Call: Horizon 2020. **FCT- 07 2016. Human Factor for the Prevention, Investigation, and Mitigation of criminal and terrorist**

Subtopic 2 **New methods to prevent, investigate and mitigate cybercriminal behaviours;**

http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/2318-sec-07-fct-2016-2017.html

Deadline: 25/08/2016

Social Engineering and online scams awareness

Initial Abstract:

The project is aimed to investigate and analyse cybercriminal actions related to social engineering scams and take advantage of this knowledge to prevent and mitigate similar actions in the short and medium terms.
In order to deal with the myriad of possibilities in this field, we will focus on a sub-group made of the most common social engineering scams identified by Interpol – in particular by experts in financial fraud and cybercrime – and by Europol – in The Internet Organised Crime Threat Assessment (IOCTA) report. This sub-group will be split into two different categories depending on the actions that can be carry out from the LEAs' perspective: The category "active response" will tackle the schemes that can be detected without being attacked (such as advance fee fraud), while the category "passive response" will deal with schemes in which the victims are directly contacted by cybercriminals (e.g. romance scam or CEO frauds). As a consequence different tools will be implemented based on scraping techniques for the former and honeypots for the latter. This will be complemented by an open communication channel for the victims, which will allow LEAs to receive updated information about the running campaigns.
The combination of the three approaches will facilitate the detection of suspicious email accounts and servers. Besides, account numbers will be earmarked for further analysis focused on money laundering and the final identification of cybercriminal groups and infrastructures.
As a result, the consortium is expected to address the big problem of social engineering and

- contribute to the better understanding of new models of cybercrime;
- be capable of forecasting future cybercriminal trends;
- further research on new ways of money laundering;
- organise pilot exercises and validations in real scenarios and
- initiate training and dissemination actions devoted to prevent citizens and enterprises from becoming a victim while supporting the daily work of LEAs.

Objectives:

- To address the challenge of preventing, investigating and mitigating the effects of social engineering scams on the Internet from two complementary perspectives:
    - a social/psychological perspective.
    - a technological perspective.
- To identify current and future trends of online social engineering attacks by means of an in-depth analysis and research of the most common approaches, including "traditional" schemes, such as e-mail scams (phishing and spear phishing), telecom fraud, romance scams or advance fee fraud, but also more recent alternatives, such as CEO fraud and virtual kidnapping.
- To detect and track online scams campaigns (e.g. job offers "asking for mules" or possible advance fee fraud in used cars websites or house rentals websites) by means of scraping techniques.
- To create social honeypots for the analysis of scam campaigns coming from diverse sources in different regions with the purpose of helping LEAs to detect new social engineering campaigns in early stages.
- To study, connect and track the different ways in which the collected money is then laundered (e.g. money mules, Bitcoin, online video games platforms, micro-laundering, etc.).
- To generate a dedicated communication channel for the victims to report online scams so as to centralise the information and adopt subsequent actions in different areas.
- To develop an application for LEAs to easily visualise and link multiple events based on big data technologies.
- To organise pilot exercises, training and demonstrations for LEAs.
- To promote cyber security education for avoiding more victims of these types of scams through different means, e.g. talks in schools and business centres, tips on social networks, etc.