Securing the Home Network

The main goals of securing the home network:
1) Preventing unauthorized users from joining the network
2) Preventing others from seeing the network traffic

Steps to secure the network

Strong Wi-Fi Password	Change the default password to a unique, complex one
Enable Encryption	Use WPA3 or WPA2 for secure Wi-Fi.
Update Firmware	Regularly update your router’s firmware for security patches.
Use Newer Hardware	Upgrade to a modern router/modem for better security and performance.
Create a Guest Network	Isolate guest users to prevent access to your main network.
Secure IoT Devices	Use strong, unique passwords and update firmware regularly
Enable Firewall	Configure your router's firewall to block unwanted traffic

Cybersecurity Awareness

We must all learn about cybersecurity to protect ourselves and our agencies. Continuous education on cyber threats, risks, and best practices is essential.
We all have a responsibility to learn about emerging threats. By doing so, we can:
1) Prevent incidents proactively
2) Identify vulnerabilities in systems
3) Adapt training, plans, and policies as needed

Incident Detection and Response

In the context of cybersecurity, an incident is an abnormal event that might impact an organization's or agency's normal operations.

Firewall

Firewalls are barriers between trusted networks and untrusted networks.
Firewall rules:
1) Deny traffic from certain network addresses or geographic regions
2) Deny services, ports, and applications
3) Allow traffic from trusted networks

Data backup

Data backup involves creating copies of digital data and storing them in a different system or location.

Data backup strategies

Incremental Backup	Only new or modified data is backed up, saving time and disk space. Ensures you always have the latest version of your data.
Full Backup	Copies all data and allows restoring different versions as needed.to the backup location. Can quickly consume storage if old backups aren’t deleted.

Cloud provider for data Backups

Recommendations while using a cloud provider for backups:
1) Use a Strong Password – Protect cloud access with a complex, unique password.
2) Limit Access – Restrict data sharing to authorized users only.
3) Encrypt Before Uploading – If possible, encrypt data for added security.
4) Monitor Usage – Track cloud activity to detect unauthorized access.

Anomalies or odd behaviors

Traffic from Unkown Network Addresses	Multiple Failed Login Attempts
Increased Network Bandwidth Usage	Suspicious Emails and Phone Calls
Unlocked Secure Areas	Deleted or Altered Files
Unusual Activities During Off-hours	New Users and Devices in the Network