SARA **L**aw **R**esearch **C**enter
International **J**ournal of **L**egal and **S**ocial **O**rder, https://www.ccdsara.ro/ijlso
ISSN 2821 – 4161 (Online), ISSN 2810-4188 (Print), ISSN-L 2810-4188
N^{o}. 1 (2023), pp. 571-579

PREVENTIVE ONLINE SAFETY EDUCATION FOR TEENAGERS

S.N. VOICU, I. CRĂCIUN

Received 15.11.2023; accepted 11.12.2023
https://doi.org/10.55516/ijlso.v3i1.165

Simona-Nicoleta VOICU
Institutul Național de Cercetare-Dezvoltare în Informatică – ICI București/
National Institute for Research and Development in Informatics - ICI Bucharest
E-mail: simona.voicu@ici.ro
ORCID ID: https://orcid.org/0009-0009-5691-0023

Ioan CRĂCIUN
Institutul Național de Cercetare-Dezvoltare în Informatică – ICI București/
National Institute for Research and Development in Informatics - ICI Bucharest
E-mail: ioan.craciun@ici.ro
ORCID ID: https://orcid.org/0000-0001-5630-6306

Abstract

The rapid evolution of digital technology has brought both opportunities and risks, particularly for adolescents navigating the online world. This paper delves into the significance of preventive online safety education tailored for teenagers. It explores the current landscape of online threats, encompassing cyberbullying, privacy breaches, and exposure to inappropriate content, among others. Additionally, it evaluates existing educational approaches, emphasizing the need for a proactive, multifaceted strategy to equip teenagers with the necessary skills and knowledge to safely navigate the digital sphere. The proposed preventive education model integrates elements of digital literacy, critical thinking, and responsible online behavior. Furthermore, it discusses potential challenges in implementing such programs and suggests collaborative efforts among educators, parents, and policymakers to ensure comprehensive online safety education for teenagers, fostering a safer and more secure digital environment for the next generation.

Keywords: *preventive education, teenagers, cyber security, online education, POSE.*

INTRODUCTION

Preventive Online Security Education (POSE) is a topic of growing international importance in the digital age. With the increase in the use of the Internet and mobile devices, teenagers around the world face increasingly complex and diverse risks when browsing online platforms. This issue has profound implications in their lives, especially in terms of personal data protection, cyberbullying, online manipulation and dealing with inappropriate content.

Therefore, Preventive Online Security Education has become a global necessity, and countries around the world are striving to develop effective strategies and programs to address these issues. Next, we will explore the initiatives, methods and importance of this preventive education for teenagers, approached both nationally and internationally. We must take into account that online education also comes with a series of advantages and disadvantage:

The online education is often celebrated for its accessibility and flexibility. It provides opportunities for individuals worldwide to access educational resources and courses, overcoming geographical barriers and allowing for learning at one's own pace. Many view online education as a convenient and cost-effective alternative to traditional classroom-based learning. It eliminates the need for commuting, offers flexible scheduling, and often reduces overall educational costs. Online education encompasses a wide range of learning formats, from short courses to full-degree programs. This diversity appeals to learners with varying needs, whether they seek specific skill development or are pursuing advanced academic qualifications. The integration of technology in online education is both praised and critiqued. Supporters see it as a way to enhance interactive learning experiences through multimedia, simulations, and collaborative tools. Critics argue that a lack of face-to-face interaction may hinder certain aspects of the learning process.

Online education is seen as a facilitator of lifelong learning. Individuals can continually update their skills and knowledge throughout their careers, promoting a culture of continuous learning in response to the demands of a rapidly changing job market. Teenagers often use social media extensively. Education in online security includes aspects of social media literacy, teaching them about privacy settings, the potential consequences of oversharing, and how to identify and report inappropriate content. Online security education encourages teenagers to strike a balance between their online and offline lives. This includes being mindful of screen time, managing online relationships responsibly, and understanding the potential impact of online actions on their well-being.

I. PREVENTIVE ONLINE SECURITY EDUCATION

Stages of POSE are: Awareness, Advice And Support, Training And Incident Management, Adapting To Changes, Figure 1.

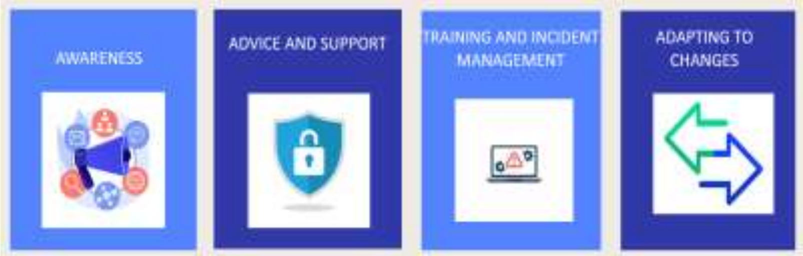

Figure 1. Stages of preventive online education

In each phase we have some methods that we should apply to improve the POSE and also by applying these methods in schools or in educational centers we will improve POSE at the national level or maybe international also.

I.1 Methods of Awareness

● INFORMATION SESSIONS AND DISCUSSIONS IN SCHOOLS: Organizing information sessions and discussions in schools or by means of educational programs can help teenagers to better understand the online risks and to openly talk about their experiences.

● AWARENESS EVENTS: Organizing special communities or school events to promote cyber security awareness. These events may include: presentations, seminars, workshops or competitions related to cyber security (Ansari, et al., 2022).

● PRACTICAL EXERCISES: Organizing of practical exercises in which teenagers can apply the acquired knowledge. These exercises may include: cyber-attack simulations, exercises for creating strong passwords or testing their phishing recognition skills.

● COMPETITIONS AND AWARDS: Holding competitions related to cyber security, offering prizes for those who demonstrate the best online security practices. These methods can stimulate teenagers' interest in the subject.

● PARENTS INVOLVEMENT: Encourage parents to be part of the awareness process and be informed about cyber risks. Parents can play an important role in supporting teenagers in online environment.

● QUESTION AND ANSWER SESSIONS: Organizing question and answer sessions during which teenagers can ask questions and talk to cyber security experts.

I.2 Methods of Advice and Support

● INDIVIDUAL AND GROUP COUNSELING SESSIONS: Organizing counselling sessions where teenagers can talk to a counsellor or cyber security specialist about their online concerns. These sessions can provide a safe environment to address personal issues and provide personalized advice.

● INFORMATION AND AWARENESS MATERIALS: Providing support resources such as: brochures, flayers, audio-video materials, tutorials and presentations that provide practical information about cyber security and resources for those experiencing difficulties.

● SUPPORT AND GUIDANCE SERVICES: Signposting teenagers to organizations and services specializing in cyber security and online protection, who can provide support and advice if they need it.

I.3 Methods of training and Incident Management

A computer security incident is any actual or suspected adverse event related to computer system or network security. Computer security incident activity can be defined as network or host activity that threatens the security potential of computer systems.

In (*Zamfiroiu and Sharma*, *2022*) the principles of cybersecurity incidents management are presented, Figure 2. These principles must be learned by young people, and they must be aware of the application of security procedures as they are applied in companies and be applied in schools or at home.

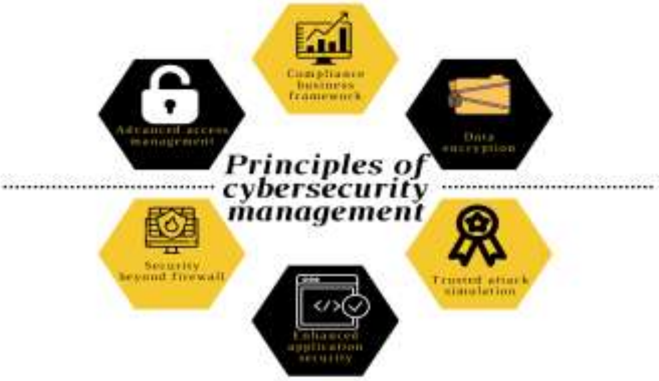
Compliance business framework
Advanced access management
Data encryption
Principles of cybersecurity management
Security beyond firewall
Trusted attack simulation
Enhanced application security

Figure 2. Principles of cybersecurity management

The methods that should be used for incident management are:

PROMOTING A CULTURE OF CYBER SECURITY

- Stimulating a responsible attitude towards the use of the Internet.
- Encouraging teenagers to report any cyber security incidents.
- SKILL TESTING

● Organizing ethical hacking competitions or cyber-attack simulation exercises to test the knowledge of teenagers.

IMPLEMENTATION OF TECHNICAL SECURITY MEASURES

● Promoting the use of strong passwords and multi-factor authentication for online accounts.

● Installing security software such as antivirus or content filtering solutions.

I.4 Methods of adapting to changes

● INVOLVEMENT OF TEENAGERS IN THE ADAPTATION PROCESS

● Solicit feedback and suggestions from teenager to improve prevention education programs.

● INCLUSION OF PERSONAL DATA PROTECTION TRAINING

● Focusing on the importance of personal data protection and online privacy.

● RAPID RESPONSE TO INCIDENTS

● Develop clear reporting and incident management procedures to act effectively in the event of a cyber-attack.

● ADDRESSING LEGAL AND ETHICAL ISSUES

Informing teenagers about the legal and ethical implications of online activities, including the consequences of inappropriate behaviour.

II. AWARENESS FOR DEEP AND DARK WEB

The terms "Deep Web" and "Dark Web" refer to distinct portions of the internet that are not indexed by traditional search engines and are often associated with anonymity and privacy concerns. The normal user access only the visible web or surface web that is available for everyone.

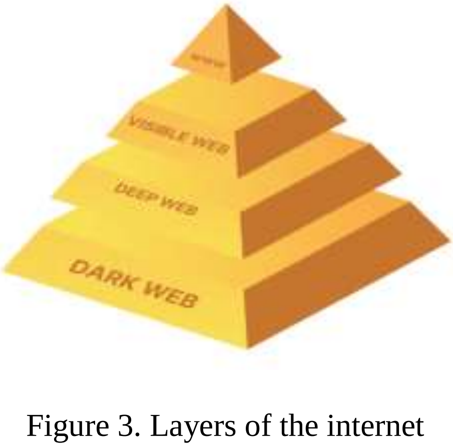

Figure 3. Layers of the internet

● The **SURFACE WEB**, also known as the Visible Web, comprises the part of the internet that is indexed by search engines and is easily accessible to the general public through standard web browsers. It includes websites, web pages, and content that can be found and accessed using search engines like Google, Bing, or Yahoo. These sites are designed to be openly available, and their content is not hidden behind paywalls, logins, or specific access restrictions.

CHARACTERISTICS OF THE SURFACE WEB:

- o **Searchable Content:** Surface web content is indexed by search engines, making it discoverable through search queries.
- o **Publicly Accessible**: The information on the Surface Web is intended for public consumption and doesn't require special permissions or access.
- o **Structured Content**: Websites are designed with navigation and linking structures, making information easy to find and navigate.
- o **Standard Web Protocols:** This part of the web operates through standard protocols such as HTTP and HTTPS, ensuring compatibility with standard web browsers.
- o **Varied Content:** It includes a vast array of content, from news articles and educational resources to e-commerce websites, blogs, forums, and much more.

● **DEEP WEB** contain the information that is not indexed on search engines and that may be available through some web pages. This vast section of the web contains content that isn't accessible through traditional search methods. It includes anything behind paywalls, private databases, password-protected sites, or content that is dynamically generated *(Kakoty and Rahman, 2018).*

CHARACTERISTICS OF THE DEEP WEB:

- ● **Unindexed Content:** The Deep Web consists of content that isn't accessible through standard search engines. This includes databases, academic resources, private networks, and more.
- o **Non-Indexed Pages:** Pages that haven't been linked to other pages or where search engines haven't crawled and indexed the content remain in the deep corners of the web.
- o **Privateand Restricted Access**: It contains content that requires specific access permissions, logins, or specialized software to view, like subscription-based content, company intranets, or personal email accounts.
- o **Significant Content Volume:** The Deep Web is estimated to be significantly larger than the Surface Web, housing a plethora of information that's not meant for public consumption.

● **DARK WEB** is a small, hidden portion of the internet that requires specific software and configurations to access. It operates on networks like Tor (The Onion Router) and I2P (Invisible Internet Project), which provide anonymity by routing internet traffic through a series of encrypted relays (Alaidi, et al., 2022).

CHARACTERISTICS OF THE DARK WEB:

- o **Anonymity:** Users on the Dark Web often remain anonymous, as their internet traffic is routed through various layers of encryption, making it challenging to trace their identity or location.

○ **Intentional Secrecy:** Content on the Dark Web intentionally remains hidden and requires specialized software (like the Tor browser) to access it.

○ **Illicit Activities:** The Dark Web is infamous for hosting illegal marketplaces, where illicit goods, such as drugs, weapons, and stolen information, are bought and sold. It's also known for hosting forums and sites that promote various illegal activities.

○ **Hidden Services:** Websites on the Dark Web use "onion" domains and offer services that are often not accessible through conventional browsers. These sites are often involved in illegal activities but can also provide a platform for free speech in regions where it's restricted.

○ **Cautionary Environment:** The Dark Web is a digital space with numerous risks, including exposure to illegal content, scams, and potential security threats.

DARK WEB is one of the most dangerours platforms where products and information are traded such as *(Koch, 2019):*

- personal databases of children (photos, movies, geographic location data, etc.);
- databases with basic information, personal data, data with access to computers and servers;
- works of art, trade secrets, organ trafficking, identity change services, drugs, weapons.

In *(Nazah et al., 2020)* eight major crime threats in the Dark Web are presented. For teenagers is very important because they use social media and a lot of applications for communication. People with bad influences can use these platforms to interact with the children. So, the dark web is used massively by Pedophiles and related criminals for child pornography.

IV. DISCUSSIONS

Online security represents all the actions we do to protect ourselves from dangers, and for teenagers is very important to pay attention to the next points:

- Exposure of teenagers to illegal and/or harmful content;
- Victimization through intimidation, harassment or threats (or "cyberbullying");
- Alienation or theft of personal data;
- Sending or receiving video sequences, images or messages of a sexual nature (or "sexting");
- Grooming (luring for the purpose of committing sexual acts).

All these represent the risks to which we can be exposed so also the teenagers can be exposed, and it is possible that they are not able to distinct the reality of the fake information and for that it is possible to be victims of these kind of attacks.

Cyber security regulations serve as a proactive measure to address the ever-growing threats in the digital realm, ensuring a safer, more secure online environment for individuals, businesses, and nations. They are essential in establishing a baseline of security practices and encouraging a collective effort towards protecting digital assets.

Cybersecurity regulations typically encompass several key components to ensure comprehensive protection in the digital space:

- **Data Protection Standards:** Regulations outline specific measures to protect sensitive data, including encryption requirements, access controls, and guidelines for data storage and transmission.
- **Incident Response Protocols:** Establishing procedures for identifying, reporting, and responding to cyber incidents is crucial. Regulations often mandate incident response plans to minimize damage in case of a security breach.
- **Compliance and Reporting Requirements:** Regulations typically mandate compliance with certain standards and reporting of cybersecurity measures. This might involve audits, assessments, or regular reporting to ensure ongoing adherence to security standards.
- **Access Control and Authentication:** Rules governing user access, authentication methods, and authorization mechanisms help prevent unauthorized entry and data breaches.
- **Security Testing and Vulnerability Assessments:** Mandating regular security testing, including vulnerability assessments, helps proactively identify weaknesses in systems, enabling their timely resolution.
- **Education and Training:** Regulations might stress the importance of educating employees or individuals on cybersecurity best practices, raising awareness about potential threats and how to mitigate them *(Vevera, 2019).*

THE NATIONAL INSTITUTE FOR RESEARCH AND DEVELOPMENT IN INFORMATICS (ICI BUCHAREST) strategies to improve online safety education for teenagers:

- create partnerships with schools and educational institutions;
- collaborate with youth organizations and ONG;
- leverage social media and online platforms;
- organize cybersecurity competitions and events;
- establish a network of cybersecurity ambassadors.

CONCLUSIONS

Implementing preventive online safety education for teens is not only a proactive measure, but a fundamental necessity in today's digital landscape. Through comprehensive education covering aspects of digital literacy, critical thinking and responsible online behavior, we are paving the way for a safer and more informed generation. By integrating such programs into educational programs and collaborating across sectors-educators, parents, policymakers, and *technology companies-we create a support network that empowers teenagers with the skills to navigate the online world safely. This not only protects them from potential threats such as cyberbullying, privacy violations and exposure to inappropriate content, but also empowers them to harness the positive potential of the internet.*

The education isn't just about cautionary tales but also an empowerment tool, enabling teenagers to harness the positive aspects of the online realm while protecting themselves from potential risks. Creating a culture of responsible digital citizenship ensures that these young individuals not only safeguard themselves but also contribute positively to the digital community.

Ultimately, the success of online safety education lies in its ability to shape conscientious and informed digital citizens, promoting a safer, more supportive online environment for teenagers to explore, learn, and thrive.

BIBLIOGRAPHY

1. Alaidi, A. H. M., Roa'a, M., ALRikabi, H. T. S., Aljazaery, I. A., & Abbood, S. H. (2022). *Dark web illegal activities crawling and classifying using data mining techniques*. iJIM, 16(10), 123;

2. Ansari, M. F., Sharma, P. K., & Dash, B. (2022). *Prevention of phishing attacks using AI-based Cybersecurity Awareness Training. Prevention;*

3. Kakoty, N., & Rahman, M. (2018). *A Survey on the Concepts of Surface Web, Deep Web and Dark Web.* International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 3(3), 544-549;

4. Koch, R. (2019, May). *Hidden in the shadow: The dark web-a growing risk for military operations?* In 2019 11th International Conference on Cyber Conflict (CyCon) (Vol. 900, pp. 1-24). IEEE;

5. Nazah, S., Huda, S., Abawajy, J., & Hassan, M. M. (2020). *Evolution of dark web threat analysis and detection: A systematic approach.* Ieee Access, 8, 171796-171819;

6. Vevera A.V. (2019), *Reglementări legislative cu privire la securitatea cibernetică [Legislative regulations regarding cyber security],* Ed. ICI, București;

7. Zamfiroiu A., Sharma R.C., *"Cybersecurity Management for Incident Response"*, Romanian Cyber Security Journal, ISSN 2668-6430, vol. 4(1), pp. 69-75, 2022. https://doi.org/10.54851/v4i1y202208.