enisa
European Network and Information Security Agency

Homeland Security

Involving Intermediaries in Cyber-security Awareness Raising

Homeland Security

About ENISA

The European Network and Information Security Agency (ENISA) is a centre of network and information security expertise for the EU, its Member States, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU Member States in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU Member States by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu

Follow us on Facebook Twitter LinkedIn Youtube & RSS feeds

Contact details

For contacting ENISA or for general enquiries on **this report** refer to Daria CĂTĂLUI, editor of the report, using the following details:

- E-mail: awareness@enisa.europa.eu
- Internet: http://www.enisa.europa.eu

Acknowledgements

ENISA wishes to thank the speakers and the participants at the 'EU-US event on intermediaries in cybersecurity awareness raising' that took place on 12 June 2012 in Brussels. Also the ENISA project team (Giorgos Dimitriou, Manel Medina, Isabella Santa), DG CONNECT member(Ann-Sofie Ronnlund) and US HQ DHS member(Erin Meehan).

Contents

1 Executive summary

This document summarises the work carried out to involve intermediaries in cyber-security awareness raising by the European Commission and the European Network and Information Security Agency in cooperation with the United States Department of Homeland Security.[1]

The approach was to use an event to bring intermediaries together in order to capitalise on existing approaches during the European Cyber-security Month. Intermediaries were asked to contribute to awareness raising (AR) and the dissemination effort on topics pertaining to information security. For the purposes of this document, intermediaries (or third parties) are people, organisations or bodies that are already involved in cyber-security.[2]

The emphasis was placed on mechanisms for cross-border cooperation as well as for public–private cooperation and information exchange.

Discussion involving speakers, panellists and participants was triggered on thematic topics such as 'The role of intermediaries and the benefits for them to get involved' and 'The role of cyber-security education and workforce development'.

Part 3 of this report presents the **conclusions,** broken down into action points for the medium term, with the main message that 'International cooperation is key in awareness raising.'

[1] *More information is available on ENISA's website: http://www.enisa.europa.eu/activities/cert/security-month/events [accessed October 2012]*

[2] *More information on this topic is available in the following ENISA report: http://www.enisa.europa.eu/activities/cert/security-month/deliverables/2011/europeansecuritymonth [accessed October 2012]*

2 The event

On 12 June 2012, 45 EU and US representatives from the private and public sectors gathered in Brussels to discuss the topic of 'Involving Intermediaries in Cyber-Security Awareness Raising'. The agenda of the event was balanced between presentations from public bodies with experience in raising network and information security (NIS) awareness and private bodies with initiatives or public–private partnerships (PPPs) in the field. The keynote from the European Commission was followed by two sessions and three panels on relevant topics, plus Q&As.

In his keynote speech, **Paul Timmers** (Director, DG CONNECT) underlined that the event should be seen in the context of preparing for a joint EU–US cyber-security awareness raising month in 2014. The involvement of intermediaries is key for reaching out to end-users like citizens or SMEs, with information on how to protect themselves against risks, how to take corrective measures should they face malware or inappropriate behaviour online, how to clean their devices, and also how to have back-ups prepared to allow for quick restoration of normal daily life and business in case of incidents. **A challenge was set by Mr Timmers to find ways to make hacking look 'uncool'.** He also underlined the importance of creating appropriate mechanisms for cross-border cooperation, as well as for public–private cooperation and information exchange.

Session I: The role of intermediaries and the benefits to them of getting involved

Invited experts presented several best practices on the role of intermediaries and the benefits to them of getting involved.[3] During this session the floor was given to the US National Cyber Security Alliance (NCSA) Board Vice-Chairperson Ms Jacqueline Beauchere (Microsoft)[4] in order to present details about the extended public–private partnership that hosted its 9th cyber-security awareness month in the US in October 2012.[5] The US experience was followed by United Kingdom and Luxembourg presentations that provided more details on what the European Security week pilots of 2012[6] would be promoting.

---

[3] *See Annex II*

[4] *Presentation by Jacqueline Beauchere: http://www.enisa.europa.eu/activities/cert/security-month/eu-u.s.-event-on-intermediaries-in-cybersecurity-awareness-raising/eu-us-event-on-intermediaries-in-cyber-security-awareness-raising [accessed September 2012]*

[5] *http://www.dhs.gov/stopthinkconnect [accessed October 2012]*

[6] *http://www.enisa.europa.eu/activities/cert/security-month/pilots [accessed September 2012]*

The panel discussion (moderated by ENISA) with the participation of the speakers and DIGITALEUROPE,[7] touched upon dependencies that would need to be taken into account when implementing awareness raising (AR) and projects like European cyber-security month.[8] Panellists stated that in an interrelated world of information technology, it is important to measure and document efficiency – a topic that raised interventions from the speakers and audience alike.

Session II: The role of cyber-security education and workforce development

The invited experts discussed the role of cyber-security education and workforce development.[9] Presentations from Spain and Slovenia detailed the importance of using new technology channels, implementing a **'follow the trend and the digital citizen' communication strategy.**

The panel discussion (moderated by ISMS Forum Spain) touched on the added value of initiatives and projects such as the EU KIDS online research network[10] for solid research that would feed sound decisions, CERT-EU[11] and the e-Learning Europa portal,[12] which stands for learning from best practices.

Best practices for PPPs and future actions

Best practices gained from the experience of speakers and participants in building awareness-raising public–private partnerships (PPPs) and identifying messaging opportunities included the following:

- Make companies aware that awareness raising will help in creating **business opportunities** and make money, through a favourable brand image. Building consensus among decision-makers that a cyber-security awareness project is important and worthy of funding in a long-term, sustainable manner (both private and public sources) is perhaps the most time-consuming and difficult task for a PPP. This

[7] http://www.digitaleurope.org/ *[accessed October 2012]*

[8] *The first, pilot European Security Month took place in October 2012, promoting cyber security to citizens.* http://www.enisa.europa.eu/media/news-items/european-cyber-security-month-in-all-23-languages *[accessed September 2012]*

[9] *See Annex II*

[10] http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/Home.aspx *[accessed July 2012]*

[11] http://cert.europa.eu/cert/filteredition/en/CERT-LatestNews.html *[accessed July 2012]*

[12] http://www.elearningeuropa.info/ *[accessed July 2012]*

can be facilitated by Ministers acting as patrons, and obtaining appropriate CEO support and funding to the project.

- Cyber-security is a matter of cultural challenge and **behavioural change**. Getting people to act is the primary challenge; usually they will act only when they have been exposed to security problems, or somebody they know has been. Citizens are aware to some extent of the means for technical protection, but not of how they are applied in their individual case. They are not interested in technical details but just want protection to work effectively in the background.
- It is important **not to scare the users** but to encourage them to get online and get safe at the same time. Do not start off by giving them too much technical information. This is about communication and therefore messages have to be appropriate for the target audiences.
- Young users can be good promoters of a message and through educating them we can often reach the parents as well. The earlier the **education** starts, the stronger the effects on users' Internet behaviour.
- **Media** should be considered as a main channel to get key messages out and we should take into account the popularity of social media networks. But traditional media (such as TV) play an important role in creating a momentum for change and in reaching users who are less familiar with the Internet.
- We should improve measurement of the impact and success of the AR (key performance indicators, KPIs). The challenge is to go from measuring activities to **measuring outcomes**. Traditional marketing metrics are of limited value when applied to AR; it is advisable instead to look for ways to link metrics to corporate social responsibility (CSR) related activities.
- **Stakeholders** should be involved in all stages of the process and become part of it, by being empowered. Encourage using multipliers or 'train the trainer'-type programmes to reach target groups.
- **Multilingualism** is an opportunity to exploit through international cooperation, through *actionable* messages.

Homeland Security

3 Conclusions

In the wrap-up panel (moderated by DG CONNECT), and with the participation of EuroISPA and TechAmerica Europe, ideas discussed during the day were elaborated in more detail and were taken as action points for the medium term.[13] The organisers and participants agreed to work on the following concrete steps on 'Involving Intermediaries in Cyber-security Awareness Raising':

- Creation of PPPs in the Member States and to exchange and disseminate **awareness** material jointly at EU level;
- Production of guidelines for the creation of those PPPs, as well as recommendations for their sustainable funding (possibly through a working group or task force to develop recommendations and joint policies);
- Creation of a **repository** of references to awareness campaigns launched in the EU and USA, that could be a well-known source of information for stakeholders interested in launching new campaigns. This repository could also store some material produced for those campaigns and made publicly available by the authors for other intermediaries;
- Collection of available tools to promote the cooperation between PPPs and Member States;
- Encourage ENISA to support the implementation of those recommendations.[14]

The model for awareness raising in the EU–US Working Group has the potential to show the way for broader cooperation on these issues internationally. And it will put the EU–US cooperation on cyber-security on an even stronger footing.

To conclude with a broader message of the meeting: **'International cooperation is key in awareness raising.'**

[13] *The work will continue*

[14] *The recommendations will be tackled in future working groups and projects.*

4 Annex I: References

- http://www.enisa.europa.eu/activities/cert/security-month/eu-u.s.-event-on-intermediaries-in-cybersecurity-awareness-raising/eu-us-event-on-intermediaries-in-cyber-security-awareness-raising accessed September 2012;
- http://www.enisa.europa.eu/activities/cert/security-month/pilots accessed September 2012;
- http://www.enisa.europa.eu/media/news-items/european-cyber-security-month-in-all-23-languages accessed September 2012;
- http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/Home.aspx accessed July 2012;
- http://cert.europa.eu/cert/filteredition/en/CERT-LatestNews.html accessed July 2012;
- http://www.elearningeuropa.info/ accessed July 2012;
- http://www.digitaleurope.org/ accessed October 2012;
- http://www.dhs.gov/stopthinkconnect accessed October 2012;
- http://www.enisa.europa.eu/activities/cert/security-month/events accessed October 2012 ;
- http://www.enisa.europa.eu/activities/cert/security-month/deliverables/2011/europeansecuritymonth accessed October 2012.

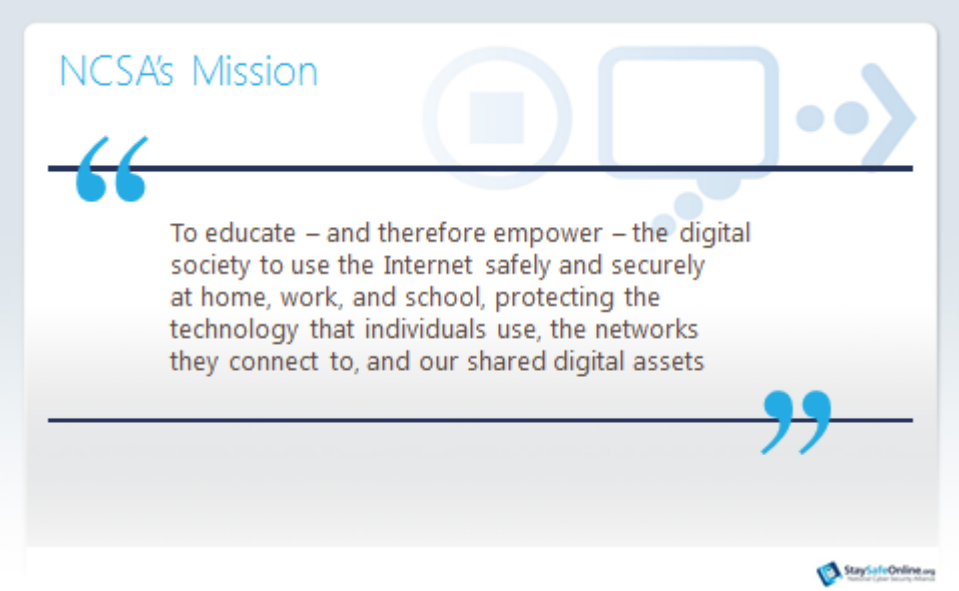
Homeland Security

5 Annex II: Initiatives mentioned in report

US National Cyber Security Alliance example of PPP in action

www.staysafeonline.org

Stop.Think.Connect initiative www.stopthinkconnect.org



Luxembourg example of collaborative approach in AR

https://www.bee-secure.lu/

http://www.cases.public.lu/fr/index.html

Outlook

- Reduce the digital divide in security
- Reduce complexity of methodologies
- Reduce solutions' costs

CASES

Include lessons learnt from BEE-SECURE into the behavioural, organisational and technological layers of experise

Produce less discriminatory methodologies

Provide risk assessment platform for all through a dynamic risk assessment, including metrics from CERT

Foster product and services

Homeland Security

PPP from UK: ‘Get safe online’

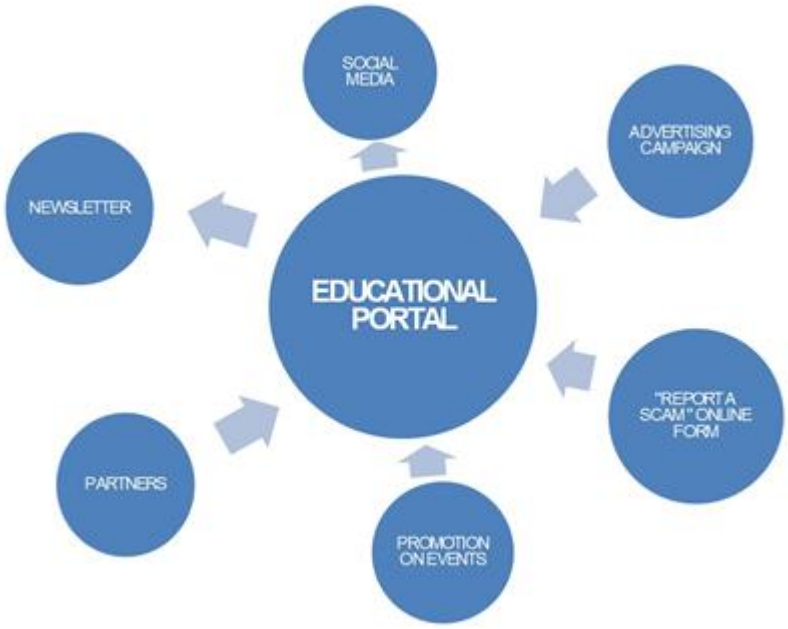
Spain AR

www.osi.es

http://www.ismsforum.es/

www.Protegetuinformacion.com

Slovenian AR campaign: http://www.varninainternetu.si



P.O. Box 1309, 71001 Heraklion, Greece
www.enisa.europa.eu