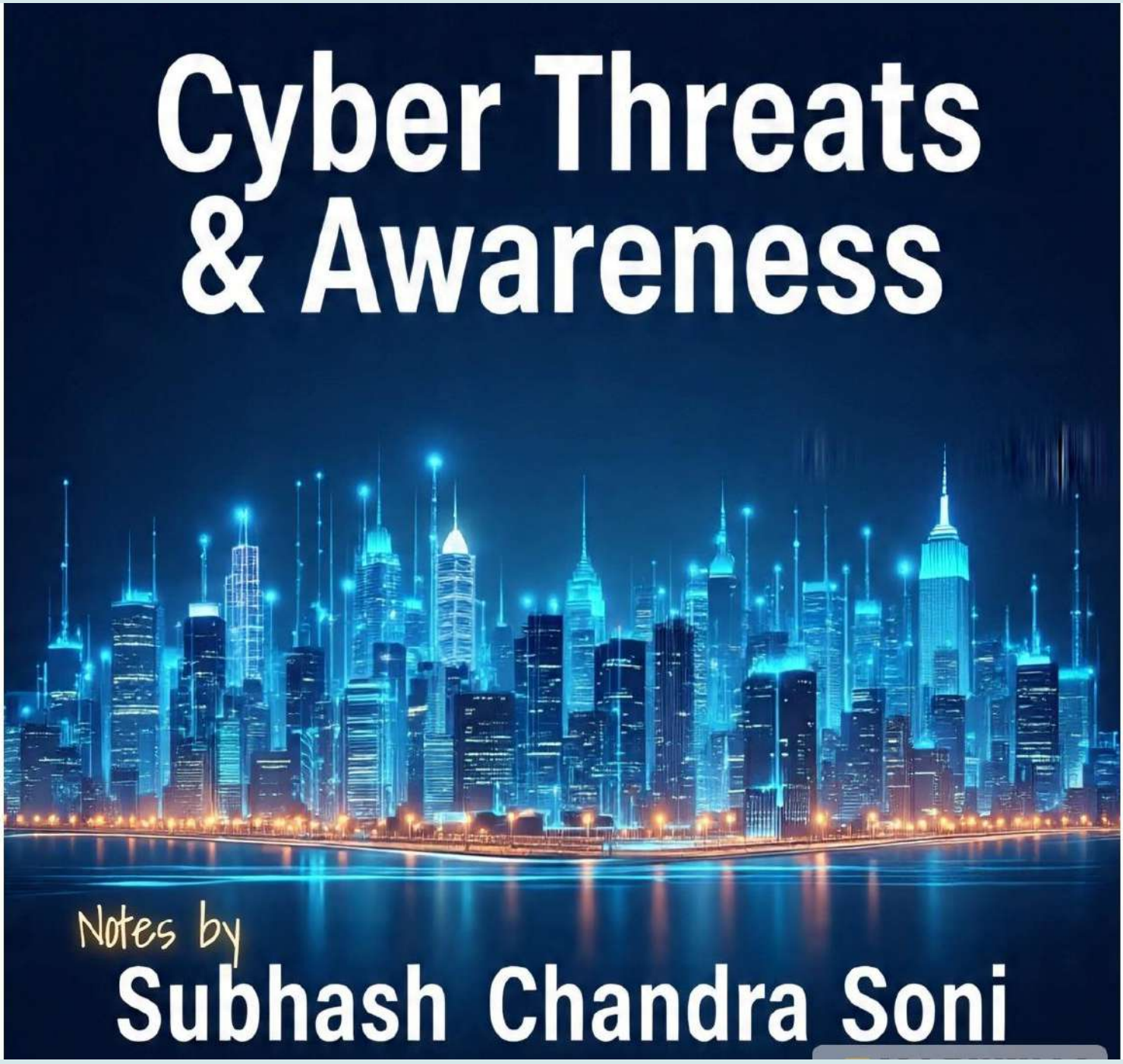


Programmer

Govt. Polytechnic Bhatapara (C.G.)

Chhattisgarh Swami Vivekanand Technical University, Bhilai (CG)

Diploma Engineering Common to all Branches (NEP)

SEMESTER-I

Introduction to Cyber Security and Threats

Cyber Security

Cybersecurity is the practice of protecting computer systems, networks, and sensitive information from unauthorized access, use, disclosure, disruption, modification, or destruction. This includes protection against malware, viruses, Trojan horses, spyware, adware, ransomware, and other types of cyber threats.

What Cybersecurity Does

- **Protects systems and networks**:
  It secures the infrastructure that enables digital operations from external threats.
- **Safeguards data**:
  It ensures the confidentiality, integrity, and availability of digital information, whether it's in storage or being transmitted.
- **Defends against various attacks**:
  Cybersecurity professionals work to prevent and respond to threats like ransomware, malware, phishing, data breaches, and other malicious activities.

Why Cybersecurity Is Important

- **Personal protection**:
  It helps individuals keep their data private and have a safe online experience by protecting their devices and online accounts.
- **Organizational resilience**:
  Businesses rely on digital technology to function, and strong cybersecurity helps prevent financial losses, service disruptions, regulatory fines, and reputational damage that can result from cyber attacks.
- **National infrastructure**:
  Cybersecurity is vital for the smooth operation of critical national infrastructure, such as power grids, hospitals, and government services, in our connected society.

Key Aspects of Cybersecurity

- **Technology**:
  This includes security tools like firewalls, malware protection, and antivirus software to detect and prevent threats.
- **Processes**:
  These are the structured methods used to manage and secure digital assets, such as disaster recovery plans and operational protocols.
- **People**:
  Individuals play a crucial role by following security best practices, such as using strong passwords and being vigilant about suspicious emails, to prevent human error from creating vulnerabilities.

Basics of Cyber security

Some of the basic principles of cyber security include:

1. Confidentiality: Ensuring that sensitive information is only accessible to authorized individuals.
2. Integrity: Ensuring that data is not modified or deleted without authorization.
3. Availability: Ensuring that systems and data are available when needed.
4. Authenticity: Verifying the identity of users and systems.
5. Monitoring and Response: Detecting and responding to cyber threats in a timely manner.

Basic Cyber security Principles

Some basic cybersecurity principles include:

1. Password Security: Using strong passwords and changing them regularly.
2. Firewall and Antivirus: Using firewalls and antivirus software to protect systems.
3. Regular Updates: Keeping software and operating systems up-to-date with the latest security patches.
4. Backup: Regularly backing up important data.

5. User Education: Educating users about cybersecurity best practices and promoting safe online behavior.

Relevance of Cyber security in Everyday Life

In today's digital age, cyber security is crucial in everyday life. Here are some reasons why:

1. Personal Data Protection: Cyber security helps protect personal data, such as financial information, addresses, and medical records, from unauthorized access.
2. Online Transactions: Cyber security ensures secure online transactions, such as online banking, e-commerce, and digital payments.
3. Smart Devices: With the increasing use of smart devices, cyber security helps protect these devices from hacking and data breaches.
4. Social Media: Cyber security helps protect social media accounts from hacking and identity theft.
5. Remote Work: With the rise of remote work, cyber security ensures that remote access to company networks and data is secure.
6. Identity Theft Prevention: Cyber security helps prevent identity theft by protecting personal data and preventing unauthorized access.
7. Business Protection: Cyber security helps protect businesses from cyber threats, such as data breaches, ransom ware, and intellectual property theft.

Consequences of Poor Cybersecurity

Poor cyber security can lead to:

1. Financial Loss: Cyber attacks can result in significant financial losses.
2. Reputation Damage: Cyber attacks can damage an individual's or organization's reputation.
3. Data Loss: Cyber attacks can result in data loss, which can be irreparable.
4. Identity Theft: Cyber attacks can lead to identity theft, which can have serious consequences.

Best Practices

To ensure cyber security in everyday life:

1. Use Strong Passwords: Use unique and complex passwords for all accounts.
2. Keep Software Up-to-Date: Regularly update software and operating systems.
3. Use Antivirus Software: Install and regularly update antivirus software.
4. Be Cautious Online: Be cautious when clicking on links or downloading attachments.
5. Use Two-Factor Authentication: Use two-factor authentication whenever possible.

Cyber-attack (Threats)

A cyber-attack is a malicious attempt to steal, alter, disrupt, or destroy data or computer systems by gaining unauthorized access to them. Cyber threats are the potential harmful activities and actors behind these attacks, such as malware, phishing, ransom ware, and social engineering, which can cause significant financial and operational damage to individuals and organizations alike.

What is a Cyber-attack?

- It is a deliberate action targeting computer systems, networks, or digital devices.
- The goal is to compromise information resources, leading to data theft, alteration, destruction, or disruption of services.
- Attackers, known as threat actors, use various tactics to gain unauthorized access and achieve their objectives.

What are Cyber Threats?

- These are the harmful activities or tools used to execute cyber-attacks, such as malicious code, phishing emails, or social engineering tactics.
- They also refer to the individuals or groups (threat actors) with the intent and capability to launch these attacks.
- Examples include malware (like viruses and ransomware), phishing scams, denial-of-service (DDoS) attacks, and attacks stemming from insider threats.

Goals of Cyber-attacks:

- **Financial Gain:**

Stealing financial information, demanding ransom payments (ransomware), or using compromised data for fraud.

- **Information Theft:**
  Stealing intellectual property, customer data, or personal identifiable information (PII).
- **Disruption of Operations:**
  Shutting down critical infrastructure, damaging systems, or halting business operations.
- **Political/Ideological Motives:**
  Acts of cyber warfare or terrorism to cause widespread disruption or damage.

Who is behind cyber-attacks?

- **Criminal organizations**: These groups are motivated by financial gain through ransomware, data theft, and extortion.
- **Nation-state actors**: Governments or their proxies conduct attacks for political reasons, such as espionage or cyber warfare.
- **Hacktivists**: These attackers are motivated by ideological or political causes and seek to disrupt services or damage an organization's reputation.
- **Malicious insiders**: Disgruntled employees, contractors, or partners with authorized access can intentionally misuse their privileges to steal data or cause harm

Common Types of Cyber Threats:

Malware:
Malicious software, including viruses, worms, and ransomware, designed to infiltrate and damage systems or steal data.

Phishing:
Sending fraudulent communications (often email) that appear to be from a trusted source to steal sensitive information.

Social Engineering:
Manipulating people into revealing confidential information or performing actions that compromise security.

Denial-of-Service (DDoS) Attacks:
Overwhelming a network or system with traffic to make it unavailable to legitimate users.

Insider Threats:
Threats originating from within an organization by employees or other trusted individuals who have legitimate access to systems.

Malware:

Malware (Malicious Software) refers to any software designed to harm or exploit a computer system, network, or mobile device. Malware can:

1. Steal sensitive information (e.g., passwords, credit card numbers)
2. Disrupt system operations
3. Hijack system resources
4. Spread to other devices

Types of malware:

1. Viruses: Replicate and spread to other files/programs
2. Worms: Self-replicating malware that spreads without user interaction
3. Trojans: Disguise themselves as legitimate software
4. Ransomware: Encrypts files, demanding payment for decryption
5. Spyware: Monitors user activity, stealing sensitive info
6. Adware: Displays unwanted ads, potentially collecting user data
7. Rootkits: Hide malware or themselves from system detection

Protection tips:

1. Keep software/OS updated

2. Use antivirus software
3. Avoid suspicious downloads/links
4. Use strong passwords
5. Regularly back up data

Phishing:

Phishing is a type of cyber attack where attackers try to trick you into revealing sensitive information like passwords, credit card numbers, or personal data.

Phishing attacks often come via:

1. Emails: Fake emails that appear legitimate
2. Messages: Text messages or social media messages
3. Phone calls: Scammers posing as legitimate entities

To avoid phishing:

1. Be cautious with links and attachments: Don't click on suspicious links or open attachments from unknown sources.
2. Verify sender information: Check if the email or message is from a legitimate source.
3. Check website URLs: Ensure the website address is correct and secure (HTTPS).
4. Use strong passwords: Use unique and complex passwords.
5. Enable two-factor authentication: Add an extra layer of security.

If you're a victim of phishing:

1. Change passwords: Immediately update your passwords.
2. Notify the relevant institution: Inform your bank, social media platform, or other affected institutions.

Ransomware

Ransomware is a type of malware that encrypts your data and demands payment in exchange for the decryption key.

Symptoms of a ransomware attack:

1. Data encryption: Your files and data are encrypted, making them inaccessible.
2. Ransom demand: The attacker demands payment in exchange for the decryption key.
3. Threats: Attackers often threaten to delete or leak your data if the ransom isn't paid.

Protection tips:

1. Regular backups: Back up your data regularly to restore it in case of an attack.
2. Keep software updated: Update your operating system and software to patch vulnerabilities.
3. Use antivirus software: Install and regularly update antivirus software.
4. Avoid suspicious links and attachments: Be cautious when clicking on links or opening attachments.

If you're a victim:

1. Don't pay the ransom: Avoid paying the ransom; instead, restore your data from backups.
2. Isolate the system: Disconnect the infected system from the internet.
3. Seek professional help: Contact your IT department or a cybersecurity expert.

Hacking

Hacking refers to unauthorized access or manipulation of computer systems, networks, or data. Hackers may:

1. Steal sensitive information: Personal data, financial info, or confidential business data.
2. Disrupt systems: Crash systems, causing downtime and losses.
3. Malicious activities: Spread malware, conduct phishing, or ransomware attacks.

Types of hackers:

1. **Black hat hackers**: Malicious hackers seeking personal gain or causing harm.
2. **White hat hackers**: Ethical hackers helping organizations improve security.
3. **Gray hat hackers**: Hackers who may exploit vulnerabilities but don't necessarily cause harm.

Protection tips:

1. Strong passwords: Use unique, complex passwords.
2. Keep software updated: Patch vulnerabilities.
3. Use antivirus software: Detect and remove malware.
4. Be cautious online: Avoid suspicious links and downloads.

Cybercrime:

1. Criminal activities: Cybercrime refers to illegal activities conducted through computers, networks, or the internet.
2. Examples: Identity theft, online fraud, phishing, cyber stalking, and distribution of illegal content.
3. Motivations: Financial gain, personal revenge, or causing harm.

Cyberattack:

1. Deliberate disruption: A cyber attack is a deliberate attempt to disrupt, disable, or exploit a computer system or network.
2. Examples: Malware, ransom ware, SQL injection.
3. Motivations: Various, including financial gain, espionage, sabotage, or hacktivism.

Key differences:

1. Legality: Cybercrime is always illegal, while cyber attacks can be illegal or legitimate (e.g., penetration testing).
2. Scope: Cybercrime encompasses a broader range of activities, while cyber attacks focus on disrupting or exploiting systems.

Data Breach:

A data breach is an incident where sensitive, protected, or confidential data is accessed, stolen, or exposed without authorization. This can include personal identifiable information (PII), financial data, intellectual property, or other sensitive information.

Causes of Data Breaches:

1. Hacking: Cyber attackers exploit vulnerabilities to gain unauthorized access.
2. Insider Threats: Employees or authorized personnel intentionally or unintentionally compromise data.
3. Phishing: Social engineering tactics trick individuals into revealing sensitive information.
4. Physical Theft: Laptops, devices, or storage media containing sensitive data are stolen.
5. Human Error: Accidental exposure or improper handling of data.

Consequences of Data Breaches:

1. Financial Loss: Stolen data can be used for fraud, identity theft, or sold on the dark web.
2. Reputation Damage: Organizations face loss of trust and credibility.
3. Regulatory Penalties: Non-compliance with data protection laws can result in fines.
4. Identity Theft: Individuals may face financial and personal harm.

Prevention and Mitigation:

1. Implement robust security measures: Encryption, firewalls, and access controls.
2. Conduct regular audits and risk assessments: Identify vulnerabilities and address them.
3. Train employees: Educate on data handling best practices and security protocols.
4. Have an incident response plan: Quickly respond to and contain breaches.

Real-life examples of data breaches:

Major Breaches:

- Yahoo: 3 billion user accounts compromised in 2013, including names, email addresses, phone numbers, birth dates, passwords, and security questions.

- Marriott International: 500 million guest records stolen in 2018, including names, home addresses, email addresses, phone numbers, passport numbers, and dates of birth.
- First American Financial Corp: 885 million user records exposed in 2019, including bank account numbers, bank statements, Social Security numbers, tax records, and transaction receipts.
- National Public Data: 2.9 billion records exposed in 2024, including names, email addresses, phone numbers, Social Security numbers, and mailing addresses.

- Recent Breaches:
  - Kido International: 8,000 children's records stolen in 2025, including names, photos, home addresses, and family contact information.
  - Stellantis: basic contact information of North American customers exposed in 2025 due to a third-party provider breach.
  - Dell: 49 million customer records exposed in 2024, including names, addresses, and order information.
- Notable Breaches:
  - Equifax: 147.9 million consumer records compromised in 2017, including Social Security numbers, birth dates, and addresses.
  - Capital One: 100 million customer accounts and credit card applications breached in 2019, including names, physical addresses, credit scores, and other sensitive information.
  - LinkedIn: 700 million user records exposed in 2021, including full names, phone numbers, email addresses, and usernames

Major Data Breaches in India

- **ICMR COVID-19 Data Breach (2023):** A massive cybersecurity incident impacted the Indian Council of Medical Research, resulting in the theft of sensitive data belonging to approximately 815 million Indian citizens, including names, Aadhaar numbers, passport information, and COVID-19 test results.
- **Aadhaar Data Breach (2018**): A significant breach compromised the personal data of millions of citizens, highlighting weaknesses in data protection measures.
- **NACH Data Breach (2025):** A "configuration gap" at fintech firm Nupay exposed hundreds of thousands of NACH documents, containing sensitive information such as names, bank account numbers, and transaction amounts.

- Recent Breaches:
  - **Hathway Data Breach (2024):** A leading Indian Internet Service Provider experienced a major security breach, compromising the personal information of over 41.5 million customers.
  - **BSNL Data Breach (2024**): A telecommunications provider suffered a data breach, exposing sensitive data of millions of users, including IMSI numbers and SIM card details.
  - **boAt Data Breach (2024):** A prominent Indian consumer electronics brand experienced a cybersecurity incident, leading to the exposure of sensitive personal data for over 7.5 million customers.
- Other notable incidents:
  - **AIIMS Ransomware Attack**: A cyberattack on the All India Institute of Medical Sciences compromised 40 million patient records, highlighting weaknesses in healthcare cybersecurity.
  - **WazirX Data Breach**: A cryptocurrency exchange faced a significant data breach, resulting in the theft of over $230 million

These incidents emphasize the need for robust cybersecurity measures and strict data protection regulations in India. The Digital Personal Data Protection Act of 2023 aims to combat data breaches with strict laws and penalties, including fines of up to ₹250 crores for non-compliance.

Importance of Awareness and Alertness in Cyber Security

1. Prevention: Awareness helps prevent cyber attacks by identifying potential threats.
2. Early Detection: Alertness enables early detection of security incidents, minimizing damage.
3. Proactive Measures: Awareness and alertness prompt proactive measures to protect against emerging threats.

4. Reduced Risk: Informed individuals and organizations can reduce the risk of cyber attacks.
5. Improved Incident Response: Awareness and alertness facilitate swift and effective incident response.

Key Aspects

1. Stay Informed: Stay up-to-date with the latest cyber threats and trends.
2. Be Vigilant: Be cautious when interacting with emails, links, and attachments.
3. Use Strong Passwords: Use unique and complex passwords.
4. Keep Software Updated: Regularly update software and systems.
5. Report Incidents: Report suspicious activity and security incidents.

Benefits

1. Enhanced Security: Awareness and alertness enhance overall security posture.
2. Reduced Losses: Proactive measures reduce financial and reputational losses.
3. Improved Compliance: Awareness and alertness help meet regulatory requirements.

Some basic cyber safety tips

1. Use strong and unique passwords: Create complex and different passwords for each account.
2. Keep software up-to-date: Regularly update your operating system, browser, and other software to patch vulnerabilities.
3. Be cautious with emails and links: Be careful when opening emails and links from unknown sources, and avoid suspicious attachments.
4. Use antivirus software: Install and regularly update antivirus software to detect and remove malware.
5. Use a firewall: Enable the firewall on your computer and network to block unauthorized access.
6. Use two-factor authentication: Enable two-factor authentication (2FA) whenever possible to add an extra layer of security.
7. Back up your data: Regularly back up your important data to a secure location.
8. Use secure networks: Use secure and trusted networks, especially when accessing sensitive information.
9. Avoid public computers: Avoid using public computers or public Wi-Fi for sensitive activities.
10. Stay informed: Stay up-to-date with the latest cyber threats and trends.

साइबर सुरक्षा क्या है?

साइबर सुरक्षा एक प्रकार की सुरक्षा है जो कंप्यूटर सिस्टम, नेटवर्क, और डेटा को अनधिकृत पहुंच, उपयोग, या नुकसान से बचाने के लिए डिज़ाइन की गई है। इसका उद्देश्य है कि डिजिटल जानकारी और संसाधनों को सुरक्षित रखा जाए और साइबर हमलों से बचाव किया जाए।

साइबर सुरक्षा के मूल तत्व

1. गोपनीयता (Confidentiality): यह सुनिश्चित करना कि केवल अधिकृत व्यक्ति ही संवेदनशील जानकारी तक पहुंच सकते हैं।
2. अखंडता (Integrity): यह सुनिश्चित करना कि डेटा को अनधिकृत तरीके से बदला या हटाया नहीं जा सकता।
3. उपलब्धता (Availability): यह सुनिश्चित करना कि सिस्टम और डेटा हमेशा उपलब्ध हों जब उनकी आवश्यकता हो।
4. प्रामाणिकता (Authenticity): यह सुनिश्चित करना कि उपयोगकर्ता और सिस्टम की पहचान सत्यापित हो।
5. निगरानी और प्रतिक्रिया (Monitoring and Response): साइबर हमलों का पता लगाने और उन पर प्रतिक्रिया करने के लिए निगरानी और प्रतिक्रिया प्रणाली का होना।

साइबर सुरक्षा के बुनियादी सिद्धांत

1. पासवर्ड सुरक्षा: मजबूत पासवर्ड का उपयोग करना और उन्हें नियमित रूप से बदलना।
2. फायरवॉल और एंटीवायरस: फायरवॉल और एंटीवायरस सॉफ़्टवेयर का उपयोग करके सिस्टम को सुरक्षित करना।
3. नियमित अद्यतन: सॉफ़्टवेयर और ऑपरेटिंग सिस्टम को नियमित रूप से अद्यतन करना।
4. बैकअप: महत्वपूर्ण डेटा का नियमित बैकअप लेना।
5. उपयोगकर्ता शिक्षा: उपयोगकर्ताओं को साइबर सुरक्षा के बारे में शिक्षित करना और उन्हें सुरक्षित ऑनलाइन व्यवहार के लिए प्रोत्साहित करना।

बुनियादी साइबर सुरक्षा सुझाव:

1. मजबूत और अनोखे पासवर्ड का उपयोग करें: प्रत्येक खाते के लिए जटिल और अलग पासवर्ड बनाएं।
2. सॉफ़्टवेयर अद्यतन रखें: कमजोरियों को दूर करने के लिए अपने ऑपरेटिंग सिस्टम, ब्राउज़र और अन्य सॉफ़्टवेयर को नियमित रूप से अद्यतन करें।
3. ईमेल और लिंक के साथ सावधान रहें: अज्ञात स्रोतों से ईमेल और लिंक खोलते समय सावधान रहें और संदिग्ध अटैचमेंट से बचें।
4. एंटीवायरस सॉफ़्टवेयर का उपयोग करें: मैलवेयर का पता लगाने और हटाने के लिए एंटीवायरस सॉफ़्टवेयर स्थापित करें और नियमित रूप से अद्यतन करें।
5. फ़ायरवॉल का उपयोग करें: अनधिकृत पहुंच को रोकने के लिए अपने कंप्यूटर और नेटवर्क पर फ़ायरवॉल सक्षम करें।
6. दो-कारक प्रमाणीकरण का उपयोग करें: सुरक्षा की एक अतिरिक्त परत जोड़ने के लिए दो-कारक प्रमाणीकरण (2FA) को सक्षम करें।
7. अपने डेटा का बैकअप लें: अपने महत्वपूर्ण डेटा का नियमित रूप से एक सुरक्षित स्थान पर बैकअप लें।
8. सुरक्षित नेटवर्क का उपयोग करें: विशेष रूप से संवेदनशील जानकारी तक पहुंचते समय सुरक्षित और विश्वसनीय नेटवर्क का उपयोग करें।
9. सार्वजनिक कंप्यूटर से बचें: संवेदनशील गतिविधियों के लिए सार्वजनिक कंप्यूटर या सार्वजनिक वाई-फाई का उपयोग करने से बचें।
10. अद्यतित रहें: नवीनतम साइबर खतरों और रुझानों से अद्यतित रहें।

दैनिक जीवन में साइबर सुरक्षा की प्रासंगिकता

आज के डिजिटल युग में, साइबर सुरक्षा दैनिक जीवन में बहुत महत्वपूर्ण है। यहाँ कुछ कारण हैं:

1. व्यक्तिगत डेटा संरक्षण: साइबर सुरक्षा व्यक्तिगत डेटा, जैसे कि वित्तीय जानकारी, पते, और चिकित्सा रिकॉर्ड, को अनधिकृत पहुंच से बचाती है।
2. ऑनलाइन लेनदेन: साइबर सुरक्षा ऑनलाइन लेनदेन, जैसे कि ऑनलाइन बैंकिंग, ई-कॉमर्स, और डिजिटल भुगतान, को सुरक्षित बनाती है।
3. स्मार्ट डिवाइस: स्मार्ट डिवाइस के बढ़ते उपयोग के साथ, साइबर सुरक्षा इन डिवाइसों को हैकिंग और डेटा चोरी से बचाती है।
4. सोशल मीडिया: साइबर सुरक्षा सोशल मीडिया अकाउंट्स को हैकिंग और पहचान चोरी से बचाती है।

5. दूरस्थ कार्य: दूरस्थ कार्य के बढ़ते उपयोग के साथ, साइबर सुरक्षा कंपनी के नेटवर्क और डेटा तक दूरस्थ पहुंच को सुरक्षित बनाती है।

खराब साइबर सुरक्षा के परिणाम

1. वित्तीय नुकसान: साइबर हमले से महत्वपूर्ण वित्तीय नुकसान हो सकता है।
2. प्रतिष्ठा क्षति: साइबर हमले से व्यक्ति या संगठन की प्रतिष्ठा को नुकसान पहुंच सकता है।
3. डेटा हानि: साइबर हमले से डेटा हानि हो सकती है, जो अपूरणीय हो सकती है।

सर्वोत्तम अभ्यास

1. मजबूत पासवर्ड: सभी अकाउंट्स के लिए अद्वितीय और जटिल पासवर्ड का उपयोग करें।
2. सॉफ़्टवेयर अद्यतन: नियमित रूप से सॉफ़्टवेयर और ऑपरेटिंग सिस्टम को अद्यतन करें।
3. एंटीवायरस सॉफ़्टवेयर: एंटीवायरस सॉफ़्टवेयर स्थापित करें और नियमित रूप से अद्यतन करें।
4. ऑनलाइन सावधानी: ऑनलाइन लिंक्स पर क्लिक करने या अटैचमेंट डाउनलोड करने से सावधानी बरतें।
5. दो-कारक प्रमाणीकरण: जहां संभव हो, दो-कारक प्रमाणीकरण का उपयोग करें।

साइबर हमला क्या है?

साइबरहमला, डेटा या कंप्यूटर सिस्टम तक अनधिकृत पहुंच प्राप्त करके उन्हें चुराने, बदलने, बाधित करने या नष्ट करने का एक दुर्भावनापूर्ण प्रयास है।साइबर खतरे इन हमलों के पीछे संभावित हानिकारक गतिविधियां और अभिनेता हैं, जैसे मैलवेयर, फ़िशिंग, रैनसमवेयर और सोशल इंजीनियरिंग, जो व्यक्तियों और संगठनों दोनों को महत्वपूर्ण वित्तीय और परिचालन क्षति पहुंचा सकते हैं।

- यह कंप्यूटर सिस्टम, नेटवर्क या डिजिटल उपकरणों को लक्ष्य करके की गई जान बूझ कर की गई कार्रवाई है।
- इसका लक्ष्य सूचना संसाधनों से समझौता करना है, जिससे डेटा चोरी, परिवर्तन, विनाश या सेवाओं में व्यवधान उत्पन्न हो सकता है।
- हमलावर, जिन्हें खतरा पैदा करने वाले अभिनेता के रूप में जाना जाता है, अनधिकृत पहुंच प्राप्त करने और अपने उद्देश्यों को प्राप्त करने के लिए विभिन्न रणनीतियों का उपयोग करते हैं।

साइबर खतरे क्या हैं

ये हानिकारक गतिविधियाँ या उपकरण हैं जिनका उपयोग साइबर हमलों को अंजाम देने के लिए किया जाता है, जैसे दुर्भावनापूर्ण कोड, फ़िशिंग ई मेल या सोशल इंजीनियरिंग रणनीतियाँ।

- वे ऐसे व्यक्तियों या समूहों (खतरा पैदा करने वाले) का भी उल्लेख करते हैं, जिनका इरादा और क्षमता इन हमलों को शुरू करने की है।
- उदाहरणों में मैलवेयर (जैसे वायरस और रैनसमवेयर), फ़िशिंग घोटाले, सेवा अस्वीकार (DDoS) हमले, और अंदरूनी खतरों से उत्पन्न हमले शामिल हैं।

साइबर खतरों के सामान्य प्रकार:

मैलवेयर :
वायरस, वर्म्स और रैनसमवेयर सहित दुर्भावनापूर्ण सॉफ़्टवेयर, सिस्टम में घुसपैठ करने, उसे नुकसान पहुंचाने या डेटा चुराने के लिए डिज़ाइन किए गए हैं।

फ़िशिंग :
संवेदन शील जानकारी चुराने के लिए धोखाधड़ी पूर्ण संचार (अक्सर ईमेल) भेजना जो विश्वसनीय स्रोत से आता प्रतीत होता है।

सोशल इंजीनियरिंग :
लोगों को गोपनीय जानकारी प्रकट करने के लिए प्रेरित करना या ऐसी गतिविधियां करना जिनसे सुरक्षा को खतरा हो।

- **सेवा अस्वीकार (DDoS) हमले** :
किसी नेटवर्क या सिस्टम पर अत्यधिक ट्रैफिक लादना जिससे वह वैध उपयोगकर्ताओंके लिए अनुपलब्ध हो जाए।

अंदरूनी ख़तरे :
किसी संगठन के भीतर कर्मचारियों या अन्य विश्वसनीय व्यक्तियों द्वारा उत्पन्न खतरे, जिनकी प्रणालियों तक वैध पहुंच है।

साइबर हमलों के लक्ष्य:

- **वित्तीय लाभ**:
वित्तीय जानकारी चुराना, फिरौती की मांग करना (रैंसमवेयर), या धोखाधड़ी के लिए समझौता किए गए डेटा का उपयोग करना।
- **सूचना चोरी**:

बौद्धिक संपदा, ग्राहक डेटा या व्यक्तिगत पहचान योग्य जानकारी (PII) की चोरी करना।

- **परिचालन में व्यवधान:**
  महत्वपूर्ण बुनियादी ढांचे को बंद करना, प्रणालियों को नुकसान पहुंचाना, या व्यावसायिक परिचालन को रोकना।
- **राजनीतिक /वैचारिक उद्देश्य:**
  साइबर युद्ध या आतंकवाद के कृत्य व्यापक व्यवधान या क्षति का कारण बनते हैं।

1. मैलवेयर: सिस्टम को नुकसान पहुँचाने या शोषण करने के लिए डिज़ाइन किया गया सॉफ़्टवेयर, जिसमें वायरस, वर्म्स, ट्रोजन, रैंसमवेयर और स्पाइवेयर शामिल हैं।
2. फ़िशिंग: संवेदनशील जानकारी (जैसे पासवर्ड, क्रेडिट कार्ड विवरण) प्राप्त करने के लिए ईमेल, फ़ोन या टेक्स्ट के माध्यम से धोखाधड़ी वाले प्रयास।
3. रैंसमवेयर: मैलवेयर जो फ़ाइलों को एन्क्रिप्ट करता है और डिक्रिप्शन के लिए भुगतान की मांग करता है।
4. DDoS (डिस्ट्रिब्यूटेड डेनियल ऑफ़ सर्विस): सिस्टम को अनुपलब्ध बनाने के लिए ट्रैफ़िक के साथ ओवरवेल्म करना।
5. SQL इंजेक्शन: संवेदनशील डेटा को निकालने या संशोधित करने के लिए डेटाबेस में दुर्भावनापूर्ण कोड इंजेक्ट करना।
6. क्रॉस-साइट स्क्रिप्टिंग (XSS): उपयोगकर्ता डेटा चोरी करने या नियंत्रण लेने के लिए वेबसाइट्स में दुर्भावनापूर्ण कोड इंजेक्ट करना।
7. आइडेंटिटी चोरी: व्यक्तियों को प्रतिरूपित करने के लिए व्यक्तिगत जानकारी चोरी करना।
8. मैन-इन-द-मिडल (MitM) हमले: डेटा चोरी करने या मैलवेयर इंजेक्ट करने के लिए संचार को बाधित करना।
9. ज़ीरो-डे एक्सप्लॉइट्स: पहले से अज्ञात कमजोरियों का शोषण करना।
10. सोशल इंजीनियरिंग: संवेदनशील जानकारी का पता लगाने के लिए व्यक्तियों को हेरफेर करना।
इन खतरों से बचने के लिए, मजबूत साइबर सुरक्षा उपायों को लागू करना आवश्यक है, जैसे:
- सॉफ़्टवेयर को अद्यतन रखना
- मजबूत पासवर्ड का उपयोग करना
- फ़ायरवॉल और एंटीवायरस सॉफ़्टवेयर लागू करना
- नियमित बैकअप करना
- उपयोगकर्ताओं को साइबर सुरक्षा सर्वोत्तम प्रथाओं के बारे में शिक्षित करना

मैलवेयर (दुर्भावनापूर्ण सॉफ़्टवेयर) किसी भी सॉफ़्टवेयर को संदर्भित करता है जो कंप्यूटर सिस्टम, नेटवर्क या मोबाइल डिवाइस को नुकसान पहुँचाने या शोषण करने के लिए डिज़ाइन किया गया है। मैलवेयर कर सकता है:
1. संवेदनशील जानकारी चोरी करना (जैसे पासवर्ड, क्रेडिट कार्ड नंबर)
2. सिस्टम संचालन को बाधित करना
3. सिस्टम संसाधनों को हाईजैक करना
4. अन्य उपकरणों में फैलना

मैलवेयर के प्रकार:
1. वायरस: अन्य फ़ाइलों/कार्यक्रमों में पुनरुत्पादन और फैलना
2. वर्म्स: उपयोगकर्ता की बातचीत के बिना स्वयं पुनरुत्पादन और फैलना
3. ट्रोजन: वैध सॉफ़्टवेयर के रूप में खुद को छिपाना
4. रैंसमवेयर: फ़ाइलों को एन्क्रिप्ट करना, डिक्रिप्शन के लिए भुगतान की मांग करना
5. स्पाइवेयर: उपयोगकर्ता गतिविधि की निगरानी करना, संवेदनशील जानकारी चोरी करना
6. एडवेयर: अवांछित विज्ञापन प्रदर्शित करना, संभावित रूप से उपयोगकर्ता डेटा एकत्र करना
7. रूटकिट्स: सिस्टम का पता लगाने से मैलवेयर या खुद को छिपाना

सुरक्षा युक्तियाँ:
1. सॉफ़्टवेयर/ओएस को अद्यतन रखें
2. एंटीवायरस सॉफ़्टवेयर का उपयोग करें
3. संदिग्ध डाउनलोड/लिंक से बचें
4. मजबूत पासवर्ड का उपयोग करें
5. नियमित रूप से डेटा का बैकअप लें

Phishing

Phishing एक प्रकार का साइबर हमला है जिसमें हमलावर आपको धोखा देकर आपकी संवेदनशील जानकारी जैसे कि पासवर्ड, क्रेडिट कार्ड नंबर, या अन्य व्यक्तिगत जानकारी प्राप्त करने का प्रयास करते हैं।
फ़िशिंग हमले अक्सर ईमेल, टेक्स्ट मैसेज, या फ़ोन कॉल के माध्यम से होते हैं, और वे अक्सर वैध संस्थाओं जैसे कि बैंकों, ऑनलाइन स्टोर, या सोशल मीडिया प्लेटफ़ॉर्म के रूप में छिपे होते हैं।

फ़िशिंग से बचने के लिए कुछ युक्तियाँ:

1. संदिग्ध ईमेल/संदेशों से सावधान रहें: अज्ञात स्रोतों से आए ईमेल या संदेशों पर क्लिक न करें।
2. लिंक और अटैचमेंट से सावधान रहें: अज्ञात लिंक या अटैचमेंट खोलने से पहले दो बार सोचें।
3. वेबसाइट की जांच करें: सुनिश्चित करें कि वेबसाइट का पता सही है और यह सुरक्षित है (HTTPS)।
4. पासवर्ड सुरक्षित रखें: मजबूत पासवर्ड का उपयोग करें और उन्हें नियमित रूप से बदलें।
5. दो-कारक प्रमाणीकरण का उपयोग करें: अतिरिक्त सुरक्षा के लिए दो-कारक प्रमाणीकरण का उपयोग करें।

Ransomware एक प्रकार का मैलवेयर है जो आपके डेटा को एन्क्रिप्ट करता है और फिरौती की मांग करता है ताकि आपका डेटा वापस मिल सके।

रैंसमवेयर हमले के लक्षण:

1. डेटा एन्क्रिप्ट हो जाता है: आपकी फाइलें और डेटा एन्क्रिप्ट हो जाते हैं और आप उन तक नहीं पहुंच पाते।
2. फिरौती की मांग: हमलावर फिरौती की मांग करता है ताकि आपका डेटा वापस मिल सके।
3. धमकी: हमलावर अक्सर धमकी देते हैं कि अगर फिरौती नहीं दी गई तो आपका डेटा हटा दिया जाएगा।

रैंसमवेयर से बचाव के लिए कुछ युक्तियाँ:

1. नियमित बैकअप लें: अपने डेटा का नियमित बैकअप लें ताकि आप हमले के समय अपना डेटा वापस पा सकें।
2. सॉफ़्टवेयर अपडेट रखें: अपने सॉफ़्टवेयर और ऑपरेटिंग सिस्टम को अद्यतन रखें।
3. एंटीवायरस सॉफ़्टवेयर का उपयोग करें: एंटीवायरस सॉफ़्टवेयर का उपयोग करके रैंसमवेयर हमलों से बचाव करें।
4. संदिग्ध लिंक और अटैचमेंट से बचें: संदिग्ध लिंक और अटैचमेंट पर क्लिक न करें।

यदि आप रैंसमवेयर हमले का शिकार हो जाते हैं:

1. फिरौती न दें: फिरौती देने से बचें और इसके बजाय अपने डेटा को पुनर्स्थापित करने के लिए बैकअप का उपयोग करें।
2. सिस्टम को अलग करें: अपने सिस्टम को इंटरनेट से अलग करें ताकि हमलावर आपके डेटा तक नहीं पहुंच सके।
3. पेशेवर मदद लें: पेशेवर मदद लेने के लिए अपने आईटी विभाग या साइबर सुरक्षा विशेषज्ञ से संपर्क करें।

हैकर्स:

1. संवेदनशील जानकारी चोरी कर सकते हैं: व्यक्तिगत डेटा, वित्तीय जानकारी या गोपनीय व्यावसायिक डेटा।
2. सिस्टम को बाधित कर सकते हैं: सिस्टम को क्रैश करना, डाउनटाइम और नुकसान पहुंचाना।
3. दुर्भावनापूर्ण गतिविधियाँ: मैलवेयर फैलाना, फ़िशिंग या रैंसमवेयर हमले करना।

हैकर्स के प्रकार:

1. ब्लैक हैट हैकर्स: दुर्भावनापूर्ण हैकर्स जो व्यक्तिगत लाभ के लिए या नुकसान पहुंचाने के लिए हैकिंग करते हैं।
2. व्हाइट हैट हैकर्स: नैतिक हैकर्स जो संगठनों को सुरक्षा में सुधार करने में मदद करते हैं।
3. ग्रे हैट हैकर्स: हैकर्स जो कमजोरियों का फायदा उठा सकते हैं लेकिन जरूरी नहीं कि नुकसान पहुंचाएं।

सुरक्षा युक्तियाँ:

1. मजबूत पासवर्ड: अद्वितीय, जटिल पासवर्ड का उपयोग करें।
2. सॉफ़्टवेयर अद्यतन रखें: कमजोरियों को पैच करें।
3. एंटीवायरस सॉफ़्टवेयर का उपयोग करें: मैलवेयर का पता लगाएं और हटाएं।
4. ऑनलाइन सावधानी बरतें: संदिग्ध लिंक और डाउनलोड से बचें।

साइबर अपराध:

1. अपराधिक गतिविधियाँ: साइबर अपराध कंप्यूटर, नेटवर्क या इंटरनेट के माध्यम से की जाने वाली अवैध गतिविधियों को संदर्भित करता है।
2. उदाहरण: पहचान की चोरी, ऑनलाइन धोखाधड़ी, फ़िशिंग, साइबरस्टॉकिंग और अवैध सामग्री का वितरण।
3. प्रेरणाएँ: वित्तीय लाभ, व्यक्तिगत प्रतिशोध या नुकसान पहुंचाना।

साइबर हमला:

1. जानबूझकर व्यवधान: साइबर हमला एक जानबूझकर कंप्यूटर सिस्टम या नेटवर्क को बाधित करने, अक्षम करने या शोषण करने का प्रयास है।
2. उदाहरण: मैलवेयर, रैंसमवेयर, DDoS हमले और SQL इंजेक्शन।
3. प्रेरणाएँ: विभिन्न, जिनमें वित्तीय लाभ, जासूसी, तोड़फोड़ या हैक्टिविज्म शामिल हैं।

मुख्य अंतर:

1. कानूनी: साइबर अपराध हमेशा अवैध होता है, जबकि साइबर हमले अवैध या वैध हो सकते हैं (जैसे प्रवेश परीक्षण)।
2. क्षेत्र: साइबर अपराध गतिविधियों की एक विस्तृत श्रृंखला को शामिल करता है, जबकि साइबर हमले सिस्टम को बाधित करने या शोषण करने पर ध्यान केंद्रित करते हैं।

दोनों साइबर अपराध और साइबर हमले व्यक्तियों, संगठनों और राष्ट्रों के लिए महत्वपूर्ण खतरे पैदा करते हैं, जो मजबूत साइबर सुरक्षा उपायों के महत्व को उजागर करता है।

डेटा चोरी:

डेटा चोरी एक ऐसी घटना है जहां संवेदनशील, संरक्षित या गोपनीय डेटा बिना अधिकृत के एक्सेस, चोरी या उजागर किया जाता है। इसमें व्यक्तिगत पहचान योग्य जानकारी (पीआईआई), वित्तीय डेटा, बौद्धिक संपदा या अन्य संवेदनशील जानकारी शामिल हो सकती है।

डेटा चोरी के कारण:

1. हैकिंग: साइबर हमलावर कमजोरियों का फायदा उठाकर अनधिकृत पहुंच प्राप्त करते हैं।
2. आंतरिक खतरे: कर्मचारी या अधिकृत व्यक्ति जानबूझकर या अनजाने में डेटा को समझौता करते हैं।
3. फ़िशिंग: सामाजिक इंजीनियरिंग रणनीति व्यक्तियों को संवेदनशील जानकारी प्रकट करने के लिए धोखा देती है।
4. भौतिक चोरी: लैपटॉप, डिवाइस या भंडारण मीडिया जिसमें संवेदनशील डेटा होता है, चोरी हो जाते हैं।
5. मानव त्रुटि: आकस्मिक प्रदर्शन या डेटा के अनुचित हैंडलिंग।

डेटा चोरी के परिणाम:

1. वित्तीय नुकसान: चोरी हुआ डेटा धोखाधड़ी, पहचान की चोरी या डार्क वेब पर बेचा जा सकता है।
2. प्रतिष्ठा क्षति: संगठन विश्वास और विश्वसनीयता खो देते हैं।
3. नियामक दंड: डेटा सुरक्षा कानूनों का पालन न करने पर जुर्माना लग सकता है।
4. पहचान की चोरी: व्यक्तियों को वित्तीय और व्यक्तिगत नुकसान हो सकता है।

रोकथाम और शमन:

1. मजबूत सुरक्षा उपाय लागू करें: एन्क्रिप्शन, फ़ायरवॉल और एक्सेस नियंत्रण।
2. नियमित ऑडिट और जोखिम मूल्यांकन करें: कमजोरियों की पहचान करें और उन्हें संबोधित करें।
3. कर्मचारियों को प्रशिक्षित करें: डेटा हैंडलिंग सर्वोत्तम अभ्यास और सुरक्षा प्रोटोकॉल पर शिक्षित करें।
4. एक घटना प्रतिक्रिया योजना रखें: जल्दी से प्रतिक्रिया दें और उल्लंघनों को रोकें।

डेटा चोरी के गंभीर परिणाम हो सकते हैं, इसलिए संवेदनशील जानकारी की रक्षा के लिए सक्रिय उपाय आवश्यक हैं।

डेटा चोरी के वास्तविक उदाहरण:

प्रमुख उल्लंघन:

1. याहू: 2013 में 3 अरब उपयोगकर्ता खाते समझौता किए गए, जिनमें नाम, ईमेल पते, फ़ोन नंबर, जन्म तिथियां, पासवर्ड और सुरक्षा प्रश्न शामिल थे।
2. मैरियट इंटरनेशनल: 2018 में 500 मिलियन मेहमानों के रिकॉर्ड चोरी हुए, जिनमें नाम, घर के पते, ईमेल पते, फ़ोन नंबर, पासपोर्ट नंबर और जन्म तिथियां शामिल थीं।
3. इक्विफैक्स: 2017 में 147.9 मिलियन उपभोक्ता रिकॉर्ड समझौता किए गए, जिनमें सामाजिक सुरक्षा नंबर, जन्म तिथियां और पते शामिल थे।

हाल के उल्लंघन:

1. डेल: 2024 में 49 मिलियन ग्राहक रिकॉर्ड उजागर हुए, जिनमें नाम, पते और ऑर्डर जानकारी शामिल थी।
2. नेशनल पब्लिक डेटा: 2024 में 2.9 अरब रिकॉर्ड उजागर हुए, जिनमें नाम, ईमेल पते, फ़ोन नंबर, सामाजिक सुरक्षा नंबर और मेलिंग पते शामिल थे।

महत्वपूर्ण उल्लंघन:

1. कैपिटल वन: 2019 में 100 मिलियन ग्राहक खाते और क्रेडिट कार्ड आवेदन भंग हुए, जिनमें नाम, भौतिक पते, क्रेडिट स्कोर और अन्य संवेदनशील जानकारी शामिल थी।
2. लिंक्डइन: 2021 में 700 मिलियन उपयोगकर्ता रिकॉर्ड उजागर हुए, जिनमें पूर्ण नाम, फ़ोन नंबर, ईमेल पते और उपयोगकर्ता नाम शामिल थे।

भारत में डेटा चोरी के उदाहरण:

प्रमुख डेटा चोरी:

1. आईसीएमआर कोविड-19 डेटा चोरी (2023): एक बड़े पैमाने पर साइबर सुरक्षा घटना ने भारतीय चिकित्सा अनुसंधान परिषद को प्रभावित किया, जिससे लगभग 815 मिलियन भारतीय नागरिकों के संवेदनशील डेटा की चोरी हुई।
2. आधार डेटा चोरी (2018): एक महत्वपूर्ण उल्लंघन ने लाखों नागरिकों के व्यक्तिगत डेटा को समझौता किया, जिससे डेटा सुरक्षा उपायों में कमजोरियों को उजागर किया गया।

हाल के उल्लंघन:

1. हैथवे डेटा चोरी (2024): एक प्रमुख भारतीय इंटरनेट सेवा प्रदाता ने एक बड़े सुरक्षा उल्लंघन का अनुभव किया, जिससे 4.15 करोड़ से अधिक ग्राहकों की व्यक्तिगत जानकारी समझौता हुई।
2. बीएसएनएल डेटा चोरी (2024): एक दूरसंचार प्रदाता ने डेटा उल्लंघन का सामना किया, जिससे लाखों उपयोगकर्ताओं के संवेदनशील डेटा को उजागर किया गया।

अन्य उल्लेखनीय घटनाएं:

1. एम्स रैंसमवेयर हमला: ऑल इंडिया इंस्टीट्यूट ऑफ मेडिकल साइंसेज पर एक साइबर हमले ने 4 करोड़ रोगी रिकॉर्ड को समझौता किया, जिससे स्वास्थ्य देखभाल साइबर सुरक्षा में कमजोरियों को उजागर किया गया।

ये घटनाएं भारत में मजबूत साइबर सुरक्षा उपायों और सख्त डेटा सुरक्षा नियमों की आवश्यकता पर जोर देती हैं। डिजिटल व्यक्तिगत डेटा संरक्षण अधिनियम 2023 का उद्देश्य सख्त कानूनों और दंडों के साथ डेटा उल्लंघनों से निपटना है, जिसमें अनुपालन न करने पर ₹250 करोड़ तक का जुर्माना शामिल है।

साइबर सुरक्षा में जागरूकता और सतर्कता का महत्व:

1. रोकथाम: जागरूकता संभावित खतरों की पहचान करके साइबर हमलों को रोकने में मदद करती है।
2. प्रारंभिक पहचान: सतर्कता सुरक्षा घटनाओं की प्रारंभिक पहचान करने में सक्षम बनाती है, जिससे नुकसान कम होता है।
3. सक्रिय उपाय: जागरूकता और सतर्कता उभरते खतरों से बचाव के लिए सक्रिय उपायों को प्रेरित करती है।
4. जोखिम में कमी: सूचित व्यक्ति और संगठन साइबर हमलों के जोखिम को कम कर सकते हैं।
5. घटना प्रतिक्रिया में सुधार: जागरूकता और सतर्कता त्वरित और प्रभावी घटना प्रतिक्रिया की सुविधा प्रदान करती है।

महत्वपूर्ण पहलू:

1. अद्यतित रहें: नवीनतम साइबर खतरों और रुझानों से अद्यतित रहें।
2. सतर्क रहें: ईमेल, लिंक और अटैचमेंट के साथ बातचीत करते समय सावधान रहें।
3. मजबूत पासवर्ड का उपयोग करें: अद्वितीय और जटिल पासवर्ड का उपयोग करें।
4. सॉफ़्टवेयर अद्यतन रखें: नियमित रूप से सॉफ़्टवेयर और सिस्टम अद्यतन करें।
5. घटनाओं की रिपोर्ट करें: संदिग्ध गतिविधि और सुरक्षा घटनाओं की रिपोर्ट करें।

लाभ:

1. बेहतर सुरक्षा: जागरूकता और सतर्कता समग्र सुरक्षा मुद्रा को बढ़ाती है।
2. नुकसान में कमी: सक्रिय उपाय वित्तीय और प्रतिष्ठित नुकसान को कम करते हैं।
3. नियामक अनुपालन में सुधार: जागरूकता और सतर्कता नियामक आवश्यकताओं को पूरा करने में मदद करती है।

जागरूकता और सतर्कता को प्राथमिकता देकर, व्यक्ति और संगठन साइबर खतरों से प्रभावी ढंग से अपनी रक्षा कर सकते हैं।

Unit 2: Safe Use of Internet and Devices

Safe Internet Practices:

1. **Use strong passwords**: Use unique, complex passwords for all accounts, and change them regularly.
2. **Enable two-factor authentication**: Add an extra layer of security to your accounts with two-factor authentication.
3. **Keep software up-to-date**: Regularly update your operating system, browser, and other software to ensure you have the latest security patches.
4. **Use antivirus software**: Install and regularly update antivirus software to protect against malware and viruses.
5. **Be cautious with emails and links**: Avoid suspicious emails and links, and never provide personal or financial information in response to unsolicited emails.
6. **Use secure connections**: Use secure connections (https) when accessing sensitive information online.
7. **Use a VPN**: Consider using a virtual private network (VPN) when accessing public Wi-Fi networks.
8. **Monitor your accounts**: Regularly monitor your bank and credit card statements for suspicious activity.
9. **Use secure online storage**: Use secure online storage services, such as encrypted cloud storage, to protect your data.
10. **Educate yourself**: Stay informed about online safety and security best practices.

Online Safety Tips:

1. Avoid public computers: Avoid using public computers or public Wi-Fi networks for sensitive activities.
2. Use a firewall: Enable the firewall on your computer and network to block unauthorized access.
3. Back up your data: Regularly back up your important data to a secure location.
4. Use strong firewall settings: Configure your firewall settings to block unauthorized access.
5. Be cautious with downloads: Only download software and files from trusted sources.

Cybersecurity Best Practices:

1. Implement incident response plan: Have a plan in place for responding to cybersecurity incidents.
2. Conduct regular security audits: Regularly conduct security audits to identify vulnerabilities.
3. Use encryption: Use encryption to protect sensitive data.
4. Train employees: Educate employees on cybersecurity best practices.
5. Stay informed: Stay informed about the latest cybersecurity threats and trends.

सुरक्षित इंटरनेट अभ्यास:

1. मजबूत पासवर्ड का उपयोग करें: सभी खातों के लिए अद्वितीय और जटिल पासवर्ड का उपयोग करें और उन्हें नियमित रूप से बदलें।
2. दो-कारक प्रमाणीकरण सक्षम करें: अपने खातों में दो-कारक प्रमाणीकरण जोड़कर अतिरिक्त सुरक्षा परत जोड़ें।
3. सॉफ़्टवेयर अद्यतित रखें: अपने ऑपरेटिंग सिस्टम, ब्राउज़र और अन्य सॉफ़्टवेयर को नियमित रूप से अद्यतित करें ताकि आपके पास नवीनतम सुरक्षा पैच हों।
4. एंटीवायरस सॉफ़्टवेयर का उपयोग करें: मैलवेयर और वायरस से बचाव के लिए एंटीवायरस सॉफ़्टवेयर स्थापित करें और नियमित रूप से अद्यतित करें।
5. ईमेल और लिंक के साथ सावधानी बरतें: संदिग्ध ईमेल और लिंक से बचें और कभी भी अनचाहे ईमेल के जवाब में व्यक्तिगत या वित्तीय जानकारी न दें।

6. सुरक्षित कनेक्शन का उपयोग करें: संवेदनशील जानकारी ऑनलाइन एक्सेस करते समय सुरक्षित कनेक्शन (https) का उपयोग करें।
7. वीपीएन का उपयोग करें: सार्वजनिक वाई-फाई नेटवर्क एक्सेस करते समय वीपीएन का उपयोग करने पर विचार करें।
8. अपने खातों की निगरानी करें: अपने बैंक और क्रेडिट कार्ड विवरणों की नियमित रूप से निगरानी करें।
9. सुरक्षित ऑनलाइन भंडारण का उपयोग करें: अपने डेटा की सुरक्षा के लिए सुरक्षित ऑनलाइन भंडारण सेवाओं का उपयोग करें।
10. शिक्षित करें: ऑनलाइन सुरक्षा और सुरक्षा सर्वोत्तम अभ्यासों के बारे में सूचित रहें।

ऑनलाइन सुरक्षा युक्तियाँ:

1. सार्वजनिक कंप्यूटर से बचें: संवेदनशील गतिविधियों के लिए सार्वजनिक कंप्यूटर या सार्वजनिक वाई-फाई नेटवर्क का उपयोग करने से बचें।
2. फ़ायरवॉल का उपयोग करें: अनधिकृत पहुंच को रोकने के लिए अपने कंप्यूटर और नेटवर्क पर फ़ायरवॉल सक्षम करें।
3. अपने डेटा का बैकअप लें: अपने महत्वपूर्ण डेटा का नियमित रूप से बैकअप लें।
4. मजबूत फ़ायरवॉल सेटिंग्स का उपयोग करें: अनधिकृत पहुंच को रोकने के लिए अपनी फ़ायरवॉल सेटिंग्स को कॉन्फ़िगर करें।
5. डाउनलोड के साथ सावधानी बरतें: केवल विश्वसनीय स्रोतों से सॉफ़्टवेयर और फ़ाइलें डाउनलोड करें।

साइबर सुरक्षा सर्वोत्तम अभ्यास:

1. घटना प्रतिक्रिया योजना लागू करें: साइबर सुरक्षा घटनाओं के लिए प्रतिक्रिया करने के लिए एक योजना बनाएं।
2. नियमित सुरक्षा ऑडिट करें: कमजोरियों की पहचान करने के लिए नियमित सुरक्षा ऑडिट करें।
3. एन्क्रिप्शन का उपयोग करें: संवेदनशील डेटा की सुरक्षा के लिए एन्क्रिप्शन का उपयोग करें।
4. कर्मचारियों को प्रशिक्षित करें: कर्मचारियों को साइबर सुरक्षा सर्वोत्तम अभ्यासों पर शिक्षित करें।
5. सूचित रहें: नवीनतम साइबर सुरक्षा खतरों और रुझानों के बारे में सूचित रहें।

Strong Passwords:

A strong password is a password that is difficult for others to guess or crack. Here are some characteristics of strong passwords:

1. Length: A minimum of 12 characters, but longer is better.
2. Complexity: A mix of:
   - Uppercase letters (A-Z)
   - Lowercase letters (a-z)
   - Numbers (0-9)
   - Special characters (!, @, #, $, etc.)
3. Uniqueness: Use a unique password for each account.
4. Randomness: Avoid using easily guessable information such as:
   - Your name or birthdate
   - Common words or phrases
   - Sequences (e.g., "123456")
5. Avoid password reuse: Don't use the same password across multiple accounts.

Tips for creating strong passwords:

1. Use a password manager to generate and store unique, complex passwords.

2. Avoid using words or phrases that can be found in a dictionary.

3. Use a passphrase, which is a sequence of words that is easy for you to remember, but hard for others to guess.

4. Change your passwords regularly (every 60-90 days).

5. Don't share your passwords with anyone.

Why strong passwords matter:

1. Protects against unauthorized access: Strong passwords help prevent others from accessing your accounts and sensitive information.

2. Reduces risk of identity theft: Strong passwords can help protect your identity and prevent identity theft.

3. Safeguards sensitive information: Strong passwords help protect sensitive information, such as financial data and personal documents.

मजबूत पासवर्ड:

एक मजबूत पासवर्ड वह होता है जो दूसरों के लिए अनुमान लगाना या क्रैक करना मुश्किल होता है। मजबूत पासवर्ड की कुछ विशेषताएं हैं:

1. लंबाई: न्यूनतम 12 वर्ण, लेकिन लंबा बेहतर है।
2. जटिलता: एक मिश्रण:
- बड़े अक्षर (A-Z)
- छोटे अक्षर (a-z)
- संख्या (0-9)
- विशेष वर्ण (!, @, #, $, आदि)
3. अद्वितीयता: प्रत्येक खाते के लिए एक अद्वितीय पासवर्ड का उपयोग करें।
4. यादृच्छिकता: आसानी से अनुमान लगाने योग्य जानकारी का उपयोग करने से बचें जैसे:
- आपका नाम या जन्म तिथि
- सामान्य शब्द या वाक्यांश
- अनुक्रम (जैसे, "123456")
5. पासवर्ड पुन: उपयोग से बचें: एक ही पासवर्ड का उपयोग कई खातों में न करें।

मजबूत पासवर्ड के उदाहरण:

1. G#8dL4pM$eJ#
2. P@ssw0rd!23K
3. Tr0ub4d3!K1ng

मजबूत पासवर्ड बनाने के लिए सुझाव:

1. अद्वितीय और जटिल पासवर्ड उत्पन्न करने और संग्रहीत करने के लिए पासवर्ड मैनेजर का उपयोग करें।
2. शब्दकोश में पाए जाने वाले शब्दों या वाक्यांशों का उपयोग करने से बचें।
3. एक पासफ़्रेज़ का उपयोग करें, जो शब्दों का एक क्रम है जो आपके लिए याद रखना आसान है, लेकिन दूसरों के लिए अनुमान लगाना मुश्किल है।
4. अपने पासवर्ड नियमित रूप से बदलें (हर 60-90 दिनों में)।
5. अपने पासवर्ड किसी के साथ साझा न करें।

मजबूत पासवर्ड क्यों महत्वपूर्ण हैं:

1. अनधिकृत पहुंच से बचाता है: मजबूत पासवर्ड दूसरों को आपके खातों और संवेदनशील जानकारी तक पहुंचने से रोकने में मदद करते हैं।
2. पहचान की चोरी के जोखिम को कम करता है: मजबूत पासवर्ड आपकी पहचान की रक्षा करने और पहचान की चोरी को रोकने में मदद करते हैं।

3. संवेदनशील जानकारी की रक्षा करता है: मजबूत पासवर्ड संवेदनशील जानकारी, जैसे कि वित्तीय डेटा और व्यक्तिगत दस्तावेजों की रक्षा करने में मदद करते हैं।

Two-Factor Authentication (2FA):

Two-factor authentication is a security process that requires a user to provide two different authentication factors to access a system, network, or application. This adds an additional layer of security to the traditional username and password combination.

How 2FA Works:

1. First Factor: You enter your username and password.
2. Second Factor: You provide a second form of verification, such as:
- A one-time password (OTP) sent to your phone or email.
- A fingerprint or facial recognition scan.
- A smart card or token.
- A code generated by an authenticator app.

Benefits of 2FA:

1. Improved Security: 2FA makes it much harder for attackers to gain unauthorized access to your accounts.
2. Reduced Risk of Identity Theft: 2FA adds an extra layer of protection against phishing and other types of attacks.
3. Compliance: 2FA is often required by regulatory bodies to protect sensitive information.

Types of 2FA:

1. SMS-based 2FA: One-time passwords are sent to your phone via SMS.
2. Authenticator App 2FA: Apps like Google Authenticator or Authy generate time-based one-time passwords.
3. Biometric 2FA: Fingerprint or facial recognition scans.
4. Smart Card 2FA: Physical tokens or smart cards.

Best Practices:

1. Use 2FA whenever possible: Enable 2FA on all accounts that support it.
2. Use a strong password: Combine 2FA with a strong, unique password.
3. Keep your 2FA device secure: Protect your 2FA device or token from unauthorized access.

दो-कारक प्रमाणीकरण (2FA):

दो-कारक प्रमाणीकरण एक सुरक्षा प्रक्रिया है जिसमें उपयोगकर्ता को सिस्टम, नेटवर्क या एप्लिकेशन तक पहुंचने के लिए दो अलग-अलग प्रमाणीकरण कारक प्रदान करने होते हैं। यह पारंपरिक उपयोगकर्ता नाम और पासवर्ड संयोजन में एक अतिरिक्त सुरक्षा परत जोड़ता है।

2FA कैसे काम करता है:

1. पहला कारक: आप अपना उपयोगकर्ता नाम और पासवर्ड दर्ज करते हैं।
2. दूसरा कारक: आप दूसरी प्रमाणीकरण विधि प्रदान करते हैं, जैसे:
- आपके फ़ोन या ईमेल पर भेजा गया एक-बार का पासवर्ड (OTP)।
- उंगलियों के निशान या चेहरे की पहचान स्कैन।
- एक स्मार्ट कार्ड या टोकन।
- एक प्रमाणक ऐप द्वारा उत्पन्न कोड।

2FA के लाभ:

1. सुधारित सुरक्षा: 2FA हमलावरों के लिए आपके खातों तक अनधिकृत पहुंच प्राप्त करना बहुत कठिन बना देता है।

2. पहचान की चोरी के जोखिम में कमी: 2FA फिशिंग और अन्य प्रकार के हमलों के खिलाफ अतिरिक्त सुरक्षा प्रदान करता है।
3. अनुपालन: संवेदनशील जानकारी की सुरक्षा के लिए नियामक निकायों द्वारा अक्सर 2FA की आवश्यकता होती है।

2FA के प्रकार:

1. एसएमएस-आधारित 2FA: एक-बार के पासवर्ड आपके फ़ोन पर एसएमएस के माध्यम से भेजे जाते हैं।
2. प्रमाणक ऐप 2FA: गूगल प्रमाणक या ऑथी जैसे ऐप समय-आधारित एक-बार के पासवर्ड उत्पन्न करते हैं।
3. बायोमेट्रिक 2FA: उंगलियों के निशान या चेहरे की पहचान स्कैन।
4. स्मार्ट कार्ड 2FA: भौतिक टोकन या स्मार्ट कार्ड।

सर्वोत्तम अभ्यास:

1. जहां भी संभव हो 2FA का उपयोग करें: सभी खातों पर 2FA सक्षम करें जो इसका समर्थन करते हैं।
2. एक मजबूत पासवर्ड का उपयोग करें: 2FA को एक मजबूत, अद्वितीय पासवर्ड के साथ जोड़ें।
3. अपने 2FA डिवाइस को सुरक्षित रखें: अपने 2FA डिवाइस या टोकन को अनधिकृत पहुंच से बचाएं।

Avoiding Suspicious Links:

1. Be cautious with emails: Avoid clicking on links from unknown senders, especially those with generic greetings or spelling mistakes.
2. Verify website authenticity: Check the website's URL and ensure it's legitimate before entering sensitive information.
3. Use antivirus software: Install and regularly update antivirus software to protect against malware.
4. Use a web browser extension: Use a web browser extension that blocks suspicious links, such as uBlock Origin or Malwarebytes.
5. Hover over links: Check the link's destination URL before clicking.
6. Avoid shortened URLs: Be cautious of shortened URLs, especially from unknown sources.
7. Keep software up-to-date: Regularly update your operating system, browser, and other software to ensure you have the latest security patches.
8. Use strong passwords: Use unique and complex passwords for all accounts, and consider using a password manager.
9. Use two-factor authentication: Enable two-factor authentication (2FA) whenever possible.
10. Stay informed: Stay up-to-date with the latest online threats and security best practices.

Red Flags:

1. Urgent or threatening language: Be wary of links that create a sense of urgency or threaten consequences.
2. Suspicious URLs: Be cautious of URLs that are misspelled, contain random characters, or have unusual extensions.
3. Unknown senders: Be cautious of links from unknown senders, especially if the email or message is unsolicited.
4. Too good to be true: Be wary of links that promise unrealistic rewards or benefits.

Avoiding Suspicious Links:

1. Verify the source: Check if the link is from a trusted source or website.
2. Check the URL: Look for spelling mistakes, unusual characters, or suspicious domains.
3. Hover over links: Check the link's destination URL before clicking.
4. Use antivirus software: Install and regularly update antivirus software to protect against malware.
5. Use a web browser extension: Use a web browser extension that blocks suspicious links.
6. Be cautious of shortened URLs: Avoid clicking on shortened URLs from unknown sources.
7. Avoid clicking on pop-ups: Be wary of pop-ups that ask you to click on links or download software.
8. Use strong passwords: Use unique and complex passwords for all accounts.
9. Enable two-factor authentication: Add an extra layer of security to your accounts.

10. Stay informed: Stay up-to-date with the latest online threats and security best practices.

Tips for Mobile Users:

1. Use mobile security apps: Install mobile security apps that detect and block suspicious links.
2. Be cautious of QR codes: Scan QR codes from trusted sources only.
3. Use secure browsers: Use secure web browsers that have built-in security features.

Consequences of Ignoring Suspicious Links:

1. Malware infection: Your device may be infected with malware.
2. Data theft: Your sensitive information may be stolen.
3. Identity theft: Your personal data may be used for identity theft.

Concept of secure browsing

Secure browsing is the practice of protecting your online activities and personal information from cyber threats like malware and phishing by using tools and techniques such as encryption, secure connections (HTTPS), and updated software. Key concepts include ensuring data is encrypted, avoiding suspicious websites and downloads, using strong passwords, and regularly updating all software.

Secure browsing refers to the practice of accessing the internet in a way that protects your personal data, identity, and device from unauthorized access, theft, or damage. It involves using various techniques and tools to ensure the confidentiality, integrity, and authenticity of online communications.

Core concepts of secure browsing

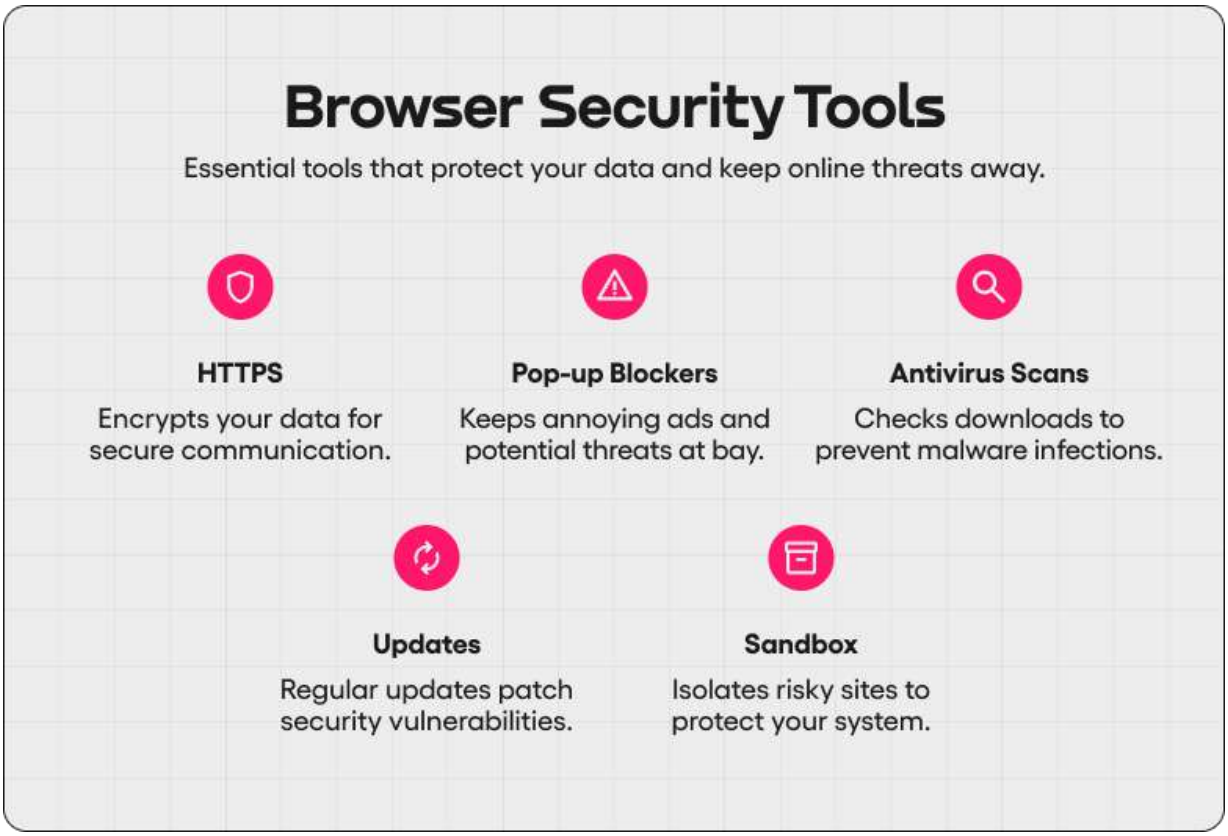
- ***Encryption:***
  The process of converting data into a code to prevent unauthorized access. When you see https:// and a padlock icon in your browser's address bar, it means the connection to the website is encrypted, protecting your data from being intercepted.
- ***Secure connections:***
  Using encrypted connections like HTTPS is the foundation of secure browsing, ensuring the data exchanged between your browser and the website is private and cannot be easily tampered with.
- ***Malware and phishing prevention:***
  This involves using tools to block harmful software (malware) and websites designed to trick you into revealing sensitive information (phishing). Some browsers have built-in features like pop-up blockers and anti-phishing filters, and you should be cautious about what you download or click on.
- ***Software updates:***
  Browsers, operating systems, and plugins often receive security updates that patch vulnerabilities. Keeping your software up to date is crucial to protect against known threats.
- ***Strong and unique passwords:***
  Using a unique and complex password for each online account is vital. Consider using a password manager to help you create and store these strong passwords securely.
- ***Privacy settings and tools:***
  Secure browsing also involves configuring your browser's privacy settings to block third-party cookies, limit tracking, and control website permissions. Using a VPN can further mask your IP address, and some browsers offer enhanced privacy modes.

Key Concepts:

1. HTTPS (Hypertext Transfer Protocol Secure): A secure protocol that encrypts data transmitted between your browser and websites.
2. Encryption: The process of converting plaintext data into unreadable ciphertext to prevent unauthorized access.
3. SSL/TLS (Secure Sockets Layer/Transport Layer Security): Protocols that provide end-to-end encryption for online communications.
4. Browser Security: Features and settings that protect your browser from malware, phishing, and other online threats.
5. Password Management: The practice of securely storing and managing passwords for online accounts.
6. Two-Factor Authentication (2FA): An additional layer of security that requires a second form of verification, such as a code sent to your phone or a biometric scan.
7. Cookie Management: Controlling how websites store and access cookies, which can track your online activities.
8. Private Browsing: A feature that allows you to browse the internet without storing your browsing history, cookies, or other data.

Best Practices:

1. Use a reputable web browser: Choose a browser that prioritizes security and privacy.
2. Keep software up-to-date: Regularly update your browser, operating system, and other software to ensure you have the latest security patches.
3. Use strong passwords: Use unique and complex passwords for all accounts, and consider using a password manager.
4. Be cautious of phishing: Be wary of suspicious emails, links, and websites that may attempt to steal your sensitive information.
5. Use a VPN (Virtual Private Network): Consider using a VPN to encrypt your internet traffic and protect your data when using public Wi-Fi networks.



सुरक्षित ब्राउज़िंग:

सुरक्षित ब्राउज़िंग इंटरनेट का उपयोग करने का एक तरीका है जो आपकी व्यक्तिगत डेटा, पहचान और डिवाइस को अनधिकृत पहुंच, चोरी या नुकसान से बचाता है। इसमें ऑनलाइन संचार की गोपनीयता, अखंडता और प्रामाणिकता सुनिश्चित करने के लिए विभिन्न तकनीकों और उपकरणों का उपयोग करना शामिल है।

मुख्य अवधारणाएं:

1. HTTPS (हाइपरटेक्स्ट ट्रांसफर प्रोटोकॉल सिक्योर): एक सुरक्षित प्रोटोकॉल जो आपके ब्राउज़र और वेबसाइटों के बीच प्रेषित डेटा को एन्क्रिप्ट करता है।
2. एन्क्रिप्शन: अनधिकृत पहुंच को रोकने के लिए सादे पाठ डेटा को अपठनीय सिफरटेक्स्ट में परिवर्तित करने की प्रक्रिया।
3. SSL/TLS (सिक्योर सॉकेट लेयर/ट्रांसपोर्ट लेयर सिक्योरिटी): प्रोटोकॉल जो ऑनलाइन संचार के लिए एंड-टू-एंड एन्क्रिप्शन प्रदान करते हैं।
4. ब्राउज़र सुरक्षा: आपके ब्राउज़र को मैलवेयर, फ़िशिंग और अन्य ऑनलाइन खतरों से बचाने वाली सुविधाएँ और सेटिंग्स।
5. पासवर्ड प्रबंधन: ऑनलाइन खातों के लिए पासवर्ड को सुरक्षित रूप से संग्रहीत और प्रबंधित करने का अभ्यास।
6. दो-कारक प्रमाणीकरण (2FA): एक अतिरिक्त सुरक्षा परत जो एक दूसरे रूप में सत्यापन की आवश्यकता होती है, जैसे कि आपके फ़ोन पर भेजा गया कोड या बायोमेट्रिक स्कैन।
7. कुकी प्रबंधन: नियंत्रित करना कि वेबसाइटें कुकीज़ को कैसे संग्रहीत और एक्सेस करती हैं, जो आपकी ऑनलाइन गतिविधियों को ट्रैक कर सकती हैं।
8. निजी ब्राउज़िंग: एक सुविधा जो आपको अपने ब्राउज़िंग इतिहास, कुकीज़ या अन्य डेटा को संग्रहीत किए बिना इंटरनेट ब्राउज़ करने की अनुमति देती है।

सर्वोत्तम अभ्यास:

1. एक प्रतिष्ठित वेब ब्राउज़र का उपयोग करें: एक ब्राउज़र चुनें जो सुरक्षा और गोपनीयता को प्राथमिकता देता है।
2. सॉफ़्टवेयर अद्यतित रखें: अपने ब्राउज़र, ऑपरेटिंग सिस्टम और अन्य सॉफ़्टवेयर को नियमित रूप से अद्यतन करें ताकि आपके पास नवीनतम सुरक्षा पैच हों।
3. मजबूत पासवर्ड का उपयोग करें: सभी खातों के लिए अद्वितीय और जटिल पासवर्ड का उपयोग करें, और एक पासवर्ड मैनेजर का उपयोग करने पर विचार करें।
4. फ़िशिंग से सावधान रहें: संदिग्ध ईमेल, लिंक और वेबसाइटों से सावधान रहें जो आपकी संवेदनशील जानकारी चोरी करने का प्रयास कर सकते हैं।
5. एक VPN (वर्चुअल प्राइवेट नेटवर्क) का उपयोग करें: अपने इंटरनेट ट्रैफ़िक को एन्क्रिप्ट करने और सार्वजनिक वाई-फ़ाई नेटवर्क का उपयोग करते समय अपनी डेटा की सुरक्षा करने के लिए एक VPN का उपयोग करने पर विचार करें।

Essential Mobile/Computer Safety:

1. Use strong passwords: Use unique and complex passwords for all accounts.
2. Enable two-factor authentication: Add an extra layer of security to your accounts.
3. Keep software up-to-date: Regularly update your operating system, browser, and other software.
4. Use antivirus software: Install and regularly update antivirus software.
5. Be cautious of phishing: Be wary of suspicious emails, links, and websites.
6. Use a VPN: Consider using a VPN to encrypt your internet traffic.
7. Use secure networks: Use secure, password-protected Wi-Fi networks.
8. Back up your data: Regularly back up your important data.
9. Use a firewall: Enable the firewall on your computer and network.
10. Monitor your accounts: Regularly monitor your accounts for suspicious activity.

Mobile-Specific Safety Tips:

1. Use a screen lock: Lock your device with a PIN, password, or fingerprint.
2. Be cautious of app permissions: Only grant necessary permissions to apps.
3. Use secure messaging apps: Use end-to-end encrypted messaging apps.
4. Keep your device updated: Regularly update your device's operating system.
5. Use mobile security software: Install mobile security software to protect against malware.

Computer-Specific Safety Tips:

1. Use a reputable antivirus: Install and regularly update antivirus software.
2. Use strong passwords: Use unique and complex passwords for all accounts.
3. Keep your operating system updated: Regularly update your operating system.
4. Use a firewall: Enable the firewall on your computer and network.
5. Be cautious of downloads: Only download software and files from trusted sources.

मोबाइल और कंप्यूटर सुरक्षा के आवश्यक उपाय:

मोबाइल सुरक्षा:

1. पासवर्ड और पिन का उपयोग करें: अपने मोबाइल डिवाइस को सुरक्षित करने के लिए पासवर्ड या पिन का उपयोग करें।
2. एंटीवायरस सॉफ़्टवेयर स्थापित करें: अपने मोबाइल डिवाइस पर एंटीवायरस सॉफ़्टवेयर स्थापित करें।
3. सुरक्षित वाई-फाई नेटवर्क का उपयोग करें: सुरक्षित वाई-फाई नेटवर्क का उपयोग करें और सार्वजनिक वाई-फाई नेटवर्क से बचें।
4. ऐप्स को सावधानी से डाउनलोड करें: ऐप्स को केवल विश्वसनीय स्रोतों से डाउनलोड करें।
5. नियमित रूप से अपडेट करें: अपने मोबाइल डिवाइस और ऐप्स को नियमित रूप से अपडेट करें।

कंप्यूटर सुरक्षा:

1. एंटीवायरस सॉफ़्टवेयर स्थापित करें: अपने कंप्यूटर पर एंटीवायरस सॉफ़्टवेयर स्थापित करें।
2. पासवर्ड और लॉगिन विवरण सुरक्षित रखें: अपने पासवर्ड और लॉगिन विवरण को सुरक्षित रखें।
3. सुरक्षित ब्राउज़िंग: सुरक्षित ब्राउज़िंग का अभ्यास करें और संदिग्ध वेबसाइटों से बचें।
4. नियमित रूप से अपडेट करें: अपने ऑपरेटिंग सिस्टम और सॉफ़्टवेयर को नियमित रूप से अपडेट करें।
5. फ़ायरवॉल सक्षम करें: अपने कंप्यूटर पर फ़ायरवॉल सक्षम करें।

सामान्य सुरक्षा सुझाव:

1. मजबूत पासवर्ड का उपयोग करें: मजबूत पासवर्ड का उपयोग करें और उन्हें नियमित रूप से बदलें।
2. दो-कारक प्रमाणीकरण का उपयोग करें: दो-कारक प्रमाणीकरण का उपयोग करके अपने खातों को सुरक्षित करें।
3. सावधानी से ईमेल और लिंक खोलें: संदिग्ध ईमेल और लिंक से सावधान रहें।
4. नियमित रूप से बैकअप लें: अपने महत्वपूर्ण डेटा का नियमित रूप से बैकअप लें।
5. सुरक्षित नेटवर्क का उपयोग करें: सुरक्षित नेटवर्क का उपयोग करें और सार्वजनिक वाई-फाई नेटवर्क से बचें।

एंटीवायरस:

एंटीवायरस एक प्रकार का सॉफ़्टवेयर है जो आपके कंप्यूटर या मोबाइल डिवाइस को वायरस, मैलवेयर, और अन्य प्रकार के दुर्भावनापूर्ण सॉफ़्टवेयर से बचाने के लिए डिज़ाइन किया गया है।

एंटीवायरस के मुख्य कार्य:

1. वायरस स्कैनिंग: आपके कंप्यूटर या मोबाइल डिवाइस को वायरस और मैलवेयर के लिए स्कैन करना।
2. वायरस हटाना: आपके सिस्टम से वायरस और मैलवेयर को हटाना।
3. रियल-टाइम सुरक्षा: आपके सिस्टम को वास्तविक समय में सुरक्षित रखना और दुर्भावनापूर्ण सॉफ़्टवेयर को आपके सिस्टम में प्रवेश करने से रोकना।

4. ऑटोमैटिक अपडेट्स: एंटीवायरस सॉफ़्टवेयर को नियमित रूप से अपडेट करना ताकि यह नवीनतम वायरस और मैलवेयर के खतरों से सुरक्षित रख सके।

एंटीवायरस के लाभ:

1. वायरस और मैलवेयर से सुरक्षा: एंटीवायरस सॉफ़्टवेयर आपके सिस्टम को वायरस और मैलॉगेयर से बचाता है।
2. डेटा सुरक्षा: एंटीवायरस सॉफ़्टवेयर आपके डेटा को सुरक्षित रखने में मदद करता है।
3. सिस्टम प्रदर्शन में सुधार: एंटीवायरस सॉफ़्टवेयर आपके सिस्टम को तेजी से और कुशलता से चलाने में मदद करता है।
4. नवीनतम खतरों से सुरक्षा: एंटीवायरस सॉफ़्टवेयर आपको नवीनतम वायरस और मैलवेयर के खतरों से सुरक्षित रखता है।

एंटीवायरस सॉफ़्टवेयर का चयन करते समय ध्यान रखने योग्य बातें:

1. विश्वसनीयता: एंटीवायरस सॉफ़्टवेयर की विश्वसनीयता और प्रतिष्ठा की जाँच करें।
2. फीचर्स: एंटीवायरस सॉफ़्टवेयर के फीचर्स और सुरक्षा सुविधाओं की जाँच करें।
3. सिस्टम आवश्यकताएं: एंटीवायरस सॉफ़्टवेयर की सिस्टम आवश्यकताओं की जाँच करें और सुनिश्चित करें कि यह आपके सिस्टम के साथ संगत है।
4. ग्राहक समर्थन: एंटीवायरस सॉफ़्टवेयर के ग्राहक समर्थन की जाँच करें और सुनिश्चित करें कि यह आपकी आवश्यकताओं को पूरा करता है।

Antivirus:

Antivirus software is a type of computer program designed to detect, prevent, and remove malware, including viruses, worms, trojans, and other types of malicious software.

Key Features:

1. Virus scanning: Scans your computer or device for malware.
2. Real-time protection: Provides ongoing protection against malware.
3. Malware removal: Removes detected malware from your system.
4. Automatic updates: Regularly updates virus definitions to stay protected against new threats.

Benefits:

1. Protection against malware: Antivirus software helps protect your computer or device from malware.
2. Data protection: Antivirus software helps protect your data from unauthorized access.
3. System performance: Antivirus software can help improve system performance by removing malware.
4. Latest threat protection: Antivirus software provides protection against the latest malware threats.

Choosing Antivirus Software:

1. Reputation: Research the reputation of the antivirus software.
2. Features: Consider the features and security capabilities of the antivirus software.
3. System requirements: Ensure the antivirus software is compatible with your system.
4. Customer support: Evaluate the customer support offered by the antivirus software provider.

Updates and App Permissions in Essential Mobile and Computer Safety:

Updates:

1. Keep operating system and apps updated: Regularly update your operating system and apps to ensure you have the latest security patches and features.
2. Enable automatic updates: Enable automatic updates for your operating system and apps to stay protected against known vulnerabilities.
3. Prioritize updates: Prioritize updates for critical security patches and updates that fix known vulnerabilities.

App Permissions:

1. Review app permissions: Carefully review app permissions before installing an app.
2. Grant only necessary permissions: Grant only the permissions that are necessary for the app to function.
3. Monitor app permissions: Regularly review and update app permissions to ensure they align with your comfort level.
4. Use app permission managers: Consider using app permission managers or features like Android's permission manager to control app permissions.

Best Practices:

1. Stay informed: Stay informed about the latest security threats and updates.
2. Use strong passwords: Use strong passwords and enable two-factor authentication.
3. Use antivirus software: Use antivirus software to protect against malware.
4. Back up data: Regularly back up your data to prevent loss in case of a security breach.

Benefits:

1. Improved security: Updates and app permissions can help protect against known vulnerabilities and malware.
2. Data protection: Updates and app permissions can help protect your personal data from unauthorized access.
3. Peace of mind: By staying up-to-date and controlling app permissions, you can have peace of mind knowing your device and data are secure.

अपडेट्स और ऐप अनुमतियाँ मोबाइल और कंप्यूटर सुरक्षा में:

अपडेट्स:

1. ऑपरेटिंग सिस्टम और ऐप्स को अद्यतन रखें: अपने ऑपरेटिंग सिस्टम और ऐप्स को नियमित रूप से अद्यतन करें ताकि आपके पास नवीनतम सुरक्षा पैच और विशेषताएं हों।
2. स्वचालित अपडेट्स सक्षम करें: अपने ऑपरेटिंग सिस्टम और ऐप्स के लिए स्वचालित अपडेट्स सक्षम करें ताकि आप ज्ञात कमजोरियों से सुरक्षित रहें।
3. अपडेट्स को प्राथमिकता दें: महत्वपूर्ण सुरक्षा पैच और अपडेट्स को प्राथमिकता दें जो ज्ञात कमजोरियों को ठीक करते हैं।

ऐप अनुमतियाँ:

1. ऐप अनुमतियों की समीक्षा करें: ऐप इंस्टॉल करने से पहले ऐप अनुमतियों की सावधानी से समीक्षा करें।
2. केवल आवश्यक अनुमतियाँ दें: ऐप को केवल वही अनुमतियाँ दें जो उसके कार्य के लिए आवश्यक हैं।
3. ऐप अनुमतियों की निगरानी करें: नियमित रूप से ऐप अनुमतियों की समीक्षा करें और उन्हें अद्यतन करें ताकि वे आपके आराम के स्तर के अनुसार हों।
4. ऐप अनुमति प्रबंधकों का उपयोग करें: ऐप अनुमति प्रबंधकों या एंड्रॉइड की अनुमति प्रबंधक जैसी सुविधाओं का उपयोग करके ऐप अनुमतियों को नियंत्रित करें।

सर्वोत्तम अभ्यास:

1. सूचित रहें: नवीनतम सुरक्षा खतरों और अपडेट्स के बारे में सूचित रहें।
2. मजबूत पासवर्ड का उपयोग करें: मजबूत पासवर्ड का उपयोग करें और दो-कारक प्रमाणीकरण सक्षम करें।
3. एंटीवायरस सॉफ़्टवेयर का उपयोग करें: मैलवेयर से बचाव के लिए एंटीवायरस सॉफ़्टवेयर का उपयोग करें।
4. डेटा का बैकअप लें: सुरक्षा भंग की स्थिति में डेटा के नुकसान को रोकने के लिए नियमित रूप से डेटा का बैकअप लें।

लाभ:

1. सुधारित सुरक्षा: अपडेट्स और ऐप अनुमतियाँ ज्ञात कमजोरियों और मैलवेयर से बचाव में मदद कर सकती हैं।
2. डेटा सुरक्षा: अपडेट्स और ऐप अनुमतियाँ आपके व्यक्तिगत डेटा को अनधिकृत पहुंच से बचा सकती हैं।

3. मन की शांति: अद्यतन रहकर और ऐप अनुमतियों को नियंत्रित करके, आप अपने डिवाइस और डेटा की सुरक्षा के बारे में सुनिश्चित हो सकते हैं।

Device Lock in Essential Mobile and Computer Safety:

Why Device Lock is Important:

1. Protects personal data: Device lock helps protect your personal data, such as contacts, photos, and messages, from unauthorized access.
2. Prevents theft and loss: Device lock can help prevent theft and loss of your device, and make it harder for others to access your data.
3. Secures sensitive information: Device lock can help secure sensitive information, such as financial data and login credentials.

Types of Device Locks:

1. PIN or password lock: A numeric PIN or password lock can be used to secure your device.
2. Biometric lock: Biometric locks, such as fingerprint or facial recognition, can provide an additional layer of security.
3. Pattern lock: A pattern lock can be used to secure your device, but it may not be as secure as a PIN or password lock.

Best Practices:

1. Use a strong PIN or password: Use a strong and unique PIN or password to secure your device.
2. Enable biometric lock: Enable biometric lock, such as fingerprint or facial recognition, for added security.
3. Lock your device when not in use: Lock your device when not in use to prevent unauthorized access.
4. Use device encryption: Use device encryption to protect your data, even if your device is lost or stolen.

Benefits:

1. Improved security: Device lock can help protect your personal data and prevent unauthorized access.
2. Peace of mind: Knowing that your device is secure can give you peace of mind, especially if you store sensitive information on it.
3. Protection against theft and loss: Device lock can help protect your device against theft and loss, and make it harder for others to access your data.

डिवाइस लॉक मोबाइल और कंप्यूटर सुरक्षा में:

डिवाइस लॉक क्यों महत्वपूर्ण है:

1. व्यक्तिगत डेटा की सुरक्षा: डिवाइस लॉक आपके व्यक्तिगत डेटा, जैसे कि संपर्क, फ़ोटो और संदेशों को अनधिकृत पहुंच से बचाता है।
2. चोरी और नुकसान से बचाव: डिवाइस लॉक आपके डिवाइस को चोरी और नुकसान से बचा सकता है, और दूसरों के लिए आपके डेटा तक पहुंचना मुश्किल बना सकता है।
3. संवेदनशील जानकारी की सुरक्षा: डिवाइस लॉक संवेदनशील जानकारी, जैसे कि वित्तीय डेटा और लॉगिन क्रेडेंशियल्स को सुरक्षित रखता है।

डिवाइस लॉक के प्रकार:

1. पिन या पासवर्ड लॉक: एक संख्यात्मक पिन या पासवर्ड लॉक आपके डिवाइस को सुरक्षित कर सकता है।
2. बायोमेट्रिक लॉक: बायोमेट्रिक लॉक, जैसे कि फिंगरप्रिंट या फेसियल रिकग्निशन, अतिरिक्त सुरक्षा प्रदान कर सकते हैं।
3. पैटर्न लॉक: एक पैटर्न लॉक आपके डिवाइस को सुरक्षित कर सकता है, लेकिन यह पिन या पासवर्ड लॉक जितना सुरक्षित नहीं हो सकता है।

सर्वोत्तम अभ्यास:

1. मजबूत पिन या पासवर्ड का उपयोग करें: अपने डिवाइस को सुरक्षित करने के लिए एक मजबूत और अद्वितीय पिन या पासवर्ड का उपयोग करें।
2. बायोमेट्रिक लॉक सक्षम करें: अतिरिक्त सुरक्षा के लिए बायोमेट्रिक लॉक, जैसे कि फिंगरप्रिंट या फेसियल रिकग्निशन, सक्षम करें।
3. डिवाइस को निष्क्रिय होने पर लॉक करें: अनधिकृत पहुंच को रोकने के लिए अपने डिवाइस को निष्क्रिय होने पर लॉक करें।
4. डिवाइस एन्क्रिप्शन का उपयोग करें: अपने डेटा को सुरक्षित करने के लिए डिवाइस एन्क्रिप्शन का उपयोग करें, भले ही आपका डिवाइस खो जाए या चोरी हो जाए।

लाभ:

1. सुधारित सुरक्षा: डिवाइस लॉक आपके व्यक्तिगत डेटा की सुरक्षा में सुधार कर सकता है और अनधिकृत पहुंच को रोक सकता है।
2. मन की शांति: यह जानना कि आपका डिवाइस सुरक्षित है, आपको मानसिक शांति प्रदान कर सकता है, खासकर यदि आप उस पर संवेदनशील जानकारी संग्रहीत करते हैं।
3. चोरी और नुकसान से बचाव: डिवाइस लॉक आपके डिवाइस को चोरी और नुकसान से बचा सकता है, और दूसरों के लिए आपके डेटा तक पहुंचना मुश्किल बना सकता है।

Social Media Safety:

Social media safety refers to the practices and guidelines that help individuals protect their personal information, security, and well-being while using social media platforms. Here are some key aspects of social media safety:

Personal Safety:

1. Use strong passwords: Use unique and strong passwords for each social media account.
2. Be cautious with personal info: Avoid sharing sensitive personal information, such as address, phone number, or financial details.
3. Set boundaries: Set boundaries for what you share online and with whom.

Online Etiquette:

1. Be respectful: Treat others with respect and kindness online.
2. Avoid cyberbullying: Refrain from engaging in or encouraging cyberbullying.
3. Verify information: Verify the accuracy of information before sharing it.

Security:

1. Use two-factor authentication: Enable two-factor authentication to add an extra layer of security.
2. Keep software up-to-date: Keep your device and social media apps up-to-date with the latest security patches.
3. Be cautious of phishing: Be cautious of suspicious messages or links that may be phishing attempts.

Reputation Management:

1. Post thoughtfully: Think before you post, and consider how your content may be perceived.
2. Monitor your online presence: Regularly search for your name and monitor your online presence.
3. Report inappropriate content: Report any inappropriate or harassing content.

Additional Tips:

1. Use social media platforms' built-in features: Familiarize yourself with social media platforms' built-in features, such as blocking and reporting.
2. Be mindful of online relationships: Be cautious when interacting with people you don't know online.
3. Take breaks: Take breaks from social media to maintain a healthy online-offline balance.

सोशल मीडिया सुरक्षा:

सोशल मीडिया सुरक्षा से तात्पर्य उन प्रथाओं और दिशानिर्देशों से है जो व्यक्तियों को सोशल मीडिया प्लेटफॉर्म का उपयोग करते समय अपनी व्यक्तिगत जानकारी, सुरक्षा और कल्याण की रक्षा करने में मदद करते हैं।

व्यक्तिगत सुरक्षा:

1. मजबूत पासवर्ड का उपयोग करें: प्रत्येक सोशल मीडिया खाते के लिए अद्वितीय और मजबूत पासवर्ड का उपयोग करें।
2. व्यक्तिगत जानकारी के साथ सावधानी बरतें: संवेदनशील व्यक्तिगत जानकारी, जैसे कि पता, फोन नंबर या वित्तीय विवरण साझा करने से बचें।
3. सीमाएँ निर्धारित करें: ऑनलाइन साझा करने और किसके साथ साझा करने के बारे में सीमाएँ निर्धारित करें।

ऑनलाइन शिष्टाचार:

1. आदरपूर्ण रहें: ऑनलाइन दूसरों के साथ आदरपूर्ण और दयालु व्यवहार करें।
2. साइबरबुलिंग से बचें: साइबरबुलिंग में शामिल होने या प्रोत्साहित करने से बचें।
3. जानकारी की पुष्टि करें: जानकारी साझा करने से पहले उसकी पुष्टि करें।

सुरक्षा:

1. दो-कारक प्रमाणीकरण का उपयोग करें: अतिरिक्त सुरक्षा के लिए दो-कारक प्रमाणीकरण सक्षम करें।
2. सॉफ़्टवेयर अद्यतन रखें: अपने डिवाइस और सोशल मीडिया ऐप्स को नवीनतम सुरक्षा पैच के साथ अद्यतन रखें।
3. फ़िशिंग से सावधान रहें: संदिग्ध संदेशों या लिंक से सावधान रहें जो फ़िशिंग के प्रयास हो सकते हैं।

प्रतिष्ठा प्रबंधन:

1. विचारपूर्वक पोस्ट करें: पोस्ट करने से पहले सोचें और विचार करें कि आपका कंटेंट कैसे माना जा सकता है।
2. अपनी ऑनलाइन उपस्थिति की निगरानी करें: नियमित रूप से अपना नाम खोजें और अपनी ऑनलाइन उपस्थिति की निगरानी करें।
3. अनुचित सामग्री की रिपोर्ट करें: अनुचित या उत्पीड़न सामग्री की रिपोर्ट करें।

अतिरिक्त सुझाव:

1. सोशल मीडिया प्लेटफ़ॉर्म की अंतर्निहित सुविधाओं का उपयोग करें: सोशल मीडिया प्लेटफ़ॉर्म की अंतर्निहित सुविधाओं, जैसे कि ब्लॉकिंग और रिपोर्टिंग से परिचित हों।
2. ऑनलाइन संबंधों के प्रति सावधान रहें: ऑनलाइन अज्ञात लोगों के साथ बातचीत करते समय सावधान रहें।
3. विराम लें: स्वस्थ ऑनलाइन-ऑफ़लाइन संतुलन बनाए रखने के लिए सोशल मीडिया से विराम लें।

Avoiding Public Wi-Fi for Device Safety:

Risks of Public Wi-Fi:

1. Data theft: Public Wi-Fi networks can be vulnerable to hacking, allowing thieves to steal sensitive information.
2. Malware and viruses: Public Wi-Fi networks can be used to spread malware and viruses.
3. Man-in-the-middle attacks: Hackers can intercept communication between your device and the public Wi-Fi network.

Tips to Stay Safe:

1. Use a VPN: A Virtual Private Network (VPN) can encrypt your internet traffic, making it more secure.
2. Avoid sensitive activities: Avoid accessing sensitive information, such as online banking or personal data, on public Wi-Fi.
3. Use two-factor authentication: Enable two-factor authentication to add an extra layer of security.
4. Keep your device and software up-to-date: Ensure your device and software are updated with the latest security patches.
5. Use a mobile hotspot: Consider using a mobile hotspot instead of public Wi-Fi.

Alternatives to Public Wi-Fi:

1. Mobile data: Use your mobile data plan instead of public Wi-Fi.
2. Private Wi-Fi networks: Use private Wi-Fi networks, such as those provided by your employer or a trusted organization.
3. VPN-enabled Wi-Fi: Use Wi-Fi networks that require a VPN connection.

Best Practices:

1. Be cautious of public Wi-Fi: Be aware of the risks associated with public Wi-Fi and take necessary precautions.
2. Use security software: Install and regularly update security software on your device.
3. Monitor your accounts: Regularly monitor your accounts for suspicious activity.

सार्वजनिक वाई-फाई से बचने के लिए डिवाइस सुरक्षा:

सार्वजनिक वाई-फाई के जोखिम:

1. डेटा चोरी: सार्वजनिक वाई-फाई नेटवर्क हैकिंग के प्रति संवेदनशील हो सकते हैं, जिससे चोर संवेदनशील जानकारी चुरा सकते हैं।
2. मैलवेयर और वायरस: सार्वजनिक वाई-फाई नेटवर्क का उपयोग मैलवेयर और वायरस फैलाने के लिए किया जा सकता है।
3. मैन-इन-द-मिडल हमले: हैकर आपके डिवाइस और सार्वजनिक वाई-फाई नेटवर्क के बीच संचार को बाधित कर सकते हैं।

सुरक्षित रहने के लिए सुझाव:

1. वीपीएन का उपयोग करें: एक वर्चुअल प्राइवेट नेटवर्क (वीपीएन) आपके इंटरनेट ट्रैफिक को एन्क्रिप्ट कर सकता है, जिससे यह अधिक सुरक्षित हो जाता है।
2. संवेदनशील गतिविधियों से बचें: सार्वजनिक वाई-फाई पर ऑनलाइन बैंकिंग या व्यक्तिगत डेटा जैसी संवेदनशील जानकारी तक पहुंचने से बचें।
3. दो-कारक प्रमाणीकरण का उपयोग करें: अतिरिक्त सुरक्षा के लिए दो-कारक प्रमाणीकरण सक्षम करें।
4. अपने डिवाइस और सॉफ़्टवेयर को अद्यतन रखें: सुनिश्चित करें कि आपके डिवाइस और सॉफ़्टवेयर नवीनतम सुरक्षा पैच के साथ अद्यतन हैं।
5. मोबाइल हॉटस्पॉट का उपयोग करें: सार्वजनिक वाई-फाई के बजाय मोबाइल हॉटस्पॉट का उपयोग करने पर विचार करें।

सार्वजनिक वाई-फाई के विकल्प:

1. मोबाइल डेटा: सार्वजनिक वाई-फाई के बजाय अपने मोबाइल डेटा प्लान का उपयोग करें।
2. निजी वाई-फाई नेटवर्क: निजी वाई-फाई नेटवर्क का उपयोग करें, जैसे कि आपके नियोक्ता या एक विश्वसनीय संगठन द्वारा प्रदान किए गए।
3. वीपीएन-सक्षम वाई-फाई: वाई-फाई नेटवर्क का उपयोग करें जिनके लिए वीपीएन कनेक्शन की आवश्यकता होती है।

सर्वोत्तम अभ्यास:

1. सार्वजनिक वाई-फाई के प्रति सावधान रहें: सार्वजनिक वाई-फाई से जुड़े जोखिमों से अवगत रहें और आवश्यक सावधानियां बरतें।
2. सुरक्षा सॉफ़्टवेयर का उपयोग करें: अपने डिवाइस पर सुरक्षा सॉफ़्टवेयर स्थापित करें और नियमित रूप से अद्यतन करें।
3. अपने खातों की निगरानी करें: नियमित रूप से अपने खातों की निगरानी करें और संदिग्ध गतिविधि की जांच करें।

Risks of Public Wi-Fi:

1. Data Theft: Public Wi-Fi networks can be vulnerable to hacking, allowing thieves to steal sensitive information such as login credentials, credit card numbers, and personal data.

2. Malware and Viruses: Public Wi-Fi networks can be used to spread malware and viruses, which can infect your device and compromise your data.

3. Man-in-the-Middle (MitM) Attacks: Hackers can intercept communication between your device and the public Wi-Fi network, allowing them to steal sensitive information or inject malware.

4. Sniffing: Hacking**: Hackers can intercept unencrypted data, including login credentials, financial information, and other sensitive data.

5. Identity Theft: Public Wi-Fi networks can be used to steal personal data, which can be used for identity theft.

6. Malicious Hotspots: Some public Wi-Fi networks may be set up by hackers to steal sensitive information or inject malware.

7. Unencrypted Data: Public Wi-Fi networks often don't encrypt data, making it easier for hackers to intercept sensitive information.

8. Session Hijacking: Hackers can hijack your online sessions, allowing them to access your accounts and steal sensitive information.

Protect Yourself:

1. Use a VPN: A Virtual Private Network (VPN) can encrypt your internet traffic, making it more secure.

2. Use strong passwords: Use strong, unique passwords for all accounts.

3. Keep your device and software up-to-date: Ensure your device and software are updated with the latest security patches.

4. Use two-factor authentication: Enable two-factor authentication to add an extra layer of security.

5. Be cautious of public Wi-Fi: Be aware of the risks associated with public Wi-Fi and take necessary precautions.

सार्वजनिक वाई-फाई से बचाव के लिए डिवाइस सुरक्षा

सार्वजनिक वाई-फाई नेटवर्क का उपयोग करते समय अपनी डिवाइस और डेटा की सुरक्षा के लिए कुछ सावधानियां बरतनी चाहिए। यहाँ कुछ सुझाव दिए गए हैं:

सावधानियां

1. वीपीएन का उपयोग करें: एक वर्चुअल प्राइवेट नेटवर्क (वीपीएन) आपके इंटरनेट ट्रैफिक को एन्क्रिप्ट कर सकता है, जिससे यह अधिक सुरक्षित हो जाता है।
2. संवेदनशील जानकारी से बचें : सार्वजनिक वाई-फाई पर संवेदनशील जानकारी तक पहुंचने से बचें, जैसे कि ऑनलाइन बैंकिंग या व्यक्तिगत डेटा।
3. दो-कारक प्रमाणीकरण सक्षम करें: अतिरिक्त सुरक्षा के लिए दो-कारक प्रमाणीकरण सक्षम करें।
4. अपने डिवाइस और सॉफ़्टवेयर को अद्यतन रखें: सुनिश्चित करें कि आपके डिवाइस और सॉफ़्टवेयर नवीनतम सुरक्षा पैच के साथ अद्यतन हैं।

सुरक्षित ब्राउज़िंग

1. HTTPS का उपयोग करें: वेबसाइटों पर जाने के लिए HTTPS का उपयोग करें, जो एक सुरक्षित कनेक्शन प्रदान करता है।
2. संदिग्ध लिंक से बचें: संदिग्ध लिंक पर क्लिक करने से बचें, जो मैलवेयर या फ़िशिंग स्कैम हो सकते हैं।

वैकल्पिक विकल्प

1. मोबाइल डेटा का उपयोग करें: सार्वजनिक वाई-फाई के बजाय अपने मोबाइल डेटा प्लान का उपयोग करें।
2. निजी वाई-फाई नेटवर्क का उपयोग करें: निजी वाई-फाई नेटवर्क का उपयोग करें, जैसे कि आपके नियोक्ता या एक विश्वसनीय संगठन द्वारा प्रदान किए गए।

निष्कर्ष

सार्वजनिक वाई-फाई नेटवर्क का उपयोग करते समय सावधानी बरतना महत्वपूर्ण है। वीपीएन का उपयोग करके, संवेदनशील जानकारी से बचकर, और अपने डिवाइस और सॉफ़्टवेयर को अद्यतन रखकर, आप अपने डेटा और डिवाइस की सुरक्षा में मदद कर सकते हैं।

Unit 3: Online Scams and Frauds

Online Scams:

Online scams are fraudulent activities that occur on the internet, where scammers deceive and manipulate individuals into revealing sensitive information, sending money, or providing access to their devices or accounts. Here are some common types of online scams:

Types of Online Scams:

1. Job Offer Scams

Scammers fool job seekers with fake postings on real job boards. They offer high pay for easy work but just want personal details or money for identity theft and financial crimes.

How To Avoid: Check job postings carefully, research companies, and don't send money or details upfront. Report suspected scam listings to job sites with fraud detection.

2. Lottery Scams

Lottery scams try to make people think they've won a lottery or sweepstakes that isn't real. People get emails, letters, or calls saying they've won lots of money or prizes. But to get the winnings, they have to pay fees for taxes, processing, or delivery. They never get that money back.

How To Avoid: Don't respond if someone says you've won a prize, especially if you didn't enter a contest. Real lotteries don't make winners pay fees first. Don't give personal info or send money to anyone claiming to be from a lottery. Check if a lottery or sweepstakes is real before doing anything. Official lottery organizations contact real winners directly, not through random messages.

3. Beneficiary Scams

Beneficiary scams are when criminals trick victims into thinking they have inherited from a far away relative who requires either their payment details or personal information to claim it.

How To Avoid: Be skeptical of unexpected inheritance claims. Verify estates independently and consult legal professionals without paying fees upfront.

4. Online Dating Scams

Online dating scammers use fake profiles on dating sites and apps. They start relationships but later ask for cash with made-up stories about emergencies or travel costs. Online dating fraud tricks people who want partners.

How To Avoid: Be cautious online and wary if talks quickly move off dating platforms. Never send money or give financial info to people you haven't met in person. Use reverse image searches to check profile pictures.

5. Charity Fraud Scams

Some scams try to get money from kind people. They say they need cash for pretend groups or events. This often happens during times like disasters and holidays when people feel like helping out. These fraudsters take advantage of people's emotions to steal money.

How To Avoid: Before giving money, look up charities online to make sure they are real. Use trusted sites to check if they are legitimate groups. Be careful if someone you don't know asks for cash. Real charities share clear info about themselves. Don't send cash; use checks or credit cards so you have records. If someone pressures you to give money right away, that's a red flag. Take your time to know about groups before donating.

6. Repair Scams

Repair scams involve people or businesses offering to fix your home or computer without you asking first. They say they noticed an issue that needs to get fixed immediately. But these crooks often do low-quality work or repairs that aren't needed at all. And they overcharge for the bad service.

How To Avoid: Getting an estimate is important before hiring someone to fix something. Don't just hire the first person who offers. That's risky. Ask around and get multiple estimates from different businesses. Check that they have good reviews and references. Only pay after the work is done, using safe payment methods.

Never pay before work starts. People going door-to-door must show ID and licenses. Legitimate businesses won't pressure you to decide or pay immediately.

7. Social Media Scams

Social media scams spread fraudulent schemes through platforms like Facebook, Twitter, and Instagram. They include fake advertisements, cloned profiles, and phishing links, leading to financial loss and identity theft.

How To Avoid: Privacy settings help block strangers from seeing personal details, photos, posts, etc. Don't accept friend requests from people you don't know, even if they seem real. Duplicates could be scammers. Verify any offers or information before clicking links or entering info. Set strong, unique passwords for each account and enable two-factor authentication. Report suspicious accounts and activities to the platforms. Stay updated on new scam tactics being used.

8. Robocall Scams

Automated robocalls deliver fraudulent messages, often posing as official agencies to solicit personal information or payments.

How To Avoid: End unsolicited robocalls asking for personal details or money. Avoid pressing buttons during such calls and register with the Do Not Call Registry. Use call-blocking tools and verify claims through official contacts.

9. Messaging Scams

Scammers send fraudulent SMS, emails, or app messages with phishing links or false promises to extract personal information.

How To Avoid: Ignore links or attachments from unknown sources. Stay alert to urgent or too-good-to-be-true messages. Confirm the sender's identity through official means, use spam filters, and learn to recognize scam signs.

10. Online Shopping Scams

Online shopping scams involve fake online stores or sellers that offer products at significantly lower prices. These stores may deliver counterfeit goods, inferior products, or nothing at all.

How To Avoid: Use well-known websites with secure payments, read reviews, and be wary of wire transfers or gift card payments. Confirm the site's legitimacy and use credit cards for fraud protection. Document purchases and be skeptical of deals that seem unreal.

Some another online Scame

- Phishing Scams: Scammers send fake emails, messages, or create websites that appear to be from legitimate companies, asking for sensitive information such as login credentials, credit card numbers, or personal data.
- Online Auction Scams: Scammers create fake online auctions, where they promise to sell products or services that don't exist or are not as described.
- Romance Scams: Scammers create fake profiles on dating websites or social media, build relationships with victims, and ask for money or gifts.
- Investment Scams: Scammers promise unusually high returns on investments, such as stocks, real estate, or cryptocurrencies, but the investments are often fake or unsound.
- Lottery Scams: Scammers claim that the victim has won a lottery or contest, but to claim the prize, they need to pay a fee or provide sensitive information.
- Identity Theft Scams: Scammers steal personal data, such as social security numbers, credit card numbers, or driver's licenses, to commit identity theft.
- Malware Scams: Scammers distribute malware, such as viruses, trojans, or ransomware, to gain unauthorized access to devices or data.

8. Fake Job Scams: Scammers create fake job postings or offer employment opportunities that require upfront payments or sensitive information.

How to Protect Yourself:

1. Be cautious of suspicious emails and messages: Look for spelling and grammar mistakes, and verify the sender's identity.

2. Use strong passwords and 2FA: Protect your accounts with strong, unique passwords and enable two-factor authentication.

3. Verify websites and companies: Research the company and check for reviews, ratings, and contact information.

4. Don't send money to strangers: Be wary of requests for money, especially from people you've never met.

5. Keep your software and devices up-to-date: Regularly update your operating system, browser, and antivirus software.

What to Do If You're Scammed:

1. Report the scam: File a complaint with the relevant authorities, such as the Federal Trade Commission (FTC) or your local police department.

2. Contact your bank and credit card companies: Inform them of the scam and request that they monitor your accounts for suspicious activity.

3. Change your passwords: Update your passwords and enable two-factor authentication to prevent further unauthorized access.

By being aware of these online scams and taking necessary precautions, you can protect yourself and your sensitive information.

Cyber Fraud:

Internet scams involve illegal activities done through the web. They use the anonymity, convenience, and global reach of the internet for criminal activities. Cyber fraud covers many illegal practices aiming to take advantage of online opportunities dishonestly.

Cyber fraud refers to any type of fraudulent activity that occurs online or uses digital technologies to deceive and exploit individuals or organizations. Here are some common types of cyber fraud:

Types of Cyber Fraud:

1. Identity Theft: Stealing personal data, such as social security numbers, credit card numbers, or login credentials, to commit fraud or other crimes.

2. Phishing: Using fake emails, messages, or websites to trick individuals into revealing sensitive information or installing malware.

3. Online Auction Fraud: Selling fake or non-existent products or services online, often through auction sites or social media.

4. Credit Card Fraud: Using stolen credit card information to make unauthorized transactions or purchases.

5. Investment Scams: Promising unusually high returns on investments, such as stocks, real estate, or cryptocurrencies, but the investments are often fake or unsound.

6. Romance Scams: Building relationships with individuals online to gain their trust and extract money or sensitive information.

7. Business Email Compromise (BEC): Hacking into business email accounts to steal sensitive information or initiate unauthorized transactions.

8. Ransomware: Encrypting data and demanding payment in exchange for the decryption key.

9. Online Job Scams: Posting fake job ads or offering employment opportunities that require upfront payments or sensitive information.

How to Protect Yourself:

1. Use strong passwords and 2FA: Protect your accounts with strong, unique passwords and enable two-factor authentication.

2. Be cautious of suspicious emails and messages: Look for spelling and grammar mistakes, and verify the sender's identity.

3. Verify websites and companies: Research the company and check for reviews, ratings, and contact information.

4. Keep your software and devices up-to-date: Regularly update your operating system, browser, and antivirus software.

5. Monitor your accounts and credit reports: Regularly check your accounts and credit reports for suspicious activity.

What to Do If You're a Victim:

1. Report the incident: File a complaint with the relevant authorities, such as the Federal Trade Commission (FTC) or your local police department.

2. Contact your bank and credit card companies: Inform them of the incident and request that they monitor your accounts for suspicious activity.

3. Change your passwords: Update your passwords and enable the two-factor authentication to prevent further unauthorized access.

4. Seek support: Reach out to friends, family, or a professional counselor for support and guidance.

By being aware of these types of cyber fraud and taking necessary precautions, you can protect yourself and your sensitive information.

Protecting Yourself from Online Scams and Cyber Fraud

Here are some effective ways to protect yourself from online scams and cyber fraud:

Precautions:

1. Use strong passwords: Use unique and complex passwords for all online accounts.

2. Enable two-factor authentication: Add an extra layer of security to your accounts with two-factor authentication.

3. Be cautious of suspicious emails and links: Avoid clicking on links or providing sensitive information in response to unsolicited emails.

4. Verify websites: Research the website and check for reviews, ratings, and contact information before making online transactions.

Security Software:

1. Antivirus software: Install and regularly update antivirus software to protect against malware and viruses.

2. Firewall: Enable the firewall on your device to block unauthorized access.

Protecting Personal Information:

1. Don't share personal info: Avoid sharing sensitive information online, especially on social media or with unknown individuals.

2. Use secure connections: Ensure that the website uses HTTPS (SSL/TLS) encryption when entering sensitive information.

Reporting and Response:

1. Report scams: If you suspect you've been scammed, report it to the relevant authorities immediately.

2. Notify your bank and credit card companies: Inform your bank and credit card companies of any suspicious activity and request that they monitor your accounts.

How to Prevent Fraud?

1. Guard Your Passwords

Treat your passwords like prized keys. Avoid predictable options like birthdays or pet names, opting for a complex mix of letters, numbers, and symbols.

2. Watch Out for Calls

Be wary of unsolicited calls, emails, and texts, especially those offering "too-good-to-be-true" deals. Phishing schemes are common.

3. Secure Your System

Update your software regularly, from your operating system to your apps. These updates often patch security vulnerabilities, making your digital walls harder to breach.

4. Monthly Bank Reconciliation Procedures

Require reconciliation by an independent person without bookkeeping or check signing responsibilities or ensure supervisory review.

5. Be alert, not alarmed

Knowledge is power! Stay informed about common fraud tactics and scams circulating online. Awareness empowers you to identify suspicious activity and avoid falling victim.

6. Trust but Verify

When shopping online, stick to reputable websites with established reviews. Look for security badges and encryption protocols that indicate secure transactions.

7. Lock Down Your Finances

Monitor your bank accounts and credit reports regularly. Spotting unauthorized activity early can help minimize damage and prevent further losses.

8. Spread the Word

Share your knowledge! Educating your friends, family, and colleagues about fraud prevention tactics creates a safer digital community for everyone.

Common Types of Online Scams:

1. Phishing Scams: Scammers send fake emails, messages, or create websites that appear to be from legitimate companies, asking for sensitive information such as login credentials, credit card numbers, or personal data.

2. Online Auction Scams: Scammers create fake online auctions, where they promise to sell products or services that don't exist or are not as described.

3. Romance Scams: Scammers create fake profiles on dating websites or social media, build relationships with victims, and ask for money or gifts.

4. Investment Scams: Scammers promise unusually high returns on investments, such as stocks, real estate, or cryptocurrencies, but the investments are often fake or unsound.

5. Lottery Scams: Scammers claim that the victim has won a lottery or contest, but to claim the prize, they need to pay a fee or provide sensitive information.

6. Identity Theft Scams: Scammers steal personal data, such as social security numbers, credit card numbers, or driver's licenses, to commit identity theft.

7. Malware Scams: Scammers distribute malware, such as viruses, trojans, or ransomware, to gain unauthorized access to devices or data.

8. Fake Job Scams: Scammers create fake job postings or offer employment opportunities that require upfront payments or sensitive information.

9. Cryptocurrency Scams: Scammers promise unusually high returns on cryptocurrency investments or offer fake cryptocurrency giveaways.

10. Social Media Scams: Scammers use social media platforms to spread malware, steal personal data, or conduct phishing attacks.

How to Protect Yourself:

1. Be cautious of suspicious emails and messages: Look for spelling and grammar mistakes, and verify the sender's identity.

2. Use strong passwords and 2FA: Protect your accounts with strong, unique passwords and enable two-factor authentication.

3. Verify websites and companies: Research the company and check for reviews, ratings, and contact information.

4. Keep your software and devices up-to-date: Regularly update your operating system, browser, and antivirus software.

Tricks Used by Fraudsters:

1. Phishing: Fraudsters send fake emails, messages, or create websites that appear to be from legitimate companies, asking for sensitive information.

2. Social Engineering: Fraudsters use psychological manipulation to trick people into revealing sensitive information or performing certain actions.

3. Pretexting: Fraudsters create a fake scenario or story to gain the trust of their victims and obtain sensitive information.

4. Baiting: Fraudsters offer something of value, such as a free gift or service, to lure victims into providing sensitive information.

5. Malware: Fraudsters use malware to gain unauthorized access to devices or data.

6. Identity Theft: Fraudsters steal personal data, such as social security numbers or credit card numbers, to commit identity theft.

7. Fake Websites: Fraudsters create fake websites that appear to be legitimate, but are designed to steal sensitive information.

8. Urgency: Fraudsters create a sense of urgency, such as claiming that an account will be closed or a limited-time offer will expire, to pressure victims into taking action.

How to Protect Yourself:

1. Be cautious of suspicious emails and messages: Look for spelling and grammar mistakes, and verify the sender's identity.

2. Use strong passwords and 2FA: Protect your accounts with strong, unique passwords and enable two-factor authentication.

3. Verify websites and companies: Research the company and check for reviews, ratings, and contact information.

4. Keep your software and devices up-to-date: Regularly update your operating system, browser, and antivirus software.

5. Monitor your accounts and credit reports: Regularly check your accounts and credit reports for suspicious activity.

By being aware of these tricks and taking necessary precautions, you can protect yourself and your sensitive information.

How to Identify and Avoid Online Scams:

Red Flags:

1. Urgent or threatening messages: Scammers often create a sense of urgency or threaten consequences if you don't act immediately.

2. Suspicious emails or messages: Look for spelling and grammar mistakes, generic greetings, and unfamiliar senders.

3. Too good to be true offers: If an offer seems too good to be true, it probably is.

4. Requests for sensitive information: Legitimate companies will never ask for sensitive information, such as passwords or financial information, via email or text.

Prevention:

1. Verify sender information: Check the sender's email address or phone number to ensure it's legitimate.

2. Use strong passwords: Use unique and complex passwords for all online accounts.

3. Enable two-factor authentication: Add an extra layer of security to your accounts with two-factor authentication.

4. Keep software up-to-date: Regularly update your operating system, browser, and antivirus software.

Avoid:

1. Suspicious links: Avoid clicking on links from unfamiliar senders or websites.

2. Unknown attachments: Don't open attachments from unfamiliar senders or websites.

3. Public Wi-Fi: Avoid using public Wi-Fi for sensitive transactions.

What to Do If You're Scammed:

1. Report the scam: File a complaint with the relevant authorities, such as the Federal Trade Commission (FTC).

2. Contact your bank: Inform your bank and credit card companies of any suspicious activity.

3. Change your passwords: Update your passwords and enable two-factor authentication.

How to Identify Online Scams:

1. Check the URL: Scammers often use fake websites with URLs that are similar to legitimate ones. Look for "https" and a lock icon in the address bar.

2. Be cautious of emails: Scammers often send fake emails that appear to be from legitimate companies. Look for spelling and grammar mistakes, and verify the sender's email address.

3. Watch for red flags: Be wary of requests for sensitive information, such as passwords, financial information, or personal data.

4. Check for reviews: Research the company and read reviews from other customers to see if they have a good reputation.

5. Be skeptical of unsolicited offers: If you didn't ask for an offer, be cautious of responding to it.

6. Verify the company's contact information: Check if the company has a physical address and a working phone number.

7. Be cautious of pop-ups: Be wary of pop-ups that ask you to download software or provide sensitive information.

8. Use antivirus software: Install and regularly update antivirus software to protect your device from malware.

Common Online Scam Tactics:

1. Phishing: Scammers send fake emails or messages that appear to be from legitimate companies.

2. Malware: Scammers use malware to gain unauthorized access to devices or data.

3. Identity theft: Scammers steal personal data to commit identity theft.

4. Online auctions: Scammers create fake online auctions to steal money or goods.

What to Do If You're Scammed:

1. Report the scam: File a complaint with the relevant authorities.

2. Contact your bank: Inform your bank and credit card companies of any suspicious activity.

3. Change your passwords: Update your passwords and enable two-factor authentication.

How to Avoid Online Scams:

1. Be cautious of suspicious emails and messages: Don't click on links or provide sensitive information in response to unsolicited emails or messages.

2. Verify the authenticity of websites: Check the URL and look for "https" and a lock icon in the address bar.

3. Use strong passwords: Use unique and complex passwords for all online accounts.

4. Enable two-factor authentication: Add an extra layer of security to your accounts with two-factor authentication.

5. Keep software up-to-date: Regularly update your operating system, browser, and antivirus software.

6. Use antivirus software: Install and regularly update antivirus software to protect your device from malware.

7. Be wary of public Wi-Fi: Avoid using public Wi-Fi for sensitive transactions.

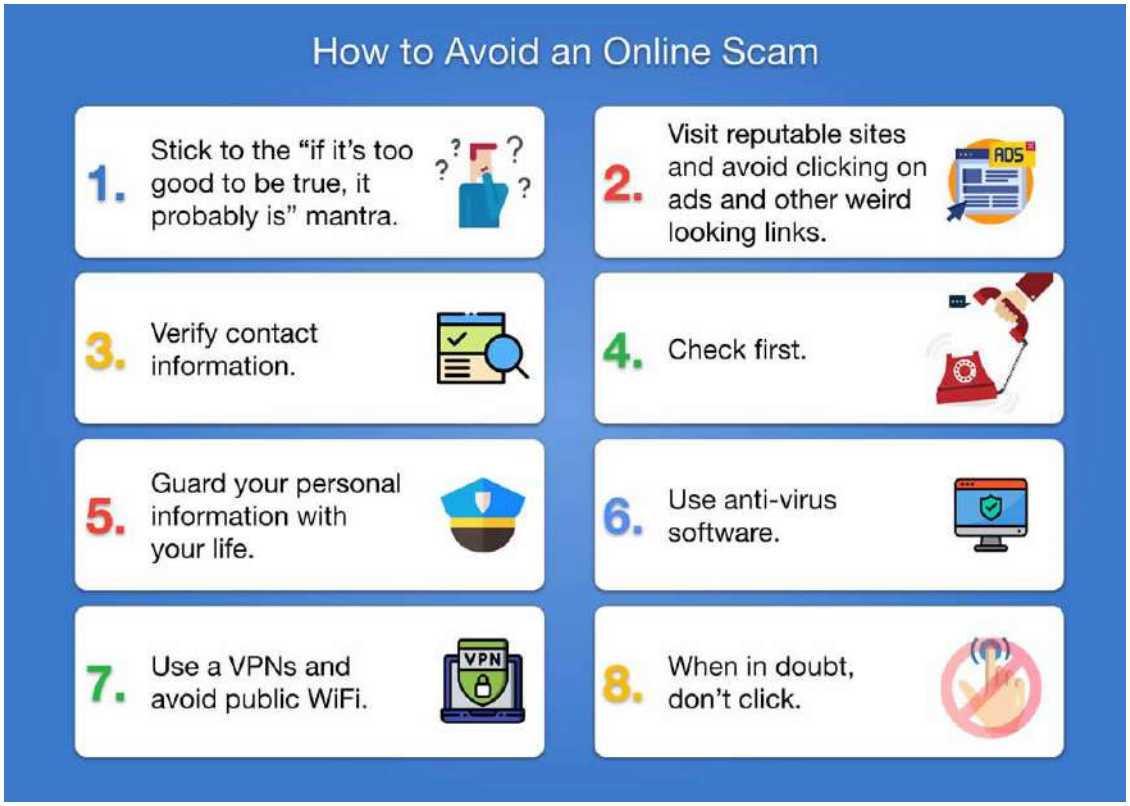
8. Monitor your accounts: Regularly check your accounts and credit reports for suspicious activity.

Additional Tips:

1. Use a VPN: Consider using a virtual private network (VPN) to encrypt your internet traffic.

2. Use a password manager: Consider using a password manager to generate and store unique passwords.

3. Back up your data: Regularly back up your important data to prevent losses in case of a scam or attack.



ऑनलाइन स्कैम:

ऑनलाइन स्कैम इंटरनेट पर होने वाली धोखाधड़ी गतिविधियाँ हैं, जहाँ स्कैमर्स व्यक्तियों को धोखा देकर संवेदनशील जानकारी प्रकट करने, पैसे भेजने या अपने डिवाइस या खातों तक पहुँच प्रदान करने के लिए मजबूर करते हैं।

ऑनलाइन स्कैम के प्रकार:

1. फ़िशिंग स्कैम: स्कैमर्स नकली ईमेल, संदेश या वेबसाइट बनाते हैं जो वैध कंपनियों से होने का दिखावा करते हैं, संवेदनशील जानकारी मांगते हैं।

2. ऑनलाइन नीलामी स्कैम: स्कैमर्स नकली ऑनलाइन नीलामी बनाते हैं, जहाँ वे उत्पादों या सेवाओं को बेचने का वादा करते हैं जो मौजूद नहीं हैं या जैसा बताया गया है वैसा नहीं हैं।

3. रोमांस स्कैम: स्कैमर्स डेटिंग वेबसाइटों या सोशल मीडिया पर नकली प्रोफाइल बनाते हैं, पीड़ितों के साथ संबंध बनाते हैं और पैसे या उपहार मांगते हैं।

4. निवेश स्कैम: स्कैमर्स असामान्य रूप से उच्च रिटर्न का वादा करते हैं, लेकिन निवेश अक्सर नकली या अस्थिर होते हैं।

अपनी सुरक्षा के लिए:

1. संदिग्ध ईमेल और संदेशों से सावधान रहें: वर्तनी और व्याकरण की गलतियों को देखें और प्रेषक की पहचान सत्यापित करें।

2. मजबूत पासवर्ड और 2FA का उपयोग करें: अपने खातों को मजबूत, अद्वितीय पासवर्ड और दो-कारक प्रमाणीकरण के साथ सुरक्षित करें।

3. वेबसाइटों और कंपनियों की सत्यता जांचें: कंपनी के बारे में शोध करें और समीक्षाएं, रेटिंग और संपर्क जानकारी देखें।

4. अज्ञात लोगों को पैसे न भेजें: अज्ञात लोगों से पैसे मांगने वाले अनुरोधों से सावधान रहें।

यदि आप स्कैम का शिकार हो जाते हैं:

1. स्कैम की रिपोर्ट करें: संबंधित अधिकारियों, जैसे कि एफटीसी या स्थानीय पुलिस विभाग में शिकायत दर्ज करें।

2. अपने बैंक और क्रेडिट कार्ड कंपनियों से संपर्क करें: उन्हें स्कैम के बारे में सूचित करें और अपने खातों की निगरानी करने का अनुरोध करें।

3. अपने पासवर्ड बदलें: अपने पासवर्ड अपडेट करें और दो-कारक प्रमाणीकरण सक्षम करें।

साइबर धोखाधड़ी

साइबर धोखाधड़ी ऑनलाइन होने वाली धोखाधड़ी गतिविधियाँ हैं जो डिजिटल तकनीकों का उपयोग करके व्यक्तियों या संगठनों को धोखा देती हैं और उनका शोषण करती हैं।

साइबर धोखाधड़ी के प्रकार:

1. पहचान की चोरी: व्यक्तिगत डेटा चोरी करना, जैसे कि सामाजिक सुरक्षा संख्या, क्रेडिट कार्ड नंबर या लॉगिन क्रेडेंशियल।

2. फ़िशिंग: नकली ईमेल, संदेश या वेबसाइट का उपयोग करके संवेदनशील जानकारी चोरी करना।

3. ऑनलाइन नीलामी धोखाधड़ी: ऑनलाइन नीलामी में नकली उत्पाद या सेवाएं बेचना।

4. क्रेडिट कार्ड धोखाधड़ी: चोरी हुए क्रेडिट कार्ड जानकारी का उपयोग करके अनधिकृत लेनदेन करना।

अपनी सुरक्षा के लिए:

1. मजबूत पासवर्ड और 2FA का उपयोग करें: अपने खातों को मजबूत पासवर्ड और दो-कारक प्रमाणीकरण के साथ सुरक्षित करें।

2. संदिग्ध ईमेल और संदेशों से सावधान रहें: वर्तनी और व्याकरण की गलतियों को देखें और प्रेषक की पहचान सत्यापित करें।

3. वेबसाइटों और कंपनियों की सत्यता जांचें: कंपनी के बारे में शोध करें और समीक्षाएं, रेटिंग और संपर्क जानकारी देखें।

यदि आप धोखाधड़ी का शिकार हो जाते हैं:

1. घटना की रिपोर्ट करें: संबंधित अधिकारियों को घटना की रिपोर्ट करें।

2. अपने बैंक और क्रेडिट कार्ड कंपनियों से संपर्क करें: उन्हें घटना के बारे में सूचित करें और अपने खातों की निगरानी करने का अनुरोध करें।

3. अपने पासवर्ड बदलें: अपने पासवर्ड अपडेट करें और दो-कारक प्रमाणीकरण सक्षम करें।

ऑनलाइन स्कैम और साइबर धोखाधड़ी से बचने के उपाय

ऑनलाइन स्कैम और साइबर धोखाधड़ी से बचने के लिए कुछ महत्वपूर्ण उपाय हैं:

- **सावधानियां:**

1. मजबूत पासवर्ड का उपयोग करें: अपने सभी ऑनलाइन खातों के लिए मजबूत और अद्वितीय पासवर्ड का उपयोग करें।

2. दो-कारक प्रमाणीकरण सक्षम करें: अपने खातों में दो-कारक प्रमाणीकरण सक्षम करें ताकि अतिरिक्त सुरक्षा मिल सके।

3. संदिग्ध ईमेल और लिंक से बचें: अज्ञात प्रेषकों से आए ईमेल और लिंक पर क्लिक न करें।

4. वेबसाइटों की सत्यता जांचें: ऑनलाइन लेनदेन करने से पहले वेबसाइट की सत्यता जांचें।

- **सुरक्षा सॉफ़्टवेयर का उपयोग करें:**

1. एंटीवायरस सॉफ़्टवेयर: अपने डिवाइस में एंटीवायरस सॉफ़्टवेयर स्थापित करें और नियमित रूप से अद्यतन करें।

2. फ़ायरवॉल: अपने डिवाइस में फ़ायरवॉल सक्षम करें ताकि अनधिकृत पहुंच को रोका जा सके।

- **व्यक्तिगत जानकारी की सुरक्षा:**

1. व्यक्तिगत जानकारी साझा न करें: अज्ञात व्यक्तियों या वेबसाइटों के साथ व्यक्तिगत जानकारी साझा न करें।

2. सामाजिक मीडिया पर सावधानी बरतें: सामाजिक मीडिया पर व्यक्तिगत जानकारी साझा करते समय सावधानी बरतें।

- **शिकायत और रिपोर्ट:**

1. स्कैम की रिपोर्ट करें: यदि आप स्कैम का शिकार होते हैं, तो तुरंत संबंधित अधिकारियों को रिपोर्ट करें।

2. अपने बैंक और क्रेडिट कार्ड कंपनियों को सूचित करें: अपने बैंक और क्रेडिट कार्ड कंपनियों को घटना के बारे में सूचित करें और अपने खातों की निगरानी करने का अनुरोध करें।

ऑनलाइन स्कैम:

ऑनलाइन स्कैम इंटरनेट पर होने वाली धोखाधड़ी गतिविधियाँ हैं, जहाँ स्कैमर्स व्यक्तियों को धोखा देकर संवेदनशील जानकारी प्रकट करने, पैसे भेजने या अपने डिवाइस या खातों तक पहुँच प्रदान करने के लिए मजबूर करते हैं।

ऑनलाइन स्कैम के प्रकार:

1. फ़िशिंग स्कैम: स्कैमर्स नकली ईमेल, संदेश या वेबसाइट बनाते हैं जो वैध कंपनियों से होने का दिखावा करते हैं, संवेदनशील जानकारी मांगते हैं।

2. ऑनलाइन नीलामी स्कैम: स्कैमर्स नकली ऑनलाइन नीलामी बनाते हैं, जहाँ वे उत्पादों या सेवाओं को बेचने का वादा करते हैं जो मौजूद नहीं हैं या जैसा बताया गया है वैसा नहीं हैं।

3. रोमांस स्कैम: स्कैमर्स डेटिंग वेबसाइटों या सोशल मीडिया पर नकली प्रोफाइल बनाते हैं, पीड़ितों के साथ संबंध बनाते हैं और पैसे या उपहार मांगते हैं।

4. निवेश स्कैम: स्कैमर्स असामान्य रूप से उच्च रिटर्न का वादा करते हैं, लेकिन निवेश अक्सर नकली या अस्थिर होते हैं।

अपनी सुरक्षा के लिए:

1. संदिग्ध ईमेल और संदेशों से सावधान रहें: वर्तनी और व्याकरण की गलतियों को देखें और प्रेषक की पहचान सत्यापित करें।

2. मजबूत पासवर्ड और 2FA का उपयोग करें: अपने खातों को मजबूत, अद्वितीय पासवर्ड और दो-कारक प्रमाणीकरण के साथ सुरक्षित करें।

3. वेबसाइटों और कंपनियों की सत्यता जांचें: कंपनी के बारे में शोध करें और समीक्षाएं, रेटिंग और संपर्क जानकारी देखें।

4. अज्ञात लोगों को पैसे न भेजें: अज्ञात लोगों से पैसे मांगने वाले अनुरोधों से सावधान रहें।

यदि आप स्कैम का शिकार हो जाते हैं:

1. स्कैम की रिपोर्ट करें: संबंधित अधिकारियों, जैसे कि एफटीसी या स्थानीय पुलिस विभाग में शिकायत दर्ज करें।

2. अपने बैंक और क्रेडिट कार्ड कंपनियों से संपर्क करें: उन्हें स्कैम के बारे में सूचित करें और अपने खातों की निगरानी करने का अनुरोध करें।

3. अपने पासवर्ड बदलें: अपने पासवर्ड अपडेट करें और दो-कारक प्रमाणीकरण सक्षम करें।

ऑनलाइन घोटालों के प्रकार:

1. फ़िशिंग घोटाले: स्कैमर्स नकली ईमेल, संदेश या वेबसाइट बनाते हैं जो वैध कंपनियों से होने का दिखावा करते हैं, संवेदनशील जानकारी मांगते हैं।

2. ऑनलाइन नीलामी घोटाले: स्कैमर्स नकली ऑनलाइन नीलामी बनाते हैं, जहाँ वे उत्पादों या सेवाओं को बेचने का वादा करते हैं जो मौजूद नहीं हैं या जैसा बताया गया है वैसा नहीं हैं।

3. रोमांस घोटाले: स्कैमर्स डेटिंग वेबसाइटों या सोशल मीडिया पर नकली प्रोफाइल बनाते हैं, पीड़ितों के साथ संबंध बनाते हैं और पैसे या उपहार मांगते हैं।

4. निवेश घोटाले: स्कैमर्स असामान्य रूप से उच्च रिटर्न का वादा करते हैं, लेकिन निवेश अक्सर नकली या अस्थिर होते हैं।

अपनी सुरक्षा के लिए:

1. संदिग्ध ईमेल और संदेशों से सावधान रहें: वर्तनी और व्याकरण की गलतियों को देखें और प्रेषक की पहचान सत्यापित करें।

2. मजबूत पासवर्ड और 2FA का उपयोग करें: अपने खातों को मजबूत पासवर्ड और दो-कारक प्रमाणीकरण के साथ सुरक्षित करें।

3. वेबसाइटों और कंपनियों की सत्यता जांचें: कंपनी के बारे में शोध करें और समीक्षाएं, रेटिंग और संपर्क जानकारी देखें।

धोखेबाजों द्वारा उपयोग की जाने वाली तरकीबें:

1. फ़िशिंग: धोखेबाज नकली ईमेल, संदेश या वेबसाइट बनाते हैं जो वैध कंपनियों से होने का दिखावा करते हैं।

2. सोशल इंजीनियरिंग: धोखेबाज मनोवैज्ञानिक हेरफेर का उपयोग करके लोगों को संवेदनशील जानकारी प्रकट करने या कुछ कार्यों को करने के लिए मजबूर करते हैं।

3. प्रीटेक्स्टिंग: धोखेबाज अपने पीड़ितों का विश्वास जीतने और संवेदनशील जानकारी प्राप्त करने के लिए एक नकली परिदृश्य या कहानी बनाते हैं।

अपनी सुरक्षा के लिए:

1. संदिग्ध ईमेल और संदेशों से सावधान रहें: वर्तनी और व्याकरण की गलतियों को देखें और प्रेषक की पहचान सत्यापित करें।

2. मजबूत पासवर्ड और 2FA का उपयोग करें: अपने खातों को मजबूत पासवर्ड और दो-कारक प्रमाणीकरण के साथ सुरक्षित करें।

3. वेबसाइटों और कंपनियों की सत्यता जांचें: कंपनी के बारे में शोध करें और समीक्षाएं, रेटिंग और संपर्क जानकारी देखें।

ऑनलाइन स्कैम की पहचान और बचाव

चेतावनी संकेत:

1. अत्यावश्यक या धमकी भरे संदेश: स्कैमर्स अक्सर अत्यावश्यक स्थिति बनाते हैं या धमकी देते हैं अगर आप तुरंत कार्रवाई नहीं करते हैं।

2. संदिग्ध ईमेल या संदेश: वर्तनी और व्याकरण की गलतियों, सामान्य अभिवादन और अपरिचित प्रेषकों की जांच करें।

3. बहुत अच्छे लगने वाले ऑफर: अगर कोई ऑफर बहुत अच्छा लगता है, तो शायद वह सच नहीं है।

बचाव:

1. प्रेषक की जानकारी सत्यापित करें: प्रेषक की ईमेल पते या फोन नंबर की जांच करें ताकि यह सुनिश्चित हो सके कि यह वैध है।

2. मजबूत पासवर्ड का उपयोग करें: सभी ऑनलाइन खातों के लिए अद्वितीय और जटिल पासवर्ड का उपयोग करें।

3. दो-कारक प्रमाणीकरण सक्षम करें: अपने खातों में दो-कारक प्रमाणीकरण के साथ अतिरिक्त सुरक्षा जोड़ें।

बचने के लिए:

1. संदिग्ध लिंक: अपरिचित प्रेषकों या वेबसाइटों से लिंक पर क्लिक करने से बचें।

2. अज्ञात अटैचमेंट: अपरिचित प्रेषकों या वेबसाइटों से अटैचमेंट खोलने से बचें।

3. सार्वजनिक वाई-फाई: संवेदनशील लेनदेन के लिए सार्वजनिक वाई-फाई का उपयोग करने से बचें।

यदि आप स्कैम का शिकार हो जाते हैं:

1. स्कैम की रिपोर्ट करें: संबंधित अधिकारियों को स्कैम की रिपोर्ट करें।

2. अपने बैंक से संपर्क करें: अपने बैंक और क्रेडिट कार्ड कंपनियों को किसी भी संदिग्ध गतिविधि के बारे में सूचित करें।

3. अपने पासवर्ड बदलें: अपने पासवर्ड अपडेट करें और दो-कारक प्रमाणीकरण सक्षम करें।

ऑनलाइन स्कैम की पहचान कैसे करें:

1. URL की जांच करें: स्कैमर्स अक्सर नकली वेबसाइट बनाते हैं जिनके यूआरएल वैध वेबसाइटों के समान होते हैं।

2. ईमेल से सावधान रहें: स्कैमर्स अक्सर नकली ईमेल भेजते हैं जो वैध कंपनियों से होने का दिखावा करते हैं।

3. लाल झंडों की तलाश करें: संवेदनशील जानकारी मांगने वाले अनुरोधों से सावधान रहें।

4. समीक्षाएं जांचें: कंपनी के बारे में शोध करें और अन्य ग्राहकों की समीक्षाएं पढ़ें।

5. अनचाहे ऑफर से सावधान रहें: अगर आपने कोई ऑफर नहीं मांगा है, तो उससे सावधान रहें।

ऑनलाइन स्कैम के सामान्य तरीके:

1. फ़िशिंग: स्कैमर्स नकली ईमेल या संदेश भेजते हैं जो वैध कंपनियों से होने का दिखावा करते हैं।

2. मैलवेयर: स्कैमर्स मैलवेयर का उपयोग करके डिवाइस या डेटा तक अनधिकृत पहुंच प्राप्त करते हैं।

यदि आप स्कैम का शिकार हो जाते हैं:

1. स्कैम की रिपोर्ट करें: संबंधित अधिकारियों को स्कैम की रिपोर्ट करें।

2. अपने बैंक से संपर्क करें: अपने बैंक और क्रेडिट कार्ड कंपनियों को किसी भी संदिग्ध गतिविधि के बारे में सूचित करें।

3. अपने पासवर्ड बदलें: अपने पासवर्ड अपडेट करें और दो-कारक प्रमाणीकरण सक्षम करें।

ऑनलाइन स्कैम से बचने के तरीके:

1. संदिग्ध ईमेल और संदेशों से सावधान रहें: अनचाहे ईमेल या संदेशों के लिंक पर क्लिक न करें और न ही संवेदनशील जानकारी प्रदान करें।

2. वेबसाइटों की प्रामाणिकता सत्यापित करें: यूआरएल की जांच करें और एड्रेस बार में "https" और लॉक आइकन देखें।

3. मजबूत पासवर्ड का उपयोग करें: सभी ऑनलाइन खातों के लिए अद्वितीय और जटिल पासवर्ड का उपयोग करें।

4. दो-कारक प्रमाणीकरण सक्षम करें: अपने खातों में दो-कारक प्रमाणीकरण के साथ अतिरिक्त सुरक्षा जोड़ें।

5. सॉफ़्टवेयर को अद्यतन रखें: अपने ऑपरेटिंग सिस्टम, ब्राउज़र और एंटीवायरस सॉफ़्टवेयर को नियमित रूप से अद्यतन करें।

6. एंटीवायरस सॉफ़्टवेयर का उपयोग करें: अपने डिवाइस को मैलवेयर से बचाने के लिए एंटीवायरस सॉफ़्टवेयर स्थापित करें और नियमित रूप से अद्यतन करें।

7. सार्वजनिक वाई-फाई से सावधान रहें: संवेदनशील लेनदेन के लिए सार्वजनिक वाई-फाई का उपयोग करने से बचें।

8. अपने खातों की निगरानी करें: अपने खातों और क्रेडिट रिपोर्ट की नियमित जांच करें और किसी भी संदिग्धम्भ गतिविधि की रिपोर्ट करें।

Unit 4: Cyber Laws and Ethics
Cyber Laws (IT Law) in India

Cyber Law also called IT Law is the law regarding Information-technology including computers and the internet. It is related to legal informatics and supervises the digital circulation of information, software, information security, and e-commerce.

IT law does not consist of a separate area of law rather it encloses aspects of contract, intellectual property, privacy, and data protection laws. Intellectual property is a key element of IT law. The area of software license is controversial and still evolving in Europe and elsewhere.

According to the Ministry of Electronics and Information Technology, Government of India :

Cyber Laws yields legal recognition to electronic documents and a structure to support e-filing and e-commerce transactions and also provides a legal structure to reduce, check cyber crimes.

Importance of Cyber Law:

1. It covers all transactions over the internet.
2. It keeps eye on all activities over the internet.
3. It touches every action and every reaction in cyberspace.

Area of Cyber Law:

Cyber laws contain different types of purposes. Some laws create rules for how individuals and companies may use computers and the internet while some laws protect people from becoming the victims of crime through unscrupulous activities on the internet. The major areas of cyber law include:

1. ***Fraud*:**
   Consumers depend on cyber laws to protect them from online fraud. Laws are made to prevent identity theft, credit card theft, and other financial crimes that happen online. A person who commits identity theft may face confederate or state criminal charges. They might also encounter a civil action brought by a victim. Cyber lawyers work to both defend and prosecute against allegations of fraud using the internet.
2. ***Copyright*:**
   The internet has made copyright violations easier. In the early days of online communication, copyright violations were too easy. Both companies and individuals need lawyers to bring an action to impose copyright protections. Copyright violation is an area of cyber law that protects the rights of individuals and companies to profit from their creative works.
3. ***Defamation*:**
   Several personnel uses the internet to speak their mind. When people use the internet to say things that are not true, it can cross the line into defamation. Defamation laws are civil laws that save individuals from fake public statements that can harm a business or someone's reputation. When people use the internet to make statements that violate civil laws, that is called Defamation law.
4. ***Harassment and Stalking*:**
   Sometimes online statements can violate criminal laws that forbid harassment and stalking. When a person makes threatening statements again and again about someone else online, there is a violation of both civil and criminal laws. Cyber lawyers both prosecute and defend people when stalking occurs using the internet and other forms of electronic communication.
5. ***Freedom of Speech*:**
   Freedom of speech is an important area of cyber law. Even though cyber laws forbid certain behaviors online, freedom of speech laws also allows people to speak their minds. Cyber lawyers must advise their clients on the limits of free speech including laws that prohibit obscenity. Cyber lawyers may also defend their clients when there is a debate about whether their actions consist of permissible free speech.

6. ***Trade Secrets*:**
   Companies doing business online often depend on cyber laws to protect their trade secrets. For example, Google and other online search engines spend lots of time developing the algorithms that produce search results. They also spend a great deal of time developing other features like maps, intelligent assistance, and flight search services to name a few. Cyber laws help these companies to take legal action as necessary to protect their trade secrets.
7. ***Contracts and Employment Law*:**
   Every time you click a button that says you agree to the terms and conditions of using a website, you have used cyber law. There are terms and conditions for every website that are somehow related to privacy concerns.

Advantages of Cyber Law:

- Organizations are now able to carry out e-commerce using the legal infrastructure provided by the Act.
- Digital signatures have been given legal validity and sanction in the Act.
- It has opened the doors for the entry of corporate companies for issuing Digital Signatures Certificates in the business of being Certifying Authorities.
- It allows Government to issue notifications on the web thus heralding e-governance.
- It gives authority to the companies or organizations to file any form, application, or any other document with any office, authority, body, or agency owned or controlled by the suitable Government in e-form using such e-form as may be prescribed by the suitable Government.
- The IT Act also addresses the important issues of security, which are so critical to the success of electronic transactions.
- Cyber Law provides both hardware and software security.

Overview of Indian Cyber Laws (IT Act 2000)

Cyber laws in India are primarily governed by the Information Technology Act, 2000, which provides a legal framework for digital transactions and electronic communication. These laws address a range of issues, including cybercrimes like hacking and fraud, data protection, and e-commerce, ensuring a safe and legally compliant online environment. The act grants legal recognition to digital signatures and electronic records while also defining punishments for various offenses.

Key aspects of India's cyber laws:

- **Information Technology Act, 2000**:
  The core legislation that provides legal recognition to electronic commerce, facilitates electronic filing with government agencies, and addresses cybercrimes.
- **Legal recognition of digital data**:
  The act gives legal validity to electronic documents and digital signatures, which is crucial for online transactions and e-commerce.
- **Cybercrime prevention**:
  It defines and provides for the punishment of various cybercrimes such as:
- Hacking and unauthorized access
- Identity theft
- Data theft and fraud
- Publishing obscene content
- Cyber terrorism
- **Other applicable laws**:
  Traditional laws like the Indian Penal Code, 1860, and the Indian Evidence Act, 1872, are also applied to cybercrimes.
- **Penalties**:
  The act specifies penalties, which can include imprisonment and fines, for different cybercrimes.

- **Data protection**:
  While the IT Act covers aspects of data protection, the Personal Data Protection Bill, 2019 is a separate but related bill that is expected to have a significant impact on privacy regulations.
- **Intermediary guidelines**:
  Rules like the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 govern the conduct of intermediaries in the digital space.

भारत में साइबर कानून मुख्य रूप से सूचना प्रौद्योगिकी अधिनियम, 2000द्वारा शासित होते हैं , जो डिजिटल लेनदेन और इलेक्ट्रॉनिक संचार के लिए कानूनी ढांचा प्रदान करता है। ये कानून कई मुद्दों को संबोधित करते हैं, जिनमें हैकिंग और धोखाधड़ी जैसे साइबर अपराध, डेटा संरक्षण और ई-कॉमर्स शामिल हैं, तथा एक सुरक्षित और कानूनी रूप से अनुपालन योग्य ऑनलाइन वातावरण सुनिश्चित करते हैं। यह अधिनियम डिजिटल हस्ताक्षरों और इलेक्ट्रॉनिक अभिलेखों को कानूनी मान्यता प्रदान करता है, साथ ही विभिन्न अपराधों के लिए दंड भी परिभाषित करता है।

भारत के साइबर कानून के प्रमुख पहलू:

- **सूचना प्रौद्योगिकी अधिनियम, 2000**:

  मुख्य कानून इलेक्ट्रॉनिक वाणिज्य को कानूनी मान्यता प्रदान करता है, सरकारी एजेंसियों के साथ इलेक्ट्रॉनिक फाइलिंग की सुविधा प्रदान करता है, और साइबर अपराधों को संबोधित करता है।

- **डिजिटल डेटा की कानूनी मान्यता**:

  यह अधिनियम इलेक्ट्रॉनिक दस्तावेजों और डिजिटल हस्ताक्षरों को कानूनी वैधता प्रदान करता है, जो ऑनलाइन लेनदेन और ई-कॉमर्स के लिए महत्वपूर्ण है।

- **साइबर अपराध की रोकथाम**:

  यह विभिन्न साइबर अपराधों को परिभाषित करता है और उनके लिए दंड का प्रावधान करता है, जैसे:

- हैकिंग और अनधिकृत पहुँच
- चोरी की पहचान
- डेटा चोरी और धोखाधड़ी
- अश्लील सामग्री प्रकाशित करना
- साइबर आतंकवाद

- **अन्य लागू कानून**:

  भारतीय दंड संहिता, 1860 और भारतीय साक्ष्य अधिनियम, 1872 जैसे पारंपरिक कानून भी साइबर अपराधों पर लागू होते हैं।

- **दंड**:

  अधिनियम में विभिन्न साइबर अपराधों के लिए दंड का प्रावधान किया गया है, जिसमें कारावास और जुर्माना शामिल हो सकता है।

- **डेटा सुरक्षा**:

  जबकि आईटी अधिनियम डेटा संरक्षण के पहलुओं को शामिल करता है, व्यक्तिगत डेटा संरक्षण विधेयक, 2019 एक अलग लेकिन संबंधित विधेयक है, जिसका गोपनीयता नियमों पर महत्वपूर्ण प्रभाव पड़ने की उम्मीद है।

- **मध्यस्थ दिशानिर्देश**:

  सूचना प्रौद्योगिकी (मध्यस्थ दिशानिर्देश और डिजिटल मीडिया आचार संहिता) नियम, 2021जैसे नियम डिजिटल स्पेस में मध्यस्थों के आचरण को नियंत्रित करते हैं।

Offences like cyberbullying, identity theft, data breaches

Cybercrime offences include a wide range of unlawful acts like financial fraud, hacking, online harassment, and the distribution of illegal content, which are addressed by laws such as the Information Technology Act and the Indian Penal Code. Common offenses include phishing, identity theft, cheating, defamation, cyber terrorism, and the creation or dissemination of sexually explicit material, with penalties varying based on the specific crime.

Cyberbullying

Cyberbullying is harassment, threats, or embarrassment using electronic devices like phones, computers, and gaming systems. It can occur on social media, through text messages, apps, or other online platforms, and includes spreading rumours, posting embarrassing information, or creating fake profiles to harm someone. Cyberbullying can have severe mental and emotional effects, and victims should not respond but should instead save evidence and report the behaviour to a trusted adult.

What is cyberbullying?

- **Definition:**

  Cyberbullying is when someone uses technology to harass, threaten, or make another person feel bad.

- **Platforms:**

  It can happen on social media, in games, through text messages, emails, or any online service.

- **Examples:**

  1. Sending mean or hurtful messages.
  2. Sharing embarrassing photos or videos.
  3. Spreading false rumours or gossip online.
  4. Creating fake profiles to impersonate someone.
  5. Intentionally leaving someone out of online groups.

What are the effects of cyberbullying?

- **Emotional:** Victims may feel anxious, depressed, ashamed, or fearful.
- **Mental:** It can lead to social isolation, a loss of self-esteem, and difficulty concentrating in school.
- **Physical:** In some cases, victims may experience physical symptoms like headaches or stomach-aches, and may have changes in eating or sleeping habits.
- **Extreme cases:** In severe situations, cyberbullying can lead to self-harm or suicide.

How can you deal with cyberbullying?

- **Don't respond:** Never reply to the person. They are often looking for a reaction, and replying can make the situation worse.
- **Save evidence:** Take screenshots of messages, posts, or other hurtful content.
- **Block the person:** Use the tools on the platform to block the bully.
- **Report the behaviour:** Report the content and the person to the website, app, or game's administrators.
- **Tell a trusted adult:** Talk to a parent, teacher, counsellor, or another trusted adult about what is happening.
- **Do not give up your technology:** If your parents are considering taking away your device, let them know you are worried that this will prevent you from talking to them in the future.

Identity Theft

Stealing personal information like credit card numbers or Aadhaar details to commit fraud. This can be done through phishing emails or by accessing stolen data from a data breach.

Identity theft is a crime that involves using another person's private identifying information—like their Social Security number, credit card information, or passwords—without their permission to commit fraud. This can result in significant financial losses, damage to credit, and other serious consequences for the victim.

How identity theft occurs

Thieves use a variety of digital and physical methods to steal information.

- **Data breaches:** Gaining unauthorized access to a company's database that stores sensitive customer information.
- **Phishing scams:** Sending deceptive emails or text messages that trick recipients into revealing personal data.
- **Malware:** Installing malicious software on a victim's device that can secretly record keystrokes or steal files.
- **Card skimming:** Using a hidden device on a payment terminal or ATM to steal credit or debit card information.
- **Mail theft and dumpster diving:** Stealing bills, bank statements, or other personal documents from mailboxes or trash.
- **Unsecured Wi-Fi:** Eavesdropping on a public, unsecure Wi-Fi connection to intercept data.
- **Lost or stolen wallets and phones:** Physically stealing devices or documents that contain sensitive information.

Common types of identity theft

- **Financial identity theft:** Using another person's financial information to open accounts, make purchases, or take out loans.
- **Tax identity theft:** Stealing a Social Security number to file a fraudulent tax return and claim the refund.
- **Medical identity theft:** Using stolen personal information to receive medical care, fill prescriptions, or submit fake claims to an insurer.
- **Criminal identity theft:** Posing as another individual when arrested to avoid prosecution.
- **Child identity theft:** Using a minor's Social Security number to open fraudulent accounts, which can go undetected for years.
- **Synthetic identity theft:** Combining real and fake information to create a new, fraudulent identity.

How to protect yourself

- **Use strong passwords and multi-factor authentication:** Use unique, complex passwords for all accounts and enable two-factor or multi-factor authentication whenever possible.
- **Be cautious online:** Stick to secure websites (those with an "https" web address and a padlock icon) and limit the personal information you share on social media.
- **Protect personal documents:** Shred documents that contain personal or financial information before throwing them away.
- **Monitor financial and credit accounts:** Regularly check your bank and credit card statements for any suspicious activity. You can also get free copies of your credit report from each of the three major credit bureaus (Experian, Equifax, and TransUnion).
- **Freeze your credit:** Placing a freeze on your credit reports restricts access to them, making it difficult for a thief to open new accounts in your name. This is free and highly effective.
- **Protect your devices:** Keep all software and antivirus programs up to date, and secure your mobile devices with strong passwords or biometrics.

What to do if your identity is stolen

If you suspect you are a victim of identity theft, act quickly to minimize the damage.

1. **Contact your financial institutions:** Alert your bank and credit card companies about any fraudulent charges and close compromised accounts.
2. **File an official report:** In the U.S., report the theft to the Federal Trade Commission (FTC) at IdentityTheft.gov.
3. **Place fraud alerts:** Contact one of the three major credit bureaus (Equifax, Experian, or TransUnion) to place a fraud alert on your credit report. This requires lenders to verify your identity before opening a new account.
4. **File a police report:** Contact your local police department to file a report. This can be important for disputing charges with creditors.
5. **Secure accounts:** Change all of your account passwords and enable two-factor authentication.

Data Breaches

The unauthorized access and theft of sensitive or private information from a company or organization. This can lead to identity theft, financial fraud, and other problems for individuals whose data was compromised.

A data breach is a security incident where confidential or sensitive information is accessed, exposed, or stolen by an unauthorized individual or party. Breaches can result from malicious cyberattacks or from human error, such as an employee accidentally exposing data.

Common causes of data breaches

- **Cyberattacks:** Malicious external actors often use various tactics to infiltrate networks and systems. Common examples include:
  - **Phishing and social engineering:** Manipulating individuals into revealing credentials or other sensitive information, often through fake emails or websites.
  - **Malware and ransomware:** Deploying malicious software to disrupt operations, steal data, or hold it hostage for a ransom payment.
  - **Credential theft:** Compromising login details through brute-force attacks or by using credentials stolen from other breaches.
- **Human error and internal threats:** Not all breaches are malicious. Unintentional errors, like emailing sensitive information to the wrong person, or a malicious insider who purposely leaks data, are common causes.
- **System vulnerabilities:** Attackers exploit weaknesses in software, hardware, or network security to gain access. Failing to install security patches promptly is a major risk.
- **Third-party vendors:** Many organizations rely on third-party vendors for services. If a vendor has weak security, it can be a gateway for attackers to access the main company's network, as seen in the 2013 Target breach.

Consequences of a data breach

- **Financial losses:** Organizations face high costs, including regulatory fines, legal fees from class-action lawsuits, and compensation for customers. For example, the 2017 Equifax breach cost the company billions in fines and legal settlements.
- **Reputational damage:** A breach can erode customer trust and cause significant damage to a company's public image.
- **Personal impact:** Individuals whose data is exposed are at an elevated risk of identity theft, financial fraud, and other crimes for years after the incident.
- **Operational disruption:** Breaches can force companies to take systems offline for investigation and recovery, leading to lost business and reduced productivity.

Notable recent and large-scale breaches

- **Chinese Surveillance Database (June 2025):** The largest-ever data leak, exposing 4 billion records containing personal and financial information of hundreds of millions of Chinese citizens.
- **AT&T (March 2024):** A data set from 2019 was released on the dark web, affecting over 70 million current and former customers.
- **23andMe (Fall 2023):** Hackers accessed the data of 6.9 million users, including highly personal genetic and ancestry information. The breach occurred via "credential stuffing," a tactic that reuses credentials from other data leaks.

How to protect yourself and your data

For individuals, proactive measures are key to minimizing your risk of harm from data breaches:

- **Use strong, unique passwords and a password manager.** Avoid reusing passwords across multiple sites. A password manager can help you manage complex, unique passwords.

- **Enable multi-factor authentication (MFA).** This adds a crucial layer of security, making it difficult for attackers to access your accounts even if they have your password.
- **Be wary of phishing scams.** Be cautious of unexpected emails or texts that ask for personal information. Never click on suspicious links.
- **Stay up-to-date.** Keep all your software and operating systems updated with the latest security patches.
- **Encrypt your devices.** Use encryption on your laptop and smartphone to protect data if the device is lost or stolen.
- **Monitor your credit.** After a major breach, it is wise to place a fraud alert or credit freeze with the major credit bureaus.
- **Check if your data has been compromised.** Use services like Have I Been Pwned to see if your email address has appeared in public data breaches.

What is cyberbullying?

साइबरबुलिंग इलेक्ट्रॉनिक उपकरणों जैसे फोन, कंप्यूटर और गेमिंग सिस्टम का उपयोग करके उत्पीड़न, धमकी या शर्मिंदगीहै । यह सोशल मीडिया पर, टेक्स्ट मैसेज, एप या अन्य ऑनलाइन प्लेटफॉर्म के माध्यम से हो सकता है, और इसमें अफवाहें फैलाना, शर्मनाक जानकारी पोस्ट करना या किसी को नुकसान पहुंचाने के लिए फर्जी प्रोफाइल बनाना शामिल है। साइबर बदमाशी के गंभीर मानसिक और भावनात्मक प्रभाव हो सकते हैं, और पीड़ितों को प्रतिक्रिया नहीं देनी चाहिए, बल्कि साक्ष्य को सुरक्षित रखना चाहिए और किसी विश्वसनीय वयस्क को इस व्यवहार की सूचना देनी चाहिए।

साइबर-बुलिंग क्या है?

- **परिभाषा:**

  साइबरबुलिंग तब होती है जब कोई व्यक्ति किसी अन्य व्यक्ति को परेशान करने, धमकाने या बुरा महसूस कराने के लिए प्रौद्योगिकी का उपयोग करता है।

- **प्लेटफार्म:**

  यह सोशल मीडिया, गेम्स, टेक्स्ट मैसेज, ईमेल या किसी भी ऑनलाइन सेवा के माध्यम से हो सकता है।

- **उदाहरण:**
- बुरे या चोट पहुँचाने वाले संदेश भेजना।
- शर्मनाक तस्वीरें या वीडियो साझा करना।
- ऑनलाइन झूठी अफवाहें या गपशप फैलाना।
- किसी का प्रतिरूपण करने के लिए फर्जी प्रोफाइल बनाना।
- जानबूझकर किसी को ऑनलाइन समूह से बाहर रखना।

साइबरबुलिंग के क्या प्रभाव हैं?

- **भावनात्मक:** पीड़ित व्यक्ति चिंतित, उदास, शर्मिंदा या भयभीत महसूस कर सकता है।
- **मानसिक:** इससे सामाजिक अलगाव, आत्म-सम्मान में कमी, तथा स्कूल में ध्यान केंद्रित करने में कठिनाई हो सकती है।
- **भौतिक:** कुछ मामलों में, पीड़ितों को सिरदर्द या पेट दर्द जैसे शारीरिक लक्षण अनुभव हो सकते हैं, तथा उनके खाने या सोने की आदतों में भी परिवर्तन हो सकता है।
- **चरम मामले:** गंभीर परिस्थितियों में, साइबर धमकी से आत्म-क्षति या आत्महत्या तक हो सकती है।

आप साइबरबुलिंग से कैसे निपट सकते हैं?

- **जवाब न दें:** उस व्यक्ति को कभी जवाब न दें। वे अक्सर प्रतिक्रिया की तलाश में रहते हैं, और जवाब देने से स्थिति और बिगड़ सकती है।
- **साक्ष्य सहेजें:** संदेशों, पोस्टों या अन्य आहत करने वाली सामग्री का स्क्रीनशॉट लें।
- **व्यक्ति को ब्लॉक करें:** धमकाने वाले को रोकने के लिए प्लेटफॉर्म पर मौजूद उपकरणों का उपयोग करें।
- **व्यवहार की रिपोर्ट करें:** वेबसाइट, ऐप या गेम के व्यवस्थापकों को सामग्री और व्यक्ति की रिपोर्ट करें.
- **किसी विश्वसनीय वयस्क को बताएं:** जो कुछ हो रहा है उसके बारे में माता-पिता, शिक्षक, परामर्शदाता या किसी अन्य विश्वसनीय वयस्क से बात करें।
- **अपनी तकनीक को न छोड़ें:** यदि आपके माता-पिता आपका डिवाइस छीनने पर विचार कर रहे हैं, तो उन्हें बताएं कि आप चिंतित हैं कि इससे भविष्य में आप उनसे बात नहीं कर पाएंगे।

पहचान की चोरी (Identity Theft)

पहचान की चोरी (Identity Theft) एक अपराध है जिसमें कोई व्यक्ति आपकी व्यक्तिगत जानकारी जैसे नाम, सोशल सिक्योरिटी नंबर, या बैंक खाते की जानकारी चुराता है और उसका उपयोग धोखाधड़ी करने के लिए करता है। इस चोरी की गई जानकारी का उपयोग अक्सर आपके नाम पर नए खाते खोलने, क्रेडिट कार्ड लेने, या धोखाधड़ी वाले टैक्स रिटर्न दाखिल करने जैसे कामों के लिए किया जाता है।

पहचान की चोरी कैसे होती है

- **ऑनलाइन:**

  फिशिंग ईमेल, मैलवेयर, या कॉर्पोरेट डेटाबेस को हैक करके आपकी जानकारी चुराई जा सकती है।

- **ऑफलाइन:**

  कूड़ेदान में फेंके गए दस्तावेजों से जानकारी प्राप्त करना, या "डंपस्टर डाइविंग" जैसे तरीकों का इस्तेमाल किया जा सकता है।

- **अन्य तरीके:**

  सोशल इंजीनियरिंग (लोगों को धोखा देकर जानकारी निकलवाना) और स्किमिंग डिवाइस (क्रेडिट कार्ड से जानकारी चुराना) भी इसके तरीके हैं।

पहचान की चोरी के परिणाम

- आपके नाम पर धोखाधड़ी वाले क्रेडिट कार्ड और ऋण खाते खोले जा सकते हैं।
- आपकी साख और प्रतिष्ठा को नुकसान पहुंच सकता है।
- आपकी वित्तीय स्थिति खराब हो सकती है और इससे उबरने में महीनों या साल लग सकते हैं।
- आपको सरकारी लाभ या टैक्स रिफंड के लिए भी आपकी पहचान का दुरुपयोग किया जा सकता है।

क्या करें

- **शिकायत करें:**

  आप cybercrime.gov.in पर ऑनलाइन या 1930 पर कॉल करके शिकायत दर्ज करा सकते हैं, Bajaj Finserv।

- **बचाव:**

  अपनी व्यक्तिगत जानकारी को सुरक्षित रखें और संदिग्ध लिंक या ईमेल पर क्लिक करने से बचें।

- **जांच करें:**

  अपने बैंक स्टेटमेंट और क्रेडिट रिपोर्ट की नियमित रूप से समीक्षा करें ताकि किसी भी धोखाधड़ी वाले लेनदेन का पता चल सके।

Data Breaches

डेटा उल्लंघन एक सुरक्षा घटना है जिसमें गोपनीय या संवेदनशील जानकारी को किसी अनधिकृत व्यक्ति या समूह द्वारा एक्सेस, उजागर या चोरी किया जाता है। उल्लंघन दुर्भावनापूर्ण साइबर हमलों या मानवीय त्रुटि के कारण हो सकते हैं, जैसे कि किसी कर्मचारी द्वारा गलती से डेटा उजागर कर देना।

डेटा उल्लंघन के सामान्य कारण

- **साइबर हमले:** दुर्भावनापूर्ण बाहरी लोग नेटवर्क और सिस्टम में घुसपैठ करने के लिए विभिन्न तरीकों का इस्तेमाल करते हैं। इनमें शामिल हैं:
  - **फ़िशिंग और सोशल इंजीनियरिंग:** व्यक्तियों को नकली ईमेल या वेबसाइटों के माध्यम से क्रेडेंशियल या अन्य संवेदनशील जानकारी प्रकट करने के लिए प्रेरित करना।
  - **मैलवेयर और रैंसमवेयर:** संचालन को बाधित करने, डेटा चोरी करने, या फिरौती के लिए डेटा को बंधक बनाने के लिए दुर्भावनापूर्ण सॉफ़्टवेयर तैनात करना।
  - **क्रेडेंशियल चोरी:** ब्रूट-फ़ोर्स हमलों या अन्य उल्लंघनों से चोरी हुए क्रेडेंशियल्स का उपयोग करके लॉगिन विवरण से समझौता करना।
- **मानवीय त्रुटि और आंतरिक खतरे:** सभी उल्लंघन दुर्भावनापूर्ण नहीं होते हैं। अनजाने में हुई गलतियाँ, जैसे किसी गलत व्यक्ति को संवेदनशील जानकारी ईमेल करना, या एक दुर्भावनापूर्ण अंदरूनी व्यक्ति जो जानबूझकर डेटा लीक करता है, सामान्य कारण हैं।
- **सिस्टम की कमजोरियाँ:** हमलावर एक्सेस हासिल करने के लिए सॉफ़्टवेयर, हार्डवेयर या नेटवर्क सुरक्षा में कमजोरियों का फायदा उठाते हैं। सुरक्षा पैच को तुरंत इंस्टॉल करने में विफलता एक बड़ा जोखिम है।
- **तृतीय-पक्ष विक्रेता:** कई संगठन सेवाओं के लिए तृतीय-पक्ष विक्रेताओं पर निर्भर रहते हैं। यदि किसी विक्रेता की सुरक्षा कमजोर है, तो यह हमलावरों के लिए मुख्य कंपनी के नेटवर्क तक पहुँचने का एक प्रवेश द्वार बन सकता है।

डेटा उल्लंघन के परिणाम

- **वित्तीय नुकसान:** संगठनों को भारी लागत का सामना करना पड़ता है, जिसमें नियामक जुर्माना, वर्ग-कार्रवाई मुकदमों से कानूनी शुल्क, और ग्राहकों के लिए मुआवजा शामिल है।
- **प्रतिष्ठा को नुकसान:** एक उल्लंघन ग्राहक के विश्वास को कम कर सकता है और कंपनी की सार्वजनिक छवि को महत्वपूर्ण नुकसान पहुँचा सकता है।
- **व्यक्तिगत प्रभाव:** जिन व्यक्तियों का डेटा उजागर होता है, उन्हें घटना के बाद वर्षों तक पहचान की चोरी, वित्तीय धोखाधड़ी और अन्य अपराधों का खतरा होता है।
- **परिचालन में व्यवधान:** उल्लंघनों के कारण कंपनियों को जांच और रिकवरी के लिए सिस्टम को ऑफ़लाइन लेना पड़ सकता है, जिससे व्यवसाय का नुकसान और उत्पादकता में कमी हो सकती है।

हाल के और बड़े पैमाने के उल्लेखनीय उल्लंघन

- **चीनी निगरानी डेटाबेस (जून 2025):** सबसे बड़ा डेटा लीक, जिसमें करोड़ों चीनी नागरिकों की व्यक्तिगत और वित्तीय जानकारी सहित 4 अरब रिकॉर्ड उजागर हुए।
- **एटी एंड टी (मार्च 2024):** 2019 के एक डेटा सेट को डार्क वेब पर जारी किया गया, जिससे 70 मिलियन से अधिक वर्तमान और पूर्व ग्राहक प्रभावित हुए।
- **23एंडमी (पतन 2023):** हैकरों ने "क्रेडेंशियल स्टफिंग" का उपयोग करके 6.9 मिलियन उपयोगकर्ताओं के डेटा तक पहुँच प्राप्त की, जिसमें अत्यधिक व्यक्तिगत आनुवंशिक और वंश संबंधी जानकारी शामिल थी।

अपनी और अपने डेटा की सुरक्षा कैसे करें

व्यक्तियों के लिए, डेटा उल्लंघनों से होने वाले नुकसान के जोखिम को कम करने के लिए सक्रिय उपाय महत्वपूर्ण हैं:

- **मजबूत, अद्वितीय पासवर्ड और एक पासवर्ड मैनेजर का उपयोग करें।** एकाधिक साइटों पर पासवर्ड का पुन: उपयोग करने से बचें।
- **मल्टी-फैक्टर ऑथेंटिकेशन (एमएफए) सक्षम करें।** यह सुरक्षा की एक महत्वपूर्ण परत जोड़ता है।
- **फ़िशिंग घोटालों से सावधान रहें।** व्यक्तिगत जानकारी मांगने वाले अप्रत्याशित ईमेल या टेक्स्ट से सावधान रहें। कभी भी संदिग्ध लिंक पर क्लिक न करें।
- **अप-टू-डेट रहें।** अपने सभी सॉफ़्टवेयर और ऑपरेटिंग सिस्टम को नवीनतम सुरक्षा पैच के साथ अपडेट रखें।
- **अपने उपकरणों को एन्क्रिप्ट करें।** डिवाइस के खो जाने या चोरी हो जाने पर डेटा की सुरक्षा के लिए अपने लैपटॉप और स्मार्टफोन पर एन्क्रिप्शन का उपयोग करें।
- **अपने क्रेडिट की निगरानी करें।** किसी बड़े उल्लंघन के बाद, प्रमुख क्रेडिट ब्यूरो के साथ धोखाधड़ी अलर्ट या क्रेडिट फ्रीज लगाना बुद्धिमानी है।
- **जांचें कि क्या आपका डेटा खतरे में है।** यह देखने के लिए कि क्या आपका ईमेल पता सार्वजनिक डेटा उल्लंघनों में दिखाई दिया है, **हैव आई बीन पॉन्ड** जैसी सेवाओं का उपयोग करें।

Ethical online behaviour

Ethical online behavior involves acting with respect, honesty, and integrity in the digital world by protecting others' privacy, respecting intellectual property, and not engaging in harmful activities like cyberbullying or theft. It includes being a responsible digital citizen by safeguarding your own information, communicating considerately, thinking before you post, and reporting illegal activities when you see them.

Importance of ethical online behaviour

Ethical online behaviour is crucial for building trust, protecting your reputation, and fostering a respectful digital environment. It prevents harm from things like cyberbullying and misinformation, ensures fair treatment, and promotes responsible use of technology and data. Ultimately, it creates a safer and more positive online community for everyone.

Key reasons why ethical online behavior is important:

- **Builds trust and credibility:**
  Acting ethically builds trust with other users and organizations, which is fundamental for positive online interactions.
- **Protects reputation:**
  Maintaining good online conduct helps preserve your personal and professional reputation, while unethical actions can cause lasting damage.
- **Fosters a positive environment:**
  Ethical behavior encourages respect and fairness, which is essential for creating a welcoming and inclusive online space for everyone.
- **Prevents harm:**
  It helps to prevent the spread of misinformation and protect individuals from harm, such as cyberbullying or data breaches.
- **Encourages responsibility:**
  Being ethical means taking responsibility for your actions online, including the use of data, respecting intellectual property, and considering the impact of your digital footprint.
- **Ensures privacy and security:**
  Ethical practices include respecting others' privacy, protecting your own personal information, and being mindful of data security.
- **Promotes fairness and equity:**

Ethical considerations ensure that technology and its use are fair and benefit everyone, rather than exacerbating existing inequalities.

- **Leads to legal and social consequences:**
  Unethical actions online can have serious consequences, including legal penalties and social isolation.

ऑनलाइन नैतिक व्यवहार (Ethical online behaviour)

ऑनलाइन नैतिक व्यवहार का मतलब है इंटरनेट का उपयोग करते समय स्वीकार्य और सम्मानजनक तरीके से पेश आना। इसमें ईमानदार रहना, दूसरों के अधिकारों और संपत्ति का सम्मान करना, और दूसरों के प्रति दयालु और विचारशील होना शामिल है। यह नियमों का एक समूह है जो ऑनलाइन बातचीत को सुरक्षित और सकारात्मक बनाता है।

Importance of ethical online behaviour

विश्वास का निर्माण करने, अपनी प्रतिष्ठा की रक्षा करने और एक सम्मानजनक डिजिटल वातावरण को बढ़ावा देने के लिएनैतिक ऑनलाइन व्यवहार महत्वपूर्ण है । यह साइबर धमकी और गलत सूचना जैसी चीजों से होने वाले नुकसान को रोकता है, निष्पक्ष व्यवहार सुनिश्चित करता है, तथा प्रौद्योगिकी और डेटा के जिम्मेदार उपयोग को बढ़ावा देता है। अंततः, यह सभी के लिए एक सुरक्षित और अधिक सकारात्मक ऑनलाइन समुदाय का निर्माण करता है।

नैतिक ऑनलाइन व्यवहार महत्वपूर्ण क्यों है इसके प्रमुख कारण:

- **विश्वास और विश्वसनीयता का निर्माण:**

  नैतिक रूप से कार्य करने से अन्य उपयोगकर्ताओं और संगठनों के साथ विश्वास का निर्माण होता है, जो सकारात्मक ऑनलाइन बातचीत के लिए मौलिक है।

- **प्रतिष्ठा की रक्षा:**

  अच्छा ऑनलाइन आचरण बनाए रखने से आपकी व्यक्तिगत और व्यावसायिक प्रतिष्ठा को बनाए रखने में मदद मिलती है, जबकि अनैतिक कार्य स्थायी क्षति का कारण बन सकते हैं।

- **सकारात्मक वातावरण को बढ़ावा देता है:**

  नैतिक व्यवहार सम्मान और निष्पक्षता को प्रोत्साहित करता है, जो सभी के लिए स्वागतयोग्य और समावेशी ऑनलाइन स्थान बनाने के लिए आवश्यक है।

- **नुकसान से बचाता है:**

  यह गलत सूचना के प्रसार को रोकने और व्यक्तियों को साइबर धमकी या डेटा उल्लंघन जैसे नुकसान से बचाने में मदद करता है।

- **जिम्मेदारी को प्रोत्साहित करता है:**

  नैतिक होने का अर्थ है अपने ऑनलाइन कार्यों की जिम्मेदारी लेना, जिसमें डेटा का उपयोग, बौद्धिक संपदा का सम्मान करना और अपने डिजिटल पदचिह्न के प्रभाव पर विचार करना शामिल है।

- **गोपनीयता और सुरक्षा सुनिश्चित करता है:**

  नैतिक आचरण में दूसरों की गोपनीयता का सम्मान करना, अपनी व्यक्तिगत जानकारी की सुरक्षा करना तथा डेटा सुरक्षा के प्रति सचेत रहना शामिल है।

- **निष्पक्षता और समानता को बढ़ावा देता है:**

  नैतिक विचार यह सुनिश्चित करते हैं कि प्रौद्योगिकी और उसका उपयोग निष्पक्ष हो तथा सभी को लाभ पहुंचाए, न कि मौजूदा असमानताओं को बढ़ाए।

- **कानूनी और सामाजिक परिणाम उत्पन्न होते हैं:**

ऑनलाइन अनैतिक कार्यों के गंभीर परिणाम हो सकते हैं, जिनमें कानूनी दंड और सामाजिक अलगाव शामिल हैं।

Importance of privacy

Privacy is important because it protects individuals from surveillance, harm like identity theft and fraud, and allows for freedom of expression and personal development. It is a fundamental right that is crucial for human dignity, safety, and self-determination, enabling other rights like freedom of thought, assembly, and association. For organizations, it is essential for building customer trust and maintaining a good reputation.

For individuals

- **Protection from harm:**
  Privacy shields you from risks like identity theft, fraud, financial loss, reputational damage, and emotional distress that can arise from the misuse of personal data.
- **Freedom of expression and thought:**
  It provides a space for developing your own personality and beliefs without fear of government or private entity surveillance. This is essential for freedom of speech, religion, and association.
- **Personal autonomy:**
  Privacy allows you to make personal choices without undue influence or scrutiny. This includes personal beliefs like political views, which can be shared confidentially.
- **Human dignity:**
  It is a key component of human dignity, allowing individuals to maintain control over their personal lives and information.

For organizations

- **Building trust:**
  Demonstrating a commitment to data privacy helps build and maintain trust with customers who are increasingly cautious about sharing their information.
- **Reputation management:**
  Protecting customer data and respecting their privacy helps organizations build a positive reputation and avoid the negative consequences of data breaches.
- **Ethical responsibility:**
  Organizations have an ethical and legal responsibility to handle personal information securely and transparently, which builds a more trustworthy relationship with users.

Broader societal impacts

- **Democratic foundation:**
  Privacy is a cornerstone of a democratic society, enabling citizens to participate freely in public life and hold their governments accountable.
- **Public trust:**
  Failing to respect privacy can lead to a breakdown of public trust in both government and organizations, which can have a negative impact on their effectiveness and the achievement of their goals.

Importance of privacy

गोपनीयता महत्वपूर्ण है क्योंकि यह व्यक्तियों को निगरानी, पहचान की चोरी और धोखाधड़ी जैसे नुकसान से बचाती है, तथा अभिव्यक्ति की स्वतंत्रता और व्यक्तिगत विकास की अनुमति देती है। यह एक मौलिक अधिकार है जो मानव गरिमा, सुरक्षा और आत्मनिर्णय के लिए महत्वपूर्ण है, तथा विचार, एकत्रीकरण और संगठन की स्वतंत्रता जैसे अन्य अधिकारों को सक्षम बनाता है। संगठनों के लिए, ग्राहक विश्वास का निर्माण करना और अच्छी प्रतिष्ठा बनाए रखना आवश्यक है।

व्यक्तियों के लिए

- **नुकसान से सुरक्षा**:
  गोपनीयता आपको पहचान की चोरी, धोखाधड़ी, वित्तीय हानि, प्रतिष्ठा को नुकसान, तथा भावनात्मक संकट जैसे जोखिमों से बचाती है, जो व्यक्तिगत डेटा के दुरुपयोग से उत्पन्न हो सकते हैं।

- **अभिव्यक्ति और विचार की स्वतंत्रता:**

  यह सरकार या निजी संस्थाओं की निगरानी के डर के बिना आपके अपने व्यक्तित्व और विश्वासों को विकसित करने के लिए एक स्थान प्रदान करता है। यह अभिव्यक्ति, धर्म और संघ की स्वतंत्रता के लिए आवश्यक है।

- **व्यक्तिगत स्वायत्तता:**

  गोपनीयता आपको बिना किसी अनुचित प्रभाव या जांच के व्यक्तिगत निर्णय लेने की अनुमति देती है। इसमें राजनीतिक विचार जैसे व्यक्तिगत विश्वास भी शामिल हैं, जिन्हें गोपनीय रूप से साझा किया जा सकता है।

- **मानवीय गरिमा:**

  यह मानव गरिमा का एक प्रमुख घटक है, जो व्यक्तियों को अपने व्यक्तिगत जीवन और जानकारी पर नियंत्रण बनाए रखने की अनुमति देता है।

संगठनों के लिए

- **विश्वास निर्माण:**

  डेटा गोपनीयता के प्रति प्रतिबद्धता प्रदर्शित करने से उन ग्राहकों के साथ विश्वास बनाने और उसे बनाए रखने में मदद मिलती है, जो अपनी जानकारी साझा करने के बारे में अधिक सतर्क हो रहे हैं।

- **प्रतिष्ठा प्रबंधन:**

  ग्राहक डेटा की सुरक्षा और उनकी गोपनीयता का सम्मान करने से संगठनों को सकारात्मक प्रतिष्ठा बनाने और डेटा उल्लंघनों के नकारात्मक परिणामों से बचने में मदद मिलती है।

- **नैतिक जिम्मेदारी:**

  संगठनों की नैतिक और कानूनी जिम्मेदारी है कि वे व्यक्तिगत जानकारी को सुरक्षित और पारदर्शी तरीके से संभालें, जिससे उपयोगकर्ताओं के साथ अधिक भरोसेमंद संबंध बनते हैं।

व्यापक सामाजिक प्रभाव

- **लोकतांत्रिक आधार:**

  गोपनीयता लोकतांत्रिक समाज की आधारशिला है, जो नागरिकों को सार्वजनिक जीवन में स्वतंत्र रूप से भाग लेने और अपनी सरकारों को जवाबदेह बनाने में सक्षम बनाती है।

- **लोगों का विश्वास:**

  गोपनीयता का सम्मान न करने से सरकार और संगठनों दोनों में जनता का विश्वास टूट सकता है, जिसका उनकी प्रभावशीलता और लक्ष्यों की प्राप्ति पर नकारात्मक प्रभाव पड़ सकता है।

Digital footprints

A digital footprint is the trail of data left behind from a person's online activities, including browsing history, social media posts, and online purchases. This footprint can be "active," meaning data you intentionally share (like posting on social media), or "passive," which is data collected without your active input, such as cookies or your IP address. The accumulation of these actions creates a unique online identity that can be difficult to alter and is important to manage for privacy and security.

डिजिटल फुटप्रिंट किसी व्यक्ति की ऑनलाइन गतिविधियों से बचा हुआ डेटा है, जिसमें ब्राउज़िंग इतिहास, सोशल मीडिया पोस्ट और ऑनलाइन खरीदारी शामिल हैं। यह पदचिह्न "सक्रिय" हो सकता है, जिसका अर्थ है वह डेटा जिसे आप जानबूझकर साझा करते हैं (जैसे सोशल मीडिया पर पोस्ट करना), या "निष्क्रिय", जो आपके सक्रिय इनपुट के बिना एकत्र किया गया डेटा है, जैसे कुकीज़ या आपका आईपी पता। इन कार्यों के संचय से एक अद्वितीय ऑनलाइन पहचान बनती है, जिसे बदलना कठिन हो सकता है तथा गोपनीयता और सुरक्षा के लिए इसका प्रबंधन करना महत्वपूर्ण है।

Digital footprint – meaning and definition

A digital footprint – sometimes called a digital shadow or an electronic footprint – refers to the trail of data you leave when using the internet. It includes websites you visit, emails you send, and information you submit online. A digital footprint can be used to track a person's online activities and devices. Internet users create their digital footprint either actively or passively.

What is a digital footprint?

Whenever you use the internet, you leave behind a trail of information known as your digital footprint. A digital footprint grows in many ways – for example, posting on social media, subscribing to a newsletter, leaving an online review, or shopping online.

Sometimes, it's not always obvious that you are contributing to your digital footprint. For example, websites can track your activity by installing cookies on your device, and apps can collate your data without you knowing it. Once you allow an organization to access your information, they could sell or share your data with third parties. Worse still, your personal information could be compromised as part of a data breach.

You often hear the terms 'active' and 'passive' in relation to digital footprints:

Active digital footprints

An active digital footprint is where the user has deliberately shared information about themselves – for example, through posting or participating on social networking sites or online forums. If a user is logged into a website through a registered username or profile, any posts they make form part of their active digital footprint. Other activities that contribute to active digital footprints include completing an online form – such as subscribing to a newsletter – or agreeing to accept cookies on your browser.

Passive digital footprints

A passive digital footprint is created when information is collected about the user without them being aware that this is happening. For example, this occurs when websites collect information about how many times users visit, where they come from, and their IP address. This is a hidden process, which users may not realize is taking place. Other examples of passive footprints include social networking sites and advertisers using your likes, shares, and comments to profile you and target you with specific content.

Digital footprint examples

An internet user could have hundreds of items form part of their digital footprint. Some of the ways in which users add to their digital footprint include:

Online shopping

- Making purchases from e-commerce websites
- Signing up for coupons or creating an account
- Downloading and using shopping apps
- Registering for brand newsletters

Online banking

- Using a mobile banking app
- Buying or selling stocks
- Subscribing to financial publications and blogs
- Opening a credit card account

Social media

- Using social media on your computer or devices
- Logging into other websites using your social media credentials
- Connecting with friends and contacts
- Sharing information, data, and photos with your connections
- Joining a dating site or app

Reading the news

- Subscribing to an online news source
- Viewing articles on a news app
- Signing up for a publication's newsletter
- Reposting articles and information you read

Health and fitness

- Using fitness trackers
- Using apps to receive healthcare
- Registering your email address with a gym
- Subscribing to health and fitness blogs

Protect your digital footprint

Because employers, colleges, and others can look up your online identity, it's a good idea to be mindful of your digital footprint. Here are some tips for protecting your personal data and managing your online reputation.

Use search engines to check your digital footprint

Enter your name into search engines. Include your first and last name and any variations on spellings. If you have changed your name, search for both current and former names. Reviewing the search engine results will give you a sense of what information about you is publicly available. If any of the results show you in a negative light, you could contact the site administrator to see if they can remove it. Setting up Google Alerts is one way to keep an eye on your name.

Reduce the number of information sources that mention you

For example, real estate websites and whitepages.com may have more information about you than you may wish. These sites can often include personal information like your phone number, address, and age. If you are not comfortable with this, you can contact the websites and request that the information is removed.

Limit the amount of data you share

Every time you provide your personal information to an organization, you widen your digital footprint. You also increase the possibility that one of the organizations storing your data will misuse it or suffer a breach, putting your data in the wrong hands. So, before you submit that form, consider if it's worth it. Are there other ways to obtain that information or service without sharing your data?

Double-check your privacy settings

Privacy settings on social media allow you to control who sees your posts. Review these settings and ensure they are set to a level you are comfortable with. For example, Facebook allows you to limit posts to friends and make customized lists of people who can see certain posts. However, bear in mind that privacy settings only protect you on the relevant social media site.

Avoid oversharing on social media

Social media makes it easy to connect with others but can also make oversharing easy. Think twice before revealing your location or travel plans, or other personal information. Avoid disclosing your phone number or email address in your social media bio. It's also a good idea to avoid 'liking' your own bank, healthcare provider, pharmacy, etc. – as this can lead cybercriminals to your critical accounts.

Avoid unsafe websites

Make sure you're transacting with a secure website – the URL should start with https:// rather than http:// - the "s" stands for "secure" and indicates that the site has a security certificate. There should also be a padlock

icon to the left of the address bar. Never share any confidential information on unsecured sites, especially payment details.

Avoid disclosing private data on public Wi-Fi

A public Wi-Fi network is inherently less secure than your personal one since you don't know who set it up or who else might be watching. Avoid sending personal information when using public Wi-Fi networks.

Delete old accounts

One way to reduce your digital footprint is by deleting old accounts – for example, social media profiles you no longer use or newsletter subscriptions you no longer read. Getting rid of dormant accounts minimizes your exposure to potential data breaches.

Create strong passwords and use a password manager

A strong password will help you maintain internet security. A strong password is long – made up of at least 12 characters and ideally more – and contains a mix of upper- and lower-case letters plus symbols and numbers. The more complex and involved your password, the harder it is to crack. Using a password manager will help generate, store, and manage all your passwords in one secure online account. Keep your passwords private – avoid sharing them with others or writing them down. Try to avoid using the same password for all your accounts, and remember to change them regularly.

Keep an eye on your medical records

Practice good data hygiene by periodically reviewing your medical records. Identity thieves target medical and health information as well as financial data. When criminals use your personal information to obtain medical treatment in your name, their health records can become intertwined with your own.

Don’t log in with Facebook

Logging into websites and apps using Facebook is convenient. However, every time you sign into a third-party website using your Facebook credentials, you give that company permission to mine your Facebook user data – potentially placing your personal information at risk.

Keep software up to date

Outdated software could house a wealth of digital footprints. Without the latest updates, cybercriminals could gain access to this information. Cybercriminals can easily access a victim’s devices and data by exploiting vulnerabilities in software. You can help prevent this by keeping your software up to date. Older software can be more vulnerable to attacks by hackers.

Review your mobile use

Set a passcode for your mobile device so that it can't be accessed by other people if you lose it. When installing an app, read the user agreement. Many apps disclose what kind of information they collect and what it may be used for. These apps may mine personal data like your email, location, and online activities. Check that you are comfortable with the information being shared before you use the app.

Think before you post

What you post or say online sends a message about who you are, as does what others reveal about you. Aspects of your digital footprint, such as uploaded photographs, blog comments, YouTube videos, and Facebook posts, might not portray the way you would like to be seen. Create a positive digital footprint by posting only those things that contribute to the image of you that you want others to see.

Act fast after a breach: If you suspect your data might have been compromised in a breach, take action immediately. If a financial loss is involved, contact your bank or credit card provider to report the breach. Change any passwords that might have been exposed. If it's a password you have used for other accounts, update it across the board.

Use a VPN

Using a virtual private network, or VPN, can help safeguard your digital footprint. This is because VPNs mask your IP address which makes your online actions virtually untraceable. This protects your privacy online and can prevent websites from installing cookies that track your internet browsing history. Kaspersky Secure Connection enables you to have a secure connection between your device and an internet server that no one can monitor or access the data you are exchanging.

Importance of digital footprints

Digital footprints are important because they shape your online reputation, affect your privacy and security, and can lead to personal and professional opportunities or risks. A positive digital footprint can help with job prospects and personal branding, while a negative one can lead to cybercrimes, lost opportunities, and privacy concerns.

Impact of a digital footprint

- **Online reputation:**
  Your digital footprint builds your online reputation, which can be viewed by potential employers, clients, and partners. A positive footprint showcasing achievements and professionalism can enhance your reputation, while a negative one can harm it.
- **Personal and professional opportunities:**
  A well-managed digital footprint can open doors to career advancement, new collaborations, and business opportunities. Conversely, a negative one can limit job prospects and partnerships.
- **Privacy and security risks:**
  Your digital footprint can reveal personal information, making you vulnerable to cybercriminals who might use it for theft, scams, or targeted attacks like spear phishing. This includes data breaches that expose sensitive information on the dark web.
- **Targeted advertising:**
  Companies use your digital footprint to gather data for targeted advertising, which can feel like an invasion of privacy.
- **Personal branding:**
  Your online activity, posts, and interactions contribute to your personal brand, influencing how you are perceived by others. Managing it helps you present yourself in a way that aligns with your goals.

Importance of digital footprints

डिजिटल फुटप्रिंट महत्वपूर्ण हैं क्योंकि वे आपकी ऑनलाइन प्रतिष्ठा को आकार देते हैं, आपकी गोपनीयता और सुरक्षा को प्रभावित करते हैं, और व्यक्तिगत और व्यावसायिक अवसरों या जोखिमों को जन्म दे सकते हैं। सकारात्मक डिजिटल पदचिह्न नौकरी की संभावनाओं और व्यक्तिगत ब्रांडिंग में मदद कर सकता है, जबकि नकारात्मक पदचिह्न साइबर अपराध, खोए हुए अवसर और गोपनीयता संबंधी चिंताओं को जन्म दे सकता है।

डिजिटल पदचिह्न का प्रभाव

- **ऑनलाइन प्रतिष्ठा:**

  आपका डिजिटल पदचिह्न आपकी ऑनलाइन प्रतिष्ठा का निर्माण करता है, जिसे संभावित नियोक्ता, ग्राहक और साझेदार देख सकते हैं। उपलब्धियों और व्यावसायिकता को प्रदर्शित करने वाली सकारात्मक छवि आपकी प्रतिष्ठा को बढ़ा सकती है, जबकि नकारात्मक छवि इसे नुकसान पहुंचा सकती है।

- **व्यक्तिगत और व्यावसायिक अवसर:**

  एक अच्छी तरह से प्रबंधित डिजिटल पदचिह्न कैरियर में उन्नति, नए सहयोग और व्यावसायिक अवसरों के द्वार खोल सकता है। इसके विपरीत, नकारात्मक दृष्टिकोण नौकरी की संभावनाओं और साझेदारी को सीमित कर सकता है।

- **गोपनीयता और सुरक्षा जोखिम:**

  आपका डिजिटल फुटप्रिंट आपकी व्यक्तिगत जानकारी को उजागर कर सकता है, जिससे आप साइबर अपराधियों के लिए असुरक्षित हो सकते हैं, जो इसका उपयोग चोरी, घोटाले या स्पीयर फिशिंग जैसे लक्षित हमलों के लिए कर सकते हैं। इसमें डेटा उल्लंघन शामिल है जो डार्क वेब पर संवेदनशील जानकारी को उजागर करता है।

- **लक्षित विज्ञापन:**

  कंपनियां लक्षित विज्ञापन के लिए डेटा एकत्र करने हेतु आपके डिजिटल फुटप्रिंट का उपयोग करती हैं, जो गोपनीयता के उल्लंघन जैसा लग सकता है।

- **व्यक्तिगत ब्रांडिंग:**

  आपकी ऑनलाइन गतिविधि, पोस्ट और अंतर्क्रियाएं आपके व्यक्तिगत ब्रांड में योगदान करती हैं, तथा यह प्रभावित करती हैं कि दूसरे लोग आपको किस रूप में देखते हैं। इसे प्रबंधित करने से आपको अपने लक्ष्यों के अनुरूप स्वयं को प्रस्तुत करने में मदद मिलती है।

अपने डिजिटल पदचिह्न का प्रबंधन

- आप ऑनलाइन क्या साझा करते हैं, इस पर ध्यान दें और नियमित रूप से अपने सार्वजनिक प्रोफाइल की समीक्षा करें।
- अपने खातों को हैकिंग से बचाने के लिए मजबूत, अद्वितीय पासवर्ड का उपयोग करें।
- अपनी ऑनलाइन उपस्थिति पर नजर रखें ताकि ऐसी कोई नकारात्मक सामग्री न दिखे जो आपकी प्रतिष्ठा को नुकसान पहुंचा सकती हो।
- गोपनीयता सेटिंग्स और अपने डेटा को सुरक्षित रखने के बारे में स्वयं को शिक्षित करें।

डिजिटल फ़ुटप्रिंट – अर्थ और परिभाषा

डिजिटल फ़ुटप्रिंट (जिसे डिजिटल शैडो या इलेक्ट्रॉनिक फ़ुटप्रिंट भी कहा जाता है) उस डेटा के निशान को कहते हैं जो आप इंटरनेट का उपयोग करते समय छोड़ते हैं। इसमें वे वेबसाइटें शामिल होती हैं जिन्हें आप देखते हैं, ईमेल जो आप भेजते हैं, और वह जानकारी जो आप ऑनलाइन साझा करते हैं। डिजिटल फ़ुटप्रिंट का उपयोग किसी व्यक्ति की ऑनलाइन गतिविधियों और उसके डिवाइस को ट्रैक करने के लिए किया जा सकता है। इंटरनेट उपयोगकर्ता अपना डिजिटल फ़ुटप्रिंट **सक्रिय (Active)** या **निष्क्रिय (Passive)** रूप से बनाते हैं।

डिजिटल फ़ुटप्रिंट क्या है?

जब भी आप इंटरनेट का उपयोग करते हैं, आप अपने पीछे जानकारी का एक निशान छोड़ते हैं, जिसे डिजिटल फ़ुटप्रिंट कहा जाता है। सोशल मीडिया पर पोस्ट करना, न्यूज़लेटर सब्सक्राइब करना, ऑनलाइन रिव्यू लिखना या ऑनलाइन खरीदारी करना—ये सभी आपके डिजिटल फ़ुटप्रिंट को बढ़ाते हैं।

कई बार यह स्पष्ट नहीं होता कि आप अपना डिजिटल फ़ुटप्रिंट बना रहे हैं। उदाहरण के लिए, वेबसाइटें आपके डिवाइस पर कुकीज़ इंस्टॉल करके आपकी गतिविधियों को ट्रैक कर सकती हैं, और ऐप्स आपकी जानकारी आपकी जानकारी के बिना भी इकट्ठा कर सकते हैं। जब आप किसी संगठन को अपनी जानकारी एक्सेस करने की अनुमति देते हैं, तो वे आपकी जानकारी को तीसरे पक्ष के साथ साझा या बेच सकते हैं। इससे भी गंभीर स्थिति तब होती है जब डेटा ब्रीच के कारण आपकी निजी जानकारी लीक हो जाती है।

डिजिटल फ़ुटप्रिंट के प्रकार

डिजिटल फ़ुटप्रिंट के संदर्भ में अक्सर **सक्रिय (Active)** और **निष्क्रिय (Passive)** शब्दों का उपयोग किया जाता है।

1. सक्रिय डिजिटल फ़ुटप्रिंट (Active Digital Footprint)

सक्रिय डिजिटल फ़ुटप्रिंट तब बनता है जब उपयोगकर्ता जानबूझकर अपनी जानकारी साझा करता है। उदाहरण:

- सोशल मीडिया या ऑनलाइन फ़ोरम पर पोस्ट करना
- किसी वेबसाइट पर लॉग-इन होकर कमेंट करना
- न्यूज़लेटर के लिए ऑनलाइन फ़ॉर्म भरना
- ब्राउज़र में कुकीज़ स्वीकार करना

ये सभी गतिविधियाँ आपके सक्रिय डिजिटल फ़ुटप्रिंट का हिस्सा बनती हैं।

2. निष्क्रिय डिजिटल फ़ुटप्रिंट (Passive Digital Footprint)

निष्क्रिय डिजिटल फ़ुटप्रिंट तब बनता है जब आपकी जानकारी आपकी जानकारी के बिना इकट्ठा की जाती है। उदाहरण:

- वेबसाइट द्वारा यह ट्रैक करना कि आप कितनी बार विज़िट करते हैं
- आप कहाँ से आए हैं और आपका IP एड्रेस
- सोशल मीडिया और विज्ञापन कंपनियों द्वारा आपके लाइक, शेयर और कमेंट के आधार पर आपकी प्रोफाइल बनाना और टार्गेटिड कंटेंट दिखाना

यह एक छुपी हुई प्रक्रिया होती है, जिसका उपयोगकर्ता को अक्सर पता नहीं होता।

डिजिटल फ़ुटप्रिंट के उदाहरण

एक इंटरनेट उपयोगकर्ता के डिजिटल फ़ुटप्रिंट में सैकड़ों जानकारियाँ शामिल हो सकती हैं। नीचे कुछ सामान्य उदाहरण दिए गए हैं:

ऑनलाइन शॉपिंग

- ई-कॉमर्स वेबसाइट्स से खरीदारी करना
- कूपन के लिए साइन अप करना या अकाउंट बनाना
- शॉपिंग ऐप डाउनलोड और उपयोग करना
- ब्रांड न्यूज़लेटर के लिए रजिस्टर करना

ऑनलाइन बैंकिंग

- मोबाइल बैंकिंग ऐप का उपयोग करना
- शेयर खरीदना या बेचना
- वित्तीय ब्लॉग या पत्रिकाओं को सब्सक्राइब करना
- क्रेडिट कार्ड अकाउंट खोलना

सोशल मीडिया

- कंप्यूटर या मोबाइल पर सोशल मीडिया का उपयोग करना
- सोशल मीडिया अकाउंट से अन्य वेबसाइटों में लॉग-इन करना
- दोस्तों और संपर्कों से जुड़ना
- जानकारी, डेटा और फ़ोटो साझा करना
- डेटिंग वेबसाइट या ऐप से जुड़ना

समाचार पढ़ना

- ऑनलाइन न्यूज़ वेबसाइट सब्सक्राइब करना

- न्यूज़ ऐप पर लेख पढ़ना
- न्यूज़लेटर के लिए साइन अप करना
- पढ़े गए लेखों को दोबारा शेयर करना

स्वास्थ्य और फ़िटनेस

- फ़िटनेस ट्रैकर का उपयोग करना
- हेल्थकेयर ऐप्स का इस्तेमाल करना
- जिम में ईमेल रजिस्टर कराना
- स्वास्थ्य और फ़िटनेस ब्लॉग सब्सक्राइब करना

अपने डिजिटल फ़ुटप्रिंट की सुरक्षा करें

क्योंकि नियोक्ता, कॉलेज और अन्य लोग आपकी ऑनलाइन पहचान देख सकते हैं, इसलिए अपने डिजिटल फ़ुटप्रिंट के प्रति सजग रहना बहुत ज़रूरी है। नीचे आपके व्यक्तिगत डेटा की सुरक्षा और ऑनलाइन प्रतिष्ठा को बेहतर ढंग से प्रबंधित करने के लिए कुछ सुझाव दिए गए हैं।

1. सर्च इंजन से अपना डिजिटल फ़ुटप्रिंट जाँचें

अपने नाम को सर्च इंजन में डालें। पहले और आख़िरी नाम के साथ-साथ नाम की अलग-अलग वर्तनी भी खोजें। यदि आपने कभी नाम बदला है, तो पुराने और नए दोनों नाम खोजें। इससे आपको पता चलेगा कि आपके बारे में कौन-सी जानकारी सार्वजनिक रूप से उपलब्ध है। यदि कोई जानकारी नकारात्मक लगे, तो आप वेबसाइट के एडमिनिस्ट्रेटर से उसे हटाने का अनुरोध कर सकते हैं। अपने नाम पर नज़र रखने के लिए Google Alerts सेट करना भी एक अच्छा तरीका है।

2. आपके बारे में जानकारी देने वाले स्रोतों की संख्या कम करें

कुछ वेबसाइटें (जैसे रियल एस्टेट या पब्लिक रिकॉर्ड साइट्स) आपका फ़ोन नंबर, पता और उम्र जैसी निजी जानकारी दिखा सकती हैं। यदि आप इससे असहज हैं, तो आप उन वेबसाइटों से संपर्क कर जानकारी हटाने का अनुरोध कर सकते हैं।

3. साझा की जाने वाली जानकारी सीमित रखें

हर बार जब आप किसी संस्था को अपनी निजी जानकारी देते हैं, तो आपका डिजिटल फ़ुटप्रिंट बढ़ता है। इससे डेटा के दुरुपयोग या डेटा लीक का जोखिम भी बढ़ता है। फ़ॉर्म भरने से पहले सोचें—क्या यह ज़रूरी है? क्या बिना डेटा साझा किए वही सेवा मिल सकती है?

4. प्राइवेसी सेटिंग्स दोबारा जाँचें

सोशल मीडिया की प्राइवेसी सेटिंग्स से आप तय कर सकते हैं कि आपकी पोस्ट कौन देख सकता है। इन्हें नियमित रूप से जाँचें और अपने अनुसार सेट करें। ध्यान रखें कि ये सेटिंग्स केवल उसी प्लेटफ़ॉर्म पर लागू होती हैं।

5. सोशल मीडिया पर ज़रूरत से ज़्यादा साझा करने से बचें

अपना लोकेशन, यात्रा की योजना, फ़ोन नंबर या ईमेल शेयर करने से पहले सोचें। अपने बैंक, हेल्थकेयर या फ़ार्मेसी जैसे पेज "लाइक" करने से भी बचें, क्योंकि इससे साइबर अपराधी आपके अहम अकाउंट्स तक पहुँच सकते हैं।

6. असुरक्षित वेबसाइटों से बचें

किसी भी लेन-देन से पहले देखें कि वेबसाइट का URL **https://** से शुरू होता है और एड्रेस बार में ताले (🔒) का निशान है। असुरक्षित साइट्स पर कभी भी भुगतान या गोपनीय जानकारी न डालें।

7. पब्लिक Wi-Fi पर निजी जानकारी साझा न करें

पब्लिक Wi-Fi कम सुरक्षित होता है। ऐसे नेटवर्क पर संवेदनशील जानकारी भेजने से बचें।

8. पुराने अकाउंट्स हटाएँ

जिन सोशल मीडिया अकाउंट्स या सब्सक्रिप्शन का आप उपयोग नहीं करते, उन्हें डिलीट कर दें। इससे डेटा लीक का खतरा कम होता है।

9. मज़बूत पासवर्ड बनाएँ और पासवर्ड मैनेजर का उपयोग करें

मज़बूत पासवर्ड कम से कम 12 अक्षरों का होना चाहिए और उसमें बड़े-छोटे अक्षर, नंबर और चिन्ह शामिल हों। हर अकाउंट के लिए अलग पासवर्ड रखें और उन्हें सुरक्षित रखने के लिए पासवर्ड मैनेजर का उपयोग करें।

10. अपने मेडिकल रिकॉर्ड पर नज़र रखें

समय-समय पर अपने मेडिकल रिकॉर्ड की जाँच करें। पहचान चोर मेडिकल जानकारी को भी निशाना बनाते हैं, जिससे आपकी सेहत से जुड़ी जानकारी प्रभावित हो सकती है।

11. Facebook से लॉग-इन करने से बचें

थर्ड-पार्टी वेबसाइट्स या ऐप्स पर Facebook से लॉग-इन करने पर आप उन्हें अपना यूज़र डेटा एक्सेस करने की अनुमति दे देते हैं, जो जोखिम भरा हो सकता है।

12. सॉफ़्टवेयर अपडेट रखें

पुराना सॉफ़्टवेयर साइबर हमलों के लिए ज़्यादा असुरक्षित होता है। नियमित अपडेट से सुरक्षा खामियों को ठीक किया जाता है।

13. मोबाइल उपयोग की समीक्षा करें

अपने फ़ोन पर पासकोड लगाएँ। ऐप इंस्टॉल करते समय उसकी परमिशन और प्राइवेसी पॉलिसी पढ़ें और वही ऐप इस्तेमाल करें जिनसे आप सहज हों।

14. पोस्ट करने से पहले सोचें

आप जो ऑनलाइन पोस्ट करते हैं, वही आपकी पहचान बनाता है। फ़ोटो, कमेंट्स और पोस्ट ऐसी हों जो आपकी सकारात्मक छवि दिखाएँ।

15. डेटा ब्रीच के बाद तुरंत कार्रवाई करें

यदि आपको लगता है कि आपका डेटा लीक हो गया है, तो तुरंत बैंक या कार्ड कंपनी से संपर्क करें और सभी प्रभावित पासवर्ड बदलें।

16. VPN का उपयोग करें

VPN आपकी IP एड्रेस को छुपाता है और आपकी ऑनलाइन गतिविधियों को सुरक्षित बनाता है। इससे आपकी प्राइवेसी बढ़ती है और ट्रैकिंग से बचाव होता है।

Unit 5: Cyber Hygiene and Awareness Programs

Good cyber habits

Good cyber habits encompass a range of practices designed to protect personal information, devices, and online security. The habits you mentioned are indeed fundamental components of strong cybersecurity hygiene. Here's a breakdown of these essential good cyber habits and why they are important:

1. Regular Updates

Keeping your software, operating systems, and applications updated is a critical defense mechanism.

- **Why it's important:** Updates often include security patches that fix vulnerabilities discovered by developers. Cybercriminals actively exploit these known weaknesses to gain unauthorized access to systems.
- **How to practice it:** Enable automatic updates whenever possible for your operating system, web browsers, antivirus software, and other applications.

2. Virus Scanning (Antivirus/Anti-malware)

Using reliable security software and running regular scans helps detect and remove malicious software.

- **Why it's important:** Viruses, Trojans, ransomware, and other forms of malware can steal information, damage files, or take control of your device. A good security program acts as a vigilant guard.
- **How to practice it:** Install and maintain reputable antivirus or anti-malware software. Ensure real-time protection is active and schedule regular, full-system scans.

3. Data Backup

Regularly backing up your important data ensures you can recover it in the event of a system failure, accidental deletion, or a cyberattack like ransomware.

- **Why it's important:** Data loss can be devastating. Backups provide a safety net, allowing you to restore your files and minimize disruption.
- **How to practice it:** Follow the **3-2-1 rule**:
  - **3** copies of your data.
  - **2** different storage types (e.g., internal hard drive and external hard drive).
  - **1** copy stored off-site (e.g., cloud backup service or a secure location away from your home/office).

4. Link Safety

Practicing caution with links and attachments is a primary way to prevent phishing attacks and malware infections.

- **Why it's important:** Malicious links can lead to fake websites designed to steal login credentials or automatically download malware onto your device. Phishing remains one of the most common methods for cybercriminals to compromise accounts.
- **How to practice it:**
  - **Hover before you click:** On a computer, hover your mouse over a link to see the actual web address in the bottom corner of your browser before clicking.
  - **Be skeptical:** Be wary of links in unexpected emails, text messages, or social media messages, even if they appear to come from a trusted source.
  - **Verify directly:** If you're unsure, go directly to the official website or app to access the information rather than clicking the link.

Other Important Good Cyber Habits

In addition to the ones you mentioned, consider adding these habits to your routine:

- **Use Strong, Unique Passwords:** Use complex passwords (a mix of letters, numbers, and symbols) and a different password for every account. Use a password manager to help you manage them.
- **Enable Multi-Factor Authentication (MFA):** Use MFA (like a one-time code sent to your phone) for all sensitive accounts (email, banking, social media, etc.) for an added layer of security.

- **Be Mindful of Wi-Fi Use:** Avoid accessing sensitive information (like online banking) while using public, unsecured Wi-Fi networks. Consider using a Virtual Private Network (VPN) for extra security on public networks.
- **Secure Your Home Network:** Change the default password on your home router and use strong encryption (WPA2 or WPA3).
- **Regularly Review Account Activity:** Check bank statements and online account histories for any suspicious activity.

निश्चित रूप से, आपने जिन अच्छी साइबर आदतों का उल्लेख किया है, वे मजबूत ऑनलाइन सुरक्षा के लिए आवश्यक हैं। ये आदतें आपके उपकरणों और व्यक्तिगत जानकारी को सुरक्षित रखने में मदद करती हैं।
यहां उन अच्छी साइबर आदतों और उनके महत्व का विवरण दिया गया है:

1. नियमित अपडेट (Regular Updates)

अपने सॉफ़्टवेयर, ऑपरेटिंग सिस्टम और ऐप्स को अपडेट रखना एक महत्वपूर्ण सुरक्षा उपाय है।

- **क्यों महत्वपूर्ण है:** अपडेट में अक्सर सुरक्षा पैच शामिल होते हैं जो डेवलपर्स द्वारा खोजी गई कमजोरियों को ठीक करते हैं। साइबर अपराधी इन ज्ञात कमजोरियों का फायदा उठाकर सिस्टम तक अनधिकृत पहुंच प्राप्त करते हैं।
- **कैसे अभ्यास करें:** जब भी संभव हो, अपने ऑपरेटिंग सिस्टम, वेब ब्राउज़र, एंटीवायरस सॉफ़्टवेयर और अन्य एप्लिकेशन के लिए स्वचालित अपडेट सक्षम करें।

2. वायरस स्कैनिंग (Virus Scanning)

विश्वसनीय सुरक्षा सॉफ़्टवेयर का उपयोग करना और नियमित स्कैन चलाना दुर्भावनापूर्ण सॉफ़्टवेयर का पता लगाने और उन्हें हटाने में मदद करता है।

- **क्यों महत्वपूर्ण है:** वायरस, ट्रोजन, रैंसमवेयर और अन्य प्रकार के मैलवेयर जानकारी चुरा सकते हैं, फ़ाइलों को नुकसान पहुंचा सकते हैं या आपके डिवाइस का नियंत्रण ले सकते हैं। एक अच्छा सुरक्षा प्रोग्राम एक सतर्क गार्ड के रूप में कार्य करता है।
- **कैसे अभ्यास करें:** प्रतिष्ठित एंटीवायरस या एंटी-मैलवेयर सॉफ़्टवेयर इंस्टॉल करें और बनाए रखें। सुनिश्चित करें कि रीयल-टाइम सुरक्षा सक्रिय है और नियमित, पूर्ण-सिस्टम स्कैन शेड्यूल करें।

3. डेटा बैकअप (Data Backup)

अपने महत्वपूर्ण डेटा का नियमित रूप से बैकअप सुनिश्चित करता है कि सिस्टम विफल होने, आकस्मिक विलोपन, या रैंसमवेयर जैसे साइबर हमले की स्थिति में आप इसे पुनर्प्राप्त कर सकें।

- **क्यों महत्वपूर्ण है:** डेटा का खोना विनाशकारी हो सकता है। बैकअप एक सुरक्षा जाल प्रदान करते हैं, जिससे आप अपनी फ़ाइलों को पुनर्स्थापित कर सकते हैं और व्यवधान को कम कर सकते हैं।
- **कैसे अभ्यास करें: 3-2-1 नियम** का पालन करें:
  - आपके डेटा की **3** प्रतियां।
  - **2** विभिन्न प्रकार के स्टोरेज (जैसे, आंतरिक हार्ड ड्राइव और बाहरी हार्ड ड्राइव)।
  - **1** प्रति ऑफ़-साइट संग्रहीत (जैसे, क्लाउड बैकअप सेवा या आपके घर/कार्यालय से दूर एक सुरक्षित स्थान)।

4. लिंक सुरक्षा (Link Safety)

लिंक और अटैचमेंट के साथ सावधानी बरतना फ़िशिंग हमलों और मैलवेयर संक्रमणों को रोकने का एक प्राथमिक तरीका है।

- **क्यों महत्वपूर्ण है:** दुर्भावनापूर्ण लिंक नकली वेबसाइटों तक ले जा सकते हैं जिन्हें लॉगिन क्रेडेंशियल चुराने या स्वचालित रूप से आपके डिवाइस पर मैलवेयर डाउनलोड करने के लिए डिज़ाइन किया गया है। साइबर अपराधियों के लिए खातों से समझौता करने के लिए फ़िशिंग सबसे आम तरीकों में से एक है।
- **कैसे अभ्यास करें:**
  - **क्लिक करने से पहले होवर करें:** कंप्यूटर पर, क्लिक करने से पहले वास्तविक वेब पते को अपने ब्राउज़र के निचले कोने में देखने के लिए लिंक पर अपना माउस घुमाएं।
  - **संदेहशील रहें:** अप्रत्याशित ईमेल, टेक्स्ट संदेशों या सोशल मीडिया संदेशों में लिंक के प्रति सतर्क रहें, भले ही वे किसी विश्वसनीय स्रोत से आए प्रतीत हों।
  - **सीधे सत्यापित करें:** यदि आप अनिश्चित हैं, तो लिंक पर क्लिक करने के बजाय जानकारी तक पहुंचने के लिए सीधे आधिकारिक वेबसाइट या ऐप पर जाएं।

अन्य महत्वपूर्ण अच्छी साइबर आदतें

आपके द्वारा उल्लिखित आदतों के अलावा, इन आदतों को अपनी दिनचर्या में जोड़ने पर विचार करें:

- **मजबूत, अद्वितीय पासवर्ड का उपयोग करें:** जटिल पासवर्ड (अक्षरों, संख्याओं और प्रतीकों का मिश्रण) और प्रत्येक खाते के लिए एक अलग पासवर्ड का उपयोग करें। उन्हें प्रबंधित करने में मदद के लिए पासवर्ड मैनेजर का उपयोग करें।

- **मल्टी-फ़ैक्टर ऑथेंटिकेशन (MFA) सक्षम करें:** सुरक्षा की एक अतिरिक्त परत के लिए सभी संवेदनशील खातों (ईमेल, बैंकिंग, सोशल मीडिया, आदि) के लिए MFA (जैसे आपके फोन पर भेजा गया एक बार का कोड) का उपयोग करें।
- **वाई-फ़ाई उपयोग के प्रति सचेत रहें:** सार्वजनिक, असुरक्षित वाई-फ़ाई नेटवर्क का उपयोग करते समय संवेदनशील जानकारी (जैसे ऑनलाइन बैंकिंग) तक पहुंचने से बचें। सार्वजनिक नेटवर्क पर अतिरिक्त सुरक्षा के लिए वर्चुअल प्राइवेट नेटवर्क (VPN) का उपयोग करने पर विचार करें।
- **अपने होम नेटवर्क को सुरक्षित करें:** अपने होम राउटर पर डिफ़ॉल्ट पासवर्ड बदलें और मजबूत एन्क्रिप्शन (WPA2 या WPA3) का उपयोग करें।
- **नियमित रूप से खाता गतिविधि की समीक्षा करें:** किसी भी संदिग्ध गतिविधि के लिए बैंक स्टेटमेंट और ऑनलाइन खाता इतिहास की जाँच करें।

Concept of digital cleanliness - डिजिटल स्वच्छता

Digital cleanliness, also known as **digital hygiene**, is the practice of adopting routine habits and practices to ensure one's online activities and digital environments remain secure, organized, and supportive of mental well-being.

The concept compares directly to personal hygiene: just as regular physical cleaning prevents illness, consistent digital maintenance helps prevent security breaches, data loss, and cognitive overload.

Digital cleanliness, or digital hygiene, is the practice of maintaining healthy and secure habits in the digital world. It encompasses two main areas: **cyber hygiene**, which involves taking steps to protect against online threats by using strong passwords, updating software, and being cautious of phishing scams; and **digital well-being**, which focuses on managing your digital habits to maintain mental clarity, such as reducing screen time and organizing digital files.

Core Principles

The concept of digital cleanliness encompasses two primary aspects: security and organization.

- **Security:** This involves precautionary measures to protect data, devices, and online identity from cyber threats. Key practices include:
  - **Strong, unique passwords:** Using complex, unique passwords or passphrases for every account, often managed via a password manager.
  - **Multi-factor authentication (MFA):** Enabling an extra layer of security on all critical accounts to prevent unauthorized access, even if a password is stolen.
  - **Regular software updates:** Keeping operating systems, applications, and antivirus software updated to patch security vulnerabilities.
  - **Data backup:** Regularly backing up important files to an external drive or secure cloud storage to prevent data loss from system failure or cyberattacks.
  - **Phishing awareness:** Learning to spot and avoid suspicious links, emails, and pop-ups that could lead to malware infections or data theft.
  - **Secure Wi-Fi usage:** Using a Virtual Private Network (VPN) when on public Wi-Fi and securing home networks with strong passwords and encryption.
- **Organization and Well-being:** This broader aspect focuses on managing the digital environment for enhanced productivity and mental health. Practices include:
  - **Digital decluttering:** Regularly deleting unused apps, old files, and unnecessary emails to free up storage space and improve device efficiency.
  - **Managing screen time:** Setting clear boundaries for device use and establishing "screen curfews" to promote a healthier work-life balance and better sleep.
  - **Curating content intake:** Being mindful of the information consumed online to avoid negative news cycles and information overload, which can cause stress and anxiety.
  - **Privacy management:** Regularly reviewing and adjusting privacy settings on social media and other platforms to limit the amount of personal information shared online.

Cyber hygiene (Security and safety)

- **Use strong, unique passwords** and avoid sharing them.
- **Enable multi-factor authentication** to add an extra layer of security to your accounts.
- **Keep software and apps updated** to patch security vulnerabilities.
- **Be cautious of phishing attempts** and suspicious links or downloads.
- **Back up your data regularly** and consider encrypting sensitive information.

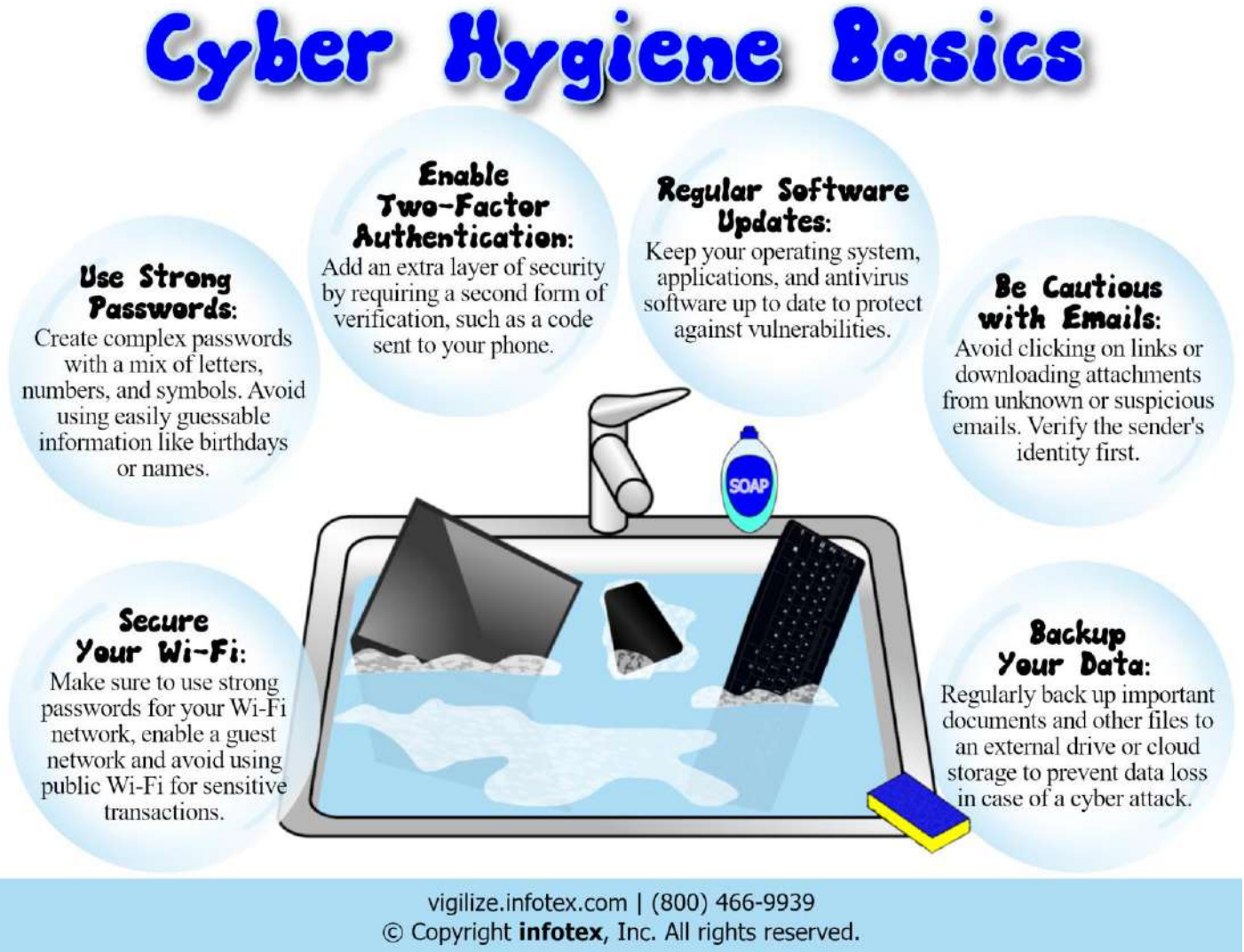
Digital well-being (Mental and environmental clarity)

- **Mindfully manage screen time** and avoid constant multitasking to prevent information overload and stress.
- **Declutter your digital spaces** by organizing files and deleting unnecessary accounts to reduce mental clutter.
- **Establish digital boundaries**, such as creating a "wind-down" routine to separate from screens.
- **Curate your information intake** to be more intentional about what you consume online.

Be aware of the broader impact of your digital actions, such as the environmental effects of data storage and energy consumption.

Importance

Practicing digital cleanliness is vital because it significantly reduces the risk of identity theft, financial fraud, and data breaches. It also enhances operational efficiency, improves focus, and fosters a healthier relationship with technology, ultimately contributing to overall personal and professional well-being in an increasingly connected world.



डिजिटल स्वच्छता, जिसे डिजिटल स्वच्छता**के रूप में भी जाना जाता है** , नियमित आदतों और प्रथाओं को अपनाने का अभ्यास है ताकि यह सुनिश्चित किया जा सके कि किसी की ऑनलाइन गतिविधियां और डिजिटल वातावरण सुरक्षित, संगठित और मानसिक कल्याण के लिए सहायक रहें।

यह अवधारणा सीधे तौर पर व्यक्तिगत स्वच्छता से तुलना करती है: जिस तरह नियमित शारीरिक सफाई बीमारी को रोकती है, उसी तरह लगातार डिजिटल रखरखाव सुरक्षा उल्लंघनों, डेटा हानि और संज्ञानात्मक अधिभार को रोकने में मदद करता है।

मूल सिद्धांत

डिजिटल स्वच्छता की अवधारणा में दो प्राथमिक पहलू शामिल हैं: सुरक्षा और संगठन।

- **सुरक्षा:** इसमें डेटा, उपकरणों और ऑनलाइन पहचान को साइबर खतरों से बचाने के लिए एहतियाती उपाय शामिल हैं। प्रमुख प्रथाओं में शामिल हैं:
  - **मजबूत, अद्वितीय पासवर्ड:** प्रत्येक खाते के लिए जटिल, अद्वितीय पासवर्ड या पासफ़्रेज़ का उपयोग करना, जिसे अक्सर पासवर्ड मैनेजर के माध्यम से प्रबंधित किया जाता है।
  - **बहु-कारक प्रमाणीकरण (MFA):** सभी महत्वपूर्ण खातों पर सुरक्षा की एक अतिरिक्त परत सक्षम करना, ताकि पासवर्ड चोरी होने पर भी अनधिकृत पहुंच को रोका जा सके।
  - **नियमित सॉफ्टवेयर अपडेट:** सुरक्षा कमजोरियों को दूर करने के लिए ऑपरेटिंग सिस्टम, एप्लिकेशन और एंटीवायरस सॉफ़्टवेयर को अपडेट रखना।
  - **डेटा बैकअप:** सिस्टम विफलता या साइबर हमलों से डेटा हानि को रोकने के लिए महत्वपूर्ण फ़ाइलों का नियमित रूप से बाहरी ड्राइव या सुरक्षित क्लाउड स्टोरेज में बैकअप लेना।
  - **फ़िशिंग जागरूकता:** संदिग्ध लिंक, ईमेल और पॉप-अप को पहचानना और उनसे बचना सीखना, जो मैलवेयर संक्रमण या डेटा चोरी का कारण बन सकते हैं।
  - **सुरक्षित वाई-फाई उपयोग:** सार्वजनिक वाई-फाई पर वर्चुअल प्राइवेट नेटवर्क (वीपीएन) का उपयोग करना और मजबूत पासवर्ड और एन्क्रिप्शन के साथ घरेलू नेटवर्क को सुरक्षित करना।
- **संगठन और कल्याण:** यह व्यापक पहलू बेहतर उत्पादकता और मानसिक स्वास्थ्य के लिए डिजिटल वातावरण के प्रबंधन पर केंद्रित है। इसमें शामिल हैं:
  - **डिजिटल डिक्लटरिंग:** स्टोरेज स्पेस खाली करने और डिवाइस की कार्यक्षमता में सुधार करने के लिए अप्रयुक्त ऐप्स, पुरानी फ़ाइलों और अनावश्यक ईमेल को नियमित रूप से हटाना।
  - **स्क्रीन समय का प्रबंधन:** डिवाइस के उपयोग के लिए स्पष्ट सीमाएं निर्धारित करना तथा स्वस्थ कार्य-जीवन संतुलन और बेहतर नींद को बढ़ावा देने के लिए "स्क्रीन कर्फ्यू" स्थापित करना।
  - **सामग्री के सेवन पर नियंत्रण रखना:** नकारात्मक समाचार चक्र और सूचना के अतिरेक से बचने के लिए ऑनलाइन उपभोग की जाने वाली जानकारी के प्रति सचेत रहना, क्योंकि इससे तनाव और चिंता हो सकती है।
  - **गोपनीयता प्रबंधन:** ऑनलाइन साझा की जाने वाली व्यक्तिगत जानकारी की मात्रा को सीमित करने के लिए सोशल मीडिया और अन्य प्लेटफार्मों पर गोपनीयता सेटिंग्स की नियमित समीक्षा और समायोजन करना।

महत्त्व

डिजिटल स्वच्छता का अभ्यास करना बेहद ज़रूरी है क्योंकि इससे पहचान की चोरी, वित्तीय धोखाधड़ी और डेटा उल्लंघन का जोखिम काफ़ी कम हो जाता है। इससे परिचालन दक्षता भी बढ़ती है, एकाग्रता बढ़ती है और तकनीक के साथ बेहतर संबंध बनते हैं, जो अंततः तेज़ी से जुड़ती दुनिया में समग्र व्यक्तिगत और व्यावसायिक कल्याण में योगदान देता है।

डिजिटल *सफ़ाई या डिजिटल स्वच्छता, डिजिटल दुनिया में स्वस्थ और सुरक्षित आदतों को बनाए रखने की प्रक्रियाहै । इसमें दो मुख्य क्षेत्र शामिल हैं: **साइबर स्वच्छता**, जिसमें मज़बूत पासवर्ड का उपयोग करके, सॉफ़्टवेयर अपडेट करके और फ़िशिंग घोटालों से सावधान रहकर ऑनलाइन खतरों से बचाव के लिए कदम उठाना शामिल है; और **डिजिटल कल्याण**, जो मानसिक स्पष्टता बनाए रखने के लिए आपकी डिजिटल आदतों के प्रबंधन पर केंद्रित है, जैसे स्क्रीन टाइम कम करना और डिजिटल फ़ाइलों को व्यवस्थित करना।*

साइबर स्वच्छता (सुरक्षा और संरक्षा)

- **मजबूत एवं अद्वितीय पासवर्ड का प्रयोग करें** और उन्हें साझा करने से बचें।
- **अपने खातों में सुरक्षा की एक अतिरिक्त परत जोड़ने के लिए**बहु-कारक प्रमाणीकरण सक्षम करें ।
- **सुरक्षा कमजोरियों को दूर करने के लिए**सॉफ्टवेयर और ऐप्स को अपडेट रखें ।
- **फ़िशिंग प्रयासों और संदिग्ध लिंक या डाउनलोड**से सावधान रहें ।

- **अपने डेटा का नियमित रूप से बैकअप लें** और संवेदनशील जानकारी को एन्क्रिप्ट करने पर विचार करें।

डिजिटल कल्याण (मानसिक और पर्यावरणीय स्पष्टता)

- **सूचना के अत्यधिक बोझ और तनाव से बचने के लिए स्क्रीन समय का सावधानीपूर्वक प्रबंधन करें** और लगातार एक साथ कई काम करने से बचें।
- **मानसिक अव्यवस्था को कम करने के लिए फाइलों को व्यवस्थित करके और अनावश्यक खातों को हटाकर**अपने डिजिटल स्थान को साफ करें।
- **डिजिटल सीमाएं स्थापित करें**, जैसे स्क्रीन से अलग होने के लिए "विंड-डाउन" रूटीन बनाना।
- **आप जो भी ऑनलाइन उपभोग करते हैं, उसके बारे में अधिक सचेत रहने के लिए**अपनी जानकारी के सेवन को व्यवस्थित करें।
- **अपने डिजिटल कार्यों के व्यापक प्रभाव के प्रति सचेत रहें** , जैसे डेटा भंडारण और ऊर्जा खपत के पर्यावरणीय प्रभाव।

cyber swachhta Kendra (https://www.csk.gov.in/)

The " **Cyber Swachhta Kendra** " (Botnet Cleaning and Malware Analysis Centre) is a part of the ***Government of India's Digital India*** initiative under the ***Ministry of Electronics and Information Technology (MeitY)*** to create a secure cyber space by detecting botnet infections in India and to notify, enable cleaning and securing systems of end users so as to prevent further infections. The " **Cyber Swachhta Kendra** " (Botnet Cleaning and Malware Analysis Centre) is set up in accordance with the objectives of the "National Cyber Security Policy", which envisages creating a secure cyber eco system in the country. This centre operates in close coordination and collaboration with Internet Service Providers and Product/Antivirus companies. This website provides information and tools to users to secure their systems/devices. This centre is being operated by the Indian Computer Emergency Response Team (CERT-In) under provisions of Section 70B of the Information Technology Act, 2000.

The Cyber Swachhta Kendra is an Indian government initiative that helps citizens protect their computers, mobile phones, and routers from malware and botnets. ***It operates under the aegis of the Indian Computer Emergency Response Team (CERT-In)*** and aims to create a safer ***cyberspace***. The centre detects malware-infected systems and provides users with tools and information to clean and secure their devices.

Main functions (Purpose and Objectives)

- **Malware detection:** It works with industry and Internet service providers to identify systems infected with botnets.
- **Tools and Guidelines:** It provides users with free malware removal tools (such as bot removal tools) and other security tools to clean and secure their devices.
- **Spreading awareness:** It educates citizens about botnets, malware, and other cyber threats and shares information on the best ways to stay safe.
- **Strengthening Cyber Security:** It helps in strengthening cyber security under India's Digital India programme.
- **Respect for privacy:** It does not monitor or collect personal information of citizens, thereby maintaining their privacy.
- **Detect and Mitigate Threats**: The primary aim is to detect, analyse, and mitigate botnet infections and other malware threats within India.
- **Provide Free Tools**: It offers a range of free-of-cost security tools and software to help end-users clean and secure their computers, mobile phones, and other devices.
- **Raise Awareness**: The initiative strives to educate citizens on cybersecurity best practices, cyber hygiene, and how to safeguard their data and systems from emerging cyber threats.
- **Collaboration**: It works closely with Internet Service Providers (ISPs), antivirus companies, and academia to identify infected systems and notify the users so they can take corrective action.

Key Services and Tools

Users can visit the official Cyber Swachhta Kendra portal (**www.cyberswachhtakendra.gov.in**) to access the following resources:

- **Bot and Malware Removal Tools**: Free downloadable tools from partners like eScan and Quick Heal to scan and remove malicious software from Windows and Android systems.
- **USB Pratirodh**: A desktop security solution to protect against threats from USB mass storage devices.
- **AppSamvid**: A desktop solution that restricts application installation to only genuine ones through whitelisting, preventing malicious applications from running.
- **M-Kavach**: An indigenously developed comprehensive mobile security solution for addressing threats on Android devices.
- **Alerts and Advisories**: The portal provides regular updates and information on current cyber threats and security measures to help users stay informed.
- **Security Best Practices**: Information and guidelines on using strong passwords, secure online behavior, and maintaining data backups to enhance overall online safety.

साइबर स्वच्छता केंद्र भारत सरकार की एक पहल है जो नागरिकों को उनके कंप्यूटर, मोबाइल और राउटर को मैलवेयर और बॉटनेट से सुरक्षित रखने में मदद करती है। यह भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया दल (सर्ट-इन) के तहत संचालित होता है और इसका उद्देश्य एक सुरक्षित साइबरस्पेस बनाना है। यह केंद्र मैलवेयर से संक्रमित सिस्टम का पता लगाता है और उपयोगकर्ताओं को अपने उपकरणों को साफ करने और सुरक्षित रखने के लिए उपकरण और जानकारी प्रदान करता है।

मुख्य कार्य:

- **मैलवेयर का पता लगाना:** यह उद्योग और इंटरनेट सेवा प्रदाताओं के साथ मिलकर बॉटनेट से संक्रमित सिस्टम की पहचान करता है।
- **उपकरण और दिशानिर्देश:** यह उपयोगकर्ताओं को अपने उपकरणों को साफ करने और सुरक्षित करने के लिए मुफ़्त मैलवेयर हटाने वाले उपकरण (जैसे बॉट रिमूवल टूल) और अन्य सुरक्षा उपकरण प्रदान करता है।
- **जागरूकता फैलाना:** यह नागरिकों को बॉटनेट, मैलवेयर और अन्य साइबर खतरों के बारे में शिक्षित करता है और सुरक्षित रहने के सर्वोत्तम तरीकों पर जानकारी साझा करता है।
- **साइबर सुरक्षा को मजबूत करना:** यह भारत के डिजिटल इंडिया कार्यक्रम के तहत साइबर सुरक्षा को मजबूत करने में मदद करता है।
- **गोपनीयता का सम्मान:** यह नागरिकों की व्यक्तिगत जानकारी की निगरानी या संग्रह नहीं करता है, जिससे उनकी गोपनीयता बरकरार रहती है।

साइबर स्वच्छता केंद्र (Cyber Swachhta Kendra - CSK) भारत सरकार की एक पहल है, जिसे इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी मंत्रालय (MeitY) के तहत भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया दल (CERT-In) द्वारा संचालित किया जाता है। इसे **बॉटनेट सफाई और मैलवेयर विश्लेषण केंद्र (Botnet Cleaning and Malware Analysis Centre)** के नाम से भी जाना जाता है।
इसका मुख्य उद्देश्य भारत में एक **सुरक्षित साइबर स्पेस (secure cyber space) बनाना** है।

मुख्य कार्य और उद्देश्य:

- **बॉटनेट संक्रमणों का पता लगाना:** यह भारत में बॉटनेट से संक्रमित सिस्टमों की पहचान करता है।
- **मैलवेयर विश्लेषण:** यह विभिन्न प्रकार के मैलवेयर (हानिकारक सॉफ्टवेयर) का विश्लेषण करता है।
- **उपयोगकर्ताओं को सूचित करना:** यह इंटरनेट सेवा प्रदाताओं (ISPs) के साथ समन्वय करके संक्रमित आईपी पते वाले उपयोगकर्ताओं को उनके सिस्टम की स्थिति के बारे में अलर्ट भेजता है।
- **मुफ़्त टूल प्रदान करना:** यह उपयोगकर्ताओं को अपने कंप्यूटर, मोबाइल फोन और अन्य उपकरणों से मैलवेयर हटाने के लिए मुफ़्त सॉफ्टवेयर और टूल उपलब्ध कराता है, जैसे 'यूएसबी प्रतिरोध' और 'एम-कवच'।
- **जागरूकता बढ़ाना:** यह नागरिकों को साइबर खतरों, सुरक्षा उपायों और अपने उपकरणों को सुरक्षित रखने के तरीकों के बारे में शिक्षित करता है।
- **सुरक्षित डिजिटल इकोसिस्टम बनाना:** यह राष्ट्रीय साइबर सुरक्षा नीति के उद्देश्यों के अनुसार देश में एक सुरक्षित डिजिटल वातावरण सुनिश्चित करने में मदद करता है।

संक्षेप में, यह केंद्र भारत के इंटरनेट उपयोगकर्ताओं को ऑनलाइन खतरों से बचाने और उनके उपकरणों की "डिजिटल स्वच्छता" बनाए रखने में मदद करता है।

Cyber Surakshit Bharat

"Cyber Surakshit Bharat" is a government initiative by the Ministry of Electronics and Information Technology (MeitY) to promote cybersecurity awareness, build capacity among IT officials, and create a secure digital ecosystem in India. Launched in 2018, it involves programs like CISO Deep-Dive training for government officials and awareness competitions for the public, including students, to help secure digital infrastructure against cyber-attacks. it operates on a Public-Private Partnership (PPP) model.

Key Details and Objectives

- **Objective:** To spread awareness about cyber-crimes and build the capacity of government officials to defend digital infrastructure.
  - **Awareness:** Spreading knowledge about the growing landscape of cyber threats and the importance of cybersecurity.
  - **Education:** Providing a deep understanding of related solutions, policies, frameworks, and best practices.
  - **Enablement:** Equipping officials with cybersecurity health toolkits and hands-on experience to manage and mitigate cyber threats.
- **Target Audience:** Chief Information Security Officers (CISOs), Chief Technology Officers (CTOs), and IT officials from central and state governments, Union Territories, Public Sector Undertakings (PSUs), public sector banks, and insurance companies.
- **Main Goal:** To enable government organizations to defend their digital infrastructures, create a cyber-resilient ecosystem, and facilitate the secure delivery of government services under the Digital India program.
- **Implementing Agency:** The National e-Governance Division (NeGD), an arm of MeitY, is responsible for designing and delivering the training programs.
- **Industry Consortium:** The program involves a first-of-its-kind partnership with an industry consortium that includes major IT companies such as Microsoft, Intel, IBM, Cisco, Palo Alto Networks, E&Y, and others, who provide access to global best practices and technology.
- **Knowledge Partners:** MeitY organizations such as the National Informatics Centre (NIC), CERT-In (Indian Computer Emergency Response Team), Standardisation Testing and Quality Certification (STQC), and the Centre for Development of Advanced Computing (C-DAC) serve as knowledge partners
- **Capacity Building:** Offers training programs to equip CISOs and IT officials with the skills to tackle cyber-attacks and create a cyber-resilient ecosystem.
- **Launch Date:** January 19, 2018.

Activities

A major component of the initiative is the "CISO Deep-Dive Training Programme," which involves intensive, multi-day training sessions and workshops conducted across the country to provide practical knowledge and enable informed decision-making on cybersecurity issues. Other activities include national-level cybersecurity awareness competitions in collaboration with bodies like the CBSE.

"साइबर सुरक्षित भारत", इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी मंत्रालय (MeitY)द्वारा साइबर सुरक्षा जागरूकता को बढ़ावा देने, आईटी अधिकारियों के बीच क्षमता निर्माण और भारत में एक सुरक्षित डिजिटल पारिस्थितिकी तंत्र बनाने के लिएएक सरकारी पहल है। 2018 में शुरू की गई इस पहल में सरकारी अधिकारियों के लिए CISO डीप-डाइव प्रशिक्षणऔर छात्रों सहित आम जनता के लिए जागरूकता प्रतियोगिताओं जैसे कार्यक्रम शामिल हैं , ताकि साइबर हमलों के खिलाफ डिजिटल बुनियादी ढांचे को सुरक्षित करने में मदद मिल सके।

मुख्य पहलू

- **उद्देश्य**: साइबर अपराधों के बारे में जागरूकता फैलाना और डिजिटल बुनियादी ढांचे की रक्षा के लिए सरकारी अधिकारियों की क्षमता का निर्माण करना।
- **लक्षित दर्शक**: मुख्य रूप से मुख्य सूचना सुरक्षा अधिकारी (सीआईएसओ) और सरकारी विभागों के अग्रिम पंक्ति के आईटी अधिकारी, लेकिन इसमें व्यापक जन जागरूकता अभियान भी शामिल हैं।
- **क्षमता निर्माण**: साइबर हमलों से निपटने और साइबर-लचीला पारिस्थितिकी तंत्र बनाने के लिए सीआईएसओ और आईटी अधिकारियों को कौशल से लैस करने के लिए प्रशिक्षण कार्यक्रम प्रदान करता है।
- **जागरूकता अभियान**: साइबर स्वच्छता और डिजिटल गोपनीयता में सुधार के लिए छात्रों के लिए राष्ट्रीय स्तर की प्रतियोगिताओं (जैसे ड्राइंग, लघु वीडियो और तकनीकी पेपर) सहित सार्वजनिक जागरूकता पहल चलाता है।
- **साझेदारियां**:अपने विभिन्न कार्यक्रमों को क्रियान्वित करने के लिए राष्ट्रीय ई-गवर्नेंस प्रभाग (एनईजीडी), सीबीएसईऔर अन्य जैसे संगठनों के साथ सहयोग करता है ।
- **लॉन्च तिथि**: 19 जनवरी, 2018.

'साइबर सुरक्षित भारत' पहल भारत सरकार के इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी मंत्रालय (MeitY) द्वारा शुरू किया गया एक व्यापक साइबर सुरक्षा कार्यक्रम है। यह साइबर अपराध के बारे में जागरूकता फैलाने और सरकारी विभागों में मुख्य सूचना सुरक्षा अधिकारियों

(CISOs) तथा अग्रिम पंक्ति के आईटी अधिकारियों की क्षमताओं का निर्माण करने के मिशन के साथ संकल्पित किया गया था। यह पब्लिक-प्राइवेट पार्टनरशिप (PPP) मॉडल पर काम करता है।

मुख्य विवरण और उद्देश्य

- **शुरुआत की तारीख:** इस पहल की शुरुआत 19 जनवरी, 2018 को हुई थी।
- **संचालन सिद्धांत:** यह कार्यक्रम तीन मुख्य सिद्धांतों पर चलता है:
  - **जागरूकता:** साइबर खतरों और साइबर सुरक्षा के महत्व के बारे में ज्ञान का प्रसार करना।
  - **शिक्षा:** संबंधित समाधानों, नीतियों, रूपरेखाओं और सर्वोत्तम प्रथाओं की गहरी समझ प्रदान करना।
  - **सक्षमता:** अधिकारियों को साइबर सुरक्षा स्वास्थ्य टूलकिट और साइबर खतरों को प्रबंधित व कम करने के लिए व्यावहारिक अनुभव से लैस करना।
- **लक्षित दर्शक:** केंद्र और राज्य सरकारों, केंद्र शासित प्रदेशों, सार्वजनिक क्षेत्र के उपक्रमों (PSUs), सार्वजनिक क्षेत्र के बैंकों और बीमा कंपनियों के मुख्य सूचना सुरक्षा अधिकारी (CISOs), मुख्य प्रौद्योगिकी अधिकारी (CTOs) और आईटी अधिकारी।
- **मुख्य लक्ष्य:** सरकारी संगठनों को अपने डिजिटल बुनियादी ढांचे की रक्षा करने, एक साइबर-लचीला पारिस्थितिकी तंत्र बनाने और डिजिटल इंडिया कार्यक्रम के तहत सरकारी सेवाओं के सुरक्षित वितरण की सुविधा प्रदान करने में सक्षम बनाना।

कार्यान्वयन और साझेदार

- **कार्यान्वयन एजेंसी:** राष्ट्रीय ई-गवर्नेंस डिवीजन (NeGD), जो MeitY की एक शाखा है, प्रशिक्षण कार्यक्रमों को डिजाइन करने और वितरित करने के लिए जिम्मेदार है।
- **उद्योग संघ:** इसमें एक अनूठी साझेदारी शामिल है जिसमें माइक्रोसॉफ्ट, इंटेल, आईबीएम, सिस्को, पालो अल्टो नेटवर्क्स, ईएंडवाई और अन्य जैसी प्रमुख आईटी कंपनियां वैश्विक सर्वोत्तम प्रथाओं और प्रौद्योगिकी तक पहुंच प्रदान करती हैं।
- **ज्ञान साझेदार:** MeitY के संगठन जैसे राष्ट्रीय सूचना विज्ञान केंद्र (NIC), CERT-In (भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया टीम), मानकीकरण परीक्षण और गुणवत्ता प्रमाणन (STQC), और सेंटर फॉर डेवलपमेंट ऑफ एडवांस्ड कंप्यूटिंग (C-DAC) ज्ञान साझेदारों के रूप में कार्य करते हैं।

गतिविधियाँ

इस पहल का एक प्रमुख घटक "CISO डीप-डाइव प्रशिक्षण कार्यक्रम" है, जिसमें व्यावहारिक ज्ञान प्रदान करने और साइबर सुरक्षा मुद्दों पर सूचित निर्णय लेने में सक्षम बनाने के लिए देश भर में गहन, बहु-दिवसीय प्रशिक्षण सत्र और कार्यशालाएं आयोजित की जाती हैं। अन्य गतिविधियों में CBSE जैसे निकायों के सहयोग से राष्ट्रीय स्तर की साइबर सुरक्षा जागरूकता प्रतियोगिताएं शामिल हैं।

"साइबर सुरक्षित भारत" पहल भारत सरकार के इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी मंत्रालय (MeitY) द्वारा शुरू किया गया एक व्यापक साइबर सुरक्षा कार्यक्रम है। इस पहल का मुख्य उद्देश्य सरकारी विभागों में साइबर अपराध के बारे में जागरूकता फैलाना और मुख्य सूचना सुरक्षा अधिकारियों (CISO) तथा अग्रिम पंक्ति के आईटी अधिकारियों की क्षमताओं का निर्माण करना है।

मुख्य विवरण और उद्देश्य

- **शुरुआत:** यह पहल 19 जनवरी 2018 को शुरू की गई थी।
- **संचालन मॉडल:** यह एक पब्लिक-प्राइवेट पार्टनरशिप (PPP) मॉडल पर काम करता है, जिसमें उद्योग जगत के साझेदार और सरकारी संगठन मिलकर काम करते हैं।
- **प्राथमिक लक्ष्य:** सरकारी संगठनों को अपने डिजिटल बुनियादी ढांचे की रक्षा करने, एक साइबर-लचीला (cyber-resilient) पारिस्थितिकी तंत्र बनाने और डिजिटल इंडिया कार्यक्रम के तहत सरकारी सेवाओं की सुरक्षित डिलीवरी को सुविधाजनक बनाने में सक्षम बनाना है।
- **लक्षित दर्शक:** केंद्र और राज्य सरकारों, केंद्र शासित प्रदेशों, सार्वजनिक क्षेत्र के उपक्रमों (PSU), सार्वजनिक क्षेत्र के बैंकों और बीमा कंपनियों के मुख्य सूचना सुरक्षा अधिकारी (CISO) और आईटी अधिकारी।

मुख्य स्तंभ

यह कार्यक्रम तीन मुख्य सिद्धांतों पर आधारित है:

- **जागरूकता:** साइबर खतरों के बढ़ते परिदृश्य के बारे में जागरूकता बढ़ाना।
- **शिक्षा:** संबंधित समाधानों, नीतियों, रूपरेखाओं और सर्वोत्तम प्रथाओं की गहरी समझ प्रदान करना।
- **सक्षमता:** अधिकारियों को साइबर सुरक्षा स्वास्थ्य टूलकिट और व्यावहारिक अनुभव के साथ साइबर खतरों का प्रबंधन और उन्हें कम करने के लिए लैस करना।

कार्यान्वयन और साझेदार

- **कार्यान्वयन एजेंसी:** राष्ट्रीय ई-गवर्नेंस डिवीजन (NeGD), जो MeitY की एक शाखा है, प्रशिक्षण कार्यक्रमों के आयोजन और वितरण के लिए जिम्मेदार है।
- **उद्योग साझेदार:** माइक्रोसॉफ्ट, इंटेल, आईबीएम, सिस्को, पालो अल्टो नेटवर्क्स, ई एंड वाई (E&Y) जैसी प्रमुख आईटी कंपनियां इस पहल में वैश्विक सर्वोत्तम प्रथाओं और तकनीकी सहायता प्रदान करती हैं।

- **ज्ञान साझेदार:** MeitY के तहत राष्ट्रीय सूचना विज्ञान केंद्र (NIC), भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया टीम (CERT-In), मानकीकरण परीक्षण और गुणवत्ता प्रमाणन (STQC), और सेंटर फॉर डेवलपमेंट ऑफ एडवांस्ड कंप्यूटिंग (C-DAC) जैसे संगठन ज्ञान साझेदार के रूप में कार्य करते हैं।
  इस पहल में "CISO डीप-डाइव प्रशिक्षण कार्यक्रम" जैसे गहन प्रशिक्षण सत्र और कार्यशालाएं शामिल हैं, जो अधिकारियों को साइबर सुरक्षा के मुद्दों पर व्यावहारिक ज्ञान और सूचित निर्णय लेने की क्षमता प्रदान करते हैं।

Promoting cyber safety among peers and families

Promoting cyber safety involves a multi-faceted approach: establishing clear family rules, using technology like parental controls and anti-virus software, and fostering open communication to discuss online experiences and risks. Educating everyone on best practices, such as using strong passwords, avoiding oversharing, and identifying phishing scams, is crucial for both peers and families.

For families

- **Establish and communicate rules:** Create a family code of conduct with clear expectations for online behavior, device usage, and consequences.
- **Utilize technology:** Install antivirus software and use parental controls to manage and monitor usage, restricting inappropriate content and time spent online.
- **Promote open communication:** Encourage children to talk about their online activities and any concerns they have, creating a trusting environment.
- **Be a role model:** Demonstrate good online habits yourself, such as being cautious about what you share and respecting privacy.

For peers

- **Foster digital empathy and etiquette:** Encourage respectful online interactions and teach peers to consider the impact of their words and actions.
- **Educate on critical thinking:** Teach friends how to question the accuracy of online information, recognize scams, and be cautious about sharing personal details.
- **Encourage mutual support:** Empower peers to report cyberbullying and support victims, while also being mindful of their own online behavior.

For everyone

- **Practice strong security habits:** Use strong, unique passwords for different accounts, enable two-factor authentication, and keep all software updated.
- **Protect personal information:** Be mindful of what you share online, such as your location, and avoid oversharing personal details in messages, posts, or photos.
- **Recognize and avoid threats:** Be cautious of phishing attempts through emails or social media links, and avoid downloading software from untrusted sources.
- **Use privacy settings:** Regularly check and adjust the privacy settings on all social media and online accounts.

Promoting cyber safety among peers and families involves a combination of **open communication**, **education** about online risks, implementing **technical safeguards**, and **modeling responsible online behavior**. A collaborative effort ensures a safer digital environment for everyone.

For Families

- **Establish Open Communication:** Create a safe, non-judgmental environment where family members, especially children and teens, feel comfortable discussing their online experiences and concerns without fear of punishment. Regularly check in with them about their digital lives.
- **Set Clear Boundaries and Rules:** Establish family guidelines for internet use, including screen time limits, appropriate websites/apps, and sharing behavior. Involve children in creating these rules to foster ownership and responsibility, and revisit them as they grow.
- **Educate on Privacy and Personal Information:** Teach the importance of safeguarding personal identifiable information (PII) such as full names, addresses, phone numbers, and school names. Explain that anything posted online can leave a permanent "digital footprint".

- **Address Cyberbullying:** Discuss what cyberbullying is, its impact, and what steps to take if they encounter it. Encourage them not to respond to bullies, save evidence (screenshots), block the user, and report the behavior to a trusted adult or platform authorities.
- **Teach Critical Thinking:** Help family members, including the elderly who are often targets of scams, to question the reliability of online information and sources. Teach them how to spot fake news, unsolicited offers ("too good to be true"), and phishing attempts.
- **Implement Technical Safeguards:** Use strong, unique passwords for all accounts and enable multi-factor authentication (MFA) whenever possible. Install and regularly update antivirus software and applications, and secure your home Wi-Fi network with a strong password. Utilize parental controls for younger children to filter content and manage screen time.
- **Model Good Behavior:** Parents should lead by example by demonstrating responsible online habits, such as limiting their own screen time, not oversharing personal information, and treating others with respect online.

साइबर सुरक्षा को बढ़ावा देने में बहुआयामी दृष्टिकोण शामिल है: स्पष्ट पारिवारिक नियम स्थापित करना, अभिभावकीय नियंत्रण और एंटी-वायरस सॉफ़्टवेयर जैसी तकनीक का उपयोग करना, और ऑनलाइन अनुभवों और जोखिमों पर चर्चा करने के लिए खुले संचार को बढ़ावा देना। सभी को सर्वोत्तम प्रथाओं के बारे में शिक्षित करना, जैसे कि मज़बूत पासवर्ड का उपयोग करना, ज़रूरत से ज़्यादा जानकारी साझा करने से बचना और फ़िशिंग घोटालों की पहचान करना, साथियों और परिवारों दोनों के लिए महत्वपूर्ण है।

परिवारों के लिए

- **नियम स्थापित करें और उन्हें संप्रेषित करें:** ऑनलाइन व्यवहार, डिवाइस उपयोग और परिणामों के लिए स्पष्ट अपेक्षाओं के साथ एक पारिवारिक आचार संहिता बनाएं।
- **प्रौद्योगिकी का उपयोग करें:** एंटीवायरस सॉफ़्टवेयर स्थापित करें और उपयोग को प्रबंधित करने और निगरानी करने, अनुपयुक्त सामग्री और ऑनलाइन बिताए गए समय को प्रतिबंधित करने के लिए अभिभावकीय नियंत्रण का उपयोग करें।
- **खुले संचार को बढ़ावा दें:** बच्चों को उनकी ऑनलाइन गतिविधियों और उनकी किसी भी चिंता के बारे में बात करने के लिए प्रोत्साहित करें, जिससे एक भरोसेमंद वातावरण बने।
- **एक आदर्श बनें:** स्वयं अच्छी ऑनलाइन आदतें अपनाएं, जैसे कि आप जो कुछ भी साझा करते हैं, उसके बारे में सतर्क रहें और गोपनीयता का सम्मान करें।

साथियों के लिए

- **डिजिटल सहानुभूति और शिष्टाचार को बढ़ावा दें:** सम्मानजनक ऑनलाइन बातचीत को प्रोत्साहित करें और साथियों को अपने शब्दों और कार्यों के प्रभाव पर विचार करना सिखाएं।
- **आलोचनात्मक सोच के बारे में शिक्षित करें:** अपने मित्रों को सिखाएं कि ऑनलाइन जानकारी की सटीकता पर कैसे सवाल उठाएं, धोखाधड़ी को कैसे पहचानें, तथा व्यक्तिगत विवरण साझा करने में सावधानी कैसे बरतें।
- **आपसी सहयोग को प्रोत्साहित करें:** साइबर धमकी की रिपोर्ट करने और पीड़ितों को सहयोग देने के लिए साथियों को सशक्त बनाएं, साथ ही अपने ऑनलाइन व्यवहार के प्रति भी सचेत रहें।

सभी के लिए

- **मजबूत सुरक्षा आदतें अपनाएं:** विभिन्न खातों के लिए मजबूत, अद्वितीय पासवर्ड का उपयोग करें, दो-कारक प्रमाणीकरण सक्षम करें, और सभी सॉफ़्टवेयर को अद्यतन रखें।
- **व्यक्तिगत जानकारी सुरक्षित रखें:** आप जो भी ऑनलाइन साझा करते हैं, जैसे कि आपका स्थान, उसके प्रति सचेत रहें और संदेशों, पोस्टों या फ़ोटो में व्यक्तिगत विवरण को अत्यधिक साझा करने से बचें।
- **खतरों को पहचानें और उनसे बचें:** ईमेल या सोशल मीडिया लिंक के माध्यम से फ़िशिंग प्रयासों से सावधान रहें, और अविश्वसनीय स्रोतों से सॉफ़्टवेयर डाउनलोड करने से बचें।
- **गोपनीयता सेटिंग्स का उपयोग करें:** सभी सोशल मीडिया और ऑनलाइन खातों पर गोपनीयता सेटिंग्स की नियमित रूप से जांच करें और उन्हें समायोजित करें।