



# Technical Skill Focus – Stronger Passwords

## SuperCyberKids Lesson Plan

### Lesson 3 - Consolidation

**Call: ERASMUS-EDU-2022-PI-FORWARD**

**Type of Action: ERASMUS-LS**

**Project No. 101087250**



**Co-funded by  
the European Union**

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. Neither the European Union nor the granting authority can be held responsible for them.

<b>Project ref. number</b>	101087250
<b>Project title</b>	<b>SCK - SuperCyberKids</b>
<b>Document title</b>	Technical Skill Focus – “Stronger Passwords” Lesson 3 Consolidation
<b>Document Type</b>	Lesson Plan
<b>Document version</b>	V1, 10/12/2024
<b>Previous version(s)</b>	V1
<b>Language</b>	English
<b>Author(s)</b>	Giorgia Bassi, IIT-CNR Ilaria Matteucci, IIT-CNR
<b>With contributions by:</b>	<author, section(s)>

# Table of Contents

1	Target info	3
2	Lesson 3 - Consolidation	4

# 1 Target info

**Main tool:** Video game “Nabbovaldo and the blackmail from cyberspace” and standard group games.

**Learning Context:**

- Ages 10-13
- 20-25 students
- 1 hour
- Location: classroom with projector or screen visible to all students
- Resources:
  - Internet-connected computer for instructor
  - NABBOVALDO game with lesson materials
  - Whiteboard
  - Paper and writing instruments for students

**Objectives:**

- The game introduces children to strategies for protecting against cyber attackers.
- The game introduces children to detecting and implementing actions against basic cyber-attacks.
- The game introduces children to understanding basic cyber threats.
- The game introduces children to basic prevention technologies.
- The game introduces children to using software tools to protect digital devices.
- The game introduces children to strategies to protect their personal information while surfing the web.

## 2 Lesson 3 - Consolidation

Activity	Time	Details	Learning Goal	Extras
Intro	5 min	<p>Announce to the class that the topic of discussion for the day will be a continuation of the class discussion on cybersecurity.</p> <p>Review prior lessons by eliciting effective tools for creating good, strong passwords</p> <p>Write the rules elicited on the board. Add any rules Students may have forgotten.</p>	Introduce topic	
Discussion	10 min	<p>Ask Students what ways people can get hold of your Passwords. Elicit ideas.</p> <p>Mention the types of attacks hackers can perform even if they don't have your Password.</p> <ul style="list-style-type: none"> <li>- Dictionary attack</li> <li>- Brute force attack</li> </ul> <p>Explain how these attacks work</p> <p>Elicit ideas for how to prevent these attacks from being successful</p>	Expand knowledge base	
Activity	20 min	<p>Explain that this activity will help students understand how Password attacks work and how password complexity can help prevent these attacks.</p> <p>Separate class into pairs.</p> <p>For each pair, choose one Student to be 'A' and the other to be 'B'.</p> <p>Instruct 'A' students to pick a single number and 'B' students to pick a single letter. These will be their Passwords.</p> <p>Note! Stick with the letters allowed by most website Password creation tools (26 base letters)</p> <p>Instruct Students to try to guess their partner's Password, recording the number of guesses needed before successfully guessing.</p> <p>Repeat this a few times for more accurate results. If time allows, switch sides as well ('A' becomes 'B' and vice versa).</p> <p>When all groups have completed the task, ask how many guesses it took to guess. Compare 'A' guesses to 'B' guesses on the board.</p> <p>Some lucky guesses may make guesses at 'B' Passwords lower, but the average should show that it takes more guesses for a letter than a number. Discuss why (10 possibilities vs. 26 possibilities)</p> <p>Now instruct 'A' Students to choose a single number OR letter OR a special character such as those allowed by Password creation tools (~!@#\$%^&amp;*()_-+={}  \:;'"&lt;,&gt;.&gt;./) (Note! Not all of these characters are</p>	Deeper understanding of password complexity	Adapted from <a href="#">this</a> activity

		<p>allowed by all Password tools, but it helps illustrate our point)</p> <p>Repeat the above process with Students writing down the number of guesses needed to correctly guess the partner’s Password character.</p> <p>Collect the numbers of guesses and write the averages on the board. Compare the outcomes of the two iterations of the activity.</p>		
--	--	--	--	--

Discussion	10 min	<p>Discuss the results on the board.</p> <p>What do the results show? Why is this important? What effect would increasing the number of characters have?</p> <p>Discuss what strategies Ss used to guess their partner’s PW and how to counter these strategies.</p> <p>Look at real-world examples of PW requirements for websites and discuss why they have the requirements they have.</p> <p>As a class, create a new list of rules for PW creation</p>	Exploration of topic in depth	
Wrap-up	5 min	<p>Consolidate lessons from the day. Answer any questions Ss may have.</p> <p>Assign homework (if any)</p>		