

Cyber Elementary School

5th Grade Lesson Plan Book

Lesson 5: Safe Wi-Fi and Network Habits: Locking Your Digital Front Door

Lesson Title: Safe Wi-Fi and Network Habits: Locking Your Digital Front Door

Lesson Number: 5 of 36

Grade/Age: Elementary School (Grade 5)

Subject: Cyber Security and Safety

Duration: 30–40 Minutes

Learning Objectives

- Students will be able to explain what Wi-Fi is and why some networks are safer to use than others.
- Students will be able to identify the difference between a trusted home/school network and an open public network.
- Students will be able to describe at least two safe habits for using Wi-Fi, especially in public places.
- Students will be able to explain why it's risky to do sensitive activities (like logging into accounts) on public Wi-Fi.

Skills

Digital literacy, risk assessment, situational awareness, personal responsibility, basic cyber hygiene habits.

Warm-Up / Hook (5 minutes)

"Open Door vs. Locked Door" Comparison. Ask students: "If you saw two houses — one with the front door wide open and no one around, and one with a locked door and a doorbell — which one would you feel safer walking into?" Discuss briefly. Explain that Wi-Fi networks are similar: some are "locked" with a password and belong to a trusted place (like home or school), while others are "wide open" with no password at all, letting anyone connect — including people who might try to snoop on what others are doing online.

Recommended Teacher Talking Points (Introduction)

- Wi-Fi is the invisible signal that lets our devices connect to the internet without wires.
 - Just like some doors are locked and some are left open, some Wi-Fi networks are protected with a password and some are completely open to anyone nearby.
 - Using a trusted, password-protected network (like at home or school) is much safer than using an open network at a coffee shop, airport, or store.
 - Today we'll learn how to spot safer networks and build habits that protect your information no matter where you connect.
-
-
-

Direct Instruction with Recommended Teacher Talking Points

Core Concept:

- A trusted network — like your home Wi-Fi or your school's Wi-Fi — usually requires a password and is set up by people you know.
- A public or open Wi-Fi network — like at a store, restaurant, or airport — often has no password, which means anyone nearby could potentially see what unprotected devices are sending and receiving.
- Always connect to Wi-Fi with a parent, guardian, or teacher's help and permission, especially away from home or school.
- Avoid doing anything sensitive, like logging into important accounts, while connected to an open public Wi-Fi network.

Increased Learning — 5th Grade Level:

- Introduce "evil twin" networks: fake Wi-Fi hotspots set up by an attacker with a name designed to look like a legitimate, trusted network (e.g., "Airport_Free_WiFi" instead of the real "Airport_WiFi").
- Introduce the idea of a VPN (Virtual Private Network) at a conceptual level: a tool that creates a protected, private tunnel for your internet traffic even on an untrusted network.
- Talking point: "Attackers sometimes set up a fake network with a very similar name to a real one, hoping people will connect without checking carefully. That's another reason to always confirm the exact network name with a trusted adult or staff member before connecting."

Guided Practice — 5th Grade Skill Activity

(Skill activity to complement the learning objective)

Real Network or Evil Twin?

- Students review a list of paired network names (e.g., "CityLibrary_WiFi" vs. "CityLibrary_WiFi_FREE") and identify which one is more likely to be a fake "evil twin" network set up to trick people, explaining their reasoning.

Independent Practice or Homework Handout — 5th Grade Worksheet

"Spot the Evil Twin"

- Look at 3 pairs of network names and circle the one more likely to be a fake "evil twin" network.
- Explain what a VPN does in your own words.
- Short answer: Why should you avoid logging into important accounts on public Wi-Fi?

Closure (5 minutes)

Bring the class back together and ask 2–3 volunteers to share one safe Wi-Fi habit they learned. Reinforce the key takeaway: "Trusted, password-protected networks are like a locked door — always safer than an open one. When you're unsure about a network, ask a trusted adult before connecting or doing anything sensitive." Preview that the next lesson will look at protecting personal information and data more broadly.

Assessment — 5th Grade Quiz

5 questions

1. What is an "evil twin" Wi-Fi network?
2. Why might an attacker name a fake network almost the same as a real one?
3. What is one benefit of using a VPN?
4. True or False: It is always fine to log into a banking app while connected to free public Wi-Fi.
5. Short answer: Explain, in 2–3 sentences, how you could double-check that you're connecting to the real network and not a fake one.

Answer Key (Teacher Use) — 5th Grade

1. An evil twin is a fake Wi-Fi hotspot set up by an attacker with a name designed to look like a real, trusted network.
2. So people will connect without noticing the difference, thinking they're joining the real, trusted network.
3. A VPN creates a protected, private tunnel for internet traffic, adding a layer of protection even on an untrusted network.
4. False — sensitive activities like banking should be avoided on public Wi-Fi whenever possible.
5. Open-ended — accept answers like checking the exact network name with staff, asking a trusted adult, or avoiding networks with slightly altered names.

Teacher Reflection / Notes

- What worked well in this lesson? _____
- Which grade level needed more scaffolding or support? _____
- Did students grasp the "locked door vs. open door" analogy? _____
- Adjustments for next time: _____