SDSC
Student Digital Safety Certification

Ensuring Child Safety in the Digital Era
Empowering Parents, Educators, and Clarifying Roles

Presented by:

Dr. Nabih Abdelmajid
Higher Colleges of Technology UAE

About the Curriculum

This curriculum aims to raise the level of quality protection for students from the dangers of cyber-crimes facing them. This is through the experiences of researchers and trainers specializing in electronic security, digital quality of life and specialists in rehabilitation and awareness in the field of the cybersecurity.

This curriculum also seeks to provide guidance to protect students from cyberbullying and various types of blackmail (sexual harassment – terrorism – control – intimidation...ect).

As well as protecting children from distorting their thoughts and beliefs about all evil.

We recognized the necessity of working to qualify different levels of students to deal with security and to make them aware of the danger of ignoring the importance of security using modern means of communication and educational application used.

Motivations

- The rapid development of information technology and the existing of diversity and easily ways of information exchange made it accessible to many groups of society, especially young group of schools' students.

- There has been a high turnout among the students to use the social networking sites, which have spread rapidly in recent times.

- Unfortunately, the use of these sites by students was not preceded by the necessary rehabilitation to use this technology properly and correctly, which led to many problems of penetration and extortion.

Motivations... cont..

- One of the most striking results for this Unconscious turnout is the many misguided security practices that have made societies ineligible to avoid the risk of hackers

- the recent successes of these hackers in penetrating users' privacy and extortion have increased in recent times

Study Sample

- The sample of this study was chosen to be school students in the Kingdom of Saudi Arabia because of the exposure of this category to many breaks recently.

- This study chose main axes to reveal the relationship between social networking sites and the penetration of the users' privacy

Study Axes

- Identify the turnout degree of using social sites
- Identify the students' goals of using social sites
- Identify percentage of those who have been hacked and exposed to blackmail
- Identify the level of users' knowledge of the seriousness of dealing with social networking sites

Degree of using social sites

Hours of use	Frequency	Percent
1 to 2	80	20.0
2 to 4	91	22.7
4 to 6	89	**22.2**
> 6	133	**33.2**
Total	393	98.0
System	8	2.0
Total	401	100.0

students' goals of using social sites

- 79% of male and female students have more than one account on these sites.

- 87.6% of the students said that it is very difficult to stop using these sites (**Addiction**)

- 15.2% of students are choosing fake names while using these sites.

- 23.2% indicated that their personal information is not real.

- 34.4% of students confirmed that they had established false relationships through these sites.

- 30.4% refused to let their parents' to see their personal accounts, while 29.7% of them reject their parents' control partially

who have been hacked and exposed to blackmail?

- 22.2% of the students reported that they had been exposed to penetration during their use of these sites.

- 34.7% of their passwords have been stolen.

- 15.2% of the students have stolen their files and their own pictures.

- **15.5% indicated that they are being subjected to extortion continuously**

level of users' knowledge

- 58.8% of students expressed their acceptance of any friendship requests through these sites.

- 38.9% believe all the information presented through these sites.

- 65.6% of the students believe that social networking sites are safe and trustworthy.

- 64.6% used the same password a long time ago and never change it.

- More than 57% do not mind telling their friends their passwords.

- More than 30% do not use any of the protection programs

Parents Affects

- The relationship between the level of parental qualification and the level of communication between them and their children

- Relationship between parents' level of education and their ability to detect attempts to blackmail their children

Parental qualification and communication with their children

Education Level	Communicate with children	fear of parents
High	High	Low
Intermediate	Intermediate	Intermediate
Low	**Low**	**High**

parents' level of education and ability to save children

Education Level	Number of Extortion	Number of success help
High	4	3
Intermediate	1	1
Low	0	0

So ….We need to:

- It has become very important to qualify STUDENTS and PARENTS and inform them about the effects of unsafe use of this technology on the preservation of their electronic privacy

- The researcher found an urgent need to get to a safe electronic community, through work on the rehabilitation of the students on how to use the new communication technology in a safe way, and not ignoring the important of this secure using

For a safe family

Motivate your child to have a nickname

Sergeant Of Digital Safety

File backup skills	Geo-tracking of the lost device	Delete photo safely
Stop tracking user activities	Privacy settings skills	Control application activities
Online anti-tracking skills	Special data recovery skills	Public visibility management skills

For a safe family

Motivate your child to win the

Captain of Digital Safety

iCloud account management skills

Steps to protect devices from hacking

Spyware stop settings

Virus removal skills

Google account management

Data hiding skills

Virtual machine building skills

Device coding skills

Introducing a Holistic Solution

SDSC
Student Digital Safety Certification

1 A comprehensive program from basics to advanced topics.

2 Developed by leading cybersecurity experts.

3 Combines theory, real-world applications and simulations.

Stepping Stone to Higher Learning

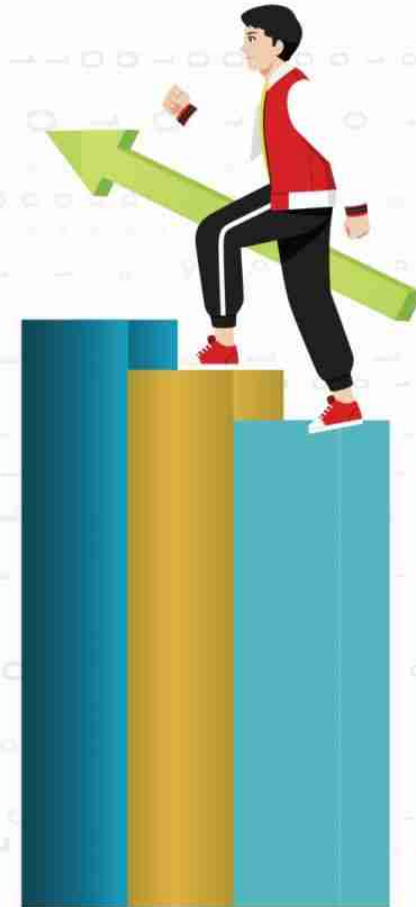**01** Provides foundational knowledge for advanced degrees.

02 Pathway for specialized cybersecurity Master's or PhD programs.

03 Potential to introduce dedicated research centers on cybersecurity.

A Collective Effort

Workshops for teachers on integrating cybersecurity in lessons.

Building a community of digital safety advocates.

Shaping Tomorrow's Leaders

1. **SDSC: Not just education but career empowerment.**

2. **An opportunity to bridge the global skill gap.**

3. **A call to be at the forefront of cybersecurity training.**

Resources:

- https://search.emarefa.net/ar/detail/BIM-836136-%D8%A7%D9%84%D8%A3%D9%85%D9%86-%D8%A7%D9%84%D8%A5%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A-%D8%B6%D8%B1%D9%88%D8%B1%D8%A9-%D9%85%D9%84%D8%AD%D8%A9-%D9%84%D8%A3%D9%85%D9%86-%D8%A7%D9%84%D9%85%D8%AC%D8%AA%D9%85%D8%B9%D8%A7%D8%AA-%D9%85%D9%82%D8%AA%D8%B1%D8%AD-%D8%A7%D9%84%D8%A3%D8%B3%D8%B1%D8%A9-%D8%A7%D9%84%D8%A2%D9%85

- https://link.springer.com/chapter/10.1007/978-3-030-01177-2_75#:~:text=The%20level%20of%20students'%20knowledge,these%20sites%20is%20very%20high.

Security Circles – SDSC Platform

Let's Discuss

01 How can we integrate SDSC with existing programs?

02 Are there potential partnerships or grants we should explore?