

Digital Safety & Security



Program Introduction

Digitization of public and private services and the advent of digital communications, especially social media, have had important implications for users' financial integrity and individual privacy. To reap maximum benefits an optimum level of digital literacy becomes a must in order to identify and avoid the pitfalls to digital safety posed by cybercrime and digital fraud.

The growing reach of the internet and smartphones has made us vulnerable to online frauds and has put our security at risk due to potential online dangers to our data. We need to protect ourselves from these dangers that put at risk our personal information and even affect our mental well-being.

In this program, we will learn about:

What is Digital Safety and Security?

Financial Scams and their Prevention

Social Media Platforms, Scams and Etiquette

Safeguarding Ourselves from Identity Theft

Being Internet Smart

Digital Rights, Laws and Redressal Mechanisms

This handbook has made an attempt to recapitulate the learning of key concepts in the online program. 20 Practical activities are listed at the end, we urge you to do them as practice work to reinforce the learning from the 6 modules.

Thank you! Best Wishes from Team Samhita!

Table of Contents

MODULE 1	1
INTRODUCTION TO DIGITAL SAFETY AND SECURITY	1
MODULE 2	8
FINANCIAL SCAMS AND THEIR PREVENTION	8
MODULE 3	13
SOCIAL MEDIA	13
MODULE 4	21
IDENTITY THEFT	21
MODULE 5	322
BEING INTERNET SMART	322
MODULE 6	39
DIGITAL RIGHTS, LAWS AND REDRESSAL MECHANISMS	39
SUGGESTED PRACTICAL ACTIVITIES	46

Module 1

Introduction to Digital Safety and Security



What is Digital Safety and Security?

Digital Safety and Security refers to protecting internet connected devices such as computers, mobile devices, tablets, etc. from intruders or hackers.

Phishing

Phishing is an attack through a digital medium that tries to steal a person's money or identity using temptation to reveal personal information such as credit card number, bank information etc.

E-mails can carry viruses that may harm your device or steal your sensitive data like card details, passwords, etc. This is known as **phishing** which is one of the many types of cyber-attacks.

Malware:

Malware is software that is designed:

By hackers

To gain access to or damage your internet-connected devices and gain profit.

Ensuring Digital Safety and Security



Never click on spam mails or on mails from an unknown sender



Always secure your personal & professional data



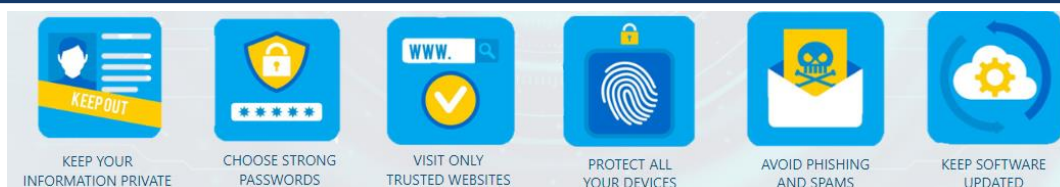
Secure your device with anti virus softwares



If you suspect a cyber fraud, immediately call the concerned organisation, register a complaint and ask them to take the best action to ensure safety of your account



File a complaint at the Govt. of India online cyber crime cell



Benefits of Digital Safety and Security

24*7 safe and secure banking experience

Hassle-free and instant transactions without visiting your branch

Prevents financial loss

Safeguard from cyber attacks such as phishing, password attack, etc











Provides a safe/private window for transactions



Cybersecurity and Privacy Myths

S No	Myth	Reality
1.	Strong passwords safeguard our devices and data stored on them.	Along with strong passwords, we need to have two-factor authentication and data monitoring.
2.	Hackers or cyber criminals do not attack small businesses and people like employees, homemakers, self-employed, etc	Due to lack of advanced security solutions and awareness, such small businesses and people are softer targets for hackers or cyber criminals.
3.	Anti-virus/anti-malware software is enough to safeguard our devices or data.	Anti-virus/anti-malware software will only safeguard the device against viruses and malware but there are many other mediums of cyber-crimes such as fake call to retrieve information
4.	We only need to safeguard our devices from hackers.	Any internal person/employee can leak the information intentionally or by mistake.
5.	Only the IT department of the internet service provider is responsible for cyber security.	It is the social responsibility of every person to safeguard their personal or professional information and device from hackers as well as from intruders around them.
6.	If the App to be downloaded is from an App store it's safe.	Apps in the App Store must go through testing and verification against viruses/malware and privacy policy.
7.	Any password-protected Wi-Fi is safe.	Any public Wi-Fi connection even with a password could be a threat to your device. Never share any confidential information or document through a public Wi-Fi connection
8.	Bring Your Own Device or BYOD is secure for use at work	Any device connected to the internet is prone to digital threats.
9.	HTTPS websites are trustworthy and cannot be hacked	Hackers can bypass HTTPS encryption; so, use only the reliable HTTPS websites e.g. your bank website as shared by the bank.
10.	100% Cybersecurity is achievable against any breach.	Every day a new threat evolves. 100% cybersecurity cannot be achieved.

By following these **best practices**, you may avoid being a cyber-crime victim:

 Always use incognito mode while using a browser.	 Never save credentials on the browser.	 Never download apps from third-party link.
 Never share personal information on any unsecured website/app.	 Keep your antivirus updated.	 Never download any file without virus scanning.
 Keep a backup of your data.	 Never leave your device unattended.	 Never share your passwords.
 Always use two-factor authentication.		

Passwords

A password is a string of characters that allows access to a computer system or service.

To create a unique password

- Avoid sequential letters or numbers
- Avoid personal information
- Make long passwords
- Use unrelated words



Use different passwords for different apps and change your passwords frequently

Unauthorized access to information can result in risks including identity theft, financial loss, increased vulnerability to digital scams, or harassment.

One-Time Password (OTP):

OTPs are one-time passwords, which provide security for online financial transactions

To keep your OTP confidential

- Never share your OTP.
- Delete OTP after completing transaction.
- Always log in through the official websites.
- Never download unknown apps.



Some Common Ways of Stealing OTPs are:

- By posing as bank officials and asking you to verify your account details.

- By sending links through SMS or WhatsApp and spreading malware when you click them.
- By asking you to download a screen-sharing app thereby gaining remote access to your data.

Credit/Debit Card Frauds:

Credit/Debit card fraud occurs when someone uses your credit card information illegally for financial transactions without your knowledge.

Staying safe from Debit/Credit Card frauds:

- Always keep your card with you.
- Change your PIN regularly.
- Do not share your PIN with anyone.
- Check your monthly Credit Card statement carefully
- Avoid using your card on unknown websites or apps.
- Don't click on suspicious links.
- Inform your bank immediately in case your card is stolen or lost

Document Fraud Pre-emption



Fraudsters fake documents like Aadhaar and PAN Card for various reasons. They use faked documents to:

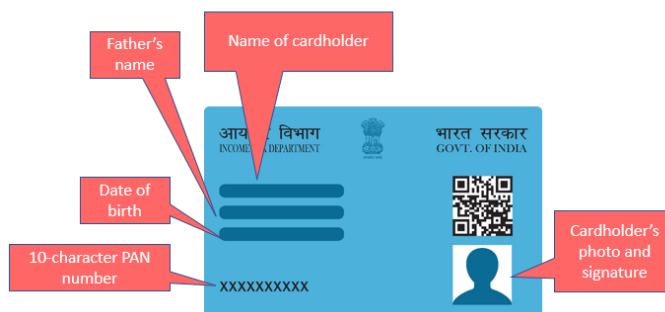
- Open a new bank account
- Apply for loans
- Purchase property
- File income tax returns/ insurance filings

- An **Aadhaar** card is so important as it:
- Enables identification for every resident Indian.
- Serves as proof of address.
- Serves as proof of identity.
- Enables holders to avail of government subsidies.
- Can be used for identification when opening a bank account.
- Can be used for identification when applying for jobs.



We need **PAN** card to perform any of the following transactions:

- Opening a bank account.
- Filing tax returns.
- Applying for a new loan.
- Purchasing or selling a new property.
- Procuring debit/credit cards.
- Making insurance premium payments



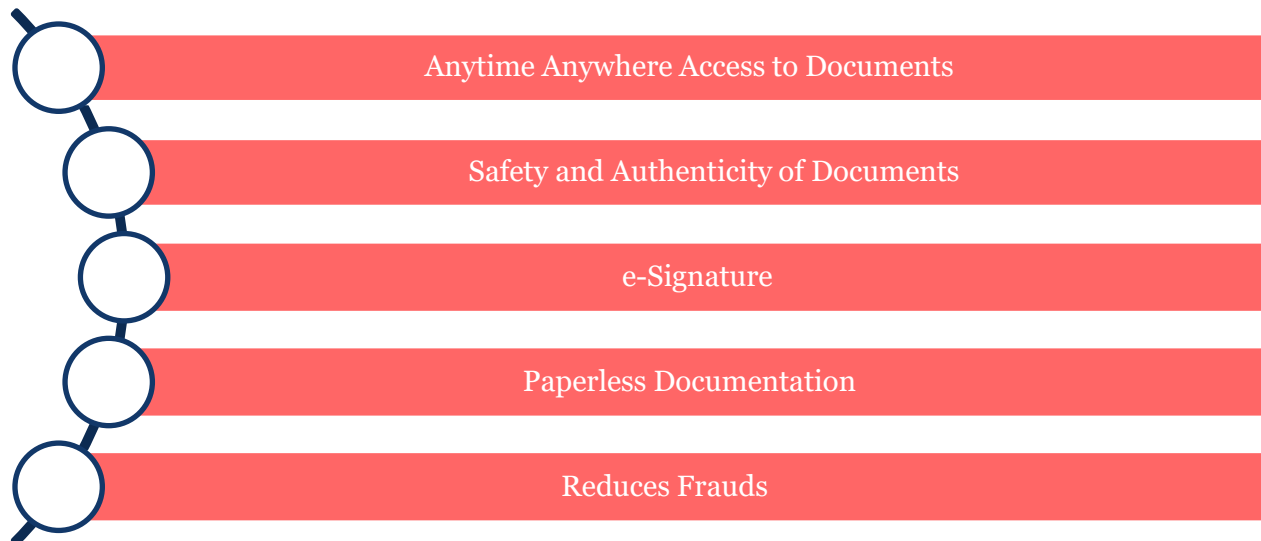
To stay safe from Aadhaar/PAN card fraud

- Do not use your Aadhaar or PAN card for casual transactions.
- Do not share Aadhaar or PAN card details with others.
- Try to submit only signed photocopies of your Aadhaar or PAN cards with specific reason for use and date of use.
- Do not enter your full name and date of birth on online portals.

Keeping Important Documents Safe

DigiLocker is a Digital Locker, a facility provided by the government of India, that enables you to store scanned copies of official documents such as Aadhaar, PAN, Driving License, Passport, Mark Sheets, Electoral voter id card, etc. You can access these documents anywhere, anytime.

Benefits of DigiLocker



Reference Reading:

- Cyber Swachhta Kendra : <https://www.csk.gov.in/>
- Full Guide on Cyber Crimes in India : <https://indiaforensic.com/compcrime.htm>
- India's Cybersecurity priorities of G 20 Presidency : <https://www.orfonline.org/expert-speak/indias-cybersecurity-priorities-for-g20-presidency/>
- Details about Indian Cybercrime Coordination Centre : https://www.mha.gov.in/en/division_of_mha/cyber-and-information-security-cis-division/Details-about-Indian-Cybercrime-Coordination-Centre-I4C-Scheme

Module 2

Financial Scams and their Prevention



Managing Calls from Unknown Numbers and International Calls to Prevent Financial Loss:

One-Ring Scam happens when the caller calls up and hangs the phone after one ring. It's a scam to trick people to give out their money.

How the One-Ring Scam works:

- The scammer hires an international premium rate number (IPRN).
- The scammer will give you one ring and then disconnect the call.
- You will think that you missed an important call and will call back on the same number.
- Your call will be taken but, nobody will talk to you from the other side.
- After receiving no answer, you will disconnect your call.
- After the call, you will realize that you have lost a large sum of money for making an international call.



To Stay Safe from a One-Ring Scam :

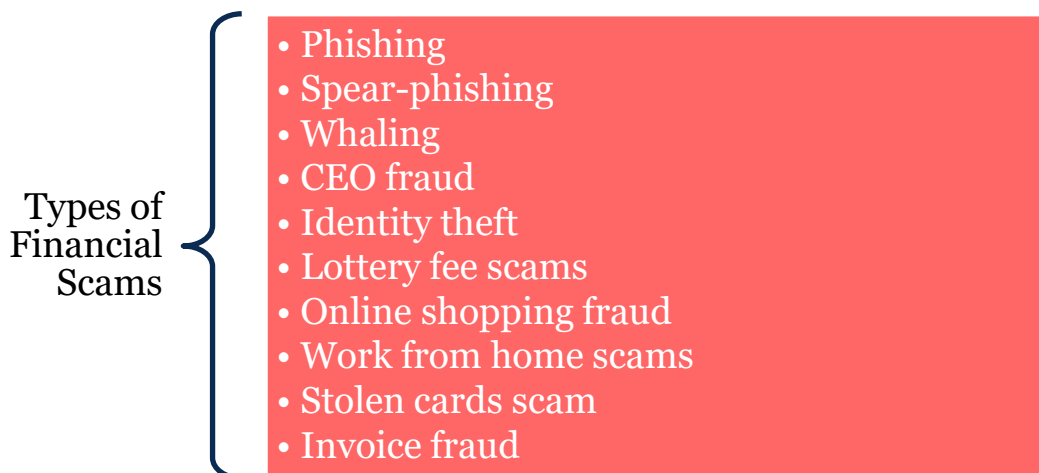
To Stay Safe from One Ring Scam

Don't answer or return any calls from numbers you don't recognize.

Before calling unfamiliar numbers, check to see if the area code is international.

Report all suspicious calls to your phone operator.

Types of Financial Scams



Phishing is an attack through a digital medium that tries to steal a person’s money or identity to reveal personal information such as credit card numbers, bank information, etc.

Spear-phishing is a type of phishing that tries to steal a person’s money or identity using very specific and personalized messages.

Similar to spear-phishing, **whaling** targets high-profile, famous and wealthy individuals such as CEOs and celebrities.

In a **CEO Fraud**, the fraudsters pretend to be the CEO of the company you work for or another authority figure and ask you to send money or give them access to your sensitive information.

In an **Identity theft**, fraudsters target your personal information, such as name, address, email address, as well as credit card or account information. They then order items online under your name and pay using your credit card information.

In a **lottery fee scam**, you get a notification that you have won a lottery and you are asked to deposit a fee to claim your prize.

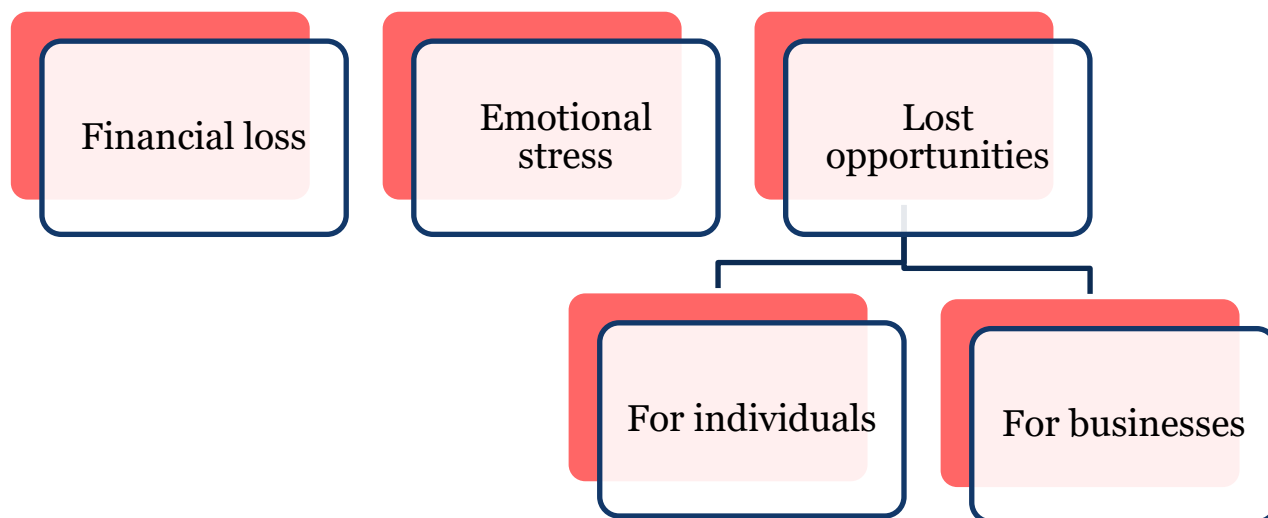
In an **online shopping fraud**, a fake shopping portal displays products at attractive prices. Once the payment is made, you receive a fake product or no product at all.

In **work-from-home scams**, fraudsters dupe people by promising that they will earn a good salary by working from home. They ask job seekers to deposit a certain amount of money. After the money is deposited, there is no track of employers.

A **debit/credit card scam** occurs when someone uses your debit/credit card information illegally for financial transactions without your knowledge.

In an **invoice fraud**, fraudsters target businesses by posing as a supplier and asking to update the details of the bank account into which invoices are paid.

Consequences of Financial Scams:



Staying Safe from Online Financial Scams:

- Keep all personal information, identity cards and bank cards safe at all times.
- Keep your PIN numbers confidential.
- Do not write your PIN numbers down or store them with bank cards.
- Never give bank account details or other security information to any person.
- Never give your money to people who offer to place it with a bank on your behalf
- Do not let anyone else use your ATM card.
- Check monthly credit card statements and other bank statements carefully for suspicious transactions.
- Promptly report the theft or loss of your card.
- Be careful when using your card to make payments on the internet.
- Disclose your Card Verification Value (CVV) only on secure payment websites
- Be careful when digitally signing any financial contract.



- Beware of calls, letters, e-mails or faxes asking for your help to place huge sums of money in an overseas bank.
- Do not reply to spam or unsolicited e-mails that promise you a job or some other benefit.

If your online banking details have been compromised, take the following measures...

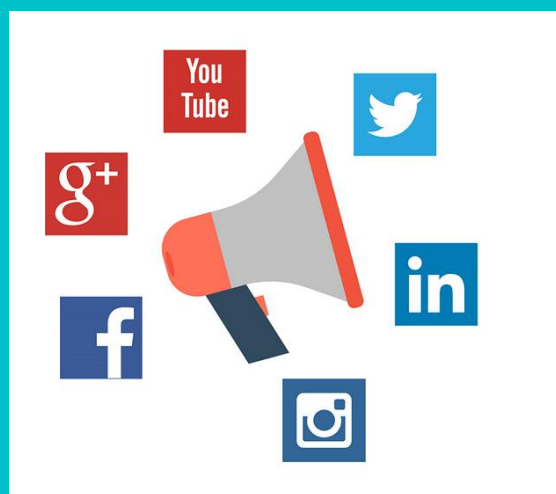
1. Notify your bank immediately
2. Block your credit/debit card or UPI app
3. Change your passwords for net banking
4. Change your UPI, Debit Card and Credit Card PINs
5. Cancel current debit/credit cards and ask for replacements
6. Set up a new security feature (multi-step authentication)

Reference Reading:

- More about Financial frauds:
<https://cybercrime.gov.in/pdf/Financial%20Fraud%20Brochures%20final.pdf>

Module 3

Social Media



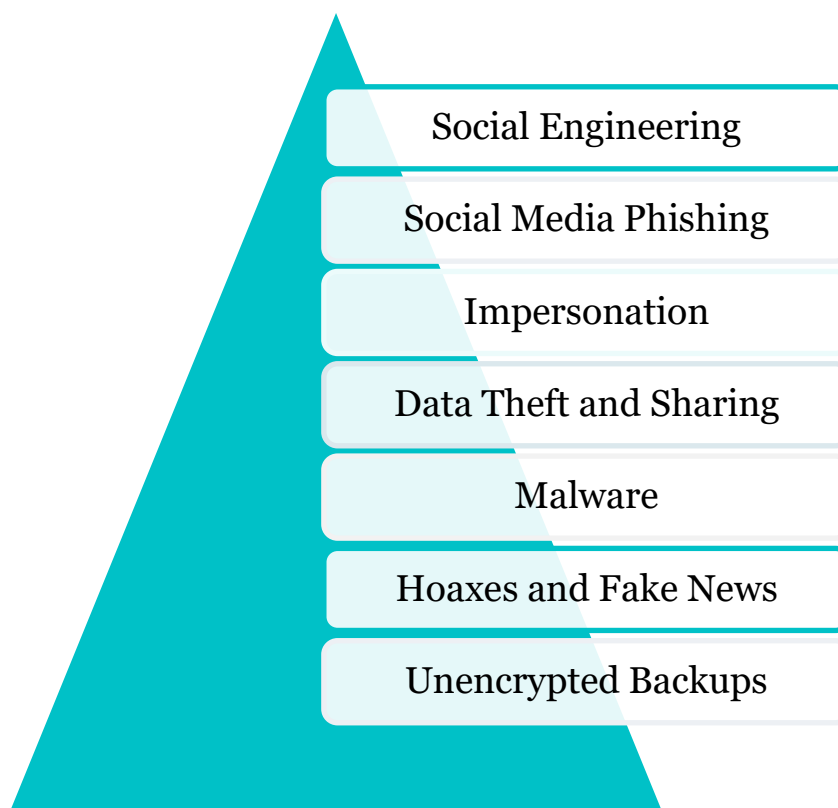
Widely Used Social Media Platforms

- WhatsApp
- Instagram
- Facebook
- Twitter
- Sharechat
- Snapchat



Social media platforms enable users to display pictures and post them publicly. Fraudsters secretly collect information without the user’s knowledge. With the collected information, fraudsters then approach users in different ways.

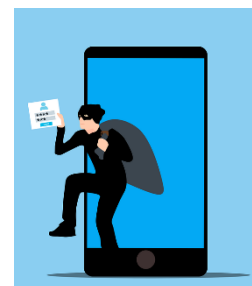
The different ways through which fraudsters scam social media users are:



Social Engineering

This attack involves manipulation to gain unauthorized access, network, and financial gain. Fraudsters trick a user by representing themselves as authentic representatives of a bank or other organization in order to make a transaction or money transfer.

To safeguard yourself, never make transactions or give bank details based on phone calls.



Social Media Phishing

The purpose of phishing is to obtain personal data or access a user's social media accounts.

Impersonation

In this scam, fraudsters pretend to be someone who can be trusted by a user to steal sensitive information.



Social Media Scrapping



This is an example of Social Media Phishing and Impersonation. Fraudsters make fake calls as customer executive to retrieve personal information. It includes names, dates of birth, personal photos, and location. The fraudsters use this information for data/identity theft in future

To safeguard yourself from social media scrapping:

- Never share your personal details
- Immediately report about such calls
- Report and block the suspicious profile

Data Theft

In this scam, fraudsters illegally transfer confidential information. Malware can be disguised typically in the Like button, audio clips, videos or links on social media.



Hoaxes and Fake News

In this scam, fraudsters spread false information to mislead users by promoting some propaganda.

To safeguard ourselves from hoax calls and messages, we should:

- Always check photos and media carefully.
- Verify the information from reliable sources.
- Block and report illegal and dangerous conversational groups.
- Use group privacy settings to prevent ourselves from being added to unwanted groups.



Unencrypted Backups

In this scam, the data is not encoded by the algorithm and can be read by anyone.

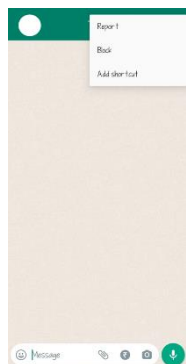
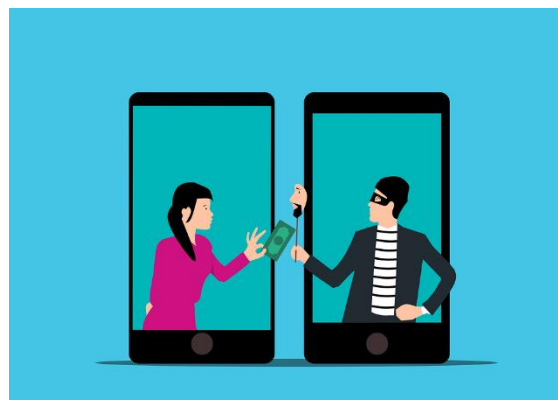
For recognizing fake accounts, observe the following behaviours of a fraudster on social media:

- Avoids taking calls and meetings
- No online presence
- Limited friends/followers
- Very recent profile
- Professional pictures
- Stolen pictures
- Asks for money
- Asks for explicit images or video

The most common form of Social Media Fraud is **Catfishing**.

Catfishing is a form of online deception. The fraudster pretends to be someone else by using a fake identity and deceives the easy targets by forming a romantic relationship

- To support the fake identity, a cat-fisher uses made-up stories and fake photos.
- A cat-fisher usually asks for money and personal information



All the social media platforms have the features of “**report**” and “**block**” with the similar function of protecting a user from another troublesome or fake user.

Block

Blocking the contact disables the receiving of messages from the user.

Report

Reporting helps to notify the company if the terms and conditions are being violated by a user or a group

Advantages of WhatsApp are:

- No pop-up ads
- Easy to use
- No charge messaging service
- Media, location and status sharing
- Groups enables mass interaction

- Video calling

Disadvantages of WhatsApp are:

- There are many privacy concerns
- There is a lot of unverified information sharing
- WhatsApp is very addictive

Social Media Etiquette:

Social media etiquette are the guidelines that social media platforms and users use to preserve their reputation online.



Social Media Do's

- Communicate with known contacts
- Ask for permission and respect boundaries
- Use group controls
- Share only rightful photos and videos
- Post appropriate photos and videos
- Follow the guidelines of social media platforms.

Social Media Don'ts

- Spam other users
- Use or share the personal information of others
- Bulk message
- Use abusive language
- Foster fake news and misleading information
- Over-share

WhatsApp Dos:



✔ Limit the visibility of profile photos, status, and about information to your known contacts.

✔ Use group privacy settings to avoid being add in random groups.

✔ Use end-to-end encryption.

✔ Turn off the live location in chat.

✔ Block the unknown users who are trying to approach you.

WhatsApp Don'ts



✘ Share your personal information with strangers.

✘ Set your privacy setting to public.

✘ Disrespect other user's privacy.

Instagram Dos



✔ Add known people in your followers.

✔ Post appropriate photos, videos, information.

✔ Respect other user's privacy.

✔ Use block/report for fraudsters.





Instagram Don'ts



-  Share sensitive information on public accounts.
-  Use other's post without permission.
-  Buy followers.
-  Disrespect others

Facebook Dos



- | | |
|---|---|
|  Share verified news and information. |  Use privacy settings to secure your data and information. |
|  Only share rightful media. |  Interact with known users. |




Facebook Don'ts



-  Share unverified news.
-  Click on random links.
-  Fill in your credentials like bank account details on any advertisement.

Twitter Dos



-  Use the Privacy and Safety option to protect your data and tweets from misuse.
-  Use appropriate language to express your thoughts through tweets.
-  Accept the requests of only known users.

Twitter Don'ts



-  Force your opinions on others.
-  Use foul language.
-  Share your live location publicly.

Social media is very helpful in communication and keeps us updated with the world. But we should use it responsibly. There are a lot of interesting facts and news available on social media. We need to be cautious before circulating them.

Reference Reading:

- Cyber Jaagrookta Diwas: <https://www.youtube.com/watch?v=6whmq4EwIIo>
- Cyberbullying Facts : <https://www.youtube.com/watch?v=oXo8N9qlJtk>

Module 4

Identity Theft



Passwords and Authentication

A Password is a string of characters used to verify the identity of a user during the authentication process.

Passwords provide the first **protection** against unauthorized access to your smart devices and personal information.



- Passwords should contain at least ten characters and have a combination of characters such as:

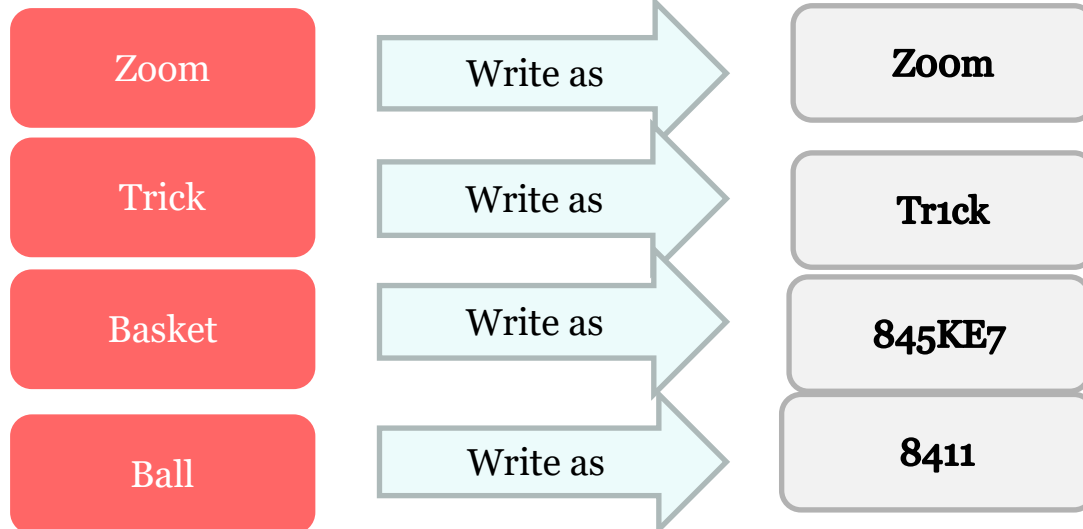
Special Characters

Upper-case and lower-case letters

Numbers

- Avoid using sequences such as “12345” or “qwerty”

- You can use look alike numbers instead of letters—use zero 0 instead of O



- You can replace the numbers with special characters too which are mentioned along with the numbers on your keyboard.



Authentication involves the following factors:

- Something the user knows such as password, PIN
- Something the user has such as Debit Card and Credit Card
- Something unique to the user such as Biometric characteristics



UPI Pin, Banking Card Pins and Biometric Authentications

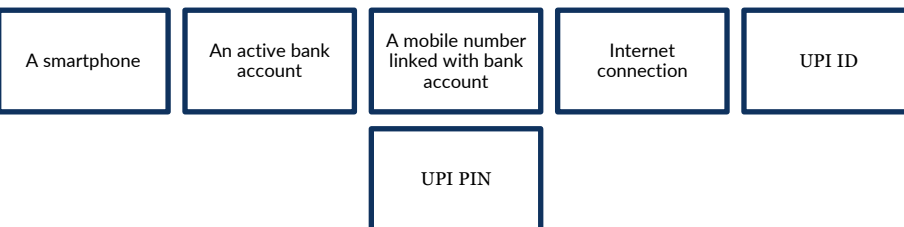
1. UPI Authentication



UPI Stands for Unified Payments Interface

A payment system that allows you to transfer funds across banks

To use UPI you need:



UPI ID

- Automatically Generated
- Required to access UPI account

UPI PIN

- Unique, 4 or 6-digit passcode created by the user
- Safeguards your UPI account

2. Banking Cards Authentication

Banking Card PIN includes PIN for:



P
Personal

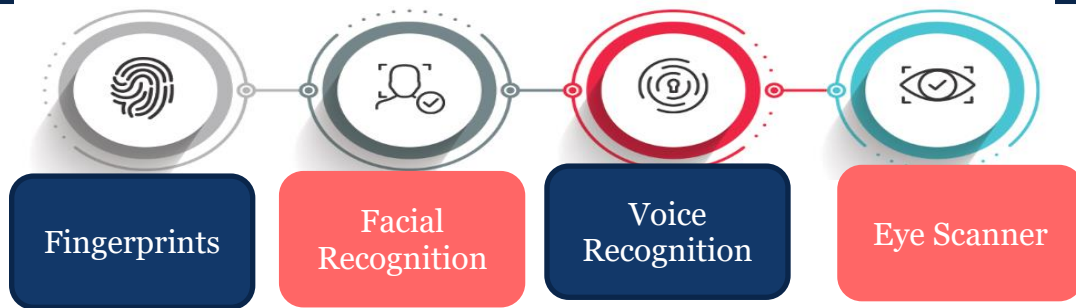
I
Identification

N
Number

A four-digit code that is unique to an account holder's card.

3. Biometric Authentication

Biometric authentication matches the following biometric features to access a smart device or your banking account.



Two-factor Authentication



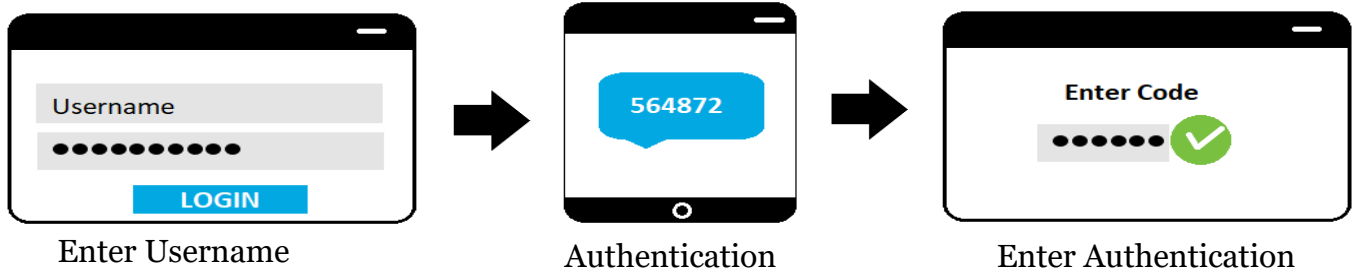
Two-factor authentication is also referred to as 2FA

Safeguards your online accounts by verifying user details and passcode

Monitors and helps safeguard your online account credentials and data

Malicious Websites and Apps

Two-factor authentication uses a password and a one-time passcode/authentication code sent to a mobile phone via SMS which when entered allows the user to finally access the account.



Malicious Websites and Apps

Malicious Websites and Apps are one of the most common forms of cyber-attack being used.

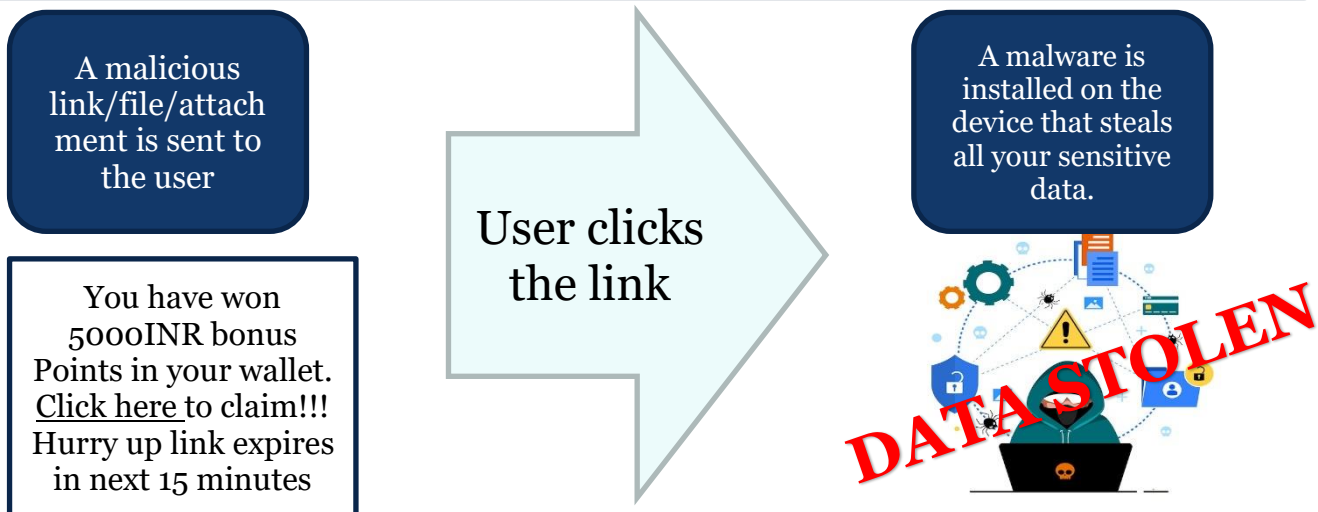
The hackers send links to you via SMS, emails or advertisements displayed on your social media accounts

You need to be alert as just on a click all your personal information will be leaked to the hackers.

Malicious Websites may instruct you to do the following:

- Download software/any invoice/file/app
- Save a file
- Run a program

How do Malicious Websites/Apps Work?



Here are few points that will help in safeguarding your device from malicious websites and App:

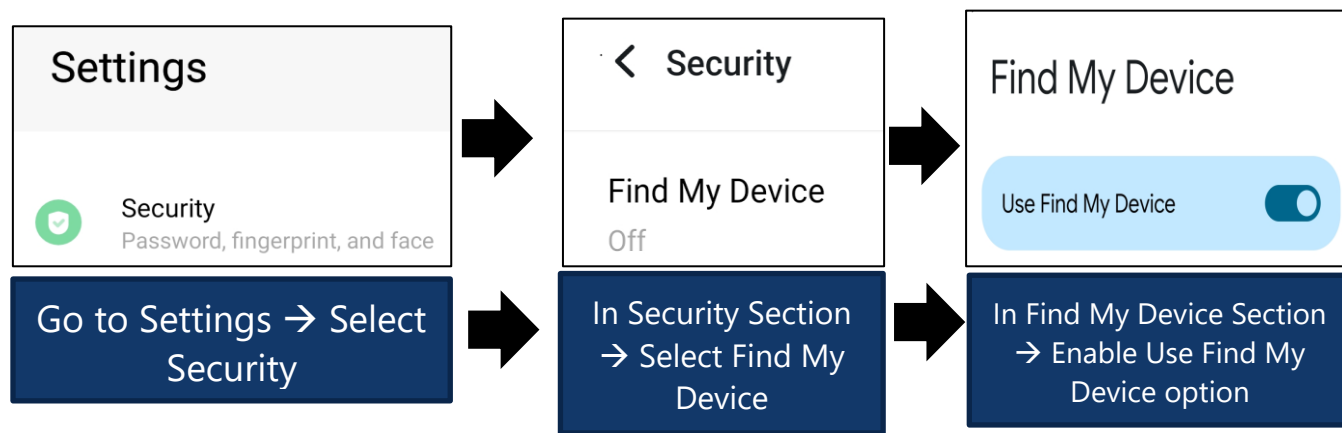
- Never click on a link embedded in an email
- Never click on a link received from any external third-party message.
- Never install any random app that asks for your personal sensitive information
- Always check for “https” in URL while making any online payments.
- Read the URL carefully. A minor twist in the spelling of the website may cause a danger.
- Install your Banking App from the link provided by the bank.
- Always check the URL before accessing any website.
- Shop at trusted websites only and not through any random links received.
- Install Secure Apps from a trusted play store.
- Check Emails before opening them. Open only if you know the sender.
- If you have logged into any account online, always log off before leaving the Website
- Update your antivirus regularly.

Managing Lost Phones Remotely

Only in the following **conditions**, the lost phone can be remotely accessed

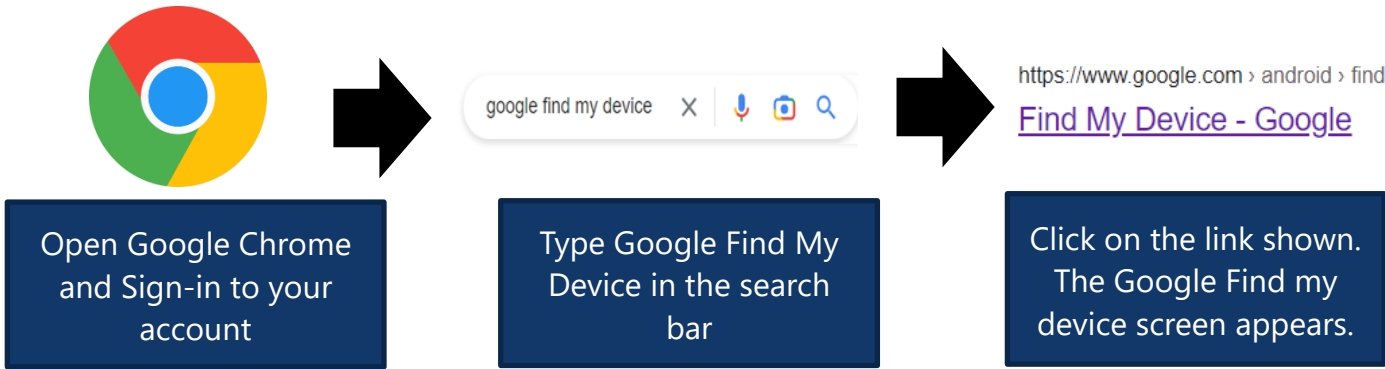
- Phone is turned on
- Signed In to a Google Account (in case of android) or iCloud in case of iPhone
- Connected to the internet
- Find My Device is enabled

To enable “Find my Device” option you need to perform the following steps:

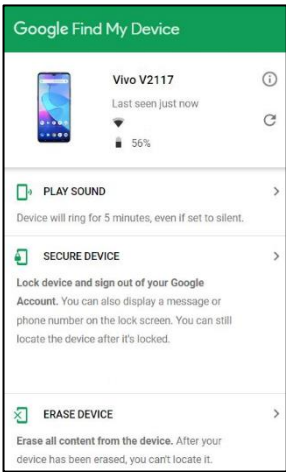


This will allow you to access your phone remotely in case of lost or theft.

To remotely erase your lost smartphone data, you need to perform the steps shown:



Now, you can secure your device or erase the content on it by selecting the appropriate option as shown on the screen.



Phishing and Online Forms

We all know that online forms are:

- Used to create survey forms containing multiple questions.
- Used to analyze the survey results in real-time.
- Accessible from any device

But they are also used by hackers often to hack your personal information.

Hackers may pretend to be your bank staff and will inform you that they have sent you an email with a form attached, asking you to fill-in and send it asap so that your savings scheme can be renewed.


Never go by such phishing scams. Immediately confirm if you need to fill in the online form from your bank.


Here is a sample of the phishing online form emails.


<p>Attention: Urgent External email</p> <p>Dear Account Holder</p> <p>This is to notify you that there is some missing information with respect to your KYC. Kindly fill in the attached form and submit it by today otherwise your account will be frozen till further notice and you won't be able to make any financial transactions from this account.</p> <p>Please click the link below to update your account:</p> <p>Update Now</p> <p>We respect your privacy!</p> <p>Thanks and Regards</p> <p>MSN20002</p> <p>Unnamed 555555.png</p>	<p>Fill in the details:</p> <p>First Name:*</p> <p>Last Name:*</p> <p>Address 1:*</p> <p>Address 2</p> <p>Email ID:*</p> <p>Registered Mobile Number:*</p> <p>Aadhaar Number:*</p>
--	--


Phishing Form e-mail

Dos and don'ts of online forms to remain safe:

 Never provide sensitive information via online forms unless and until you are sure about the source sending the form.

 Always cross-check with your bank or the concerned authority about you receiving the form via e-mail.

 Never open an email from an external third-party vendor.

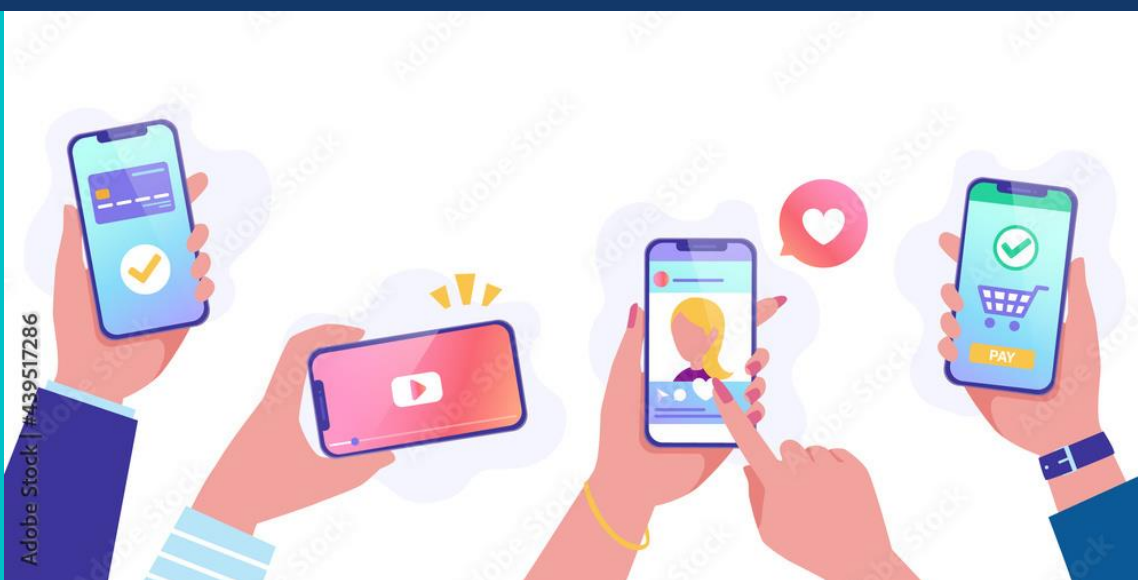
 Read the sender's email id and confirm before replying to them.

Reference Reading:

- **How to Reset your UPI PIN :** https://www.youtube.com/watch?v=ZoEqpKF_Sjw
- **Securing your Instagram account with two-factor authentication:** <https://help.instagram.com/566810106808145>
- **Securing your Facebook account with two factor authentication :** <https://www.facebook.com/help/148233965247823>
- **Managing Lost iPhone remotely :** <https://support.apple.com/en-in/guide/security/secc46f3562c/web>
- **How to Check a Website for Malware Infections :** <https://www.sitelock.com/blog/check-website-for-malware/>
- **Malicious Apps with Potential Harm to Your Smartphone:** <https://www.91mobiles.com/hub/malicious-apps-malware-google-play-store/>

Module 5

Being Internet Smart



Safe Browsing Tips:

There are some ways by which browsing online can be safe.

BE INTERNET SMART

- **Share with Care**

News travels rapidly. It is important to forethink the consequences of this on people.

- **Communicate Responsibly**

- Foster thoughtful sharing through online communication just like face-to-face communication.
- Form guidelines for appropriate communication.
- Secure family and friends' details.

- **Be Internet Alert**

- Don't Fall for Fake news.
- It's important to help people to understand
 - What's real and what's fake is a very important lesson in online safety.
 - People and situations online aren't always as they seem.

- **BE INTERNET STRONG**

- Secure Your Secrets
 - Privacy and security are as important online as they are offline.
 - Safeguarding personal information helps user to avoid damaging their devices, reputations, and relations.

- **BE INTERNET KIND**

- It's Cool to Be Kind
- The Internet is a powerful tool to spread positivity as well as negativity. The user can take the concept of "treat others as you would like to be treated" to their actions online, building a positive influence on others and eliminating improper behaviour.

- **BE INTERNET BRAVE**

- Users can make each other comfortable talking about something questionable by fostering open communication at home and in the public place.



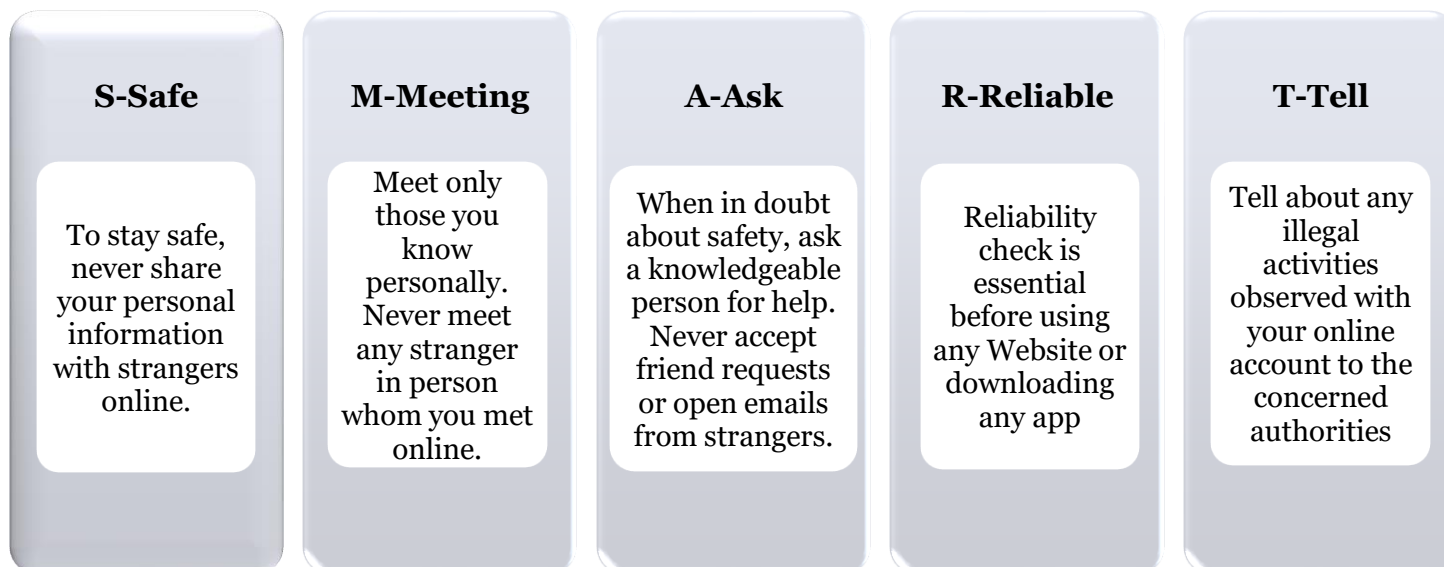
Adobe Stock | #68153307



Adobe Stock | #47036812

SMART Browsing:

Hackers can build phishing scams based on information collected from social profiles. Here are some **SMART** tips to protect yourself from scams.



- Do not share your personal information like traveling plans or details of the family. Hackers can use the information from that post against you
- Do not post, share or tweet your e-mail and contact number online.
- Do not accept strangers' friend requests.
- While sharing photos from your workstation, make sure anything from your computer system is not revealing.
- Always try to use different profile pictures across different social media platforms.

Safe Browsing Tools

Firewall: A firewall is a software that acts as the first defence line to prevent unauthorized access to the network and inspect the traffic using some rules to reduce security risks.



Antivirus:

A computer virus is a malicious code or program that replicates itself and is designed to disturb the way a computer operates. A virus operates by inserting or attaching itself to a legitimate program. A virus has the potential to damage or harm the system software by corrupting or destroying data.

Anti-virus is a security program installed on your computer or mobile device to prevent infection by malware such as viruses and worms.



Benefits of installing anti-virus in your device or system are:

- Detecting, blocking and removing viruses.
- Preventing identity theft and blocking phishing.
- Warning about malicious websites and links.
- Keeping online accounts protected with secure password encryption.
- Smooth running of computer.



The Internet is a complex mix of information, distracting advertisements, dangerous malware and deceiving click-bait links that can lead unsuspecting users into a cyber nightmare. In order to navigate the tricky terrain of the web without worrying about malware and other browser-based attacks, browser vendors provide several helpful security features.



Features offered by Browsers for Safety on the Internet

- Safe browsing feature by Google Chrome
- SmartScreen filter by Microsoft
- Phishing filter by Mozilla Firefox
- These features help protect computers from phishing attacks and malware.

Here are some steps which can keep you safe online and can help you build protective shield online.

- **Sensitive Browsing:** We often use open networks in cafes etc. for bank transactions. Cybercriminals copy your bank details in a second and rob you of your hard-earned money.
- **Spam messages** are easy to detect and avoid. Words like 'Message from RBI' or 'your help is required', etc. are used in these messages. You have to avoid them and you should not open such suspicious links.



- **Strong passwords** are difficult to crack. Always try to use different passwords for every different online account. You should always set your passwords as per the password policy of the websites. Passwords should be alpha-numeric and have special characters to make them strong.
- **Sign out from your accounts/sessions** : We generally are logged in to our mail or social media accounts or banking sessions on our devices. But this can also be a threat to our cyber security. Always log out from your accounts and your bank logins on your devices.
- **Security on social media**:Uploading pictures on Facebook or Instagram and other social sites is very common nowadays, but these images can be misused. To keep your online data safe from stalkers and other risks, you should change your account settings from public to private.
- **Data Back-up**: Always back-up your data with the help of either physical drives or online storage i.e., cloud storage. In this way, your data will be safe if anything happens to your device.
- **Websites' Safety Warning** : Several site safety extensions like McAfee Site Advisor warns you about the safety of browsing a website.












Public and Free Wi-Fi

Public Wi-Fi is unsafe and risky. Some of the potential risks from the insecure connections of Public Wi-Fi

- Man in Middle attack
- Unencrypted Networks
- Malware distribution
 - Viruses
 - Worms
 - Trojan horses
 - Ransomware
 - Adware
- Snooping & Sniffing
- Theft of personal information
 - Login Credentials
 - Financial information
 - Personal data
 - Pictures
- Session Hijacking



Staying Safe when using Public Wi-Fi

<p>Avoid</p>  <p>Opening sensitive documents/files</p>	<p>Use</p>  <p>VPN secure connections using encryption over a public Wi-Fi</p>	<p>Open</p>  <p>Only https websites</p>	<p>Enable</p>  <p>Secure browser settings</p>	<p>Use</p>  <p>A privacy screen</p>
<p>Switch-off</p>  <p>File sharing</p>	<p>Use</p>  <p>Two-factor authentication</p>	<p>Ensure</p>  <p>Your operating system & browser are up-to-date</p>	<p>Remember</p>  <p>To log out of public Wi-Fi</p>	

Types of Cybercrimes:

- **Infringing Copyrights:** Using the copyrighted work of someone without permission. For example, using an image from a company website and posting it on your personal account.
- **Ransomware attacks:** Ransomware is malware that threatens to publish or blocks access to data or a device, by encrypting it, until the ransom fee is paid to the attacker.
- **Illegal Gambling:** Online gambling is involved betting on casinos or sports over the internet.

- **Cyber Espionage:** Cyber espionage is the intentional theft of data, sensitive information, or intellectual property from or through computer devices to gain advantages in competition. For example, political parties steal the data of competitors during elections.
- **Email and Internet fraud**
- **Identity fraud**
- **Theft of financial or card payment data**
- **Cryptojacking:** Cryptojacking is a type of cybercrime that involves the unauthorized use of people's devices (computers, smartphones, tablets, or even servers) by cybercriminals to mine for cryptocurrency. Like many forms of cybercrime, the motive is profit, but unlike other threats, it is designed to stay completely hidden from the victim.
- **Cyberextortion:** Cyberextortion is a crime involving an attack or threat of an attack coupled with a demand for money or some other response in return for stopping the attack.

Methods to protect your device from hackers:

- Use Firewall
- Install Anti-virus
- Use Strong Passwords
- Use up-to-date browsers
- Secure your network
- Use two-factor authentication
- Use security PINs for apps and personal information

Reference Reading:

- **Personal Privacy: Top 12 Tips For Safer Browsing On The Internet :** <https://cybersecurityventures.com/12-tips-for-safer-browsing/>
- **5 Tips to Help Women & Girls Stay Safe Online :** <https://www.globalcitizen.org/en/content/tips-to-help-women-girls-stay-safe-online/>
- **How to Avoid Public WiFi Security Risks:** <https://www.kaspersky.co.in/resource-center/preemptive-safety/public-wifi-risks>

Module 6

Digital Rights, Laws and Redressal Mechanisms



Digital Citizen: A digital citizen is a person who uses the internet and other digital technologies responsibly









Roles of a digital citizen:

- Protect your personal information
- Carefully manage your digital footprint (the information about a particular person that exists on the internet as a result of their online activity)
- Adhere to online transaction laws
- Stand up for illegal activities
- Know your rights as digital citizen

Be a responsible **SMART** digital citizen while sharing personal information:

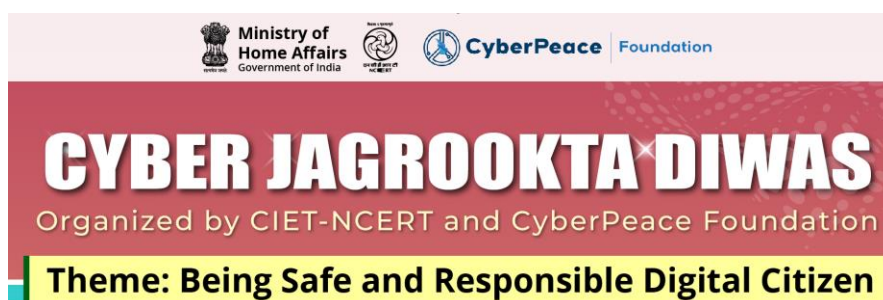
S-Safe	M-Meeting	A-Ask	R-Reliable	T-Tell
<p>To stay safe online, never share your personal information with strangers online.</p>	<p>Meet only those you know personally. Never meet any stranger in person whom you met online.</p>	<p>When in doubt about safety, ask a knowledgeable person for help. Never accept friend requests or open emails from strangers.</p>	<p>Reliability check is essential before using any Website or downloading any app</p>	<p>Tell about any illegal activities observed with your online account to the concerned authorities</p>

Responsibilities while Using Bank Account Online

 Do	 Don't
 Always use the login credentials issued by the bank.	 Never used any external link to log into your bank account.
 In case of any issue always call on the numbers mentioned on the bank documents or their official website.	 Never call on the number mentioned in any SMS. That could be a fake message.
 Ensure your KYC (Know Your Customer Details) are updated at your bank.	 Never share your KYC details with any external party/person.

Government Initiative Towards Responsibilities of Digital Citizens

- In order to create awareness amongst students of schools & colleges, teachers and parents it is proposed to observe “Cyber Jagroota Diwas” on the first Wednesday of every month.
- Initiated to create awareness about the right and responsibilities of digital citizens



Rights of Digital Citizens:



- **Right to Access:** Every citizen has right to access the internet. It is considered as an essential right towards freedom of opinion. As per Supreme court of India, Internet Access is the Basic Fundamental Right

- **Right to Freedom of Expression, Information and Communication:** Every citizen has right to use social media network to express, to access any information or communicate.



- **Right to Privacy and Data Protection:** The user has the right to safeguard their personal information presented over social media. It is mandatory for all social media platforms to provide privacy and data protection setting such as user can choose who see your profile or can keep their profile as private.

- **Right to Protection:** The Government must ensure the protection of internet users is ensured through social media platforms. Also, users have easy access to the cyber cells to report any illegal activity over the internet by calling at 1930.



Digital Tools for Online Safety of Citizens – Online Transactions

- Bharat Interface for Money-Unified Payments Interface (BHIM-UPI)
- Immediate Payment Service (IMPS)
- Pre-paid Payment Instruments (PPIs)
- National Electronic Toll Collection (NETC)
- Real-Time Gross Settlement (RTGS)



For downloading apps, use the following secure online stores:



Illegal Cyber Activities:

The most common illegal cyber activities are:

- **Cyberstalking** - Cyberstalking refers to stalking any person using electronic media. It includes:
 - Gaining information with the intention of identity theft.
 - Sending unwanted, frightening, or obscene emails, or messages.
 - Harassing or threatening on social media.

- **Breach and violation of privacy/confidentiality**
 - It includes publishing or broadcasting any private information or image on social media/any platform without consent of the person.
 - Only when required by law, the banks and social media platforms can share one's personal information.

- **Voyeurism**
 - It refers to watching, capturing or sharing images or videos of a person engaged in private act without their consent.
 - It is a punishable act under IPC section 354 (C).
 - It should be immediately reported to the Cyber cell/Women cell/nearby Police Station.

- **Steps to protect yourself from Cyberstalkers are:**
 - Report about to the cyber cell/women cell
 - Block them
 - Tell family members what is going on
 - Set privacy filters on your account
 - Save all evidence
 - Tell them to Stop



Legal Provisions for Illegal Digital Activities

As per the Indian Penal Code, 1860 following are some of the legal provisions

Section	Illegal Activity	Punishment
Section 354A	<ul style="list-style-type: none"> Showing or sharing sexual content without consent of women Asking for sexual favors Posting/sending sexual remarks/messages 	<ul style="list-style-type: none"> Rigorous imprisonment for a term which may extend to three years, or with fine, or with both.
Section 354C	<ul style="list-style-type: none"> Voyeurism 	<ul style="list-style-type: none"> Fine as well as imprisonment of up to three years on the first conviction Seven years on subsequent convictions.
Section 354D	<ul style="list-style-type: none"> Cyberstalking 	<ul style="list-style-type: none"> Imprisonment up to three years for the first offence Liable to fine and five years' imprisonment on subsequent conviction

As per the Information Technology Act, 2008 following are some of the legal provisions

Section of IT ACT	Illegal Activity	Punishment
Section 66E	<ul style="list-style-type: none"> Violation of privacy Capturing, publishing or transmitting the image of a private area of any person without their consent 	<ul style="list-style-type: none"> Imprisonment, which may extend to three years, and/or fine.
Section 66C	<ul style="list-style-type: none"> Identity theft Cyber Hacking Misuse of Electronic Signature 	<ul style="list-style-type: none"> Imprisonment which may extend to three years Fine which may extend to rupees one lakh
Section 67	<ul style="list-style-type: none"> Publication or transmission of obscene content. 	<ul style="list-style-type: none"> Imprisonment extending up to three years and fine for the first conviction Five to seven years and fine upon the second conviction

As per copyright act, when you post your creative work on social media, you own its copyright. No one can use the work without your permission, nor does the platform take ownership.

Redressal Mechanisms for Illegal Digital Activities

You can register your complaint against any cyber illegal activity at the following :

National Cyber Crime Reporting Portal

• <https://cybercrime.gov.in/Default.aspx>

National Cyber Crime Reporting Helpline Number -1930 (9.00 AM to 6 PM)

• <https://ncrb.gov.in/en/node/2318>

UMANG (Unified Mobile Application for New-age Governance)

• <https://web.umang.gov.in/landing/department/cybercrime-reporting-portal.html>

Cyber Police Portal

• <https://cyberpolice.nic.in/>

Steps to file a complaint on the Cyber Crime Portal

1. Go to the link: <https://cybercrime.gov.in/>
2. Scroll Down to the following section of the website and then click the **File a complaint** button
3. Click the **Report Anonymously** button
4. Fill in all the sections of the form and submit it for further processing. Make sure you have the evidence documents ready such as screenshots.
5. Your complaint will be registered. You can also call 1930 for any assistance or register the complaint

Reference Reading:

- Refer to the following links to learn more about Cyber Jaagrookta Diwas:
[Cyber Jaagrookta \(Awareness\) Diwas \(Day 1 - Day 5\)](#)
- Refer to the following links to learn more Safe use of social media platform:
[Be Careful While Using Social Media Platforms](#)
- Refer to the following links to learn how to report online cybercrime:
[Cyber Crime Helpline Number](#)
- Refer to the following links to learn how E-Commerce Laws And Regulations In India:
[E-Commerce Laws and Regulations in India](#)
- Refer to the following links to learn how can I Tell If My Online Transaction Is Secure?
[Is My Online Transaction Secure](#)

Suggested Practical Activities

Now that you have completed the online learning modules of the Digital Safety and Security Program, please try out these activities to practice and apply the learning in your real life. We hope these activities will reinforce your learning.

1. Create unique and strong 10-character ASCII passwords for all your social media, banking, e-commerce and email accounts
2. Back up your data every day or set up an automatic back-up facility
3. Check and update your operating system software regularly (Windows/IoS/Android)
4. Use the incognito mode while browsing the Internet and find out what is different about it
5. Set up your anti-virus software to enable banking and payment protection for facilitating safe financial transactions on your bank websites
6. Set up your antivirus software to enable parental control to block dangerous and offensive websites when young children use your devices
7. Keenly observe calls from unknown numbers on your phone and don't answer if they are from International Unknown Numbers
8. Submit only signed photocopies of Aadhaar/PAN and also mention the date, to whom you are submitting the photocopies and the purpose of submitting them
9. Create a DigiLocker account and upload your Aadhaar, PAN, Driving License and Education certificates
10. Change settings on WhatsApp to prevent yourself from being added to groups
11. Try out the "block" feature on WhatsApp for an unknown person (or number) repeatedly sending you messages
12. Change Facebook/Instagram/other social media settings to private
13. Create 2-Factor authentication for your mail id
14. Enable find my phone on your google account/IoS account
15. Enable security features on your web browser (Google Chrome/Microsoft Edge/Mozilla Firefox /Opera/IoS)
16. Delete browsing history from your device once a week
17. Watch out, support and help anyone/young children who are experiencing cyberstalking or any illegal cyber activities
18. Explore the various services and precautions shared on the National Cyber Crime Reporting Portal (<https://cybercrime.gov.in/Default.aspx>)

19. Explore UMANG Website
(<https://web.umang.gov.in/landing/department/cybercrime-reporting-portal.html>)
20. Explore the various cells for redressal on the National Commission for Women Portal (<http://ncw.nic.in/ncw-cells>)

