CYBER AWARENESS CAMPAIGN

CYBER POLICE STATION

MIRA-BHAINDER, VASAI-VIRAR POLICE COMMISSIONERATE

☎ **1930**
HELPLINE NUMBER

3rd Floor, Crime Branch Building, Kanakia Road, Mira Road East, Thane 401107

Email - cybercrime.mb-vv@mahapolice.gov.in

"I Do not Invest **My Hard Earned Money** in Unregulated Plans."

"Never Share **OTP**

"I SEARCH GOOGLE **WISELY.**"

"I know Making **FAKE PROFILE** IS CRIME"

"I'm a **CYBER "SAVIOUR"**

"**CYBER CRIME** is the greatest profile threat to everyone. Be aware always"

"I Post decent messages on **SOCIAL MEDIA**

"At the end of the day, the goals are ***Simple, Safety,*** and ***Security.***"

"I Do Online Shopping with **Reputed website**"

"Before **Downloding** any App I do Search and then **Accept/Allow.**"

https://www.youtube.com/@MBVV_Police

सायबर जागरूकता मोहीम

सायबर पोलीस ठाणे

मिरा-भाईंदर, वसई-विरार पोलीस आयुक्तालय

1930
HELPLINE NUMBER

(काशिमीरा Email-pi.kashimira.mb-vv@mahapolice.gov.in)

Email - cybercrime.mb-vv@mahapolice.gov.in

ISSUED IN PUBLIC INTEREST

सायबर फसवणूक झाल्यास तात्काळ 1930 वर संपर्क साधा आपल्या बँकेला / क्रेडिट कार्ड कंपनीला तात्काळ संपर्क साधा ऑनलाईन पोर्टल वर तात्काळ तक्रार नोंद करा

www.cybercrime.gov.in

स्कॅन करा

हरविलेले/ गहाळ झालेले कागदपत्र/ वस्तू यांच्या तक्रारीसाठी

www.mbvv.mahapolice.gov.in/

स्कॅन करा

फसवे SMS / Email / Calls प्राप्त झाल्यास तक्रार नोंद करा

www.sancharsaathi.gov.in (chakshu)

स्कॅन करा

मोबाईल हरविल्यास / चोरी गेल्यास तात्काळ तक्रार नोंद करा

www.ceir.gov.in

स्कॅन करा

बँक / विमा कंपनी यांच्या विषयीची तक्रार तात्काळ नोंद करा म्युच्युअल फंड, स्टॉक ब्रोकर्स, सामूहिक गुंतवणूक योजना (CIS) गृहनिर्माण वित्त कंपन्या, विमा कंपन्या, पेन्शन योजना, बिगर बँकिंग वित्तीय कंपन्या

www.sachet.rbi.org.in

स्कॅन करा

स्कॅन करा

INDIAN GRIEVANCE OFFICER CONTACT
FORM FOR FACEBOOK

INDIAN GRIEVANCE OFFICER CONTACT
FORM FOR INSTAGRAM

INDIAN GRIEVANCE OFFICER CONTACT
FORM FOR WHATSAPP

For additional information subscribe our YouTube *https://www.youtube.com/@MBVV_Police*

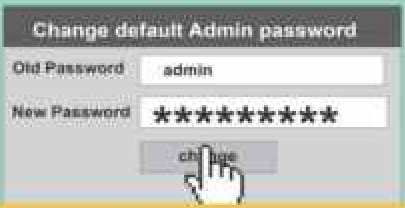
महाराष्ट्र पोलीस

सद्रक्षणाय खलनिग्रहणाय

WiFi SECURITY

सी डैक CDAC

Change the default username and Password of the Access Point



Change default Admin password

Old Password: admin

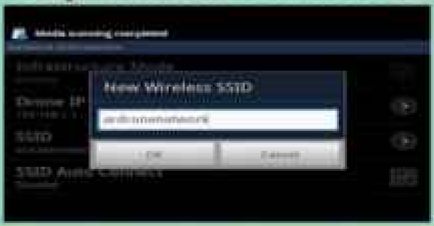
New Password: **********

Switch off the wireless router when not in use

Never Auto-Connect to open Wi-Fi Networks

Use Firewalls and Security Software

Change SSID regularly and keep it in hidden mode



Media scanning completed

Infrastructure Mode

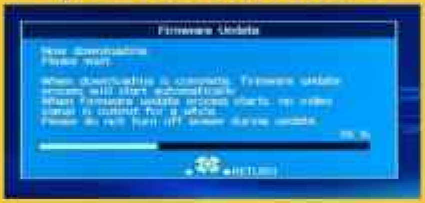
Device IP

SSID

SSID Auto Connect

New Wireless SSID: ardunonetwork

Always maintain a updated firmware

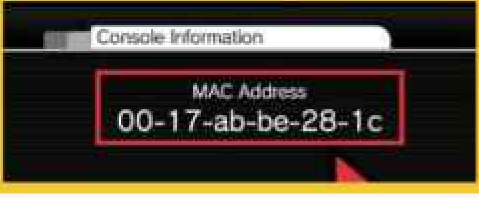


Firmware Update

Now downloading
Please wait.

When downloading is complete, firmware update process will start automatically.
When firmware update process starts, no video signal is output for a while.
Please do not turn off power during update.

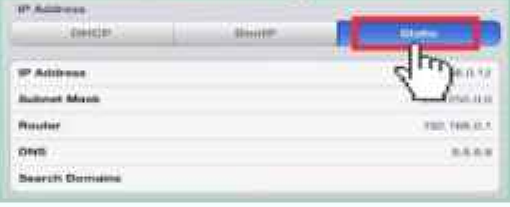
Enable MAC Address Filtering



Console Information

MAC Address
00-17-ab-be-28-1c

Always use static IPs instead of enabling DHCP



IP Address

IP Address

Subnet Mask

Router: 192.168.0.1

DNS: 8.8.8.8

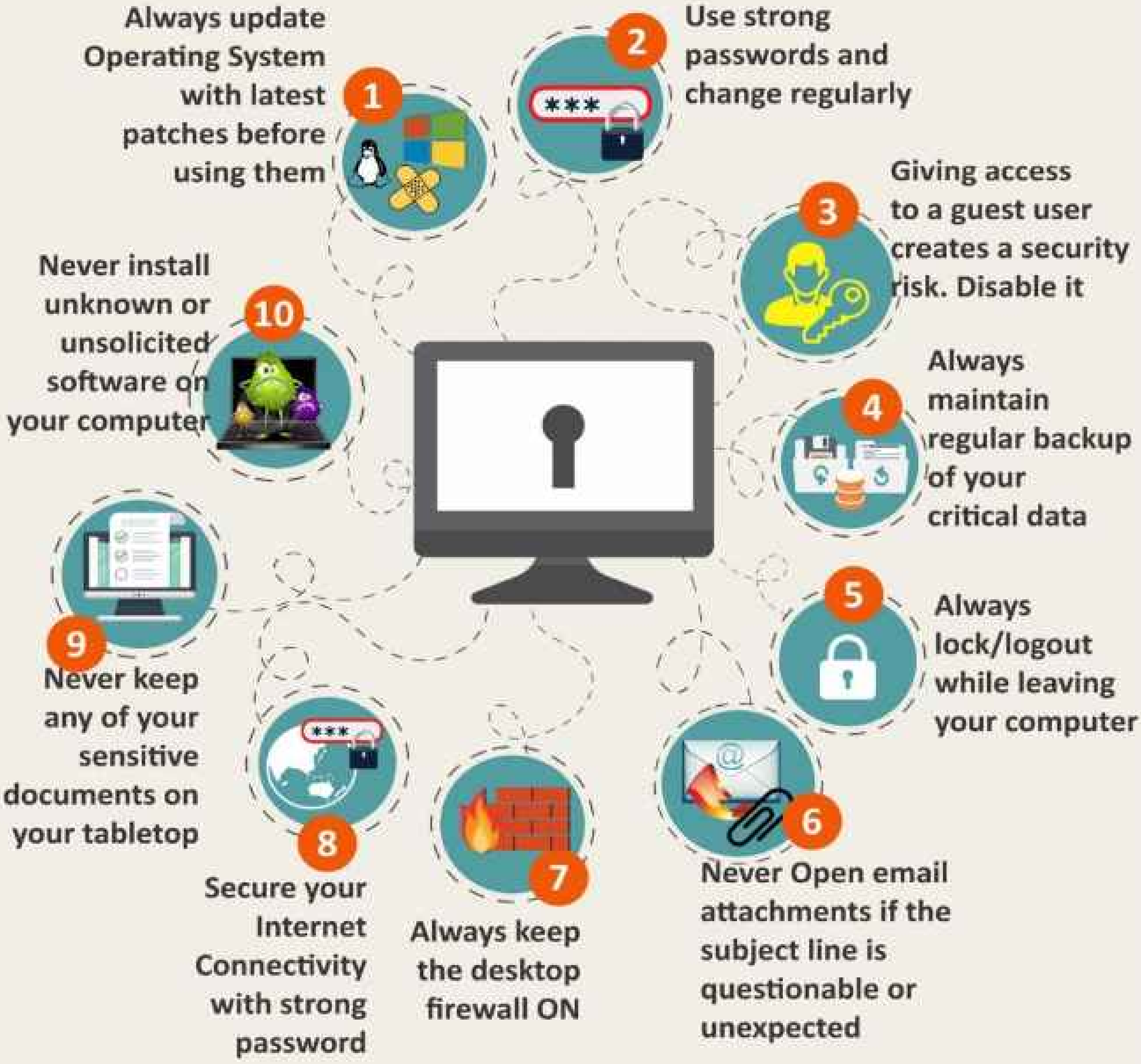
Search Domains

महाराष्ट्र पोलीस

सी डैक
CDAC

DESKTOP SECURITY

Secure Yourself, Your System & Your Network



1. Always update Operating System with latest patches before using them

2. Use strong passwords and change regularly

3. Giving access to a guest user creates a security risk. Disable it

4. Always maintain regular backup of your critical data

5. Always lock/logout while leaving your computer

6. Never Open email attachments if the subject line is questionable or unexpected

7. Always keep the desktop firewall ON

8. Secure your Internet Connectivity with strong password

9. Never keep any of your sensitive documents on your tabletop

10. Never install unknown or unsolicited software on your computer

महाराष्ट्र पोलीस

MOBILE APPLICATION SECURITY

सी डैक
CDAC

Do good research about apps and their developers by reading the reviews

Use only official stores for downloading Apps

Check for spelling mistakes in the title or description

Reset your phone to factory settings to remove any malware

Beware of apps that promise shopping discounts

Make sure you review and manage permissions for each app you download

Avoid installing apps by clicking on links in emails, social media etc.,

Uninstall apps when you no longer use

Look at the publish date. A fake app will have a recent publish date

Always keep an updated anti virus security solution installed

Browser Security

Best practices and guidelines for strengthening your browser security

Always use secured web browsers which enables safe browsing over internet

Keep your OS and Browser software up to date with the latest versions and security patches.

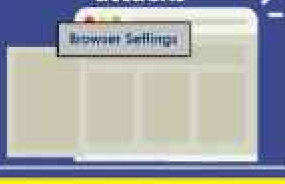
Turn off all JavaScript or Active X support in your web browser before you visit unknown websites

Use strong passwords and Never store passwords in your browser

Block Pop-ups and scripts

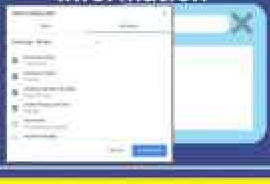
Use Virtual Private Network (VPN) or Proxy Servers while accessing public Wi-Fi

Optimize your browser's settings to protect your device from malicious attacks



Make sure the URL of the websites has "https://" or a padlock icon

Clear your browsing activity on regular basis to avoid threat to confidential information



सी-डैक
CDAC

IDENTITY THEFT

PROTECT YOUR PERSONAL DATA

Limit use of personal information in social networking sites

Monitor your financial accounts for suspicious activity on a regular basis

Check all your online accounts and social networking accounts for any unauthorized use

Beware of onlookers when using your credit/debit card and entering your PIN number

Use security features provided by all websites

Do business only with trusted companies/websites

Password protect all documents you send

Always read and check privacy policies

Do online shopping only through sites that uses secure payment gateway

Take immediate action if you think your personal information has been misused

ONLINE SCAMS

सीडैक
CDAC

BE AWARE

@uma41.co
JOB OFFER
DEPOSIT THE AMOUNT TO JOIN THE JOB
MEGA SALE
CONGRATULATIONS YOU HAVE WON LOTTERY OF $50,000
CLICK THE LINK TO UPDATE YOUR BANK DETAILS

WARNING EMAIL SCAMS

- Banks will never ask for personal credentials via email. Don't give
- Check subject line like "your account has been suspended"
- Don't click on the links that you receive through email

DANGER JOB SCAMS

- Be aware of spoofed interviews
- Beware if a recruiter offers you a job immediately without verifying your previous work experience
- Never believe emails, asking to deposit money for a job offer

DISCOUNTS! BEWARE

- Beware of fake websites
- Never believe in fake coupon email that may ask you to enter personal / financial information
- Always check the authenticity of the website before placing

LOTTERY SCAMS STOP DO NOT ENTER

- Never believe lottery emails
- Beware - Lottery scams will ask you to pay for claiming your winning amount.
- Just think why you won lottery without your participaion

महाराष्ट्र पोलीस

WhatsApp Security Tips

सी डैक
CDAC

Enable two-factor authentication, to ensure that nobody can set up your WhatsApp without knowing the secret 6-digit code

Always read the terms and conditions before downloading any APP

Make sure cloud backups are off. They are not secured when sharing with the cloud provider

Never accept files or begin downloads from messages sent to you by strangers or unknown numbers

Manage WhatsApp Web effectively, Log out from all computers

WhatsApp Web

To block an unknown number, open that particular chat window go to more option and block

Never trust message that claims to come from WhatsApp and demands payment for the service

Your subscription is ending soon

Never send private information like bank account details, PINs or passwords through WhatsApp

Restrict Access to Your Profile Pic to only contacts.

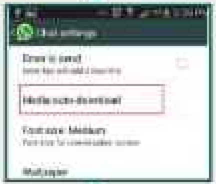
Privacy

Last seen

Profile photo

Status

Keep automatic downloads disabled



Chat settings

Media auto-download

Font size: Medium

Wallpaper

Avoid using WhatsApp when you are connected to open Wi-Fi networks

Never respond to suspicious messages from unknown numbers

Always keep an updated anti virus security solution installed on your mobile device

Complete Security against Virus, Malware, Spyware and Trojans

Minimum Resource Usage and Extra Fast

Antivirus Database Updated Regularly

Deactivate WhatsApp if you lose your phone

SECURE USAGE OF CREDIT / DEBIT CARD

After receiving the card from the bank make sure the mail is completely sealed and there is no damage and immediately sign on the card

Ensure that your transaction is ended/completed at ATM machine before leaving the premise

Change the default pin number and don't forget to change it frequently

Do not respond to e-mail's asking for personal information including financial information, banks never ask for such information

Monitor your credit card account statement regularly for suspicious / unauthorized activity

Before you use an ATM ensure that there are no strange objects in the insertion panel of the card

Always keep an eye on how the vendor swipes your card and make sure that the transactions happen at your presence

Never keep your credit / debit card and the PIN at one place

When you dispose a card for renewal/up gradation, please make sure to cut it diagonally before disposal

Always log off from any website after completing online transaction with your credit / debit card and delete the browser cookies

BE AWARE OF FAKE JOBS

- Many of the students apply online for jobs. The accused collect the details posted in the websites and send fake e-mails.
- The e-mail looks like a mail from genuine companies through fake mailer sites and also conducts interviews.
- The victim receives a fake job offer letter. In return this fraudster asks for huge amount before and after receiving the offer letter.
- Stranger may send the offer letter using fake mailer service and make spoofing call in the name of MNC and send the offer letters and get the amounts deposited in the various places/Bank accounts and immediately withdraw the amounts and they may cheat you.

Precautions:

Always prefer for personal interview Scammers also conduct telephonic interview, which can be fake/risky

Don't respond to spam mails without verification of the e-mail origin

Check for spelling mistakes.Fake job offer mails generally have spelling mistakes and grammatical errors

Don't deposit money unless the candidate is interviewed personally by the company

Never believe in the job offer to which you have not applied or if they ask for your personal information / bank details

Don't beleive in emails received from personal mail id. Authentic job offers are sent from company registered e-mails

Using weak Passwords or blank passwords

Weak and blank passwords are one of the easiest ways to attackers to crack into your system. Cyber criminals can use the same techniques used to guess the answers to secret questions can also be used to guess passwords. Anything based on something your friends will know, or that is available from a website, is a very poor choice as a password.

Always you need to "Use Strong Passwords"

TIPS TO PROTECT YOUR PASSWORD

Password are like socks change them regularly

Never share your password with others

Use different passwords for different accounts

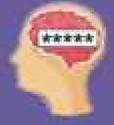
Remember password

yes [✓ no]

Do not select 'Yes' when any application ask you if you want them to remember your passwords

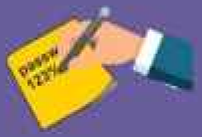
Be aware of Shoulder Surfers at public places while you are entering your passwords into the login accounts

Make passwords more complex to increase the difficulty of attacks that rely on brute force / guessing



Your brain is the best place to store your passwords

Never use dictionary words (like animal, plants, etc.) while creating passwords



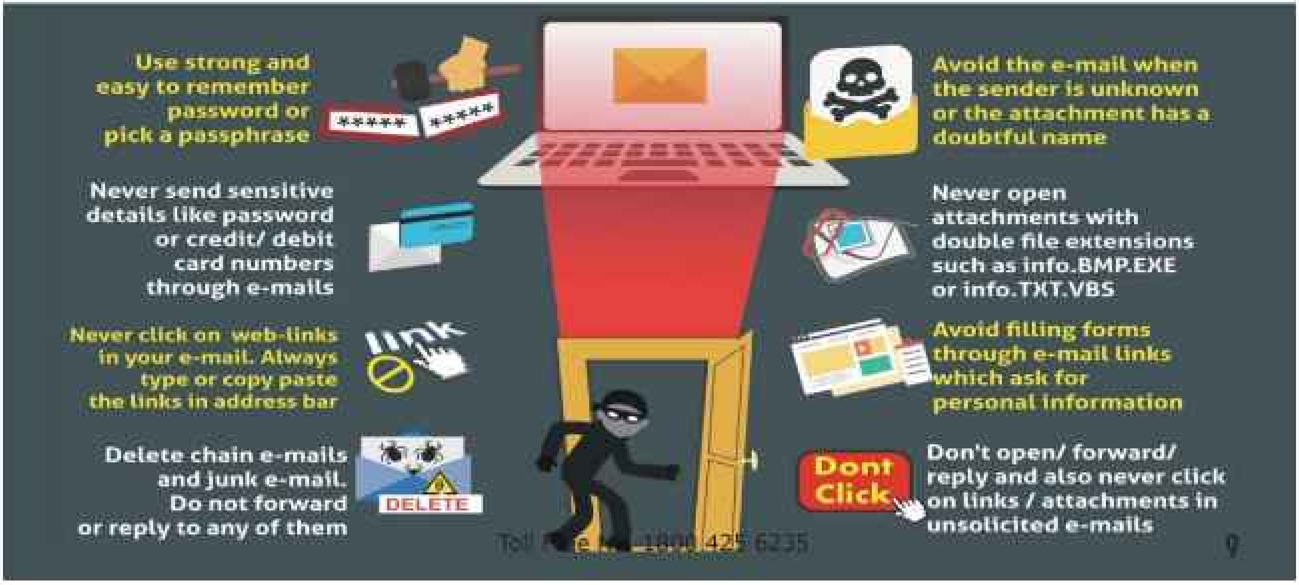
Never write passwords on paper or on any disk drive to store it

Internet Security:

- Check the copyright issues before using the content of Internet. Follow Internet Ethics while browsing.
- Always access the site which uses https (Hyper Text Transfer Protocol Secure) while performing online transactions, downloads etc, which is secure.
- If the site uses SSL, verify the certificate details like who is the owner, expiry date of the certificate etc to confirm whether it is trusted or not. You can do this by clicking the lock icon.
- Use only original websites for downloading the files rather than third party websites.
- Scan the downloaded files with an updated Anti-Virus Software before using it.
- Install and properly configure a software firewall, to protect against malicious traffic.

Data Security

- Enable auto-updates of your operating system and update it regularly.
- Download Anti-Virus Software from a trusted website and install. Make sure it automatically gets updated with latest virus signatures.
- Download Anti-Spyware Software from a trusted website and install. Make sure it automatically updates with latest definitions.
- Use "Encryption" to secure your valuable information.
- Strong password should be used for "Admin" Account on computer and for other important applications like email client, financial applications (accounting etc).
- Backup: Periodically backup your computer data on CD / DVD or USB drive etc... In case it may get corrupted due to Hard Disk failures or when reinstalling/formatting the system.
- Recovery Disk: Always keep recovery disk supplied by Manufacturer / Vendor of the Computer System to recover the Operating System in the event of boot failures due to system changes such as uncertified Drivers/ unknown Software publisher.
- Startup programs should be monitored / controlled for optimal system performance.



Use strong and easy to remember password or pick a passphrase

Never send sensitive details like password or credit/ debit card numbers through e-mails

Never click on web-links in your e-mail. Always type or copy paste the links in address bar

Delete chain e-mails and junk e-mail. Do not forward or reply to any of them

Avoid the e-mail when the sender is unknown or the attachment has a doubtful name

Never open attachments with double file extensions such as info.BMP.EXE or info.TXT.VBS

Avoid filling forms through e-mail links which ask for personal information

Don't open/ forward/ reply and also never click on links / attachments in unsolicited e-mails

USB STORAGE DEVICE SECURITY

USB (Universal Serial Bus) storage devices are very convenient to transfer data between different computers. You can plug it into a USB port, copy your data, remove it and be on your way. Unfortunately this portability, convenience and popularity also brings different threats to your information.

Data thefts and Data leakage are everyday news now! All these can be controlled or minimized with care, awareness and by using appropriate tools to secure the information.

Threats

- Malware Spreads through USB storage devices. Somebody may intentionally sell USB storage devices with malware to track your activities, files, systems and networks.
- Malware may spread from one device to another device through USB Storage Devices using autorun.exe, which is by default enabled.

Unauthorized Usage

Somebody may steal your USB Devices for Data.

Baiting

Somebody intentionally leave USB devices at your Desk or Place with Malware

How to stop Data Leakage via USB storage ?

- Design and adopt a good security policy to limit the usage of USB Storage devices.
- Monitor the employees what they are copying.
- Implement Authentication, Authorization and Accounting to secure your information.

Threats to women while using Wi-Fi

Free Wi-Fi s hotspots for cyber attacks

Most of the women tend to connect to Wi-Fi if it is available for free in the public places to use their favorite social media or chatting applications. Browsing internet using public wireless computer network at railway stations and airports may leave you vulnerable to cyber attacks. Successful exploitation of these vulnerabilities allows an attacker to obtain sensitive information such as credit card numbers, passwords, chat messages, emails etc, It is suggested that users avoid public Wi-Fi and instead use secured networks only. Few of the tips to note when using free public Wi-Fi

> *Never auto-connect to open Wi-Fi networks in public places*
> *Visit only secured websites while using public Wi-Fi*
> *Disable sharing of data*
> *Keep Wi-Fi Off when you don't Need It*
> *Avoid using sensitive passwords*

Tracking an Individual

Like mobile phones, Wi-Fi devices have unique identifiers that can be used for tracking purposes which can cause potential security issues. Tracking by using a Wi-Fi hotspot can also lead to cyber crimes like stalking. To receive or use a service, often websites require the user to share their personal information such as name, age, ZIP code, or personal preferences.

By authorities: the authorities have easier access to people's browsing details and habits, and with justification in the name of national security, could be used to monitor the people without their consent.

By hackers: steal information and hack into unsuspecting victim's bank accounts and misuse corporate financial information and secrets

Never Auto connect to open / free wi-fi networks

Ways to Stay Safe On Public Wi-Fi Networks

1. Use HTTPS
2. Run Anti-Virus Software
3. Turn Off Sharing
4. Protect Your Passwords

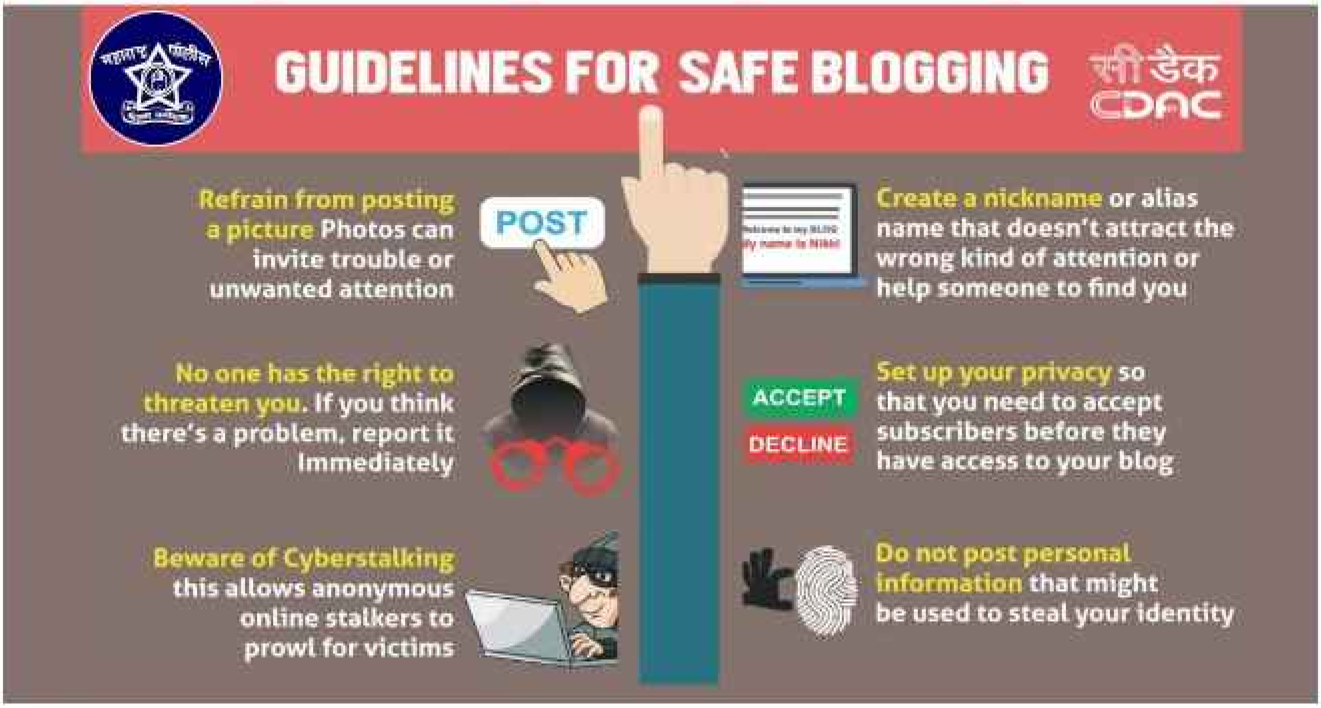
Wow!!
Free Wi-Fi
freeWiFi
www.infosecawareness.in

SAFETY MEASURES TO PROTECT YOUR MOBILE PHONE

- Enable Autolock and a Strong Passcode. Consider changing it frequently
- Record your phone's unique ID number (IMEI number)
- Make sure you log off from banking and other important Apps in your mobile phone after use
- Consider tracking software
- Regularly back up your Mobile phone

WHAT TO DO IF YOUR MOBILE PHONE IS LOST

- Report theft of your mobile phone to your bank and nearest police station immediately
- Try to locate your phone via GPS
- Block your SIM card and Apply for a duplicate SIM card
- Don't forget to remotely lock your phone
- Change your important passwords immediately



GUIDELINES FOR SAFE BLOGGING

Refrain from posting a picture Photos can invite trouble or unwanted attention

No one has the right to threaten you. If you think there's a problem, report it immediately

Beware of Cyberstalking this allows anonymous online stalkers to prowl for victims

Create a nickname or alias name that doesn't attract the wrong kind of attention or help someone to find you

Set up your privacy so that you need to accept subscribers before they have access to your blog

Do not post personal information that might be used to steal your identity

ONLINE SCAMS

- Banks will never ask for personal credentials via email. Don't give
- Don't click on the links that you receive through email
- Be aware of spoofed interviews
- Never believe emails, asking to deposit mone for a job offer

- Never believe in fake coupon email that may ask you to enter personal / financial information
- Always check the authenticity of the website before placing any order
- Beware - Lottery scams will ask you to pay for claiming your winning amount.
- Just think why you won lottery without your participaion

GUIDELINES FOR SAFE INSTANT MESSAGING

सी डैक
CDAC

Never reveal your full name,address, phone number,location or other personal information.
Use alias names or nick name

Opening attachments or clicking on the links sent from strangers may be harmful, they may contain virus.
Never open or click on them

Some times strangers may offer free gifts through instant message with false information.
Never believe or accept them

If anything turns worse or if you find something creepy,
leave the chat room or block the person

सी डैक
CDAC

Tips for secure usage of ATM

- Be aware of skimming machines
- Remember to collect the receipt after your transaction
- Cover the keypad while entering the pin
- Beware of shoulder surfing
- Donot accept assistance from strangers

What women should do while using social networking sites

1 Always check the authenticity of the person before you accept a request on social networking sites

2 Keep some privacy setting like share your photos and activities only with your families and known friends

3 While choosing a Social Networking site, privacy issues should be considered, think before you post, chat, upload or download

4 Take your father/husband/ brother's or any family members permission if you want to meet the person whom you met in the networking site, so they can give you some suggestions and always know with whom you are meeting

5 Never respond to harassing or rude comments which are posted on your profile

6 If you think that your social networking account details have been compromised or stolen, report your suspicions to the networking site support team immediately

What women should avoid while using social networking sites

1 Don't give or post any personal information like your name, address of the company / home, phone numbers, age, sex, credit card details.

2 Do not post your friends information in networking sites, which may possibly put them at risk

3 Avoid posting the plans and activities which you are going to do in networking sites

4 Don't give out your password to anyone

5 Don't use a webcam with people you do not know

6 Don't click the links which you are getting through social networking sites. If you want to visit the site then directly go through the original websites

Privacy Issues

You may be in risk if you ignore some privacy issues like-

- Sharing your photos and activities publically.
- Sharing your location on your post give chance to the scammers to track your location.
- Adding friends whom you don't know without any proper identification become risk for you while using social networking sites.

Best practices to avoid Financial Frauds

Never handover your device to strangers

Avoid using open Wi-Fi for making payments

Disclose your banking details only in secure payment websites

Keep a watch on transaction logs and alerts

Always verify and install authentic e-wallet Apps

Immediately block your SIM if your device gets lost or stolen

Report promptly the theft or loss of your card on the toll free numbers

Ensure that you securely dispose your payment receipts & bank statements

Use strong passwords and change frequently

Refrain from clicking suspicious links received in SMS or email