Spondon Nath

Documented Commands / GUI Steps Used:

I used **Windows Firewall with Advanced Security** to set and test firewall rules:

1. Opened : Control Panel → Windows Defender Firewall → Advanced Settings.
2. Clicked **Inbound Rules** → **New Rule**.
3. Selected **Port**, then chose **TCP** and entered 23 (Telnet port).
4. Selected **"Block the connection"** and applied it to all profiles (Domain, Private, Public).
5. Named the rule: **Block Telnet Port 23** and clicked **Finish**.
6. To test, I opened **Command Prompt** and typed: **telnet localhost 23.**

   The connection failed as expected.
7. Finally, I went back and **deleted** the rule to restore default settings.

Summary:

- A firewall works like a gatekeeper that checks every network packet entering or leaving the system.
- It filters traffic based on **rules** we define—like port number, protocol (TCP/UDP), IP address, or direction (inbound/outbound).
- In my case, when I blocked **port 23**, the firewall automatically **dropped all incoming traffic** trying to use that port. This means even if a Telnet request was sent, my PC didn't respond—keeping the service protected.
- By controlling which ports and programs can communicate, firewalls help prevent **unauthorized access, malware spread**, or **data leaks**.