CYBER SECURITY

CYBER SECURITY

30-Day Beginner Cybersecurity Learning Plan

2025

Prepared By :

ABU SINAN

https://github.com/AbuSinann

Here's a **30-day step-by-step plan** to help you, as a beginner, build foundational skills in cybersecurity. This plan emphasizes simple, practical tasks and learning to ensure you gain confidence and real-world understanding.

Week 1: Cybersecurity Fundamentals

Day 1: Understand Cybersecurity Basics

- Learn what cybersecurity is and why it's important.
- Study the CIA Triad (Confidentiality, Integrity, Availability).
- Watch a beginner-friendly video like "What is Cybersecurity?" on YouTube.

Day 2: Common Cyber Threats

- Learn about:
    - Malware (viruses, ransomware).
    - Phishing (fake emails/websites).
    - Denial of Service (DoS) attacks.
- Use resources like Cybrary or blogs for real-world examples.

Day 3: Password Security

- Learn how to create strong passwords: at least 12 characters, with a mix of letters, numbers, and symbols.
- Practice using a password manager (e.g., Bitwarden, LastPass).

Day 4: Safe Browsing

- Understand the importance of HTTPS websites.
- Learn to identify secure sites (padlock in the browser address bar).
- Install browser extensions like HTTPS Everywhere.

Day 5-6: Basic Networking Concepts

- Learn how the internet works (IP addresses, DNS, TCP/IP).
- Watch beginner networking videos.
- Explore tools like Ping and Tracert on your computer.

Day 7: Firewalls and Antivirus

- Understand how firewalls protect networks.
- Install or ensure you have antivirus software on your devices (e.g., Windows Defender).
- Learn how to configure basic firewall settings.

Week 2: Hands-On Practice

Day 8-9: Recognizing Phishing Attacks

- Study examples of phishing emails.

- Take Google's phishing quiz.
- Learn to verify links and email headers.

Day 10-11: Introduction to Cryptography

- Learn the basics of encryption and hashing.
    - Encryption: Protects data (e.g., AES).
    - Hashing: Verifies data integrity (e.g., MD5, SHA256).
- Use online tools to encrypt/decrypt text.

Day 12: Setting Up Two-Factor Authentication (2FA)

- Enable 2FA on your email, social media, and bank accounts.
- Use apps like Google Authenticator or Authy for 2FA codes.

Day 13-14: Introduction to Wireshark

- Download and install Wireshark.
- Follow a beginner tutorial to analyze basic network traffic.
- Learn to identify protocols like HTTP and HTTPS.

Week 3: Exploring Tools and Techniques

Day 15-16: Virtual Machines and Kali Linux

- Set up a virtual machine using VirtualBox.
- Install Kali Linux, a tool used by ethical hackers.
- Explore the Kali Linux interface.

Day 17-18: Vulnerability Scanning

- Learn about vulnerability scanners like Nessus or OpenVAS.
- Use a free trial to scan a test environment.
- Identify common vulnerabilities.

Day 19-20: Introduction to Ethical Hacking

- Learn basic ethical hacking concepts.
- Use tools like Nmap to scan a local network.
- Study how penetration testers identify and report vulnerabilities.

Week 4: Advanced Topics and Practice

Day 21-22: Understanding Incident Response

- Learn the basics of responding to a cybersecurity incident:
    - Identify, Contain, Eradicate, Recover, Review.

- Study an incident response framework like NIST.

Day 23: Compliance and Regulations

- Learn about GDPR, HIPAA, or PCI DSS.
- Understand how cybersecurity ties into data protection laws.

Day 24-25: Secure Configuration

- Practice securing a device:
    - Disable unnecessary services.
    - Change default passwords.
    - Enable software updates.

Day 26-27: Explore Cloud Security

- Learn the basics of cloud platforms like AWS or Google Cloud.
- Understand common cloud threats and best practices.

Day 28: Simulate a Phishing Attack

- Use a free platform (like GoPhish) to simulate a phishing campaign.
- Analyze how users respond and learn from the data.

Final Two Days: Review and Build a Roadmap

Day 29: Review and Test Your Knowledge

- Take online quizzes to assess your understanding.
- Review key tools: Wireshark, Nmap, and password managers.

Day 30: Plan Your Next Steps

- Identify a specialization (e.g., ethical hacking, network security, cloud security).
- Enroll in a beginner certification course like CompTIA Security+ or learn more on platforms like Coursera or Cybrary.

Tips for Success

1. **Set Aside Time Daily:** Dedicate 1–2 hours every day for consistent learning.
2. **Join Communities:** Engage with cybersecurity forums like Reddit's r/cybersecurity or local meetups.
3. **Stay Updated:** Follow cybersecurity news to learn about new threats and solutions.

By following this 30-day plan, you'll build a solid foundation in cybersecurity and be ready for more advanced learning paths.