गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS

सत्यमेव जयते

Indian Cyber Crime Coordination Centre

CYBER SAFETY

TIPS BY

CYBER DOST

Indian cyber crime coordination center (MHA)

Published by:

Ministry of Home Affairs,

Government of India

North Block

New Delhi – 110001

Disclaimer:

Indian Cyber Crime Coordination Center (I4C), under Ministry of Home Affairs, Cyber & Information Security (CIS) Division has prepared this document based on the tweets posted on MHA twitter handle@cyberdost. This should not be considered as an exhaustive list but basic minimum precautions to be taken.

Table of Contents

Introduction

With the growing adoption of Digital platforms by citizens of India, rate of digital crimes is also increasing day by day. Since internet is widely used by people in their daily lives, it is necessary to spread awareness among users for safe and secure use of these platforms/services accessible through internet. Indian Cyber Crime Coordination Centre (I4C) has taken up the task of educating the people on cyber frauds and online safety. As a part of this initiative, I4C has a twitter handle @Cyber Dost, on which, cyber safety awareness content is tweeted regularly.

This e-book is a collection of awareness tips tweeted by @Cyber Dost and aims to educate internet users to reap the benefits of Digital India in a safe and secure manner.

1. *Online Transaction/Financial Frauds*

1.1 Always be sure about the correct web address of the bank website and look for the "lock" icon on the browser's status bar while visiting bank's website or conducting any online transaction.

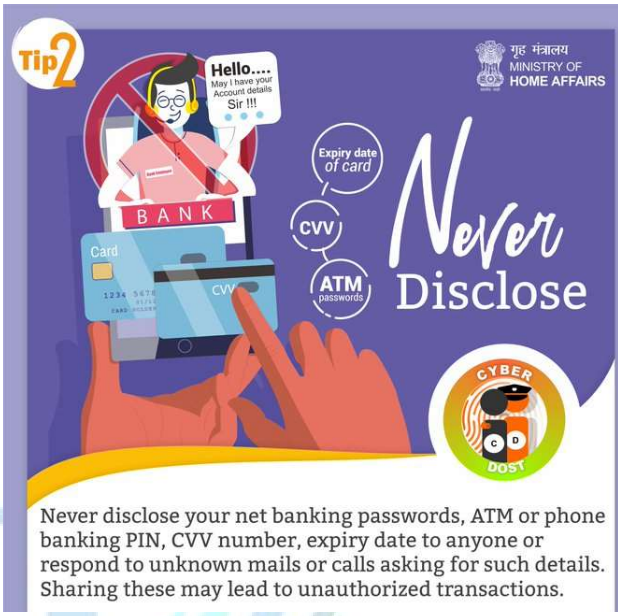
1.2 Secure way of swiping credit/debit cards

Tip 1
गृह मंत्रालय
MINISTRY OF HOME AFFAIRS
CYBER DOST

- Keep an Eye -

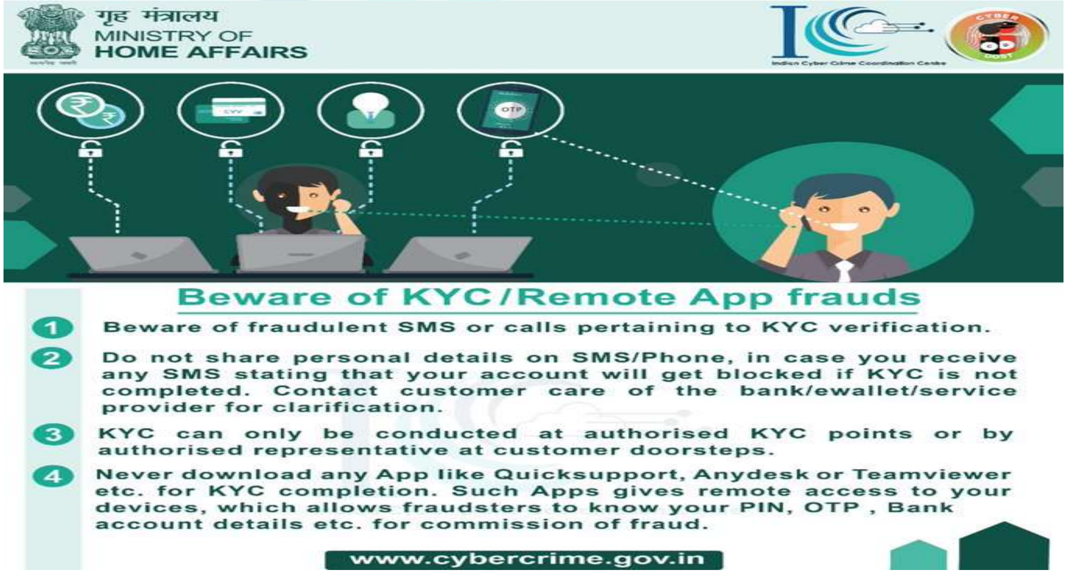
Always ensure that credit or debit card swipes are done in your presence to avoid cloning/unauthorized copying of your card information

1.3 Do not share your Net Banking password, One Time Password (OTP), ATM or phone banking PIN, CVV number etc. to any person even, if he is claiming to be employee or representative of bank and report such instances to your bank.



Never disclose your net banking passwords, ATM or phone banking PIN, CVV number, expiry date to anyone or respond to unknown mails or calls asking for such details. Sharing these may lead to unauthorized transactions.

1.4 Beware of KYC/Remote App Frauds

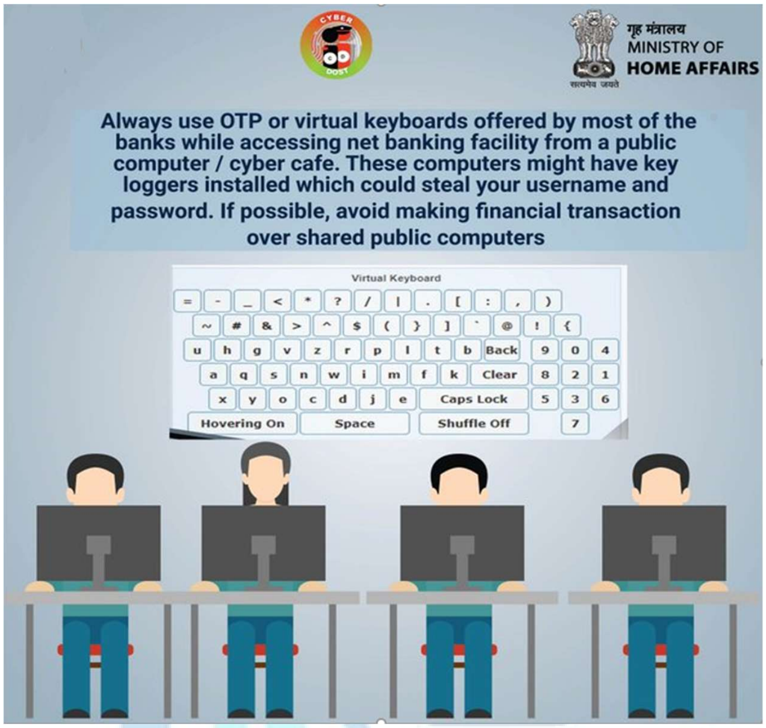


Beware of KYC/Remote App frauds

1. Beware of fraudulent SMS or calls pertaining to KYC verification.
2. Do not share personal details on SMS/Phone, in case you receive any SMS stating that your account will get blocked if KYC is not completed. Contact customer care of the bank/ewallet/service provider for clarification.
3. KYC can only be conducted at authorised KYC points or by authorised representative at customer doorsteps.
4. Never download any App like Quicksupport, Anydesk or Teamviewer etc. for KYC completion. Such Apps gives remote access to your devices, which allows fraudsters to know your PIN, OTP , Bank account details etc. for commission of fraud.

www.cybercrime.gov.in

1.5 Enhance your protection by deploying additional layer of security to access your online accounts or doing online financial transactions by enabling two factor authentication (2FA) - username with password and OTP on your mobile



Always use OTP or virtual keyboards offered by most of the banks while accessing net banking facility from a public computer / cyber cafe. These computers might have key loggers installed which could steal your username and password. If possible, avoid making financial transaction over shared public computers

Virtual Keyboard
= - _ < * ? / | . [: ,)
~ # & > ^ $ (}] ` @ ! {
u h g v z r p l t b Back 9 0 4
a q s n w i m f k Clear 8 2 1
x y o c d j e Caps Lock 5 3 6
Hovering On Space Shuffle Off 7

1.6 Do not respond to any message assuring credit of money into your bank account with request to share personal details. It may be an attempt to defraud you.

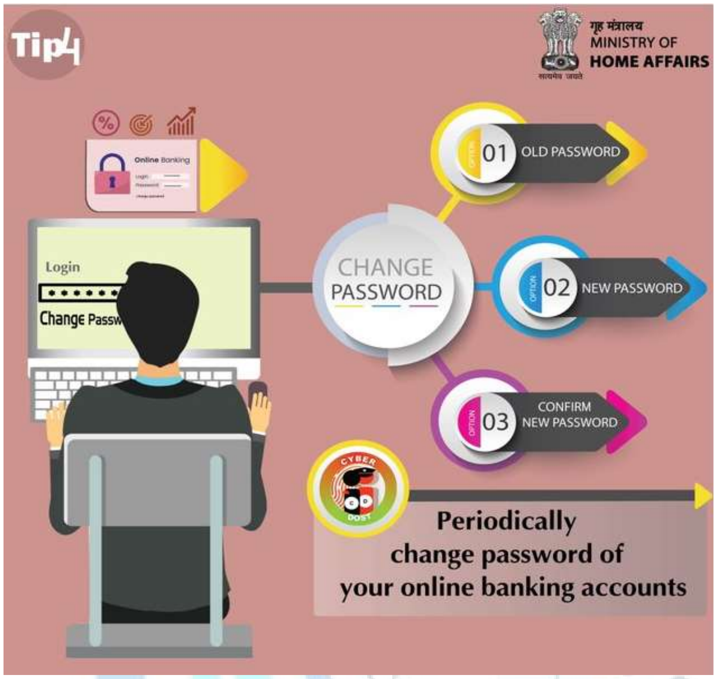
गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS
BANK
Card
CVV
EMAIL
CYBER DOST

STAY ALERT !

No bank or its employees will ever call or email you requesting for your password, PINs, OTP, and CVV details etc. If you get such a call, immediately report the incident to your bank

1.7 Always review transaction alert received on your registered mobile number and reconcile with the amount of your purchase.

1.8 Secure password practice



Periodically change password of your online banking accounts

1.9 Public networks might not be secured. Avoid financial transactions on these networks. Alternatively, use personal mobile data or VPN (Virtual Private Network).

Tip6
गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS
सत्यमेव जयते
CYBER DOST
public computers
Want to Save Password?
****
Save
Never
public computers

Avoid using public computers for online banking/ transaction. In-case you want to use public computers for financial transactions, check for the presence of anti-virus on their system. Do not save your password when prompted by the browser

1.10 Check for HTTPs in URL:

Tip7
गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS
SECURE https://www.
CYBER
DOST

While visiting your bank's website or conducting an online transaction, always look for the "lock" icon on the browser's status bar and be sure "https" appears in the website's address bar before making an online purchase. The "s" stands for "secure" and indicates that the communication with the webpage is encrypted

1.11 Monitor banking activities/transactions periodically

Tip8
CYBER
DOST
गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS
ABC Bank
Username
Login
pass : *****
Bank statement

Login and view your bank account activity multiple times every week to make sure there are no unexpected transactions. Report any discrepancies to your financial institution immediately

1.12 Keep bank’s customer care number handy.

Tip9
CYBER DOST
गृह मंत्रालय
MINISTRY OF HOME AFFAIRS
Bank
₹ ₹
XXXXXX XXXXX
CUSTOMER CARE
CALL

KEEP YOUR BANK’S CUSTOMER CARE NUMBER HANDY SO THAT YOU CAN REPORT ANY SUSPICIOUS OR UNAUTHORIZED TRANSACTIONS ON YOUR ACCOUNT IMMEDIATELY

1.13 Security against fake banking E-mails.

Tip10
CYBER DOST
गृह मंत्रालय
MINISTRY OF HOME AFFAIRS
SPAM
https://www.xyz.com/index.php?goto
SPAM

It is easy for cyber criminals to send convincing emails which appears to be from your bank. Don’t click on the links provided in such emails even if they look genuine. They could lead you to malicious websites. Instead, type in the bank’s web address in your browser and navigate from there

1.14 Secure use of ATM

Tip 11
CYBER DOST
गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS
Take extra precaution while typing your password/PIN so that no one sees it. Try to cover the key-pad with your other hand while you type your PIN to avoid the number being picked up by someone monitoring CCTV footage
ATM MOCKUP

1.15 Always remember to log off from website after completing an online transaction with your credit/ debit card. It is a good practice to delete the browser cookies.

1.16 Always use virtual keyboard to access net banking facility; and log off from banking portal/website after completion of online transaction. Also ensure to delete browsing history from web browser (Internet Explorer, Chrome, Firefox etc.) after completion of online banking activity

1.17 Using mobile notification for security

Register your personal phone number with your bank and subscribe to mobile notifications. These notifications will alert you quickly of any suspicious transaction. Not just the transactions, the bank will alert you of the unsuccessful login attempts to your net-banking account

Tip 13
CYBER DOST
गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS
Bank
Mobile notifications
Phone Banking
Registered mobile
+91 -1234567890
login
Log ou
Bank
customer care

1.18 Always check for transaction receipt

Always check your transaction receipt

Review your purchase and bill receipt before making payments. Always ensure that your transaction is billed according to your purchase

Tip 15
CYBER DOST
गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS
Transaction
₹
BILL
PAID
RECEIPT

1.19 Do not autofill forms.

Tip16
CYBER DOST
गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS
DO NOT AUTO-FILL FORMS
NAME
Your full name
USERNAME
Username
EMAIL
Email adress
CARD NUMBER
******
CVV
******
MAKE PAYMENT
Auto fill personal information?
Yes
No
Name
DoB
Add
REGISTER
SIGN UP
Card
CVV

Do not Auto-fill forms

Always type the information in online forms.Don't use the auto-fill option to fill your online forms as these forms may store your personal information such as card number, CVV number, bank account number, etc

1.20 Refrain from saving card details online

Tip18
CYBER DOST
गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS
e-wallet

Always verify and install authentic e-wallet apps

Do not save your card or bank account details in your e-wallet

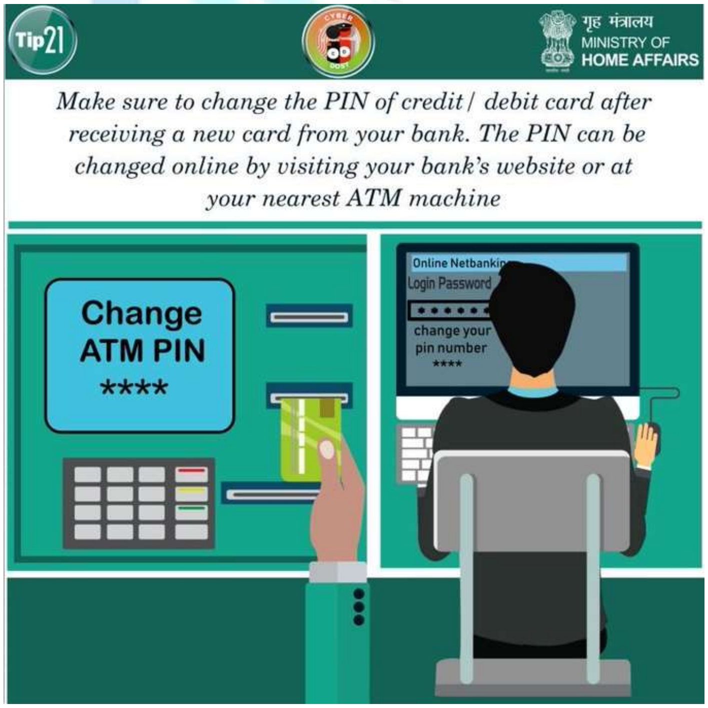
It increases the risk of theft or fraudulent transactions in case of a security breach

1.21 Tampering check – credit/debit card

Tip 20
CYBER DOST
गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS
I have received the card in a tampered envelope

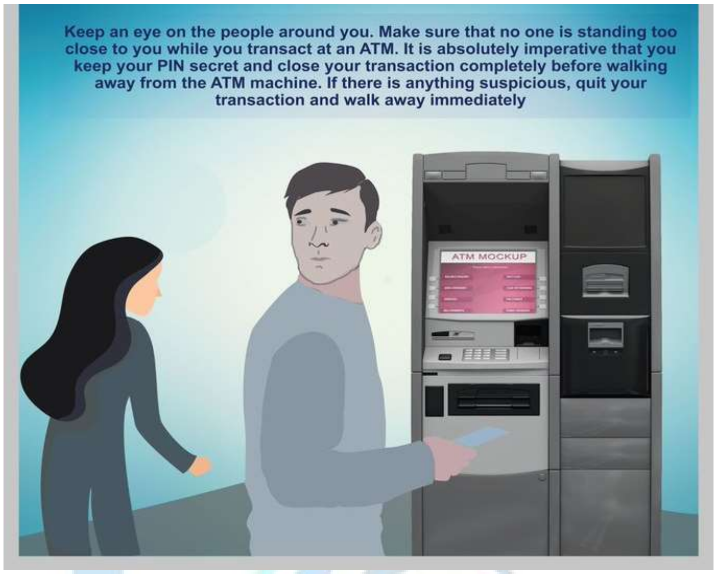
Whenever you receive a credit / debit card from the bank, make sure the letter is not damaged and it is sealed properly. In-case, there are any signs of tampering with the package, you should notify your bank immediately

1.22 PIN change – Newly received credit/debit card



Make sure to change the PIN of credit / debit card after receiving a new card from your bank. The PIN can be changed online by visiting your bank's website or at your nearest ATM machine

1.23 Beware of shoulder surfing! Be careful while entering credentials like passwords, bank account details, etc., whenever someone is sitting beside or behind you



Keep an eye on the people around you. Make sure that no one is standing too close to you while you transact at an ATM. It is absolutely imperative that you keep your PIN secret and close your transaction completely before walking away from the ATM machine. If there is anything suspicious, quit your transaction and walk away immediately

1.24 Enable international transaction option on your credit card only when you are travelling abroad. Always ensure to disable international transaction option on your card upon return to your country.

1.25 Lottery and e-commerce Frauds

a) Be cautious of promotional scams where cyber criminals can offer you unbelievable deal or cash prize, etc.! They will try to get money from you or ask for your personal data such as bank account details, address, identity proof, etc. which can be misused

b) Beware of lottery frauds! Remember you can never win a lottery if you have not participated in it. Scammers try to entice you by sending email or SMS stating that you were randomly selected as a winner. Ignore such e-mails/SMSs

2. *Identity Theft / Cyber Impersonation*

2.1 Protect your identity online by restricting personal information that you share and securing your accounts with strong passwords

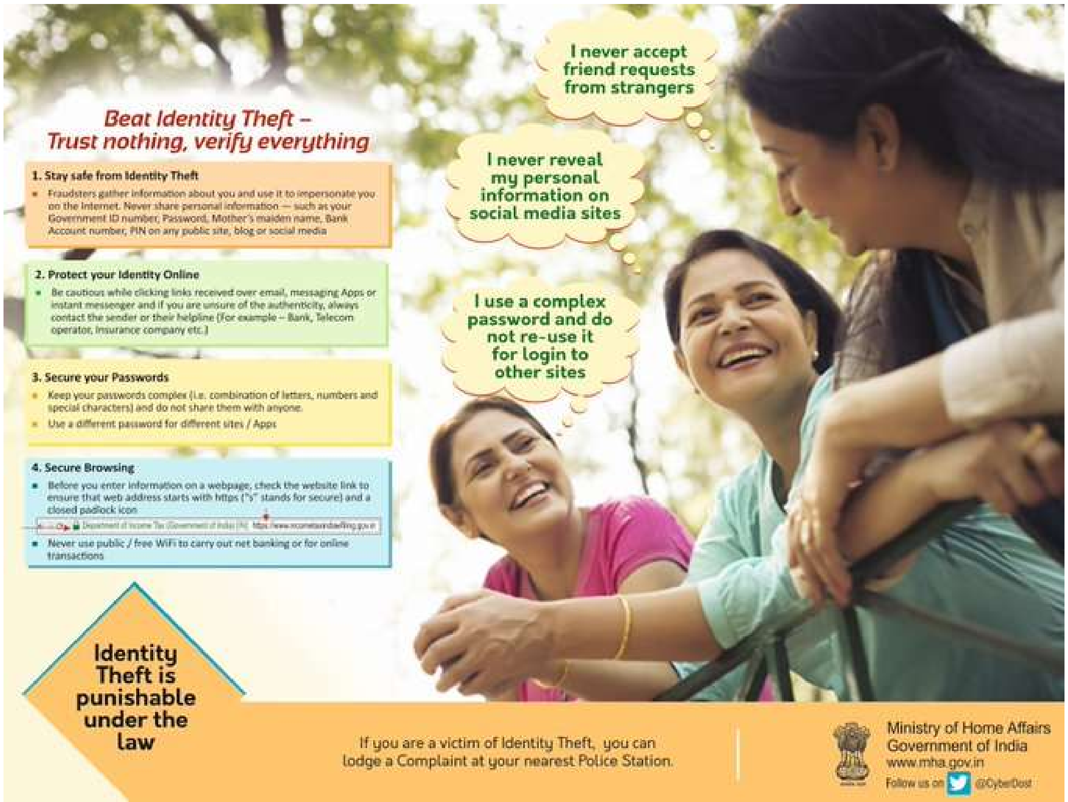
2.2 Immediately inform to social media service provider, if you notice that fake account has been created by using your personal information.

2.3 Be very cautious about your online identity! Ensure that your personal information such as date of birth, address, phone number is not publicly available on social media platforms as it may be misused

2.4 Do not trust online users unless you know and trust them in real life. Also do not share your personal information such as address, phone number, date of birth etc. on social media. Identity thieves can easily access and misuse this information.

2.5 Do you know that using electronic signature or password or any other unique identification feature of any other person fraudulently can be considered as identity theft or cheating and is a punishable offense ?

2.6 In case you suspect your social networking account details have been compromised, immediately report to social networking site support team.



Beat Identity Theft – Trust nothing, verify everything

1. Stay safe from Identity Theft

- Fraudsters gather information about you and use it to impersonate you on the Internet. Never share personal information — such as your Government ID number, Password, Mother's maiden name, Bank Account number, PIN on any public site, blog or social media

2. Protect your Identity Online

- Be cautious while clicking links received over email, messaging Apps or instant messenger and if you are unsure of the authenticity, always contact the sender or their helpline (For example – Bank, Telecom operator, Insurance company etc.)

3. Secure your Passwords

- Keep your passwords complex (i.e. combination of letters, numbers and special characters) and do not share them with anyone.
- Use a different password for different sites / Apps

4. Secure Browsing

- Before you enter information on a webpage, check the website link to ensure that web address starts with https ("s" stands for secure) and a closed padlock icon
- Never use public / free WiFi to carry out net banking or for online transactions

Identity Theft is punishable under the law

If you are a victim of Identity Theft, you can lodge a Complaint at your nearest Police Station.

Ministry of Home Affairs
Government of India
www.mha.gov.in
Follow us on @CyberDost

I never accept friend requests from strangers
I never reveal my personal information on social media sites
I use a complex password and do not re-use it for login to other sites
Department of Income Tax (Government of India) [IN] https://www.incometaxindiaefiling.gov.in

2.7 Do not give any personal information about yourself or your friends and family members like name, address of the school / home, phone numbers, age, sex, credit card details, etc. to a person you have met online.

2.8 Be careful while providing details or copy of PAN Card, Aadhaar, Voter Card, Driving License, Address Proof etc. to unknown person/ organization. Such personal documents may enable fraudsters to apply for a duplicate SIM cards in your name without your prior knowledge and use it for illegal activities.

2.9 Do not share your personal identifiable information or family details like name, date of birth, mobile number, marriage date, PAN number, Passport number, Aadhaar details etc. on social media sites, matrimonial sites, e-wallets, etc.

3. Online Job Fraud

3.1 Many organisations conduct interviews through telephone, chat services, Skype calls or Google hangouts. Please check credentials of organisation and its representative before the online interview. Make sure to ask detailed questions related to job and organisation from interviewer.

3.2 Beware of the emails, which offer jobs in exchange for money, such e-mails are spam. No organization/ company ever asks for money to work for them.

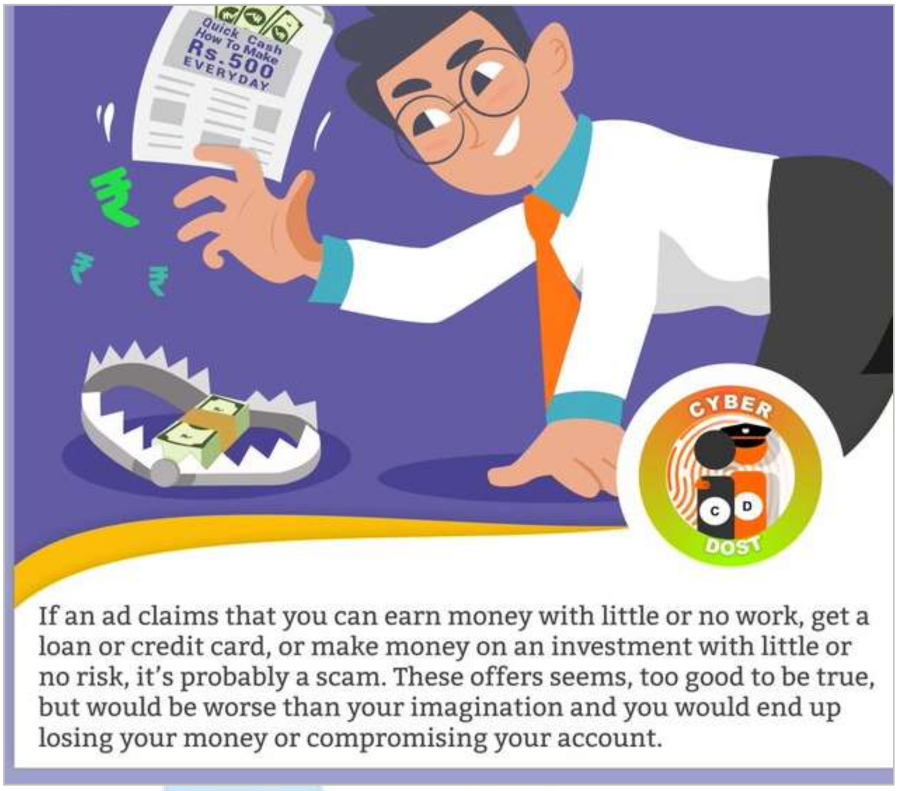
Source: www.infosecawareness.in

3.3 Many job portals offer paid services for resume writing, resume promotion, and job alerts. Before paying to these portals, check authenticity and reviews of the website. Consult your family and friends to know about reliable websites.

3.4 Always look for the spelling errors in the e-mail address and job descriptions. If an email has spelling, grammatical and punctuation errors, it could be a scam.

3.5 Always check the website of the Government organisations for details about the job openings in a Government department. All government websites have “[dot]gov[dot]in” or [dot]nic[dot]in as part of their website address (e.g. mha.gov.in).

3.6 Beware of unrealistic/attractive job offers



If an ad claims that you can earn money with little or no work, get a loan or credit card, or make money on an investment with little or no risk, it’s probably a scam. These offers seems, too good to be true, but would be worse than your imagination and you would end up losing your money or compromising your account.

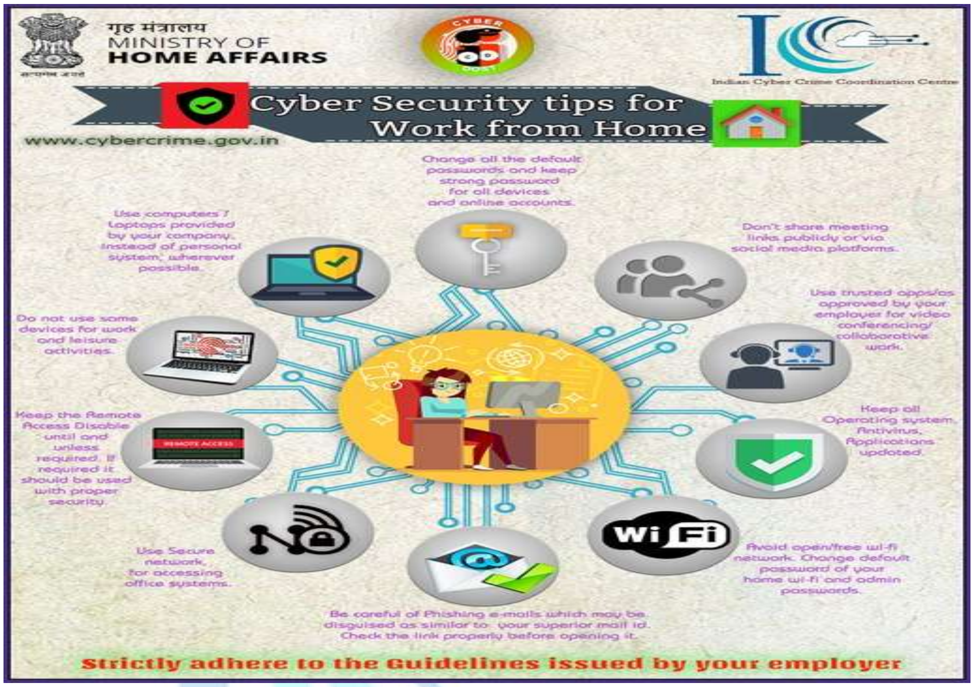
3.7 Always check the company's website if you have found a job opportunity on another website to check the authenticity of the job and know more about the profile. Very often companies put their manpower requirements on their official website under the 'careers' section.

3.8 Always keep a note of where you've applied for the job. Do not respond to any generic emails from an unknown source/company, as it could be a scam.

3.9 Prior to registering on job search portal, check the privacy policy of the website to know the type of information collected from the user and how it will be processed by the website.

3.10 Always search and apply for jobs posted on authentic job portals or newspapers. It is advisable not to apply for jobs posted on search engine and social media advertisements, labelled sponsored links or results.

3.11 Cyber Security tips for Work from Home:



गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS

Indian Cyber Crime Coordination Centre

Cyber Security tips for
Work from Home

www.cybercrime.gov.in

Change all the default passwords and keep strong password for all devices and online accounts.

Use computers / Laptops provided by your company, instead of personal system, wherever possible.

Don't share meeting links publicly or via social media platforms.

Use trusted apps/as approved by your employer for video conferencing/ collaborative work.

Do not use same devices for work and leisure activities.

Keep all Operating system, Antivirus, Applications updated.

Keep the Remote Access Disable until and unless required. If required it should be used with proper security.

Use Secure network, for accessing office systems.

Avoid open/free wi-fi network. Change default password of your home wi-fi and admin passwords.

Be careful of Phishing e-mails which may be disguised as similar to your superior mail id. Check the link properly before opening it.

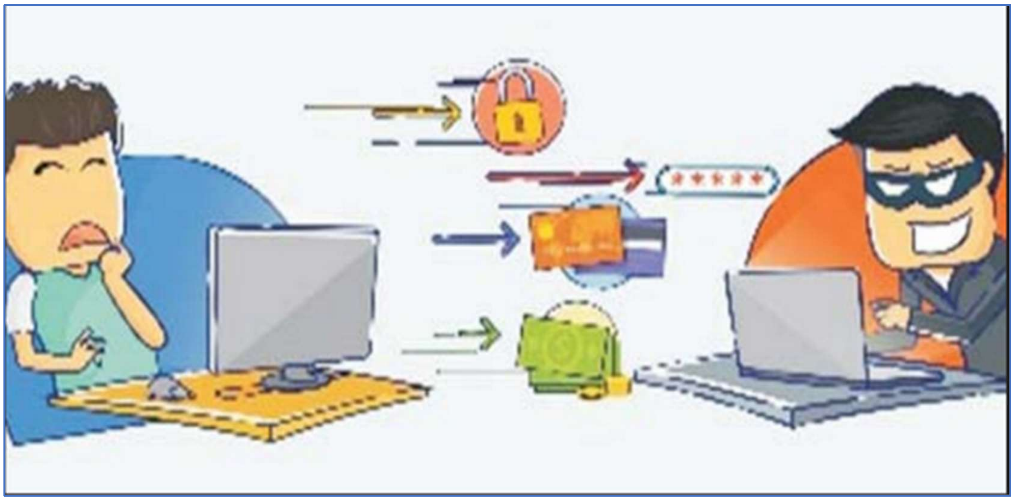
Strictly adhere to the Guidelines issued by your employer

3.12 Remain vigilant against the job frauds. Always check the senders e-mail address, grammatical mistakes in the mail, background of the hiring company and most importantly, never deposit any money.

3.13 Beware of the job fraudsters, disguising as company officials. They try to collect your personal information or demand money for the job.

3.14 Beware of the fake callers impersonating themselves as recruiters. They request for personal information like date of birth, identity card details etc. & sell this information to unauthorised users. Verify the authenticity of your recruiter before sharing any details

4. *Unauthorized Access/ data breach*



4.1 Awareness on device [mobile & computer] security

4.1.1. Do not leave your phone unattended in public places and refrain from sharing your phone password / pattern lock with anybody.

4.1.2. Always enable a password on the home screen to restrict unauthorized access to your mobile phone. Configure your device to automatically lock beyond certain duration.

4.1.3. If you store or download any personal information on computers in cybercafé, make sure you delete permanently all the documents after you are done with your work. You may press Shift and Delete button together to make it difficult to recover deleted files.

4.1.4. Many mobile apps ask for many permissions to access data and functions regardless of the necessity for functioning of the app. Identify nature of app, assess the necessity of permissions asked while installing app and avoid giving unwanted permissions.

4.1.5. Allowing apps to access various features of your electronic gadgets /Mobile phone may lead to security risks and expose your personal information for misuse. Be careful of the associated risks while granting access permissions.

4.1.6. Enable mobile device access to third-party applications selectively. Do you know some malicious apps, if given SMS access, may read OTP and other sensitive information from your messages.

Source: www.infosecawareness.in

4.1.7. Passwords should not be stored in readable form in computers, notebook, notice board or in any other location where unauthorized persons might discover or use them.

4.1.8. Remove files or data you no longer need to prevent unauthorized access to such data. Merely deleting sensitive material is not sufficient, as it does not actually remove the data from your system. File shredder software should be used to delete sensitive files on computers.

Source: www.infosecawareness.in

4.1.9. Always lock your computer before leaving workplace to prevent unauthorized access. A user can lock computer by pressing ‘ctrl +alt+del’ and choosing ‘lock this computer’ or “window button+ L”.

4.1.10. Enable a password-protected screen saver with a timeout period of 5 minutes or less to ensure that computers that were left unsecured will be protected.

4.1.11. Always lock your computer screen, when not in use. To lock your Windows system, press Windows Button + 'L' and to lock Mac system, press Shift + Ctrl + Eject or Control + Shift + Power.

4.1.12. Use several combinations of characters while creating a strong password. For example, create a password containing a combination of uppercase, lowercase, numbers and special characters.

4.2 Account security

4.2.1. Use 'non-administrator account' privileges for login to the computer and avoid accessing with 'administrator' privileges for day-to-day usage of computers.

4.2.2. Enable security features on all digital devices you use! Ensure that the devices offer security features like passwords to open/get access. Make it a habit to update/change passwords regularly.

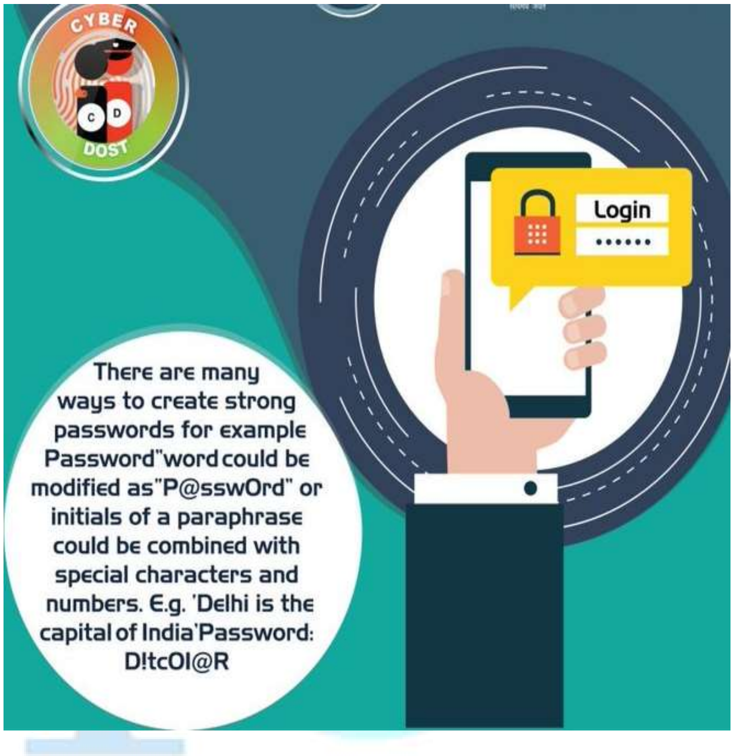
4.2.3. Thinking of selling your old electronic gadgets such as mobile, tab, laptop etc.? Do ensure that all the device data is securely erased before your handover it to vendor. This is important to avoid possible leakage of your personal information

4.2.4. Protecting your email & social media accounts is important as any breach can result in loss of personal data. Always use two factor authentication features (password & verification code on your registered mobile) to secure your email/social media accounts.

4.2.5. When accessing online accounts via public computers ensure that remember me / save password is not selected when prompted.

4.2.6. In the password recovery settings do not set the questions which can be easily answered or identified from your social media accounts like date of birth, first school name etc.

4.2.7. Don't use same password for all your online accounts. Imagine if one account gets compromised, the hacker can get access to your other accounts as well. A strong password & two factor authentication is a good practice and can help you in protecting your online accounts.

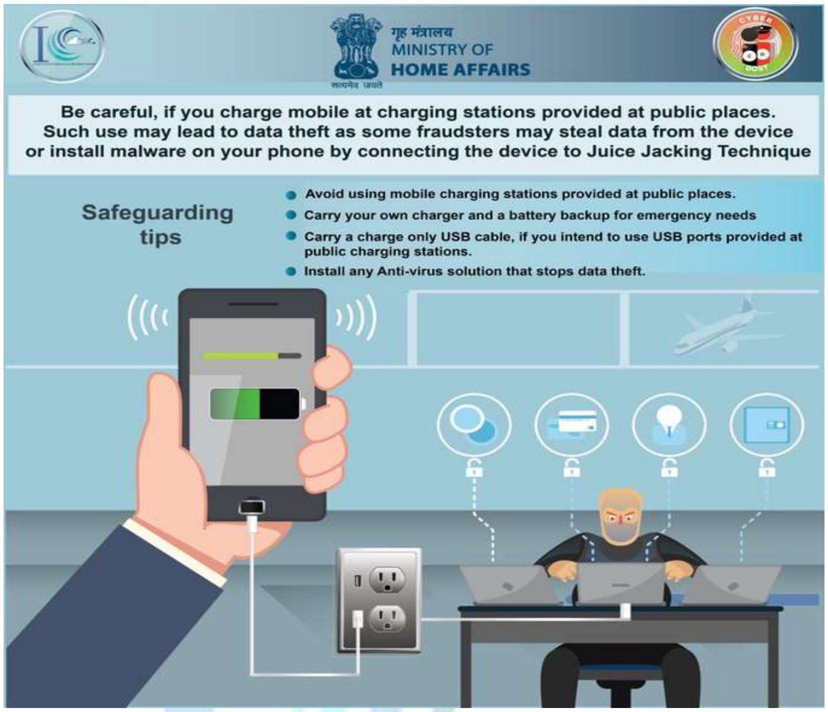


There are many ways to create strong passwords for example Password"word could be modified as"P@sswOrd" or initials of a paraphrase could be combined with special characters and numbers. E.g. 'Delhi is the capital of India'Password: D!tcOI@R

4.2.8. As a best practice, while sending private and confidential information online, protect the document with a password and choose two communication channels. One for the document and other for the credentials/password to open the file.

4.2.9. If your work requires you to communicate passwords, such as while sending password for an encrypted file sent as an attachment through email, it must be communicated through a different channel such as over a phone call or SMS.

4.2.10. Be aware while using public charging points.



गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS

Be careful, if you charge mobile at charging stations provided at public places. Such use may lead to data theft as some fraudsters may steal data from the device or install malware on your phone by connecting the device to Juice Jacking Technique

Safeguarding tips

- Avoid using mobile charging stations provided at public places.
- Carry your own charger and a battery backup for emergency needs
- Carry a charge only USB cable, if you intend to use USB ports provided at public charging stations.
- Install any Anti-virus solution that stops data theft.

4.2.11. Still using default passwords? Avoid using passwords such as Jan@2018, admin@123, password@123 etc. These can be easily guessed by nefarious users.

4.2.12. While registering/ creating an online account do not select common secret questions (for password recovery option) that can be guessed easily. Nefarious users can guess straightforward answers via recovery options and may hack your account.

4.2.13. Just like you lock your house, your car, your bike; you must protect your online assets (e-banking, wallet, email, social media accounts) & devices (like phones, laptops, tablets) with strong passwords and PINs & change them regularly.

4.2.14. Be careful when you are using computer in a cybercafé. Use computer only if an anti-virus is installed in the system. Do not save your password when prompted by the browser. Always log out of your accounts and close the browser.

4.2.15. Before selling your old electronic gadget, ensure that all the device data is erased securely and you have signed out from all the app such as e-mail, social media, bank, e-wallets etc.

4.2.16. Have you ever taken any print-out or photocopy of confidential document through Photocopy machines or Printers? – Be careful they can store information in internal hard drive of machine. Make sure you delete the data inside the drive before you dispose or sent it for repair.

4.2.17. Have an awareness about privacy policy (like what information is getting collected from you, purpose of collection, security of that collected information, circulation of the collected information if any etc.) about the website you visit frequently.

4.2.18. Review your access to the third-party application via social networking sites and selectively enable or disable as per your usage. As a good practice maintain separate professional and personal email accounts with unique but strong passwords.

4.2.19. As e-mail messages are transferred in clear text, it is advisable to use some encryption software to encrypt messages before sending sensitive data. It can be decrypted only by the specified recipient.

Source: www.infosecawareness.in

4.2.20. Avoid using third-party extensions, plug-ins or add-ons for your web browser as it may secretly track your activity and steal your personal details.

5. *Wireless / Bluetooth security awareness*

5.1. Secure all the wireless access points (Wi-Fi, Routers) with a strong password. Hackers usually scan for open access points, a method called as war-driving to anonymize their identity.

5.2. Be cautious while browsing through a public Wi-Fi and avoid logging in to personal & professional accounts like e-mail, banking transactions on these networks.

5.3. Be careful while using public Wi-Fi at Airports, Railway Stations, Bus Stops etc. Public Wi-Fi is an easy target for any hacker to steal your information. Use secure VPN or proxy to avoid unauthorised access to your personal information.

5.4. Consider using the Media Access Control, or "MAC," address filter in your wireless router. Every electronic device that can connect to a Wi-Fi network has a unique ID called the "physical address" or "MAC" address. Wireless router can screen the MAC addresses of all devices connected to it, and users can set their wireless network to accept connections only from devices with MAC addresses recognized by router. To prevent unauthorized access to your device, consider activating your wireless router's MAC address filter to allow your devices only.

5.5. Thinking to offer internet via hotspot to your friend? Do ensure your device access is protected via a strong password and your hotspot is closed immediately after usage. Open hotspots can lead anyone to connect to your device and may steal your personal data.

5.6. Always browse shopping or banking websites or apps only on a device that belongs to you or on a network that you trust. Avoid using a friend’s phone, a public computer, or a cafe’s free Wi-Fi for sensitive browsing as your data can be stolen or copied

6. *Virus, Worms and Trojans*

6.1. Do not use public computer/ cybercafé to access social networking websites, it may be infected/ installed with a key logger application to capture your keystrokes including the login credentials.

Source: www.infosecawareness.in

6.2. Be careful of what you plug in to your computer. Malware can spread through infected USB drives, external hard drives, and even smart phones.

6.3. Computers should be protected from virus/worms using an Antivirus software.

Source: www.infosecawareness.in

6.4. Ensure that your computer and mobile devices have updated antivirus software and always keep it turned on.

6.5. It is advisable to scan all removable media with anti-virus software before use.

6.6. It is advisable to keep Auto run / Auto play feature disabled for all removable media.

6.7. Do not download any type of files/software from any source without ascertaining its credibility

6.8. Regularly check for software update on your mobile device whenever prompted. This empowers your mobile software to achieve optimization and equips it to face the latest cyber security threats.

Source: www.infosecawareness.in

6.9. Make sure your operating system, application and software patches including anti-virus software are up to date; and auto updates are turned on in your computer.

6.10. Do not give remote access, file and print sharing access to untrusted computers.

6.11. Be extra cautious like opening a downloaded file with extensions like '.exe', '.vbs' and '.scr'; Enable the 'Show file extensions' options in the Windows settings on your computer to identify these.

Source: www.infosecawareness.in

6.12. Never share malicious or infected USB thumb drives with unknown people. Scan all the USB drives with anti-virus each time before exploring.

6.13. Always keep your personal computer/ laptop and devices secured. One of the ways to ensure standard safety is to install good antivirus and to update it regularly.

6.14. Always check trustworthiness of the source and functionality of a mobile application before installing it.

6.15. Your mobile devices can be infected with viruses/Trojans/malware, etc. Protect your mobile device by installing good antivirus. Read reviews of antivirus apps to select suitable one. Make it a habit to update antivirus to enhance your protection against latest threats.

6.16. Before latching removable storage such as pen drive, external hard disc on your laptop/computer ensure it is well scanned for virus/ worms using an updated antivirus software.

6.17. If you see a pop-up message while using internet, never click on any buttons present on the pop-up (not even the close button), they might contain malware. On Windows System, press ALT + F4 (Command-W on Mac Systems) on your keyboard to close the dialog box.

Source: www.infosecawareness.in

6.18. Never download any content like Images, Videos, Apps, Games, System Software, Software Drivers, Operating Systems etc. from unknown sources. They might contain malware.

6.19. Beware of the sites that offer free antivirus or anti-spyware software. These may spread malicious content in your device. Always download antivirus and spyware software from trusted sites only.

6.20. Beware of risky free online games that can secretly download malicious software & gain control over your devices. Always read reviews of games before downloading to know about any potential security threat. Make it a habit to download games from a trustworthy source.

6.21. Be cautious on tiny or shortened URLs (appears like http://tiny.cc/ba1j5y). Don't click on it as it may take you to a malware infected website.

6.22. Remember that things on the internet are rarely free. "Free" Screensavers etc., generally contain malware. So be aware of such online free offers.

7. *Phishing & Spamming*

7.1 Heard a lot about Phishing, but how to identify it? Hackers generally use link manipulation as a method to create illegitimate URLs. E.g. For a legitimate link like yourbank.com, a phished link would look like y0urbnk.com

7.2 Avoid downloading email attachments or clicking on suspicious links received in emails from unknown or untrusted sources.

7.3 Don't click on the links provided in suspicious emails even if they look genuine as this may lead you to malicious websites and this may be an attempt to defraud your hard earned money.

7.4 Always be careful when clicking on links or downloading. If it is unexpected or suspicious for any reason, don’t click on it.

7.5 Use caution while clicking on links received as a message from your friends, posts on social networking websites, e-mails, etc. It can be a malicious link that may compromise your personal information

7.6 Smishing:

a. Beware of “Smishing”, where hacker uses cell phone text to trick the users. Attackers use URL link or number in text messages, make sure you don’t click on the link.

b. Never click on any UNKNOWN messages with links and do not reply to text messages

7.7 Spamming:

a. Never open spam emails unless the source is authentic as such emails may download malware silently in the background and may lead to personal data loss.

It is easy for cyber criminals to send convincing emails which appears to be from your bank. Don’t click on the links provided in such emails even if they look genuine. They could lead you to malicious websites. Instead, type in the bank’s web address in your browser and navigate from there

b. Use e-mail filters to avoid spam so that only messages from authorized users are received. Most e-mail providers offer filtering services by default.

c. Do not allow social networking sites to access your email account to look for your friends, as it may be used to send spam mails to them without their consent.

8. Beware of Software Piracy:

a) Never download or install pirated software, applications etc. on your computer, laptops or hand-held devices. It is not only illegal but also increases your vulnerability to potential cyber threats.

b) Software hosted on third party domains might be a pirated version or infected with malware. Use only authentic vendor websites while downloading software.

c) Always use genuine software and applications to avoid potential security lapses. Genuine software gets regular updates to protect your data from new cyber threats.

d) Do not use illegal file hosting sites to download software, movies, and games. They are pirated versions and may also contain malicious links/ malware which can compromise safety of your devices.

9. Phishing & Spamming Cyber Bullying / Stalking / Grooming / Sexting:

9.1 If you are victim of cyber stalking, consult your parents, friends or relatives and file complaint against the cyber stalker on National Cyber Crime Reporting Portal/ Police. Also save all communications with the stalker as evidence.

9.2 Have you ever heard of “CyberStalking”? It means, using internet or any electronic means to harass or stalk any individual/ group or an organization.

9.3 Two dangers that can haunt social media users are stalking and cyber-bullying. To deter stalkers, disable auto location update services of social media sites/Apps and refrain from tagging your location on your posts.

9.4 If you feel that you are being Cyberstalked, end the communication with the stalker immediately. If there is an option available on the social media platform “report and block” the stalker.

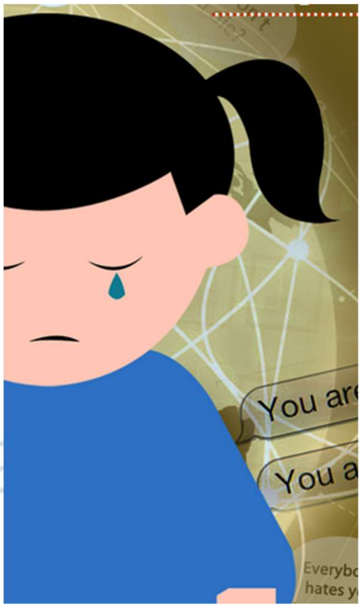
9.5 Be careful to upload your photos on social media which show your location or places you frequent visit as cyber stalker may keep tab on your daily life.

9.6 Be careful to share your personal details such as address, phone number, date of birth etc. on social media. This would make it easier for a stalker to access your personal details and use it to harass you.

9.7 Cautiously announce your vacations and check-ins on social media. Nefarious users can track your activity and might carry out actions with criminal intention such as burglary etc.

9.8 Do not announce your vacations, travel plans etc. on social media. Criminals can use it as an opportunity for theft etc.

9.9 Sharing your location on social networking sites by "checking in" to places can also provide potential hackers with too much information. Always remember to check for location services on your devices and turn off when not in use



Source: www.infosecawareness.in

9.10 Always take advantage of the available Security and Privacy Settings like showing your contact details, hiding profile picture, locking album, blocking the unwanted contacts etc. on the social networking sites.

9.11 Be cautious while accepting friend request from strangers on social networking sites. Do not reveal all your personal details to them, instead use pseudo name and details to protect your identity

9.12 Do not share your personal identifiable information to log-in to online games or chat rooms. Use nickname or alias name to log-in to online games or chat room.

9.13 Restrict access to your profile! Social media sites offer privacy settings for you to manage who can view your posts, pics, send you friend request etc. You can make your social media profile private by changing privacy settings.

Source: www.infosecawareness.in

9.14 Think about how much personal information to share on the Internet. Change settings to control who can see your profile or photos or search for you by using search engines. Few sites make Info accessible to anyone on the Internet by default.

9.15 Always make two separate e-mail accounts. One for communicating with people you trust and for your financial transactions. Use separate e-mail account for registering on social networking sites. This will protect your primary account from online stalkers.

9.16 Ensure your personal information, photos and videos are accessible only to your trusted ones. Select privacy settings on social media, accordingly.

9.17 Do not put your events calendar on your social media accounts, as it could be misused.

9.18 Do not accept friend requests from strangers on social networking sites.

9.19 Be careful while accepting friend request from strangers on social media. Do not forget to reset passwords for all your accounts while discontinuing a relationship.

Source: www.infosecawareness.in

9.20 You can never be sure about the true identity of someone you meet online. Confirm the identity of a person before adding them to your social network or instant messenger.

9.21 Avoid adding any unknown contact to your friend list and avoid accepting friend request from unknown person on social media platforms.

9.22 Share your photos and videos only with your trusted friends by selecting right privacy settings on social media.

9.23 Do not share your sensitive personal photographs and videos on social media.

9.24 Do you know cyber bullying is a common cyber threat for children? Teachers and parents should regularly discuss about cyber threats with children and encourage them to inform in case they are a victim.

9.25 Act against Cyberbullying! Delete any unwanted messages or friends who continuously leave inappropriate comments. Children must share such incidents with their parents. Such inappropriate comments can be flagged and reported to the networking site for action

9.26 Talk to your children about potential online threats such as cyberbullying and stalking. Always keep track of their online activities and restrict un-monitored access to social media sites

9.27 New generation is tech-smart… let's make them cyber safety conscious as well. Parents should discuss with their kids about potential cyber threats and ways to safeguard oneself against cybercrimes

9.28 Parents must effectively monitor online activities of their children and communicate with them about cyber threats such as cyber-bullying. This helps in having a positive and supportive relationship with their children and can protect them from cyber threats

9.29 Speak to your children about games online games and let them know why these games are unworthy to indulge into.

9.30 Do not let your kids be part of any chat group where you do not know the Administrator or purpose of the group seems shady.

9.31 Do not respond to private messages sent by an unknown person on social media platform.

9.32 Parents should guide their children on safe use of social networking platforms, chat rooms, instant messaging, SMS & mobile phones. This will help in protecting children against serious threats such as cyber-bullying, identity theft, etc.

9.33 "Report & Block" any message that asks you to harm yourself. Immediately inform your parents/ elders about such messages and report the incident to police.

9.34 Parents should monitor their children's usage of social media and should be vigilant about any abrupt changes in their behaviour.

9.35 Do not add unknown contacts challenging, daring or scaring you through messages. Avoid getting into unsettling interactions.

9.36 Avoid using voice chat or web-cam with strangers while using online internet services like social media, online games etc.

9.37 Always enable parental controls on the browsers to filter and block access to illicit websites. This helps to keep you and your children safe from potential online threats.

9.38 Parents should be aware of their child's presence on social media. This will help them to track their activities and identify fake profile if circulated under his/her name.

9.39 Regularly check browsing history of the devices such as computers, laptop, smartphones, tablets, etc. accessed by children to check their internet behaviour.

9.40 Be cautious and think before you post your personal images on social media. Remember the content may be stored forever!

9.41 Conduct yourself online the way you conduct yourself in the real world. The internet is a public platform of expression and communication. Use proper "netiquette" when online. Remember - whatever you share online is ALWAYS there!

Source: www.infosecawareness.in

9.42 Discuss safe internet practices and netiquettes with your friends and family regularly! Motivate them to learn more about cybercrimes and safe cyber practices.

9.43 Catfishing:

a. Cyber criminals often create fake social media profile to befriend potential victims & obtain their confidential or personal data. Be careful of online friend requests you accept. Never trust online friends unless you know & can trust them in real life

b. Do you know how to identify a fake account on social media? One of the ways is to monitor their historic online activities and look out for a pattern like no profile images, celebrity profile images and reluctance to engage in real time conversation

c. Be vigilant of Fake accounts! Fake account creators rely on the basic trust nature of humans that lead them to believe in the authenticity of an account. They leverage this trust to fraud, bully, defame the person or others.

10. Online Matrimonial Frauds

10.1 Always choose to meet the prospective match in a public place as you don't know what kind of person he or she might be. Also, keep your family and friends informed about the meeting. This will help avoid matrimony frauds.

10.2 While chatting on matrimonial website, avoid talking to a person, if he/ she pressurizes you to reveal your personal information. Always refrain from sharing your personal information until you are completely sure and have done a thorough background check.

10.3 Always be careful while dealing with 'NRI' profiles on matrimonial websites. Commit to marriage only after face-to-face meetings, especially the prospective match's parents/ relatives and validating any documents related to their address and employment abroad.

Source: www.infosecawareness.in

10.4 To avoid matrimonial online fraud, do not transfer funds or offer financial help to the prospective match. Be cautious, the moment someone asks you for money citing some reason or the other and avoid further communication with him/her.

10.5 To avoid matrimonial fraud, share the information about the prospective match with your family. Your family should be aware of the information shared, if any, by you with the prospective match found on matrimonial website.

10.6 Create and use new e-mail id for registering on matrimonial websites. Preferably, use e-mail as a source of communication and do not share your personal data such as; photo, phone number, residential address, etc. on matrimonial websites.

10.7 Conduct an end-to-end background check of the prospective match to avoid matrimonial frauds. Try to contact at workplace with family, friends, relatives, neighbours or associates of a prospective match to know more about him/ her.

10.8 Prior to registering on a matrimonial website, check authenticity and reviews of the website. Consult your friends and family to know about reliability of website. If possible, try to speak to people who might have found their life partners through online matrimonial platforms.

10.9 Do not share your sensitive personal pictures while chatting with anybody, whom you have met through matrimonial website. These pictures can be used by the potential fraudster to blackmail you and defraud. These images may be leaked on internet as well.

10.10 Never share personal information or your personal sensitive photos while chatting/ communicating with someone on matrimonial website.

11. Ransomware

11.1 Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

11.2 Do not pay the ransom. Even if the ransom is paid, there is no guarantee that you will be able to regain access to your files.

Source: www.infosecawareness.in

11.3 Lookout for the latest scams! Currently, “ransomware” is on the rise. Make sure you do not click or download links from unknown sources. Hackers can steal your credentials and encrypt your data and demand ransom to decrypt it

11.4 Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks.

11.5 Always perform regular backups on important data and keep the backup copies disconnected from the computer

--------------------------------------END--

CYBER C D DOST

Indian Cyber Crime Coordination Centre

@CyberDost

सत्यमेव जयते

गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS