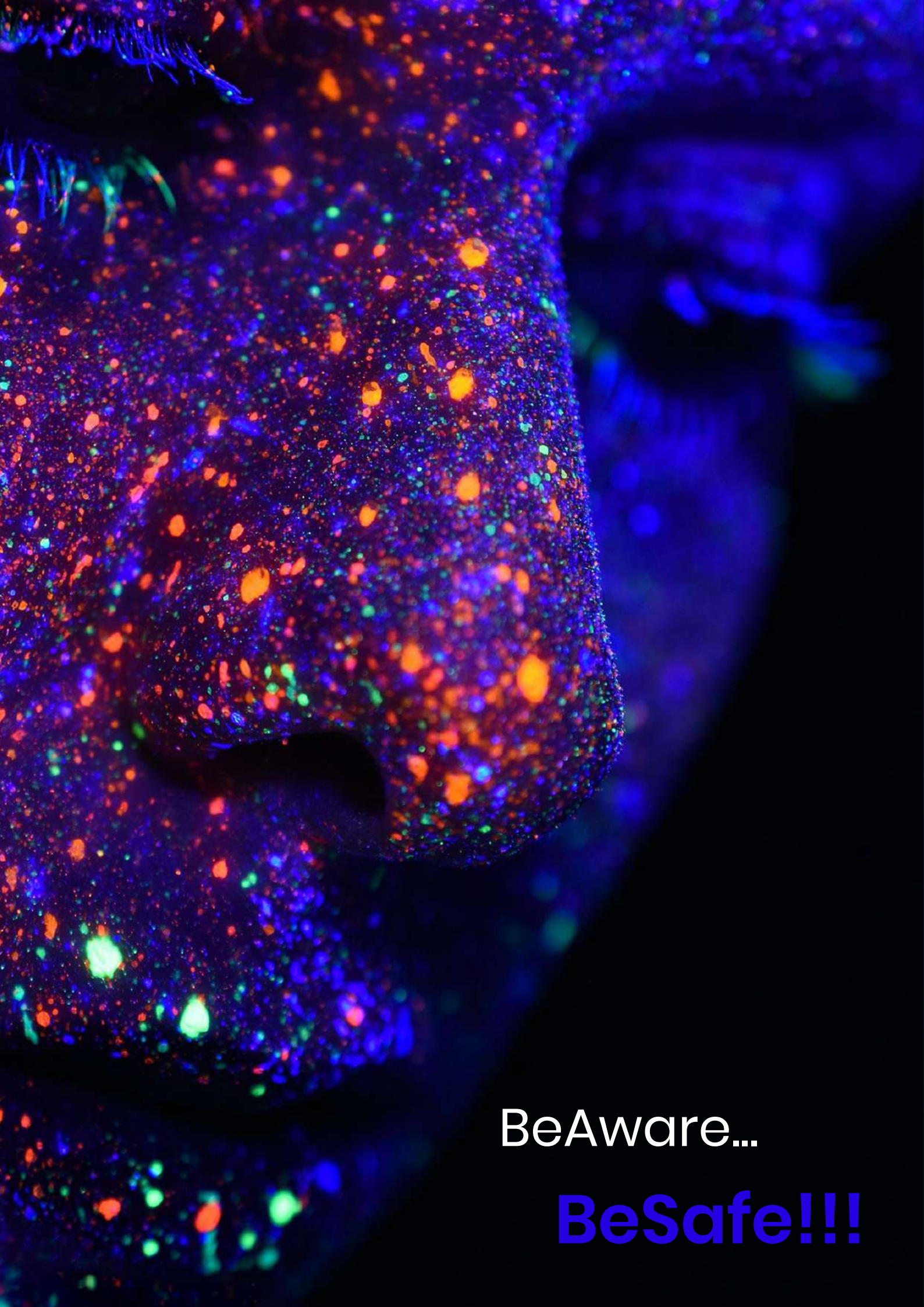
SAFE IN SPACE

An Awareness Handbook

KERALA POLICE


BeAware...
BeSafe!!!

FOREWORD

LOKNATH BEHERA IPS
DGP & STATE POLICE CHIEF , KERALA

Cyber security is a global phenomenon representing a complex socio technical challenge not only for Governments, but requiring the involvement of all citizens. The crux of the problem of cyber security lies in lack of public awareness and education. Almost everybody has heard of cyber security, however, the urgency and behaviour of persons do not reflect the high level of awareness. The role of every individual, every section of the Society, the public and private Sector, Government etc is crucial to ensure that our cyber resources are safe.

With this objective in mind, Kerala Police is coming forth with this booklet titled " SAFE IN 'C' SPACE" which is a booklet on the do's and don'ts on cyber security for all sections of the society for handling the current cyber threats and challenges. I am sure that the book would be immensely beneficial to one and all in ensuring that our cyber space remains safe and secure.

MESSAGE

MANOJ ABRAHAM IPS
ADGP & NODAL OFFICER KERALA POLICE CYBERDOME

The Internet is all too often considered as a safe environment for sharing information, transactions and controlling the physical world, but this notion is far from true. Cyber Crime is now a global phenomenon which hampers not only the security of the State, but also is a threat to the individual on different fronts. All sections of the society are under threats of cyber attacks, particularly, Women and children, who are soft targets. The proliferation of social media handles, cheap and fast internet, the increasing dependence on onlinte transactions, online shopping, online education & conferences have made this problem more acute. This problem can be tackled to a great extent at the user level, with basic awareness on the do's and don'ts of cyber security. Kerala Police is proud to bring forth this awareness booklet which is current to the latest threats in cyber security. I congratulate Team Cyberdome & its volunteer community for coming out with this wonderful booklet for online safety would keep oneself protected from various crimes and in helping us to build a protective cocoon online. For Awareness is the key and everyone must engage in responsible internet surfing to secure our digital resources.

STAY SAFE ONLINE! AND PARTNER US TO MAKE A SAFE CYBER WORLD

TABLE OF CONTENTS

FINANCIAL FRAUDS

- LOTTERY FRAUD/FAKE PRIZE FRAUDS
- CVV/OTP FRAUDS
- UPI FRAUDS
- FRAUD USING ONLINE MARKETPLACES
- FRAUD USING REMOTE ACCESSING APPS
- SIM SWAPPING
- GOOGLE BUSINESS
- FRAUDS USING MATRIMONIAL SITES
- PHISHING/VISHING/SMISHING PAYMENT FRAUD
- BUSINESS E-MAIL COMPROMISE

ONLINE JOB FRAUDS

- USING FAKE WEBSITES AND ASKING TO PAY MONEY IN ADVANCE
- CAPTCHA ENTRY JOB SCAM
- FORM FILLING SCAM FOLLOWED BY LEGAL THREAT

SOCIAL MEDIA PLATFORMS

- CYBER STALKING
- CYBER BULLYING
- SEXTORTION
- ACCOUNT TAKEOVER

OTHER CYBER CRIMES

- RANSOMWARE
- COMPUTER, MOBILE OR DEVICE HACKING
- MALWARE / RAT/MALICIOUS APPS
- CALL/EMAIL SPOOFING
- IDENTITY THEFT SOCIAL ENGINEERING
- KEY LOGGERS
- PUBLIC WI-FI AND HOTSPOTS
- SERVICE CENTERS
- ATTACKS ON IOT

ONLINE CODE OF CONDUCT
TO KEEP YOU SAFE

GENERAL TIPS TO PARENTS

ONLINE SAFETY RULES
FOR KIDS

WHERE TO REPORT A
CYBER CRIME

FINANCIAL FRAUDS

01 / LOTTERY FRAUD / FAKE PRIZE FRAUDS

The fraud in which, victims receive phone calls, emails, SMS's, WhatsApp messages, or letters etc. telling them that they have won a lottery or an expensive gift. Victims are subsequently requested to deposit money in a bank account as processing fee or tax.

Modus Operandi

1. Victims receive emails from fraudster informing that they have won a lottery worth 50 Crores.

2. Victim replies to fraudster on email to complete formalities and get the money.

3. Victim is asked to deposit money for processing fees, Customs clearance, Income Tax authorisation etc.

4. Thinking about 50 Crores, victim deposited 20 lakhs in 10 installments.

5. Victim lost 20 lakhs

TIPS

1. Never respond to unsolicited offers received through emails, messages, phone calls, and other social media.

2. Never transfer money to anyone in the name of a lottery or gifts.

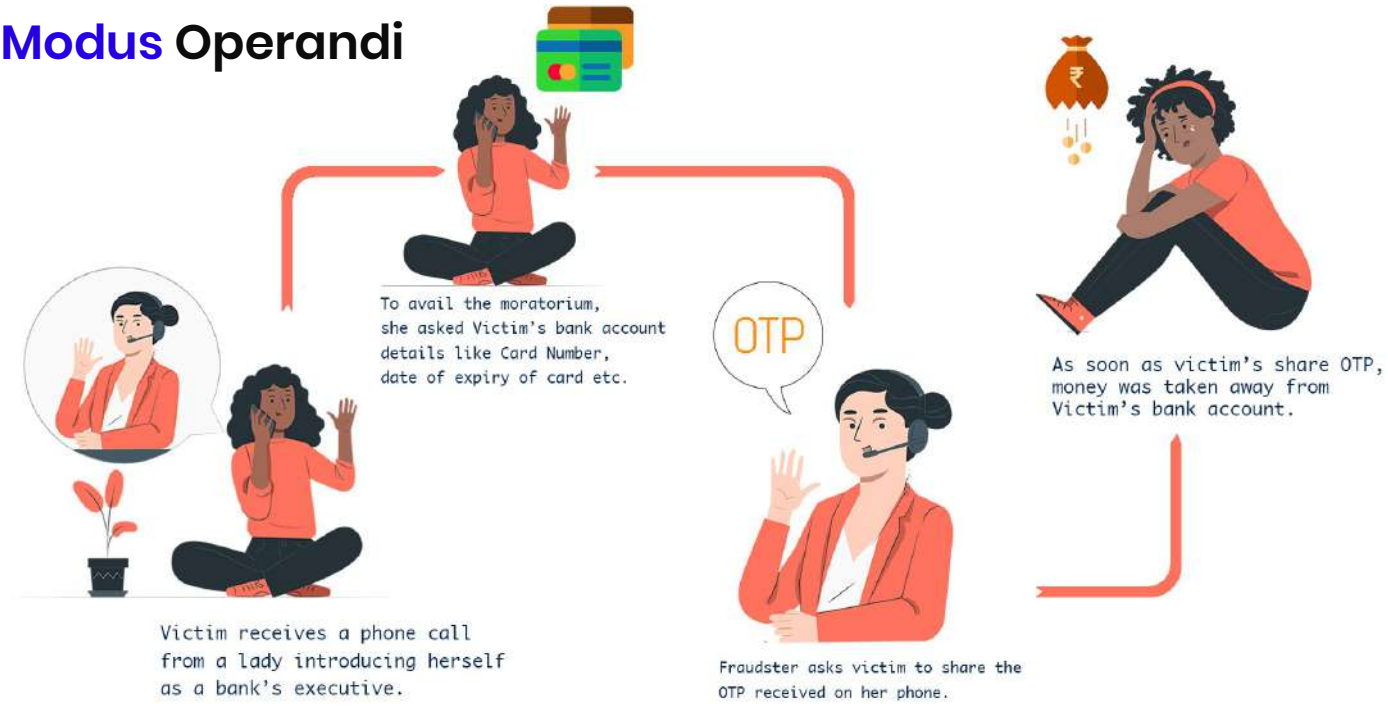
02 / CVV / OTP FRAUDS

One-time password (OTP), a two-factor authentication, is effective deterrent against cyber criminals trying to steal money from victim's bank account through online transaction. This OTP is valid for one transaction only and has time limit. In OTP Fraud, cyber criminals dupe bank customers into revealing OTP and siphon off money from bank account online.

Common pretext used by Fraudster to Cheat/Dupe Victims are:

1. Renewing debit or credit cards
2. Updating KYC
3. Reward points or cashbacks

Modus Operandi



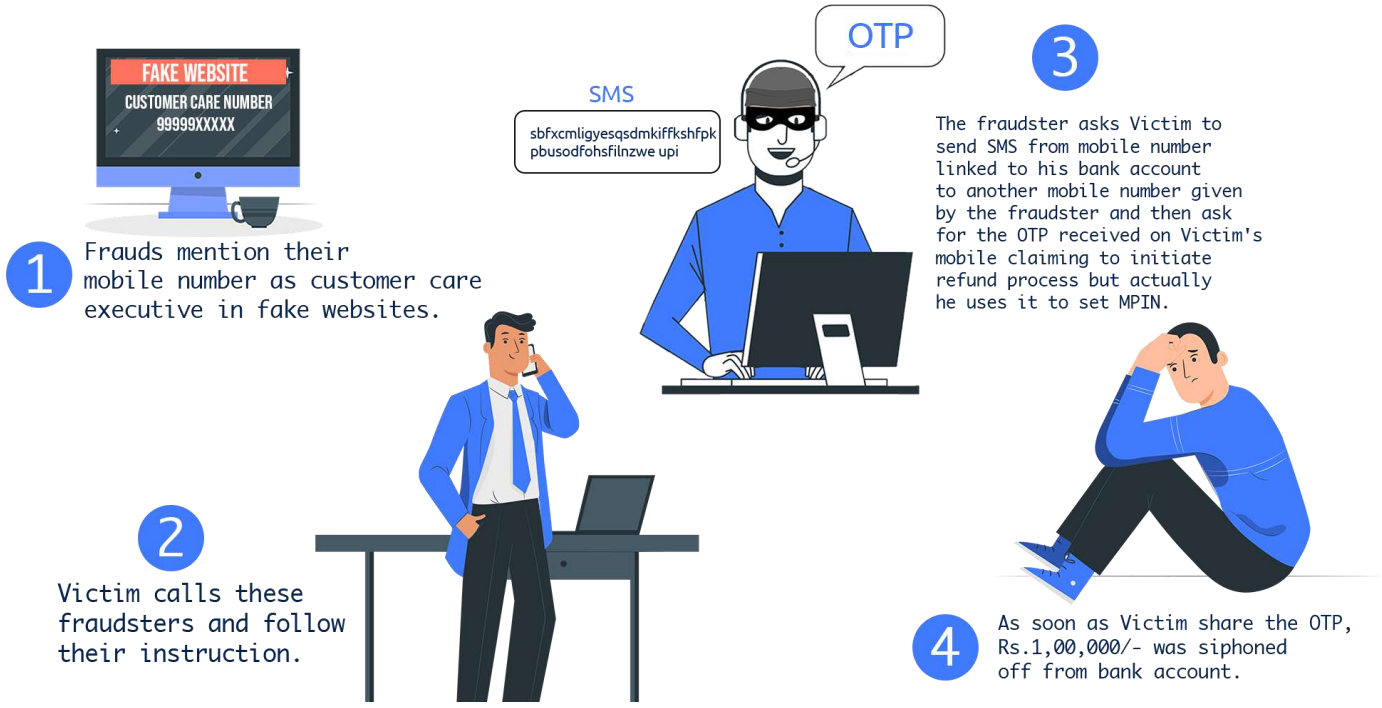
TIPS

1. Never share OTP, CVV, MPIN, Card Number to anyone.
2. Banks will never ask you for your banking credentials over phone or via email communication.

03 / UPI FRAUDS

In UPI Fraud, UPI mobile app installed on Fraudster's mobile get linked to victim's bank account when victim sends some code to another number. Once the victims account gets linked with the frauds UPI app, money will be siphoned off from the victims account.

Modus Operandi



TIPS

1. DO NOT Share any financial credentials.
2. Never forward any SMS from mobile number linked your bank account to another mobile number.

04 / FRAUD USING ONLINE MARKETPLACES

(OLX, Quikr etc.)

Classified ads are one of the prominent sources for different kind of scammers to find potential victims where frauds pose both as buyers and sellers. In these type of fraud, scammers posing as sellers, ask for pre-payment for delivery of items and DOES NOT deliver it.

While posing as buyers, scammers send Money request of UPI Mobile App with instruction to type in MPIN to receive the money. As soon as victim, enters MPIN amount is transferred to fraudster's account.

Modus Operandi

1. Victim upload online advertisement to sell his motorbike.

2. Immediately, he receives a call from fraudster claiming to be a CISF personnel deployed on airport duty and agrees to the price.

3. To finalize the deal, fraudster offered to pay Rs. 10,000/- as token advance. Fraud offers to pay the amount through mobile wallet and asked to share his Googlepay UPI ID.

4. To gain trust, fraud sent a copy of photo identity cards - PAN Card, Aadhar Card, Official ID and few photos in uniform.

5. Fraudster sends pay request for Rs. 10,000/- with subject "Please accept the money by typing your MPIN".

6. Victim types-in the MPIN and Rs. 10,000/- is debited from his bank account.

TIPS

1. MPIN is not required to receive money.

05 / FRAUD USING REMOTE ACCESSING APPS (TEAMVIEWER, ANYDESK)

Fraudsters trick the victim to install app to allow remote access on the device. The fraudster gain access to all OTP based transactions and siphons off all the fund.

Remote Accessing Mobile App: AnyDesk, Teamviewer.

Modus Operandi

1. Victim wants to get a refund on a product, ordered from an e-commerce website and searches for the customer care number from internet.

2. Victim gets mobile number from a website hosted by fraudsters and calls that mobile number and follows all the instructions given to him.

3. Fraudsters ask Victim to download the remote accessing mobile app and ask him to share the access code for initiating the refund process.

4. Once the access code is shared, the Victim's mobile will be remotely accessed and money siphoned off from the bank account.

TIPS

1. Do not install any remote accessing app as per direction of any unknown entities.

06 / SIM SWAPPING

Your Mobile phone, through your mobile number, could provide a way for cybercriminals to access your financial accounts. Such fraud is known as SIM swapping, and it can be used to take over your financial accounts. SIM swapping relies on phone-based authentication. In a successful SIM swap scam, cybercriminals could hijack your cell phone number and use it to gain access to your sensitive personal data and accounts.

Modus Operandi

1) Fraudsters obtain customer personal data through phishing or Social engineering to get access to subscriber account.
2) Fraudsters creates a fake ID based on existent one
3) Fraudsters contact the mobile operator under the pretexts such as having lost the phone.
4) After customer verification, mobile operator deactivates the old SIM card in customer possession and issue a new SIM card to the fraudster.
5) With the new SIM and the same mobile number, fraudsters receive authentication codes, for the services such as banking or social media accounts.
6) With the account takeover process completed fraudsters can now operate the genuine customer account and initiate financial transactions or publishing fake news on social media accounts.

TIPS

1. Beware of phishing emails and other ways attackers may try to access your personal data to help them convince your bank or cell phone carrier that they are you.
2. Boost your cellphone's account security with a unique, strong password and strong questions-and-answers.
3. If your phone carrier allows you to set a separate passcode or PIN for your communications, consider doing it.
4. Don't build your security and identity authentication solely around your phone number.

07 / GOOGLE BUSINESS

Fraudsters have created hundreds of fake websites having “business.site” as part of domain name of different e-commerce companies and they mention their mobile numbers as customer support. These sites are created using Google My Business facility and such websites are ranked higher in Google Search. Trusting the fraudsters to be customer care executive, people call them, follow their instruction and lose money.

Modus Operandi

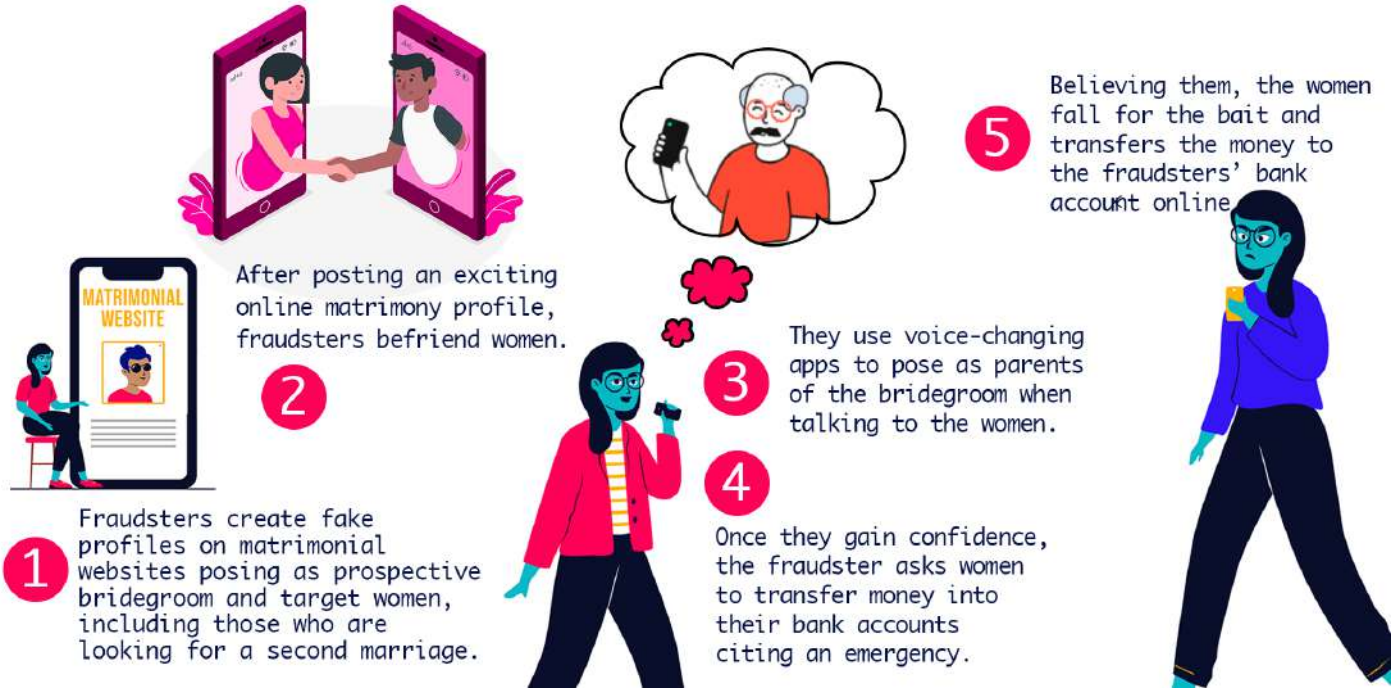
TIPS

1. Toll free/customer care numbers of banks will be given on back/flip side of debit/ credit card, Bank passbooks etc.
2. Google results should not always be treated as verified information on searches.
3. Always search for customer care number from the official website of the entity.

08 / FRAUDS USING MATRIMONIAL SITES

Fraudsters befriend men/women after creating an impressive online profile on a matrimonial site, posing as prospective bride/bridegroom. After gaining confidence, the fraudsters ask to transfer money into their bank accounts stating various emergencies. Once the money has been transferred the fraudster cuts all the contacts with the victim and disappear without a trace.

Modus Operandi



TIPS

1. Starts enquiring about your properties and income and starts demanding money.
2. They are not willing to show their face reluctant to come on video chat.
3. Reluctant to meet in person.
4. They express 'love' quickly even before fully understanding each other.
5. Voice inconsistent or confusing when asked for his or her personal details.

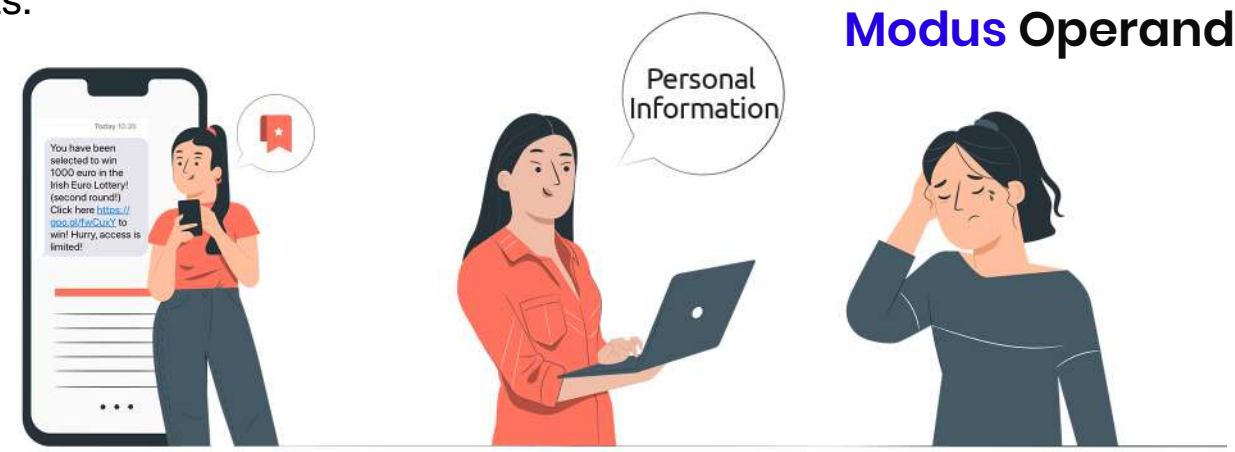
09 / PHISHING / VISHING / SMISHING

Phishing: It is one of the well-known forms of social engineering technique of sending a link via email or text or embedding a link on a website or downloads malware onto the user's device.

Vishing (or voice phishing) in which Scammers will call targets from a phone (or spoofed) phone number, typically claiming to be representatives of banks or financial organizations.

Smishing: It is SMS phishing attack in which attacker ask target to download an app or open a link. Individuals are more often the victims of smishing exploits.

Modus Operandi



1. Victim receives an email/ SMS/IM message informing they have won a Lottery or an expensive prize.
2. Victim shares all the required personal information, including her bank account Number, IFSC Code, telephone number, and all the other details that were asked in the message.
3. With the collected details the fraudster lures money from the victims account using various means.

TIPS

1. Do not trust random messages or those containing obvious mistakes.
2. Always check the link received via any means before clicking. Hover over it to preview the URL if possible, and look carefully for misspelling or other irregularities.
3. If you have shared financial details, call the bank or the credit card company immediately to stop or deactivate any payments.

10 / PAYMENT FRAUD USING FAKE E-COMMERCE SITES

In This type of fraud a cybercriminal came up with a fake merchant website which looks similar to that of a legitimate business. The culprit then goes ahead and places fake offers on expensive/branded products on a very hard -to-resist prices and popularize the site through social media Ads. Victim clicks on one such link to buy products, with payment being done through UPI or online banking and will gets cheated.

Modus Operandi

TIPS

1. Pay attention to the address bar and check the domain name.
2. Look for customer feedback on the internet, research about the website.
3. Don't be fooled by logos, it can be replicated easily.
4. Fake websites usually have UPI payment facility only and don't have CoD facility.

11 / BUSINESS E-MAIL COMPROMISE

Business e-mail compromise (BEC) is a sophisticated scam targeting businesses that often work with foreign suppliers and/or businesses and regularly perform online money transfers. The Email Account Compromise (EAC) is the variation of BEC that targets individuals who regularly perform online transactions with foreign entities/companies. It should be noted while most BEC and EAC victims reported using wire transfers as their regular method of transferring business funds. Both scams typically involve one or more fraudsters, who compromise legitimate business email accounts through social engineering or computer intrusion techniques to conduct unauthorised transfers of funds.

Modus Operandi

TIPS

1. Enable two-factor authentication on all business and personal email accounts.
2. Learn how to spot phishing schemes and protect yourself from them.
3. Use SmartScreen to identify suspicious websites.
4. Consider blocking email auto-forwarding to make it harder for cybercriminals to steal your information.

ONLINE JOB FRAUDS

01 / USING FAKE WEBSITES AND ASKING TO PAY MONEY IN ADVANCE

Cyber criminals advertise fake job offers using various online platforms. Victim, in search of a job, goes through these offers and contacts the cybercriminal. Upon contacting cyber criminals, victim is asked to pay registration fee or make an advance payment (which they claim is refundable) to avail their services for getting a job. Victim transfers the money and follows the guidelines of the fraudster and falls prey to the cyber-crime

Modus Operandi

02 / CAPTCHA ENTRY JOB SCAM

“CAPTCHA” is a mechanism that prevents misuse of online services like webmail or new account creation like Gmail and Yahoo-Mail. The page, which uses CAPTCHA, ask the user to enter a series of characters/letters from an image into a box. The page only process user’s request if all the typed characters/letters are correct.

Scammers hire freelancers for data entry work without payment and threaten them of legal action by creating fake agreement document in PDF with image court fee stamp, victim’s photo and signature.

Modus Operandi

1

The victims register their name for data entry job at websites. The details of job aspirants are taken from these job portals by the fraudsters and calls them.

2

They offer them to fill 10,000 captchas in 10 days with 90% accuracy failing to which the person has to pay the registration fees.

3

Frauds will send the link of application to work. The app will crash most of the time and it will not work.

4

When victim come to know that the company is a fraud company and refuse to work, they are threatened with legal notice and asked to pay 5,000-10,000/-.

03 / FORM FILLING SCAM FOLLOWED BY LEGAL THREAT

Modus Operandi

1) Victims come in contact with these fraudsters when they look for “work from home” job.
2) Victim will be offered to fill form in package.
3) Then frauds will deactivate the working account and ask to pay 4500 to activate the account and 7000 for not completing the work.
4) Fraudsters will send victim a statement of non-accuracy for your work and demand reimbursement.
5) Fraudster will create an agreement in PDF using a photo of court fee stamp, victim’s photo and signature mentioning it as formality, to be used later to threaten the victim.
6) When Victim realize the trap and refuse to work. Victim receive phone call introducing himself of advocate threating legal action at court away from home.
7) Fraud will save their name as Advocate in True Caller
8) Fraudster will threaten the Victim with legal action based on the fake digital agreement created using their photo and signature.

TIPS

1. Do your research. Contact the prospective employer directly to verify whether the listed position is available.
2. It's a fake job call if you are asked to disclose your date of birth, social security number or any other personal details.
3. Never pay in advance.
4. No legitimate company asks for money in the name of bond or security deposits in advance.
5. Submit your application through a registered website only.
6. Your Photo, Signature, Identity documents like Aadhar card, PAN Card, License can be misused by fraudsters for illegal activities.

SOCIAL MEDIA
PLATFORMS

01 / CYBER STALKING

Cyber stalking is a crime in which the stalker targets the victim with threatening/abusive messages and/or follows them/their activities in the real world. Cyber stalkers usually use digital platforms like email, instant messages, phone calls, and other communication modes to stalk you. Cyber stalking can be a sexual harassment, inappropriate contact or an unwelcome attention in your life and your family's activities.

Modus Operandi

1 Victim uses Location tagging/check in feature of social media and makes public posts on his/her online calendars or itineraries.

3 Stalker uses the information and makes advantage of favourable opportunity to intimidate/molest/rob the victim.

2 Stalker keeps a watch on the posts of the victim and will know about the victims itineraries.

TIPS

1 Be careful about allowing physical access to your computer and other web-enabled devices like smartphones.

2 Delete or make private any online calendars or itineraries — even on your social network — where you list events you plan to attend.

3 Use the privacy settings in all your online accounts to limit your personal information getting shared with those outside your trusted circle.

4 If you post photos online via social networks or other methods, be sure to turn off the location services and metadata in the photo.

5 Use a security software program installed onto your computer Security software could allow you to detect spyware on your device and decrease your chances of being cyberstalked.

6 If you break up with someone that you were in a relationship with, be sure to change all of your online passwords.

7 Restrict unauthorised access to your profile.

02 / CYBER BULLYING

Cyber bullying is sharing personal or private information about someone else with an intention to cause embarrassment or humiliation, over digital communication, such as e-mail, instant messaging (IM), messages posted on a website or a discussion group. It includes sending, posting, or sharing negative, harmful, false, or abusive content about other persons over social media or other digital platforms.

Modus Operandi

1 Cyber bullies collect the personal photographs and details of the victim from various social media sites.

2 Creates a fake account either in the name of the victim or a random name

3 Post several memes and videos making fun of the victim, make false, fake, private, embarrassing information or pictures, which goes viral.

TIPS

1. Understand exactly what it is, how and where it occurs, and talk with you are friends, family about what they are seeing and experiencing.
2. Protect your password: Safeguard your password and all private information.
3. Pause before you post: Don't post anything that can compromise your reputation.
4. Set up privacy controls: Restrict who can see your online profiles to only trusted friends.
5. Never open messages from people you don't know.
6. Don't be a cyberbully.
7. Log out of your accounts on public computers.

03 / SEXTORTION

Sextortion is extorting money or sexual favours from people by threatening to reveal evidence of their sexual activity.

Modus Operandi

TIPS

1. Don't get too much private with strangers.
2. Do not give them any money or send any more pictures of yourself. It will only result in more demands for payment.
3. Notify the relevant social media platform.
4. Stop all contact with the blackmailer.

04 / ACCOUNT TAKEOVER

The genuine account of a person when accessed through illicit means and gained control of the same, by another person, for the purpose of committing fraud is called Account takeover. We have seen a rapid increase in segments such as social media, e-commerce in recent years.

Modus Operandi

1 Attacker gathers publically available information like date of birth, phone number, etc. about the user from sources such as social media sites.

2 Using the information gathered, targets the user's social media, e-mail accounts.

3 Once the access is gained, the attacker changes all the details like recovery email, phone number, etc. from the profile so that the user can't get back his account.

TIPS

1. Never use personal information such as phone number, date of birth as passwords.
2. Change passwords periodically.
3. Never share personal information publicly.
4. Use Two Factor Authentication to the accounts.

OTHER CYBER CRIMES

01 / RANSOMWARE

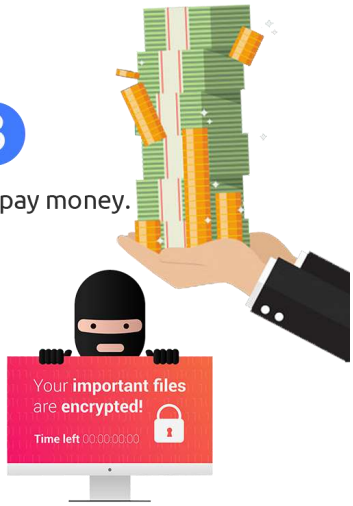
Ransomware is as vicious malware that locks users out of their devices or blocks access to files until a sum of money or ransom is paid. Ransomware attacks cause downtime, data loss, possible intellectual property theft, and in certain industries an attack is considered a data breach.

Modus Operandi

1 Victim gets his device infected via an email with an attachment or a link to a software download, visiting a compromised website, by installing a free version of a piece of software such as "cracked" versions of expensive games or software or by RDP exploitation.

2 The criminal asks victim to pay ransom to get their data decrypted.

3 The victims pay money.



4 Usually even after paying the ransom, the decryption key will not be provided.

TIPS

1 Use Strong Password for Social media accounts, emails an PCs.

2 Never click on unverified links.

3 Do not open emails from unknown sources containing suspicious attachment or phishing links.

4 Only download from sites you trust.

5 Keep your antivirus up-to-date and windows firewall turned on and properly configured.

6 Back up your most important files on a regular basis.

7 Keep the important data on a separate hard disk.

8 Have proper spam filters enabled in your e-mail account.

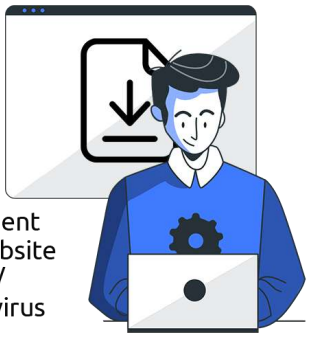
02 / COMPUTER, MOBILE OR DEVICE HACKING

Hacking is the unauthorised access to or control over computer network or digital devices for some illicit purpose like data deletion, data loss or stealing of sensitive data such as financial information or company/personal secrets. Some of the common hacking techniques used by cyber criminals are Social Engineering & Phishing, Malware-Injecting to Devices or Distributed Denial-of -Service (DDoS) attack.

Modus Operandi

1 Hacker send malicious attachments to the victim hidden in the form of attractive advertisements

3 No antivirus or security features enabled in the victims device.



2 Victim downloads the attachment or apps from an un-trusted website after which his / her computer/ device gets infected with the virus

4 Hacker gets the malicious code injected into Victim's system and gets full control of the victims device.

5 Hacker now has access to victims personal photos, videos, SMS, camera etc.

TIPS

1 Use a firewall/ antivirus software.

2 Use complex passwords which is harder for a hacker to invade your device.

3 Never install applications from untrusted sources.

4 Keep your OS, Apps and Browser up-to-date; updates include security fixes that prevent accessing and exploiting of your data.

5 Ignore spam email messages from unknown parties.

03 / MALWARE / RAT / MALICIOUS APPS

Malware, or malicious software, is any program or file that is harmful to a computer user. Types of malware can include computer viruses, worms, Trojan horses and spyware. These applications may have viruses which pass sensitive information or give control of your phone/device to some outside agent, who gets access to your contacts, passwords, financial data etc.

RAT- A Remote Access Trojan (RAT) is a type of malware that allows covert surveillance, a backdoor for administrative control and unfettered and unauthorised remote access to a victim's machine or mobile.

Affected through:

1. Email attachments
2. Malicious URLs
3. Remote desktop protocol
4. Malvertising
5. Drive-by downloads
6. Network propagation
7. Pirated software
8. USB drives and portable computers

Modus Operandi

1) Victim, downloads the mobile/desktop application from untrusted sources or through a link he/she receives through messaging apps/SMS.
2) Victim installs the app ignoring security warnings and/or grants unnecessary permissions to the application.
3) Cyber criminals gets a remote connection via the malicious app and can access the victim's device.
4) Cyber criminals gets access to the victim's messages, cameras, contacts, photos etc. and can be used for malicious activities.

TIPS

1. Do not open suspicious and irrelevant emails, especially those received from unknown/ suspect senders.
2. Block the installation of applications from unknown sources.
3. Download from trusted Sources.
4. Use trusted Antivirus.
5. If suspicious activities are noted, Do Factory reset on your Mobile Phone.

04 / CALL / EMAIL SPOOFING

Spoofing is when someone disguises an email address, sender name, phone number, or website URL—often just by changing one letter, symbol, or number—to convince you that you are interacting with a trusted source. Criminals can manipulate you into believing that these spoofed communications are real, which can lead you to download malicious software, send money, or disclose personal, financial, or other sensitive information

Email spoofing

An email header is forged so that the message appears to have originated from someone or somewhere other than the actual source. Email spoofing is a popular tactic used in phishing and spam campaigns because people are more likely to open an email when they think it has been sent by a legitimate or familiar source. The goal of email spoofing is to get recipients to open, and possibly even respond to, a solicitation.

Modus Operandi

Call spoofing

A caller deliberately falsifies the information transmitted to your caller ID display to disguise their identity. Scammers often use number spoofing so it appears that an incoming call is coming from a local number, or spoof a number from a company or a government agency that you may already know and trust. If you answer, they use scam scripts to try to steal your

money or valuable personal information, which can be used in fraudulent activity.

Modus Operandi

1 The caller, who will identify himself/herself as an employee of the company, calls victim and tells them that their documents are incomplete and that they could be deported lest they pay up a certain sum through google pay/paytm or ask for OTPs/passwords.

2 If the victim search for the company number in some search engine he will get the same number which he/she got the call. So he/she beliefs that it was genuine number.

3 Following the instructions based on such communications, the victim deposits the money in unknown accounts, incurring heavy losses.

TIPS

1. Do not open suspicious and irrelevant emails, especially those received from unknown/ suspect senders.
2. Look up the phone number on your own, and call the company/person to ask if the request is legitimate.
3. Carefully examine the email address, URL, and spelling used in any correspondence.
4. Be careful with what information you share online. By openly sharing your private information, you are giving scammer all the information they need.

05 / IDENTITY THEFT

Identity theft is the crime of obtaining the personal or financial information of another person to use their identity to commit a crime. Identity Theft takes place whenever a criminal gets hold of a piece of your information, and then uses that information for their own personal gain. There are mainly two types of Identity theft:

Modus Operandi

- Financial Identity Theft

  In this, the stolen credentials are used to attain a financial benefit.

- Social Media Identity Theft

1) Someone uses your information to impersonate you on a fake social media profile.

2) Scammers can use personal information and photos from your social media accounts to create fake profiles that they then use to scam others.

TIPS

1. Use Strong Passwords and do not share your PIN with anyone on or off the phone.
2. Use two-factor notification for Social media accounts/emails.
3. Secure all your devices with a password.
4. Don't install random software from the internet.

TIPS

5 Don't post sensitive information over social media.

6 While entering passwords at payment gateway ensure its authenticity.

7 Do not fill personal data on the website that claims to offer benefits in return.

06 / SOCIAL ENGINEERING

Social Engineering is one of the simplest methods to gather information about a target through the process of exploiting human weakness. It uses deceitful techniques to deliberately manipulate human targets. It is primarily used to induce victims towards disclosing confidential data, or to perform actions that breach device security, unknowingly infecting systems or releasing confidential information. Throughout the interaction, victims are unaware of the destructive nature of their actions. The social engineer exploits the innocent instincts of common people.

Modus Operandi

1) Criminals will pose as technical support engineer, or bank staff, and will exploit the victim's inclination to trust.
2) The victim then willingly divulges any information requested by the criminal.

OR

1) In other cases, victims are guided by the criminal, purporting to be a technical support engineer requested to follow several steps to "fix" something on their computer.
2) The victim then unwittingly installs malware, which sends their personal or confidential information back to the criminal.

TIPS

1. Keep your software up to date, using the latest security patches available.
2. Ensure that you have the latest anti-virus software applications installed on your computer.
3. Do not give control of your computer to a third party who call you unexpectedly.
4. Do not click on links or icons on unsolicited email.
5. Never provide your online ID, password or PIN to anyone.

07 / KEY LOGGERS

A Keylogger is a hardware or software device which monitors every keystroke, screen shots, chats etc. typed on computer. Keyloggers are used as a tools by attacker to steel user's usernames and passwords in e-commerce, social network, Mail service etc. There are two type of keyloggers- software-based and hardware based.

Modus Operandi

1. Scammers Sends/Spread keyloggers over the Internet.
2. Software keyloggers get installed on the computer/mobile when the user downloads an infected application.
3. Keyloggers track and record keystrokes. Then it transmits the confidential information to the hacker.

TIPS

1. Enable 2-Step Verification.
2. Use Key Encryption Software.
3. Install Anti Malware Software.
4. Use Computer Case.
5. Disable the USB Ports.

08 / PUBLIC WI-FI AND HOTSPOTS

Public WI-FI

Using a public Wi-Fi network poses danger to the users as the data over this type of open connections are often unencrypted and unsecured, leaving the users vulnerable to a man-in-the-middle (MITM) attack. A cybercriminal exploits a security flaw in the network to intercept data transmitting through the network. This gives a hacker access to sniff out any information that passes between you and the websites you visit — details of browsing activities, account logins, and purchase transactions. Your sensitive information, such as passwords and financial data, are then vulnerable to identity theft.

Rogue Hotspots

Another risk of using free public Wi-Fi is that you may be connecting via a rogue hotspot. This is an open hotspot, usually with a name similar to that of a legitimate hotspot, which cybercriminals set up to lure people into connecting to their network. Once a victim connects to the rogue Wi-Fi hotspot, the host hacker can then intercept data and even use tools to inject malware into the connected devices.

Modus Operandi

1 User Connects to the internet through a Public Wi-Fi.

2 Attacker Exploits security flaw in Wi-Fi Router.

3 Attacker sniffs data between Wi-Fi Router and the connected device or Injects malware into victims device.

TIPS

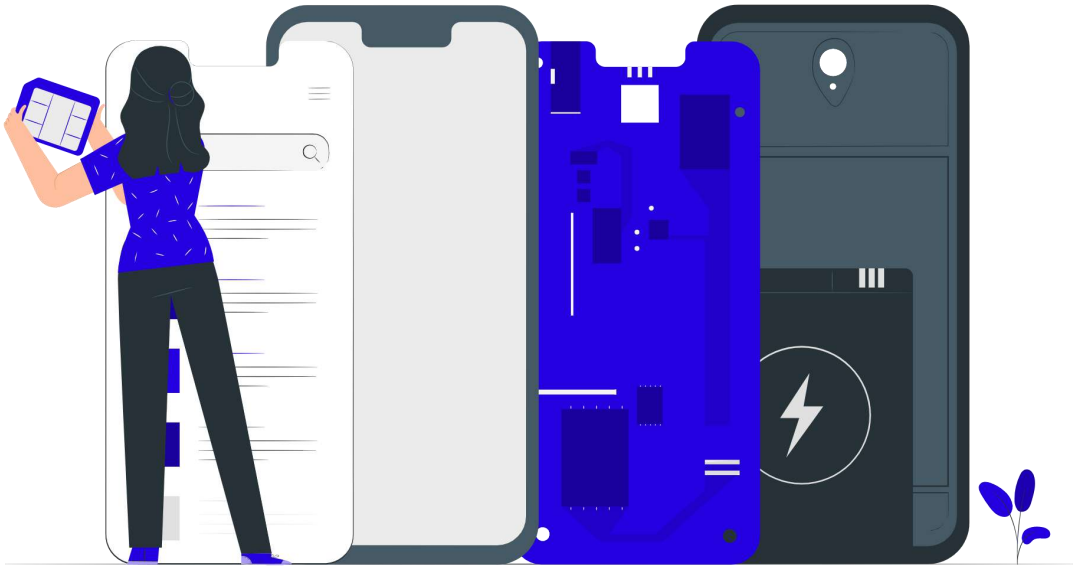
1. Make sure you connect to only encrypted Wi-Fi points.
2. If you connect to a website, and then make sure it uses only HTTPS.
3. Never connect to open Wi-Fi routers directly.

09 / SERVICE CENTERS

Smartphones are bound to get damaged which have full of personal and important data. There is a chance of the repair person can access your data and may misuse it. They can steal your data, photos, camera module, speakers or microphone depending upon smartphone models.

TIPS

1. Create a Full Back Up.
2. Remove Your SIM Card SD Card.
3. Note down Your IMEI.
4. Encrypt your data.
5. Perform a Factory Reset.
6. Log out from your Google
7. Disable Factory Reset Protection.



10 / Attacks on IOT

Internet of Things (IoT) is an ecosystem of connected physical objects that are accessible through the internet. various vulnerabilities are observed which shall keep IoT as a technology in danger. The IoT attack surface is the sum total of all potential security vulnerabilities in devices and associated software and infrastructure in a given network. Any device in that list can be hacked if connected to the Internet and not adequately protected. The hacked devices can also provide an attacker with access to sensitive data

Victim IoT system with potential vulnerability

Modus Operandi

1 Attacker identifies the victim device which is unprotected and is having vulnerability.

2 Attacker exploits the vulnerability and will get access to the victim system.

3 Attacker now will have access to sensitive data and devices of the victim.

TIPS

1. Use stronger passwords.
2. Update security patches.
3. Buy Devices from reliable manufacturers.
4. Always remember to change the default username and passwords.

Keep Your Antivirus Program Up To Date.

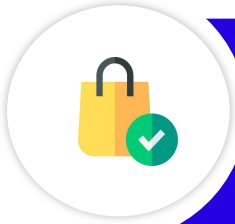
Keep Your Privacy Settings On.

Practice Safe Browsing.

Always Make Sure Your Internet Connection is Secure.

Be Careful about downloads and clicking links.

Always use Strong Passwords.



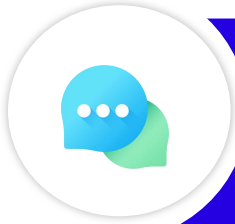
Make Online Purchases From Secure Sites.

Know what to do if you become a victim

Be Careful What You Post.

Be Careful Who You Meet Online.

Type #06# to get IMEI, note it and keep it safe.



Do not respond to messages for payment.

ONLINE CODE OF CONDUCT

TO KEEP YOU SAFE

Search the job on official website only.

You can never win a lottery without participating in it.

Never save your username and password in the web.

Never do financial transaction over free Wi-Fi.

If you are a victim of online fraud, report it.

Keep Personal Information Protected and Limited.

ONLINE CODE OF CONDUCT

TO KEEP YOU SAFE

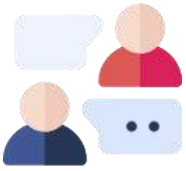
01

Place computer in a common area

02

Discuss about dangers on internet with children

03



Teach them not to talk to strangers to keep them away from harm.

04

Implement parental controls and use filtering software

Eg: Google Family Link app

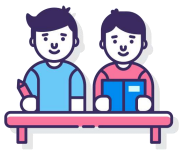
05

Ask them never share personal information with strangers on social media.

06

Watch for any change in child's behaviour.

07



Encourage your child to be respectful to classmates.

08

Talk children about cyberbullying.

GENERAL TIPS
TO PARENTS

09

Be a friend on your Child's Social network. This will act as deterrent to online child predators.

10

Do not delete offensive messages as it will help the police in investigation.

11

Know your child's online friends.

12

Use search engines meant for children so that they do not see age Inappropriate Content.

- https://www.kiddle.co/
- https://wackysafe.com
- https://www.youtubekids.com/

GENERAL TIPS
TO PARENTS

For more Info:
https://www.kidglove.in

01 Never give out personal information such as address, phone number etc.

02 Always inform parents if you come across something that makes you feel uncomfortable.

03 Never agree to get together with someone you meet online.

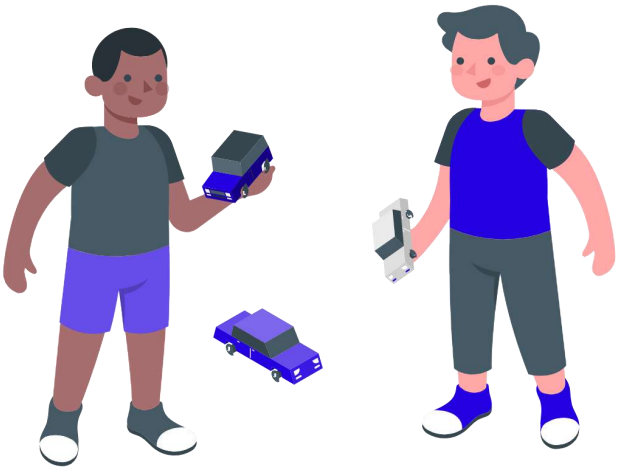
04 Talk to your parents before posting your pictures or any pictures online that they consider to be inappropriate.

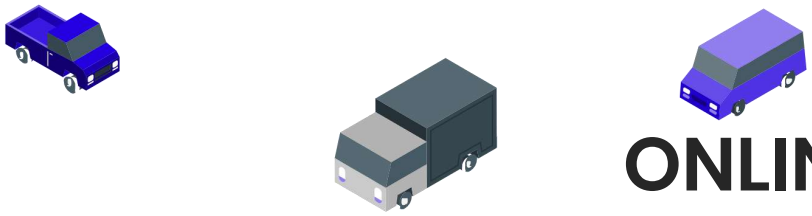
05 Never respond to any messages that are mean or in any way making you feel disturbed.

06 Don't give out your passwords to anyone other than your parents.

07 Always check with parents before downloading or installing software.

08 Always be a good online citizen and not do anything that hurts other people or something which is illegal.





ONLINE SAFETY RULES
FOR KIDS

01 Report to the nearest police station immediately.

02 National Cyber Crime Reporting Portal.

https://cybercrime.gov.in

03 Kerala Police

https://keralapolice.gov.in
https://thuna.keralapolice.gov.in

04 For blocking / unblocking lost / stolen mobile

https://ceir.gov.in

WHERE TO REPORT A CYBER CRIME?

IN A NUTSHELL

~$ You are the key to security

~$ Security is not a product, it is a continuous process.

~$ Trust is good, but control is better.

KERALA POLICE
CYBERDOME
Public-Private Partnership for Cyber Security

Partner us
in making
a secure cyber world

KERALA POLICE

CYBERDOME

Public-Private Partnership for Cyber Security

Partner us
in making
a secure cyber world