Beginner's Guide to Cybersecurity

Provider: IBM (edX)
Completion Date: May 8, 2025

Overview

This entry-level course introduced the fundamentals of cybersecurity, including threats, defenses, and best practices for personal and organizational protection. It emphasized the importance of confidentiality, integrity, and availability (CIA Triad), common attack vectors, and layered defense strategies. Hands-on labs reinforced concepts like patching, antivirus, firewalls, and encryption, providing a strong foundation for future specialization.

Key Topics Covered

- CIA Triad: confidentiality, integrity, and availability of data
- Common threats: phishing, malware, ransomware, insider threats, and social engineering
- Security best practices: password management, MFA, device hardening, and patching
- Safe browsing techniques: VPNs, browser security, and phishing detection
- Data privacy: PII, PHI, intellectual property, and regulatory compliance (HIPAA, GDPR)
- Defensive tools: Windows Defender, firewalls, encryption, and antivirus labs
- Case studies: Yahoo, Equifax, Court Ventures, T-Mobile breaches

Practical Applications

- Recognizing and responding to phishing, malware, and social engineering attacks
- Configuring firewalls, antivirus, and Windows updates for system protection
- Creating and enforcing strong password and authentication policies
- Safeguarding confidential data with encryption and access controls
- Applying layered defense for resilience against breaches and outages

Personal Reflection

This course gave me a strong foundation in cybersecurity essentials and hands-on practice with core defensive tools. I gained confidence in identifying threats, hardening systems, and protecting sensitive data. These fundamentals strengthen my readiness for compliance and risk management work, where a solid grasp of security basics is essential.