Common Types of Malware (Bad Software) and What They Do

1. Virus – The Hidden Attacker

A **virus** is like a sneaky germ that spreads when you touch an infected surface. It attaches itself to files or programs, and when you open them, the virus spreads to other files.

🔹 **Example:** You download what looks like a helpful medical app for studying, but when you open it, it infects your laptop and slows everything down.

2. Worm – The Fast Spreader

A **worm** spreads like a contagious virus, but it doesn't need you to open anything—it moves on its own through networks.

🔹 **Example:** A hospital's Wi-Fi gets infected by a worm, and suddenly, all the computers in the hospital slow down because the worm is spreading nonstop.

3. Trojan Horse – The Trickster

A **Trojan** pretends to be something useful, like a free nursing guide, but secretly allows hackers to control your device.

🔹 **Example:** You find a free "NCLEX Study Guide" online, but after downloading it, strange pop-ups appear, and your passwords start getting stolen.

4. Ransomware – The Digital Kidnapper

Ransomware locks your files and demands payment to unlock them, like a kidnapper asking for ransom.

🔹 **Example:** A nurse tries to access patient records, but a message appears: **"Your files are locked! Pay $500 in Bitcoin to unlock them."**

5. Spyware – The Silent Watcher

Spyware secretly watches what you do, tracking passwords, messages, and websites you visit.

🔹 **Example:** You log in to your nursing school portal, but spyware records your username and password and sends it to hackers.

6. Adware – The Annoying Salesperson

Adware fills your screen with unwanted ads and sometimes redirects your internet searches.

🔹 **Example:** You try to look up medical symptoms, but your browser keeps redirecting to shady websites selling fake pills.

7. Keylogger – The Password Stealer

A **keylogger** records everything you type, including passwords and private messages.

🔹 **Example:** You type your exam login details, but a hacker secretly sees every letter you type and can now log in as you.

8. Rootkit – The Invisible Intruder

A **rootkit** hides deep in the computer's system, making it nearly impossible to detect and remove.

🔹 **Example:** A hacker installs a rootkit on a hospital's main computer. Even after updating security software, the hacker still has secret access.

9. Botnet – The Army of Infected Computers

A **botnet** is a network of hacked computers controlled by an attacker to send spam, attack websites, or spread malware.

🔹 **Example:** A nurse's computer gets infected and unknowingly helps send thousands of spam emails without their knowledge.

10. Fileless Malware – The Ghost Attacker
Unlike normal malware, **fileless malware** doesn't install anything. Instead, it tricks the system into running harmful commands.
🔹 **Example:** A hacker uses a hospital's own security software to run hidden commands that give them control of the system.

11. Wiper Malware – The Eraser
Wiper malware is made to **delete** all data instead of stealing it.
🔹 **Example:** A hacker sends wiper malware to a hospital, erasing all patient records before anyone can stop it.

12. Mobile Malware – The Phone Thief
Mobile malware targets smartphones and tablets, stealing information or sending texts without permission.
🔹 **Example:** A nurse downloads a fake medication tracking app, and soon, their phone starts sending spam texts to everyone in their contacts.