

Supported by:



<http://www.cyberabadpolice.gov.in/>

<https://cyberabadsecuritycouncil.org/>

www.endnowfoundation.org



SMARTPHONES

THE BIGGEST NON - DRUG ADDICTION OF THE 21ST CENTURY

If your smartphone has made you it's slave,
Here's a step - by - step approach to detach from it



Disable notification on your smartphone.



Keep your phone away during meals with your friends and family.



Charge your device outside the bedroom.



Device free meetings.



Access social media from your computer instead of your smartphone.



Use grey scale mode on your phone.



Keep only most important tools on your home screen.



Screen time for IOS and digital wellbeing for android to control the technology usage.



ONLINE GAMING IS PUBGECTED TO A LOTS OF RISKS

Read on to know it's negative consequences.



All day addiction to games.



Bad influence on health.



Isolation from family & friends.



Waste of precious time.



Face a problem of insomnia.



An expensive hobby.



Rising level of aggression.



Affects the eyesight.

We will hack your account !!

Should i put a new password ??



SOCIAL MEDIA IS A LOT MORE FUN WHEN YOU PAY ATTENTION TO SAFETY

Here are some tips to stay safe in the cyberworld



Use a strong password.



Click on Links with caution.



Use a different password for each of your social media accounts.



Be careful about the personal information you share.



Set up your security answers. (this option is available in most social media platforms.)



Become familiar with the privacy policies of the social media channels.



Access social media from computer only.



Protect your computer by installing antivirus software.



Be cautious while accepting friend requests.



Remember to log off when you are done.

CYBER BULLYING

TYPES



Cyber stalking

Repeatedly sending the messages that include threats of harm or are highly intimidating.



Impersonation

Pretending to be someone else & sending or posting any material online that makes that person look bad, gets that person in trouble.



Denigration

Dissing' someone online. Sending or posting any cruel gossip about a person to damage his or her reputation or friendship.



Harassment

Repeatedly sending some offensive, rude, and insulting messages.



Outing & trickery

Sharing someone's secret or embarrassing information online.



Flaming

Online fights using electronic messages with angry and vulgar language.



Exclusion

Intentionally excluding someone from online group, like a 'buddy list'.

FAILURE **DEFORMED** **UGLY**
MENTAL **SELFISH**
WORTHLESS **LOSER**

CYBER BULLYING

AFTER EFFECTS

Health issues

Suicide



Depression



Alcohol



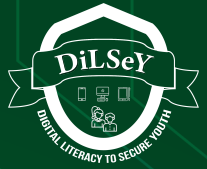
Violent



FAILURE DEFORMED UGLY
MENTAL SELFISH
WORTHLESS LOSER

COMMON CYBER THREATS

Here are some common forms of cyber threats to protect against.



RANSOMWARE

Malevolent software which locks user access by encrypting data using cryptovirology while extorting the payment from the victim in order to decrypt and restore the files.



MALWARE

Malicious software installed on a machine unknowingly and performs criminal actions for a third party.



BOTNETS

A "secret key" that provides entry to devices and connections to be controlled by an attacker for criminal purpose.



SPOOFING

Email messages sent from a fraudulent account masquerading as a legitimate and trusted source as an attempt to gain access to a user's system or confidential information.



WORM

Stand alone software which does not require a host program in order to propagate and replicate itself onto other networks and drives damaging data and software as it spreads.



TROJANS

Computer program that contains destructive code disguised as the harmless programming.



DENIAL OF SERVICE {DDOS}

Floods bandwidth which makes online systems unavailable.



VIRUS

A type of malware that when executed spreads from computer by replicating its programming and infecting user programs and files to change the way they operate or to stop working altogether.



PHISHING

A DNS server software vulnerability is exposed or a host file is swapped and a legitimate website is maliciously redirected to a scam site where unknowing visitors enter their confidential information.



SPYWARE

Criminal malware on the hard drive used to covertly monitor user activities.



PHARMING

A DNS server software vulnerability is exposed or a host file is swapped and a legitimate website maliciously redirects to a scam site where unknowing visitors can enter into their own confidential information.



ADWARE

Can redirect the search requests or automatically render some of advertisements producing the revenue for its creator.





PHISHING ATTACK ALERT

Gear up to protect yourself from cyber criminals.

TOP 5 RED FLAGS

Web links can lead to unfamiliar sites (hover over them to check).



There is an attachment you weren't expecting.



You notice poor spelling & grammar throughout.



It asks for personal info (passwords, all of bank information, etc.)



The sender doesn't address you by name.



HOW TO STAY PROTECTED

1



Do not click on any links or attachments you can't verify

2



Call to verify requests for info (even if it seems to come from someone you know!)

3



Whenever in doubt, always contact optimal for help!

HOW EXPOSURE TO **BLUE LIGHT** AFFECTS YOUR BRAIN AND BODY

By disrupting melatonin, smartphone light ruins sleep schedules. This leads to all kinds of health problems:

The disruption to your sleep schedule might leave you distracted and also impair your Memory the next day.



There's some evidence that blue light could damage our vision by harming the Retina over time — though some more research is needed.



A poor night's sleep caused by smartphone light can make it Harder To Learn.



Researchers are investigating whether or not blue light could lead to Cataracts.



Over the long term, not getting enough sleep can lead to Neurotoxin buildup that makes it even harder for you to get good sleep.



There is a connection between light exposure at night and the disturbed sleep that come with it and an increased risk of breast and prostate Cancers.



People whose melatonin levels are suppressed and whose body clocks are thrown off by light exposure are more prone to Depression.



By disrupting melatonin and sleep, smartphone light can also mess with the hormones that can control hunger and potentially increasing Obesity Risk.

Call at 919xxxxxxx
to know more



This looks interesting.
i should call !



PEOPLE ARE MISUSING SOCIAL MEDIA, MESSAGING AND INTERNET TO SPREAD FAKE NEWS

Here are ways how you can spot fake news.



Check the source and url.



Refer fact checking sites
(www.factly.in).



Read beyond the headline.



Check if it's a joke.



Check the date.



Check your biases before
judgement.



Watch for any unusual
formatting.



Do Google Reverse Image Check.

SPOTTING **FAKE NEWS** ON SOCIAL MEDIA & INTERNET!



Consider the source

Is the source credible, trustworthy and well known? i.e. Consider the source that is from a reputed news paper, news channel or online news website.



Check the url

Does it seem legitimate? Does the website have a track record of being reliable? Many sites use similar sites ending with .io .co .com.



Who's the author?

Did you search for the author's name online to see if they are credible & very well respected? Many fake sites won't use the author's name.



Read beyond headline

Does the article seems balanced, fair & objective? Always study it critically, detecting the tone & viewpoint while checking your bias at the door.



Disregard your bias

It is easier to believe stories that confirm your internal views. But the next time you see on social media post that flames your political, racial or religious views.

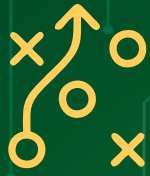


Get a second opinion

If a story makes you very angry and a dig deeper, consult known contact or use debunking sites before forwarding.

SPOTTING FAKE NEWS

9 TYPES OF MIS AND DISINFORMATION



False Connection

When the headlines, visuals or the captions do not support the content.



False Context

When the genuine content is shared with the false contextual information.



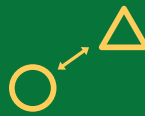
Manipulated Content

When some of genuine information or the imagery is manipulated to deceive.



Satire or Parody

No intention to cause harm but has potential to fool.



Misleading Content

Misleading the use of information to frame an issue or individual.



Imposter Content

When genuine sources are impersonated.



Fabricated Content

Content that is 100% false, and designed to deceive and do harm.



Propaganda

When content is used to manage attitudes, values and knowledge.



Sponsored Content

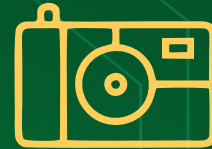
Advertising or PR is disguised as editorial content.

SPOTTING FAKE NEWS

PHOTO VERIFICATION



Identify and verify the original source and the content (which includes location, date and the approximate time).



Always use tools like FotoForensics/Findexif for the information on camera model/timestamp.



Try to find multiple sources. Challenge the original source to prove veracity - ask follow up questions.



Using Wolfram Alpha, check if the weather captured in photo (e.g. sunny, rainy, overcast) was actually the weather in that area.



Always use tools like www.tineye.com and <https://images.google.com> on Google.

SPOTTING FAKE NEWS

VIDEO VERIFICATION



Identify and verify the original source and the content (which includes location, date and the approximate time).



Try to find some multiple sources. Challenge the original source to prove veracity - ask follow up questions.



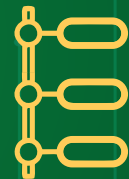
Use the Amnesty International's Data Viewer. (<https://citizenevidence.amnestyusa.org>).



Scrutinize uploader's name and the date of upload.



What information does the social media / affiliated accounts give that indicate location, activity, reliability, bias or agenda of uploader?



How long have these accounts been active? How active are they?



Is the person listed in online databases or the networking platforms e.g. LinkedIn?



Are the other accounts, including social media, a blog or website - affiliated with the uploader?



10 SECURITY TIPS FOR WORK FROM HOME



Use your workplace device having all of the security precautions in place.



Always use the two - factor - authentication and complex passwords for all accounts and devices.



Use VPN to access the data through secure connection.



Always enable the Data Loss Prevention (DLP) tools to ensure sensitive data is not lost.



Regularly update OS and Antivirus to protect against malware attacks.



Be aware of the COVID-19 scams, phishing, e-mails, malicious domains and fake apps.



Avoid using the unsecured, free, public wi-fi hotspot or network.



Ensure that only authentic verified URLs are accessed.



Regular backup of data in your system and cloud (One Drive, G-Drive, etc.).



Disable USB ports & System Bluetooth connectivity.



THOUSANDS ARE FALLING PREY TO **ONLINE JOB SCAMS** EACH DAY. DON'T BE ONE OF THEM!

Here's how you can spot an internet job scam



You are immediately selected for the Job.



The interview is scheduled on the instant messaging platforms.



Vague job requirement and job description.



Search results about the Company or the job doesn't show up.



Unprofessionally written e-mails.



You are asked to provide Confidential Information.



E-mails with or no contact information or Company Signature.



You're asked to Pay.

DON'T BE A VICTIM OF FRAUD!



DO NOT



Pay in Advance.



Check before approving
Payment Requests.



Share Personal Details like
PIN , OTP, Account Number,
etc.



Report the Questionable
Accounts immediately.

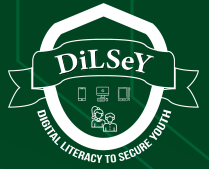


Facilitate any Monetary
Transactions while on Call.

BEWARE : Payments through Online Platforms are robust
but Susceptible to Fraud.

99% of Payments are prone to Phishing and Social
Engineering Crimes.

CARD FRAUD



Always guard your Cards and the Card details.



Do not let your Card out of your sight when making a transaction.



Ask the retailer to confirm the amount being debited from your Card.



Sign the New Cards as soon as they arrive.



Check your Receipts against your Online Statements.



Carefully discard your receipts from your Card transactions and the Information related to your financial affairs.



Don't leave your cards Unattended in a Public Place. Keep personal belongings with you at all time.



Never write down your PIN nor disclose to anyone.



When making Online transactions make sure you are using Updated Antivirus & Operating System Software.



Only buy from trusted sources. For Internet purchases, use the Security Protocol 3D - Secure.



When replacement card arrive, cut Expired / Unused / Blocked cards into several pieces, including through the magnetic strip and / or chip.

CASH MACHINES (ATM'S)

Always try to be aware of others around you.

Don't use the ATM if there are any signs of tampering.



If the ATM does not return your Card, then report it to your Bank.

Shield your PIN.

PAYMENT TERMINALS (POS)

Card - skimming can also occur at the retail outlets, particularly bars, restaurant areas, the parking ticket machines & the (unnamed) petrol stations.

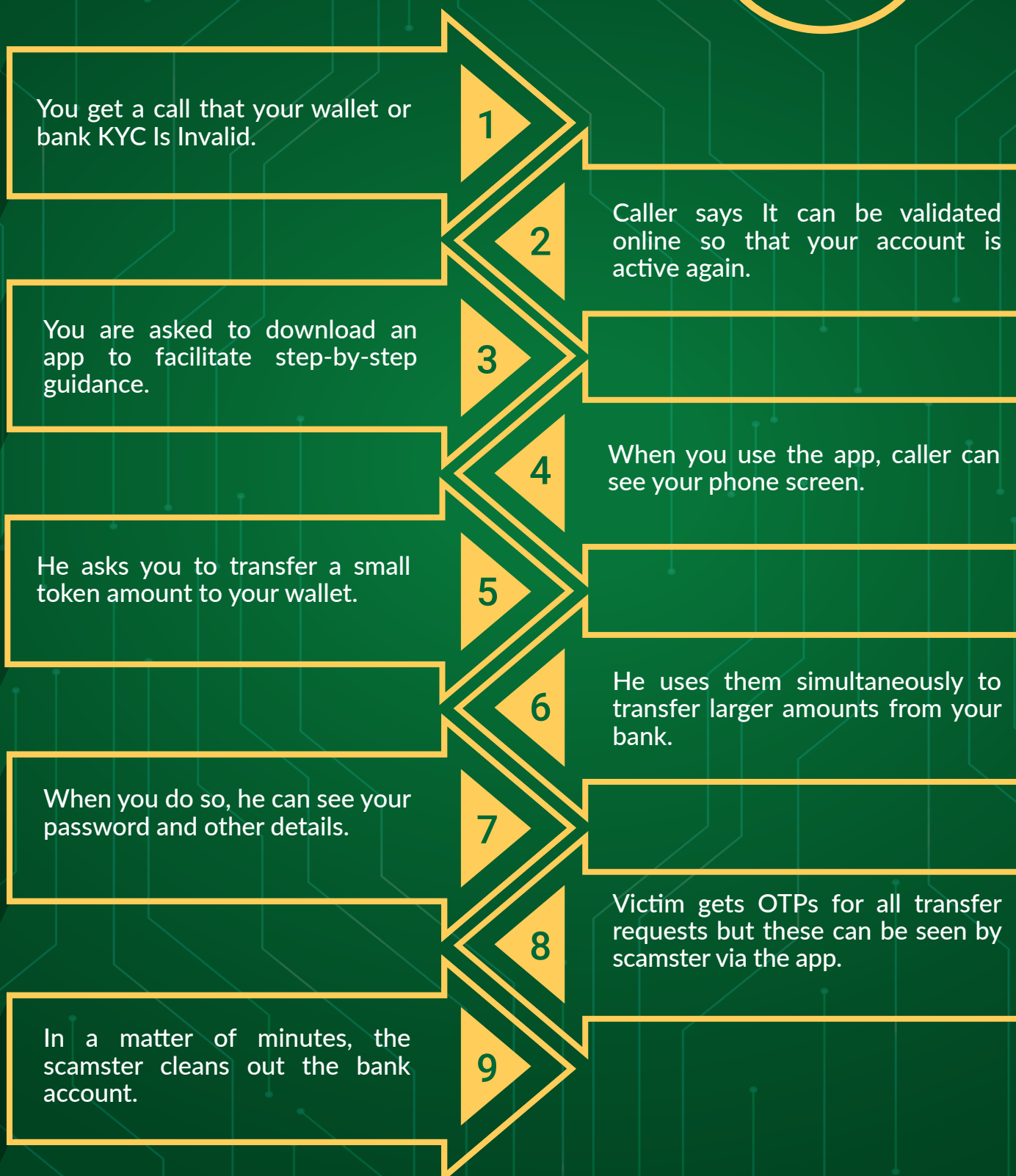


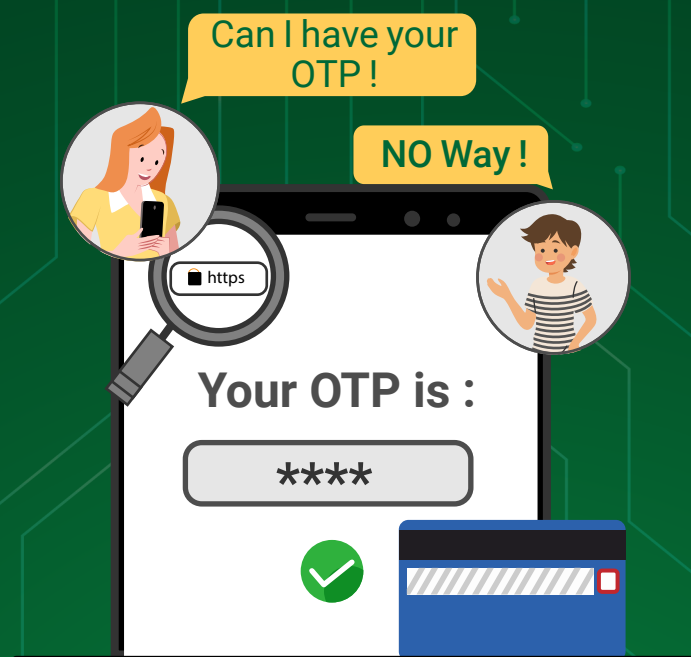
Never lose sight (and if possible, touch) of ATM card during the payment transactions.

Insist that your card is visible to you at all times.



HOW THE 'KYC' SCAM WORKS





GUARD THAT OTP

Your one-time password can be used to steal money from your bank account. Refrain from sharing it to stay out of trouble.



Never share your One Time Password (OTP).



Keep Changing Your ATM Pin frequently.



Never share your CVV.



Check for https:// and the Lock Icon for Secure Online Transaction.



Never save Credit / Debit - Card details on Ecommerce Websites.



THINK
BEFORE YOU
ENTER YOUR

PIN.

SAY NO TO

- Advance Payments.
- Sharing Personal Details, PIN Number, OTP, Account Number, etc.
- Transferring, Receiving Money while on Call.

Your PIN is NOT required when RECEIVING UPI Payments via

paytm



PhonePe

Pay

BEWARE: Payments through Online Platforms
are Robust but Susceptible to Fraud.

99% of Payments are Prone to
Phishing and Social Engineering Crimes.

HOW DEBIT CARD SKIMMING WORKS

Here are some of the ways thieves steal bank information from ATMs :

Fraudsters switch the entire device.



Fraudsters install a Skimmer.



Fraudsters install a new keypad.



Fraudsters install a camera.



How to protect yourself

- ATMs at banks may be safer than those at gas stations and stores.
- Jiggle the card as you withdraw it from the slot, it might loose a card skimmer.
- As you enter your PIN, cover the keypad with your other hand.
- Don't use an ATM or payment machine if it appears altered.
- If having trouble using an ATM, don't accept help from strangers.
- Check your bank statements regularly to see any suspicious activity.

WHAT IS SIM SWAP FRAUD?

STEP 1



Fraudsters gather customer's personal information through Phishing, Vishing, Smishing or any other means.

STEP 2



They then approach the mobile operator and get the SIM blocked. After this, they visit the mobile operator's retail outlet with the take ID proof posing as the Customer.

STEP 4

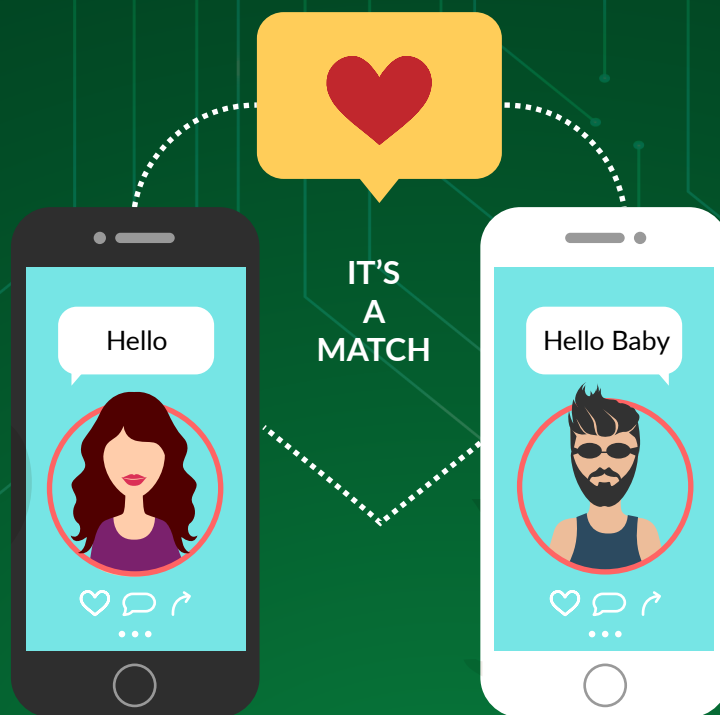


Fraudster then generates One Time Password (OTP) required to facilitate transactions, using the stolen banking information. This OTP is received on the new SIM held by the fraudster.

STEP 3



The mobile operator deactivates the genuine SIM card and issues a new one to the fraudster.



AVOID FALLING PREY TO ROMANCE FRAUD

- Do not indulge in online chatting, dating or get emotionally involved with people without verifying the truthfulness of clients.
- Never spend money or your details to online strangers/social media friends.
- Online follower asks to communicate outside the dating website/platform only after a few contacts or conversations.
- Do a www.tineye.com or Google Reverse Image Check of your fan to help determine if they really are who they say.

- No sharing of intimate pictures or videos online. Scammers are known to blackmail their targets using past shared pictures or videos of you that you don't want others to see.





PREVENT MATRIMONIAL FRAUDS

How to prevent yourself from being a victim
of matrimonial fraud :



- Do a thorough Profile Check.
- Always look for 'Verified' Profile Matches on Marriage Portal.
- Never give money to anyone.
- Never reveal your Portal Account Information.
- Stay Informed while meeting in person.
- Stay Informed while signing on any document.





BEWARE OF LOAN FRAUD

WARNING SIGNS

- No credit check required.
- Lender is not registered with the Government Legally.
- No Physical Address.
- Advance Payment.
- Offer Expired in a few days.

SAFETY TIPS

- Look for a secure Payment (<https://> URL with a Pad Lock Symbol).
- Never share OTP/PIN Numbers to the buyer or seller.
- Never do the Payment while you are on the call.
- Do not click and fill up any Short Links provided by the buyer or seller.
- Do not fill google form links provided by the buyer or seller.
- Do not Scan the QR Code.
- Never pay advance loans fees for any loans.
-





GUARD YOURSELF AGAINST LOTTERY FRAUD

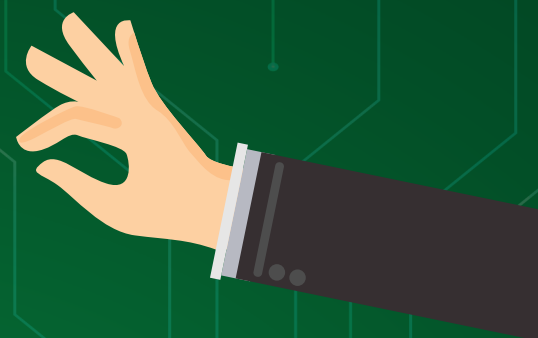
FEW FRAUDS

- Kaun Banega Karodpathi
- Scratch Card Gift
- RBI Lottery
- European Lottery

SAFETY TIPS

- Never Click on Short Links sent through e-mail/SMS.
- Click on Websites that start with https://.
- There is an Attachment that you were not expecting.
- Sender doesn't address you by name.
- No need to pay advances for winning a Lottery Prize.
- We cannot win money in a lottery or competition unless we have purchased or participated personally.
- Competitions and lotteries do not require you to pay advance fee to collect winnings.
- Never transfer funds to unknown person or entities in anticipation of high returns.





STAY SECURE FROM IDENTITY FRAUD

How to safeguard yourself being an identity victim :

- Do not open short links that have been sent via e-mail or SMS.
- Update Antivirus software both on PC and Mobile phone.
- Don't communicate about financial / password information on e-mail or SMS.
- Do not post D.O.B, Birthplace or Mailing Address on Social Media Platforms.
- Change Passwords periodically.
- Don't have same format of passwords for all applications.
- Periodically check the Bank Statements and Credit Card Statements.
- Mention the purpose when you give Xerox copy of the PAN Card/Aadhar Card.





CYBER SAFETY



How to stay safe online



Always keep your information & the passwords private



Be careful of what you are posting online



Always check your privacy settings



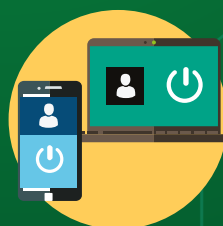
Shop safely on the trusted websites



Choose the strong passwords



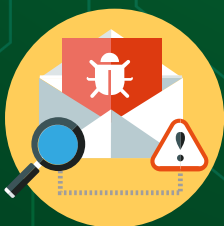
Protect all of your devices with an antivirus



Remember to log off



Check the website url



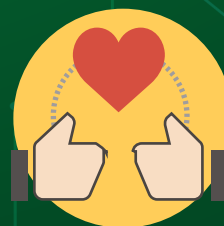
Always check the e-mails before you open them



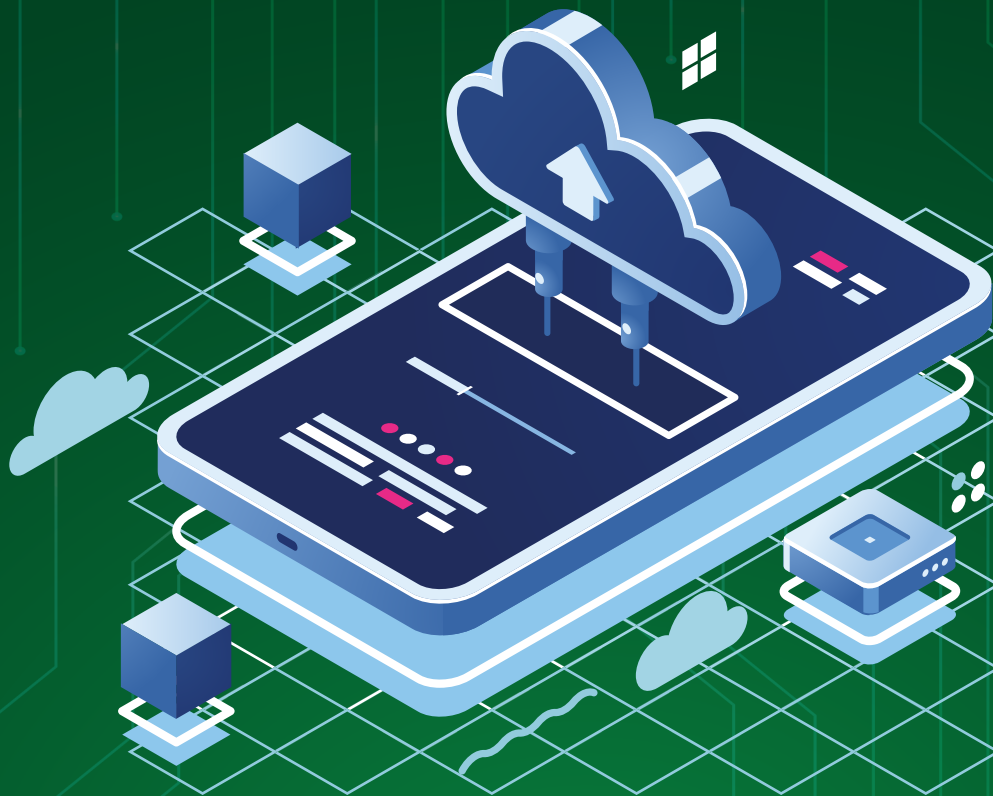
Avoid phishing & other scams



Always keep your children safe online



Respect yourself & others online



KEEPING YOUR SMARTPHONES & TABLETS SAFE !



Smartphones and Tablets need even more Protection than your 'Desktop' equipment.



Use 'Automatically Update' and keep your devices (and all installed apps) up to date.



Switch on the PIN / Password or the Protection / Fingerprint Recognition for mobile devices.



Don't connect to Public Wi-Fi, use 3G or 4G connections or use VPNs.



Configure that can be Tracked, Remotely wiped or Remotely locked.



Replace devices that are no longer supported by the manufacturers with up-to- date alternatives.



BACKING UP YOUR DATA

A better approach !



Take the regular backups of your important data and test that they can be restored.



Test the restoration of data at regular intervals to an alternate device.



Identify what needs to be backed up, i.e. documents, photos, e-mails, contacts and calendars.



Consider backing up to the cloud and you'll also be able to access it from anywhere.



Ensure that the device containing your backup is not permanently connected to any network.



PREVENTING MALWARE DAMAGE

Avoid unexpected pop-ups ,
strange e-mails & .exe extension files



Use Antivirus Software on all devices. Install only approved software.



Control all of the access to the removable media. Encourage to transfer files via e-mail or cloud storage instead.



Prevent from downloading third party apps from unknown sources.



Switch on your firewall to create a buffer zone between your network and the internet.



Patch all Software and Firmware by using the 'Automatic Update' option.



USING PASSWORDS

To protect your data !



Make sure all use encryption products that require a password to boot.



Enforce Password changes at Periodic Intervals.



Switch on the password / PIN protection or the fingerprint recognition for all devices.



Change manufacturers' default passwords on device.



Use Two Factor Authentication (2FA) for banking, e-mail & social media sites.



Provide secure storage and user can reset their own passwords easily.



Avoid using easily predictable passwords (i.e. Family, Pet, First Names, etc).



Use a Password Manager Tool 'Master Password' (that provides access to all other passwords)

CARRYMINATI'S YOUTUBE CHANNEL (CARRYISLIVE) GOT HACKED

ENABLE TWO - FACTOR AUTHENTICATION

If their accounts are hacked, yours can be easily hacked too



10 INTERNET SAFETY TIPS FOR KIDS

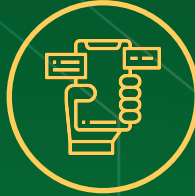


Digital citizenship and internet safety

Don't block all access to technology. Help your child learn to use tech safely and positively.



Take interest in your child's favourite applications or sites. Co-view or co-create at times.



Be the parent. You are in charge. Set boundaries and consider using the filtering software.



Create the family media agreement with tech free zones such as bedrooms, cars, and meals.



Always teach your child what personal informations they should never reveal online (YAPPY acronym).



Help your child learn to filter information online and also navigate fact from fiction.



Navigate digital dilemmas with your child. Avoid using devices as the rewards or punishments.



Balance the Green time and Screen time at home. Focus on the basic developmental needs.



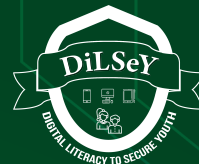
Don't support your child to sign up for sites with the age restrictions (e.g. 15+) if they are underage.



Learn more: Explore reliable resources for parents so you can educate yourself.



10 INTERNET SAFETY TIPS FOR KIDS



Digital citizenship and internet safety

Laws : Many sites and web tools are 13+. Most images and work online are protected by copyright.



Friends : Don't add or meet online friends without parent permission. Do not trust on everything friends tell you.



Reputation : Do not post anything you wouldn't want teachers, family, friends, and future employers to see.



Bullying : Tell someone if you think / see cyberbullying is happening to you or other people you know.



Manners : Be polite and respectful at all times. Treat others online how you'd like to be treated.



Talk : Tell your parents what you're doing online. Always ask a trusted adult if you're unsure of anything.



Privacy : Keep your personal info private : Your full name, address, phone number, your plans, password and your birthday.



Question : You can't believe everything you read and see online as there is a lot of incorrect and biased info.



Accounts : Choose some sensible email addresses and usernames and use strong passwords and don't share them with others.

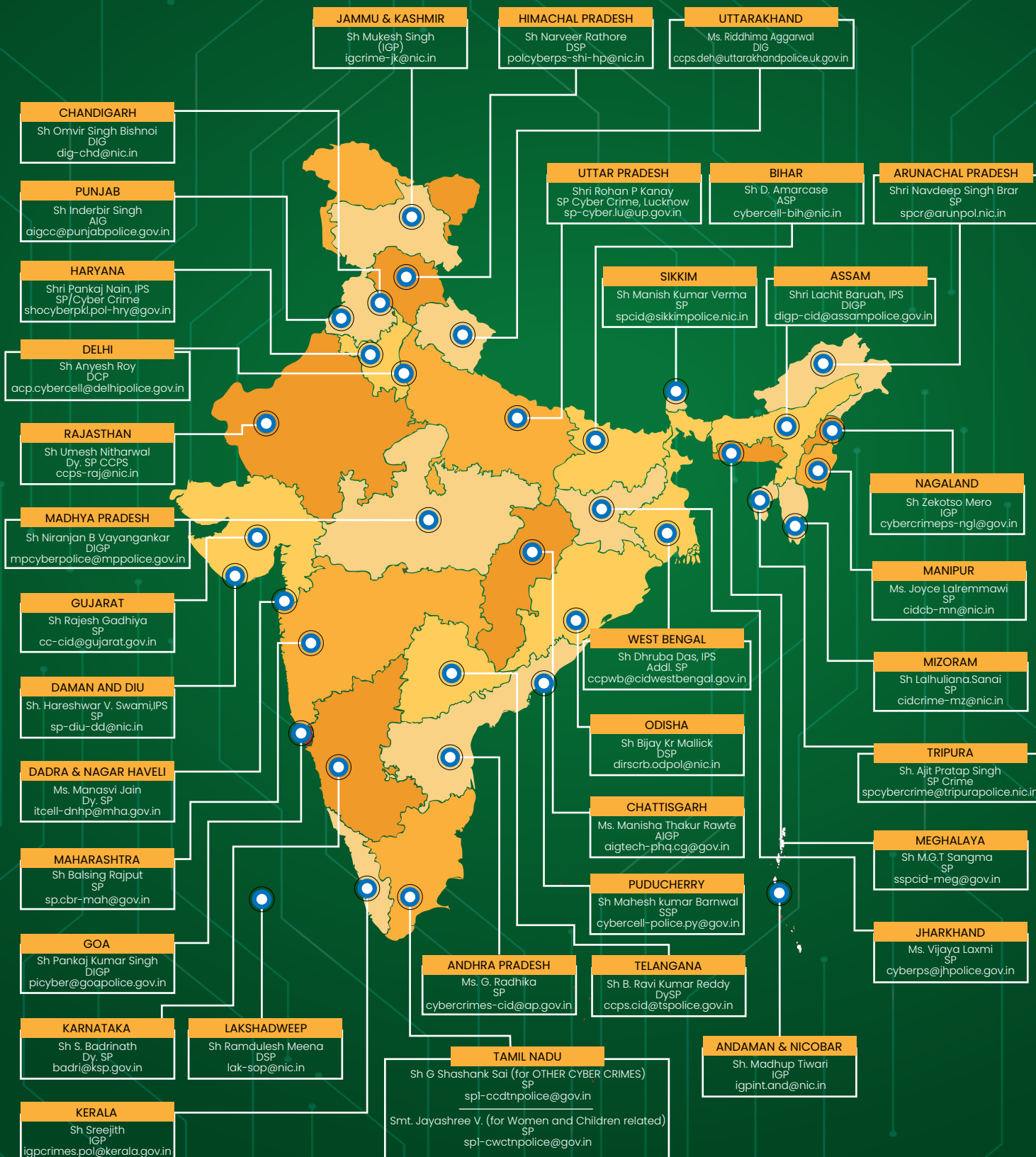


Unplug : Balance your screen time and green time. Get outdoors, move, play, and interact face to face.

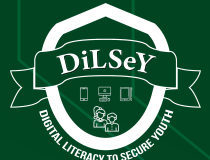


Nodal Cyber Cell Officers

Cyber Crime Reporting Portal
www.cybercrime.gov.in



Grievance Officers Cyber Cell



Cyber Crime Reporting Portal
www.cybercrime.gov.in

JAMMU & KASHMIR

Sh. B Srinivas
ADGP (0191-2582996)
adgpcidjk@jkpolice.gov.in

HIMACHAL PRADESH

Sh. Sandeep Dhawal
SP (0177-2627955)
sp-cybercr-hp@nic.in

UTTARAKHAND

Sh. Deepam Seth
IGP (0135-2712563)
dgc-police-ua@nic.in

CHANDIGARH

Ms. Nilambari Jagdale
SSP (0172-2760001)
pssput-chd@nic.in

PUNJAB

Sh. Hardial Singh Mann
DIGP (0172-2226258)
aigcc@punjabpolice.gov.in
shocc@punjabpolice.gov.in

HARYANA

Shri Desh Raj Singh, IPS
ADGP(Crime) (01733-253230)
adgp.crime@hry.nic.in

DELHI

Mr. Prem Nath
Addl.CP (011-20892633)
adlcp.cybertech@delhipolice.gov.in

RAJASTHAN

Sh. Abhijeet Singh
SP SOG (0141-2309547)
singh.kadian@ips.gov.in

MADHYA PRADESH

Smt. Aruna Mohan Rao
SPL DGP (0755-2770248)
spl.dgp-cybercell@mppolice.gov.in

GUJARAT

Dr. Shamsher Singh
ADGP (079-23250798)
cc-cid@gujarat.gov.in

DAMAN AND DIU

Sh. Vikramjit Singh IPS
SP (0260-2250942)
sp-dmn-dd@nic.in

DADRA & NAGAR HAVELI

Sh. Sharad Bhaskar
SP (0260-2643022)
sp-sil-dnh@nic.in

MAHARASHTRA

Sh. Brijesh Singh
SPL IGP / DGP (022-22160080)
ig.cbr-mah@gov.in

GOA

Sh. Paramaditya
DIGP (0832-2420883)
digpgoa@goapolice.gov.in

KARNATAKA

Sh. T D Pawar
DIGP (080-22251817)
digadmincod@ksp.gov.in

LAKSHADWEEP

Sh. Shibesh Singh
SSP (04896-262258)
lak-sop@nic.in

KERALA

Sh. Dr. Shaik Darvesh
ADGP (0471-2722215)
adgpcrimes.pol@kerala.gov.in

UTTAR PRADESH

Dr. Kalluri SP Kumar
ADG(Crime) (0522-2208598)
ccpsstf.gb-up@gov.in

BIHAR

Sh. Shiv Kumar Jha
DIGP (0612-2238098)
dgp-bih@nic.in

ARUNACHAL PRADESH

Sh. Take Ringu
DIGP (0360-2215518)
sit@arunpol.nic.in

SIKKIM

Sh. Sonam Detchu Bhutia
DySP (03592-204297)
spcid@sikkimpolice.nic.in

ASSAM

Sh. Surendra kumar
IGP (0361-2524494)
igp-cid@assampolice.gov.in

NAGALAND

Sh. Renchamo P. Kikon
ADGP (0370-2223897)
renchamo.p@gov.in

MANIPUR

Sh. Themthing Ngashangva
DIGP (0385-2450573)
themthing.ng@gov.in

MIZORAM

Sh. Balaji Srivastava IPS
DGP (0389-2334682)
palmizo@rediffmail.com

TRIPURA

Shri Subrata Chakraborty
AIGP/Crime (0381-232174)
aigcrime@tripurapolice.nic.in

MEGHALAYA

Sh. F G Kharshiling
DIGP (364-2550141)
fg.kharshiling@ips.gov.in

JHARKHAND

Sh. Ranjit Prasad
IGP (0651-2490046)
ig-orgcid@jhpolic.gov.in

WEST BENGAL

Sh. Ashok Kumar Prasad
IGP (033-24791830)
ig2@cidwestbengal.gov.in

ODISHA

Sh. Madkar Sandeep Sampat
SP (0671-2306071)
splcidcb.orpol@nic.in

CHATTISGARH

Sh. R K Vij
SPL DGP (0771-2511623)
vijrk@gov.in

PUDUCHERRY

Sh. Dr. VJ Chandran
DIGP (0413-2231386)
dig.pon@nic.in

ANDHRA PRADESH

Shri M.Sunil Kumar Naik IPS
DIGP (0863-2340152)
cybercrimes-cid@ap.gov.in

TELANGANA

Smt. Swathi Lakra IPS
ADGP (040-23147604)
igp_wpc@cid.tspolice.gov.in

TAMIL NADU

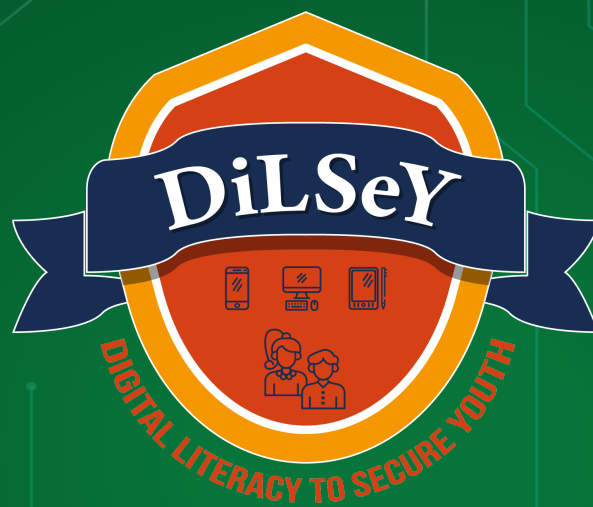
Shri Shankar K. (FOR OTHER CYBER CRIMES)
IGP (044-28447712)
spl-ccatnpolice@gov.in
Shri Shankar K. (FOR WOMEN & CHILDREN RELATED)
IGP (044-28447620)
spl-cwatnpolice@gov.in

ANDAMAN & NICOBAR

Sh. Deependra Pathak
DGP (03192-230216)
dgp.and@nic.in

<https://cyberabadsecuritycouncil.org/>

Notes



<https://cyberabadsecuritycouncil.org/>



<http://www.cyberabadpolice.gov.in/>

Supported by:



www.endnowfoundation.org