

Day 7 Lesson Plan: Operating Systems & Security Settings

Objective

Students will explore how operating systems provide security and learn how to locate, evaluate, and adjust key security settings on their devices.

Word Bytes

- **Permissions** – The settings that let apps or websites access parts of your device, like your camera, contacts, or location.
- **Two-Factor Authentication (2FA)** – An extra layer of security that asks for a second piece of information (like a code sent to your phone) before letting you log in.
- **Firewall** – A digital wall that helps block harmful content or hackers from getting into your device or network.

Activities

Mini-Lesson: Why OS Security Matters

- Explain how an operating system (OS) helps manage device functionality and protect users from threats. Highlight features like user permissions, automatic updates, and firewalls.

Start by asking:

“What keeps your phone or computer from being completely open to strangers or hackers?”

Guide students to understand that the operating system (OS) plays a major role in keeping devices secure.

- Key Teaching Points
 - a. **The OS as the Control Center**

Think of the operating system as the "brain" of your device. It's what allows your phone, tablet, or computer to run programs, connect to Wi-Fi, and manage files. But it also acts like a gatekeeper—deciding who gets in and what they can do.

- b. **Permission Settings**
Explain how every time an app asks to access your location, camera, microphone, or contacts, it's actually asking the OS for permission.
 - Why it matters: Apps don't always need access to everything they ask for, and saying "yes" too often can lead to privacy risks.
 - c. **Two-Factor Authentication (2FA)**
Many operating systems allow or even encourage you to turn on two-factor authentication.
 - Example: When you log into an account, you not only enter your password but also a code sent to your phone.
 - Why it matters: This extra layer makes it much harder for hackers to access your data, even if they know your password.
 - d. **Automatic Updates & Security Patches**
The OS regularly pushes out updates to fix bugs and patch security holes.
 - Why it matters: Ignoring updates can leave your device vulnerable to known threats.
 - e. **Firewalls and Built-in Protection**
The OS often includes a firewall or similar protection that monitors incoming and outgoing traffic.
 - Why it matters: A firewall can block suspicious programs or hackers from accessing your device.
- You can wrap the lesson with a quick reflection question:
"What is one OS feature you've never used but will check out later today?"

Security Settings Scavenger Hunt

- Students use classroom devices (or sample screenshots) to locate specific security settings:
 - ☐ Find and describe how to enable two-factor authentication.
 - ☐ Check where app permissions are managed.
 - ☐ Locate firewall settings or security update options.
- If classroom devices are unavailable, use the worksheet with labeled screenshots for students to annotate.

Discussion: Personal Device Safety

- In small groups, students reflect on:
 - ☐ What settings did they not know existed before?
 - ☐ What surprised them about their own or classroom device settings?
 - ☐ What will they check on their personal device later today?
-

Word Bytes Dictionary Update

Students add "**permissions**," "**two-factor authentication (2FA)**," and "**firewall**" to their Word Bytes dictionary with examples.

Suggested examples:

- Permissions – A photo app asking to access your camera.
- Two-Factor Authentication – Getting a text code to log into your email.
- Firewall – A system on your computer that blocks suspicious activity.