CSNP
CYBERSECURITY NON-PROFIT

Middle School Cybersecurity Lesson Plan

A comprehensive 5-day module for grades 6-8 educators to build essential digital safety skills and empower the next generation of responsible digital citizens.

MODULE OVERVIEW

Five Days to Digital Citizenship

01

Digital Footprint & Online Reputation

Students explore how their online actions create a permanent digital trail and learn strategies to build a positive online presence.

02

Social Media Privacy

Understanding privacy settings, data collection, and making informed decisions about what to share across platforms.

03

Cyberbullying Prevention

Recognizing, responding to, and preventing cyberbullying while fostering empathy and positive online interactions.

04

Phishing & Scam Recognition

Identifying red flags in emails, messages, and websites to protect personal information from digital threats.

05

Becoming Digital Citizens

Synthesizing skills into a personal action plan for responsible, ethical, and safe online behavior.

Day 1: Digital Footprint & Online Reputation

Learning Targets

- Define digital footprint and explain its permanence
- Identify positive vs. negative online behaviors
- Evaluate the impact of posts on future opportunities

Key Activities

- Interactive "footprint mapping" exercise
- Case study analysis of real-world scenarios
- Personal audit worksheet

Discussion Questions

1. What might a college admissions officer learn about you from your social media?
2. How can you turn your digital footprint into an asset?
3. What's one thing you'd delete from the internet if you could?

Materials Needed

Student devices, digital footprint worksheet, chart paper, markers, case study handouts

Day 2: Social Media Privacy

Understanding Data Collection

Students examine how apps collect, share, and monetize personal data. Includes hands-on privacy policy analysis activity.

Privacy Settings Walkthrough

Guided tutorial across major platforms (Instagram, TikTok, Snapchat). Students create a privacy checklist they can use at home.

The Sharing Decision Tree

Interactive tool to evaluate what's safe to post. Students practice using the "pause before you post" framework with real scenarios.

Teacher Tip: Have students screenshot their current privacy settings before class. This creates immediate engagement and personalized learning.

Day 3: Cyberbullying Prevention

Recognize

Identify cyberbullying behaviors including harassment, impersonation, exclusion, and doxing through multimedia examples.

Respond

Learn the "Stop, Block, Tell" framework. Practice bystander intervention and appropriate ways to support peers.

Prevent

Build classroom norms for digital kindness. Create an empathy-based action plan for positive online communities.

Role-Playing Scenarios

Students work in groups to act out appropriate responses to cyberbullying situations, building confidence and practical skills.

School Resource Connection

Provide students with specific staff contacts, reporting procedures, and anonymous reporting options available at your school.

SECURITY

Day 4: Phishing & Scam Recognition

The Red Flag Checklist

Urgent language, suspicious sender addresses, spelling errors, requests for personal information, too-good-to-be-true offers, and mismatched links.

Interactive Scam Lab

Students analyze real phishing emails and texts in a safe environment, voting on legitimacy and explaining their reasoning to build critical thinking skills.

Family Safety Extension

Take-home activity where students teach family members to spot scams, reinforcing learning through teaching and extending impact beyond the classroom.

Day 5: Creating Digital Citizens

Synthesis Project Options

- Personal cybersecurity action plan
- Public service announcement video
- Infographic for younger students
- Digital citizenship pledge poster

1

Reflect

Review key concepts from the week through guided reflection

2

Create

Design chosen project demonstrating understanding

3

Share

Present work and commit to digital citizenship pledge

Students conclude by setting three personal cybersecurity goals and sharing one key takeaway with the class community.

Assessment & Differentiation

Performance Rubric

Standards-aligned assessment measuring knowledge, application, and critical thinking across all five lesson domains.

Differentiation Strategies

Scaffolded activities, visual supports, technology accommodations, and extension challenges for all learners.

Formative Checks

Daily exit tickets, peer discussions, self-assessments, and observation protocols to monitor understanding.

Accessibility Note: All materials include text alternatives, adjustable font sizes, and multiple means of engagement to support diverse learning needs.

TEACHER RESOURCES

Implementation Tools

Reproducible Handouts

Ready-to-print worksheets, graphic organizers, parent letters, and student resource guides included in complete lesson package.

Slide Decks

Fully designed, editable presentations for each day with embedded videos, discussion prompts, and activity instructions.

Pacing Guides

Flexible timing suggestions adaptable to 45-minute or block schedules, with options for condensed or extended versions.

Extension Activities

Enrichment projects, cross-curricular connections, and ongoing initiatives to sustain digital citizenship throughout the year.

Parent Communication Template

What's Included

- Overview of weekly topics and objectives
- Conversation starters for home discussions
- Resources for continued family learning
- Warning signs parents should monitor

Communication Goals

Build home-school partnership in cybersecurity education. Empower parents with knowledge and tools to support their children's digital safety beyond the classroom.

Available in multiple languages and formats for accessibility.

> "The letter helped me understand what my daughter is learning and gave me specific questions to ask about her online activities."
>
> — *Parent feedback from pilot program*

Standards Alignment & Learning Outcomes

ISTE Standards

Aligned with Digital Citizen and Knowledge Constructor standards

State Requirements

Meets cybersecurity education mandates in 40+ states

21st Century Skills

Develops critical thinking, communication, and digital literacy

Expected Learning Outcomes

Knowledge

- Define key cybersecurity concepts
- Identify online threats and risks
- Explain digital citizenship principles

Skills

- Analyze privacy settings effectively
- Recognize phishing attempts
- Apply safety strategies online

Dispositions

- Value personal digital security
- Demonstrate empathy online
- Commit to responsible behavior

About CSNP

The Cybersecurity Non-Profit (CSNP) is dedicated to making cybersecurity knowledge accessible to everyone through education, community support, and practical resources.

Our Programs

Business & Non-Profit Security

Family Cybersecurity

Kids Safety

Senior Digital Safety

Women's Security

Parents & Educators

Everything we offer is completely free. Visit **csnp.org** to explore our programs or access additional resources at **csnp.org/resources**