European Crime Prevention Award (ECPA)

Annex I

Approved by the EUCPN Management Board in 2014

Please complete the template in English in compliance with the ECPA criteria contained in the Rules and procedures for awarding and presenting the European Crime Prevention Award (Par.2 §3).

General information

- Please specify your country.

Denmark

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

This is my country´s ECPA entry.

- What is the title of the project?

"Danskernes digitale selvforsvar " – The Danes´ digital self-defense.

- Who is responsible for the project? Contact details.

Mette Raun Fjordside, Director of Strategy & Policy, Danish Consumer Council,
Fiolstræde 17 B, box 2188, DK-1017 Copenhagen K
Tel.: +45 7741 7746, e-mail: mrf@fbr.dk

- 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.

01/04/2017. Yes, the project is still running until 01/04/2017.

- 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://taenk.dk/aktiviteter-og-kampagner/apps-fra-forbrugerraadet-taenk/app-mit-digitale-selvforsvar

https://taenk.dk/om-os/about-us?genvej=footer

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

According to surveys done in 2014, estimated 150.000 Danish citizens had been the victim of it-crime in the form of identity theft, fraud, harassment and/or ransomware within the last 12 months. About half of which was concerned with credit card fraud estimated to a cost of 200 million DKK (approx. 25 million EUR) in 2014.

This evidences that the Danish consumers meet many new kinds of crime online t.ex. phishing, smishing, ransomware or fake websites. In 2016 the Danish Consumer Council www.Taenk.dk, and the Danish foundation 'Tryg Fonden' www.trygfonden.dk, therefore agreed to collaborate with the purpose to investigate 'the consumers´ experience of digital safety – and the most significant challenges'. A report was published in December 2016 stating that the majority of the Danes basically feel safe online, but unsafe when confronted with a number of everyday online scenarios:

- 78 % feel unsecure about the risk of having their credit card information abused online.
- 74 % feel unsecure about the risk of their social security number (CPR) being abused online.
- 70 % do not trust the public sector to keep their personal information safe
- 66 % feels unsecure about the fact that private services sell their data to third party services

The report also stated, that the more knowledge the consumer has on internet-security and possibilities to protect themselves online, the more they do protect themselves. Also the experience of digital safety turned out to rely strongly on the consumer´s amount of knowledge.

That context fostered the idea of an app with the purpose of alerting and guiding the consumers with the help from private and public organizations whose brands are subjects to misuse online.

The Danish Crime Prevention Council (DKR) , the foundation 'TrygFonden', and the Danish Consumer Council took a common interest to collaborate with a twofold objective:

1. To develop and run the app 'My digital self-defense' with the Danish public as target group.
2. To research the field of citizens´ self-protection against digital threats in order to describe a long term effort to support the consumers digital education, safety and security.

The project management was placed with the Danish Consumer Council.

The first version of the free app 'My digital self-defense' was launched on April 7th 2017 on AppStore and GooglePlay and has had more than 50.000 downloads within the first 6 months.

The app alerts it´s app-users of current threats and waves of ongoing cyber-attacks. Messages are pushed by a large group of associated partners, counting both private and public organizations as well as NGO´s, see below. More than 80 alerts have been sent out in the first 6 months, more than half by the associated partners.

Through the app the app-users can also tip the project team on the threats and/or scams they experience and thereby contribute to the knowledge sharing. 1700 tips on digital threats have been received from the app-users since April 7th 2017.

The project team researches the incoming tips, spot waves of attacks and trends, and when patterns arise, new alerts are published to the users through the app and the relevant company, whose brand are being misused is alerted.

> The app also holds sections with information on
>
> 1. <u>What to do, if the damage is done.</u>
>   (Block credit card, reboot system, notify police etc.)
> 2. <u>General characteristics</u> of how to distinguish fraud from trustworthy messages
>   (Analyze links sent by unknown distributors, look for physical addresses of webshops, look for the Danish e-mark on webshops etc.)
> 3. <u>How to improve your personal, digital protection</u> (Secure use of passwords, backup data, keep security software updated, browser settings, and use of VPN etc.)

- **<u>The project shall focus on prevention and/or reduction of everyday crime and fear of crime within the theme.</u>**

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

> The app addresses the risk that consumers often receives information on ongoing attacks/waves of fraud too late or through a variety of media and channels that are not necessarily obliged to the specific task of providing the consumers with information on *what to do to prevent* the further spreading of the threats. The content providers have taken on this challenge, facilitated by the app.
>
> The specific consumer behavior aimed to be influenced is the choice the average consumer makes regarding 'what to click on, and what not to click on'. With estimated 150.000 Danish citizens in 2014 victimized by it-criminals clearly illustrate, that the average Dane click on too many links.
>
> The app is providing a consumer-trustworthy channel for the content providers to alert consumers of fraud attempts in their name. For a consumer it can be a challenge to distinguish, since the attempted frauds appear increasingly professional.

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

> The December 2016 report stated that the Danes basically feel safe online, but unsafe in a number of everyday online scenarios. The report also told that the most important remedy for this is knowledge, including instructions to follow to strengthen online protection.
>
> The app addresses this by supplying various guides as described above and contributes to the general raising of consumers´ awareness of cyber threats through the communication in the app in general. In brief, the app-users are reminded at least twice a week of current threats and now know of one source of knowledge about cybercrime, and it´s easy to find: In their pockets.
>
> The project is fully aware *not* to *create* fear of threats, but it appears that the app users are capable of sorting in the information provided. With an average of 1-2 alerts pushed every week, the recurrent number of app-uninstalls is minimal.

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

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

It was and is a challenge among the actors in and/or adjacent to the it-industry, that there wasn't a current, joint channel for reaching the consumers with alerts of ongoing cyber-attacks. Until the app was launched, it was the responsibility of each individual consumer to seek out trustworthy information in the case of attacks, but from a variety of different actors, aiming on informing only their target groups with their specific messages; Banks, the police, e-trade specialists, the it-security industry and organizations of special interests (Ældresagen, foreningen Ligeværd, Medierådet for børn og unge etc.)

At the projects 4 initial co-creation workshops the participants described the situation as a 'knowledge gap' between the professional actors and the consumers; the industry lacks knowledge of the consumers, and the consumers lack knowledge of it-security.

The project therefore sat out with the objectives to reach 20.000 downloads of the app and at least 4 associated partners by December 31st 2017.
Both objectives were reached in the month of May 2017.

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

In 2016, an extensive study on 'Digital Safety' was carried out by The Danish Consumer Council and the foundation TrygFonden with the aim to investigate if the experience of insecurity among the Danes was increasing due to newer uses of data (Data brooking, and trading) the complexity of digital technologies and the regulatory requirements on Danish citizens to interact digitally with public institutions. A report was published in December 2016 stating a series of challenges in the matter: Inadequate legislation, digital business models not transparent to the consumers, and last but not least to what extent the average Dane experience a lack of digital competences.

A project was then defined specifically to both support communication between the it-security industry and the Danish public and to research the field of citizens´ self-protection against digital threats and to gather and provide up-to-date knowledge on the matter to and with the public.

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

The objectives of the project are:

1. To develop, launch and maintain the app 'My digital self-defense' in the remaining year 2017, including the collection of quantitative and qualitative data about the consumers´ need for knowledge and use of the app.

2. Carry out a co-creation process with the multitude of stakeholders in the field to harvest knowledge and recommendations for the development of a wider, long term effort with the purpose of strengthening the consumers digital education, safety and security.

The process were based on the findings from the project 'Digital Safety' from 2016.

- 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 following internal goals are measured continuously throughout the project:

- The effect of the launch campaign, 'Sikker, når du klikker' in the shape of traffic generated from Facebook-ads and Google-Adwords to both Facebook-group, campaign site, and to download of the app.

- The publicity received by the project in national and local media, and by the content providing partners of the app, listing more than 35 entries in off- an online medias since April 2017, including several national TV-channels and newspapers.

- The progressive amount of app downloads.

- Rate of active app users (allow push-messages from the app in the settings of their phone) and the push open rate of each individual alert sent.

- The progressive amount of tips received from the app users, and the quality hereof.

- Has there been a process evaluation? 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*

The project is subject to weekly internal evaluation in the project team, and monthly evaluations by the steering group. Apart from the download and stakeholder targets, there were 2 focus points:

1. App user performance: Do the average user use it more than once and how many users choose to uninstall the app in periods where the content providers pushed a lot of alerts?
   App statistics showed that more than 67% of the sessions in the app were performed by users *not* interacting with the app for the first time. Only 33 % of the sessions in the app were performed by users interacting with the app for the first time.
   Also we learned, that the app users tended to uninstall the app *less* if we attempted to limit the number of alerts being pushed to the users to a maximum of 3 per week.
   In general the project team was positively surprised by the eagerness of the app users to tip about current threats. Also the general amount of interest generated in the public since launch. The app users have sent in more than 1700 tips through the app since launch, and several institutions have unsolicited helped promote the app.

2. Content provider performance: It is a pivotal point in the app to create and ensure ownership among the content providers to the app. Therefore we have held a series of workshops, provided tutorials for publishing alerts and guidelines on how to formulate alerts in order to catch the attention of the app users.
   The effect has been that the content providers have published more than half the alerts in the app since launch, a total of 36 alerts over a period of 4 months.

- 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*

During first 6 months of the project internal evaluations were conducted, focusing on the following parameters (Per October 1st 2017):

1. The number of app downloads: 50,499 downloads.
2. The number of active app users (Agreed to receive push) 38,032 app users.
3. The number of content providing partners: 13.
4. The number of tips from the app users: 1,700.
5. The number of alerts published in the app: 85.
6. The average number of users opening push messages: 15 %
7. Average session length in the app: 2,19 min.

The app is quantitatively evaluated weekly/monthly using GoogleAnalytics and Pushwoosh statistics.

In 4th Quarter of 2017, a larger qualitative evaluation is planned with the following purposes:

1. To map and generate knowledge on the apps current user-demographics, to generate knowledge and to enable upcoming User Experience improvements to the app.
2. To systematize the projects´ overall knowledge of our target group, adults from the age of 18 yrs, focusing on behavioral change[1]:
   a. To what extent do the app users protect their own digital devices?
      (Maintain software updated to latest version from software provider.)
   b. To what extent are the app users able to detect fraud attempts – and what features are they looking for (Sender´s e-mail-adress, spelling problems etc.)
   c. To what extent do the app users reuse the same password on various online services/social media? And are their passwords strong?
   d. To what extent do the app users backup their data on a regular basis?
   e. To what extent do the app users have a critical understanding of the consequences of their sharing of information in a digital context?

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

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

1. <u>Co-creation with stakeholders</u>: Co-creation with stakeholders from various societal sectors; Private companies, public institutions and NGO´s creating trustworthy value for the app users AND for the stakeholders, since the mutual knowledge sharing also generates learning across the industry as well.
2. <u>Digital technology</u>: Takes advantage of digital technology in itself – and the fact that the majority of the Danes carry a Smartphone.

---

[1] Referring to the analytical framework from the report 'Danskernes it-sikkerhed', March 2017 by the Danish agency for digitization, DeIC and DKCERT.

3. Crowdsourcing: The experiences of app-users as laymen, allowing them to tip and contribute to the buildup of knowledge on cyber risks and threats.

4. A neutral, national communication channel: The neutrality of the app´s warnings and messages distinguishes it from other media channels spreading warnings (or not) about cybercrime. The purpose of the app is not to 'sell' newspapers, subscriptions to software or generate public interest, but only to provide reliable, relevant info on cyber threats from insightful national specialists on the matter.

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

Which partners or stakeholders were involved in the project and what was their involvement? (**Max. 200 words**) *The project shall be based on cooperation between partners, where possible.*

The project has a stakeholder strategy with 3 groups of stakeholders in focus:

1. The initiating and funding partners of the project are The Danish Consumers Council, The Danish Crime Prevention Council and the foundation TrygFonden that function as steering group, working partners and advisors.

2. The app´s content providing partners:

   Private sector:
   Kaspersky Lab, www.kaspersky.dk, private it-security/anti-virus provider.
   Microsoft Denmark, www.microsoft.dk, private software-provider.
   Nets, www.nets.dk, Nordic payment transaction provider.
   PostNord, www.postnord.dk, postal company in DK and S.
   Nordea Denmark, www.nordea.dk, Scandinavian bank.
   The Danske Bank, www.danskebank.dk, Scandinavian bank.
   Dansk Supermarket Group, www.dansksupermarked.dk
   Bilka Supermarket, www.bilka.dk
   Public sector:
   NC3/The Danish police, www.politi.dk
   DKCERT, www.DKCERT.dk, monitors digital security incidents in Denmark.
   SKAT, www.skat.dk, the Danish tax administration.
   NGO´s:
   e-maerket, www.emaerket.dk, the Danish cooperation for secure, transparent online shopping.

   The app´s content providers are the pivotal point of the content creation of the app.

3. 24 organizations across societal functions, both NGO´s private, public organizations, that all participated in one or more of the project´s 4 initial co-creation workshops held from may – august 2017, contributing greatly to the project´s gathering of knowledge.

The project is also endorsed by Finance Denmark (www.finansdanmark.dk), Danish Consumer ombudsmand (www.forbrugerombudsmanden.dk) and the agency for Digitization/Ministry of Finance (www.digst.dk)

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

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

Initially by The Danish Crime Prevention Council, to launch and support the app first 3 months, backed by additional funding from the foundation TrygFonden, to maintain the app

throughout the year 2017 & to further the research into the field of the consumers digital safety and security.

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

Operation and ongoing development of the app has a yearly budget of 3 million DKK (approx. 403.000 EUR)
This is divided into:
- Development and technical operation of the app.
- Employee support of the app.
- The promotion of the app.

- **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)**

A 2014-analysis from the Danish Crime Prevention Council estimated the annual costs of online fraud to 200 million DKK, including credit card fraud.
The relatively small investment this project is, to help consumers distinguish between what´s safe and what´s unsafe and to take the precautions to prevent the real threats supports societal innovation through digitization.
These years many digital consumers have a hard time keeping pace with the ongoing digital switch in general. An example from the app: An app user sent in a tip through the app with a screen dump of an SMS he had received from his local county stating that his garden waste would be collected the following Thursday. He accompanied the screen dump with the comment: "I have never received one of these before. Is it something I should be afraid of?"
If citizens cannot comply in the proper way, societal innovation is unnecessarily slowed down.

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

It is a prerequisite for a successful maintenance of the app´s alerts that the edition takes place in a close working relation with knowing actors in the field, to ensure trustworthiness' of the alerts. The demands to maintain the apps´ alerts and secure they are up-to-date, on a daily, regular basis must not be underestimated.

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

The European Consumer Organization, BEUC, representing consumer organizations in the European countries, has a strong focus on privacy and personal data protection, recognizing that digital information technologies and the emergence of new services, although beneficial to consumers, also represent a major challenge to consumers' fundamental rights to privacy and protection of their personal data. For that reason, it is important to ensure the definition, application and enforcement of strong data protection legislation to the digital environment.

But one thing is legislation – another is the behavioral aspect; how are the consumers best assisted in making the right and safe decisions on their devices?

The basic problem addressed by 'The Danes digital self-defense' is in no way only a Danish problem, but common to all European internet users. The cyber threats are of international origins, spanning the globe, why national versions of the app could potentially benefit all European citizens.

We hope that the app will inspire other institutions within the EU that are working to prevent cybercrime. That is probably also why the European Consumer Organization BEUC chose to publish the news of the app to their readers on April 26th 2017:

http://www.beuc.eu/press-media/news-events/new-app-helps-danish-consumers-protect-themselves-online-fraud

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

Crowdsourcing among consumers and co-creation with various societal actors has turned out to be a viable and relevant approach when it comes to raising awareness and stimulating online behavioral change among the Danes.

In April 2017 the Danish Consumer Council, the foundation TrygFonden and The Danish Crime Prevention Council launched the free app 'My digital self-defense', that has been downloaded by more than 50,000 Danes to their Smartphones.

The app pushes current alerts to the consumers, provided by a wide array of societal actors from public organizations, private companies and NGO´s, when waves of cyber-attacks hit Danish mail-accounts. Also, the app provides guides and advice on digital self-protection.

Last, but not least interesting the app also provides the consumers with a channel to tipping the project on current threats, which the app users have done 1700 times since the launch of the app.