https://www.sworldjournal.com/index.php/swj/article/view/swj19-03-028
DOI: 10.30888/2663-5712.2023-19-03-028

УДК 378.147

CYBER HYGIENE PRACTICES AND PROVIDING PROPER EDUCATION

Podlinyayeva O.O.
c.p.s., as. prof.,
ORCID: 0000-0002-0009-3126
Sytnyk L.G.
c.t.s, as. зrof,
Sumy Regional Institute of Postgraduate Pedagogical Education,
Sumy, Rymskogo-Korsakova, 5, 40007

Abstract. *The article discusses the essence of the concept of "cybersecurity" and the problems of solution. This area is related to the protection of: digital information, operating systems, computer networks, servers, databases, public and private institutions from unauthorized interference by unauthorized persons.*

Key words: *Cyber hygiene, cybersecurity, education.*

Introduction.

Pandemic of the coronavirus COVID-19, Russia's open military attack on Usual conditions of life collapsed in Ukraine, radically changed our life and accelerated the transition to new digital technologies and online services.

Cyber hygiene refers to the practices that individuals and organizations follow to ensure their digital security and prevent cyber attacks. It includes actions such as using strong passwords, regularly updating software, being cautious when clicking on links or downloading attachments, and using antivirus software. Good cyber hygiene is essential to protect against threats such as malware, phishing, and identity theft.

One of the most popular scientific theories of cyber hygiene is the concept of defense in depth. This theory suggests that a layered approach to cybersecurity is the most effective way to protect against cyber threats. This involves implementing multiple layers of security controls, such as firewalls, antivirus software, intrusion detection systems, and access controls, to provide multiple barriers that an attacker must overcome to gain access to sensitive data or systems. Additionally, this theory emphasizes the importance of regular updates and maintenance of these security controls to ensure they are effective against the latest threats.

Main text.

Cyber hygiene for children at schools refers to the practices and measures implemented to ensure the safe and responsible use of technology and the internet. Here are some key aspects of cyber hygiene for children at schools:

1. Internet Safety Education: Schools should provide age-appropriate training on internet safety, including guidance on safe online behavior, recognizing and avoiding online risks, and understanding the potential consequences of sharing personal information.
2. Strong Passwords: Teach children how to create strong passwords and emphasize the importance of not sharing them with anyone. Encourage regular password updates and the use of password management tools.
3. Privacy Settings: Educate children about privacy settings on social media platforms and other online services. Teach them to limit the amount of personal

information shared publicly and to be cautious about accepting friend requests or communicating with strangers online.

4. Phishing Awareness: Teach children to identify phishing attempts, such as suspicious emails or messages asking for personal information. Emphasize the importance of not clicking on unknown links or downloading attachments from unfamiliar sources.
5. Cyberbullying Prevention: Schools should have policies and educational programs in place to address cyberbullying. Teach children about the impact of cyberbullying, encourage reporting, and promote a positive and respectful online environment.
6. Safe Downloading and App Usage: Instruct children on the importance of downloading files and apps from trusted sources only. Teach them to be cautious of malware and to verify the legitimacy and permissions of apps before installation.
7. Social Media Awareness: Help children understand the potential risks associated with social media, such as online harassment or inappropriate content. Encourage responsible use, mindful posting, and teach them how to report and block abusive accounts.
8. Regular Updates and Antivirus Software: Emphasize the importance of keeping devices and software up to date with the latest security patches. Install reputable antivirus software to protect against malware and other threats.
9. Secure Wi-Fi Usage: Teach children about the risks of using public Wi-Fi networks and encourage the use of secure, password-protected networks. Remind them not to share personal information or conduct sensitive transactions on unsecured networks.
10. Open Communication: Foster an open dialogue between children, parents, and educators regarding online activities and any concerns they may have. Encourage children to report any suspicious or inappropriate online encounters.

By promoting cyber hygiene practices and providing proper education, schools can empower children to navigate the digital world safely and responsibly. Studying cyber hygiene can be an engaging and interactive experience. Here are some interesting practices to study cyber hygiene:

1. Gamified Learning: Utilize gamification techniques to make the learning process more enjoyable and engaging. Create interactive quizzes, puzzles, or online games that focus on cyber hygiene concepts and encourage students to test their knowledge while having fun.
2. Role-playing Exercises: Organize role-playing scenarios where students can simulate real-life cyber situations. Assign roles such as hacker, victim, or cybersecurity expert, and encourage students to think critically and make decisions based on cyber hygiene principles.
3. Ethical Hacking Challenges: Introduce ethical hacking challenges or capture-the-flag (CTF) competitions where students can apply their knowledge of cybersecurity and cyber hygiene to solve puzzles, find vulnerabilities, and protect digital assets.
4. Case Studies and Discussions: Present real-world case studies of cyber incidents,

data breaches, or online safety issues. Engage students in discussions to analyze the causes, impacts, and preventive measures associated with each case. Encourage critical thinking and problem-solving skills.

5. Guest Speakers and Experts: Invite guest speakers, such as cybersecurity professionals or law enforcement personnel, to share their experiences and insights on cyber hygiene. They can provide practical tips, industry trends, and engage students in discussions and Q&A sessions.
6. Simulations and Virtual Labs: Provide access to virtual labs or simulations that replicate cyber-attacks, allowing students to observe and respond to different scenarios in a controlled environment. This hands-on experience can enhance their understanding of cyber hygiene best practices.
7. Peer-to-Peer Learning: Encourage students to collaborate and learn from each other. Assign group projects or discussions where they can exchange knowledge, share resources, and brainstorm ideas related to cyber hygiene.
8. Cybersecurity Awareness Campaigns: Organize cybersecurity awareness campaigns within the school or local community. Students can create posters, videos, or social media campaigns to raise awareness about cyber hygiene and educate their peers and community members.
9. Field Trips and Industry Visits: Arrange visits to cybersecurity companies, data centers, or law enforcement agencies involved in combating cybercrime. Students can observe real-world security measures and learn about the importance of cyber hygiene in various professional settings.
10. Simulated Phishing Exercises: Conduct simulated phishing exercises to test students' ability to identify phishing emails or messages. This activity can help them understand the tactics used by cybercriminals and reinforce the importance of vigilance in practicing cyber hygiene.

These practices can make the study of cyber hygiene more dynamic, interactive, and memorable, fostering a deeper understanding of the subject matter among students.

Pedagogical research on the methods of studying cyber hygiene aims to identify effective teaching and learning approaches that promote understanding, engagement, and retention of cyber hygiene concepts. While specific studies may vary, here are some common areas of pedagogical research in the field:

1. Instructional Design: Researchers investigate the design and development of instructional materials, including curriculum frameworks, lesson plans, and educational resources, tailored to teach cyber hygiene effectively. This research examines how to structure content, integrate interactive elements, and optimize learning experiences.
2. Active Learning Strategies: Pedagogical research explores active learning strategies that engage students in the learning process. These may include problem-based learning, case studies, hands-on activities, and collaborative projects that require students to apply cyber hygiene principles in practical scenarios.
3. Gamification and Serious Games: Researchers explore the effectiveness of gamification techniques and serious games in teaching cyber hygiene. They investigate how game elements, such as challenges, rewards, and leaderboards,

can enhance motivation, knowledge acquisition, and retention of cyber hygiene concepts.

4. Simulation and Virtual Environments: Pedagogical research examines the use of simulations and virtual environments to provide realistic experiences and allow students to practice cyber hygiene skills in a controlled setting. These studies investigate the impact of virtual labs, cyber ranges, or cybersecurity simulations on learning outcomes.
5. Peer Learning and Collaboration: Researchers investigate the benefits of peer learning and collaborative activities in the context of cyber hygiene. They examine how group discussions, teamwork, and peer feedback contribute to deeper understanding, critical thinking, and knowledge sharing among students.
6. Assessment Methods: Pedagogical research explores different assessment methods to evaluate students' understanding of cyber hygiene. This may include traditional tests, project-based assessments, scenario-based evaluations, or practical demonstrations of skills.
7. Technology-Enhanced Learning: Researchers investigate the role of technology in cyber hygiene education, exploring the effectiveness of online platforms, interactive tools, virtual reality, and mobile applications in delivering engaging and effective learning experiences.
8. Teacher Professional Development: Pedagogical research focuses on teacher training and professional development programs to enhance educators' pedagogical skills and knowledge in cyber hygiene education. It examines effective strategies for supporting teachers in delivering engaging lessons and staying up to date with the evolving landscape of cyber threats.
9. Transfer of Learning: Researchers investigate the transfer of cyber hygiene knowledge and skills from the classroom to real-life situations. They explore how to promote the application of learned principles in students' daily online activities and encourage responsible and secure behaviors beyond the educational setting.
10. Longitudinal Studies and Impact Assessment: Pedagogical research examines the long-term impact of cyber hygiene education on students' attitudes, behaviors, and digital citizenship. It investigates the effectiveness of educational interventions in developing a culture of cyber hygiene and reducing cyber risks among students.

These pedagogical research areas contribute to the development of evidence-based practices and inform educators on effective strategies to teach cyber hygiene in ways that maximize student engagement, understanding, and the application of knowledge in real-world contexts. Teaching cyber hygiene and cyber safety to children should be age-appropriate, taking into consideration their cognitive abilities and understanding. Here are some general recommendations for different age groups:

1. Preschool (3-5 years):
   - Introduce basic concepts of online safety, such as not sharing personal information or photos with strangers.
   - Teach them to ask for help from a trusted adult if they encounter something they don't understand or find uncomfortable online.

- Encourage responsible device usage and establish time limits for screen time.

2. Early Elementary (6-8 years):
   - Teach the importance of strong passwords and not sharing them with others.
   - Introduce the concept of cyberbullying and discuss ways to be kind and respectful online.
   - Emphasize the need to obtain permission before downloading or installing apps or games.
   - Introduce safe search practices and explain the difference between reliable and unreliable sources of information.
3. Upper Elementary (9-11 years):
   - Teach about the risks of sharing personal information online and the potential consequences.
   - Discuss the importance of privacy settings on social media platforms and online accounts.
   - Teach critical thinking skills to evaluate online content for accuracy and credibility.
   - Discuss the implications of cyberbullying and encourage open communication about online experiences.
4. Early Adolescence (12-14 years):
   - Discuss the permanence of online actions and the potential impact on future opportunities.
   - Teach about phishing attempts and how to recognize and avoid them.
   - Promote responsible social media use, including appropriate sharing of personal information and mindful posting.
   - Discuss the potential risks associated with online gaming and the importance of setting boundaries.
5. Late Adolescence (15-18 years):
   - Discuss the importance of managing digital footprints and the potential consequences of inappropriate online behavior.
   - Teach about online reputation management and the impact of social media on college admissions and job opportunities.
   - Discuss legal and ethical considerations related to hacking, piracy, and copyright infringement.
   - Provide guidance on safe online shopping, financial transactions, and protecting personal information.

Inference.

It's important to adapt the recommendations to individual children's maturity levels and monitor their online activities regularly. Encouraging open communication, establishing clear rules and boundaries, and being actively involved in their online experiences are essential regardless of age. Additionally, involving parents and caregivers in the educational process can reinforce cyber hygiene and safety practices.

References:

1. Howard, R. The Cybersecurity Canon: Must-Read Books on Cybersecurity. URL: https://www.bankinfosecurity.com/raj-shah-a-6561.

2. Implications of Artificial Intelligence for Cybersecurity: Proceedings of a Workshop. URL: http://surl.li/hddwt.

3. Cyber Hygiene: The Big Picture. URL: https://link.springer.com/chapter/10.1007/978-3-030-03638-6_18.

4. Биков В. Ю., Буров О. Ю., Дементієвська Н. П. Кібербезпека в цифровому навчальному середовищі. Інформаційні технології і засоби навчання. 2019. № 70 (2). С. 313-331. URL: https://doi.org/10.33407/itlt.v70i2.2876_.

5. Горбенко А. А. Кібербезпека освітнього середовища в умовах карантину URL: https://conf.ztu.edu.ua/wp-content/uploads/2020/05/94.pdf.

6. Основні правила захисту даних – кібергігієна для активного Інтернет-користувача URL: https://eset.ua/ua/blog/view/38/osnovnyye-pravilazashchity-dannykh-kibergigiyena-dlya-aktivnogo-Internet-polzovatelya.

The article has been sent: 19.05.2023 p.