MARCH EVENTS

MAR 4	**ACADEMY UP: CLOUD FOUNDATIONS** 6:00pm to 8:00m Kenneth C Rowe Management Building
MAR 4	**SHIFTKEY LOUNGE: ENTREPRENEURSHIP** 6:00pm-7:00pm Goldberg Computer Science Building
MAR 5	**ACADEMY UP: PRACTICAL CYBERSECURITY** 6:00pm to 8:00pm Kenneth C Rowe Management Building
MAR 6	**WOMEN'S EXCELLENCE GALA** 5:00pm to 7:00pm Dalhousie Student Union Building
MAR 12	**INDUSTRY SHOWCASE: AVANADE** 4:00pm to 5:30pm Goldberg Computer Science Building
MAR 12	**ACADEMY UP: PRACTICAL CYBERSECURITY** 6:00pm to 8:00pm Kenneth C Rowe Management Building
MAR 13	**INDUSTRY SHOWCASE: RBC** 4:00pm to 5:30pm Goldberg Computer Science Building
MAR 15	**SNOWBALL AWARDS** 5:00pm to 11:30pm The Westin Nova Scotian
MAR 17	**HAPPY SAINT PATRICK'S DAY**
MAR 18	**SHIFTKEY LOUNGE: FINTECH** 6:00pm to 7:00pm Goldberg Computer Science Building
MAR 19	**ACADEMY UP: PRACTICAL CYBERSECURITY** 6:00pm to 8:00pm Kenneth C Rowe Management Building
MAR 20	**SPEECH CRAFT WORKSHOP** 5:30pm to 8:30pm Goldberg Computer Science Building
MAR 22	**CONSULTING 101 WORKSHOP** 1:00pm to 5:00pm Goldberg Computer Science Building
MAR 24	**ALUMNI SPEAKS: ANDRES COLLART** 4:00pm to 5:30pm Goldberg Computer Science Building
MAR 26	**ACADEMY UP: PRACTICAL CYBERSECURITY** 6:00pm to 8:00pm Kenneth C Rowe Management Building
MAR 28	**INDUSTRY SHOWCASE: VOLTA** 4:00 pm to 5:30pm Goldberg Computer Science Building

Practical Cybersecurity

Instructor – Aman Bhalla

Course Syllabus

Week 1: Introduction to Cybersecurity

- What is cybersecurity, and why does it matter?
- Common cyber threats (malware, phishing, ransomware).
- Understanding attack vectors (social engineering, network attacks).

Hands-on Activity: Phishing Email Analysis.

Week 2: Network & Data Security

- Basics of firewalls, intrusion detection, and secure communication.
- Encryption fundamentals (symmetric vs. asymmetric).
- Best practices for authentication (MFA, password security).

Hands-on Activity: Team Activity (TBA)

Week 3: Application Security & Cyber Defense

- Secure software development practices & common vulnerabilities.
- OWASP Top 10 (SQL Injection, Cross-Site Scripting).
- Incident response planning & threat intelligence basics.
- Cybersecurity Frameworks

Hands-on Activity: Web Application Scanning with OWASP ZAP.

Week 4: Ethical Hacking & Exam Prep

- Basics of penetration testing & reconnaissance techniques.
- Cyber laws, ethical responsibilities in hacking.

Hands-on Activity: Reconnaissance Exercise & Case Study.

- Exam format overview & revision session.

Course Schedule & Assessment

Course Meeting Schedule:

- **Time:** Wednesdays, **6:00 - 8:00 PM**
- **Location: Rowe 1020**

Session Dates:

- **Week 1:** March 5th
- **Week 2:** March 12th
- **Week 3:** March 19th
- **Week 4:** March 26th

Final Assessment (April 2nd)

- The **final assessment** will be held **in-person**.
- Exam format: **MCQs, Short Answer, and Long Answer Questions**.
- More details on the exam structure will be announced in Week 4.

Important Notes:

- Attendance is **highly recommended** to maximize learning.
- **Minimum of 3** sessions need to be attended to qualify for the certification.
- Hands-on activities will **directly help in assessment preparation**.
- Reach out if you have **any questions** or **need extra resources!**

Grade Breakdown

Assessment Components:

Lecture Quizzes (4 total) (Held Every Week)

- Each quiz is worth **2.5%**
- Total: **10%**

Team Assignment (In-Class, Week 2)

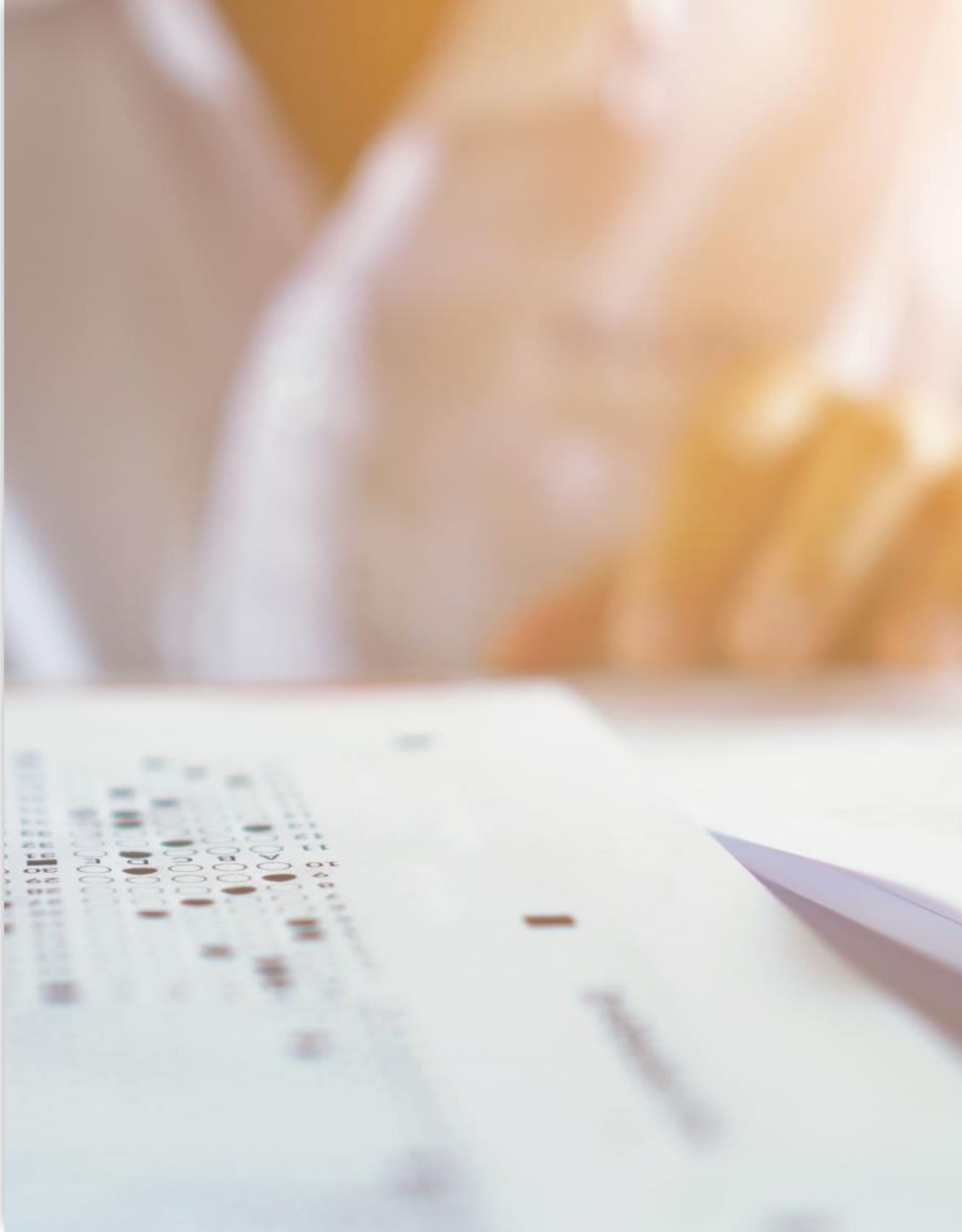
- Worth **10%**

Final Exam (In-Person on April 2nd)

- Worth **80%**

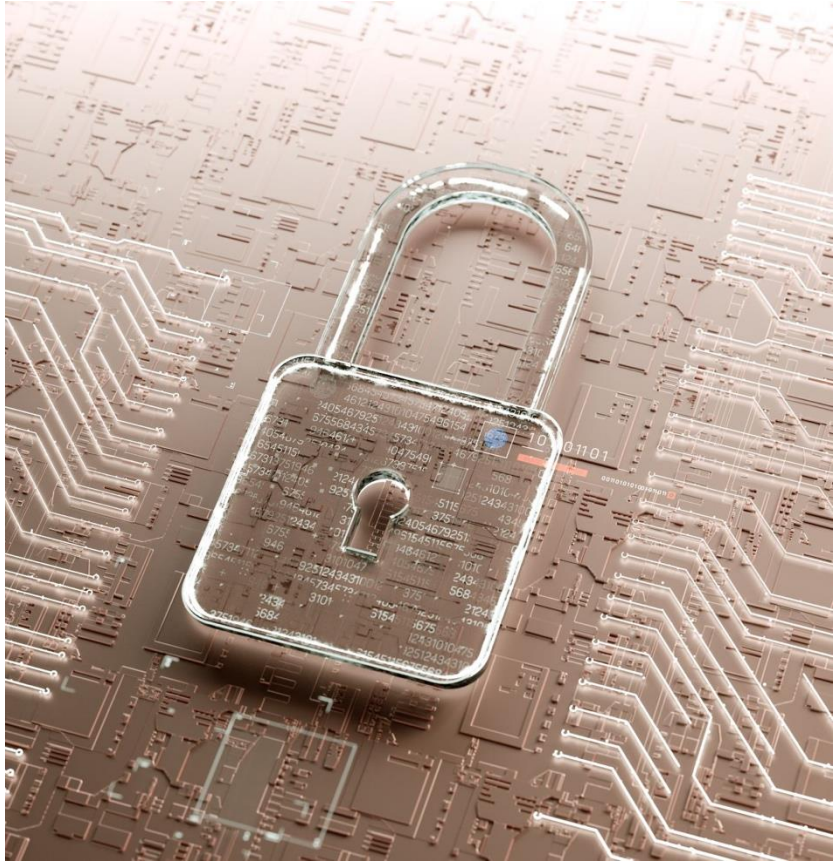
Course Passing Requirement:

- **Minimum passing percentage: 80%**



What is Cybersecurity?

- Cybersecurity is the practice of **protecting networks, devices, and data** from unauthorized access, attacks, and damage. It ensures that information remains **confidential, accurate, and accessible** to authorized users. At its core, cybersecurity is built on the **CIA Triad**:
- **Confidentiality:** Only authorized users can access sensitive data.
- **Integrity:** Ensuring data is not altered or tampered with by unauthorized users.
- **Availability:** Keeping data and systems functional and accessible at all times.

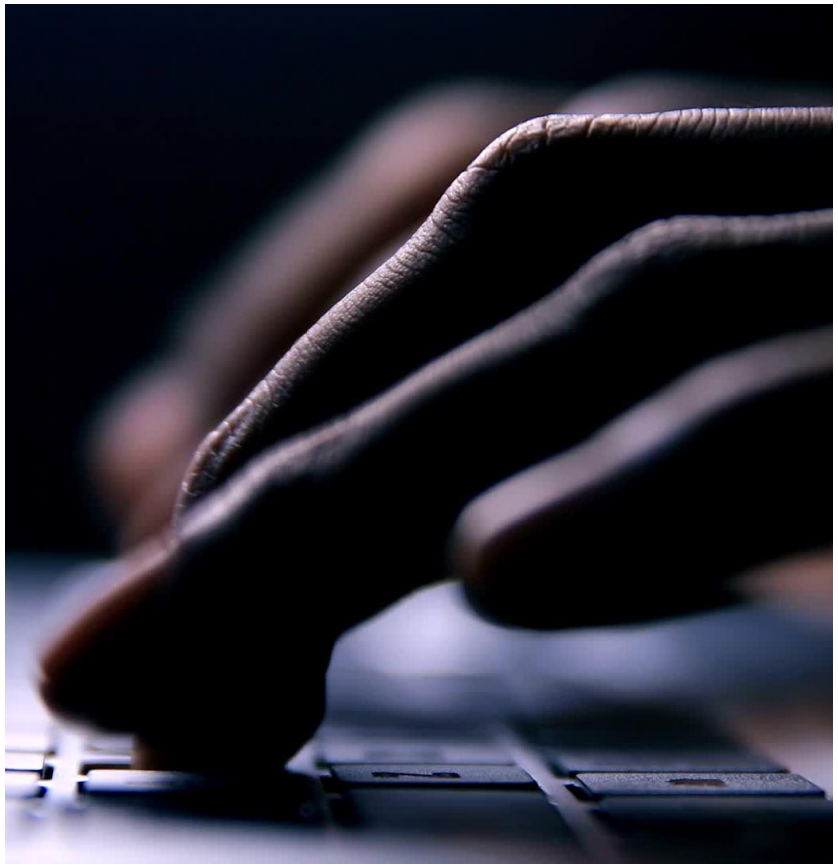


Why Cybersecurity Matters?

Cybercrime is a growing global threat, affecting businesses, governments, and individuals. In **2023** alone**, cybercrime cost the world over $8 trillion**. Common attacks include **data breaches, ransomware, and fraud** that lead to financial losses and reputational damage.

- Every **39 seconds**, a cyberattack occurs worldwide.
- **Over 80% of hacking attacks** exploit weak passwords or outdated software.
- **Small businesses are frequent targets**—60% go bankrupt within six months of a major cyberattack.

Example: In 2021, the **Colonial Pipeline ransomware attack** shut down the U.S. fuel supply, showing the **real-world consequences of poor cybersecurity.**



Common Cyber Threats

There are various types of **cyber threats** that individuals and organizations face:

- **Malware:** Malicious software that infects systems (e.g., viruses, trojans, worms).
- **Phishing:** Deceptive emails that trick users into providing sensitive information.
- **Ransomware:** Hackers encrypt data and demand payment for decryption.
- **Man-in-the-Middle (MITM) Attacks:** Cybercriminals intercept communication between two parties to steal data.

Phishing Attacks – The Silent Threat

Fake emails impersonating trusted sources

Phishing Attacks – The Silent Threat

Fake emails impersonating trusted sources

Suspicious links leading to credential theft

Phishing Attacks – The Silent Threat

Fake emails impersonating trusted sources

Suspicious links leading to credential theft

Poor grammar, urgent requests, and unknown senders are warning signs

Phishing Attacks – The Silent Threat

Fake emails impersonating trusted sources

Suspicious links leading to credential theft

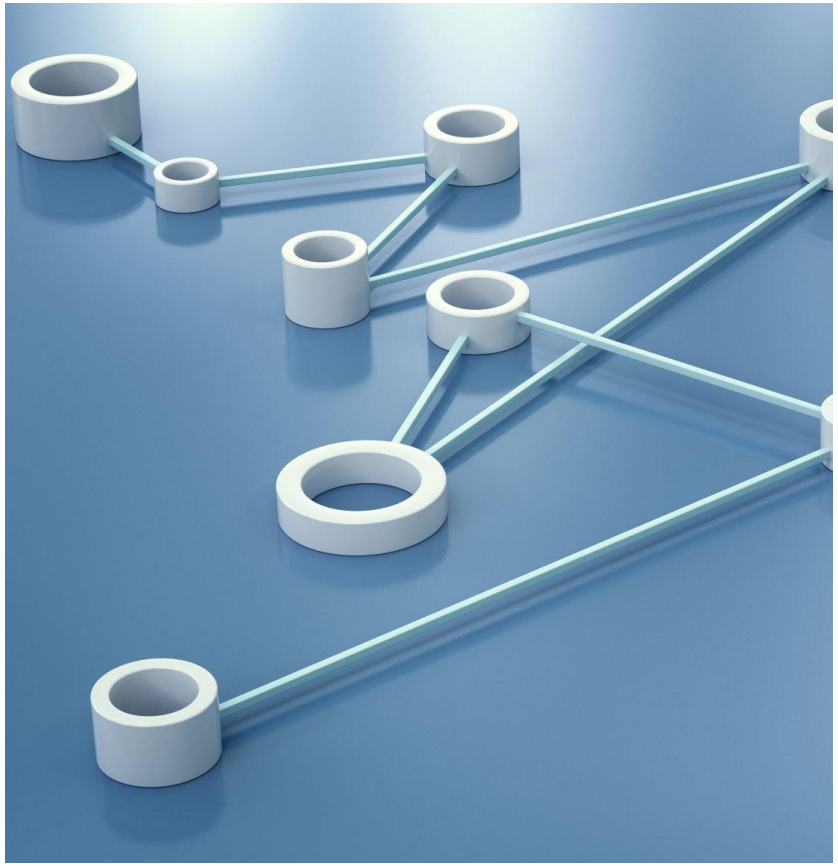
Poor grammar, urgent requests, and unknown senders are warning signs

Example: “Your account is locked! Click to verify”

Practical Activity – Phishing Email Analysis

- Visit **Google's Phishing Quiz** and analyze sample emails.
- Identify **red flags** like **fake domains, urgency, and typos**.

Link to website: https://phishingquiz.withgoogle.com

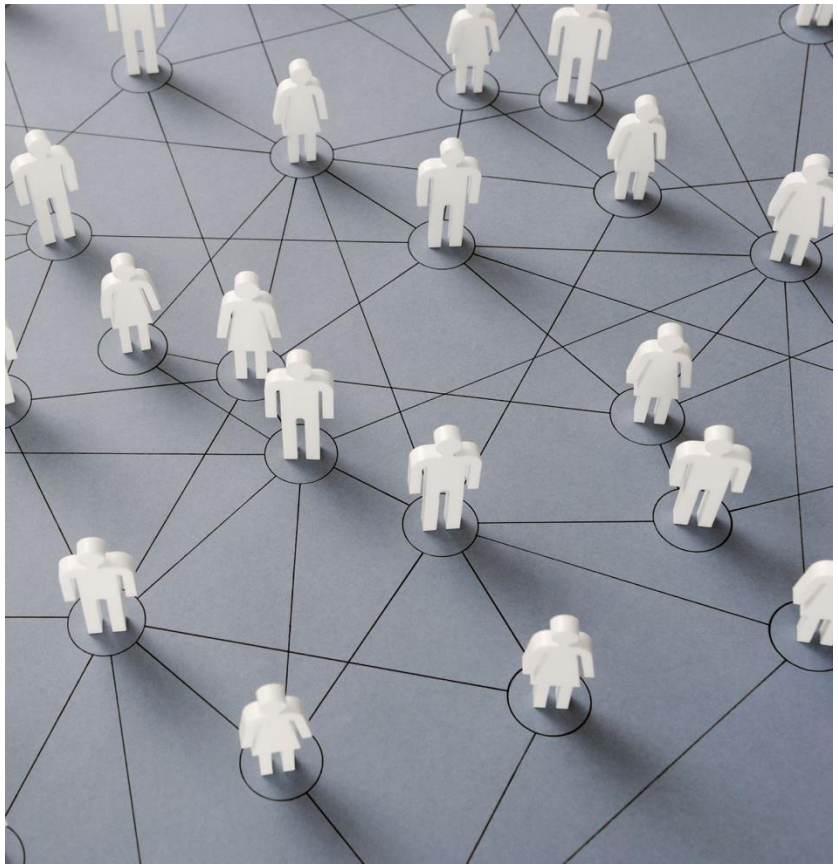


Understanding Attack Vectors

Attack vectors are **entry points that hackers use to exploit vulnerabilities**:

- **Social Engineering:** Manipulating people into revealing passwords or installing malware.
- **Network-Based Attacks:** Exploiting weak Wi-Fi security and unpatched systems.
- **Insider Threats:** Employees or contractors intentionally or accidentally leaking data.

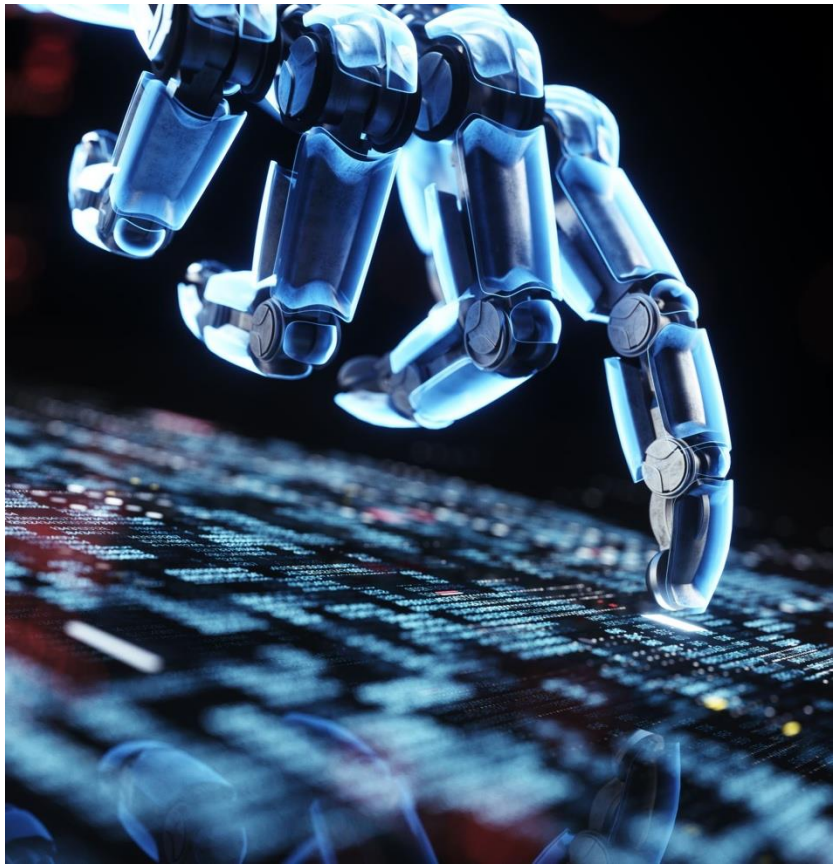
Example: A hacker pretending to be IT support calls an employee, claiming they need to reset their password. If the employee shares their credentials, the attacker gains access.



Cybersecurity Best Practices

- **Use Strong, Unique Passwords** – A mix of uppercase, numbers, and special characters.
- **Enable Multi-Factor Authentication (MFA)** – Extra security beyond passwords.
- **Avoid Clicking Suspicious Links** – Always hover over links before clicking.
- **Keep Software Updated** – Security patches prevent attacks.

Example: 81% of hacking-related breaches are due to **weak or stolen passwords**.



Discussion & Q&A

What is the biggest cybersecurity threat you have encountered?

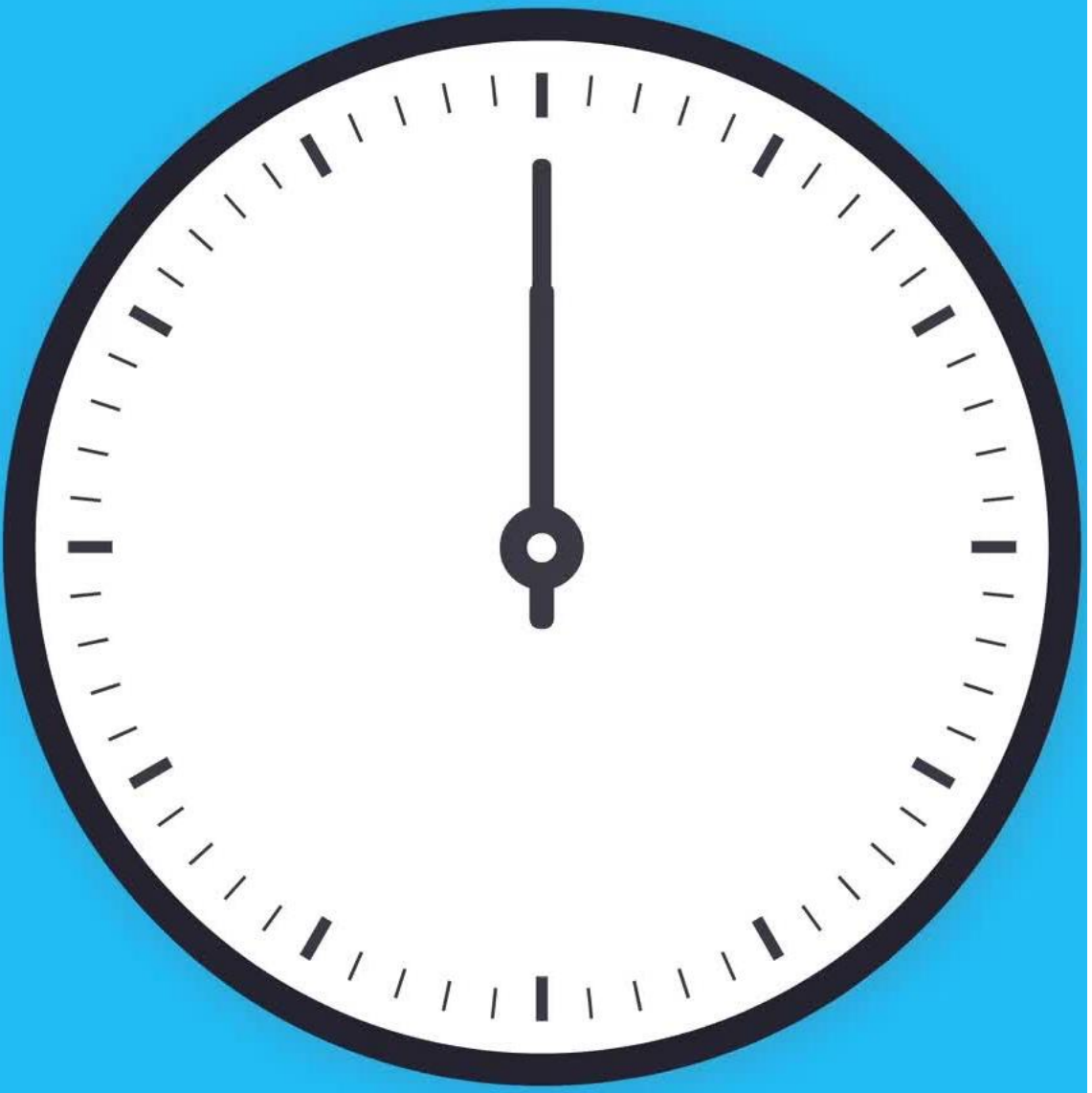
How do you protect yourself online?

Have you or anyone you know faced a cyber attack?

Key Takeaways

- Cybersecurity is **a global concern** affecting businesses & individuals.
- **Phishing, malware, and ransomware** are major security threats.
- **Attack vectors** include social engineering, network vulnerabilities, and insider threats.
- **Awareness, strong passwords, and multi-factor authentication** are key to online safety.

Final Thought: Cybersecurity isn't just an **IT issue—it's a life skill** in today's digital world.



Quiz Time!

- Time Limit – 15 Minutes. Quiz begins at 7:45 pm and will close at 8:00 pm.
- Questions: MCQ’s, True or False and Short Answer.

Next Week Preview

Preview of Week 2 Topics:

- **Firewalls & Intrusion Detection Systems (IDS/IPS)** – Blocking cyber threats.
- **Secure Communication Protocols (HTTPS, SSL/TLS)** – Keeping data safe online.
- **Encryption & Hashing Basics** – Protecting sensitive data.

Next week, we'll talk about what tools hackers may use to crack passwords and how we can use encryption to keep data secure.