CYBERSECURITY DAILY DAIRY

Day 3: Phishing Attack using CamPhish & Hack Camera (June 20, 2025)

Topics Covered:

- Camera-based phishing with **Hack-Camera**.
- Downloading hacking tools from GitHub.
- Assigning script execution permissions in Linux.
- Launching phishing attacks via terminal.
- Real-world example: capturing webcam images.
- Awareness of **social engineering risks**.

What I Did:

I learned how to do webcam-based phishing using **Hack-Camera**. It makes a fake page asking for camera access and secretly takes pictures.

Steps Performed:

1. Downloaded **Hack-Camera** from GitHub.
2. Navigated to the tool folder.
3. Switched to root user.
4. Gave execution permission to the script.
5. Ran the phishing script.
6. Chose YouTube video phishing.
7. Provided a YouTube video ID.
8. Opened the phishing link.
9. When camera access was granted: a video played, webcam images were captured and sent to the attacker's terminal/folder.

Real-World Implications:

Attackers exploit trust. Users often allow webcam access without thinking, and phishing pages can look innocent.

Key Learnings:

- GitHub is good for hacking tools.
- Linux permissions are vital for scripts.
- Shell scripts can automate attacks.
- **Social engineering** is a powerful hacker tool.

Tools Used:

- **Hack-Camera** (GitHub tool)
- **Linux Terminal (Kali)**
- **Browser** (for phishing simulation)