Cyber Security Awareness Rising: Rules for turning work-based learning material into private-sector engagement

A part of the ISALIP Seeding Materials

Co-funded by the European Union

Co-funded by the European Union

ISALIP

This document was produced as part of the Erasmus+ project.

"Information Security Awareness, Literacy and Privacy – ISALIP"

Project Partners:

Betriebswirtschaftliches Forschungszentrum für Fragen der mittelständischen Wirtschaft e. V. an der Universität Bayreuth
(Business Research Center for Small and Medium-Sized Enterprises e. V. at the University of Bayreuth),
Germany
https://www.bfm-bayreuth.de

eCampus-Lausitz e. V.,
Germany
https://www.ecampus-lausitz.de

MYKOLO ROMERIO UNIVERSITETAS,
Lithuania
https://www.mruni.eu

This document was produced as part of the ERASMUS+ project "Information Security Awareness, Literacy and Privacy – ISALIP", Project ID: 2021-2-DE02-KA210-ADU-000051308

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

1 Introduction

This output document was developed in the ERASMUS+ project ISALIP (“Information Security Awareness, Literacy and Privacy”) as part of the ISALIP Seeding Materials and is intended to give a practical tool for SME in the field of information security.

As a result of a lot of different project activities – like the development of the ISALIP Seeding Materials, a Lead User Workshop or the Piloting of the Seeding Materials - it was measured, that employees with little connection to cyber security find it difficult to access the materials developed and the sometimes very complex information on cyber security in general.

The project team therefore decided, to formulate rules for the creation of information material that would make it easier for employees to access and to adapt the project outputs to the target group of European citizens. The project group developed 20 rules for converting professional learning material into private use material to answer the question: "What are best practices for communicating these topics to citizens?"

In this way the ISALIP-project makes an effective communication of cyber security topics to citizens available, which is very important to ensure that they understand and apply the best practices.

2 Cyber Security Awareness Rising: Rules for turning work-based learning material into private-sector engagement

1. Use Plain Language:

Avoid technical jargon and use plain, understandable language that the average citizen can grasp easily.

2. Engaging Multimedia:

Create engaging and visually appealing materials, such as videos, infographics, and interactive websites, to make the information more accessible and memorable.

3. Storytelling:

Share real-world stories and examples of cyber incidents and their consequences to illustrate the importance of cybersecurity.

4. Relatable Scenarios:

Use relatable scenarios that citizens may encounter in their daily lives, such as online shopping, social media, and email, to demonstrate cybersecurity principles.

5. Interactive Workshops and Webinars:

Conduct workshops or webinars where participants can actively engage with the content, ask questions, and practice cybersecurity skills.

6. Gamification:

Develop cybersecurity games or quizzes that make learning fun while reinforcing key concepts.

7. Personalization:

Tailor communication to specific demographics or age groups. For example, content for children and seniors may need to be different.

8. Frequent Reminders:

Use multiple channels for communication and provide regular reminders about cybersecurity best practices to reinforce the message.

9. Promote Positive Behaviour:

Focus on positive messages that highlight the benefits of practicing good cybersecurity, such as protecting personal information and online safety.

10. Visual Aids:

Utilize visuals and graphics to illustrate concepts, such as the importance of strong passwords, safe browsing, and recognizing phishing emails.

11. Social Media Campaigns:

Use social media platforms to share cybersecurity tips, news, and updates, reaching a wide audience.

12. Collaboration with Trusted Sources:

Partner with trusted organizations, government agencies, or cybersecurity experts to lend credibility to your messaging.

13. Feedback Mechanism:

Establish a way for citizens to ask questions or seek clarification on cybersecurity topics and provide timely responses.

14. Local Community Engagement:

Engage with local communities through in-person events, neighbourhood meetings, and community centres to directly address their concerns.

15. Accessibility:

Ensure that all communication materials are accessible to individuals with disabilities, considering features like screen readers and captioning for videos.

16. Multi-Language Support:

Provide information in multiple languages to reach a diverse audience.

17. Continual Updates:

Stay informed about emerging threats and update communication materials and strategies accordingly.

18. User-Friendly Resources:

Make resources easily downloadable and shareable so that citizens can refer to them at their convenience.

19. Incentives and Recognition:

Consider offering incentives or recognition for citizens who actively participate in and promote good cybersecurity practices.

20. Measurable Goals:

Set clear objectives and key performance indicators (KPIs) to measure the effectiveness of your cybersecurity awareness efforts.

We thank the co-authors from:

BF/M-Bayreuth

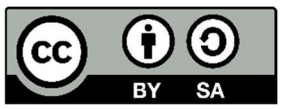
eCampus-Lausitz

Mykolas Romeris University

Information Security Awareness, Literacy and Privacy - ISALIP

Co-funded by the European Union

Co-funded by
the European Union



ISALIP