**🧠 FIRST Security Bootcamp – Beginner Summary**

**Source:** [FIRST.org](https://www.first.org/) – Global authority on cybersecurity incident response  
**Purpose:** Teach basic internet, cybercrime, protection, and response knowledge in simple terms.

**🌐 Part 2–5: How Does the Internet Work?**

**💡 Simple Summary:**

* The **Internet is a network of networks** — computers talk to each other using IP addresses and protocols.
* Devices connect via **routers, switches, servers**, and use **DNS** (Domain Name System) to find websites.
* Communication uses protocols like:
  + **TCP/IP** – For sending and receiving data packets
  + **HTTP/HTTPS** – For browsing websites
* When you visit a website, a **chain of devices** helps your request go from your PC → DNS → server → back to you.

**🧠 Why It Matters for Security:**

* Hackers exploit these layers (e.g., DNS hijacking, man-in-the-middle attacks).
* Knowing how traffic flows helps you find weak points (like open ports or unencrypted data).

**🕵️‍♂️ Cybercrime (Covered in 2-5 & 4-5)**

**💡 Simple Summary:**

Cybercrime = Crimes using technology, including:

| **Type** | **Example** |
| --- | --- |
| **Phishing** | Fake email asking for login/password |
| **Malware** | Virus or ransomware infection |
| **Data Breach** | Hacker steals your private info |
| **DDoS** | Attack that floods a website with traffic |
| **Identity Theft** | Criminal uses your data for fraud |

**⚖️ Cybercrime Impact:**

* Financial loss
* Reputational damage
* Legal issues
* Emotional/psychological toll

**🔐 Part 4–5: How to Protect Yourself (Basic Cyber Hygiene)**

**✅ Do This:**

| **Tip** | **Why It Helps** |
| --- | --- |
| Use **strong, unique passwords** | Prevents easy account takeover |
| Turn on **2FA (Two-Factor Authentication)** | Adds extra protection |
| Keep **software updated** | Fixes security bugs |
| Be careful of **phishing emails** | Avoid giving away credentials |
| Use **VPN on public Wi-Fi** | Encrypts your traffic |
| Regularly **backup your data** | Protects against ransomware |

🎯 Goal: Be **hard to hack** and **easy to recover**.

**💥 Part 5–5: You Got Hacked – Now What? (Incident Response)**

**🚨 What to Do After a Hack:**

1. **Stay calm** — Panic leads to mistakes.
2. **Disconnect** the affected device from the network (if possible).
3. **Report** the incident to your IT/security team or CSIRT.
4. **Preserve evidence** – Don’t delete or format!
5. **Start incident response** steps:
   * Detect what happened
   * Contain the damage
   * Eradicate the root cause (malware, account, etc.)
   * Recover and restore
   * Learn and document

**🔁 Why It’s Important:**

* Fast, smart action **limits damage**
* Proper handling ensures **legal and recovery success**
* Learning from it helps **improve defenses**

**📘 Summary Table**

| **Topic** | **Summary** |
| --- | --- |
| 🌍 Internet | Network of devices using protocols like TCP/IP, DNS |
| 💻 Cybercrime | Includes phishing, malware, identity theft |
| 🛡️ Protect Yourself | Use passwords, updates, backups, and 2FA |
| 🚨 Incident Response | Calmly contain, report, and recover from attack |