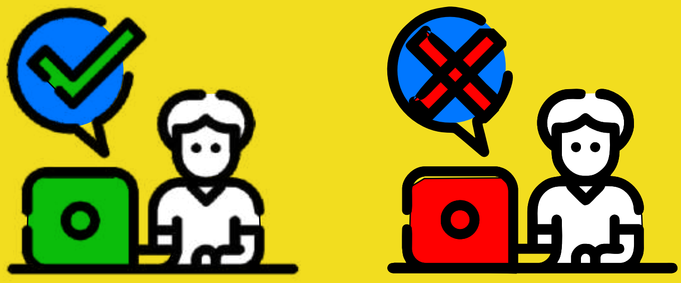
गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS

CYBER HYGIENE

FOR CYBER SPACE

DOs & Don'ts



BASIC

Published by:
Indian Cyber Crime Coordination Centre (I4C)
Cyber and Information Security (CIS) Division
Ministry of Home Affairs
Government of India
North Block
New Delhi – 110001

Introduction

Cyber space is a complex and dynamic environment of interactions among people, software and services supported by worldwide distribution of Information and Communications Technology (ICT) devices and networks. The exponential increase in the number of internet users in India clubbed with rapidly evolving technologies has brought in its own unique challenges.

Indian Cyber Crime Coordination Centre (I4C) under Cyber & Information Security (CIS) Division of the Ministry of Home Affairs, has prepared this manual to disseminate Cyber Hygiene Best Practices for the benefit of Industrial Bodies/General Public/Government Officials. This should not be considered as an exhaustive list of precautions for Cyber Hygiene but baseline precautions that are to be taken.

Disclaimer: This document is for guidance and awareness only. The contents of this document are not to be used in any legal validation in investigation, etc. The purpose is to share basic information on these matters.

CONTENTS

INTRODUCTION

Information Technology has made a significant contribution and impact on socio-economic scenarios. Rapid adoption of digital technology has led to employment generation, ease of living, ease of doing business and access to information.

Adoption of digital technology and internet have also led to increase in cyber crime incidents. It can be controlled or minimized with care, precaution, awareness and with the use of appropriate tools to secure the information. The tips and recommendations provided in this document may help the user to keep the information/data & device secure.

COMPUTER SAFETY TIPS

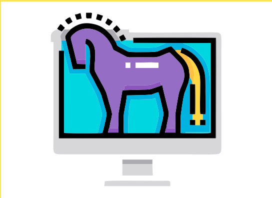
What is computer security?

Computer security is the protection of computer systems and information from theft and unauthorized access. It is the process of prevention and detection of unauthorized use of the computer systems.

Computer security threats

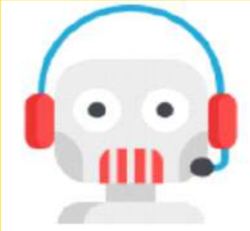
Computer security threats are possible dangers that can cause impediment to the normal functioning of the computer. Some of the common and harmful computer threats are depicted below:-

Computer Viruses



Computer Trojans

Phishing Mail/URL



Botnet

Keylogger

DOs

COMPUTER SAFETY TIPS

- Always download applications/ software from trusted sources
- Regularly update Operating System, Applications and Anti-Virus software of the system
- Ensure backup of important data/files/ documents at regular intervals
- Lock the computer screen when not in use
- Always keep the computer firewall “ON”

DOs

COMPUTER SAFETY TIPS

- Use account with limited privileges on systems
- Always insist on using genuine/ licensed software applications
- Scan all the files/contents downloaded from websites, e-mails or USBs
- Uninstall unnecessary programs or software

DOs

COMPUTER SAFETY TIPS

Use "Task Manager" to identify any unwanted programs running on the computer system

Access to servers should be allowed via Multi-Factor Authentication (MFA)

Disable Remote Desktop Connection and network file sharing , when not in use

Set Operating System update settings to "Auto-Download" option for regular updates

Don’ts

COMPUTER SAFETY TIPS

- Do not install or use pirated copies of software/ applications under any circumstances. These may contain malware

- Do not use guessable/weak passwords like “password@123", etc.

- Do not click on untrusted/unexpected Pop-Up advertisements/ programs

- Do not dispose computer or hard drive without deletion and wiping of data

1.1 USB DEVICE SECURITY

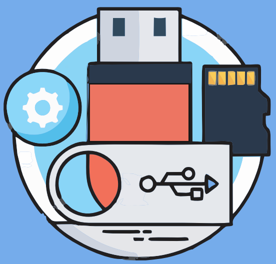
USB devices are very convenient to transfer data between different computers. One can plug it into a USB port, transfer important data, remove and use it appropriately as desired. However, this portability, convenience and popularity also bring different threats to the information system.

Threats

Unsecured use of USB drive can lead to data thefts, data leakages and malware infection. USB security can be ensured with care, awareness and by using appropriate scanning tools to secure the information.

Types of devices which support USB

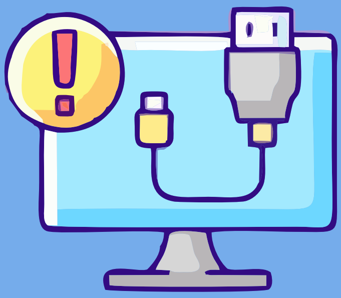
- Flash Drive/ Pendrive
- Portable Hard Drive/ SSD
- Mobile Phone



- Digital Camera
- Card Reader
- USB Keyboard/ Mouse

USB DEVICE SECURITY

DOs



Scan USB device with Antivirus/ Endpoint Protection before its use

Autorun/ Autoplay feature shall be disabled in all the computers, while using USB

PASSWORD SECURITY MANAGEMENT

Password helps in protection of information accessible via computers. It allows access to information only to authorised users. Strong multi character passwords must be enforced in all the systems.

Password attack

Cyber criminals use many methods to access accounts, including dictionary brute-force attack (attacks made to guess passwords), as well as comparing various word combinations against a dictionary file.

Cyber criminals may also use password capturing tools like "Keyloggers" on victim's computer.

Dos

PASSWORD SECURITY MANAGEMENT

- Always use different passwords for different accounts. Ensure password is strong

- Strong passwords should contain combination of upper case, lower case, numbers,"Special" characters (e.g., @#$%^&*()_+|~--=\’{}[]: ";<>/,etc.)

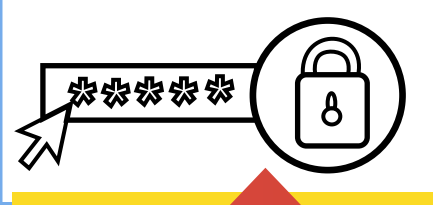
- Immediately, change any password which might have been shared or revealed by mistake

- Passwords must be changed at regular intervals

A PASSWORD **SHOULD NOT** CONTAIN

- ✗ Birth dates, names, ID proofs and other personal information such as addresses and phone numbers
- ✗ Commonly used words such as names of family members, pets, friends, colleagues, movie/novel/comics characters, etc.
- ✗ Password recovery answers should not be guessable
- ✗ Password should not be less than eight characters

Don'ts



PASSWORD SECURITY MANAGEMENT

- Do not use public systems to access banking/ sensitive sites
- Do not share password, OTP through e-mail, chat or any other electronic communication
- Do not reveal password on questionnaires or security forms

Don’ts

PASSWORD SECURITY MANAGEMENT

- Do not choose/ select “remember my password” option for banking/ sensitive sites
- Never write down your password anywhere, especially as a ‘note stick’ to the computer
- Don’t use your biometrics (finger print, etc.) at untrusted terminals/ places

GENERAL INTERNET SAFETY PRECAUTIONS

Invention of internet has revolutionized the way of communication and information sharing. However, unsecured usage of internet may pose risks to an organization. Internet security includes browser security, website security, network security, software applications, etc. Its objective is to enforce rules and measures against attacks over the internet.

Unsafe internet practices may lead to risks from phishing, online viruses, trojans, worms, ransomware, business email compromise, financial loss, etc.

DOs

GENERAL INTERNET SAFETY PRECAUTIONS

Be vigilant while clicking/ downloading from suspicious links/ URLs

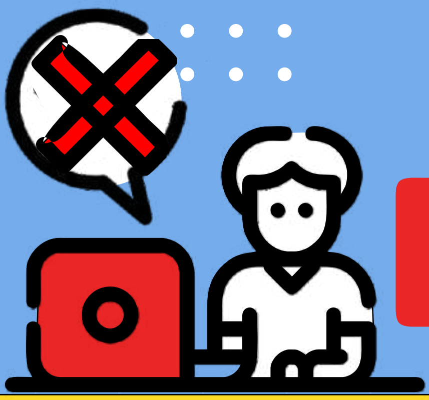
Make it a habit of clearing browser history after confidential activities/ transactions

Cloud storage to be used with appropriate security/ privacy settings

Verify the Authenticity and Identity of social media profiles before getting involved in any correspondence

Judiciously use services that require location information. Also, avoid posting photos with GPS-coordinates

Be vigilant and verify the advertisements/ sponsored contents on search results or websites



Don'ts

GENERAL INTERNET SAFETY PRECAUTIONS

Do not use any public computer or Wi-Fi for carrying out financial transactions like online shopping, internet banking, UPI transaction, etc.

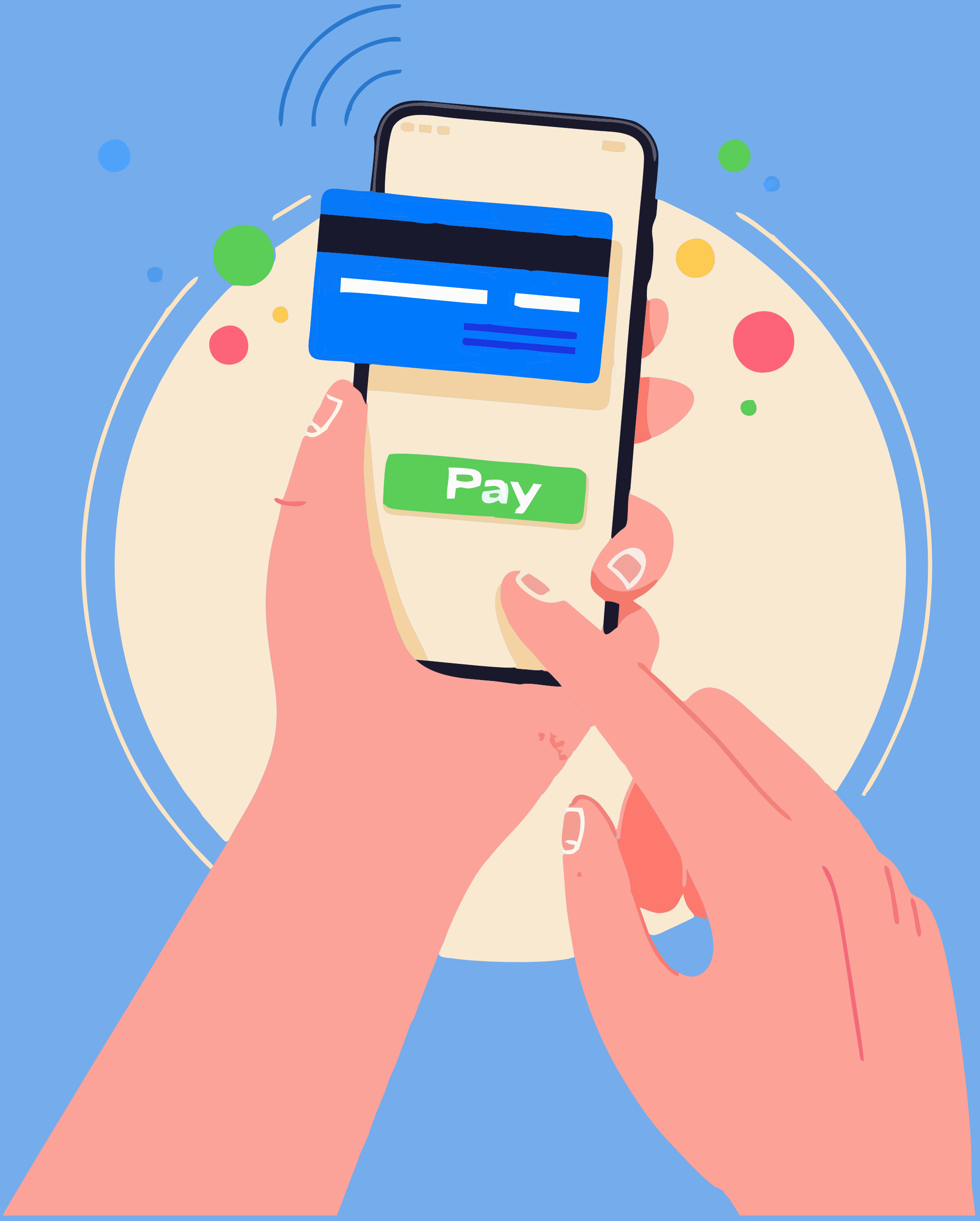
Do not use email address, phone number and details of payment cards on untrusted and unsecured websites

Do not trust and share unverified content on social media and messaging apps.

Always verify the source and authenticity of content before sharing

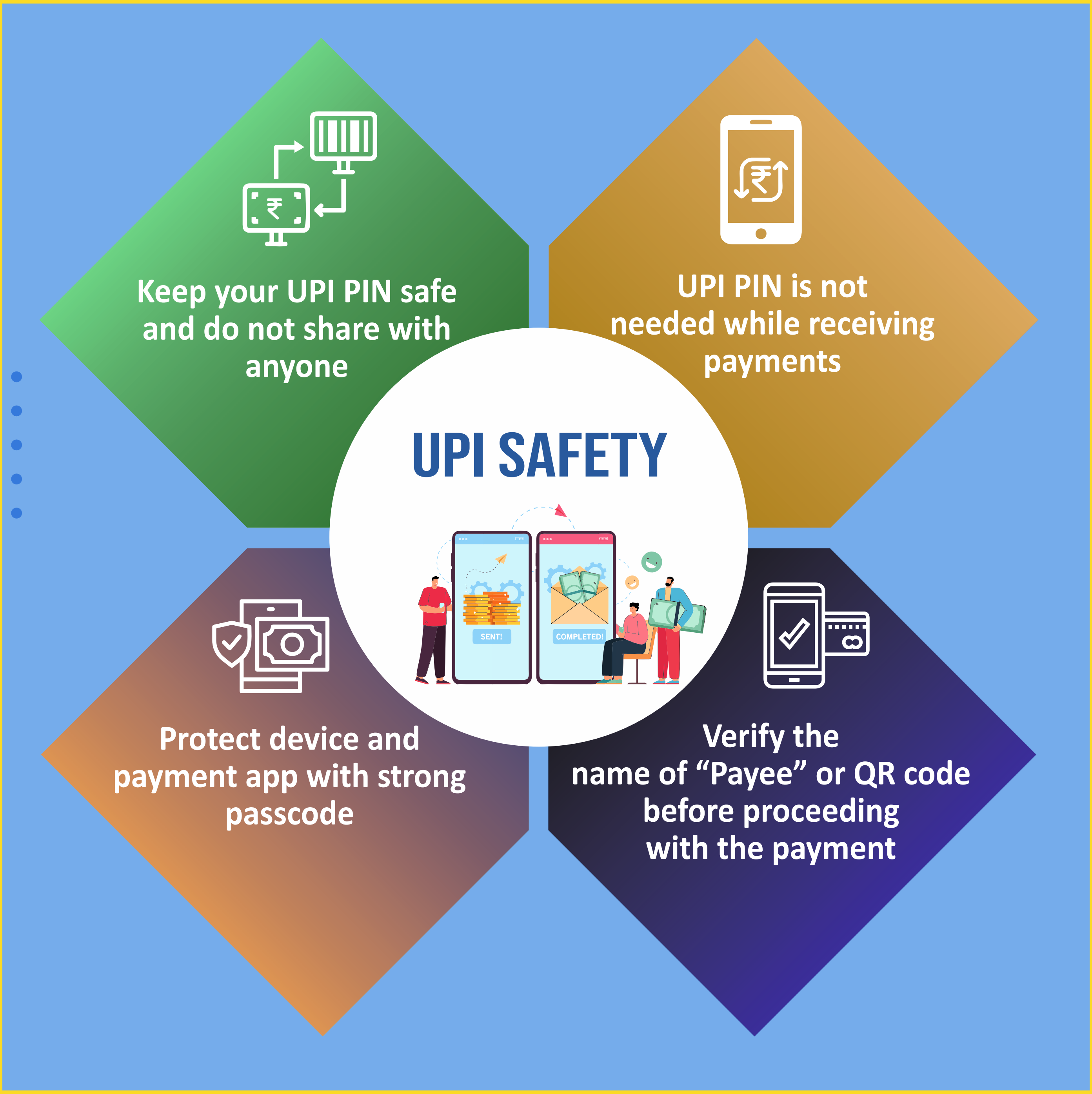
FINANCIAL TRANSACTION - SAFE PRACTICES

Digital modes of payments like internet banking, UPI, cards, mobile banking have made day-to-day payments very convenient. Any security lag in online transactions may result in financial loss to an individual or an organization.



DOs

FINANCIAL TRANSACTIONS - SAFE PRACTICES



UPI SAFETY

Keep your UPI PIN safe and do not share with anyone

UPI PIN is not needed while receiving payments

Protect device and payment app with strong passcode

Verify the name of "Payee" or QR code before proceeding with the payment

DOs

FINANCIAL TRANSACTIONS - SAFE PRACTICES

CARD SAFETY

Card Number, Expiry & CVV number are confidential. Never share with anyone

Use cards only after verifying authenticity of PoS/terminals/ATMs and websites

Manage your card limit using mobile banking apps for additional safety

Sharing OTP may result in unauthorized debits

DOs

FINANCIAL TRANSACTIONS - SAFE PRACTICES

INTERNET / MOBILE BANKING

Use genuine/licensed Operating System for internet banking transactions

Verify Internet Banking URLs received in SMS/Email before entering your credentials

Example-https://retail.onlinesbi.com ✓

http://xyz.com/SBIBank ✗

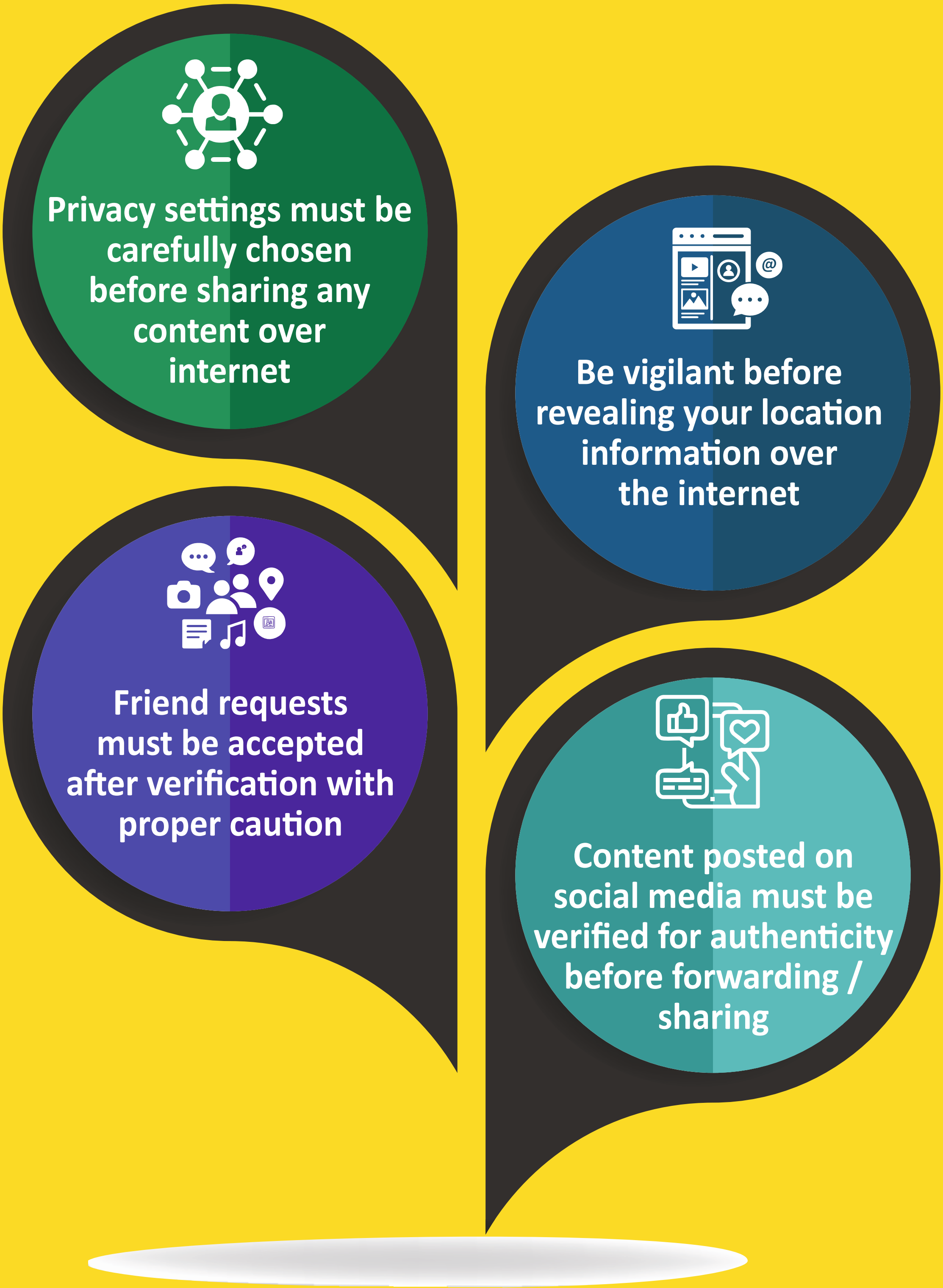
Public computers and insecure internet connections must be avoided

Use a strong internet banking password which is different from other accounts like e-mail, e-commerce, etc.

SOCIAL MEDIA PLATFORMS - SAFETY TIPS

DOs

SOCIAL MEDIA PLATFORMS - SAFETY TIPS



Privacy settings must be carefully chosen before sharing any content over internet

Be vigilant before revealing your location information over the internet

Friend requests must be accepted after verification with proper caution

Content posted on social media must be verified for authenticity before forwarding / sharing

Don'ts

SOCIAL MEDIA PLATFORMS - SAFETY TIPS

Do not use social media account without Multi-Factor Authentication (MFA)

Never log into social media accounts from untrusted systems

MOBILE PHONE SAFETY

Mobile phones are integral part of any organization. Secure usage of phone is essential for personal and organizational data protection.

Data theft, financial loss, unauthorized access, malware infection, etc., may be a result of mobile phone compromise.

DOs

MOBILE PHONE SAFETY

Be cautious with public Wi-Fi

Information shared over public network may be misused

Review the default privacy settings of the smartphone, mobile applications and social media accounts

Personal photos posted on social media with public visibility may be misused

Before downloading any App, same should be checked for its reputation/ authenticity

Read vendor privacy policies and verify app permission before downloading apps

DOs

MOBILE PHONE SAFETY

Prefer downloading mobile apps from genuine sources

Turn off / remove unnecessary apps

Register for Do Not Disturb (DND) service with Telecom Operators

DOs

MOBILE PHONE SAFETY

Use Parental control mode, while handing over mobile phones to kids or minors

Use device / SD card encryption to safeguard confidential data

DOs

MOBILE PHONE SAFETY

Protect your device with a strong PIN/Password or Biometrics and enable auto lock setting in mobile phone

Always take back-up of data (contacts, personal photos, etc.)

Don'ts

MOBILE PHONE SAFETY

Do not reply or click on link sent through SMS, e-mails or chat messenger by strangers

Do not store any classified/ sensitive data (text /video / photograph) in the device

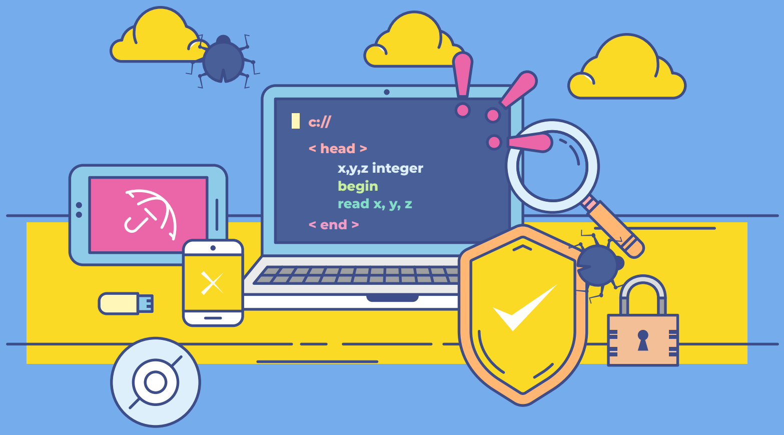
Do not log into accounts, especially the financial accounts, when using public wireless networks

MALWARE PROTECTION

The Term Malware is a combination of words, ‘Malicious’ and ‘Software’. Malware is intentionally developed to perform various unauthorized and destructive tasks on the victim's system without one’s knowledge.

Malware performs various tasks that include locking of important files, stealing sensitive information from the system, gaining unauthorized remote access, spy on the user activity, consuming computer memory, internet bandwidth, corrupting important files, etc.

The various types of malwares are spyware, viruses, worms and trojans, ransomware, Botnet, etc.



How to protect against malware?

Keep all software up to date, including the Operating System and applications.

- Do not click on untrusted URL links
- Use anti-malware solutions
- Patch Management to be ensured to overcome vulnerabilities

DOs

MALWARE PROTECTION

Scan USBs,
Files on your computer regularly or before use.
Disable USB devices if not needed

Use Licensed Version of Operating Systems and Application Software

Keep your system and Antivirus up-to-date with regular patches

E-MAIL SECURITY PRACTICES

E-MAIL SECURITY PRACTICES

Don't open/reply to e-mail links (hyperlinks/ web-links/ URLs mentioned in the body of such mails) giving any luring offer. It may result in compromising your personal and financial details.

Do not access to any spam e-mails, until the sender is properly verified