DEPARTMENT OF COMPUTER SCIENCE

P23CSG22 - CYBER SECURITY

(Generic Elective - Common Paper for all PG Programmes in the II Semester)

UNIT – 1

INTRODUCTION TO CYBER SPACE

Cyberspace can be defined as an intricate environment that involves interactions between people, software, and services. It is maintained by the worldwide distribution of information and communication technology devices and networks.

With the benefits carried by the technological advancements, the cyberspace today has become a common pool used by citizens, businesses, critical information infrastructure, military and governments in a fashion that makes it hard to induce clear boundaries among these different groups. The cyberspace is anticipated to become even more complex in the upcoming years, with the increase in networks and devices connected to it.

The word Cyberspace first made its appearance in Wiliam Gibson's Science fiction book Necromancer. The book described an online world filled with computers and associated societal elements. In that book, the author described Cyberspace as a 3D virtual landscape created by a network of computers. Although it looks like a physical space, it is generated by a computer, representing abstract data.

After the publication of the book, the word Cyberspace became a mainstay in many English dictionaries. The New Oxford Dictionary of English provides Cyberspace definition as the notional environment used by the people to communicate over networks of the computer.

As per the Cyberspace meaning, Cyberspace is a virtual space with no mass, gravity or boundaries. It is the interconnected space between networks of computer systems. Bits and Bytes-Zeroes and ones are used to define Cyberspace. It is a dynamic environment where these values change continuously. It can also be defined as the imaginary location where two parties can converse.

HISTORY OF INTERNET

The earliest iteration of the internet was the ARPANET (Advanced Research Projects Agency Network), which was created in the late 1960s by the United States Department of Defense. The ARPANET was designed as a means for researchers at different universities and government agencies to share information and collaborate on research projects. The first ARPANET message was sent in 1969 between two computers located at the University of California, Los Angeles (UCLA) and the Stanford Research Institute (SRI).

In the 1970s, the ARPANET grew to include additional universities and research centers, and email was introduced as a means of communication. In the early 1980s, the National Science Foundation (NSF) established the Computer Science Network (CSNET) to provide networking capabilities to researchers who did not have access to the ARPANET. This was the first step toward creating a more widespread network of interconnected computers.

In the mid-1980s, the NSF established the NSFNET, a backbone network that provided high-speed connectivity to researchers across the country. This network was instrumental in facilitating the growth of the internet as we know it today. The first domain name was registered in 1985, and the first website was created in 1991.

The 1990s saw explosive growth in the internet, driven in part by the creation of the World Wide Web by Tim Berners-Lee in 1989. The World Wide Web provided a graphical user interface for accessing information on the internet, making it more accessible to non-technical users. This led to an explosion of websites, as well as the development of search engines like Yahoo! and Google.

The early 2000s saw the rise of social media, with the launch of Friendster in 2002, followed by MySpace and Facebook. These platforms allowed users to connect with each other and share information on a massive scale. The rise of mobile devices like smartphones and tablets in the late 2000s and early 2010s further accelerated the growth of the internet, making it even more accessible to people around the world.

CYBER CRIME

Cybercrime or a computer-oriented crime is a crime that includes a computer and a network. The computer may have been used in the execution of a crime or it may be the target. Cybercrime is the use of a computer as a weapon for committing crimes such as committing fraud, identity theft, or breaching privacy. Cybercrime, especially through the Internet, has grown in importance as the computer has become central to every field like commerce, entertainment, and government. Cybercrime may endanger a person or a nation's security and financial health. Cybercrime encloses a wide range of activities, but these can generally be divided into two categories:

1. Crimes that aim at computer networks or devices. These types of crimes involve different threats (like virus, bugs etc.) and denial-of-service (DoS) attacks.
2. Crimes that use computer networks to commit other criminal activities. These types of crimes include cyber stalking, financial fraud or identity theft.

Classification of Cyber Crime:

1. **Cyber Terrorism –**
   Cyber terrorism is the use of the computer and internet to perform violent acts that result in loss of life. This may include different type of activities either by software or hardware for threatening life of citizens.
   In general, Cyber terrorism can be defined as an act of terrorism committed through the use of cyberspace or computer resources.

2. **Cyber Extortion –**
   Cyber extortion occurs when a website, e-mail server or computer system is subjected to or threatened with repeated denial of service or other attacks by malicious hackers. These hackers demand huge money in return for assurance to stop the attacks and to offer protection.

3. **Cyber Warfare –**
   Cyber warfare is the use or targeting in a battle space or warfare context of computers, online control systems and networks. It involves both offensive and defensive operations concerning to the threat of cyber attacks, espionage and sabotage.

4. **Internet Fraud –**
   Internet fraud is a type of fraud or deceit which makes use of the Internet and could include hiding of information or providing incorrect information for the purpose of deceiving victims for money or property. Internet fraud is not considered a single, distinctive crime but covers a range of illegal

and illicit actions that are committed in cyberspace.

5. **Cyber Stalking –**
   This is a kind of online harassment wherein the victim is subjected to a barrage of online messages and emails. In this case, these stalkers know their victims and instead of offline stalking, they use the Internet to stalk. However, if they notice that cyber stalking is not having the desired effect, they begin offline stalking along with cyber stalking to make the victims' lives more miserable.

Challenges of Cyber Crime:

1. **People are unaware of their cyber rights-**
   The Cybercrime usually happen with illiterate people around the world who are unaware about their cyber rights implemented by the government of that particular country.

2. **Anonymity-**
   Those who Commit cyber crime are **anonymous** for us so we cannot do anything to that person.

3. **Less numbers of case registered-**
   Every country in the world faces the challenge of cyber crime and the rate of cyber crime is increasing day by day because the people who even don't register a case of cyber crime and this is major challenge for us as well as for authorities as well.

4. **Mostly committed by well educated people-**
   Committing a cyber crime is not a cup of tea for every individual. The person who commits cyber crime is a very **technical** person so he knows how to commit the crime and not get caught by the authorities.

5. **No harsh punishment-**
   In Cyber crime there is no harsh punishment in every cases. But there is harsh punishment in some cases like when somebody commits cyber terrorism in that case there is harsh punishment for that individual. But in other cases there is no harsh punishment so this factor also gives encouragement to that person who commits cyber crime.

Prevention of Cyber Crime:

Below are some points by means of which we can prevent cyber crime:

1. **Use strong password –**
   Maintain different password and username combinations for each account and resist the temptation to write them down. Weak passwords can be easily cracked using certain attacking methods like Brute force attack, Rainbow table attack etc, So make them complex. That means combination of letters, numbers and special characters.

2. **Use trusted antivirus in devices –**
   Always use trustworthy and highly advanced antivirus software in mobile and personal computers. This leads to the prevention of different virus attack on devices.

3. **Keep social media private –**
   Always keep your social media accounts data privacy only to your friends. Also make sure only to make friends who are known to you.

4. **Keep your device software updated –**
   Whenever you get the updates of the system software update it at the same time because sometimes the previous version can be easily attacked.

5. **Use secure network –**
   Public Wi-Fi are vulnerable. Avoid conducting financial or corporate transactions on these networks.

6. **Never open attachments in spam emails –**
   A computer get infected by malware attacks and other forms of cybercrime is via email attachments in spam emails. Never open an attachment from a sender you do not know.
7. **Software should be updated –** Operating system should be updated regularly when it comes to internet security. This can become a potential threat when cybercriminals exploit flaws in the system.

INFORMATION SECURITY

Information security is the practice of protecting information by mitigating information risks. It involves the protection of information systems and the information processed, stored and transmitted by these systems from unauthorized access, use, disclosure, disruption, modification or destruction. This includes the protection of personal information, financial information, and sensitive or confidential information stored in both digital and physical forms. Effective information security requires a comprehensive and multi-disciplinary approach, involving people, processes, and technology.

Information Security is not only about securing information from unauthorized access. Information Security is basically the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information. Information can be a physical or electronic one. Information can be anything like Your details or we can say your profile on social media, your data on mobile phone, your biometrics etc. Thus Information Security spans so many research areas like Cryptography, Mobile Computing, Cyber Forensics, Online Social Media, etc.

Here are some key reasons why information security is important:

1. **Protecting sensitive information:** Information security helps protect sensitive information from being accessed, disclosed, or modified by unauthorized individuals. This includes personal information, financial data, and trade secrets, as well as confidential government and military information.
2. **Mitigating risk:** By implementing information security measures, organizations can mitigate the risks associated with cyber threats and other security incidents. This includes minimizing the risk of data breaches, denial-of-service attacks, and other malicious activities.
3. **Compliance with regulations**: Many industries and jurisdictions have specific regulations governing the protection of sensitive information. Information security measures help ensure compliance with these regulations, reducing the risk of fines and legal liability.
4. **Protecting reputation**: Security breaches can damage an organization’s reputation and lead to lost business. Effective information security can help protect an organization’s reputation by minimizing the risk of security incidents.

5. **Ensuring business continuity**: Information security helps ensure that critical business functions can continue even in the event of a security incident. This includes maintaining access to key systems and data, and minimizing the impact of any disruptions.

Information Security programs are build around 3 objectives, commonly known as CIA – Confidentiality, Integrity, Availability.

1. **Confidentiality –** means information is not disclosed to unauthorized individuals, entities and process. For example if we say I have a 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.
2. **Integrity –** means maintaining accuracy and completeness of data. This means data cannot be edited in an unauthorized way. For example if an employee leaves an organisation 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.
3. **Availability –** means information must be available when needed. For example 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 operations, incident response and policy/change management. Denial of service attack is one of the factor that can hamper the availability of information.

Apart from this there is one more principle that governs information security programs. This is Non repudiation.

- **Non repudiation –** means one party cannot deny receiving a message or a transaction nor can the other party deny sending a message or a transaction. For example in cryptography it is sufficient to show that message matches the digital signature signed with sender's private key and that sender could have a sent a message and nobody else could have altered it in transit. Data Integrity and Authenticity are pre-requisites for Non repudiation.

- **Authenticity –** means verifying that users are who they say they are and that each input arriving at destination is from a trusted source.This principle if followed guarantees the valid and genuine message received from a trusted source through a valid transmission. For example if take above example sender sends the message along with digital signature which was generated using the hash value of message and private key. Now at the receiver side this digital signature is decrypted using the public key generating a hash value and message is again hashed to generate the hash value. If the 2 value matches then it is known as valid transmission with the authentic or we say genuine message received at the recipient side
- **Accountability –** means that it should be possible to trace actions of an entity uniquely to that entity. For example as we discussed in Integrity section Not every employee should be allowed to do changes in other employees data. For this there is a separate department in an organization that is responsible for making such changes and when they receive request for a change then that letter must be signed by higher authority for example Director of college and person that is allotted that change will be able to do change after verifying his bio metrics, thus timestamp with the user(doing changes) details get recorded. Thus we can say if a change goes like this then it will be possible to trace the actions uniquely to an entity.

advantages to implementing an information classification system in an organization’s information security program:

1. **Improved security:** By identifying and classifying sensitive information, organizations can better protect their most critical assets from unauthorized access or disclosure.
2. **Compliance**: Many regulatory and industry standards, such as HIPAA and PCI-DSS, require organizations to implement information classification and data protection measures.
3. **Improved efficiency**: By clearly identifying and labeling information, employees can quickly and easily determine the appropriate handling and access requirements for different types of data.
4. **Better risk management**: By understanding the potential impact of a data breach or unauthorized disclosure, organizations can prioritize resources and develop more effective incident response plans.
5. **Cost savings**: By implementing appropriate security controls for different types of information, organizations can avoid unnecessary spending on security measures that may not be needed for less sensitive data.
6. **Improved incident response**: By having a clear understanding of the criticality of specific data, organizations can respond to security incidents in a more effective and efficient manner.

There are some potential disadvantages to implementing an information classification system in an organization’s information security program:

1. **Complexity:** Developing and maintaining an information classification system can be complex and time-consuming, especially for large organizations with a diverse range of data types.
2. **Cost**: Implementing and maintaining an information classification system can be costly, especially if it requires new hardware or software.
3. **Resistance to change:** Some employees may resist the implementation of an information classification system, especially if it requires them to change their usual work habits.
4. **Inaccurate classification:** Information classification is often done by human, so it is possible that some information may be misclassified, which can lead to inadequate protection or unnecessary restrictions on access.
5. **Lack of flexibility:** Information classification systems can be rigid and inflexible, making it difficult to adapt to changing business needs or new types of data.
6. **False sense of security**: Implementing an information classification system may give organizations a false sense of security, leading them to overlook other important security controls and best practices.
7. **Maintenance:** Information classification should be reviewed and updated frequently, if not it can become outdated and ineffective.

Uses of Information Security :

Information security has many uses, including:

1. **Confidentiality:** Keeping sensitive information confidential and protected from unauthorized access.
2. **Integrity:** Maintaining the accuracy and consistency of data, even in the presence of malicious attacks.
3. **Availability:** Ensuring that authorized users have access to the information they need, when they need it.
4. **Compliance:** Meeting regulatory and legal requirements, such as those related to data privacy and protection.
5. **Risk management:** Identifying and mitigating potential security threats to prevent harm to the organization.

6. **Disaster recovery:** Developing and implementing a plan to quickly recover from data loss or system failures.
7. **Authentication:** Verifying the identity of users accessing information systems.
8. **Encryption:** Protecting sensitive information from unauthorized access by encoding it into a secure format.
9. **Network security:** Protecting computer networks from unauthorized access, theft, and other types of attacks.
10. **Physical security:** Protecting information systems and the information they store from theft, damage, or destruction by securing the physical facilities that house these systems.

Issues of Information Security :

Information security faces many challenges and issues, including:

1. **Cyber threats:** The increasing sophistication of cyber attacks, including malware, phishing, and ransomware, makes it difficult to protect information systems and the information they store.
2. **Human error:** People can inadvertently put information at risk through actions such as losing laptops or smartphones, clicking on malicious links, or using weak passwords.
3. **Insider threats:** Employees with access to sensitive information can pose a risk if they intentionally or unintentionally cause harm to the organization.
4. **Legacy systems:** Older information systems may not have the security features of newer systems, making them more vulnerable to attack.
5. **Complexity:** The increasing complexity of information systems and the information they store makes it difficult to secure them effectively.
6. **Mobile and IoT devices:** The growing number of mobile devices and internet of things (IoT) devices creates new security challenges as they can be easily lost or stolen, and may have weak security controls.
7. **Integration with third-party systems:** Integrating information systems with third-party systems can introduce new security risks, as the third-party systems may have security vulnerabilities.
8. **Data privacy:** Protecting personal and sensitive information from unauthorized access, use, or disclosure is becoming increasingly important as data privacy regulations become more strict.
9. **Globalization:** The increasing globalization of business makes it more difficult to secure information, as data may be stored, processed, and transmitted across multiple countries with different security requirements.

DATA STEALING OR DATA THEFT

Data theft – also known as information theft – is the illegal transfer or storage of personal, confidential, or financial information. This could include passwords, software code or algorithms, and proprietary processes or technologies. Data theft is considered a serious security and privacy breach, with potentially severe consequences for individuals and organizations.

Definition

Data theft is the act of stealing digital information stored on computers, servers, or electronic devices to obtain confidential information or compromise privacy. The data stolen can be anything from bank account information, online passwords, passport numbers, driver's license numbers, social security numbers, medical records, online subscriptions, and so on. Once an unauthorized person has access to personal or financial information, they can delete, alter, or prevent access to it without the owner’s permission.

Data theft usually occurs because malicious actors want to sell the information or use it for identity theft. If data thieves steal enough information, they can use it to gain access to secure accounts, set up credit cards using the victim's name, or otherwise use the victim's identity to benefit themselves. Data theft was once primarily a problem for businesses and organizations but, unfortunately, is now a growing problem for individuals.

While the term refers to 'theft', data theft doesn't literally mean taking information away or removing it from the victim. Instead, when data theft occurs, the attacker simply copies or duplicates information for their own use.

The terms 'data breach' and 'data leak' can be used interchangeably when discussing data theft. However, they are different:

- A **data leak** occurs when sensitive data is accidentally exposed, either on the internet or through lost hard drives or devices. This enables cybercriminals to gain unauthorized access to sensitive data without effort on their part.
- By contrast, a **data breach** refers to intentional cyberattacks.

Causes of Data Theft

Data theft or digital theft occurs through a variety of means. Some of the most common include:

Social engineering:
The most common form of social engineering is phishing. Phishing occurs when an attacker masquerades as a trusted entity to dupe a victim into opening an email, text message, or instant message. Users falling for phishing attacks is a common cause of data theft.
Weak passwords:

Using a password that is easy to guess, or using the same password for multiple accounts, can allow attackers to gain access to data. Poor password habits – such as writing passwords down on a piece of paper or sharing them with others – can also lead to data theft.

System vulnerabilities:

Poorly written software applications or network systems that are poorly designed or implemented create vulnerabilities that hackers can exploit and use to steal data. Antivirus software that is out of date can also create vulnerabilities.

Insider threats:
Employees who work for an organization have access to customers' personal information. Rogue employees or disgruntled contractors could copy, alter, or steal data. However, insider threats are not necessarily restricted to current employees. They can also be former employees, contractors, or partners who have access to an organization's systems or sensitive information. Insider threats are reportedly on the rise.
Human error

Data breaches don't have to be the result of malicious actions. Sometimes they can be the result of human error instead. Common errors include sending sensitive information to the wrong person, such as sending an email by mistake to the incorrect address, attaching the wrong document, or handing a physical file to someone who shouldn't have access to the information. Alternatively, human error could involve misconfiguration, such as an employee leaving a database containing sensitive information online without any password restrictions in place.

Compromised downloads

An individual might download programs or data from compromised websites infected by viruses like worms or malware. This gives criminals unauthorized access to their devices, allowing them to steal data.

Physical actions

Some data theft is not the result of cybercrime but physical actions instead. These include the theft of paperwork or devices such as laptops, phones, or storage devices. With remote working increasingly widespread, the scope for devices to go missing or be stolen has also increased. If you're working in a public place such as a coffee shop, someone could watch your screen and keyboard to steal information like your login details. Card-skimming – where criminals insert a device into card readers and ATMs to harvest payment card information – is another source of data theft.

Database or server problems

If a company storing your information is attacked because of a database or server problem, the attacker could access customers' personal information.

Publicly available information

A lot of information can be found in the public domain – i.e., through internet searches and looking through user posts on social networks.

Types of data stolen

Any information stored by an individual or organization could be a potential target for data thieves. For example:

- Customer records
- Financial Data such as credit card or debit card information
- Source codes and algorithms
- Proprietary process descriptions and operating methodologies
- Network credentials such as usernames and passwords
- HR records and employee data
- Private documents stored on computer computers

COMPUTER ETHICS AND SECURITY POLICIES

COMPUTER ETHICS

With the help of internet, world has now become a global village. Internet has been proven to be a boon to individuals as well as various organizations and businesses. e-Commerce is becoming very popular among businesses as it helps them to reach a wide range of customers faster than any other means.

Computer ethics deals with the procedures, values and practices that govern the process of consuming computer technology and its related disciplines without damaging or violating the moral values and beliefs of any individual, organization or entity.

GUIDELINES OF ETHICS

Generally, the following guidelines should be observed by computer users:

1. Honesty: Users should be truthful while using the internet.

2. Confidentiality: Usersshould not share any important information with unauthorized people.

3. Respect: Each user should respect the privacy of other users.

4. Professionalism: Each user should maintain professional conduct.

5. Obey The Law: Users should strictly obey the cyber law in computer usage.

6. Responsibility: Each user should take ownership and responsibility for their actions

SECURITY POLICIES

Policies are divided in two categories −

- User policies
- IT policies.

User policies generally define the limit of the users towards the computer resources in a workplace. For example, what are they allowed to install in their computer, if they can use removable storages.

Whereas, IT policies are designed for IT department, to secure the procedures and functions of IT fields.

- **General Policies** − This is the policy which defines the rights of the staff and access level to the systems. Generally, it is included even in the communication protocol as a preventive measure in case there are any disasters.
- **Server Policies** − This defines who should have access to the specific server and with what rights. Which software's should be installed, level of access to internet, how they should be updated.
- **Firewall Access and Configuration Policies** − It defines who should have access to the firewall and what type of access, like monitoring, rules change. Which ports and services should be allowed and if it should be inbound or outbound.

- **Backup Policies** − It defines who is the responsible person for backup, what should be the backup, where it should be backed up, how long it should be kept and the frequency of the backup.
- **VPN Policies** − These policies generally go with the firewall policy, it defines those users who should have a VPN access and with what rights. For site-to-site connections with partners, it defines the access level of the partner to your network, type of encryption to be set.

Types of Policies

- **Permissive Policy** − It is a medium restriction policy where we as an administrator block just some well-known ports of malware regarding internet access and just some exploits are taken in consideration.
- **Prudent Policy** − This is a high restriction policy where everything is blocked regarding the internet access, just a small list of websites are allowed, and now extra services are allowed in computers to be installed and logs are maintained for every user.
- **Acceptance User Policy** − This policy regulates the behavior of the users towards a system or network or even a webpage, so it is explicitly said what a user can do and cannot in a system. Like are they allowed to share access codes, can they share resources, etc.
- **User Account Policy** − This policy defines what a user should do in order to have or maintain another user in a specific system. For example, accessing an e-commerce webpage.
- **Information Protection Policy** − This policy is to regulate access to information, hot to process information, how to store and how it should be transferred.
- **Remote Access Policy** − This policy is mainly for big companies where the user and their branches are outside their headquarters. It tells what should the users access, when they can work and on which software like SSH, VPN, RDP.
- **Firewall Management Policy** − This policy has explicitly to do with its management, which ports should be blocked, what updates should be taken, how to make changes in the firewall, how long should be the logs be kept.
- **Special Access Policy** − This policy is intended to keep people under control and monitor the special privileges in their systems and the purpose as to why they have it. These employees can be team leaders, managers, senior managers, system administrators, and such high designation based people.
- **Network Policy** − This policy is to restrict the access of anyone towards the network resource and make clear who all will access the network. It will also ensure whether that person should be authenticated or not. The documentation of network changes. Web filters and the levels of access.
- **Email Usage Policy** − This is one of the most important policies that should be done because many users use the work email for personal purposes as well. As a result information can leak outside. Some of the key points of this policy are the employees should know the importance of

this system that they have the privilege to use. They should not open any attachments that look suspicious. Private and confidential data should not be sent via any encrypted email.

- **Software Security Policy** − This policy has to do with the software's installed in the user computer and what they should have. Some of the key points of this policy are Software of the company should not be given to third parties. Only the white list of software's should be allowed, no other software's should be installed in the computer.

VIOLENCE AGAINST WOMEN & CYBER SECURITY FOR WOMEN

Cyber violence uses Computer Technology to access women's personal information and use the internet for harassment and exploitation. Women are becoming soft targets as they often trust other people and are unaware of the consequences.

Cyber crime has increased because it is seldom reported and difficult to detect and prove. Cyber crime is away from traditional monitoring, investigation, or audit and requires specialists to understand the nature of the crime.

Cyber crime affects women the most by subjecting them to mental and emotional harassment. Most women become distressed, humiliated, and depressed under this type of crime which is challenging to address and resolve.

Cyber Crime Types

Cyber crime against women includes gender-based and sexual remarks and activities performed through a computer network or mobile phones, affecting the dignity of women and causing emotional distress.

The different types of cyber crime against women are explained as follows:

- **Cyber Stalking:** It includes attempting to contact women via social networking sites without any legitimate purpose, putting threatening messages on the chat page, and constantly disturbing the victims with objectionable emails and messages to create mental distress.
- **Cyber Defamation:** This activity involves defaming the victim through blackmailing and disclosing their details or modified pictures. It often involves extorting and seeking sexual favors from the victim.
- **Cyber Hacking:** When asked to click on unauthorised URLs or download apps that leak all their personal information on their phones, the women became victims of cyber hacking. The criminals utilise these details for unauthorised monetary transactions and other unlawful activities.
- **Cyber Bullying**: It is an act of regular harassment and bullying of the victim through the digital communication device by posting abusive and misleading content, pictures, or videos and sending rape and death threats.

- **Pornography**: This criminal activity involves posting morphed images of victims and using them for pornographic purposes, sometimes demanding money to remove them from social networking sites.
- **Cyber Grooming:** In this case, a person builds a relationship with a woman through an online platform and pressurizes her for undue favors or doing sexual acts.

Measures for Cyber Safety

These are some of the measures that can be taken to protect oneself from cyber crimes:

- Keep a watch on irrelevant or fraudulent messages or emails.
- Avoid responding to emails asking for personal information.
- Avoid accessing fraudulent websites or apps that require personal information.
- Take care of the email address and password.
- Use strong and secure passwords and keep on changing them regularly.
- Don’t click on unrecognized UPL or download unknown apps.
- Remain updated about cyber laws and policies.

Cyber Laws for Women’s Safety

All users of cyberspace are subject to specific laws applicable worldwide. Cyber laws deal with legal issues arising from networked computer technology and digital platforms. These laws protect the victims against cyber crimes and help them address the issues and get justice.

The following **acts under the Indian Penal Code (IPC, 1860) section 354** mention the following crimes as punishable under the law.

- **Section 354A:** Demand for sexual favors or displaying objectionable pictures against a woman’s consent or making sexual remarks and sexual harassment will cause imprisonment of up to 3 years with fines.
- **Section 354C:** An act of photographing or publishing a picture of a woman engaged in a private act without her consent will lead to imprisonment of 3 to 7 years.
- **Section 354D:** Contacting a woman online and sending irrelevant emails/messages despite the woman’s evident disinterest will cause imprisonment of 5 years with fines.

The Information Technology Act of 2000 also has provisions for punishment under the following sections:

- **Section 66C**-Identify cyber hacking is a punishable offense with imprisonment of 3 years and fines of Rs. 1 lakh.
- **Section 66E-** Deals with the offense of capturing, publishing, or sending pictures of women in circumstances that violate privacy. This causes imprisonment of 3 years.
- **Section 67A-** Makes it illegal to publish and transmit sexually explicit content and is punishable with imprisonment of up to 5 to 7 years.

The Cyber Crime Prevention Act of 2012 focuses on preventing and prosecuting offenders involved in cyber crimes like violating privacy, confidentiality, and integrity of information through computer-related criminal activities.

The Indecent Representation of Women (Prohibition) Act regulates and prohibits the indecent representation of women through the media and publications, which also includes the audio-visual media, the content in electronic form, and distribution of material on the Internet and the portrayal of women over the web.

Cyber-Security and Government of India

The Cyber Crime Prevention against Women and Children (CCPWC) scheme is introduced to develop effective measures to handle cyber-crimes against women and children in India. It allows a cybercrime victim to file a complaint through an online cybercrime reporting platform.

The platform also provides details of law enforcement and regulatory agencies at the local and national levels. The CCPWC also conducts awareness programs starting from the school level as a proactive measure to mitigate cyber crimes.

Preventing Cyber Crime Against Women

The most important part is to have a thorough knowledge and awareness about privacy and cyber-crimes to avoid people being vulnerable to such threats. There has to be more education on cyber-crimes and online fraud and how to get rid of them or handle them.

Cyber literacy should start from the basic level with adequate knowledge about good operating practices. It is necessary to remain extra vigilant about cyber privacy and security. Proper awareness and education can help teach good habits and practices while working online with digital devices.

There is also a need for stricter law enforcement and punishment for offenders. Media interventions for creating public awareness can make an effective contribution in bringing about changes in the attitudes of people towards gender norms.

Cyber Violence Against Women- Data

Here is some important data on cyber harassment of women in India:

- A total of 10,405 cyber crimes against women were reported in 2020, with an increase of 24%.
- The Information Technology Act of 2000 is the primary law in India dealing with cyber crime.

CYBER STALKING

In **Cyber Stalking**, a cyber criminal uses the internet to consistently threaten somebody. This crime is often perpetrated through email, social media, and the other online medium. Cyber Stalking can even occur in conjunction with the additional ancient type of stalking, wherever the bad person harasses the victim offline. There’s no unified legal approach to cyber Stalking, however, several governments have moved toward creating these practices punishable by law. Social media, blogs, image sharing sites and lots of different ordinarily used online sharing activities offer cyber Stalkers with a wealth of data that helps them arrange their harassment. It includes actions like false accusations, fraud, information destruction, threats to life and manipulation through threats of exposure. It has stalkers take the assistance of e-mails and other forms of message applications, messages announce to an online website or a discussion cluster, typically even the social media to send unwanted messages, and harass a specific person with unwanted attention. Cyber Stalking is typically cited as internet stalking, e-stalking or online stalking.

Types of Cyber Stalking:

- **Webcam Hijacking:** Internet stalkers would attempt to trick you into downloading and putting in a malware-infected file that may grant them access to your webcam. the method is therefore sneaky that it's probably you wouldn't suspect anything strange.
- **Observing location check-ins on social media:** In case you're adding location check-ins to your Facebook posts, you're making it overly simple for an internet stalker to follow you by just looking through your social media profiles.
- **Catfishing:** Catfishing happens via social media sites, for example, Facebook, when internet stalkers make counterfeit user-profiles and approach their victims as a companion of a companion.
- **Visiting virtually via Google Maps Street View:** If a stalker discovers the victim's address, then it is not hard to find the area, neighbourhood, and surroundings by using Street View. Tech-savvy stalkers don't need that too.
- **Installing Stalkerware:**One more method which is increasing its popularity is the use of Stalkerware. It is a kind of software or spyware which keeps track of the location, enable access to text and browsing history, make an audio recording, etc. And an important thing is that it runs in the background without any knowledge to the victim.
- **Looking at geotags to track location:**Mostly digital pictures contain geotags which is having information like the time and location of the picture when shot in the form of metadata. Geotags comes in the EXIF format embedded into an image and is readable with the help of special apps. In this way, the stalker keeps an eye on the victim and gets the information about their whereabouts.

Protective Measures:

- Develop the habit of logging out of the PC when not in use.
- Remove any future events you're close to attending from the social networks if they're recorded on online approaching events and calendars.
- Set strong and distinctive passwords for your online accounts.
- Cyber Stalkers can exploit the low security of public Wi-Fi networks to snoop on your online activity. Therefore, avoid sending personal emails or sharing your sensitive info when connected to an unsecured public Wi-Fi.
- Make use of the privacy settings provided by the social networking sites and keep all info restricted to the nearest of friends.
- Do a daily search on the internet to search out what information is accessible regarding you for the public to check.

PORNOGRAPHY

Responding to online pornography exposure and other risks

Exposure to explicit online content may cause children and young people to develop different "sexual literacies" to previous generations. Australian Government and non-government services have taken steps to reduce children and young people's exposure to online risks - including pornography - and enact harm minimisation strategies. Three key types of intervention have been identified:

- legal and regulatory avenues to existing legislation regarding online pornography and online behaviour such as sexting and the sharing of explicit images;
- education for children and young people (e.g., critical media and digital literacy, respectful relationships, sexuality and sexual health); and
- education and resources for teachers and parents about how they can support safe, respectful relationships for children and young people both online and IRL (in real life).

The following measures can be taken

Open communication

It is important for parents and caregivers to be able to initiate open conversations about their child's online experiences. Schools too can play an important role in assisting children and young people to make sense of their exposure to online pornography in healthy ways.

Critical thinking

Young people should be encouraged to question pornography, asking: "Seeing porn might seem normal. But what does porn say? Who makes it and why? And what does it all mean for you?" (Reality & Risk Project, 2016).

Young people are not just passive consumers of pornography. Critical thinking helps viewers to reflect on the messages contained in online pornography. It fosters discussion while respecting the agency of the young people involved.

Arming children and young people with tools to engage critically with media is important to their understanding of the differences between online pornography and their offline sexual relationships.

Digital literacy

Parents and caregivers are encouraged to educate themselves about the internet and social media, in order to be aware of the current online dangers and opportunities facing their children. Parents and caregivers are less likely to be intimidated by online risks if they are informed and take an active role in their children's digital lives.

Mediation

Parental controls are essential to harm-minimisation strategies. The Office of the e-Safety Commissioner (2016) cautions parents and caregivers: "You can teach your child strategies about how to deal with offensive material, but be vigilant, especially if your child is prone to taking risks or is emotionally or psychologically vulnerable".

Support

Support for children and young people who have been exposed to online pornography is extremely important to their ability to process their experience in healthy ways. In *What can I do if my child sees content that's offensive?*, the Office of the Children's e-Safety Commissioner (2016) advises:

- Encourage your child to talk if they have seen something online that has upset them.
- Let them know that if they report viewing inappropriate content they won't be punished or have their access to the internet taken away.
- Educate them so that if they are sent something inappropriate online they know not to respond.

USAGE OF SOCIAL MEDIA AND CYBER SECURITY FOR WOMEN.

Social media serves as a platform for women to overcome societal norms and familial responsibilities that may limit their ability to showcase their innate skills and talents. By leveraging social media, women can tap into their hidden potential and exhibit their abilities to a wider audience.

Social media offers an avenue for women to break free from these limitations and express themselves authentically. It provides an opportunity to showcase their talents, whether in the realms of art, music, writing, entrepreneurship, or any other domain.

Women can share their creations, expertise, and ideas with a global audience through social media. They can leverage the power of visual content, videos, blogs, or podcasts to highlight their unique talents and skills. By doing so, they not only gain recognition but also inspire and empower others who may face similar challenges.

Social media platforms provide a valuable space for women to connect with each other, establish communities, and offer support. These communities can revolve around diverse topics such as parenting, entrepreneurship, mental health, or shared interests. Within these online spaces, women find a sense of solidarity, exchange advice, and seek guidance from one another.

Through social media, women can discover like-minded individuals who understand their unique experiences and challenges. They can join groups, follow relevant hashtags, or participate in discussions to engage with others who share similar interests or circumstances. These communities foster a supportive environment where women can openly share their stories, seek advice, and receive encouragement.

Parenting communities on social media, for example, allow women to connect with other mothers facing similar joys and struggles. They can share parenting tips, discuss child development, or seek advice on various aspects of raising children. These communities provide a space for empathy, shared experiences, and learning from one another.

Social media grants women access to abundant knowledge, educational resources, and news. Through these platforms, women can stay up-to-date with current events, delve into educational content, and acquire knowledge across various fields. This vast availability of information empowers women in their personal growth, professional development, and decision-making processes.

Access to educational resources is another advantage that social media offers. Women can find educational content through tutorials, webinars, online courses, and expert advice. These resources cater to diverse interests and areas of expertise, from entrepreneurship and career development to health and wellness. Through social media, women can acquire new skills, expand their knowledge, and enhance their professional capabilities.

The cautious handling of social media, particularly for women, is an undeniable necessity. Women should be mindful of privacy settings, secure their personal details, and be aware of the potential risks of online harassment and abuse. By practising healthy social media habits, setting boundaries, and seeking support when needed, women can harness the full potential of social media while safeguarding their well-being.

UNIT - 2

Email Security &Wi Fi Security Guidelines to choose web browsers

Email (short for electronic mail) is a digital method by using it we exchange messages between people over the internet or other computer networks. With the help of this, we can send and receive text-based messages, often an attachment such as documents, images, or videos, from one person or organization to another.

It was one of the first applications developed for the internet and has since become one of the most widely used forms of digital communication. It has an essential part of personal and professional communication, as well as in marketing, advertising, and customer support.

In this article, we will understand the concept of **email security**, how we can protect our email, email security policies, and email security best practices, and one of the features of email is an email that we can use to protect the email from unauthorized access.

Email Security:

Basically**, Email security** refers to the steps where we protect the email messages and the information that they contain from unauthorized access, and damage. It involves ensuring the confidentiality, integrity, and availability of email messages, as well as safeguarding against phishing attacks, spam, viruses, and another form of malware. It can be achieved through a combination of technical and non-technical measures.

Some standard technical measures include the encryption of email messages to protect their contents, the use of digital signatures to verify the authenticity of the sender, and email filtering systems to block unwanted emails and malware, and the non-technical measures may include training employees on how to recognize and respond to phishing attacks and other email security threats, establishing policies and procedures for email use and management, and conducting regular security audits to identify and address vulnerabilities.

We can say that email security is important to protect sensitive information from unauthorized access and ensure the reliability and confidentiality of electronic communication.

Steps to Secure Email:

We can take the following actions to protect our email.

- Choose a secure password that is at least 12 characters long, and contains uppercase and lowercase letters, digits, and special characters.
- Activate the two-factor authentication, which adds an additional layer of security to your email account by requiring a code in addition to your password.
- Use encryption, it encrypts your email messages so that only the intended receiver can decipher them. Email encryption can be done by using the programs like PGP or S/MIME.
- Keep your software up to date. Ensure that the most recent security updates are installed on your operating system and email client.
- **Beware of phishing scams:** Hackers try to steal your personal information by pretending as someone else in phishing scams. Be careful of emails that request private information or have suspicious links because these are the resources of the phishing attack.
- **Choose a trustworthy email service provider:** Search for a service provider that protects your data using encryption and other security measures.
- **Use a VPN:** Using a VPN can help protect our email by encrypting our internet connection and disguising our IP address, making it more difficult for hackers to intercept our emails.
- **Upgrade Your Application Regularly:** People now frequently access their email accounts through apps, although these tools are not perfect and can be taken advantage of by hackers. A cybercriminal might use a vulnerability, for example, to hack accounts and steal data or send spam mail. Because of this, it’s important to update your programs frequently.

Email Security Policies

The email policies are a set of regulations and standards for protecting the privacy, accuracy, and accessibility of email communication within the organization. An email security policy should include the following essential components:

- **Appropriate Use:** The policy should outline what comprises acceptable email usage inside the organization, including who is permitted to use email, how to use it, and for what purpose email we have to use.
- **Password and Authentication:** The policy should require strong passwords and two-factor authentication to ensure that only authorized users can access email accounts.
- **Encryption**: To avoid unwanted access, the policy should mandate that sensitive material be encrypted before being sent through email.
- **Virus Protection: T**he policy shall outline the period and timing of email messages and attachment collection.
- **Retention and Detection**: The policy should outline how long email messages and their attachments ought to be kept available, as well as when they should continue to be removed.
- **Training**: The policy should demand that all staff members take a course on email best practices, which includes how to identify phishing scams and other email-based threats.
- **Incident Reporting**: The policy should outline the reporting and investigation procedures for occurrences involving email security breaches or other problems.
- **Monitoring**: The policy should outline the procedures for monitoring email communications to ensure that it is being followed, including any logging or auditing that will be carried out.
- **Compliance**: The policy should ensure compliance with all essential laws and regulations, including the health
- Insurance rules, including the health portability and accountability act and the General Data Protection Regulation (GDPR)(HIPPA).
- **Enforcement:** The policy should specify the consequences for violating the email security policy, including disciplinary action and legal consequences if necessary.

Hence, organizations may help safeguard sensitive information and lower the risk of data breaches and other security incidents by creating an email security strategy.

WI FI SECURITY

Wireless network security is, therefore, the prime need of the hour. Maintaining network security is the way of designing, executing, and making sure about the security levels on a wireless computer network.

It is a subcategory of network security that protects a wireless computer network. Wireless network security primarily saves a wireless network from unauthorized and malicious access attempts. It is delivered through wireless devices (normally through a wireless router/switch) that encrypts and secures all wireless communication.

The use of an open or unsecured network can turn out to be extremely harmful to users. Adversaries using internet-connected devices can collect users' personal information and forge identities, affect financial and other confidential business data, and more. Therefore, Wi-Fi security best practices should always be considered by users.

While there are many different steps that can be taken to secure a wireless network, these 12 best practices are essential for ensuring that your data and devices are safe from malicious actors.

1. Enabling Two-Factor Authentication (2FA)

Two-factor authentication adds an extra layer of security to the login process. It requires users to enter both a username and password, as well as a code that is generated by an authenticator app. This makes it more difficult for someone to gain unauthorized access to the network.

To enable two-factor authentication, access the wireless router's configuration page and enable the feature. Be sure to download an authenticator app such as Google Authenticator or Authy and have it available when logging in.

You can also consider using passwordless authentication like cloud radius for even more robust protection. This is an important best practice because if someone does manage to get a hold of your password, they'll be able to access your network. By using a cloud-based solution, you can be sure that only authorized users will be able to access your network.

2. Using A Strong Password

Using a strong password is one of the most important best practices for wireless network security. A strong password is at least eight characters long and includes a mix of upper- and lower-case letters, numbers, and symbols. Passwords should be changed regularly to ensure that they remain secure.

3. Encrypting Data

Encrypting data is another important best practice for wireless network security. Data encryption scrambles data so that it can only be decrypted and read by authorized users. This helps to protect sensitive information from being accessed by unauthorized individuals.

Encryption can be implemented in a number of ways, including through the use of encryption software, hardware, or services. Make sure that employees are aware of the importance of encrypting sensitive data and that they know how to properly encrypt files.

4. Disabling SSID Broadcast

Disabling SSID broadcast is another best practice for wireless network security. When SSID broadcast is enabled, it allows anyone within range of the wireless network to see the network's name. You can disable SSID broadcast by accessing the wireless router's configuration page and disabling the SSID broadcast feature.

The goal is to make it more difficult for unauthorized individuals to connect to the network. The SSID can still be seen if someone is within range of the network and uses a wireless network scanner, but it will not be as easily accessible.

5. Using MAC Filtering

Using MAC filtering is another best practice for wireless network security. MAC addresses are unique identifiers assigned to devices that connect to a network.

By allowing only devices with specific MAC addresses to connect to the network, you can help to prevent unauthorized access. MAC filtering can be implemented by accessing the wireless router's configuration page and adding the MAC addresses of devices that are allowed to connect to the network.

6. Enabling WPA3 Security

Enabling WPA3 security is another best practice for wireless network security. WPA3 is the most recent and most secure wireless security protocol. It provides stronger protection than WPA2 and should be used whenever possible.

When shopping around for a router, make sure to look for ones that support this most recent security protocol. Earlier protocols were easier to compromise, so it is important to make sure that WPA3 is enabled.

7. Using A VPN

Using a VPN is another best practice for wireless network security. A VPN encrypts all traffic between a device and the VPN server, making it more difficult for someone to eavesdrop on the connection. This is especially important when using public Wi-Fi networks, as they are often less secure than private ones. Be sure to only use VPNs from trusted providers and make sure that employees are aware of the importance of using a VPN when working remotely.

8. Disabling Remote Administration

Disabling remote administration is another best practice for wireless network security. When remote administration is enabled, it allows anyone with the proper credentials to access the router's configuration page and make changes to the network. This can be a security risk, as it allows unauthorized individuals to potentially gain access to the network. To disable remote administration, access the wireless router's configuration page and disable the feature. This will help to prevent unauthorized access to the network.

9. Changing The Default Password

Changing the default password is another best practice for wireless network security. Many routers come with a default password that is easy to guess. This can be a security risk, as it allows unauthorized individuals to potentially gain access to the network.

To change the default password, access the wireless router's configuration page and change the password to something that is more difficult to guess. Be sure to choose a strong password that is at least 8 characters long and includes a mix of upper and lowercase letters, numbers, and symbols.

10. Using A Firewall

Using a firewall is another best practice for wireless network security. A firewall helps to protect the network by blocking incoming traffic that is not authorized. This can be especially important in preventing attacks from malware and other malicious software.

To use a firewall, access the wireless router's configuration page and enable the feature. There are typically two types of firewalls: network-based and host-based. Network-based firewalls are typically used in business environments, while host-based firewalls can be used on individual devices.

11. Disabling UPnP

Universal Plug and Play (UPnP) is a protocol that allows devices to automatically discover and connect to each other. This can be a security risk, as it allows unauthorized devices to potentially gain access to the network. To disable UPnP, access the wireless router's configuration page and disable the feature. You can also disable UPnP on individual devices by accessing the settings menu.

12. Disabling Unnecessary Services

You often find that routers come with a number of unnecessary services enabled. These can be a security risk, as they can provide potential attackers with information about the network. To disable unnecessary services, access the wireless router's configuration page and disable any services that are not needed. This will help to reduce the attack surface of the network. Common unnecessary services include things like telnet, SSH, and HTTP.

GUIDELINES TO CHOOSE A WEB BROWSER

The web browser is an application software to explore www (World Wide Web). It provides an interface between the server and the client and requests to the server for web documents and services. It works as a compiler to render HTML which is used to design a webpage. Whenever we search for anything on the internet, the browser loads a web page written in HTML, including text, links, images, and other items such as style sheets and JavaScript functions. Google Chrome, Microsoft Edge, Mozilla Firefox, and Safari are examples of web browsers.

To choose your web browser, you have to take into account criterias such as presentation, speed and security.

First, the presentation relates to the **visual appearance and the quality of the display**. Indeed, the visual aspect of your browser is very important because the human eye is attached to what it finds beautiful.

Secondly, there is speed, which alludes to **the speed at which search results load.** This point is very important since the ideal is to do research while saving time.

The last point is security. **It's the least considered by the majority of Internet users.** Indeed, we do not pay attention to it, yet browsing involves managing connection data.

SECURING WEB BROWSER

Web browser security consists of all measures, procedures, and policies necessary to protect users accessing the Internet from a web browser application.

Almost everyone online has a web browser available on their computer or mobile device. Since it is so common, hackers and other cybercriminals prefer to launch compromising attacks on this client-side application.

A web browser can store information for your convenience, but others may eventually access the information. Therefore, it provides a large surface area for exposure to email accounts, usernames, all sorts of passwords, and personal or corporate information. Attackers often target the web browser to hijack or sniff the web traffic from it. They may also use it as a means to access the device itself or any files available on it.

There are several ways that hackers can attack web browsers, including the following:

- **Malicious websites:** Hackers can create malicious websites designed to exploit vulnerabilities in web browsers or trick users into divulging sensitive information. For example, a hacker might create a website that looks like a legitimate login page but is actually designed to capture the user's login credentials.
- **Malicious ads:** Hackers can also use malicious ads, also known as "malvertising," to attack web browsers. These ads can contain malware or redirect users to malicious websites.
- **Malicious extensions:** Hackers can create malicious extensions or plugins for web browsers and distribute them through third-party websites or trick users into installing them. These extensions can contain malware or perform other malicious actions.
- **Exploits:** Hackers can also exploit vulnerabilities in web browsers or the software they are running on to gain access to a user's device or steal sensitive information.

To protect against these types of attacks, it is important to keep your web browser and any extensions or plugins that you have installed up to date, use caution when clicking on links, and use an antivirus program to scan your device for malware. Using a reputable web browser and enabling security features such as two-factor authentication and secure browsing (HTTPS) is also a good idea.

ANTIVIRUS

Antivirus software (antivirus program) is a security program designed to prevent, detect, search and remove viruses and other types of malware from computers, networks and other devices. Often included as part of a security package, antivirus software can also be purchased as a standalone option.

Typically installed on a computer as a proactive approach to cybersecurity, an antivirus program can help mitigate a variety of cyber threats, including keyloggers, browser hijackers, Trojan horses, worms, rootkits, spyware, adware, botnets, phishing attempts and ransomware attacks.

Due to the constantly evolving nature of cybercrimes and new versions of malware being released daily, including zero-day attacks, no antivirus program can offer detection and protection against all threat vectors.

How antivirus software works

Antivirus software typically runs as a background process, scanning computers, servers or mobile devices to detect and restrict the spread of malware. Many antivirus software programs include real-time threat detection and protection to guard against potential vulnerabilities and perform system scans that monitor device and system files, looking for possible risks.

Antivirus software usually performs the following basic functions:

- Scans directories or specific files against a library of known malicious signatures to detect abnormal patterns indicating the presence of malicious software.
- Enables users to schedule scans so they run automatically.
- Lets users initiate new scans at any time.
- Removes any malicious software it detects either automatically in the background or notifies users of infections and prompts them to clean the files.

To scan systems comprehensively, antivirus software must generally be given privileged access to the entire system. This makes antivirus software itself a common target for attackers, and researchers have discovered remote code execution and other serious vulnerabilities in antivirus software products in recent years.

Benefits of antivirus software

The purpose of antivirus software isn't only to defend a system against security threats and vulnerabilities, but also to provide real-time protection through automated vulnerability scans.

Antivirus software provides the following benefits:

- **Virus and malware protection.** The main benefit of antivirus software is to protect against malicious viruses, such as malware and spyware. Most cyber threats today present themselves as multipronged threat vectors that can attack system data, steal confidential information, spy on system resources and degrade system performance simultaneously. Therefore, having reliable antivirus software running at all times is imperative.
- **Protection against spam and pop-ups.** One of the most common ways viruses infiltrate and infect a system is through pop-up advertisements and spam-based webpages. Antivirus software keeps the system secure by automatically blocking pop-ups and spam coming from malicious websites.
- **Web protection.** Antivirus software helps protect against scam websites threat actors use to gather credit card and bank information from unsuspecting users. By restricting access to harmful websites, a reliable antivirus program can prevent users from accessing unauthorized networks.
- **Real-time protection.** Antivirus software acts as a real-time shield that scans each inbound file and program. Depending on the settings of the antivirus program, once an infected file or program is detected, it's either automatically deleted or moved to a quarantine folder for further analysis. A quarantined file is prevented from interacting with the rest of the machine and its programs to mitigate damage.
- **Boot-scan command.** Sophisticated viruses can often duplicate themselves while the system is active. However, an antivirus program can prevent a virus from self-replicating by invoking a boot-

scan command. This command shuts down the operating system (OS), restarts the computer and scans the entire hard drive for viruses and malware. During the scan, the virus is detected and doesn't get a chance to self-replicate due to the deactivation of the OS.

- **Dark web scanning.** Data from most data breaches, such as ransomware attacks, is often leaked on the dark web. Many antivirus tools can help organizations discover if their sensitive data is leaked on the dark web. For example, if they find an associated email address or account number on the dark web, they can notify the user and update the password to a new and more complex one.
- **Protection from external devices.** Most people regularly plug in external devices, such as hard drives and USB adapters, to their computers. Antivirus software scans all attached devices and peripherals to thwart potential viruses from entering the system through external sources.

GUIDELINES FOR SETTING UP A SECURE PASSWORD

A *Strong Password* is defined as a password that is reasonably difficult to guess in a short period of time either through human guessing or the use of specialized software.

Guidelines

The following are general recommendations for creating a Strong Password:
A Strong Password **should** -

- Be at least 8 characters in length
- Contain both upper and lowercase alphabetic characters (e.g. A-Z, a-z)
- Have at least one numerical character (e.g. 0-9)
- Have at least one special character (e.g. ~!@#$%^&*()_-+=)

Strong Passwords **do not** -

- Spell a word or series of words that can be found in a standard dictionary
- Spell a word with a number added to the beginning and the end
- Be based on any personal information such as user id, family name, pet, birthday, etc.

The following are several recommendations for maintaining a Strong Password:

- **Do not share your password with anyone for any reason**
  Passwords should not be shared with anyone, including any students, faculty or staff. In situations where someone requires access to another individual's protected resources, delegation of permission options should be explored. For example, Microsoft Exchange calendar will allow a user to delegate control of his or her calendar to another user without sharing any passwords. This type of solution is encouraged. Passwords should not be shared even for the purpose of computer repair. An alternative to doing this is to create a new account with an appropriate level of access for the repair person.
- **Change your password upon indication of compromise**
  If you suspect someone has compromised your account, change your password immediately. Be sure to change your password from a computer you do not typically use (e.g. university cluster computer). After resetting your password, report the incident to your local departmental administrator and/or the Information Security Office at iso-ir@andrew.cmu.edu.

- **Consider using a passphrase instead of a password**

  A passphrase is a password made up of a sequence of words with numeric and/or symbolic characters inserted throughout. A passphrase could be a lyric from a song or a favorite quote. Passphrases typically have additional benefits such as being longer and easier to remember. For example, the passphrase “My passw0rd is $uper str0ng!” is 28 characters long and includes alphabetic, numeric and special characters. It is also relatively easy to remember. It is important to note the placement of numeric and symbolic characters in this example as they prevent multiple words from being found in a standard dictionary. The use of blank spaces also makes a password more difficult to guess.
- **Do not write your password down or store it in an insecure manner**

  As a general rule, you should avoid writing down your password. In cases where it is necessary to write down a password, that password should be stored in a secure location and properly destroyed when no longer needed (see Guidelines for Data Protection). Using a password manager to store your passwords is not recommended unless the password manager leverages strong encryption and requires authentication prior to use. The ISO has vetted some password managers that meets these requirements.
- **Avoid reusing a password**

  When changing an account password, you should avoid reusing a previous password. If a user account was previously compromised, either knowingly or unknowingly, reusing a password could allow that user account to, once again, become compromised. Similarly, if a password was shared for some reason, reusing that password could allow someone unauthorized access to your account.
- **Avoid using the same password for multiple accounts**

  While using the same password for multiple accounts makes it easier to remember your passwords, it can also have a chain effect allowing an attacker to gain unauthorized access to multiple systems. This is particularly important when dealing with more sensitive accounts such as your Andrew account or your online banking account. These passwords should differ from the password you use for instant messaging, webmail and other web-based accounts.
- **Do not use automatic logon functionality**

  Using automatic logon functionality negates much of the value of using a password. If a malicious user is able to gain physical access to a system that has automatic logon configured, he or she will be able to take control of the system and access potentially sensitive information.

TWO-STEPS AUTHENTICATION

Two-factor authentication (2FA) is a security system that requires two distinct forms of identification in order to access something.

Two-factor authentication can be used to strengthen the security of an online account, a smartphone, or even a door. 2FA does this by requiring two types of information from the user—a password or personal identification number (PIN), a code sent to the user's smartphone (called a message authentication code), or a fingerprint—before whatever is being secured can be accessed.

Two-factor authentication is designed to prevent unauthorized users from gaining access to an account with nothing more than a stolen password. Users may be at greater risk of compromised passwords than they realize, particularly if they use the same password on more than one website. Downloading software and clicking on links in emails can also expose an individual to password theft.

Two-factor authentication is a combination of two of the following:

- Something you know (your password)
- Something you have (such as a text with a code sent to your smartphone or other device, or a smartphone authenticator app)
- Something you are (biometrics using your fingerprint, face, or retina)

2FA is not just applied to online contexts. It is also at work when a consumer is required to enter their zip code before using their credit card at a gas pump or when a user is required to enter an authentication code from an RSA Secure ID key fob to log in remotely to an employer’s system.

PASSWORD MANAGER

A password manager is a technology tool that helps internet users create, save, manage and use passwords across different online services. Many online services require a username and password to create an account and gain access to a specific service. Over time, users face a recurring choice: create unique passwords for each site, a challenge to remember, or reuse a single password repeatedly, a challenge to secure.

If a site is breached, exposing usernames and passwords, attackers try those passwords on other sites. These credential stuffing attacks -- the use of stolen credentials -- accounted for nearly half of the cyber-attacks in 2022, according to Verizon's yearly "Data Breach Investigations Report." Of course, sometimes, users simply forget a password, and the password reset cycle takes time, diminishing a user's overall experience.

A password manager is an attempt to improve password usability and security, enabling users to create unique, complex passwords for every online account without needing to remember them. All information is securely stored in a password vault and accessible via the password manager.

Password managers also help users manage accounts for online services and include the site or service name, web address, user account name and password. This makes a password manager crucial, even essential, to users dependent on a variety of services requiring usernames and passwords.

How does a password manager work?

The first time a user visits a site that requires a username and password while using a password manager, various outcomes can occur.

If the user has not previously created a username and password for the site, the password manager can help create a highly randomized and unique password. When the user puts the cursor in the input field for the password, the password manager prompts the user to create a new, strong password. Once the username and new password have been entered, the password manager typically prompts the user to save the information. The username and password are then securely stored in the password manager. The next time the user visits the same site, the password manager opens a prompt window, typically above where the user input is required, asking if the user wants to input the previously saved information.

On the other hand, when the user already has a username and password but visits a site for the first time with a password manager installed, it prompts the user to save account information for future visits.

Benefits of using a password manager

Password managers provide users with several benefits to accessing and using passwords on many devices, including the following:

- **Convenience.** With all the username and password combinations that internet users require, a password manager makes it significantly easier and faster to create, manage and use passwords.
- **Autofill.** A core capability of a password manager is the ability to auto fill user credentials when a login form is detected for which the system has a username and password.
- **Minimization of password reuse.** With the integrated capability to help users create new, unique passwords for every site they use, a password manager can help to minimize or eliminate password reuse.
- **Stronger passwords.** A password manager can create complex and strong passwords that are unique and more difficult for an attacker to crack.
- **Increased security.** Password managers encrypt user passwords and provide safe access. They can also alert users when credentials have been part of a data breach or phishing attempt.
- **Password mobility.** Many password managers enable synchronization of usernames and passwords across multiple devices, from desktop to mobile.
- **Compliance with best practices.** Having a password manager is considered a best practice for authentication and lifecycle management, according to the National Institute of Standards and Technology.

Types of password managers

Because the browser is the primary way most users access sites and services, the most well-known and easily accessible type of password manager is the browser-based approach. All major browser platforms, including Google Chrome, Apple Safari, Microsoft Edge and Mozilla Firefox, have long had some form of integrated password manager.

Originally, all browser-based password managers were also local password managers; they only ran and saved usernames and passwords on the local device. That's no longer the case. Many browser vendors include synchronization capabilities that enable password management across multiple devices. For example, Apple Safari's password manager is integrated with Apple iCloud Keychain, which enables secured credential sharing across devices. Besides browser-based password managers, other password managers to choose from include the following.

Local password managers

As mentioned, the first password managers were local password managers. An application on a user's device stores and manages user credentials on that specific device. Examples of local password managers are the open source Password Safe and KeePass applications.

Cloud-based password managers

These password managers enable users to retrieve passwords from any internet-connected device by storing them in the cloud. Among the vendors that provide cloud-based password managers are 1Password, Dashlane and LastPass.

Enterprise password managers

For managing passwords within a business, an enterprise password manager is built for the task. These password managers can also be integrated with role-based access control and corporate directory technology and often include privileged access management features as well. Vendors in this space include Cyber Ark and Delinea, formerly known as Thycotic.

Hardware password managers

Hardware password managers work in various ways. Some hardware devices, often deployed as USB keys, functionally hold a token that enables access to an account. Other hardware devices act solely as secure offline storage to manage passwords. Examples of hardware or token password managers are YubiKey and OnlyKey, as well Google Titan Key.

UNIT – 3

SECURITY GUIDELINES FOR SOCIAL MEDIA SECURITY

Social media security involves a set of policies and procedures used to safeguard user information, privacy and accounts on various social networking sites. It provides security against online harassment, unauthorized access, phishing attacks, malware, data breaches and identity theft. By implementing the right security measures, users can significantly lower their chance of being a target of cyber-attacks and ensure a safer online experience.

1. Develop a strong password policy

Brands should create a strong password policy and instruct employees to use it when logging into their social media accounts. Passwords should include intricate combinations of uppercase, lowercase, digits and special characters. They should also be updated regularly, and the same passwords shouldn't be used on different platforms. Avoid using common passwords or information that could be guessed, such as birthdates or pet names.

2. Enable two-factor authentication

Two-factor authentication amplifies security by requiring users to submit a second form of verification, such as a special code sent to their mobile device, in addition to their password. This approach substantially reduces the risk of unauthorized access, even if the initial credentials have been compromised. Both X, formerly Twitter and Facebook have two-factor authentication solutions. Once activated, you'll get a unique code on your phone that you'll need to input to complete the login process whenever someone tries to log in to your account from a new device.

3. Educate employees on security awareness

Security breaches can be avoided with regular training and updates on new security risks. Brands should regularly hold training sessions to inform employees of the potential hazards of social media and how to identify and react to potential threats. Employees should be taught how to spot phishing efforts, suspicious sites and social engineering tactics. Brands should also implement guidelines for using social media, managing passwords and handling data. To learn about security enhancements and best practices, follow reliable cybersecurity blogs and websites, and the directions that official social media accounts of the platforms you use provide.

4. Limit access privileges

Brands should limit access rights by allowing only authorized staff access to social media profiles. Ensure that only those employees who need access to certain accounts and functionalities for their jobs are granted administrator rights. To retain control over account security, access rights should be verified and updated regularly**.**

5. Monitor and evaluate account activity

Social media accounts should be frequently monitored to identify any unauthorized access or questionable behavior. Brands should create a procedure for content approval and review before the content is published. Keep a record of logins, posting schedules and account configuration alterations. And make sure that you respond immediately to any security or unauthorized access problems.

6. Use third-party applications with caution

Carefully examine the security procedures and reputation of third-party apps before integrating them into your social media accounts. Pay attention to the permissions given to these applications because they could give access to private information that they shouldn’t be privy to. Regularly check permissions and revoke them for unnecessary applications.

7. Protect mobile devices

With the increasing usage of mobile devices for social media management, it’s necessary to take precautions for the safe usage of these devices. Ensure that these devices have activated biometric or secure password authentication. The data that’s saved your devices should be encrypted, and operating systems and software should be updated often to fix security flaws.

8. Update and patch software regularly

Attackers may take advantage of outdated software, jeopardizing the security of your social media accounts. All social media management applications and platforms should be updated with the most recent security patches and upgrades. Brands should perform frequent scans for vulnerabilities and promptly implement any pending patches.

9. Keep an eye out for free Wi-Fi

Brand employees should avoid using public Wi-Fi networks to access their social media accounts. This is because public Wi-Fi hotspots are usually insecure, and it’s easier for hackers to intercept data on these networks. Instead, a trustworthy, dedicated Wi-Fi network or a private and secure internet connection with a strong password would be ideal.

10. Update privacy settings frequently

Social media platforms often change their privacy settings and available security alternatives. Brands should stay mindful and updated about these changes and use the available tools to manage who can view their posts, reach them and access their personal information. Privacy settings should be reviewed and modified regularly so your brand can retain control over its online visibility.

TIPS AND BEST PRACTICES FOR SAFER SOCIAL NETWORKING

Social networking is a method of communication with people through online platforms such as Facebook, LinkedIn, and Twitter. Over the years, social networking has become an important part of life for both adults and teens. The popularity is due to the ability of meeting the needs and interests of a vast majority of people. For teens it is a way to socialize with friends, by sharing the latest events, photos and videos. Adults use social platforms for the same reason as teens, while also utilizing each platform in a professional manner as well. It is a valuable tool for businesses in that it allows them to interact with like-minded professionals, customers and other businesses. With all the benefits social networking offers, it is easy to overlook the risks that are involved. Said risks include threats of criminal activity, such as, stalking, bullying, identity theft, and hacking. Also, users may fall prey to impersonators who can cause damage to their reputation and standing with the very people they are trying to network with. To make the best use of social networking while avoiding the risks, users will need to understand and follow a set of basic safety tips that are easy to remember and highly effective.

- **Manage your privacy settings.** Learn about and use the privacy and security settings on your social networking sites. They help you control who sees what you post and manage your online experience in a positive way. You'll find some information about Facebook privacy settings at the bottom of this webpage.
- **Remember: once posted, always posted.** Protect your reputation on social networks. What you post online stays online. Think twice before posting pictures you wouldn't want your parents or future employers to see. Recent research found that 70% of job recruiters rejected candidates based on information they found online.
- **Build a positive online reputation.** Recent research also found that recruiters respond to a strong, positive personal brand online. So demonstrate your mastery of the environment and showcase your talents.

- **Keep personal info personal.** Be careful how much personal info you provide on social networking sites. The more information you post, the easier it may be for someone to use that information to steal your identity, access your data, or commit other crimes such as stalking.

- **Protect your computer.** Security start with protecting your computer. Install Antivirus software. Keep your operating system, web browser, and other software current.
  Visit Microsoft support for information on automatically installing the latest security updates for Office 365 and Windows.

- **Know what action to take.** If someone is harassing or threatening you, remove them from your friends list, block them, and report them to the site administrator.

- **Use strong passwords.** Make sure that your password is at least eight characters long and consists of some combination of letters, numbers, and special characters (for example, +, @, #, or $).

- **Be cautious on social networking sites.** Even links that look they come from friends can sometimes contain harmful software or be part of a phishing attack. If you are at all suspicious, don't click it. Contact your friend to verify the validity of the link first.

BASIC SECURITY FOR WINDOWS

Windows 10 features a series of tools to help you protect your computer from threats like viruses and other malware. The three main security tools are −

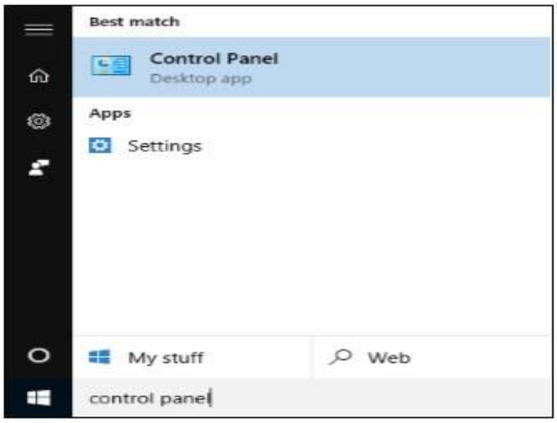
- User Account Control
- Windows Defender
- Windows Firewall

User Account Control

The Windows User Account Control is a tool that warns you when someone or something attempts to change your computer system settings. When this happens, the screen will alert you until an Administrator can confirm the change. This helps protect your computer against accidental changes or malicious software altering your settings.

Initially, this User Account Control is set at a moderate to high level, which means it will notify you only when an application tries to make changes to your computer. However, you can change this setting to your desired level by following these steps −

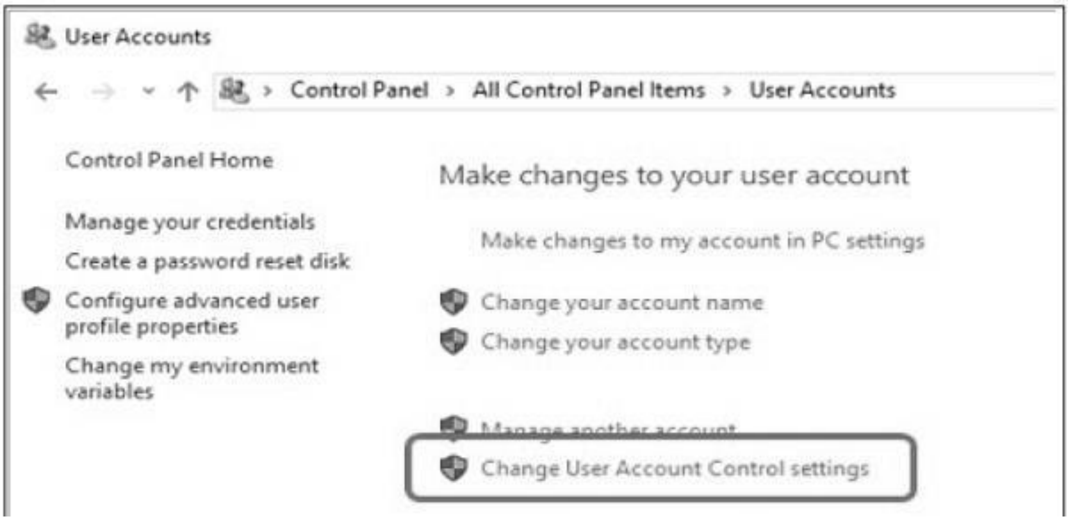
Step 1 − Open the **Control Panel** by searching for it in the Search bar.



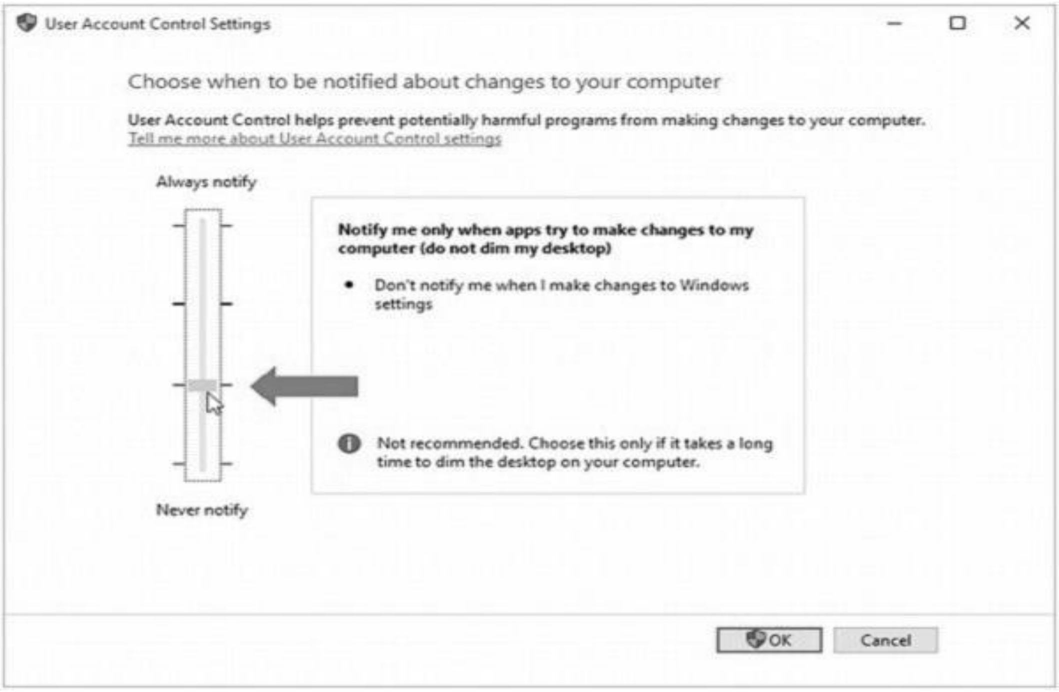
control panel

Step 2 − After the Control Panel is open, choose **User Accounts**.

After choosing User Accounts, click on “Change User Account Control settings”.


User Accounts
Control Panel > All Control Panel Items > User Accounts
Control Panel Home
Manage your credentials
Create a password reset disk
Configure advanced user profile properties
Change my environment variables
Make changes to your user account
Make changes to my account in PC settings
Change your account name
Change your account type
Manage another account
Change User Account Control settings

In the **User Account Control Settings**, you can move the slider to the desired position. Windows 10 will give you a summary of how your system will behave under that level.



Choose when to be notified about changes to your computer

User Account Control helps prevent potentially harmful programs from making changes to your computer.
Tell me more about User Account Control settings

Notify me only when apps try to make changes to my computer (do not dim my desktop)

- Don't notify me when I make changes to Windows settings

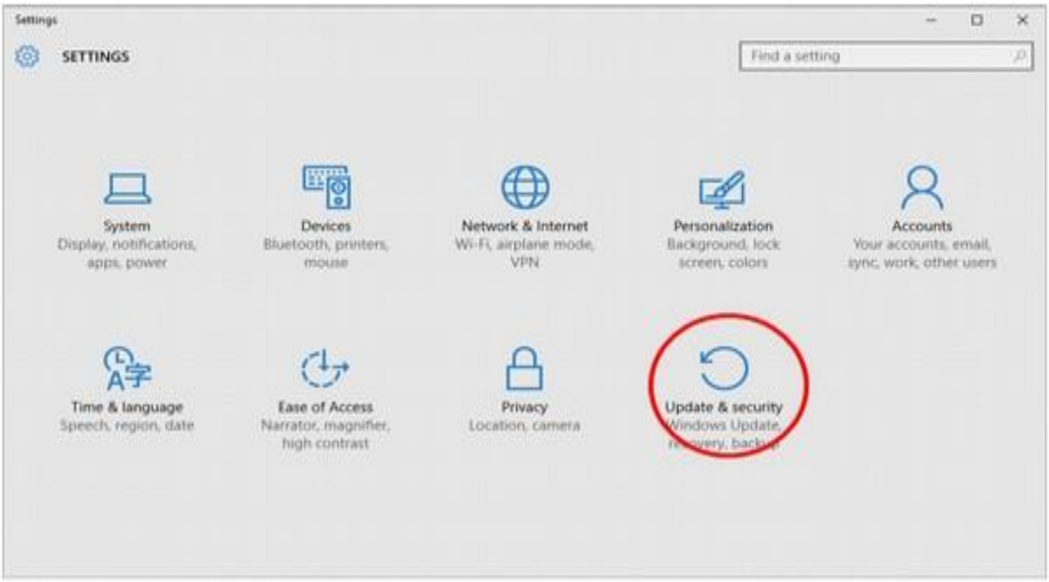
Not recommended. Choose this only if it takes a long time to dim the desktop on your computer.

Windows Defender

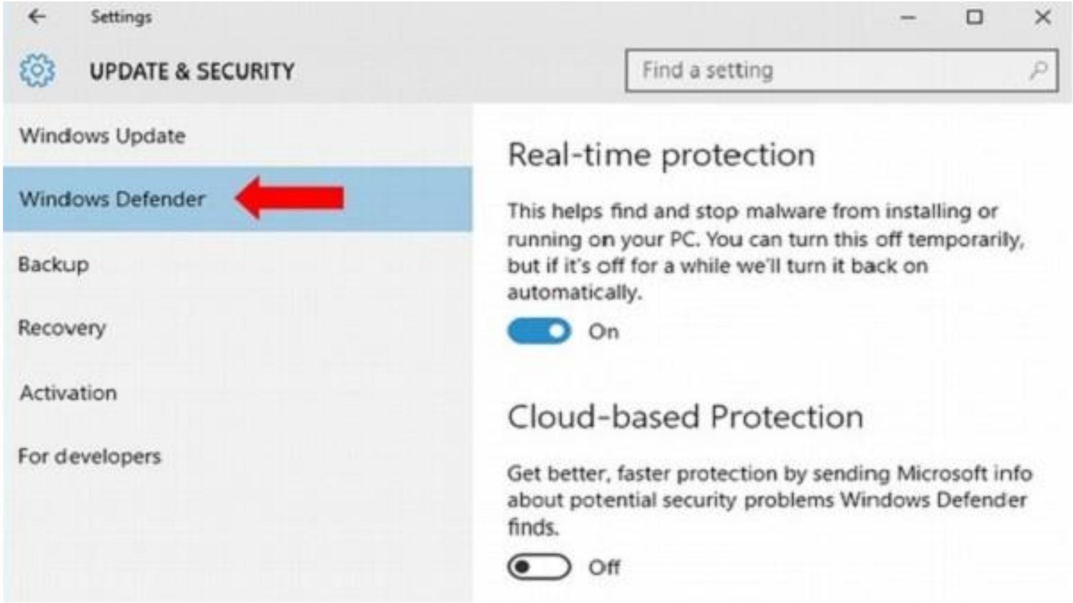
Windows Defender is an antivirus and malware protection included in your operating system. It allows you to scan your computer for malicious software, while also checking each file or program you open.

To configure Windows Defender, follow these steps −

Step 1 − Go to **SETTINGS** and select **Update & security**.


Settings
SETTINGS
Find a setting
System
Display, notifications, apps, power
Devices
Bluetooth, printers, mouse
Network & Internet
Wi-Fi, airplane mode, VPN
Personalization
Background, lock screen, colors
Accounts
Your accounts, email, sync, work, other users
Time & language
Speech, region, date
Ease of Access
Narrator, magnifier, high contrast
Privacy
Location, camera
Update & security
Windows Update, recovery, backup

Step 2 − In the **UPDATE & SECURITY** window, select **Windows Defender**.



Real-time protection

This helps find and stop malware from installing or running on your PC. You can turn this off temporarily, but if it's off for a while we'll turn it back on automatically.

On

Cloud-based Protection

Get better, faster protection by sending Microsoft info about potential security problems Windows Defender finds.

Off

Here you can customize settings like turning off real-time protection or activating cloudbased protection, which allows Defender to send Microsoft information about security threats it finds.

Windows Firewall

Windows Firewall prevents unauthorized access from outside to get into your computer. By default, it is turned on to protect your computer and your network.

If you want to customize your Firewall, follow these steps −

Step 1 − Open the **Control Panel** by searching for it in the Search bar.

Step 2 − When the Control Panel is open, choose **Windows Firewall**.

Step 3 − In the **Windows Firewall** window, you can customize the settings of it by turning it on or off or choosing when to protect your computer.

USER ACCOUNT PASSWORD

- Choose good passwords as initial passwords for accounts.
- Use different passwords as initial passwords for different accounts.
- Request users change the initial password immediately upon receiving the new password.
- Change all system default passwords, including service accounts after installing a new system.
- Ask users to change their passwords regularly, for example every 90 days.
- Automatically suspend a user account after a pre-defined number of invalid logon attempts.
- Restrict a suspended account to only allow reactivation by manual action controlled by the system/security administrator.
- Prevent users from using passwords shorter than a pre-defined length, or re-using previously used or old passwords.
- Don't send unencrypted passwords to users especially via Internet email.
- Don't disclose or reset passwords on behalf of unidentified users.
- Don't allow public access to a password database, such as UNIX password files.

SMARTPHONE SECURITY GUIDELINES: INTRODUCTION TO MOBILE PHONES

A mobile phone (also called mobile cellular network, cell phone or hand phone) is an example of mobile communication (wireless communication). It is an electric device used for full duplex two way radio telecommunication over a cellular network of base stations known as cell site.

There are following advantages of mobile communication:

- **Flexibility:** Wireless communication enables the people to communicate with each other regardless of location. There is no need to be in an office or some telephone booth in order to pass and receive messages.
- **Cost effectiveness:** In wireless communication, there is no need of any physical infrastructure (Wires or cables) or maintenance practice. Hence, the cost is reduced.
- **Speed:** Improvements can also be seen in speed. The network connectivity or the accessibility was much improved in accuracy and speed.
- **Accessibility:** With the help of wireless technology easy accessibility to the remote areas is possible. For example, in rural areas, online education is now possible. Educators or students no longer need to travel to far-flung areas to teach their lessons.
- **Constant connectivity:** Constant connectivity ensures that people can respond to emergencies relatively quickly. For example, a wireless device like mobile can ensure you a constant connectivity though you move from place to place or while you travel, whereas a wired landline can't.

SMARTPHONE SECURITY

1. Set PINs and passwords. To prevent unauthorized access to your phone, set a password or Personal Identification Number (PIN) on your phone's home screen as a first line of defense in case your phone is lost or stolen. When possible, use a different password for each of your important log-ins (email, banking, personal sites, etc.). You should configure your phone to automatically lock after five minutes or less when your phone is idle, as well as use the SIM password capability available on most smartphones.

2. Do not modify your smartphone's security settings. Do not alter security settings for convenience. Tampering with your phone's factory settings, jailbreaking, or rooting your phone undermines the built-in security features offered by your wireless service and smartphone, while making it more susceptible to an attack.

3. Backup and secure your data. You should backup all of the data stored on your phone – such as your contacts, documents, and photos. These files can be stored on your computer, on a removal storage card, or in the cloud. This will allow you to conveniently restore the information to your phone should it be lost, stolen, or otherwise erased.

4. Only install apps from trusted sources. Before downloading an app, conduct research to ensure the app is legitimate. Checking the legitimacy of an app may include such thing as: checking reviews, confirming the legitimacy of the app store, and comparing the app sponsor's official website with the app store link to confirm consistency. Many apps from untrusted sources contain malware that once installed can steal information, install viruses, and cause harm to your phone's contents. There are also apps that warn you if any security risks exist on your phone.

5. Understand app permissions before accepting them. You should be cautious about granting applications access to personal information on your phone or otherwise letting the application have access to perform functions on your phone. Make sure to also check the privacy settings for each app before installing.

6. Install security apps that enable remote location and wiping. An important security feature widely available on smartphones, either by default or as an app, is the ability to remotely locate and erase all of the data stored on your phone, even if the phone's GPS is off. In the case that you misplace your phone, some applications can activate a loud alarm, even if your phone is on silent. These apps can also help you locate and recover your phone when lost. Visit CTIA for a full list of anti-theft protection apps.

7. Accept updates and patches to your smartphone's software. You should keep your phone's operating system software up-to-date by enabling automatic updates or accepting updates when prompted from your service provider, operating system provider, device manufacturer, or application provider. By keeping your operating system current, you reduce the risk of exposure to cyber threats.

8. Be smart on open Wi-Fi networks. When you access a Wi-Fi network that is open to the public, your phone can be an easy target of cybercriminals. You should limit your use of public hotspots and instead use protected Wi-Fi from a network operator you trust or mobile wireless connection to reduce your risk of exposure, especially when accessing personal or sensitive information. Always be aware when clicking web links and be particularly cautious if you are asked to enter account or log-in information.

9. Wipe data on your old phone before you donate, resell, or recycle it. Your smartphone contains personal data you want to keep private when you dispose your old phone. To protect your privacy, completely erase data off of your phone and reset the phone to its initial factory settings. Then, donate, resell, recycle, or otherwise properly dispose of your phone.

10. Report a stolen smartphone. The major wireless service providers, in coordination with the FCC, have established a stolen phone database. If your phone is stolen, you should report the theft to your local law enforcement authorities and then register the stolen phone with your wireless provider. This will provide notice to all the major wireless service providers that the phone has been stolen and will allow for remote "bricking" of the phone so that it cannot be activated on any wireless network without your permission.

ANDROID SECURITY

Android's popularity and open marketplace mean a far wider range of security apps are available. The security of your Android operating system and device out of the box may vary, but with the right apps, you can take it to the same level of security as iOS or even further.

Below are the security features provided by Android to make the Android devices you develop as secure as possible.

App sandbox

The Android platform takes advantage of the Linux user-based protection to identify and isolate app resources. To do this, Android assigns a unique user ID (UID) to each Android app and runs it in its own process. Android uses this UID to set up a kernel-level App Sandbox.

App signing

App signing allows developers to identify the author of the app and to update their app without creating complicated interfaces and permissions. Every app that runs on the Android platform must be signed by the developer.

Authentication

Android uses the concept of user-authentication-gated cryptographic keys that requires cryptographic key storage and service provider and user authenticators. On devices with a fingerprint sensor, users can enroll one or more fingerprints and use those fingerprints to unlock the device and perform other tasks. The Gatekeeper subsystem performs device pattern/password authentication in a Trusted Execution Environment (TEE).

Android 9 and higher includes Protected Confirmation, which gives users a way to formally confirm critical transactions, such as payments.

Biometrics

Android 9 and higher includes a BiometricPrompt API that app developers can use to integrate biometric authentication into their apps in a device- and modality-agnostic fashion. Only strong biometrics can integrate with BiometricPrompt.

Encryption

Once a device is encrypted, all user-created data is automatically encrypted before committing it to disk and all reads automatically decrypt data before returning it to the calling process. Encryption ensures that even if an unauthorized party tries to access the data, they won’t be able to read it.

Keystore

Android offers a hardware-backed Keystore that provides key generation, import and export of asymmetric keys, import of raw symmetric keys, asymmetric encryption and decryption with appropriate padding modes, and more.

Security-Enhanced Linux

As part of the Android security model, Android uses Security-Enhanced Linux (SELinux) to enforce mandatory access control (MAC) over all processes, even processes running with root/superuser privileges (Linux capabilities).

Trusty Trusted Execution Environment (TEE)

Trusty is a secure Operating System (OS) that provides a Trusted Execution Environment (TEE) for Android. The Trusty OS runs on the same processor as the Android OS, but Trusty is isolated from the rest of the system by both hardware and software.

Verified Boot

Verified Boot strives to ensure all executed code comes from a trusted source (usually device OEMs), rather than from an attacker or corruption. It establishes a full chain of trust, starting from a hardware-protected root of trust to the bootloader, to the boot partition and other verified partitions.

IOS SECURITY

iOS has been one of the most popular mobile operating system in the world ever since it was first released in 2007. As of June 2014, Apple’s App Store contained more than 1.2 million iOS applications, which have collectively been downloaded more than 60 billion times.

iOS was designed and created by Apple Inc, it is distributed exclusively for Apple hardware. iOS protects not only the data stored in the iOS device, but also the data transmitted on networks when using internet services. iOS provides advanced and sophisticated security for iOS devices and it's also very easy to use. Users don't need to spend a lot of time on security configurations, as most of the security features have been automatically configured by iOS. iOS also supports biometric authentication (Touch ID), which has recently been incorporated into iOS devices, users can easily use their fingerprints to perform private and sensitive tasks such as unlocking the iPhone and making payments.

System security is central to security in iOS. It makes the hardware and software securely integrated with each other such that every component in iOS is secure and trusted. Fig.1 is a high-level overview of iOS security architecture, the details are explained in the following sections.

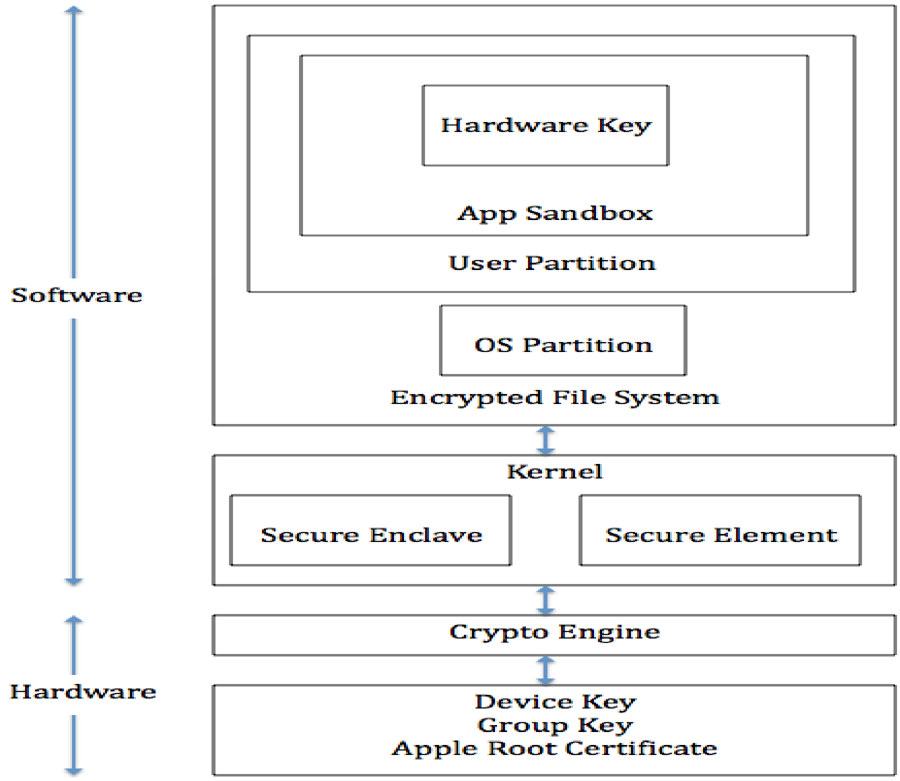


Fig.1 Security architecture diagram of iOS

2.1 Secure booting process

During the booting process, iOS uses a mechanism called "secure boot chain" to ensure that the low-level software is not compromised and iOS is running on a validated iOS device. Each step in secure boot chain verifies if the next step of chain is valid and signed by Apple. The booting process will only proceed to the next step of chain if the verification succeeds.

When you turn on an iOS device, the processor first executes the code from Boot ROM (read-only-memory). The code in Boot ROM is created during chip fabrication, hence it is trusted and immutable. The code in Boot ROM also contains the Apple Root CA public key, which will be used to verify if Low-Level Bootloader (LLB) is signed by Apple. If LLB is valid, the processor will run the next-stage bootloader, iBoot, which will in turn verify and run the iOS kernel.

2.2 Secure Enclave

The Secure Enclave is a coprocessor for Apple’s A-series processor. It has its own secure boot separated from the application processor, communication between it and the application processor is highly encapsulated. Its tasks include key management, processing cryptographic operations and maintaining the data integrity.

Each Secure Enclave comes with a unique ID (UID) during the fabrication. Other parts of the system don’t have access to UID, neither does Apple. UID is used to encrypt the Secure Enclave’s memory space and data of files stored in the file system.

The Secure Enclave is also responsible for decrypting and processing the fingerprints received from the Touch ID, verifying if the coming fingerprints match the registered fingerprints. The application processor forwards the fingerprints data to the Secure Enclave. Because the fingerprints data is encrypted with a session key between the Secure Enclave and the Touch ID, the application processor can’t read it.

2.3 Touch ID Security

Touch ID is a fingerprints sensor that can read fingerprints from the user. A user who passes the fingerprints verification can have secure access to the device, such as unlocking the iOS device, making purchases from the App Store, and making secure payment through Apple Pay (More information in the Apple Pay section).

When the user touches the home button, the capacitive steel ring on the home button detects the finger and activates the Touch ID sensor. Then Touch ID scans the fingerprints and sends a 88-by-88-pixel, 500-ppi raster scan to the Secure Enclave for authentication. The scan is vectorized for analysis and temporarily stored in encrypted memory in the Secure Enclave. After authentication, it is discarded.

UNIT - IV

CYBER SECURITY INITIATIVES IN INDIA

Initiatives Taken by Indian Government for Cyber Security were

1. The Indian Computer Emergency Response Team (CERT-In)

- The advancement in the Indian Computer Emergency Response Team (CERT-In), which operates as the national agency to address the country’s cyber security, has helped reduce the rate of cyber attacks on government networks

2. Cyber Surakshit Bharat

- Aiming to strengthen the cybersecurity ecosystem in India and following the Government’s vision of a “digital India,” the Ministry of Electronics and Information Technology (MeitY) has launched the Cyber Surakshit Bharat initiative
- The program was in partnership with the National Electronic Governance Division (NeGD)

3. National Critical Information Infrastructure Protection Center (NCIIPC)

- NCIIPC is a central government establishment, formed to protect critical information about our country, which has an enormous impact on national security, economic growth, and public health care

NCIIPC has mainly identified the following as “critical sectors”-

- Power & Energy
- Banking, Financial Services & Insurance
- Telecom Transport
- Government
- Strategic & Public Enterprises

4. Appointment of Chief Information Security Officers

- The Indian Government has published a written guideline for CISOs of government organizations, outlining best practices for safeguarding apps, infrastructure, and compliance
- Chief Information Security Officers (CISOs) can identify and document the security requirements that may arise with each technical innovation

5. Personal Data Protection Bill

- The most important one for Indian citizens is the approval of the Personal Data Protection Bill by the Union Government to protect Indian users from global breaches, which focuses on data localization
- The bill involves the storage and processing of any critical information related to people only in India
- It strictly states that individuals’ sensitive personal data is to be stored locally; however, it can be processed abroad under certain conditions
- The bill also aims to make social media companies more accountable and push them to solve the spread of offensive content

6. Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Center)

- The “Digital Swachhta Kendra” (Botnet Cleaning and Malware Analysis Center) is a part of the Government of India’s Digital India drive, overseen by the Ministry of Electronics and Information Technology (MeitY), determined to make secure cyberspace all through India by distinguishing botnet contaminations and advising, empowering cleaning, and end-client security systems to forestall new diseases
- The “Cyber Swachhta Kendra” (Botnet Cleaning and Malware Analysis Center) is intended to address the goals of the “National Cybersecurity Policy,” which calls for the development of a secure cybernetic ecosystem in the country
- The centre works in close coordination and collaboration with Internet service providers and antivirus/product companies
- The website provides users with information and tools to help them protect their systems/devices. Following Section 70B of the Information Technology Act 2000, this centre is run by the Indian Computer Emergency Response Team (CERT-In)

7. National Cyber Security Policy, 2013

- The Policy’s goal is to create safe and resilient cyberspace for citizens, businesses, and the Government
- The mission is to provide protection to cyberspace information and infrastructure, develop capabilities to prevent and respond to cyberattacks, and minimize damage through coordinated efforts of institutional structures, people, processes, and technology
- To create a workforce of 500,000 trained cybersecurity professionals in the next 5 years through capacity building, skills development and training
- Through appropriate legislative intervention, enable effective cybercrime prevention, investigation, and prosecution, as well as the enhancement of law enforcement capabilities.

IMPORTANCE OF CYBER SECURITY

Cyber security is important because it safeguards individuals and organizations against cyber attacks and theft or loss of sensitive and confidential information. Cybersecurity can monitor systems to protect personal data (PII, PHI, financial details etc.), trade secrets, intellectual property and any sensitive government information.

Obtaining a cybersecurity certification can help you protect yourself against fraud and online assaults!

Here are the 11 key advantages of Cyber Security for business:

- Protects personal data
- Helps preserves reputation
- Enhances productivity
- Assists the remote workspace
- Regulation compliance
- Improves cyber posture
- Better data management
- Helps educate and train the workforce
- Helps maintain trust and credibility
- Streamline access control
- Supports the IT team

Protects personal data

For businesses or individual users, personal data is the most valuable commodity. Malware can collect personal information and may jeopardize employees, customers’ privacy, or organizations. Cyber security protects data against internal as well external threats, whether accidental or with malicious intent helping employees access the internet as and when required without cyber attacks threats.

Helps preserves reputation

Customer retention and brand loyalty, for any organization, take years to build. Business reputation is damaged severely in case of data breaches. With a cyber security system in place, organizations can avoid sudden setbacks. Technologies such as network security and cloud security can strengthen access and authentication. This can open the pathway to future recommendations, ventures, and expansions.

Enhances productivity

As technology evolves, cybercriminals are employing sophisticated ways to breach data. Viruses negatively impact productivity by affecting networks, workflows, and functioning. The organization may come to a standstill due to the firm's downtime. With measures such as automated backups and improved firewalls, firms can improve their productivity, making it one of the most promising cyber security benefits.

Assists the remote workspace

The remote working model has led employees working from different locations to access multiple remote models for their workflows. It may be unsettling for organizations to circulate their sensitive data across the globe, where cybercrimes can occur through IoT, Wi-Fi, and personal devices.

It is substantial for businesses to protect sensitive data as remote work has led to an increase in the average data breach cost by $137,000. Sensitive data, strategies, and analytics are always vulnerable to being hacked and leaked. However, cyber security serves as a secure centre to store data and can also protect home Wi-Fi from tracking users' data.

Regulation compliance

Regulatory bodies such as HIPAA, SOC, PCI DSS, and GDPR play a substantial role in protecting individual users and organizations. Failure to comply with these regulations attracts heavy penalties.

Improves cyber posture

Cybersecurity provides organizations with comprehensive digital protection giving employees flexibility, liberty, and safety to access the internet. Sophisticated cyber security technology tracks all systems in real-time on a single dashboard with one click. This strategy allows businesses to act and respond in the event of a cyber-attack with automation for smoother operations, strengthening cybersecurity protocols against threats.

Better data management

Data forms the crux of marketing and product strategies. Losing it to hackers or competitors may result in laying the groundwork from scratch, giving a competitive edge to other companies. Hence, to ensure that data security regulations are implemented perfectly, organizations must consistently monitor their data. In addition to security, cybersecurity assists in operational efficiency as well.

Helps educate and train the workforce

You can add a layer of safety to your organization's daily operations by educating the workforce about potential risks such as ransomware, data breaches, spyware, and more. The employees will be less vulnerable to phishing attacks and know the right course of action in case anything goes wrong.

Helps maintain trust and credibility

Cyber security helps lay the foundation of trust and credibility amongst customers and investors. Breaches impact the reputation of an organization resulting in a dwindling audience base drastically. In contrast, the customer base increases when the organization has a history of safeguarding business and customer data.

Streamline access control

Organizations feel under control of all the tasks by controlling the internal and external processes. Companies can focus on other meaningful tasks enabling them to establish accountability for strategic management. Access to systems, computers, and resources is streamlined, hence reducing cybercrime threats.

Supports the IT team

Cyber-attacks attract fines from regulators and customers' claims, resulting in low sales and revenue, affecting crucial aspects of continuity. Additionally, cybercrimes can halt daily operations. With the advancement of technology, sophisticated hacking practices have evolved. The IT team should stay up to date with the rapidly evolving changes in cyberspace.

A skilled IT team equipped with tools, techniques, and assistance, as well as comprehensive knowledge, can skillfully handle even the most advanced cybercrime.

CYBER SECURITY EXERCISE

Cyber security exercises provide opportunities for organizations to demonstrate critical capabilities and reveal how effectively they integrate people, processes, and technology to protect their critical information, services, and assets. The exercises can help train organizations to improve their ability to mitigate impacts to business from cyber threats and attacks.

NIST SP 800-84 defines that exercise is a simulation of an emergency designed to validate the viability of one or more aspects of an IT plan. In an exercise, personnel with roles and responsibilities in a particular IT plan meet to validate the content of a plan through discussion of their roles and their responses to emergency situations, execution of responses in a simulated operational environment, or other means of validating responses that do not involve using the actual operational environment. Exercises are scenario-driven, such as a power failure in one of the organization's data centers or a fire causing certain systems to be damaged, with additional situations often being presented during the course of an exercise. There are several types of exercises, and this publication focuses on the following two types that are widely used by single organizations in TT&E programs:

- **Tabletop Exercises**. Tabletop exercises are discussion-based exercises where personnel meet in a classroom setting or in breakout groups to discuss their roles during an emergency and their responses to a particular emergency situation. A facilitator presents a scenario and asks the exercise participants questions related to the scenario, which initiates among the participants a discussion about roles, responsibilities, coordination, and decision-making. A tabletop exercise is discussion-based only and does not involve deploying equipment or other resources.

- **Functional Exercises.** Functional exercises allow personnel to validate their operational readiness for emergencies by performing their duties in a simulated operational environment. Functional exercises are designed to exercise the roles and responsibilities of specific team members, procedures, and assets involved in one or more functional aspects of a plan (e.g. communications, emergency notifications, IT equipment setup). Functional exercises vary in complexity and scope, from validating specific aspects of a plan to full-scale exercises that address all plan elements. Functional exercises allow staff to execute their roles and responsibilities as they would in an actual emergency situation but in a simulated manner.

CYBER SECURITY IN CURRICULUM

Cyber Security awareness is the knowledge and understanding individuals have about protecting digital systems and data. It involves recognizing cyber threats, understanding associated risks, and adopting safe practices.

This awareness aims to defend both individuals and organizations from cyber incidents, typically nurtured through training and ongoing education.
This preparation is crucial in education since school districts are a treasure trove of personal data about staff, students, and their parents, making them a prime target for data breaches.

Additionally, most teachers are learning about several new technological platforms to perform their job, from teaching to grading and communicating with parents. This type of situation is particularly dangerous from a cyber security standpoint since users might not be able to detect phishing or spoofing attempts due to being unfamiliar with the new platforms being introduced to them.

Common Cyber Incidents in the Education Sector

A recent survey revealed that most K-12 schools devote less than 8% of their funding to cyber security. Cyber attacks against these educational institutions aim to initiate a data breach via either phishing, website spoofing, malware, or a combination of these tactics.
Another common cyber attack in education is ransomware since schools are now heavily reliant on software to operate. Locking down their network can bring the entire institution to a crawl and force the administrators to comply with hackers' demands.

Phishing

Education software is often centered around notifications sent to teachers, from work being submitted by students to new messages from parents. These notifications are almost always delivered via email, giving hackers a prime opportunity to mimic the emails sent by these platforms to trick teachers and school administrators into clicking on fraudulent links by mistake.

Spoofing

Digital transformation is synonymous with using new and unfamiliar platforms, which means users are often ill-equipped to recognize the subtle signs of spoofing. Something as simple as stolen login information can quickly bring an entire school network to its knees.

Ransomware

Schools are becoming increasingly reliant on software for their operations. Though this offers numerous benefits to students and teachers, it also positions educational institutions as tempting targets for cyber criminals, especially for ransomware attacks. According to Intel, 44% of schools have experienced a ransomware attack, making it the most common type of cyber attack vector in education.

All these attacks can have damaging impacts on a school's teaching effectiveness and cause lasting effects on student privacy in the event of a data breach. Thankfully, these cyber threats all have easily recognizable signs once teachers and administrators are properly trained to detect them.

Cyber security awareness training is often the only way to counter attacks like phishing by providing the required knowledge to your user base to detect that an attack is underway.

CYBER SECURITY ASSURANCE

Cyber assurance is all about the data, and protecting that data from risk (the possibility of something bad happening), wherever it is.

Types of risks to data:

Natural disasters- tornado takes out a company building that has file servers within it. Structural failures- plumbing failure in a data center that damages servers.

Human errors- clicking on a phishy email, accidental deletion of key files, email sent out to the wrong audience.

Intentional acts of malfeasance- ransomware, data leakage, hacking (e.g. DoS, MiTM, XSS), insider threat

some potential consequences if risks are not properly mitigated:

Inability to operate- DDOS, Ransomware, integrity of data compromised

Regulatory fines- local and federal data breach laws, FTC, etc.

Loss of public trust

Loss of intellectual property, competitive advantage

Cyber assurance is all about the saying "an ounce of prevention is worth a pound of cure."

Reduce Risk by Implementing a Security Plan

Identify- categorize the data and the systems value to the organization. Inventory- Make a list of what you have (network equipment, servers, clients, etc.) and learn how everything works.

Protect- put in place measures to protect the data and the system from harm Create a risk management strategy based on your risk tolerance, your resources, and the value of the data. Leverage principles of Defense in Depth- implement redundant layers of defenses throughout the system, to provide assurance that the data is protected in the event something goes wrong. Implement a framework (ISO/IEC 27001, NIST SP 800-53, or your own custom) & capture the way you are meeting security controls Federal systems are required to utilize the NIST framework Planned system changes should be reviewed to determine their security impact Continually assess and monitor to ensure that controls remain effective at reducing risk Increase awareness of cyber security best practices within your organization via regular training and awareness campaigns.

Detect- identify efforts to thwart the purpose of the system or compromise the data.

Respond- implement defenses to mitigate damage to the system or data.

Recover- restore the system and the data so that normal operations can continue. Contingency and disaster recovery plans.

CASE STUDIES

Business disruption at chocolate manufacturer due to global cyber attack

In June 2017, the world's second largest confectionery company was affected by the global ransomware attack called NotPetya which was an untargeted campaign without a specific intended victim. Many of the impacted companies were infected after downloading a routine update for an accounting application tainted by the attackers.

Employees experienced operational difficulties to the extent that the attack caused a 5% drop in sales that quarter.

The company reported overall related costs as being $180 million, with $84 million spent cleaning up the attack, investigating its causes, removing the malware and restoring their systems and operations.

In early 2019, the company filed a legal case against its cyber insurer regarding its claim for damages incurred from the NotPetya attack which was believed would have far-reaching implications for the cyber insurance industry specifically as to the viability of war exclusion clauses.

In November 2022, it was reported that the company and their insurers had reached a settlement but details of the settlement were not disclosed publicly.

Payments giant investigating breach at gas stations

In January 2017, the card payments company experienced a breach of their internal systems limited to controllers and attempted attacks on some affiliated point-of-sale (POS) systems at approximately 24 gas stations.

As reported by security researcher, Brian Krebs, an internal memo from the company to all staff and contractors in January 2017 stated that as a result of "an IT control matter" all employees needed to change their passwords within 24 hours and that end users would no longer be able to "load any additional software" onto their company computers without explicit authorisation. Suggesting that an end user may have inadvertently installed software on their company computer which led to the breach.

The company believed the duration of the attack was short and had not seen evidence of the data having been misused.

GOVERNMENT INITIATIONS TO PREVENT CYBER-CRIMES.

1. The Indian Computer Emergency Response Team (CERT-In)

- The advancement in the Indian Computer Emergency Response Team (CERT-In), which operates as the national agency to address the country's cyber security, has helped reduce the rate of cyber attacks on government networks

2. Cyber Surakshit Bharat

- Aiming to strengthen the cyber security ecosystem in India and following the Government's vision of a "digital India," the Ministry of Electronics and Information Technology (MeitY) has launched the Cyber Surakshit Bharat initiative
- The program was in partnership with the National Electronic Governance Division (NeGD)

3. National Critical Information Infrastructure Protection Center (NCIIPC)

- NCIIPC is a central government establishment, formed to protect critical information about our country, which has an enormous impact on national security, economic growth, and public health care

NCIIPC has mainly identified the following as "critical sectors"-

- Power & Energy
- Banking, Financial Services & Insurance
- Telecom Transport
- Government
- Strategic & Public Enterprises

4. Appointment of Chief Information Security Officers

- The Indian Government has published a written guideline for CISOs of government organizations, outlining best practices for safeguarding apps, infrastructure, and compliance
- Chief Information Security Officers (CISOs) can identify and document the security requirements that may arise with each technical innovation

5. Personal Data Protection Bill

- The most important one for Indian citizens is the approval of the Personal Data Protection Bill by the Union Government to protect Indian users from global breaches, which focuses on data localization
- The bill involves the storage and processing of any critical information related to people only in India

- It strictly states that individuals' sensitive personal data is to be stored locally; however, it can be processed abroad under certain conditions
- The bill also aims to make social media companies more accountable and push them to solve the spread of offensive content.

6. Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Center)

- The "Digital Swachhta Kendra" (Botnet Cleaning and Malware Analysis Center) is a part of the Government of India's Digital India drive, overseen by the Ministry of Electronics and Information Technology (MeitY), determined to make secure cyberspace all through India by distinguishing botnet contaminations and advising, empowering cleaning, and end-client security systems to forestall new diseases
- The "Cyber Swachhta Kendra" (Botnet Cleaning and Malware Analysis Center) is intended to address the goals of the "National Cyber security Policy," which calls for the development of a secure cybernetic ecosystem in the country
- The centre works in close coordination and collaboration with Internet service providers and antivirus/product companies
- The website provides users with information and tools to help them protect their systems/devices. Following Section 70B of the Information Technology Act 2000, this centre is run by the Indian Computer Emergency Response Team (CERT-In)

7. National Cyber Security Policy, 2013

- The Policy's goal is to create safe and resilient cyberspace for citizens, businesses, and the Government
- The mission is to provide protection to cyberspace information and infrastructure, develop capabilities to prevent and respond to cyber attacks, and minimize damage through coordinated efforts of institutional structures, people, processes, and technology
- To create a workforce of 500,000 trained cyber security professionals in the next 5 years through capacity building, skills development and training
- Through appropriate legislative intervention, enable effective cybercrime prevention, investigation, and prosecution, as well as the enhancement of law enforcement capabilities.

UNIT V

ONLINE BANKING SECURITY

Online banking is a facility offered by banks and other financial institutions that allows users and customers to make their transactions and banking services easy. Most of the banks are available online and offline. With the emergence of digitalization, users can now virtually and instantly access their bank accounts, transfer money, check their balance, and provide standing orders to banks from anywhere they choose.

With increased reliance on digital technologies, bank thefts, and cybercrimes have received much attention lately as thieves take advantage of the many opportunities the digital world presents. Banking fraud has become a particularly dangerous menace in the world of cybercrimes, with the potential to cause significant financial losses. Unfortunately, this concerning tendency is anticipated to continue for some time to come.

It is highly advised that every individual who uses online banking facilities should protect their online banking system mechanism by incorporating specific precautionary steps to protect their online banking system.

Online Banking Security – Security Measures for Online Banking

1. Trust on reliable sources

Make sure whenever you are buying or making any payment either with direct website or through third party ensure the legitimacy, authenticity and reliability of the website, its address, content and contact so as to save yourself from any mishaps that might leave you in danger.

2. Implement the Use of Multi-Factor Authentication.

By requiring users to present various forms of identity before giving access to their accounts, multi-factor authentication (MFA) or, say two, two-factor authentication improves the security of online banking.

In addition to a password, this provides an additional layer of security. The banking institution asks for another piece of information, or factor, to authenticate your identity when you log in, rather than simply your login and password. It can be your fingerprint or a unique passcode texted to your smartphone the idea is that it’s an additional layer harder to steal than a password.

The basic idea behind multi-factor authentication is that even if there comes a chance when any malicious person tries to obtain your one factor, which is your password, they would still be unsuccessful in gaining access to your account. Therefore, deploying multi-factor authentication significantly decreases the possibility of unwanted access.

3. Make use of Complex Passwords.

Use hard-to-guess combinations, like a blend of capital and lowercase letters, digits, and symbols. For example, passwords for government websites often need to be at least 12 or 16 characters long. However, your password will be more challenging to crack and more likely to keep hackers out if it is longer and more complicated. Use a password manager, which can be a valuable tool for creating and keeping secure passwords that are difficult to guess.

4. Switch on Text Alerts.

Text notifications, called SMS alerts, are essential for improving online banking security and protecting our bank accounts while safeguarding our information. By instantly alerting users to specific actions or modifications made to their accounts, these notifications ultimately add another degree of security.

In text alerts, users are notified immediately in the event of an unauthorized transaction, giving them ample time to secure their account. Users can set up text notifications to notify them of any login attempts or modifications to their account settings. This enables users to spot suspicious activity, including unauthorized access, and take appropriate action fast. Adding text alerts to an extensive multi-factor authentication and monitoring system strengthens online banking security by enabling customers to identify and address potential threats quickly.

5. Prevent the use of Public WIFI and switch off PC when not in use

Public Wi–FI is widely available, but it comes with its own risk, as many people who rely on public Wi-Fi networks are bound to get connected. With this connection, there are high chances of your data and private contents getting leaked, setting a high probability of getting hacked. Malware could inadvertently enter your device using an unauthorized hotspot. If you want to protect your online banking account, you must be mindful to check that the website's URL starts with "https," which is a security feature, or think about setting up as a virtual private network (VPN) on your laptop or mobile device.

Ensure to turn off your PC when not in use as continuous running of PC even at time when not in use may present you with a situation where hackers are offered with the chance to play with your confidential or sensitive information.

6. Protect your online Banking Against Phishing Scams.

Using security safeguards offered by online services, being aware of potential threats, and exercising caution are all essential components of protecting oneself from phishing schemes like Voice Phishing, Smishing etc. Verify the sender's email address if you receive any mail from a strange email address. Use browser tools such as safe Browsing, which can assist in recognizing and blocking phishing websites.

7. Install Antivirus

Provide an additional layer of protection to your online banking by installing antivirus software to safeguard your online banking activities. There are many authentic and accountable antivirus software available that tend to detect malicious software that, including keyloggers, trojans, and other types of malware, may catch up with your login credentials and other sensitive information during online banking sessions.

8. Choose an Industry that Prioritizes to Provide Security for your Online Banking

Protect the privacy of your sensitive financial information by following standard security procedures. During online transactions, encryption and secure transmission protocols are frequently used to guard your information from interception or unauthorized access. Choose a reliable and accountable industry that provides security standards to find gaps and vulnerabilities in your online banking security measures and works to counter new threats.

Similarly when you make any purchase with any of the E- commerce website or through online transaction acquire the payment details along with product code description, account holder name etc to make sure that the online purchase which you have made is from an reliable and trusted source and if you find any discrepancy over it you can approach your bank for resolving it.

9. Prefer to Activate the Sign-up Alert for your Bank Account.

Activating sign-up alerts for your bank account can be an effective and valuable step of security, which you must consider to protect and provide security to your online banking activity. Getting notified for each alert will keep you vigilant if any suspicious or unusual transactions occur. Similarly, you may get notified if there is a change in your account password or changes in your personal information. Be proactive in monitoring your account through alerts and measures that help eliminate financial loss and risk simultaneously.

10. Install various payment alternatives

By adding extra security layers and lowering the risk involved with using standard payment methods, integrating payment alternatives can improve the security of online banking services. Payment alternatives protect data passed between the user’s device and the banking server using secure communication protocols like EV SSL certificate. By lowering the possibility of malevolent activities that might intercept critical information while it is in transit, as the encryption helps safeguard it.

MOBILE BANKING SECURITY

Mobile banking is the process of using a mobile banking application to access your bank account and perform tasks that relate to the management of your finances.

Most mobile banking applications are developed, released, and maintained by financial institutions, or they are outsourced to mobile application development companies. These apps allow customers to perform a wide range of tasks from the comfort of their mobile device, such as checking their current balance, transferring funds from one account to another, paying an individual or service provider, and canceling a lost or stolen debit or credit card, to name a few.

Mobile online banking also allows for the use of third-party payment service providers such as PayPal and the use of ‘Buy Now, Pay Later’ services such as Pay It Later, Fupay, and Afterpay. As the popularity of mobile banking applications has risen, so too has the need for robust, scalable, and reliable mobile banking app security solutions.

These security measures are designed to help protect users’ sensitive personal and financial data as well as their accounts. And they come in various types to help remedy different types of cybersecurity vulnerabilities, from the Google Play Store and Apple Store cracking down on imitation mobile banking applications to replacing the delivery of One-Time Passwords (OTPs) from SMS to Push notifications in order to combat SMS-hijacking.

So, without further ado, here are the latest mobile banking app security solutions to consider for your next application.

Secret Pins

Most mobile banking applications these days give their users the ability to log into their apps via a four or 5-digit pin. These pins are easier to remember than a conventional password, as they are shorter in length and composed of only numbers. And since secret pins are less commonly used than conventional passwords, there is less chance of a customer re-using the same 4-5 digit pin combination across multiple cards or programs to access your application.

Of course, just like any type of password or pin, it is the customer's responsibility not to set secret pins that are easy to guess. This means not using secret pins that may relate to something about you, such as your date of birth or current home address, and not using secret pins that may follow a predictable number pattern, such as 1234.

Biometrics

Fingerprint scanning and facial scanning recognition technology have become common features on most modern smartphones.

Biometrics enables customers to access a mobile banking application with the touch of a finger or a simple face scan. This is usually quicker to perform than typing in a password or pin, and the customer doesn't have to remember their credentials either.

What's more, biometrics can be a more secure means of access than traditional methods, as the customer cannot accidentally share their credentials with (or have their credentials stolen from) a malicious actor pretending to represent an official banking service.

Multi-Factor Authentication (MFA)

The purpose of MFA is to have users provide more than one form of identity verification. This usually means providing a username and password as well as another form of identification, such as typing in an answer to a secret question that was previously set up or typing in a randomly generated One-Time Password (OTP) sent to the user's smartphone via SMS.

However, while MFA is an effective way to prevent unauthorized access, there is one downside. The rise of SIM-swapping – where a malicious actor tricks a victim into transferring their phone number to a new SIM card, thus enabling the malicious actor to receive the victim's SMS messages – means that banks are slowly moving away from SMS delivery, and instead to in-app Push notifications.

Device Binding

Device binding is the act of binding one or more of a customer's mobile devices to their relevant financial institution. Doing so gives the bank a clear idea as to which devices the customer currently has access to and the devices they use to access their banking services.

Using this information, the bank can monitor for suspicious activity by notifying the customer when a login attempt is made on a device that is not on their list of registered devices. From there, the customer can either add the new device to their list of registered devices or, if the login attempt is from an unknown device, take the necessary steps to protect their account, such as changing their passwords or temporarily limiting access to their account.

When a user binds a physical device to their banking service, this will produce a key on their device, which is stored with the customer's identity record in the bank. When the user performs a sensitive action, such as logging in or trying to make financial transactions, the application will verify the act is being performed on the same device that produced that key.

SECURITY OF DEBIT AND CREDIT CARD

1. EMV chip technology

EMV technology stands for Europay, MasterCard, and Visa. It is a significant leap forward in terms of credit card security. credit cards also use this technology. EMV enhances security by providing you protection against fraudulent and unauthorized transactions. The EMV chip is a small yet powerful microprocessor integrated into credit cards.

Unlike its predecessor, the magnetic stripe card, which stores static and unchanging data, the EMV chip generates a dynamic and unique code for each transaction. This unique code is the linchpin of EMV's security prowess. It acts as a safeguard against one of the most pervasive threats in finance: card counterfeiting. With traditional magnetic stripe cards, it was easy for cybercriminals to copy card data and manufacture counterfeit cards, posing a significant risk to cardholders and financial institutions. However, the EMV chip's unique code changes with every transaction, making cloned cards useless to fraudsters.

The EMV chip adds a layer of complexity. Even if someone manages to intercept the code from one transaction, it would be worthless for any subsequent unauthorised use. This advanced technology not only protects consumers but also provides a boost to the overall security of the payment ecosystem.

2. Contactless payment

Contactless payments have experienced a surge in popularity. They give you a seamless experience along with robust security measures. credit cards also allow contactless payments. This payment method enables a secure connection between your card and the payment terminal via near-field communication (NFC) technology. Encryption protocols ensure the confidentiality of payment details. Since physical card usage is decreased, it also reduces the risk of card theft, providing you with added security. With contactless payments, you can enjoy efficiency and security.

3. PIN (Personal Identification Number)

A Personal Identification Number (PIN) is a vital security feature that enhances the safety of your financial transactions. You are required to choose the PIN for your card which is confidential and exclusive to you. It acts as your digital fingerprint that validates your identity before transactions. Since a PIN cannot be copied easily, it protects your credit card from fraudulent purchases or access to funds. If your card is lost or stolen, the PIN protects it from unauthorised purchases.

4. CVV (Card Verification Value)

The CVV is a three-digit code located at the back of credit cards. It is used primarily for online and phone transactions for verification purposes. You need to have the physical card with you for transactions as the CVV is printed on the card. This way, your card is secure from unauthorised use.

5. Two-factor authentication (2FA)

Bank credit cards offer two-factor authentication (2FA) for online transactions. This involves an additional verification step after logging in. As soon as you log in with your user ID and password, you will get a one-time PIN (OTP) on your registered mobile or email. You need to enter this code to finalise the sign-in or transaction. This way the 2FA ensures that the transaction is being done by the accountholder.

6. Transaction alerts

As an Bank credit card user, you will receive real-time alerts via text message and email for every transaction on your credit card. These alerts enable you to track and report any unauthorised or suspicious activities, preventing further fraudulent transactions.

7. Transaction preferences

All the Bank credit cards provide you with the control to manage your transaction preferences. You can choose how you want to use your card. You can enable or disable preferences such as domestic transactions and international transactions. For example, if you do not want to use your credit card for international online transactions, you can disable this simply via SMS . This feature gives you complete control over how your credit card is used, making transactions more secure. You can also block/unblock your credit card to protect it from unauthorised use.

8. Transaction limits

Bank allows you to fix and modify transaction limits on your credit card, through its app/online portal. You can set limits for online transactions, point-of-sale purchases, contactless transactions, and ATM withdrawals. Setting transaction limits prevents fraudulent transactions, as the transactions get rejected once they exceed the limit set by you.

9. Virtual Card

Virtual cards are temporary credit cards similar to physical credit cards. They come with a temporary 16-digit number, expiry date and CVV number. What differentiates these cards from physical credit cards is that they can only be used for online transactions.

Virtual cards are safe because:

1. These cards are temporary and become invalid automatically after a certain number of transactions.
2. A few of these cards are single-use virtual credit cards that become invalid in case of a data breach.
3. You can cancel a virtual credit card easily which prevents fraudulent use of the card.

Bank has introduced the ‘Virtual Commercial Card’ in collaboration with Visa and Juspay. This credit card has been designed to transform cross-border transactions for corporations and travel agents. It offers enhanced security features, allowing you to set unique parameters for each transaction and gives you complete control over international expenses. Each virtual card has customised transaction limits and expiry dates. The Virtual Commercial Card allows you to generate virtual cards in foreign currencies, thereby protecting your primary card number and ensuring maximum security.

10. Total Protect

Bank offers insurance coverage in cases of unauthorised transactions due to card loss or theft. The bank provides protection starting 48 hours before reporting the loss to the bank. Also, the bank offers insurance against counterfeit fraud, safeguarding customers from misuse of their card or card details.

Total Protect covers you for an amount equivalent to the limit on your credit card. This protection is valid for your add-on cards too.

UPI – UNIFIED PAYMENTS INTERFACE

A Unified Payments Interface (UPI) is a smartphone application that allows users to transfer money between bank accounts. It is a single-window mobile payment system developed by the National Payments Corporation of India (NPCI). It eliminates the need to enter bank details or other sensitive information each time a customer initiates a transaction.1

- The Unified Payments Interface (UPI) is a smartphone application for banking in India.
- The interface is regulated by the Reserve Bank of India (RBI), India's central bank.
- This app eliminates the need to enter bank details or other sensitive information each time a customer initiates a transaction, making it a safe way to bank.

How Unified Payments Interface (UPI) Works

The Unified Payments Interface is a real-time payment system. It is designed to enable peer-to-peer inter-bank transfers through a single two-click factor authentication process. The interface is regulated by the Reserve Bank of India (RBI), India's central bank. It works by transferring money between two bank accounts along with a mobile platform.

The system is said to be a safe and secure method of transferring money between two parties and eliminates the need to transact with physical cash or through a bank. The pilot system was launched in India on April 11, 2016. Banks across the country started to upload their interface in Aug. 2016.1

UPI uses existing systems, such as Immediate Payment Service (IMPS) and Aadhaar Enabled Payment System (AEPS), to ensure seamless settlement across accounts. It facilitates push (pay) and pull (receive) transactions and even works for over-the-counter or barcode payments, as well as for multiple recurring payments such as utility bills, school fees, and other subscriptions.

Once a single identifier is established, the system allows mobile payments to be delivered without the use of credit or debit cards, net banking, or any need to enter account details. This would not just ensure greater safety of sensitive information, but connect people who have bank accounts via smartphones to carry out hassle-free transactions.

Overall, UPI implies fewer cash transactions and potentially reduces the unbanked population.

MICRO ATM & SECURITY OF MICRO ATMs

A Micro ATM is defined as a mini version of an ATM. It is similar to modified Point-of-Sale (POS) machines. The ATM's mini version connects the banking network through GPRS to perform bank transactions. This machine provides the facility to swipe a card smoothly. The initiative of Micro ATM aims to reduce the difference between the availability and need for cash. It is run by an agent along with a card reader.

With the Micro ATM, the unbanked rural people can smoothly access micro banking services. It is broadly used in Aadhaar enabled payment systems.

The Micro ATM supports the following types of inter-operable transactions:

- Withdrawal
- Bank account mini-statement
- Fund transfer
- Deposit, and
- Balance enquiry
    - Be sure there are no strange objects in the ATMs' insertion panel to avoid skimming.
    - Cover the PIN pad when you are putting the PIN.
    - Change your ATM PIN regularly
    - Tear the receipt of the transaction securely after reviewing.
    - Keep checking your bank statements. If any unauthorized charges or withdrawal occurs, do inform the bank promptly.
    - Provide advance notice to debit/credit card issuers for address change.
    - Tear anything into pieces where you have written a credit card number.
    - Do not accept the card if the bank has delivered it with a seal open or damaged one.
    - Do not use a debit/credit card to write a PIN.
    - Do not reveal your ATM PIN/ Credit card number to any unknown person.
    - Don't be fooled by a stranger who tries to assist you in using the Micro ATM.
    - Don't give the card to any person even if he/she says they are a bank agent.
    - Do not share or transfer your account information with an unknown source.
    - Contact the bank or service provider if there is a suspected transaction or card is lost.

Best actions for service providers to secure Micro ATMs

- The service provider must keep the Micro ATMs' software and anti-virus up to date.
- Inform the user about its security best practices and basic functions.
- If there is no activity in the machine, the service provider must lock it.

E-WALLET & E-WALLET SECURITY GUIDELINES

An Electronic-wallet (e-wallet) is an electronic application that enables online e-commerce transactions like purchasing goods, paying utility bills, transferring money, booking flight etc. with a financial instrument (such as a credit card or a digital currency) using smart phones or computers. A plethora of these e-wallets are provided online for downloading through "apps" to support both Point of Sale (PoS) transactions and peer-to-peer transactions between individuals. Being preloaded with currency by the user, they are designed to be convenient to them over the traditional-wallets, by providing better manageability over their payments, accounts, receiving of offers, alerts from merchants, storing digital receipts and warranty information and being secure by requiring to access only through correct passphrase, password and such authentication information.

A number of IT companies, Banks, Telecoms firms, online e-commerce portal, taxi-services, supermarket chains etc. provide e-wallets. A number of Personally Identifiable Information (PII's) of the customer like his/her name, mobile phone number and his/her protected personal information like Customer card numbers, secret PIN, net banking credentials etc is permanently stored in e-wallets, requiring just final authorization from the user through means like biometrics authentication, one-time passwords(OTP) etc. The payment process involves security mechanisms like certificate pinning and use of encryption.

Best practices to secure e-wallet

- **Enable Passwords On Devices:** Strong passwords should be enabled on the user's phones, tablets, and other devices before e-wallets can be used. Additional layers of security provided by these devices should be used.
- **Use Secure Network Connections**: It's important to be connected only to the trusted networks. Avoid the use of public Wi-Fi networks. More secure and trusted WiFi connections identified as "WPA or WPA2" requiring strong passwords should be used.
- **Install Apps From Trusted Sources:** Reading the user ratings and reviews can provide some clues about the integrity of the e-wallet app. The user must check for the e-wallet provider to be showing strong legacy of securely, reliably and conveniently handling sensitive financial data and providing customer support (in the event of card loss or account fraud).
- **Keep Login Credential Secure:** Avoid writing down information used to access the digital wallets in plain view or storing them in an unprotected file to avoid their misuse.
- **Create a Unique Password for Digital Wallet:** Use hard-to-guess password unique to the digital wallet to prevent against the risk of unauthorized access.
- **Stay vigilant and aware of cellphone's network connectivity status and register for Alerts through SMS and emails:** The user should not switch off his cellphone in the event when numerous annoying calls are received, rather answering the calls should be avoided. This could be a ploy to get him to turn off his phone or put it on silent to prevent him from noticing that his connectivity has been tampered with. The customer should realize that when he is not receiving any calls or SMS notifications for a long time against his e-wallet uses, he should make enquiries with his mobile operator to be sure about not falling victim to such scam.
- **Identify Points of Contact in case of Fraudulent Issues:** For any fraudulent activity occurring on the user's account in the scenarios like when phone is lost or stolen, an individual card stored in the wallet is lost or account has been hacked, appropriate points of contact for resolving the issues should be understood by the user. The user must completely understand the e-wallet providers contract terms and conditions.

POS SECURITY & SECURITY GUIDELINES FOR POINT OF SALES(POS)

Point-of-sale security (POS security) creates safe environments for customers to make purchases and complete transactions. POS security measures are crucial to prevent unauthorized users from accessing electronic payment systems and reduce the risk of credit card information theft or fraud.

POS hacks represent a major opportunity for cyber criminals. POS applications contain a huge amount of customer data, including credit card information and personally identifiable information (PII) that could be used to steal money or commit wider identity fraud.

By hacking one application, malicious actors can potentially gain access to millions of credit or debit card details that they can either use fraudulently or sell to other hackers or third parties. Hackers can also exploit retailers' compromised POS applications, which can give them access to vast amounts of customer data, as well as additional applications and systems the retailer operates.

Organizations must use point-of-sale systems security to protect their applications, prevent unauthorized access, defend against mobile malware, and prevent hackers from attacking their back-end systems.

Security Guidelines

There are several measures that organizations can adopt and deploy to defend themselves against POS attacks and data breaches, prevent POS malware infection, and improve their POS security. Such measures include whitelisting applications, limiting POS application risks, ensuring POS software is always up to date, monitoring activity in POS systems, using complex and secure passwords, deploying two-factor authentication (2FA), using antivirus software, and considering physical security measures.

Here are six point-of-sale best practices for improving POS security:

Use iPads for POS

Many high-profile POS attacks have occurred as a result of malware being loaded into a POS system's memory. This enables the hacker to upload malware applications and steal data without being spotted by users or retailers. But, crucially, this attack method requires a second application to be running.

As a result, Apple's iOS systems can help prevent POS attacks because the operating system (OS) can only fully run one application at any time, whereas Windows devices rely on multiple applications at the same time. Organizations can, therefore, use iPad POS solutions to run their POS systems and reduce the chances of POS attacks.

Use End-to-End Encryption

One way for customer data to never become exposed to hackers is through encryption. Encrypting credit card and other sensitive data as soon as the POS device receives the data and when it gets sent to the POS software server will ensure it is never vulnerable, regardless of where and how hackers install malware.

Secure Your POS with an Anti-Virus

Antivirus software allows organizations to secure their systems and prevent POS attacks. It prevents malware from infiltrating organizations' systems by scanning devices to detect anomalous or problematic applications, files, and user activity that need to be blocked or removed.

An antivirus alerts organizations when there is a potential issue and enables them to initiate the cleansing process to guarantee any present malware does not result in the loss or theft of data.

Lock Down Your Systems

The chances of employees using their organizations' POS devices to initiate an attack are relatively low, but there is a potential for malicious insider activity or human error. Users could steal, lose, or accidentally misplace devices that have POS software installed, which could allow anyone that picks up the device to view or steal customer data.

Organizations need to lock down their systems to avoid these risks. This involves ensuring employees lock down their devices at the end of every working day, diligently keeping track of every corporate device throughout each day, and securing devices in locations that only a few trusted individuals have access to.

Avoid Connecting to External Networks

Sophisticated hackers can compromise POS systems remotely. This is typically possible through systems that can connect to external networks, which hackers will look to infiltrate through software that remains dormant until it connects to a POS system.

Organizations, therefore, need to avoid connecting to external networks and ensure their systems remain local, internal, and secure. They should look to restrict the handling of business-critical tasks, such as transactions and payment processing, to secure corporate networks.

Be PCI-compliant

Putting measures in place to manage and protect POS systems is crucial, but organizations also need to comply with the stipulations of data privacy and protection regulations. This includes the Payment Card Industry Data Security Standard (PCI DSS), which regulates security standards for any organization that handles credit cards from major providers. Organizations must comply on all transactions carried out on card readers, online shopping carts, networks, routers, servers, and paper files.

PCI DSS is mandated by financial organizations and administered by the PCI Security Standards Council, which is responsible for increasing cardholder data controls to reduce credit card fraud. The Council suggests that organizations eliminate cardholder data where possible, as well as maintain communication with major financial organizations and credit card providers to reduce fraud or theft issues.