Development and Certification of Skills for European Educators Focused on Safe ICT and Cyber Threat Prevention

RenataDanieliene,EugenijusTelesius, Information Technologies Institute – Lithuania

Abstract

One of the general competences of the employees is the ability to safely use computers and the Internet. The Lithuanian Computer Society (LIKS) as ECDL Foundation's national operator has launched the Endorsed Partner Programme e-Guardian in 2009. The main purpose of the e-Guardian programme is directly help getting the needed knowledge to protect children from dangers on virtual world together with the formal final ECDL Foundation approved certification. This is especially important for employees/trainers of educational institutions. Therefore five partners from Lithuania, Latvia, Germany and Switzerland in 2010 started with the new Leonardo da Vinci project seeking to help the European educators to acquire more knowledge about the Internet threats and measures how to pass these threats. This paper describes e-GUARDIAN project results, certification and skills measurement tools.

Keywords: Computer literacy, safe ICT, e-Guardianprogramme, educator skills, ECDL certification

1. Introduction

Information technologies are getting increasingly prevalent in our daily life. The Internet is used at home, at work and at school. There you can find lots of useful information, improve your knowledge, instantly learn the news, enjoy your leisure, etc. However, there are different dangers related to the Internet, such as cybercrime, fraud, viruses, etc.

Regardless of age, each computer user must be aware of the Internet opportunities and threats. To prevent distress, computer safety at home should be addressed by the parents, whereas IT professionals should tackle computer safety at work or at educational institution. That is the intended purpose of the ECDL Foundation Endorsed Partner Programme e-Guardian (www.ecdl.lt/eguardian-v1-en).

e-Guardian v.1 is a higher-level programme designed for those who want to protect children against potential Internet dangers and to safeguard their own computers from unwanted access. This programme is recommended for parents and IT administrators at primary or higher schools.

Recently ECDL Foundation has developed Module 12 - IT Security. This new security-specific module is intended for computer users at home or at work (rather than for IT professionals) and it enable those who spend a considerable amount of time online or using a computer during the course of their work or at home to protect both themselves and their data from a range of fraudulent/malicious activities.Some computer users lack basic knowledge in computer security (IT Security module), however it is not necessary to have in-depth knowledge of the hardware and software tools for Internet security administration (e-Guardian v.1).

Teachers, in particular, should know about the potential threats on the Internet and the consequences that may arise out of unsafe Internet use. They should know how to manage digital data in a safe manner and how to recover lost data. They should focus on the safe use of the Internet resources, learn about safety and privacy on the Internet and they should be able to use e-services safely.

One of the general competences of the employees is the ability to safely use computers and the Internet (i2010 Strategy).This is especially important for educational institutions employees/trainers –they transfer the knowledge and skills to their students. Under the Safer Internet Programme (2009-2013, Decision No 1351/2008/EC of the European Parliament), that continues the 2005-2008 program activities, it is expected among other activities to continue to inform the public about Internet threats and to teach to avoid them. The awareness actions and programmes addressing a range of categories of illegal, unwanted and harmful content are mentioned.

2. e-GUARDIAN project

It was appropriate time to take the project proposal action, because there is a lack of knowledge on Internet safety and there are no relevant Internet safety training standards nor syllabuses in national education systems.For this purpose four organizations from different countries started withTransfer of Innovation project e-GUARDIAN (Development and certification of skills for European Educators focused on Safe ICT and Cyber threat prevention). Project No. : LLP–LdV–TOI–2010–LT–0071. Project started at 01.11.2010 and duration is 18 months. The Transfer of Innovation project e-GUARDIAN is funded with the support from the European Commission by Leonardo da Vinci programme, which is a part of the Lifelong Learning Programme.

The project goal is to develop a complex training product (‘bundle”)for educators, focused on safe ICT and cyber threat prevention.

The project started with the modification of e-Guardian Syllabus version 1.0 to the e-GUARDIAN SyllabusVersion 2.0. The new version is dedicated for the certification of European teachers’ knowledge on safer Internet. This programme is adapted to pedagogues of educational institutions, who seek to safely use their computers and the Internet, to teach their students, and to protect them from the Internet threats.

e-GUARDIANprogramme indicates the aim of training, required knowledge, and skills for people, seeking the certification. E-GUARDIAN is a professional certification programme for educators localized for use in Lithuania, Latvia and Germany according to the socio-cultural environments.

e-GUARDIAN project partners:

- Project coordinator - Association “Langas į ateitį” (Lithuania), www.langasiateiti.lt
- Public Institution Information Technologies Institute (Lithuania), www.ecdl.lt
- The Latvian Information and Communications Technology Association (Latvia), www.likta.lv
- Bremen University (Germany), www.uni-bremen.de
- Association APTES (Switzerland) as a silent partner, www.zen3.net/aptes

Project site: www.langasiateiti.lt/eguardian

3. e-GUARDIAN project results

The project partners have combined both their experience and the training products. The project coordinator had internet safety e-course (in Lithuanian) which above 3000 people studied in 2008-2009. Information Technologies Institute had e-Guardian certification programme version 1.0 and knowledge assessment tests (in English) that were approved by the ECDL Foundation. Latvian colleagueshad online IT skills measuring tool (Barometer) which could be adapted as an on-line testing tool to assess starting information security (e-Guardian) skills. It allows examine competence level and receive an automated evaluation with indications for necessary improvements.

Partner’s initial products (e-Guardian test version 1.0, e-course and online skills measuring Barometer) were combined and adapted for this project with additional leading methodology materials into a complete e-GUARDIAN training and certification programme.

Project deliverables:

- Syllabus
- Methodology guide
- Training programme
- E-course
- Student's guide
- Barometer tests (http://dev.ecdl.lt/project/eguardtest/)
- Certification tests

3.1 e-GUARDIAN Syllabus Version 2.0

Category	Ref.	Task Item
1.Basic knowledge on e-safety	1.1.	Understand the differences of information contents (open, private, business, etc.).
	1.2.	Be aware of privacy protection legal act (be aware of the responsibility for own actions on the Internet: do not publish the information without permission, be responsible by writing comments, do not download music, movies, etc.).
	1.3.	Know about equity between opportunities & risks of web2.
	1.4.	Understand the notion of identity.
	1.5.	Be aware of different identity for authorization theft methods (skimming, pretexting, shoulder surfing, information diving).
	1.6.	Know about social engineering and it’s methods.
	1.7.	Be aware of cyber crime, online predators, financial scams, harm and who to contact if discovered illegal data.
	1.8.	Understand computer infection threats (viruses, Trojan horses, spyware, dishonest adware, etc.). Know when and how malicious software can get into computer system.
	1.9.	Know about organizational security: school security, usage of school web pages, content publishing, access, etc.
	1.10.	Know about netiquette and other basic codes of conducts in the cyberspace (RFC 1855).

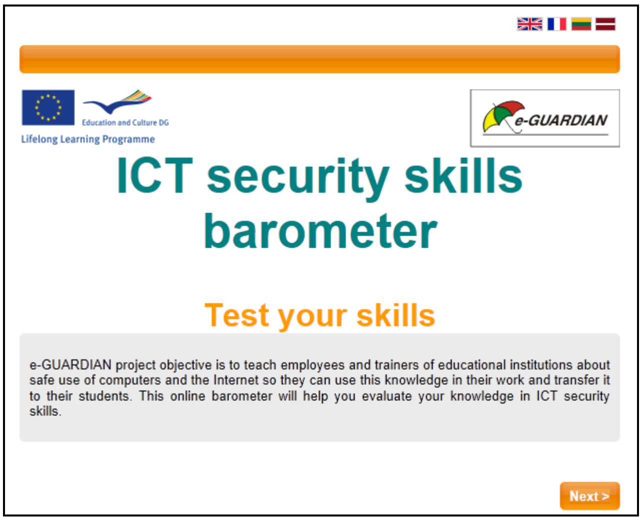
Category	Ref.	Task Item
		cyberspace (RFC 1855).
	1.11.	Understand what is Online Safety 3.0 and why digital citizenship is protective.
2. Privacy and data management	2.1	Distinguish between data and information.
	2.2	Understand the opportunities and risks of digital data management from fully collaborative to full privacy.
	2.3	Know about multi-layer password, changing and keeping password policies.
	2.4	Know about safe computer login methods.
	2.5	Know multiple user accounts on various digital environments. Understand the meaning and importance of access rights (what a personal user account is and how data of different users is separated).
	2.6	Be aware of data encryption, decryption and password protected files.
	2.7	Understand what intellectual property on Internet is.
	2.8	Understand the benefits and purpose of data backups and be able to restore lost data.
3. Security tools and network security	3.1.	Know computer network types (local area network (LAN), wide area network (WAN), virtual private network (VPN)) and why protection is needed.
	3.2.	Know different network connection methods (Cable, Wireless, Mobile networks).
	3.3.	Be able to use wireless network safe and know how to connect to a protected/unprotected wireless network.
	3.4.	Sharing and accessing resources over network (Files, Printer, Desktop).
	3.5.	Understand safety means of computer networks (Firewall, Antivirus, Anti-spyware, Spam blocker Password protection, Connection encryption – wireless).
	3.6.	Be able to use standard OS integrated protection tools.

Category	Ref.	Task Item
	3.7.	Be able to turn on / off and adjust protection level in standard security means that are integrated in the operating system (Firewall, Protection tools, etc.). Distinguish different modes of antivirus protection (active, passive).
	3.8.	Know what has to be done and in what order, if you suspect that computer system is infected. Distinguish infected files deletion, quarantining and curing.
	3.9.	Know how to follow, download and use updates for your operating system, software and importance of antivirus definition files. Understand the benefits of these updates.
	3.10.	Informal and formal periodic external checkup.
4. Minors and newcomers on the net	4.1	Understand the impact of communication with minors and new users about safety in IT World.
	4.2	Understand the purpose of monitoring, filtering and controlling tools for safer internet use of minors.
	4.3	Be aware of different ways to educate, monitor and control usage of social networking and other web sites.
	4.4	Be able to develop policies and apply methods for children's use of the computer and the Internet (depending on age and socio-cultural situation).
	4.5	Understanding advantages and limitations with protection software.
5. Social networks and safe usage of the Internet	5.1	Know how to start and finish safe browsing session (https, lock icon, always logout and close the browser window). Know consequences of unsafe browsing.
	5.2	Know about advantages, disadvantages and dangers of Internet cookies and ActiveX control. Know about tools that ensure safety when browsing the Internet.
	5.3	Be able to manage: temporary Internet files, browser history, passwords, cookies and autocomplete data.
	5.4	Be able to safely connect to e-Services and secure environments– connecting and using, recover lost passwords.
	5.5	Know when and in which cases personal information can be published on the Internet (i.e. status publishing about leaving

Category	Ref.	Task Item
		home).
	5.6	Know who you should contact if you discovered inappropriate information about you or your related digital identities.
	5.7	Understand that it is necessary to exercise critical thinking about content and identities on the internet. (i.e. blogs, Wikipedia, social networks, forums, etc.).
	5.8	Understand 'threats of inappropriate content for different groups of people (duality of personality, psychological harm, racism, religious sect, alluring to buy something or disclose your information, information about drugs, violence and so on).
	5.9	Understand what an online social network is, what are opportunities and risks of social network. Age groups of using social networks. Options and parameters for information disclosure. Understand what is the fascination to disclose private information on the internet.
	5.10	Know different social network types (Friendship-driven and Interest-driven) and be able to use them harmless and safe (appropriate account privacy settings).
	5.11	Know what type of information recommended to be published on social network, be responsible for published content, and know impacts.
	5.12	Understand that online socializing reflects "real life".
	5.13	Be able to send/receive e-mail securely: know how to reject email from specific email addresses. Know how to treat email messages from unknown senders, classified as spam and email messages infected with malware. Know about scam, hoax, chain letters.
	5.14	Be aware of safe instant messaging. Understand confidentiality while using IM like: file sharing, non-disclosure of important information, etc.
	5.15	Understand threats of online communication: virtual dating, bullying, commenting.
	5.16	Understand dependency and addiction to the Internet.

3.2 ICT security skills barometer and e-GUARDIAN tests

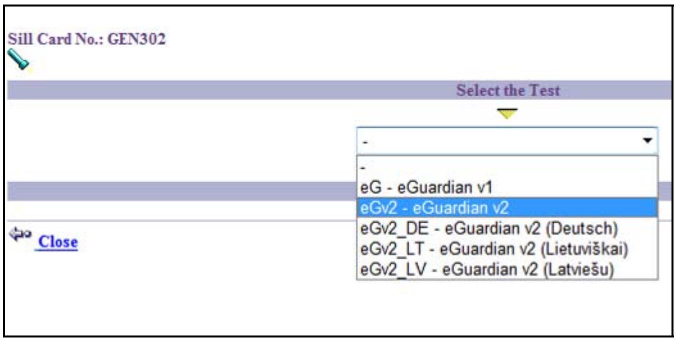
To ensure product quality and the ability to adapt it to various EU countries with different cultures, the product was localized and tested through a pilot training in all partner countries. There werepilot testsdone with Lithuanian, Latvian and Germany teachers. Teachers evaluated own knowledge level by using Online ICT security skills barometer. Then theyhavestarted with distance learning courses andfinally had possibility to make certification tests.



e-GUARDIAN project objective is to teach employees and trainers of educational institutions about safe use of computers and the Internet so they can use this knowledge in their work and transfer it to their students. This online barometer will help you evaluate your knowledge in ICT security skills.

Figure 1: ICT security skills barometer

In order to pass the e-GUARDIAN certification test, at least 80% of the answers to 30 questions must be correct. The questions are selected from the Automated Question and Test Base using a special randomization algorithm.



Sill Card No.: GEN302

Select the Test
-
-
eG - eGuardian v1
eGv2 - eGuardian v2
eGv2_DE - eGuardian v2 (Deutsch)
eGv2_LT - eGuardian v2 (Lietuviškai)
eGv2_LV - eGuardian v2 (Latviešu)
Close

Figure 2: e-GUARDIAN testing system

All the training and testing material was translated into e-GUARDIAN partners' languages – Latvian, German, French, Lithuanian and English. This certification test is expected to be endorsed by ECDL Foundation and implemented in the partner countries.

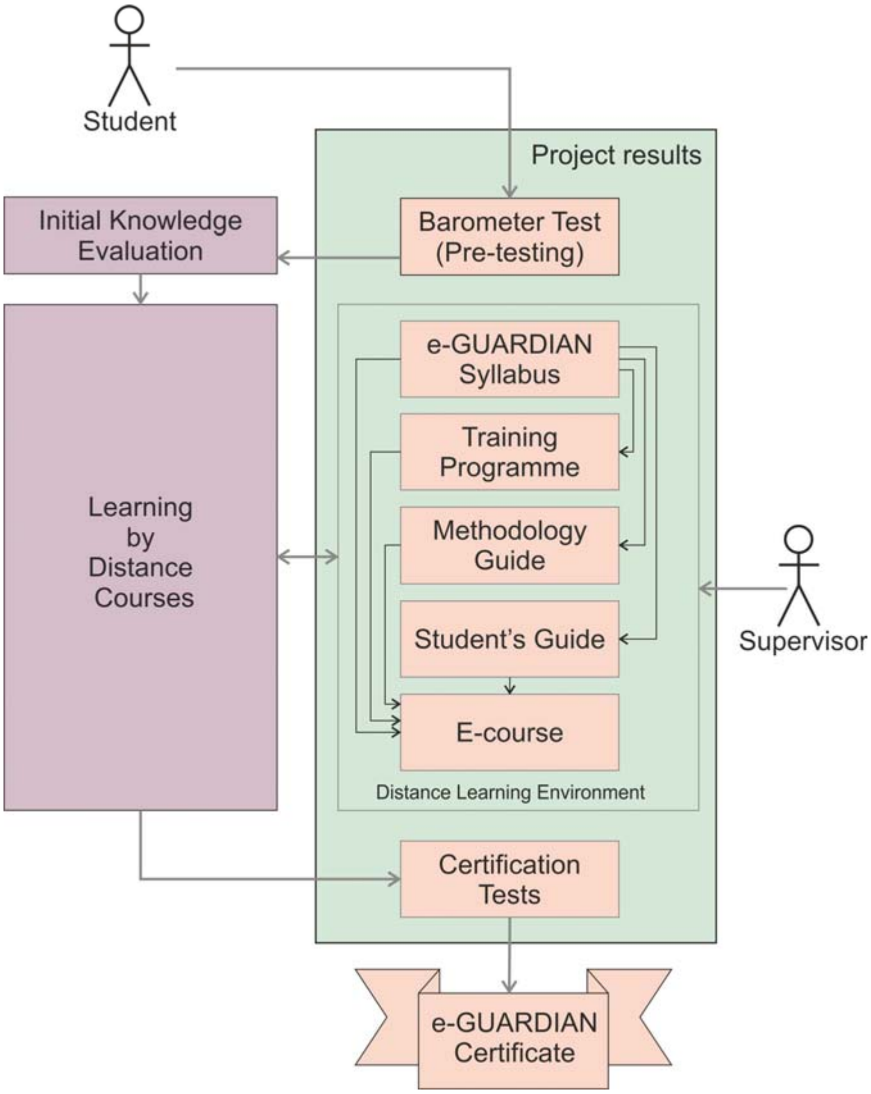


Figure 3: e-GUARDIAN training and certification process

4. Conclusions

e-GUARDIANprogramme could be easily adapted to English-speaking countries of the European Union at the same time enabling it to localize to other non-English countries and use for their educators training and certification.

It is expected the e-GUARDIAN product will give to educational institutions safer internet usage learning tool that could be included in their curriculums and used as learning standard in EU countries education systems. e-GUARDIAN isa modern product based on international standards and can be implemented in every country in the world. e-GUARDIANas a certification will ideally fill the existing market gap. European educators together with parents will create perfect lobbying group in order to make e-GUARDIAN certification more and more compulsory.

This project has been funded with the support from the European Commission. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.