European Crime Prevention Award (ECPA)

Annex I – new version 2015

Please complete the template in English in compliance with the ECPA criteria contained in the RoP (Par.2 §3).

General information

1. Please specify your country.

France

2. Is this your country's ECPA entry or an additional project?

Additional project

3. What is the title of the project?

EUPI, a European Union anti-Phishing Initiative

4. Who is responsible for the project? Contact details.

Vincent Hinderer (contact@phishing-initiative.eu)

5. Start date of the project (dd/mm/yyyy)? Is the project still running (Yes/No)? If not, please provide the end date of the project.

01/08/2014, Yes still running

6. Where can we find more information about the project? Please provide links to the project's website or online reports or publications (preferably in English).

https://phishing-initiative.eu

7. Please give a **one page** description of the project (**Max. 600 words)**

Organisation

EU-PI is a 2-years project co-founded by the European Commission's ISEC programme, involving 7 public and private organisations from France, Luxembourg and Netherlands. It leverages a concept developed by Phishing-Initiative, a French not-for-profit association created in 2011 by Microsoft, PayPal Europe and LEXSI.

Offer

EU-PI enables more than 80 millions people from 3 countries including Netherlands, or 1/6th of the EU population, to easily report Web addresses they suspect are part of a phishing attack. Each URL is analysed by algorithms and experienced human analysts, in order to:
- confirm if the URL reported is fraudulent or not and when it has been blocked.
- contribute to have the fraudulent pages quickly blocked in 98% of browsers (more than 2 billions ones including Chrome, Safari, FireFox, Internet Explorer)

Ambitions

We want to raise awareness regarding phishing among email users and provide them a simple tool to verify if a Web page belongs to a phishing attack. This system will also benefit authorities such as law enforcement, brand owners and service providers in order to detect and/or report new phishing URLs infringing their brands or located on they networks.
By reducing the phishing pages lifetime, it limits the number of potential victims, and potentially in the long term deter phishing by forcing the attackers to:

- spend additional resources, thus lowering their potential ROI
- change tactics, raising the (currently low) entry barrier for existing and new phishers
- take additional risks, increasing the probability for them to make mistakes and leave evidence Law Enforcement can leverage,

On the judiciary side, our platform could be used to cluster multiple attacks together, on a multinational level, thus enabling to focus on the most prolific phishing campaigns.

Possible research

European Commission highlights the need for offensive cyber operational activities. EU-PI is one concrete, innovative, proof-of-concept of cybercriminal infrastructure disruption. We believe opportunities will arise for further research through our datasets and experience in phishing detection and prevention:

- study the ROI and possible outcomes of disrupting phishing infrastructure;
- better understand the economics and sociocultural factors of the phishing underground economy (attackers profiling, motivations, learning curve, (dis)incentives, etc).

I. The project shall focus on prevention and/or reduction of everyday crime and fear of crime within the theme.

8. How does the project contribute to crime prevention and/or to the reduction of crime or the fear of crime? (**Max. 150 words**)

The project prevent thousands of internet users from becoming victim of identity theft and online fraud. As soon as we're having fraudulent phishing websites blocked in most main browsers, no more new victims share their personal or banking information to the attackers. those most then relaunch a new campaign, change tactics or target other countries we're not active in yet.

9. How is the project contributing to raising citizens' awareness of crime prevention? (**Max. 150 words**)

The first objective is a tool to allow in an easy way any person to verify if a suspicious address is really fraudulent. If warned, people are less likely to fall for the trick the next time they get these unsolicited requests by email or even in their social networks profiles.

II. The project shall have been evaluated and have achieved most or all of its objectives.

10. What was the reason for setting up the project? What problem(s) did it aim to tackle?

The objective for the project was to fight back phishing in countries where such crime is a big issue, but where not much arrests can be made because of the burden of international judicial cooperation on unitary low-priority, low-prejudice cases, but that impacts millions of people annually.

Another goal was to get an exhaustive view of this kind of cybercrime phenomenon (and its evolution) to identify new risks and trends. We also want to try to correlate attacks happening in multiple countries by possibly same group of attackers.

11. Was the context analysed **before** the project was initiated? How, and by whom? Which data were used? (**Max. 150 words**)

We’ve been active in the anti-phishing field since ten years , which gave us a lot of experience in detecting and tackling fraudulent addresses. We have actually started the concept as a private-private partnership since early 2011.

We noticed there was a need for that kind of resources in local languages, as most phishing databases and initiatives are dedicated to English-speaking countries.

12. What were the objective(s) of the project? Please, if applicable, distinguish between main and secondary objectives. (**Max. 150 words**)

13. Did you build in internal goals to measure the performance of the project? If so, please describe at what stage of the project and how you measured whether the project was moving in the planned direction. (**Max. 150 words**)

The goal is mainly assessed by the visibility of the reporting platform, the number of « good » submissions (i.e. fraudulent websites instead of legitimate or junk reports) and the delay before a fraudulent website is blocked thanks to our actions. We thus added an analytics module to more easily collect statistics on the reports, their status, the phishing characteristics, etc. Another point is the organizations that will make use of the platform. We developed an API to be able to share the threat data with more public and private bodies being able to act upon it.

14. Has there been a <u>process evaluation</u>? Who conducted the evaluation (internally or externally?) and what where the main results? (**max. 300 words) -** *for more information on process evaluation, see EUCPN Toolbox No.3, p.9-10 & part 2 - section 2A*

15. Has there been an <u>outcome or impact evaluation</u>? Who conducted the evaluation (internally or externally?), which data and evaluation method

where used and what were the main results? (**Max. 300 words**) *- for more information on outcome or impact evaluation, see EUCPN Toolbox No.3, p.7-9 & part 2 - section 2A*

III. The project shall, as far as possible, be innovative, involving new methods or new approaches.

16. How is the project innovative in its methods and/or approaches? (**Max. 150 words**)

Back in 2011 when we started, no such initiative. Today, a few more countries try to replicate the initiative. But it does take some effort to be successful. We not only ask people to report URLs, we commit to verify them manually and send all confirmed ones to our partners that rely on us to update their blacklists.

IV. The project shall be based on cooperation between partners, where possible.

18. Which partners or stakeholders were involved in the project and what was their involvement? (**Max. 200 words**)

The project involves 7 partners from France (Lexsi, Signal-SPam, Phishing-Initiative, Luxembourg (SMILE, Minister of Economy) and Holland (Europol, ECSG). Phishing-Initiative itself has other partners such as Microsoft and PayPal. But also the French Interior Ministry or the National INHOPE contact point.

V. The project shall be capable of replication in other Member States.

19. How and by whom is the project funded? (**Max. 150 words**)

The project is co-funded by the European Union until August 2016. It will be then a not for profit association with members, and new grants will be requested. The project can be easily extended to new Member States, with small time and technical investments. Police officers (or private staff such as Lexsi analysts) time must be budgeted, as there’s a need to confirm the reports, communication plans have to be built to promote the platform to the public.

20. What were the costs of the project in terms of finances, material and human resources? (**Max. 150 words**)

The project management is 200 days over 2 years (1/2 FTE). 1 FTE equivalent, in 24/7, is needed to verify the reported URLs. Around 100 man days of development have been spent so far.

21. Has a cost-benefit analysis been carried out? If so, describe the analysis, including how and by whom it was carried out and list the main findings of the analysis. (**Max. 150 words**)

Cost benefit has not yet been finalized

22. Are there adjustments to be made to the project to ensure a successful replication in another Member State?

Translation of the platform in local language, analysts proficient in the local language. If a reporting platform already exists, build upon it and only use some of the features of our platform through API integration for example.

23. How is the project relevant for other Member States? Please explain the European dimension of your project.

Phishing is every Member States' issue. Not a single European country can be seen as immune from this threat. Furthermore, the crime scene evolves constantly, with countries being more or less targeted over time.

Please provide a short general description of the project (abstract for inclusion in the conference booklet – **max. 150 words**).

Phishing Initiative gives to any user the ability to fight against phishing attacks. When reporting us the address of a suspected phishing website, we'll analyse it and have it blocked in most Web browsers. By contributing to this project you decrease the impact of cybercrime and prevent others from becoming victims of online fraud. Learn more about it and help us by reporting suspicious addresses here: https://phishing-initiative.eu