

TASK 1 – INTRODUCTION VIDEO

Video Link:

<https://drive.google.com/file/d/1LJcdHT21ijYohBkvoerCJorcBQhmt9BH/view?usp=drivesdk>

TASK 2 – LEARN CYBER SECURITY BASICS

Task 2 - 10 Important Cybersecurity Concepts (Detailed Explanations). Here are 10 crucial cybersecurity concepts you need to understand:

1. Malware (Malicious Software)

Malware is any software intentionally designed to damage, disrupt, or gain unauthorized access to computer systems. Types include:

- **Viruses:** Self-replicating programs that attach to other files
- **Trojans:** Disguised as legitimate software but perform malicious actions
- **Ransomware:** Encrypts files and demands payment for decryption
- **Spyware:** Secretly monitors and collects user information
- **Prevention:** Use antivirus software, avoid suspicious downloads, keep systems updated

2. Phishing

Fraudulent attempts to obtain sensitive information by impersonating trustworthy entities via email, text, or fake websites.

- **Common tactics:** Fake login pages, urgent payment requests, lottery scams
- **Red flags:** Poor grammar, suspicious URLs, urgent language, unexpected attachments
- **Prevention:** Verify sender identity, check URLs carefully, never click suspicious links

3. Firewalls

Network security systems that monitor and control incoming/outgoing network traffic based on predetermined security rules.

- **Types:** Hardware firewalls (router-based), Software firewalls (OS-based)
- **Function:** Acts as a barrier between trusted internal networks and untrusted external networks
- **Benefits:** Blocks malicious traffic, prevents unauthorized access, monitors data flow

4. Encryption

Process of converting readable data into coded format to prevent unauthorized access.

- **Symmetric encryption:** Same key for encryption and decryption (AES)
- **Asymmetric encryption:** Different keys for encryption/decryption (RSA)
- **Applications:** HTTPS websites, secure messaging, file protection, VPNs

5. Ethical Hacking (White Hat Hacking)

Authorized practice of bypassing system security to identify vulnerabilities and strengthen defenses.

- **Purpose:** Find security weaknesses before malicious hackers do
- **Methods:** Penetration testing, vulnerability assessments, security audits
- **Certifications:** CEH (Certified Ethical Hacker), CISSP, OSCP

6. Social Engineering

Psychological manipulation techniques used to trick people into divulging confidential information or performing actions that compromise security.

- **Techniques:** Pretexting, baiting, quid pro quo, tailgating
- **Examples:** Fake IT support calls, USB drops in parking lots, impersonation
- **Defense:** Security awareness training, verification procedures, healthy skepticism

7. Two-Factor Authentication (2FA)

Security process requiring two different authentication factors to verify user identity.

- **Factors:** Something you know (password), something you have (phone), something you are (biometric)
- **Methods:** SMS codes, authenticator apps, hardware tokens, biometrics
- **Benefits:** Significantly reduces risk of unauthorized access even if passwords are compromised

8. VPN (Virtual Private Network)

Creates secure, encrypted tunnel between your device and VPN server, masking your IP address and location.

- **Benefits:** Privacy protection, data encryption, bypass geo-restrictions, secure public Wi-Fi usage
- **Use cases:** Remote work, accessing restricted content, protecting sensitive data
- **Considerations:** Choose reputable providers, understand logging policies

9. Data Breach

Unauthorized access to confidential, sensitive, or protected information, often resulting in data exposure or theft.

- **Common causes:** Weak passwords, unpatched vulnerabilities, insider threats, phishing
- **Impact:** Financial loss, identity theft, reputation damage, legal consequences
- **Prevention:** Regular security audits, employee training, incident response plans, data encryption

10. Cybersecurity Frameworks

Structured guidelines and best practices for managing cybersecurity risks and implementing security controls.

- **NIST Framework:** Identify, Protect, Detect, Respond, Recover
- **ISO 27001:** International standard for information security management
- **Benefits:** Systematic approach, compliance requirements, risk management, continuous improvement

TASK 3 – BASIC CYBER SECURITY PRACTICES

Task 3 - Strong Passwords & Encryption Tools. 5 Strong Passwords (Following Security Rules):

1. Tr@il\$_Mountain2024!
2. Cyber\$ecurity#2025
3. MyP@ssw0rd_Strong!
4. Secur3_N3tw0rk@2024
5. H@ck3r_Pr00f#2025

Encryption/Decryption Websites:

- **Base64 Encoding/Decoding:** <https://www.base64encode.org/>
- **Caesar Cipher:** <https://cryptii.com/pipes/caesar-cipher>
- **Multi-tool Encryption:** <https://www.browserling.com/tools/text-encrypt>
- **AES Encryption:** <https://aesencryption.net/>

Encode to Base64 format

Simply enter your data then push the encode button.

hi today is my birthday!

To encode binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8

Destination character set.

LF (Unix)

Destination newline separator.

☐ Encode each line separately (useful for when you have multiple entries).

☐ Split lines into 76 character wide chunks (useful for MIME).

☐ Perform URL-safe encoding (uses Base64URL format).


☒ Live mode OFF

Encodes in real-time as you type or paste (supports only the UTF-8 character set).


> ENCODE <

Encodes your data into the area below.

aGkgdG9kYXkgXm9kaXkgYmlydChkYXkh

 cryptii

Visibility matters

 Students and Teachers, save up to 60% on Adobe Creative Cloud.

VIEW

+

Plaintext

If he had anything confidential to say, he wrote it in cipher, that is, by so changing the order of the letters of the alphabet, that not a word could be made out.

ENCODE DECODE

+

Caesar cipher

SHIFT

- 7 a→h +

ALPHABET

abcdefghijklmnopqrstuvwxyz

CASE STRATEGY

Maintain case

FOREIGN CHARS

Include Ignore

→ Encoded 163 chars

VIEW

+

Ciphertext

Pm ol ohk hufaopun
jvumpkluaphs av zhf, ol dyval
pa pu jpwoly, aoha pz, if zv
johunpun aol vykly vm aol
slaalyz vm aol hswohila, aoha
uva h dvyk jvbsk il thkl vba.

Windows Security

←

☰

🏠

🛡️

👤

🗨️

📁

📄

📧

🔍

⚙️

Virus & threat protection

Protection for your device against threats.

🛡️ Current threats

No current threats.
Last scan: 23/08/2025 11:39 am (quick scan)
0 threat(s) found.
Scan lasted 3 minutes 13 seconds
39711 files scanned.

Quick scan

[Scan options](#)
[Allowed threats](#)
[Protection history](#)

⚙️ Virus & threat protection settings

No action needed.

[Manage settings](#)

TASK 4 – INTERMEDIATE SECURITY TASK

Task 4 - WHOIS Lookup Report. Recommended WHOIS Lookup Tools:

- Website: <https://who.is/>
- Alternative: <https://www.whois.net/>

Registrar Information	
Registrar HOSTINGER operations, UAB	WHOIS Server whois.hostinger.com
Referral URL http://www.hostinger.com	
Important Dates	
Created 2/5/2025	Updated 4/7/2025
Expires 2/5/2026	

1. Domain Information

Domain Name	youngdevinterns.net
Registrar	HOSTINGER operations, UAB
WHOIS Server	whois.hostinger.com
Referral URL	https://www.hostinger.com
IP Address	147.93.42.193
Creation Date	5 February 2025
Updated Date	7 April 2025
Expiration Date	5 February 2026

2. Registrant Information

Name	Domain Admin
Organization	Privacy Protect, LLC (PrivacyProtect.org)
Address	Burlington, MA, US
Phone	+1.8022274003
Email	contact@privacyprotect.org

3. Technical Details

Name Server	ns1.dns-parking.com (162.159.24.201)
Name Server	ns2.dns-parking.com (162.159.25.42)
Domain Status	clientTransferProhibited
DNSSEC	Not enabled

TASK 5 – MINI CYBER SECURITY PROJECT

Task 5 - Password Strength Checker Web Application

GitHub: <https://github.com/umair-aziz025/youngdev-internship-tasks>