# Unit-8
# Social Service and Community Development

## SS-7
## *Cyber and Mobile Security*

# CYBER SECURITY

Cyber security refers to the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access. Cyber security may also be referred to as information technology security. Cyber Security is all about protecting your devices and network from unauthorized access or modification. The Internet is not only the chief source of information, but it is also a medium through which people do business.


# Types of Cyber Security

Cyber Security is classified into the following types:

(a) Information Security: Information security aims to protect the users' private information from unauthorized access, identity theft. It protects the privacy of data and hardware that handle, store and transmit that data.

(b) Network Security: Network security aims to protect the usability, integrity, and safety of a network, associated components, and data shared over the network. When a network is secured, potential threats gets blocked from entering or spreading on that network.

(c) Application Security: Application security aims to protect software applications from vulnerabilities that occur due to the flaws in application design, development, installation, and upgrade or maintenance phases.

# Threats and Challenges

## Threats

(a) Viruses
(b) Password Attacks.
(b) Spyware and Key loggers.
(c) Adware.
(d) Trojans.
(e) Ransom ware

## Challenges

(a) Network security
(b) Application security
(c) Endpoint security
(d) Data security
(e) Identity management
(f) Database and infrastructure security
(g) Cloud security
(h) Mobile security
(i) End-user education

# MOBILE SECURITY

**Introduction**:
There are three prime targets for attackers for mobile devices:

(a) **Data:** Smart phones are devices for data management, and may contain sensitive data like credit card numbers, authentication information, private information, activity logs (calendar, call logs)
(b) **Identity:** Smartphone's are highly customizable, so the device or its contents can easily be associated with a specific person. For example, every mobile device can transmit information related to the owner of the mobile phone contract, and an attacker may want to steal the identity of the owner of a smart phone to commit other offenses;
(c) **Availability:** Attacking a smart phone can limit access to it and deprive the owner of its use.

# Precautions:

(a) Use strong passwords/biometrics.
(b) Ensure public or free Wi-Fi is protected.
(c) Utilize VPN
(d) Encrypt your device
(e) Install an Antivirus application.
(f) Update to the latest software.
(g) Avoid turning on auto fill.
(h) Log out.
(j) Use only trusted stores.



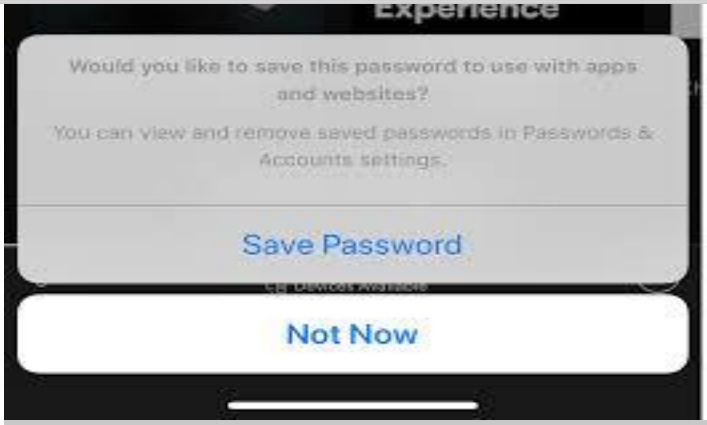


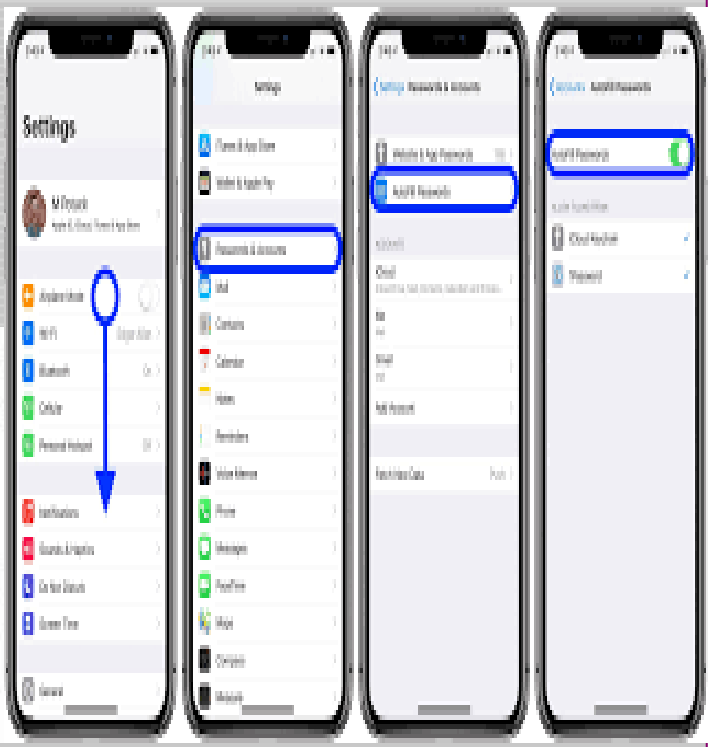
Other things to consider:

(a) Avoid turning on auto fill: Some websites and applications will automatically fill in your username when you visit them. This is due to the auto fill feature. Turn it off as soon as possible.

(b) Log out: After using mobile applications, especially those that are linked to one
another, such as Google applications, ensure that you log off each time you are done using them.

(c) Use only trusted stores: You should download apps from secure stores, such as Apple's App Store. This depends On the platform your mobile device uses.

# Conclusion

Making your mobile device secure is not an easy task, but it should be your first priority. As there are new vulnerabilities found every day, it's important to make sure that you are aware of any suspicious activity that occurs on your device.