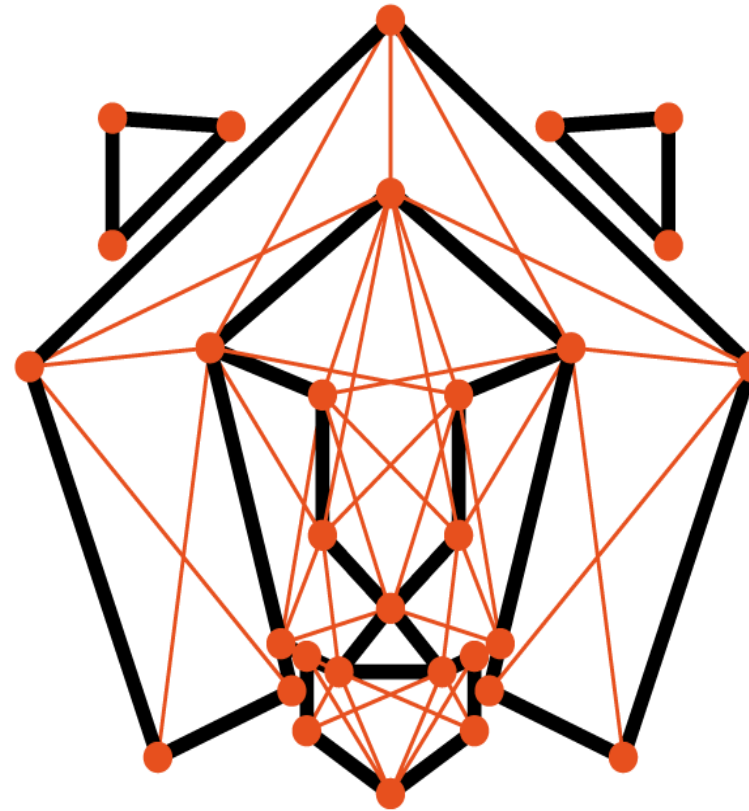
Cybercrime in International Law and in the European Union acquis

Cybercrime in International Law and in the European Union acquis:

- Cybercrime in International Law and in the European Union acquis:
- Council of Europe Convention on Cybercrime
- Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse
- Cybersecurity Strategy of the EU
- European Parliament resolution on the fight against cybercrime
- Directive 2011/92/EU - on combating the sexual abuse, sexual exploitation of children and child pornography
- Directive 2013/40/EU - on attacks against information systems
- Directive (EU) 2019/713 - on combating fraud and counterfeiting of non-cash means of payment
- Directive 2000/31/EC - on electronic commerce
- Regulation 2016/679 - general data protection regulation (GDPR)

National legal framework of cybercrime

Investigation and law enforcement main challenges



Co-funded by the European Union's Internet Security Fund - Police





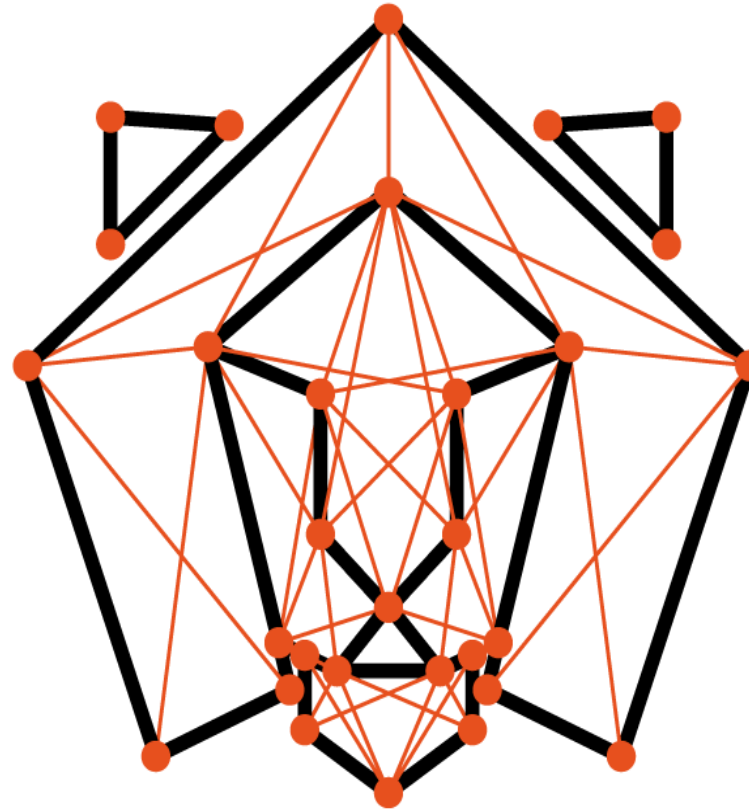
# Support to victims of cybercrime

## Understanding cybercrime: victimology and impact

Prevalence of cybercrime

Impact on individual victims:

- Physical, psychological and emotional health consequences
- Financial impact
- Fear of cybercrime and perceptions of cybersecurity



Co-funded by the  
European Union's Internet  
Security Fund - Police



# Support to victims of cybercrime

## Key aspects in specialised support to victims

Structuring specialised support to victims of cybercrime

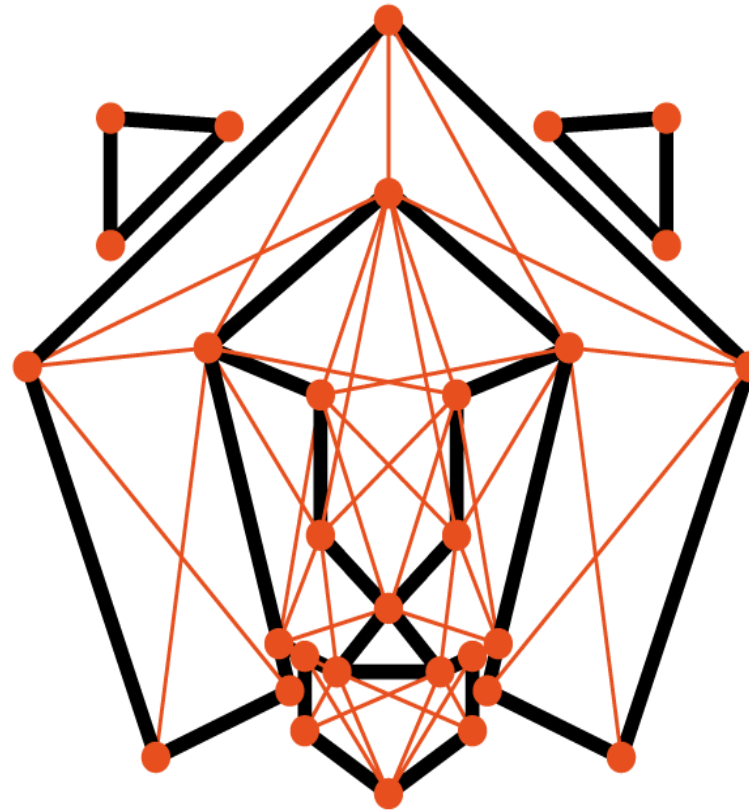
Empathy, communication techniques and emotional support

Collection information

Risk assessment and development of protection plans

Identification of support needs

Crisis intervention



# Support to victims of cybercrime

## Specialised support to victims of cyber-dependente crimes

Modi operandi and nature of the crimes

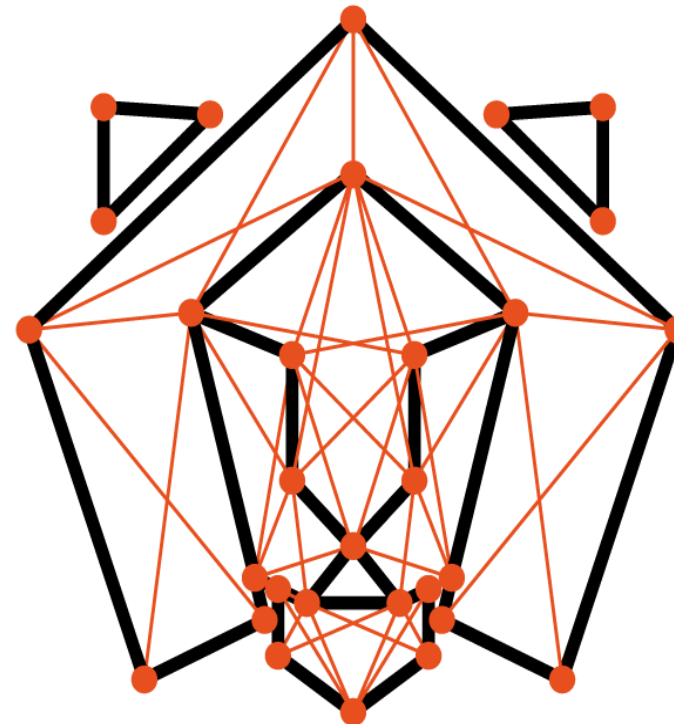
Prevention strategies

Intervention strategies:

- Strategies for preserving digital evidence
- To whom and how to report
- Strategies to overcome victimisation and its impacts



- Malware and Hacking
- Distributed denial-of-service (DDoS) attacks
- Ransomware
- Phishing, spear phishing
- Exploiting software vulnerabilities to gain remote access
- Theft of online personal/confidential information



Co-funded by the  
European Union's Internet  
Security Fund - Police



# Support to victims of cybercrime

## Specialised support to victims of online fraud

### Types of online fraud:

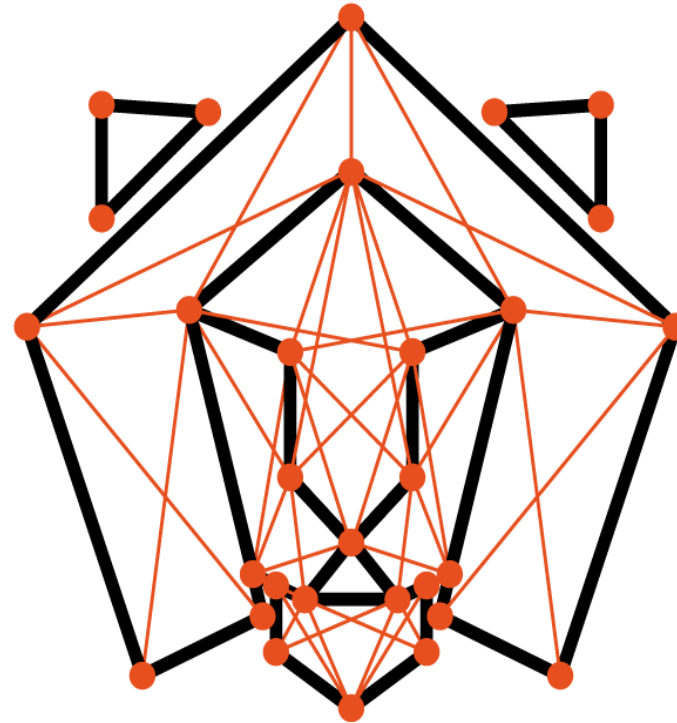
- Online (ecommerce) fraud
- Bank fraud
- Scams in intimate relationships

### Modi operandi and nature of the crimes

### Prevention strategies

### Intervention strategies:

- Strategies for preserving digital evidence
- To whom and how to report
- Strategies to overcome victimisation and its impacts



# Support to victims of cybercrime

## Specialised support to children and young people victims of online sexual abuse

### Types of online child sexual abuse:

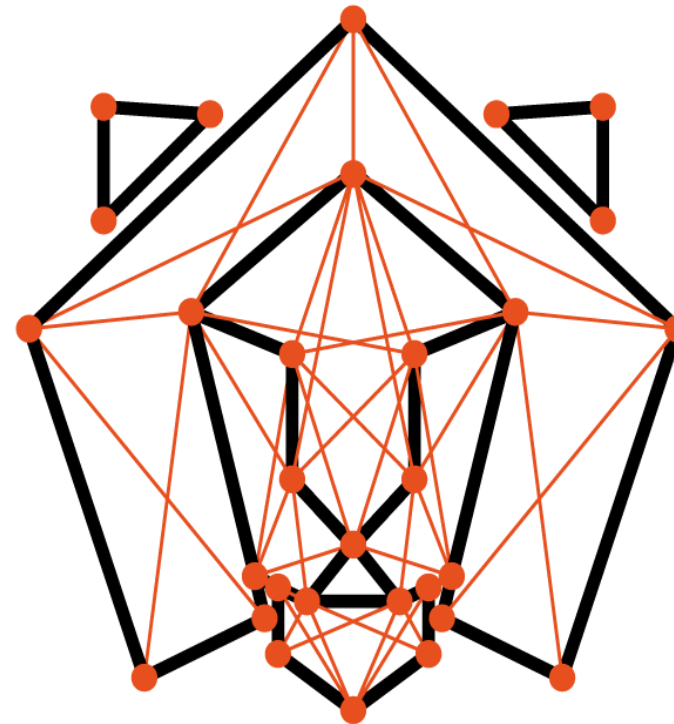
- Dissemination of child sexual abuse material: child sexual abuse content generated online; self-produced content; live streaming of child sexual abuse
- Grooming: online grooming on social networks and online video games

### Modi operandi and nature of the crimes

### Prevention strategies

### Intervention strategies:

- Strategies for preserving digital evidence
- To whom and how to report
- Strategies to overcome victimisation and its impacts



# Support to victims of cybercrime

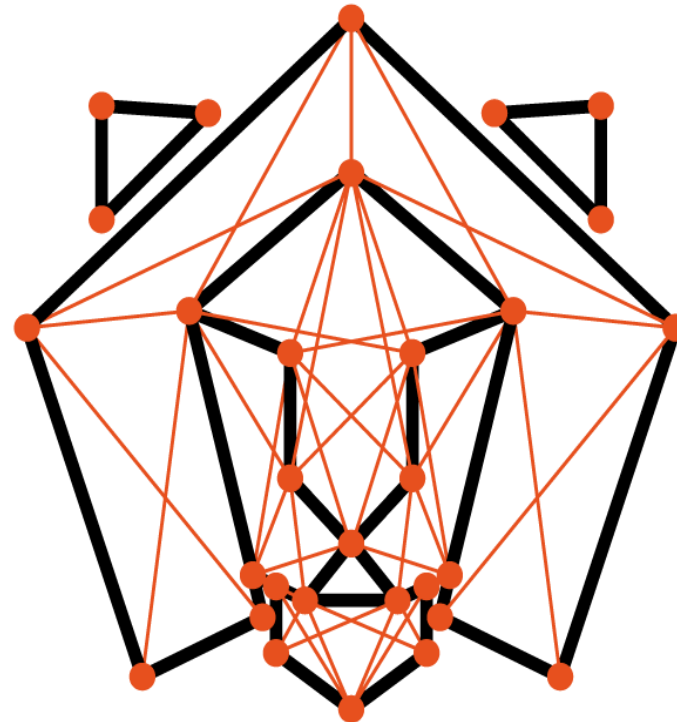
## Specialised support to victims of cyberbullying

Modi operandi and nature of the crimes

Prevention strategies

Intervention strategies:

- Strategies for preserving digital evidence
- To whom and how to report
- Strategies to overcome victimisation and its impacts



Co-funded by the European Union's Internet Security Fund - Police



# Support to victims of cybercrime

## Specialised support to victims of cyberstalking and non-consensual sharing of images

### Types:

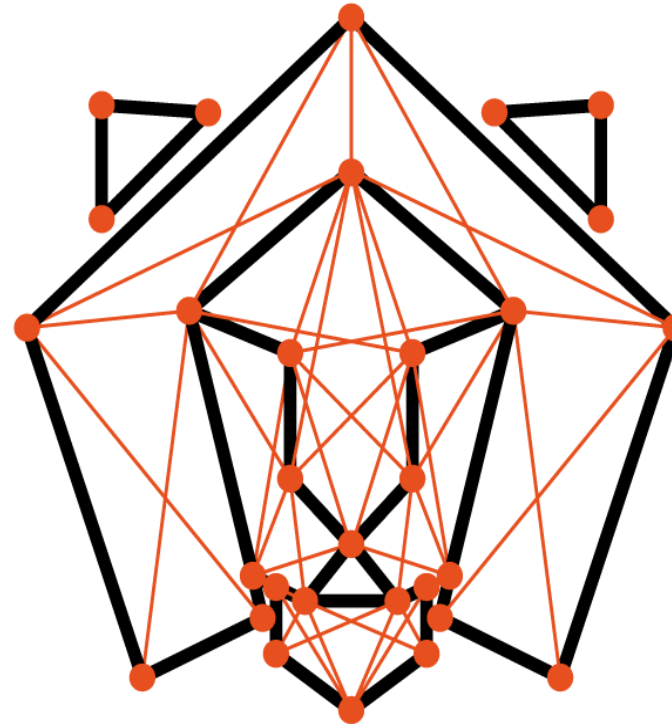
- Cyberstalking
- Non-consensual image sharing

### Modi operandi and nature of the crimes

### Prevention strategies

### Intervention strategies:

- Strategies for preserving digital evidence
- To whom and how to report
- Strategies to overcome victimisation and its impacts



obrigad@

[ricardoestrela@apav.pt](mailto:ricardoestrela@apav.pt)



**ROAR**  
empowering  
victims of  
cybercrime



Co-funded by the  
European Union's Internal  
Security Fund - Police

**APAV**<sup>®</sup>



Apoio à Vítima

**APAV**<sup>®</sup>



Victim Support