① a) **Firewall :-**

A firewall is a network security device that monitors incoming and outgoing network traffic and permits or blocks data packets based on a set of security rules. Its purpose is to establish a barrier between your internal network and incoming traffic from external source such as internet in order to block malicious traffic like viruses and hackers.

b) **Brute Force Attack :-**

It occurs when a bad actor attempts a large amount of combinations on a target. These attacks frequently involve multiple attempts on account password with the hopes that one of them will be valid. Its a bit like trying all of the possible on a padlock but on a much larger scale.

How To Prevent :-

i) Always use strong passwords.
ii) Restrict access to authentication URLs
iii) limit login attempts.
iv) Use Captchas
v) Use Two-Factor Authentication

c) Some Cyber Attacks are &

i) Dos & DDos Attack
ii) MITM Attack
iii) Phishing Attacks
iv) Ransomware Attack
v) Password Attack
vi) SQL Injection Attack
vii) URL Interpretation
viii) DNS Spoofing
ix) Session Hijacking
x) Brute force Attack
xi) Web Attacks
xii) Trojen Horses

d) Role of CCleaner &

i) Remote optimizations of endpoints.
ii) Auditing of endpoint health
iii) Remote problem solving
iv) Scheduled cleaning and defragmentation.
v) Granular Control of cleaning rules.
vi) Simple one point deployment onto endpoints
vii) Highly secure endpoint agent and encrypted communications
viii) Built in reporting and auditing tools with data export

e) Cyber Space &

It refers to the virtual space and more specifically an electronic medium that is used to facilitate online communication Cyber space involves a large computer network made up of many world wide computer subnetworks that employ TCP/IP protocol to aid in communicati and data exchange activities

(2) a) **Password Manager :**

It is an advanced tool that helps individuals and businesses securely store and manage all of their login credentials. This tool is commonly used to generate strong, unique passwords for web applications. Once generated, they are put in a centeralized vault and encrypted with one master password. Users only need to remember one password to access their services. Based on the end users needs, we can categorize password mangers into three different groups.

- For individuals
- For Teams and families
- For Enterprises

Role Of Password Manager :

- Aside from basic password storge functions, individuals use password managers to automatically fill out forms, provide login credentials and enforce strong password policies.
- Teams and families use password manager to securely share passwords for commonly used web services like Netflix, Amazon, loyal

3/14

program accounts and other web applications.

- Enterprises use password managers to securely share commonly used IT service and web application accounts, implement advanced workflow mechanisms and keep comprehensive audit trails and reports.

b) Cyber Security Assurance &

Are you confident that you have the cyber security counter measures in place? Deploying sensible countermeasures can be an arduous and time consuming task for any organization. Formal or informal security assurance or certification can provide the extra layer of confidence to you and your stakeholders, demonstrating you are in alignment with best practice.

If your organization is looking to establish a systematic, risk based approach to cyber security then our experts can help. We can conduct a comprehensive risk assessment covering processes, systems and assets.

Benefits Of Cyber Security Assurance &

- Alignment with best practice.
- Improving stackholder confidence.
- Reducing operational risk following a cyber attack.
- Avoiding the exploitation of known or unknown vulnerabilities.
- Brand protection.

(3) Guideline For Secure Password &

Choosing the righ password is something that many people find difficult, there are so many things that requires passwords these days that remembering them all can be a real problem. Perhaps because of this a lot of people choose their passwords very badly. The simple tips below are intended to assist you in choosing a good password.

Basic Guideline &

- Use at least eight characters, the more characters the better really, but most people will find anything more than about 15 characters difficult rement

- Use a random mixture of characters, upper and lower case, numbers, punctuations, spaces and symbols
- Dont use a word found in a dictionary.
- Never use the same password twice.

Things To Avoid &

- Dont just add a single digit or symbol before or after a word ~~Example~~ 'apple1'
- Dont just double up a single word. Example 'apple apple'.
- Dont just simply reverse a word. Example 'elppa'
- Dont just simply remove the vowels. Example 'ppl'
- Key sequences that can easily be repeated Example 'qwerty', 'asdf' etc.
- Dont just garble letters. Example Converting e to 3, l or i to 1 and o to 0.

6/14

Two Step Authentication &

It is an additional layer of security that you can add onto your Gmail account. This is how you enable two step verification on gmail.

i) With this enabled, a code will be sent to your phone. You then enter code in sign in prompt in order to sign in.
ii) log into your gmail account
iii) Go to setting and click sign-in & security.
iv) Now, select 2-step Verification.
v) Click Get Started It's a blue button on the page.
vi) Enter your google account password. This step is to confirm your identity with google before continuing.
vii) Click Sign in. Doing so will confirm your identity and take you to the next page.
viii) Enter your phone number. Do so in the text field below the 'What phone number do you want to you'.
ix) Click a code option. You can select Text meaesge to receeve a code.
x) Click Next. Doing so will prompt Google to send a code to you.
xi) Retrieve your code from Google.
xii) Type in your code in text field.

7/14

x(iii) Click on the Next Button.

x(iv) Now, click TURN ON By clicking it will enable two step verification for your Google account.

(4) a) Role of Information Security :-

It is not only about securing information from unauthorized access. It is basically the practice of preventing unauthorized access, use, disclosure, distruption, modification, inspection, recording of information.

Objectives :-

- Confidentiality :-

It means information is not disclosed to unauthorize individuals, entities and process. For example if we say i have password for my Gmail account but someone saw while i was doing a login into Gmail account In that case my password has been compromised and Confidentiality has been breached.

- Integrity :-

It means maintaining accuracy and completeness of data. This means data cannot be edited in an unauthorized way. If an employee leaves an

8/14

organization then in that case data for that employee in all departments like accounts should be updated to reflect status to Job left so that data is complete and accurate and in addition to this only authorized person should be allowed to edit employee data.

- Availability :-
  It means information must be available when needed If one needs to access information of a particular employee to check whether employee has outstanded the number of leaves, in that case it requires collaboration from different organizational teams like network operations development operation, incident response and policy change

b) Ethical Issues :-

- Should you read the private e-mail of your network users just because you can. Is it OK to read employee's e-mail as a security measure to ensure that sensitive company information isn't being disclosed? Is it OK to read employee's e-mail to ensure that company rules aren't being violated

9/14

If you do read employee's e-mail should you disclose that policy to them? Before or after the fact.

- Is it OK to monitor the web site visited by your network users? Should you routinely keep logs of visited sites? Is it negligent to not monitor such internet usage, to prevent the possibility of something in the workplace that could create a hostile work environment?

- Is it OK to place key loggers on machines on the network to capture everything the user types? What about screen capture programs so you can see everything that's displayed? Should users be informed that they are being watched in this way.

- Is it OK to read the documents and look at the graphics files that are stored on users computers or in their directories on the file server.

These are some ethical issues which are posed by computer security.

10/14

(3) a) Security for Micro Atm &

i) Before using micro atm, ensure that there are no strange objects in the insertion panel of Atm.
ii) Change micro atm pin on regular basis.
iii) Cover the pin pad while entering PIN.
iv) Do not disclose micro atm pin number to anyone.
v) Do not accept the card recieve directly from bank in case of it is damaged or seal is open
vi) In case of any suspected transaction or loss of cards contact bank.

b) Security for Point of Sales &

i) Use an i-pad for point of sale
ii) Use end to end encryption.
iii) Intall the antivirus on the Point Of Sale System.
iv) Avoid connecting your Point of Sale to external networks.
v) Do payment card industry data security standard (PCI-DSS) complaint from top to bottom.
vi) Use username and passwords with remote access which are unique to every user.

11/14

c) Security For Social Engineering :-

i) Set spam filters to high.
ii) Never use same passwords for the different accounts.
iii) Use two-factor or multi-factor authentication on your account.
iv) Keep changing your account password on a monthly basis.
v) Educate your employees about social engineering threats and help them exercise the necessary caution.
vi) Delete any request for financial information or password.
vii) Reject all the requests for help or offer of help.

d) Security For E-Commerce :-

i) Choose a very secure e-commerce platform.
ii) Implement SSL (Standard for Securing online Transactions) Certificate.
iii) Consider Two-Factor Authentication.
iv) Use a virtual private network.
v) Educate your customers and the employees.
vi) Use all the security protocols on your platform like - HTTPS, Transfer Layer Security, Secure sockets layer authentications.

e) I Security for Android :-

i) You should have full access to your phone.
ii) You should use encryption in your device to secure.
iii) Secure your network settings
iv) You should hide your caller id of the device
v) You should keep checking the software update and install them.

II Security for IOS :-

i) Turn off the autofill option in your browsers.
ii) Use a strong password instead of a 4-digit code.
iii) Turn on two-step verification for apple id and i-cloud.
iv) Start using virtual private network.
v) Turn off cookies in the browser.
vi) Keep your system and apps updated.

(6) Ransomware :-

It is a malware that employs encryption to hold a victim's information at ransom. A user or organization's critical data is encrypted so that they cannot access files, databases or applications. A ransom is

then demanded to provide access. Ransomware is often designed to spread across a network and target database and file servers and can thus quickly paralyze an entire organization. It is growing threat, generating billions of dollars in payment to cyber criminals and inflicting significant damage and expenses for businesses and government organizations.

Ransomware Spreading :-

- Easy availability of malware kits that can be used to create new malware samples on demand.
- Use of knowledge good generic interpreter to create cross platform ransomware.
- Use of new techniques, such as encrypting the complete disk instead of selected files.