CEPOL Research and Science Conference 2022 MRU, Vilnius
Preparing Law Enforcement for the Digital Age

Children on the Internet Law Enforcement Challenges

Nicoleta Apolozan, Chief Superintendent
Andreea Jantea, Police Inspector

General Inspectorate of Romanian Police
Crime Research and Prevention Institute

10th of June 2022

Overview

- Introduction
- Problem
- Goal
- Research outcome
- Objectives
- Methodology
- Implementation
- Results
- Conclusion

Introduction

Technological development + increased access of people of different ages to more and more devices connected to the Internet.

Children are surrounded and have instant access to a myriad of information.

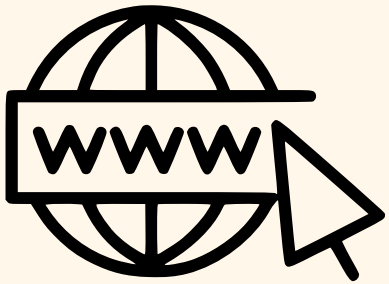
If they are not taught how to handle it, they can easily endanger themselves and others.

Problem

Law enforcement has to tackle cyber offences in which children are involved more often than before.

Law enforcement must be kept up to date to the latest technologies and special juvenile hearing techniques to investigate these types of cases.

Ro Cyberex Project - Improving, cooperating and preventing in the fight against cybercrime, funded by the European Union from the Internal Security Fund – Component for Police Cooperation



The project had 3 components:

- Research
- Police officers training
- Prevention campaign

As members of the implementation team, we were responsible of conducting the research stage.

Goal

Research goal

Identification of the main online risks and vulnerabilities of children aged 10 - 18.
Child pornography
Cyber attacks

Police training activities
Prevention activities

Based on the results of the study
Based on target group's needs

Outcome

Police officers

The results were used to train police officers in Romania which deal with prevention and investigation of cybercrimes

Children

to make them more aware of the conducts that children have on the Internet, the risky situations they are confronted with and with what determines them to commit or become victims of such crimes, according to their age.

Objectives

The First Objective

Identifying the unpleasant situations which children have been confronted with on the internet

The Second Objective

Identifying the main challenges that people dealing with children have faced in handling cyber cases

The Third Objective

Identifying ways in which the investigation and knowledge about risky conduct of children on the internet can be improved

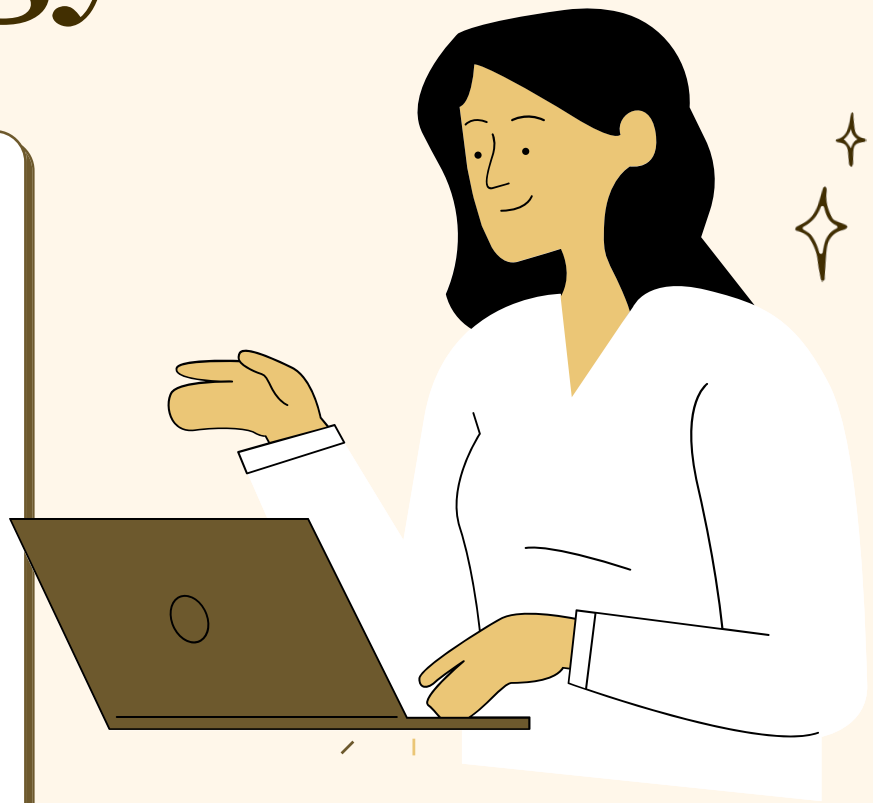
Methodology

Quantitative Method

Online survey among young students between the ages of 10 and 18 on the topic of Internet safety

Qualitative Method

Interviews with key actors involved in preventing and combating cybercrime against children



Implementation

Phase 1

Interviews with police officers from units fighting against organized crime who have investigated cases of cyber attacks involving minor victims and cases of child pornography from ten counties in Romania and Bucharest
16.03 – 30.04.2020

Phase 2

Interviews with teachers of children aged 10 to 18 (leading teachers and computer science teachers)
from ten counties in Romania and Bucharest
18.05 – 19.06.2020

Phase 3

Online survey on a sample of 1445 young students, nationally representative for the population of students aged 10-18 years
16.11 - 03.12.2020

Results

When?

96% of students use the internet every day

76% access the internet from their own mobile device

More than 1/3 of students started using the Internet when they were less than 7 years old

How?

67% of students say that they have mainly found out how to use the internet on their own (40% without any help)

Social networks are at the center of concerns (how to use the internet, account security, perceived risks)

What?

Entertainment (social networks, vlogs, movies / series) take over the agenda of minor internet users

As they get older, young internet users engage in the purchase of goods and services on the Internet, but there is also an increase in the feeling of security towards the online environment.

Results

A fairly high percentage of students said they were victims of various unpleasant situations on the Internet.

Many children noticed that they had the devices they use affected by malicious software (39%) or accidentally came across pornographic materials while browsing the internet (38%).

Results

Their accounts on social networking platforms being broken worry children quite a bit.

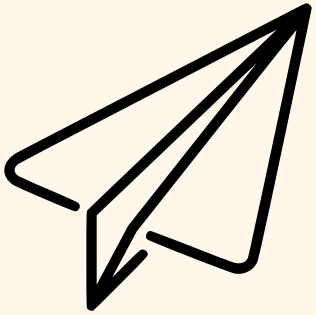
64% of respondents fear that they may be blackmailed into not sharing photos or videos with them or rumors about them.

Children who have previously been victims on the internet are more concerned than others about possible victimization.

Results

In the teachers' opinion, in general, students do not know what the risks on the Internet are, and when they know these risks, they do not take them into account, considering that nothing can happen to them.

In fact, students are not aware of how vulnerable they are to the dangers from the Internet.



Police investigators: Kids are almost safe targets for cyber attackers because they have access to multiple devices, use simple passwords, are easy to manipulate, and don't realize the importance of the data and credentials of the accounts they manage.

The victimization of minors through cyber attacks is usually aimed at obtaining personal data, access to computer systems that they use, so that later criminals can gain material benefits.

Results

In cases of child pornography, the author spends quite a lot of time choosing the perfect victim, using various information that he can access in advance.

After compiling the list of information, criminals can build their speech and approach to the victim so that they can get what they want.

Victims are usually approached progressively

Results

Factors for online victimization:
to young age and its associated naivety, lack of parental supervision, low knowledge of internet use and the risks associated with it

Under the rule of curiosity and social pressures, the risk of victimization of young people increases. Moreover, easy access to digital services is an additional factor

Children may be re-victimized by the same perpetrator several times or may be re-victimized by other persons who had nothing to do with the original event but who came into possession of the data

Conclusion

In order to reduce victimization - a strong partnership is needed between all stakeholders - school, parents, police, NGOs, IT&C actors - to have a unified message, short, direct, reaching both minors and their parents and teachers.

Awareness & prevention campaign for children:

- to be aware of the risks they face on the internet and the consequences of their actions online
- to realize that the actions they take on the internet or through devices have real-life consequences
- to know what precautions they can take to avoid victimization
- the steps they need to take when they become victims
- what are the actions on the internet that are punished by law
- to understand the fact that they can ask for help from the authorities when they faced with such situations

Thank you!