Teacher Guide – Packet Panic

1. Overview: What is Packet Panic?

Packet Panic is an interactive, text-based adventure built in Google Forms where students play the role of a data packet traveling through a school network. By making decisions, answering technical questions, and avoiding risks, they learn about the structure of computer networks, technical terminology, and cybersecurity.

The game offers three main network paths:

- **Ethernet** – secure and straightforward
- **Password-Protected Wi-Fi** – balanced, moderate risk
- **Public Wi-Fi** – risky, unpredictable, and entertaining

The story features three students – **Bryan**, **Chris**, and **Rasmus** – each representing a different connection type and approach to risk, speed, and security. Their personalities provide an extra layer of narrative engagement.

2. Purpose and Learning Goals

Students will learn to:

- Understand how data packets travel through a network
- Identify and explain the roles of key network components (e.g., switch, gateway, DNS, firewall)
- Interpret and apply terms such as IP address, MAC address, DHCP, TCP, TLS, IDS, and more
- Reflect on what network safety means and how things can go wrong

3. How to Use in Class

Preparation:

- Share the Google Forms link with your students
- Pro tip: Play through the game yourself first (approx. 10–15 minutes per path)
- If you use an LMS (Google Classroom, Teams, etc.), ask students to submit a screenshot of their final screen (Node 53 or error node)

Timing:

- 45–60 minutes (1–2 class periods, depending on depth)
- Recommended: Encourage students to try at least two paths

Follow-up:

- Host a group/class discussion using the questions below
- Optionally, ask for a short written reflection

4. Discussion Questions (Whole Class or Small Groups)

- What did you learn about how a network works?
- Which path did you take? How did it go?
- What surprised you the most?
- What makes a network feel safe to use?
- How can you tell when something is wrong in a real network?

5. Key Terms to Reinforce

- Packet
- IP Address
- MAC Address
- DHCP
- DNS
- Switch
- Gateway
- Firewall
- IDS / IPS
- TLS / SSL
- TCP / UDP
- Fragmentation
- Checksum

6. Game Structure and Quiz Nodes

The full game includes **53 core nodes + 9 error nodes**.

Most technical quiz questions appear on:

- Node 2, 3, 4
- Nodes 10–17 (Ethernet path)

- Nodes 20–28 (Password-Protected Wi-Fi)
- Nodes 30–39 (Public Wi-Fi)
- Nodes 50–52 (Shared ending path)

Security scan questions also appear on:

- Node 27 (Password Wi-Fi)
- Node 37 (Public Wi-Fi)

Wrong answers lead to:

- **Nodes 61–69**, depending on the error type (e.g., Packet Lost, Fragmentation Failure, Unknown Host). These nodes are now more narrative and humorous.

Final screen:

- **Node 53 – Delivery Complete** → Includes a final question: "Would you like to play again?"

7. Suggested Extensions

- Draw a map of the network as it appears in the game
- Design a new custom node for the game
- Write a fictional log message from a firewall that blocked the packet
- Create a narrative continuation (What happens to Rasmus or Ms. Tammie?)
- Link the game to real-world tools (e.g., Wireshark, ping, traceroute)
- Analyze a failed scenario and discuss what caused the error