वे.को.लि.
सुरक्षा विभाग

CYBER SECURITY CELL

WESTERN COALFIELDS LIMITED

SECURITY DEPARTMENT

(सक्षम, सर्वोत्तम, सर्वज्ञ)

कोल इण्डिया
Coal India

CYBER SECURITY

As Western Coalfields Limited (WCL) continues to leverage technology to enhance operational efficiency, it is crucial to prioritize the security of its digital assets and protect sensitive information from potential cyber threats.

- 🔒 Physical Security Measures
- 🔒 Theft & Pilferage Prevention
- 🔒 Technological Advancement
- 🔒 Workplace & Employee Security

CYBER
CELL

DIGITAL & INNOVATION

CYBER SECURITY CELL BROCHURE

वे.को.लि.
सुरक्षा विभाग

ABOUT

कोल इण्डिया
Coal India

CYBER SECURITY CELL BROCHURE

The Cyber Security Cell of the Security Department is dedicated to safeguarding the organization's digital infrastructure against evolving cyber threats. As technology becomes integral to coal operations——from logistics and communication to automation and data management——our cell plays a crucial role in ensuring resilience, data protection, and a secure system.

We actively monitor threats, enforce robust cyber hygiene practices, and implement security protocols in alignment with national standards and industry best practices. Through regular audits, awareness programs, and incident response mechanisms, the Cyber Security Cell supports Coal India’s mission of operational excellence while maintaining the integrity, confidentiality, and availability of critical information assets.

The "Cyber Security Cell brochure " aims to bridge knowledge gaps, enhance operational efficiency, and contribute to a more robust security environment.

SECURITY DEPARTMENT
WESTERN COALFIELDS LIMITED

वे.को.लि.
सुरक्षा विभाग

कोल इण्डिया
Coal India

MISSION

THE MISSION OF SECURITY DEPARTMENT OF WESTERN COALFIELDS LTD. IS TO PROTECT THE PROPERTIES OF THE COMPANY AND PROVIDE COLLECTIVE SECURITY TO MANAGEMENT, STAFF AND EMPLOYEES WITH A VIEW TO ACCELERATING PRODUCTION THROUGH INDUSTRIAL PEACE.

वेस्टर्न कोलफील्ड्स लिमिटेड के सुरक्षा विभाग का ध्येय कंपनी की संपत्तियों की सुरक्षा करना एवं प्रबंधन कर्मचारियों एवं कामगारों की सामूहिक सुरक्षा प्रदान करना जिससे उत्पादन एवं प्रेषण में औद्योगिक शान्ति के साथ गतिशीलता बनी रहे।

(सक्षम, सर्वोत्तम, सर्वज्ञ)

SECURITY DEPARTMENT
WESTERN COALFIELDS LIMITED

Shri Jai Prakash Dwivedi
CMD, WCL

MESSAGE FROM CMD, WCL

The increasing digitalization of business operations has transformed the way organizations function, creating new avenues for efficiency, innovation, and connectivity. However, this transformation also brings with it complex challenges in ensuring the confidentiality, integrity, and availability of information assets. In this context, Cyber Security has become an indispensable component of organizational governance and risk management.

I am pleased to note that the Security Department has taken a commendable initiative in bringing out this Brochure on Cyber Security Awareness. This publication underscores WCL's commitment to fostering a culture of cyber vigilance, resilience, and accountability across all levels of the organization.

I am confident that this initiative will contribute significantly towards enhancing the preparedness of our workforce against evolving cyber threats and will further strengthen the digital security framework of Coal India Limited.

Date : 22.10.2025
Place : Nagpur

Dr. Hemant Sharad Pande
Director (HR), WCL

MESSAGE FROM DIRECTOR (HR), WCL

In an increasingly digital workplace, information security is no longer the sole responsibility of working professionals — it is a shared responsibility of every individual within the organization. Building a cyber-secure environment requires awareness, discipline, and a collective commitment to responsible digital behavior.

The efforts of the Security Department in developing this Cyber Security Brochure are highly appreciable. This initiative reflects a forward-looking approach towards creating an informed and vigilant workforce capable of identifying and responding to cyber risks effectively.

As technology continues to integrate into every facet of our operations, ensuring data security and privacy must remain an organizational priority. Awareness and timely preventive action are the strongest shields against cyber threats.

I extend my compliments for their proactive contribution towards promoting a culture of digital responsibility and resilience across the organization.

Date : 22.10.2025
Place : Nagpur

Lt. Cdr. (Dr.) Vikrant Malhan
HOD (Sec), WCL

MESSAGE FROM HOD (SECURITY), WCL

In today's digital era, the Security of our information assets is as crucial as the safety of our physical infrastructure. This brochure is an important step toward strengthening Cyber awareness across all levels of our organization.

As technology continues to transform the Coal industry, we must remain vigilant against evolving Cyber threats. The brochure encapsulates essential guidelines, best practices, and preventive measures to protect our digital eco-system.

I encourage every employee to study it carefully and implement the Security awareness measures in their daily operations.

Let us all pledge to maintain a culture of Cyber vigilance, responsibility, and resilience — ensuring that Western Coalfields Limited continues to operate safely, efficiently and securely in the digital domain.

My sincere thanks my Team especially Shri Vishal Bhonsle, Sr SI, WCL HQ and Shri Swapnil, Security Guard for their immense contribution in making this Cyber Security Brochure.

The Cyber Security Cell, operational under Security Department WCL HQ operates 24x7 to assist employees in case they face any Cyber Security threat and can be reached Toll Free on 1800-233-5506.

Jai Hind!

Date : 22.10.2025
Place : Nagpur

INTRODUCTION

1. Western Coalfields Ltd is a premium Coal Producing PSU under the aegis of Coal India Ltd. Due to its large work force; it is one of the biggest employers in the Country with an employee count of 35000 personnel. The PSU has its operations across Maharashtra & Madhya Pradesh and has its Corporate HQ at Nagpur, Maharashtra.

2. As Western Coalfields Ltd. (WCL) continues to leverage technology to enhance its operational efficiency, it is critical to prioritize the Security of our digital assets and protect sensitive information from potential Cyber threats.

3. WCL is the first PSU to have its dedicated cyber security cell under the security department which spreads awareness amongst employees and stake holders on various facets of cyber security. It has a 24x7 dedicated support system to help employees in case of a situation and systematically guide them to be able to mitigate losses and help in critical threatening situation.

OBJECTIVE OF THE CYBER SECURITY CELL

The Cyber Security Cell will serve as the central unit responsible for safeguarding WCL's digital environment, providing a structured approach:

1. Cyber Threat Detection and Prevention: Protect WCL's digital infrastructure, systems, and data from malicious attacks, including hacking, phishing, ransom ware, and other security breaches.

2. Incident Response and Management: Establish an efficient response mechanism to detect, investigate, and resolve security incidents, ensuring minimal disruption to operations.

3. Regulatory Compliance: Ensure that WCL complies with all relevant cyber security laws, regulations, and industry standards, including the IT Act 2000 and data privacy regulations.

4. Employee Awareness and Training: Conduct regular cyber security awareness programs and training for employees to promote best practices and develop a culture of security.

5. Collaboration and Partnerships: Build partnerships with National and International cyber security agencies, experts, and law enforcement to stay ahead of emerging threats.

WHY CYBER SECURITY CELL IS NEEDED ?

1. Rising Cyber Security Threats: The energy sector, including Coal mining, is increasingly targeted by cyber criminals due to its critical infrastructure. The potential financial and operational damages from a cyber attack on WGL could be catastrophic

2. Safeguarding Sensitive Information: WCL deals with large volumes of sensitive information, including employee data, financial transactions, procurement, and contractual documents. Ensuring the confidentiality, integrity, and availability of this data is essential

3. Compliance with National Standards: The Government of India has placed increasing importance on cyber security in both public and private sectors, particularly for entities operating critical infrastructure. Establishing a dedicated cyber security cell will ensure that WCL complies with national standards and guidelines.

4. Preventing Financial Loss : Cyber attacks can lead to significant financial losses, both in terms of data breach and disruption of operations. A proactive cyber security strategy can save WCL employees and stake holders from financial and reputational damage.

KEY RESPONSIBILITIES OF THE CYBER SECURITY CELL

1. Risk Assessment: Conduct regular risk assessments and audits to identity vulnerabilities and develop mitigation strategies.

2. Security Monitoring: Implement and manage advanced security monitoring systems, firewalls, intrusion detection systems, and endpoint protection.

3. Employee Training & Awareness: Organizes periodic Cyber Security training for all Employees to prevent human error, which is often a leading cause of data breaches.

CYBER SECURITY TRAINING BROCHURE

CONTENTS

1 | KYC Scam

KYC Fraud involves cybercriminals exploiting identity verification processes to steal personal information, commit identity theft, or access financial accounts illegally. This can lead to significant financial losses and reputational damage for individuals, businesses, and financial institutions. Common tactics include tricking people, forging documents, and creating fake identities.

❖ Do's :

- ➢ Verify Requests: Contact your bank or financial institution directly to confirm any KYC update requests.
- ➢ Use Official Contacts: Obtain contact numbers or customer care details only from the official website or trusted sources.
- ➢ Report Incidents: Inform your bank or financial institution immediately if you suspect any cyber fraud.
- ➢ Check KYC Update Methods: Enquire with your bank about the available methods for updating KYC details.

❖ Don'ts :

- ➢ Protect Credentials: Never share your account login details, card information, PINS, passwords, or OTPs with anyone or on unauthorised websites/apps.
- ➢ Secure Documents: Do not share KYC documents or their copies with unknown or unidentified individuals organisations.
- ➢ Avoid Suspicious Links: Do not click on suspicious or unverified links received via mobile or email.

Toll Free Number : 1800-233-5506

2 | Phishing / Quishing

Phishing is a common cybercrime tactic that deceives victims into clicking on fake links. These links appear as emails or websites from trusted sources but redirect users to fraudulent sites designed to steal sensitive data, such as login credentials, personal information, or financial details. Phishing can also install malware, giving cybercriminals unauthorised access to your device. Some identifiable Red Flags could be unfamiliar sender addresses, urgent language asking for action (for eg., 'Reset Password Now'), suspicious links or attachments.

❖ Do’s:

- Be Suspicious: Treat unexpected messages from known sources with caution.
- Check URLs: Hover over links to reveal the genuine destination and spot discrepancies.
- Verify Senders: Contact the sender through a trusted method if you're unsure about a message's authenticity.
- Update Regularly: Keep your software and systems up-to-date to close security gaps.
- Phishing Report: Alert the relevant authorities or platforms if you encounter phishing attempts.

❖ Don'ts:

- Avoid Clicking Links: Don't click on suspicious links: delete messages from unknown senders immediately.
- Unsubscribe & Block: Unsubscribe from emails with suspicious links and block the sender's email.
- Visit Official Websites: Always go directly to the official website for financial transactions and verify website security (HTTPS with a padlock).

3 | Deepfake Cybercrime / AI Generated Imagery

Cybercriminals are now using advanced artificial intelligence (AI) to create fake videos or voice recordings that look and sound real. They take real clips and change them to trick people. These fakes are shared through social media, messages, and emails. Often, they target well-known people or those in positions of power. The goal is to fool others, change their opinions, or spread lies. In some cases, these criminals pretend to be from the defence forces to ask for money or stir up strong emotions among the public.

❖ **Do’s:**

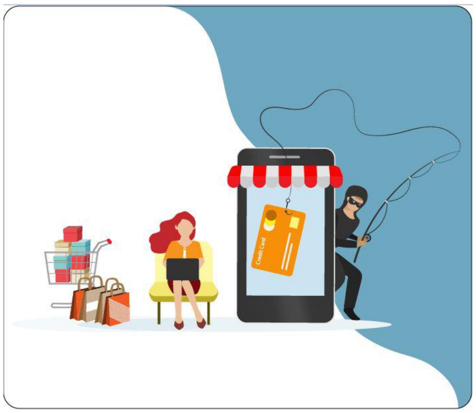
- ➢ Stay Informed: Learn about deepfake technology and its risks.
- ➢ Verify Content: Always check the authenticity of media before sharing or believing it.
- ➢ Use Trusted Sources: Rely on reputable platforms for news and updates.
- ➢ Report Suspicious Content: Alert authorities or platforms if you find potential deepfakes.

❖ **Don'ts:**

- ➢ Don't Share Unverified Media: Avoid spreading content without checking its truthfulness.
- ➢ Don't Trust Suspicious Sources: Stay away from unreliable sources that may share deepfakes.
- ➢ Don't Trust Blindly: Be cautious of content that seems exaggerated or emotional.
- ➢ Don't Ignore Privacy: Review privacy settings and limit the personal info you share online

4 | Online Shopping Fraud / Online Marketplace Fraud

Online Shopping Fraud is a cybercrime where fraudsters deceive victims into making illegitimate purchases. They create fake websites or manipulate legitimate platforms, offer deals that are too good to be true, and steal personal and financial information, leading to financial losses and mistrust in online marketplaces.



❖ Do's:

- Compare Prices: Compare prices on different commerce websites. e-
- Use Cash-on-Delivery: If a website seems suspicious, opt for the cash-on-delivery payment method.
- Choose Verified Sellers: Prefer buying from "Verified" or "Trusted" sellers on commerce websites.
- e-Verify Offers: Be cautious of offers that seem too good to be true.
- Secure Transactions: Remember, you never need to enter a PIN, password, or OTP to receive money.
- Use strong, passwords. unique

❖ Don'ts:

- Don't prepay for products on unknown or poorly designed websites.

Fraudulent sellers often disappear after receiving advance payment through insecure websites.

- Avoid clicking on shopping links received via SMS or forwarded messages.

These often redirect to phishing websites designed to steal your payment or login information.

- Don't ignore warning signs like spelling errors, fake logos, or unrealistic prices.

Such signs are common on scam websites that imitate popular brands or e-commerce portals

Toll Free Number : 1800-233-5506

5 | Mobile Application Scam / Loan App Scam

Cybercriminals create Fake Mobile Banking Apps that closely resemble legitimate ones, using similar logos and interfaces. These apps are distributed through unofficial channels like third-party app stores or phishing links. Once installed, they steal your banking credentials and personal data, leading to financial fraud

---

❖ Do's:

- Download from Official Stores: Always download banking apps from trusted sources like Google Play Store or Apple App Store or bank websites.
- Verify App Authenticity: Check the developer details and read reviews before installing any banking app.
- Keep Software Updated: Ensure your phone's OS and security software are always current.
- Enable Two-Factor Authentication (2FA): Add an extra layer of security to your accounts.
- Regularly Monitor Bank Accounts: Review your bank account statements regularly for any unauthorised transactions.

❖ Don'ts:

- Don't Download from Unofficial Links: Avoid clicking on links or downloading apps from suspicious emails or websites.
- Don't Enter Sensitive Info in Unknown Apps: Never share banking details in unfamiliar apps or sites.
- Don't Jailbreak Your Device: Rooting your device makes it vulnerable to malware and attacks.
- Don't Share Credentials: Never share your banking PIN or OTP with anyone, even if they claim to be support staff

6 | Spam / Vishing Calls / SMS, Email & Call Scams

Spam/Vishing Calls (voice phishing) are a deceptive form of cybercrime. Fraudsters use social engineering to trick victims into revealing sensitive information, like personal or financial data. They often impersonate legitimate entities, such as banks or government agencies, using tactics like caller ID spoofing and urgency to gain trust and steal information.

❖ Do’s:

- <u>Use Call Blockers</u>: Install call-blocking apps and report spam calls.
- <u>Be Cautious</u>: Exercise caution when answering calls from unknown numbers.
- <u>Spread Awareness</u>: Educate others about common phone scams.
- <u>Enable Security</u>: Use voicemail passwords for added protection.

❖ Don'ts:

- <u>Don't Share Personal Info</u>: Never provide personal or financial information unknown callers. to
- <u>Don't Trust Caller ID</u>: Caller ID can be spoofed, so don't rely on it.
- <u>Avoid Unknown Numbers</u>: Don't return calls from unfamiliar or international numbers.
- <u>Protect Your Data</u>: Genuine institutions never ask for sensitive info like usernames, passwords, or OTPs. Never share these, even with family

Toll Free Number : 1800-233-5506

7 | SIM Swapping / Online Banking Fraud

SIM Swapping is a cybercrime where fraudsters transfer your phone number to their SIM card. This gives them access to your calls, texts, and two-factor authentication codes, enabling identity theft, account hijacking, and financial fraud. Scammers often pose as network staff offering upgrades or benefits to trick you into revealing personal details.

❖ Do's:

- <u>Enable 2-Factor Authentication</u>: Add extra security to your accounts.
- <u>Use Strong PINs</u>: Set unique and hard-to-guess PINs for your accounts and SIM.
- <u>Stay Updated</u>: Keep your phone's software and apps regularly updated.
- <u>Report Suspicious Activity</u>: Contact your network provider immediately if you notice unusual activity or lose your SIM.

❖ Don'ts:

- <u>Protect Information</u>: Never store sensitive data or share OTPs with strangers via calls or texts.
- <u>Use Strong PINS</u>: Avoid easily guessable PINs for your accounts.
- <u>Report SIM Loss</u>: Notify your network provider immediately if your SIM card is lost.
- <u>Monitor Activity</u>: Watch for unusual mobile activity or extended loss of network access and act promptly.
- <u>Secure Credentials</u>: Never share identity details linked to your SIM card.

8 | Money Mules / Investment & Crypto Scams

Money Mules are individuals, knowingly or unknowingly. used to launder illegally obtained funds. Scammers persuade them to receive and transfer stolen money in exchange for commissions. These funds are moved across multiple accounts to obscure the fraudster's Identity. Involvement in such activities, whether intentional or not, is illegal and carries severe legal consequences.

❖ Do’s:

- Scrutinise Job Offers: Be cautious of unsolicited jobs involving money transfers. Research the company's or individual's legitimacy.
- Guard Financial Information: Never share bank account details or personal information with unknown parties.
- Report Suspicious Activity: Contact authorities if you suspect a money mule scheme.

❖ Don'ts:

- Don't Share Accounts: Never let others use your account to receive or transfer funds.
- Refuse Commissions: Reject offers to handle unauthorised money for a fee.
- Know the Risks: Transferring illegitimate funds can lead to serious legal action.

9 | Juice Jacking

Juice Jacking is a cybersecurity risk associated with compromised public USB charging stations. Hackers can exploit USB ports that charge and transfer data, using them to install malware or steal sensitive information. While no confirmed cases exist, staying vigilant is essential.

❖ Do's:

- Carry Your Charger: Use your own charger and cable to avoid potentially tampered public ports.
- Verify Prompts: Be cautious of "trust this device" prompts and accept only from trusted sources.
- Opt for AC Outlets: Choose standard electrical outlets whenever possible.

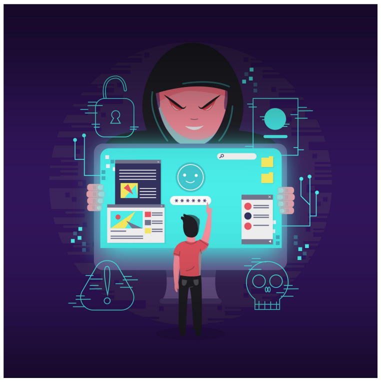
❖ Don'ts:

- Avoid Public Ports: Do not use unknown or public USB ports or cables.

Toll Free Number : 1800-233-5506

10 | Impersonation and Identity Theft

Cybercriminals steal your identity or impersonate someone you know to gain your trust and trick you into sharing sensitive data or making financial transactions.



❖ Do's:

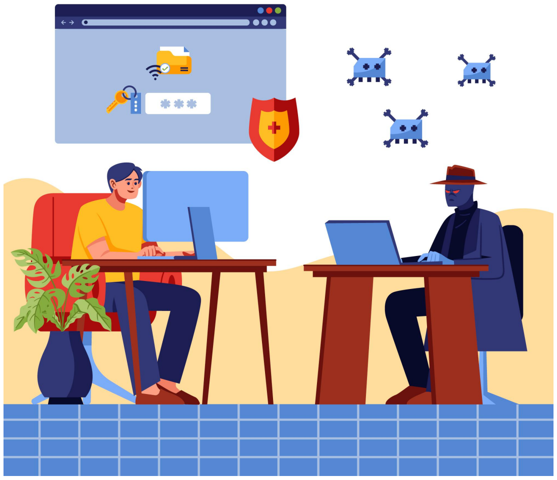
- ➢ Use strong, unique passwords and update them regularly to prevent hacking.
- ➢ Enable multi-factor authentication on all critical accounts and devices.
- ➢ Monitor your credit score and online presence for any suspicious activity.

❖ Don'ts:

- ➢ Don't share sensitive identity documents like Aadhaar or PAN on public platforms.
- ➢ Avoid accepting friend requests or messages from unfamiliar or duplicate profiles.
- ➢ Don't ignore alerts from your bank or email provider about suspicious access.

11 | Job and Employment Scams

Job scams trick job seekers with fake job offers, often promising high salaries, quick hiring, or work-from-home roles. Scammers impersonate reputed companies, HR personnel, or consultants, asking for registration fees, document verification charges, or bank details — but the job doesn't exist. These scams involve fake job offers from fraudulent recruiters or companies that ask for upfront payments for registration, training, or placement fees.



❖ Do's:

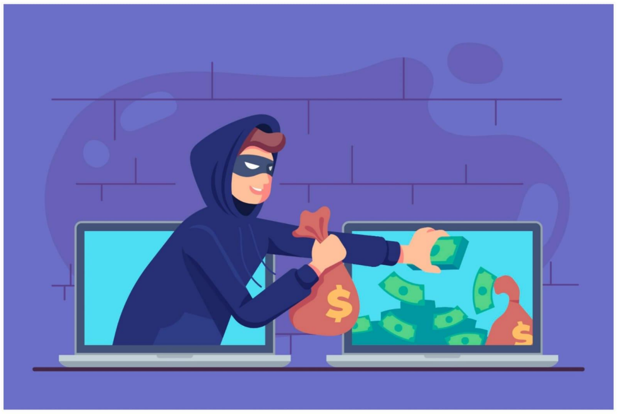
- Always verify job offers through official company websites or HR departments.
- Research the recruiter's credentials on platforms like LinkedIn or Glassdoor.
- Report fake job portals or agents to job boards or cybercrime units.

❖ Don'ts:

- Don't pay any upfront fees for interviews, training, or job placements.
- Avoid sharing your personal or banking information without verifying the employer.
- Don't fall for job offers that promise unrealistic salaries with minimal effort.

12 | Lottery and Prize Scams

Lottery and prize scams involve messages (via SMS, email, phone calls, or social media) claiming you've won a large sum of money, a car, or a prize — even if you never entered any contest. The scammer then asks for "processing fees," taxes, or bank details to release the prize, which never exists. Victims are contacted with claims of winning a lottery or prize and are asked to pay taxes, courier charges, or processing fees to receive it, which never arrives.



❖ Do's:

- ➢ Be cautious of prize notifications for contests you never entered.
- ➢ Verify the prize offer with official sources or company websites.
- ➢ Report suspicious prize claim emails or messages to cybercrime authorities.

❖ Don'ts:

- ➢ Don’t send money or personal information to claim a prize or lottery.
- ➢ Avoid clicking on links or downloading attachments in prize-related emails.
- ➢ Don’t trust prize claims that have spelling errors, poor grammar, or foreign contact numbers.

13 | Tech Support Scams

Tech support scams happen when fraudsters pose as legitimate tech support agents (from Microsoft, Apple, or other known brands). They trick users into believing their computer has a virus or issue, then ask for remote access or payment for unnecessary services or fake software. Fraudsters impersonate customer service agents from tech companies and claim your device is infected. They ask for remote access or payment to fix fake issues.

❖ **Do's:**

- ➢ Contact tech support directly through the company's official website or app.
- ➢ Keep antivirus software updated to detect and prevent threats.
- ➢ Disconnect immediately if someone requests remote access unexpectedly.

❖ **Don'ts:**

- ➢ Don't share passwords, card details, or give control of your device to strangers.
- ➢ Avoid responding to pop-ups claiming your system is infected.
- ➢ Don't install unknown software or follow instructions from unsolicited calls.

14 | Romance and Dating Scams

Romance scams occur when fraudsters create fake identities on dating apps, social media, or websites to build emotional relationships with victims. Once trust is established, they make fake stories and request money for emergencies, travel, or health issues — and then disappear. Scammers form emotional online relationships and later request money under false pretenses such as emergencies, visas, or illness.

❖ Do's:

- Verify the identity of online friends through video calls or background checks.
- Discuss online relationships with a trusted friend or family member.
- Set privacy settings on social platforms to control who sees your profile.

❖ Don'ts:

- Don’t send money or share banking information with someone you haven’t met.
- Avoid sharing sensitive or intimate content with people online.
- Don’t ignore red flags like reluctance to meet in person or sudden emergencies.

Toll Free Number : 1800-233-5506

15 | Ransomware Attacks

Ransomware is a type of malicious software that encrypts a victim's files or locks their system. The attacker demands a ransom (usually in cryptocurrency) to restore access. Victims may receive threatening messages claiming data will be leaked or permanently lost if payment isn't made. Malicious software locks your data or system until a ransom is paid. These attacks are typically delivered via email attachments or infected websites.

❖ **Do's:**

- ➢ Back up data regularly and store it offline or in a secure cloud.
- ➢ Install strong antivirus and keep your system updated to patch vulnerabilities.
- ➢ Train yourself and your team to recognize phishing emails and fake downloads.

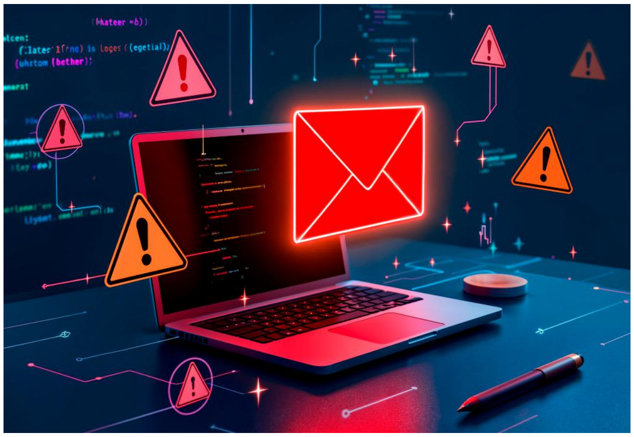
❖ **Don'ts:**

- ➢ Don't click suspicious links or open unknown attachments in emails.
- ➢ Avoid using pirated software or downloading from untrusted sources.
- ➢ Don't pay the ransom; there's no guarantee your files will be recovered.

Toll Free Number : 1800-233-5506

16 | Business Email Compromise (BEC)

Business Email Compromise is a cyber scam where attackers impersonate senior executives, vendors, or trusted partners using spoofed or hacked email accounts. They trick employees into transferring money, sharing sensitive data, or changing payment details. It targets businesses, government agencies, and even NGOs. Scammers hack or spoof executive email accounts and request unauthorized transfers or confidential information from employees.



❖ **Do's:**

- ➢ Confirm high-value transactions through a second communication channel.
- ➢ Implement email authentication protocols like SPF, DKIM, and DMARC.
- ➢ Train employees regularly to recognize suspicious or altered email IDs.

❖ **Don'ts:**

- ➢ Don’t rely solely on email for approving financial transfers.
- ➢ Avoid using predictable email passwords or reusing them across accounts.
- ➢ Don’t ignore warning signs like urgent payment requests or changed bank details.

Toll Free Number : 1800-233-5506

17 | Fake Government or Utility Calls

These scams involve fraudsters impersonating officials from government departments (like tax offices, police, or courts) or utility providers (like electricity, gas, water). The caller may claim unpaid bills, legal trouble, or verification needs, pressuring the victim to pay or share sensitive information. Scammers pretend to be officials from government or utility companies, threatening fines, disconnection, or arrest unless payment is made immediately.

❖ Do's:

- Verify the caller’s identity through official websites or contact numbers.
- Record the call and report it to the cybercrime portal or local police.
- Educate family members, especially the elderly, about such scams.

❖ Don'ts:

- Don’t make payments or share OTPs over unsolicited calls.
- Avoid panicking or taking action without proper verification.
- Don’t trust caller ID displays as they can be easily spoofed.

18 | Online Gaming Frauds

Online gaming frauds involve cybercriminals exploiting gamers through fake game apps, in-game purchases, phishing links, account takeovers, or offering free upgrades, cheats, or virtual currency. These scams can lead to financial loss, identity theft, or exposure to malware. These scams target gamers with fake in-game purchases, cheat tools, or fake tournaments designed to steal money or access.

❖ Do's:

- ➢ Use only official stores or platforms for buying in-game content.
- ➢ Enable security settings on gaming accounts and use strong passwords.
- ➢ Keep children informed about safe online gaming habits.

❖ Don'ts:

- ➢ Don’t share account credentials with strangers or friends.
- ➢ Avoid third-party cheat codes or mod apps that could be malware.
- ➢ Don’t click on links offering free game currency or rewards.

19 | Fake Charities and Donation Scams

Fake charity scams involve fraudsters pretending to represent legitimate charitable organizations (or creating fake ones) to solicit donations. These scams often arise during natural disasters, pandemics, or humanitarian crises to exploit people's empathy. They may approach victims via email, phone calls, fake websites, or social media posts. Cybercriminals exploit disasters or emotional appeals to solicit donations through fake NGOs, websites, or UPI IDs.

❖ **Do's:**

- Verify the organization’s credentials and registration before donating.
- Donate directly through official websites or government-endorsed portals.
- Request receipts and tax exemption details for transparency.

❖ **Don'ts:**

- Don’t donate through links sent on social media or messages without verification.
- Avoid sending money to unknown UPI IDs or unverified bank accounts.
- Don’t assume every emotional appeal is genuine—research before helping

BEST PRACTICES FOR MOBILE HANDLING

Securing mobile devices is more important than ever as our phones hold personal and financial information. To stay safe, your mobile must be safe. With just a few smart habits, you can keep your phone and your information safe from cybercriminals.

1. Use strong pass code or biometric lock (fingerprints/ face recognition).

2. Install apps only from trusted sources (Google Play Store/Apple App Store).

3. Use two-factor authentication (2FA) for accounts.

4. Keep your OS and apps updated to patch security vulnerabilities.

5. Install antivirus software.

6. Turn off Bluetooth, Wi-Fi, Air Drop, NFC and location when not in use to avoid tracking or unauthorized access.

7. Clear cache/contacts/data/unused apps periodically.

8. Back up data regularly using cloud or encrypted storage.

9. Avoid syncing financial payment methods with Whatsapp (similar apps).

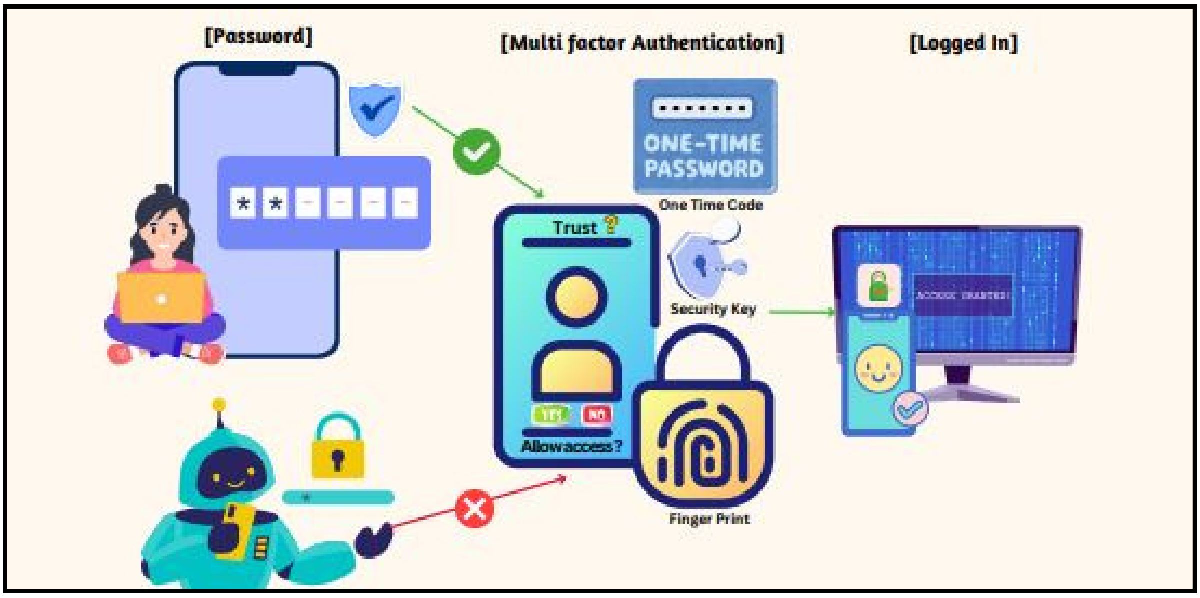
10. Avoid using public Wi-Fi's/ Hotspots while making financial transactions.

Toll Free Number : 1800-233-5506

BEST PRACTICES FOR DESKTOP SECURITY

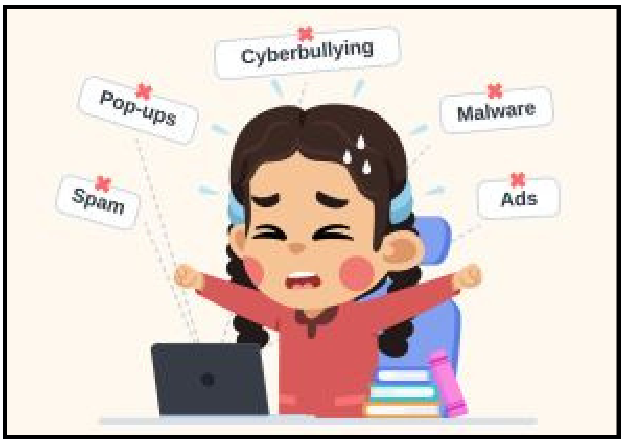
1. Use genuine Operating System and Software.
2. Keep your Operating System updated.
3. Install anti-virus and anti-malware solutions and keep them updated.
4. Use strong login password and change them periodically.
5. Regularly take backups of your important files and data.
6. Incase of incidents such as hardware failure, or cyberattacks, having backups can help you restore important information.
7. Maintain multiple copies of critical data in different locations to prevent loss in case of disasters.
8. Periodically test and verify your backups to ensure that they can be used for restoration when needed.

BEST PRACTICES FOR ONLINE ACCOUNT SECURITY



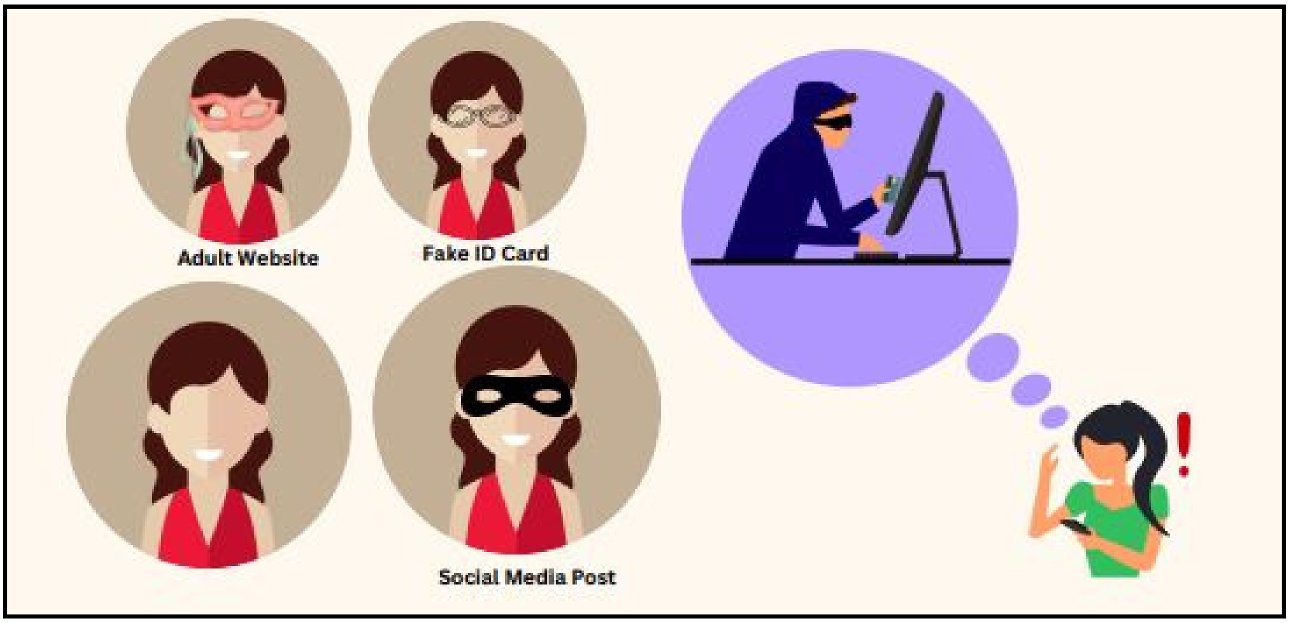
1. Enable Multi-Factor Authentication, it adds an extra layer of security by requiring a second form of verification in addition to your password.
2. Regularly update your passwords.
3. Do not reuse passwords.
4. Do not share your passwords with anyone.
5. Use unique, complex, and long passwords.
6. Regularly check your account activity and look for any suspicious login attempts.

BEST PRACTICES FOR SOCIAL MEDIA FOR WOMEN



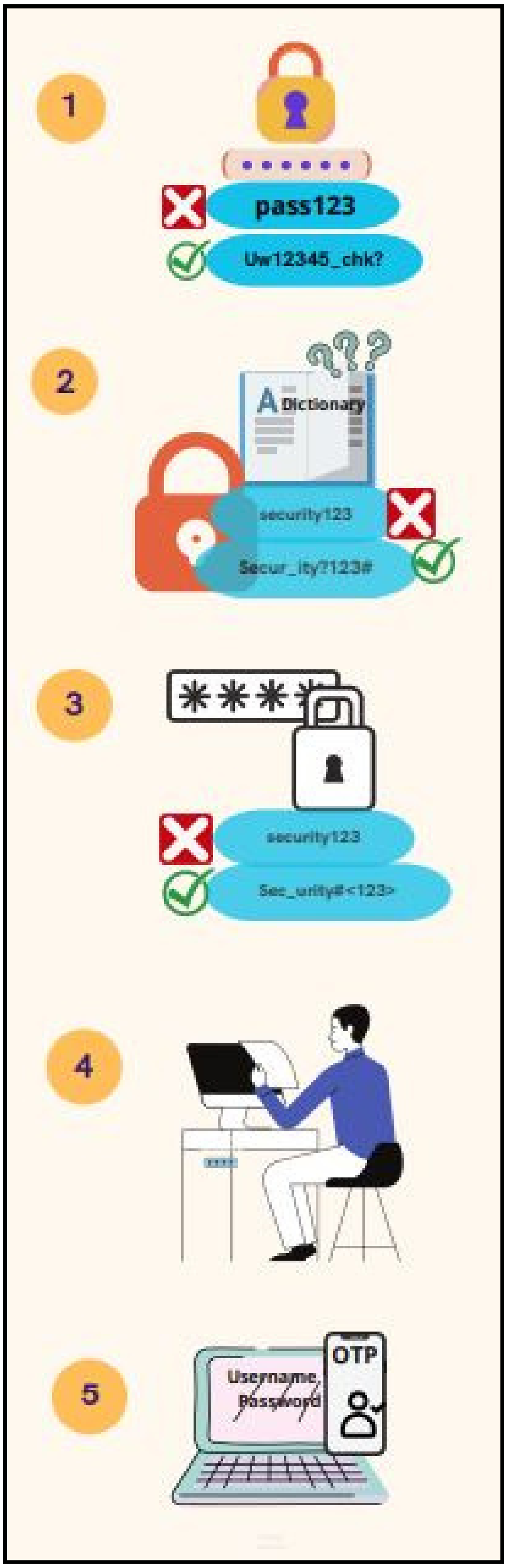
1. If an individual is causing trouble to you or others, it is recommended to block and report them to the social media platform and other concerned agencies.
2. Set the privacy settings on your social media accounts to prevent unauthorized individuals from viewing, chatting, or tagging your content.
3. Exercise caution while accepting friend requests or responding to strangers in social media.
4. Restrict visibility to your posts and profile information.
5. Avoid sharing personal and sensitive details online through posts or chats.
6. Disable automatic addition to unknown groups without your permission.
7. Keep a record of all online or virtual workplace discomforts and document every aspect of your work environment.
8. Exercise caution while sharing photos online. If you are becoming a victim of any cyber frauds or cyber harassments report to the nearest police station or report at https://www.cybercrime.gov.in or call 1930.

BEST PRACTICES FOR MORPHING



1. Enable your security and privacy features on social media accounts.
2. Never share your personal pictures online publicly on social media accounts.
3. Enable multi-factor authentication with strong passwords for your social media accounts.
4. Save the evidence and the screen shots for referring to the incident later.
5. Don’t suffer in silence, know that you are not alone, reach out and seek help from trusted family and friends.
6. If you observe your fake profile or any such objectionable posts in social media, report to the respective social media help centre .

BEST PRACTICES FOR PASSWORD MANAGEMENT



1. Use Strong and long passwords Always prefer to create lengthy passwords. Short length passwords are easy to crack
2. Don't use dictionary words as passwords Such passwords are too easy to crack.
3. Create passwords using special characters Passwords mixed with uppercase, lowercase, numerals and special characters are difficult to crack
4. Change passwords periodically Avoid using guessable patterns of password.
5. Enable Multi Factor Authentication MFA adds another layer of security to your accounts.

CYBER SAFETY TIPS FOR FOR WOMEN

DO's

1. Be selective about what information you make public. Sensitive information includes real name, date of birth, gender, town, e-mail address, school name, place of work, and personal photos.
2. Block people you don't want to interact with.
3. On WhatsApp and other messaging apps, ensure that 'media auto-download' is deactivated, especially from senders who are not in your contact list.
4. Use strong passwords and use different passwords for different accounts.
5. Contact the nearest PS immediately if you feel your privacy/safety has been compromised online. You can also report your problems online at https://cybercrime.gov.in or https://jofs.jhpolice.gov.in
6. Be extremely cautious while posting photographs and control who can view them.
7. On social media accounts keep your privacy settings to the most stringent levels. Only share information about yourself on 'need to know' basis.
8. Periodically review your internet contacts and online activities.

DON'ts

1. Never, try to meet a person with whom you've interacted only online without taking somebody else along and such meetings must always be in a public place.
2. Don't trade personal information for "freebies.".
3. Don't post personal information such as mobile numbers and personal email ids on social networking sites.
4. Don't accept a friend request only on the basis that the person is a mutual friend of a friend of yours.
5. Don't click on unsolicited links sent over Facebook messenger or other messaging services, even if they are sent from your friend's account.
6. Don't share any OTP or other passwords, even with friends.
7. Don't accept "friend requests" from people totally unknown to you and from those with whom you don't want to interact with.
8. Don't share your password with anyone or let anybody else handle your account.

GENERAL CYBER SAFETY TIPS

For Device/Computer Security

1. Keep your antivirus and operating system updated at all times. ▫ Backup your sensitive/important data at regular intervals.
2. Be careful while opening suspicious web links/URLs.
3. Always scan external storage devices (e.g. USB) for viruses, while connecting to your device.
4. To prevent unauthorized access to your device, consider activating your wireless router's MAC address filter to allow authorized devices only.
5. Wireless router can screen the MAC addresses of all devices connected to it, and users can set their wireless network to accept connections only from devices with MAC addresses recognized by the router.
6. Secure all your wireless access points with a strong password.
7. Hackers usually scan for open access points and may misuse it to carry out unwanted activities.
8. Log records may make you more vulnerable for such misuse.
9. Merely deleting sensitive material is not sufficient, as it does not actually remove the data from your device.
10. 'File Shredder Software' should be used to delete sensitive files on computers. ▫
11. Delete unwanted files or data from your computer device. It prevents unauthorized access to such data by others.
12. Use 'Non-Administrator Account' privileges for login to the computer and avoid accessing with 'Administrator' privileges for day-to-day usage of computers. ▫
13. Make sure to install reputed mobile anti-virus protection to protect your mobile from prevalent cyber threats and also keep it updated.
14. In case of loss or theft of your mobile device, immediately get your SIM deactivated and change passwords of all your accounts, which were configured on that mobile.
15. Do not leave your phone unattended in public places and refrain from sharing your phone password/ pattern lock with anybody.
16. Always enable a password on the home screen to restrict unauthorized access to your mobile phone.
17. Configure your device to automatically lock beyond a particular duration.
18. Always lock your computer before leaving your workplace to prevent unauthorized access.
19. A user can lock one's computer by pressing 'Ctrl +Alt + Del' and choosing 'Lock this Computer' or "Window button+ L".
20. Remove unnecessary programs or services from computer which are not required for day to day operation.

GENERAL CYBER SAFETY TIPS

For safe Internet Banking

1. Beware of various fraudulent lucrative advertisements regarding discount coupons, cashback and festival coupons offering payments through UPI apps popping up while browsing.
2. Some URL links on the internet are advertising to provide fake mobile Oximeter apps to check your oxygen level.
3. Do not download such fake Oximeter apps on your mobile, as these apps may steal your personal or biometric data from your mobile phone.
4. Avoid using third-party extensions, plug-ins or add-ons for your web browser as it may track your activity and steal your personal details.
5. Always browse/visit the original website for purchasing.
6. Always type the information in online forms and not use the auto-fill option on web-browser to fill online forms as these forms may store your personal information such as card number, CVV number, bank account number etc.
7. Be careful about the name of a website.
8. A malicious website may look identical to a legitimate one, but the name may use variation in spelling or a different domain (eg.,[dot]com, [dot]net etc.)
9. In general all the government websites have [dot]gov[dot]in or [dot]nic[dot]in ending.
10. Avoid clicking 'Keep me logged in' or 'Remember me' options on websites, especially on public computers.
11. Beware of fraudulent charity activities or non-existent charitable organizations having names identical to government charity funds, requesting money for victims, products or research.
12. Always check the credentials of charity organizations before donation.
13. Never allow the browser to store your username/password, especially if you use a shared computer device.
14. Also make it a habit of clearing history from the browser after each use session to protect your privacy.
15. Be cautious with tiny or shortened URLs (it appears like http://tiny.cc/ba1j5y). Don't click on it as it may take you to a malware infected website.
16. Prior to registering on a job search portal, check the privacy policy of the website to know the type of information collected from the user and how it will be processed by the website.
17. Many social networking sites prompt to download a third-party application that lets you access more pages.
18. Do not download unverified third-party applications without ascertaining its safety.
19. Beware of e-commerce websites and advertisements selling items at highly discounted prices.

GENERAL CYBER SAFETY TIPS

For Safe Internet Browsing

1. Always use virtual keyboard for accessing net banking facility and log off from banking portal/website after completion of online transaction.
2. Also ensure deletion of browsing history from web browser (internet explorer, chrome etc.) after completion of online banking activity.
3. Use multiple factor authentications for login into your bank accounts.
4. Avoid writing down or storing in mobile phones the information used to access digital wallets/bank accounts.
5. One should not use the same password for internet banking of all accounts.
6. One should not keep the same mobile number registered for all bank accounts.
7. Always enable getting notification of transactions from the banks via both SMS & e-mail.
8. Login and view your bank account activity regularly to make sure that there are no unapproved transactions.
9. Report discrepancies, if any, to your bank immediately.
10. It is preferable to have two separate e-mail accounts, one for communicating with people and another for your financial transactions.

GENERAL CYBER SAFETY TIPS

For E-wallet Security

1. Enable password/PIN on your mobile phones, tablets & other devices that you use.
2. While doing transactions using your e-wallet, you should never save the details of your debit or credit cards.
3. Use multiple factor authentication for logging into your e-wallets.
4. Avoid writing down information used to access the digital wallets in mobile phones.
5. Install e-wallet accounts from sources you trust.
6. Do not install e-wallet apps via links shared over email, SMS or social media.
7. Always verify and install authentic e-wallet apps directly from the app store (Google/ iOS store) on your smart phone.
8. Please check if the app is having the “Play Protect” shield.

GENERAL CYBER SAFETY TIPS

For E-mail Account Security

1. Never keep the same password for all your e-mail accounts. □
2. Use secure network connections.
3. Avoid the use of public Wi-Fi networks.
4. More secure Wi-Fi connections require passwords & are easily identified as “WPA or WPA2”.
5. Highly insecure Wi-Fi is open for anyone to connect to & may be labelled as a “WEP” (Wired Equivalent Privacy).
6. Don't click on the links provided in suspicious e-mails even if they look genuine as this may lead you to malicious websites and this may be an attempt to defraud your hard earned money.

GENERAL CYBER SAFETY TIPS

For Identity Proof Card's Security

1. Never leave the discarded photo copy of your identity proof card at shops.
2. Never allow the shopkeeper to keep a copy of your identity proof card in their computer.
3. Never share your identity proof cards to unknown persons on social media platforms including WhatsApp.
4. Never share your property papers or other personal information on social media platforms.

For Password Security

1. Keep a strong password of at least 13 characters with alphanumeric, special character, upper case & lower case combination.
2. Keep two factor authentication for all your accounts.
3. If you suspect that any of your account has been hacked, immediately change the password and contact the nearest Police Station.

HOW TO MAKE CYBER CRIME COMPLAINTS ?

- Compliant to Cyber Crime Helpline Number

1930

- Register a Complaint On Website

cybercrime.gov.in

- Register a Complaint By Visiting Nearest Cyber Police Station

---

HOW TO MAKE COMPLAINTS IF YOU LOST YOUR MOBILE PHONE ?

- Register a Complaint On Sanchar Saathi Website

sancharsaathi.gov.in

कोयला मंत्रालय
Ministry of Coal

FAKE JOB OFFERS

"आसान नौकरी के झांसे में न आएं!"

नकली जॉब ऑफर्स से बचाव ही सुरक्षा है
जल्दी नौकरी, ज़्यादा सैलरी – ये हो सकता है धोखा

🟥 *"सावधान! ये संकेत हो सकते हैं नकली जॉब के"*

- प्रोसेसिंग फीस या सिक्योरिटी डिपॉजिट की मांग
- इंटरव्यू के बिना सीधा ऑफर
- संदिग्ध वेबसाइट या ईमेल आईडी
- सरकारी नौकरी का वादा निजी एजेंसी द्वारा

"ना OTP दें, ना डॉक्यूमेंट – पहले जाँचें, फिर भरोसा करें!"

"सतर्क रहें, सुरक्षित रहें!"

Follow us on

Western Coalfields Limited

कोयला मंत्रालय
Ministry of Coal

"CRYPTOCURRENCY SCAM"

"लालच से नुकसान – नकली Crypto ऐप्स और मैसेज से रहें सावधान!"

- "Crypto स्कीम में तुरंत कमाई का दावा = धोखा"
- "फर्जी Crypto ऐप्स आपके पैसे और डाटा चुरा सकते हैं।"

सावधानी के उपाय :

- ☑ अनजान ऐप या वेबसाइट से दूर रहें
- ☑ सरकारी मान्यता न होने पर निवेश न करें
- ☑ किसी मैसेज या कॉल से प्रभावित न हों
- ☑ Crypto का मतलब हमेशा Risk – लालच नहीं समझदारी चुनें

"सतर्क रहें, सुरक्षित रहें"

Follow us on

Western Coalfields Limited

कोयला मंत्रालय
Ministry of Coal

सत्यमेव जयते
भारत सरकार

कोल इण्डिया
Coal India

"सस्ता दिखे, तो सोचें"

ONLINE SHOPPING FRAUD

👀 चौंकाने वाले डिस्काउंट ? सोचिए फिर से!

💻 नकली वेबसाइटें बना रही हैं आपको निशाना।

🔍 पहचानें स्कैम साइट को:

- ✅वेबसाइट का URL ध्यान से पढ़ें।
- ✅बिना रिव्यू और भरोसे के साइट से न खरीदें।
- ✅UPI पेमेंट से पहले सोचें!
- ✅अजीब डोमेन नाम (जैसे .XYZ, .STORE) से बचें।

"सतर्क रहें, सुरक्षित रहें"

Follow us on

Western Coalfields Limited

कोयला मंत्रालय
Ministry of Coal

तकनीकी सहायता के नाम पर धोखा!

Tech Support Scam

📢 चेतावनी:

✅ कोई भी तकनीकी कंपनी बिना शिकायत के आपको कॉल नहीं करती।

🚫 स्क्रीन शेयर या रिमोट एक्सेस की इजाजत न दें।

🔒 अपनी निजी जानकारी और OTP किसी से साझा न करें।

"सतर्क रहें, सुरक्षित रहें"

Follow us on

Western Coalfields Limited

12:00
100%
Secure Payment
OTP Password
* * * *
Ent

कोयला मंत्रालय
Ministry of Coal
सत्यमेव जयते
भारत सरकार

कोल इण्डिया
Coal India

OTP FRAUD आप भी हो सकते है इसके शिकार

"OTP कभी शेयर न करें!"

"किसी भी कॉल, मैसेज या लिंक पर अपना OTP न दें।"
"बैंक, कंपनी या ऐप आपसे OTP नहीं मांगते।"

Unknown Caller = Danger

OTP = Personal Secret

No Share = No Scam

"अगर कोई OTP मांगे – समझिए फ्रॉड है!"

"सतर्क रहें, सुरक्षित रहें!"

Western Coalfields Limited

कोयला मंत्रालय
Ministry of Coal
सत्यमेव जयते
भारत सरकार

कोल इण्डिया
Coal India

PHISHING FRAUD

"नकली लिंक से सावधान – एक क्लिक से हो सकता है बड़ा नुकसान!"

"ऐसे फर्जी लिंक पर क्लिक मत कीजिए!"

ALERT

🚨 पहचानिए फिशिंग लिंक के संकेत

- ☑ लिंक में अजीब या गलत स्पेलिंग
- ☑ मेल/मैसेज में डर फैलाने वाली भाषा (जैसे "तुरंत कार्रवाई करें")
- ☑ अविश्वसनीय ईमेल ID या डोमेन

✅ सावधानी के उपाय :

- ☑ हमेशा लिंक ध्यान से जांचें
- ☑ https और सही डोमेन पर भरोसा करें
- ☑ जरूरी हो तो सीधे वेबसाइट पर जाकर लॉगिन करें
- ☑ कभी भी OTP या पासवर्ड किसी से साझा न करें

सुरक्षित रहें, सतर्क रहें – आपकी सुरक्षा आपके हाथ में है।

Follow us on

Western Coalfields Limited

कोयला मंत्रालय
Ministry of Coal

सत्यमेव जयते
भारत सरकार

कोल इण्डिया
Coal India

LOAN APP TRAP

❗ "आसान लोन, भारी फंसाव"

- नकली लोन ऐप्स निजी डेटा चुराते हैं
- गैलरी, कॉन्टैक्ट्स तक पहुंच लेकर धमकी देते हैं!
- ब्याज कई गुना वसूलते हैं — बिना जानकारी के!

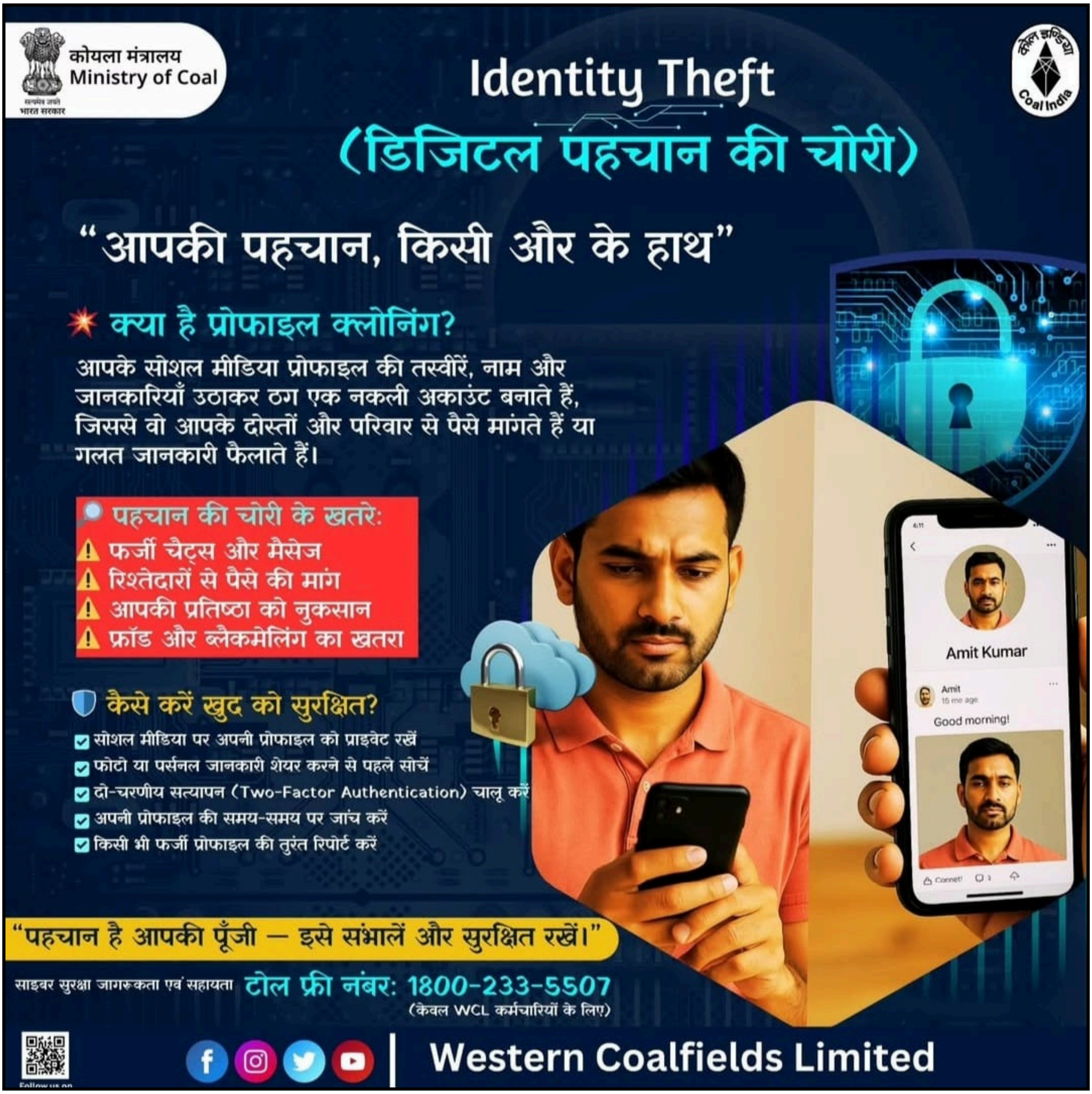
⚠ सावधानी के उपाय

- ✓ केवल RBI-रेगुलेटेड ऐप्स से लोन लें
- ✓ Permissions देते समय सतर्क रहें
- ✓ अनजान लिंक, कॉल या ऐप से बचें

"सतर्क रहें, सुरक्षित रहें"

"पैसे लौटाओ वरना फोटो वायरल करेंगे!"
Instant Loan Approved:
₹5000

Follow us on | Western Coalfields Limited



Identity Theft
(डिजिटल पहचान की चोरी)

"आपकी पहचान, किसी और के हाथ"

✷ क्या है प्रोफाइल क्लोनिंग?

आपके सोशल मीडिया प्रोफाइल की तस्वीरें, नाम और जानकारियाँ उठाकर ठग एक नकली अकाउंट बनाते हैं, जिससे वो आपके दोस्तों और परिवार से पैसे मांगते हैं या गलत जानकारी फैलाते हैं।

पहचान की चोरी के खतरे:

⚠ फर्जी चैट्स और मैसेज
⚠ रिश्तेदारों से पैसे की मांग
⚠ आपकी प्रतिष्ठा को नुकसान
⚠ फ्रॉड और ब्लैकमेलिंग का खतरा

कैसे करें खुद को सुरक्षित?

☑ सोशल मीडिया पर अपनी प्रोफाइल को प्राइवेट रखें
☑ फोटो या पर्सनल जानकारी शेयर करने से पहले सोचें
☑ दो-चरणीय सत्यापन (Two-Factor Authentication) चालू करें
☑ अपनी प्रोफाइल की समय-समय पर जांच करें
☑ किसी भी फर्जी प्रोफाइल की तुरंत रिपोर्ट करें

"पहचान है आपकी पूँजी — इसे संभालें और सुरक्षित रखें।"

साइबर सुरक्षा जागरूकता एवं सहायता **टोल फ्री नंबर: 1800-233-5507**
(केवल WCL कर्मचारियों के लिए)

Western Coalfields Limited

कोयला मंत्रालय
Ministry of Coal
सत्यमेव जयते
भारत सरकार

कोल इण्डिया
Coal India

"फर्जी अधिकारी का झांसा!"

Fake Police Call

"सतर्क रहें,

सुरक्षित रहें"

● "पुलिस कभी फोन पर पैसे नहीं मांगती!"

👮‍♂️ असली पुलिस कभी धमकी देकर भुगतान नहीं कराती

📞 नंबर की पुष्टि करें – डरें नहीं, सोचें

⚠ सावधानी के उपाय:

✅कॉलर का नाम और नंबर जांचें

✅ डरावनी भाषा पर तुरंत भरोसा न करें

✅ किसी को UPI या बैंक डिटेल न दें

✅ ज़रूरत हो तो स्थानीय थाने में संपर्क करें

Follow us on

Western Coalfields Limited

WIN
REWARDS
⚠ MONEY
DEBITED

कोयला मंत्रालय
Ministry of Coal
भारत सरकार

Coal India

QR CODE SCAM

हर QR कोड भरोसेमंद नहीं!

**कहीं ठगी के जाल में तो नहीं फंस रहे आप?
स्कैन करने से पहले सोचें
हर QR कोड रिवार्ड नहीं, नुकसान भी हो सकता है!**

🕵️‍♂️ QR कोड फ्रॉड कैसे होता है?

- धोखेबाज़ नकली QR कोड भेजते हैं (WhatsApp/SMS या फिजिकल पेपर पर)
- "पैसे पाने" के बहाने आपको स्कैन कराते हैं
- स्कैन करते ही आपके बैंक अकाउंट से पैसे उड़ जाते हैं

🛡 सावधान रहें:

✅ अनजान QR कोड कभी स्कैन न करें
✅ केवल पैसे भेजने के लिए QR कोड स्कैन करें, पैसे पाने के लिए नहीं
✅ पेमेंट रिक्वेस्ट्स की डिटेल्स ध्यान से पढ़ें
✅ QR कोड स्कैन करने के बाद कोई भी PIN/OTP न डालें

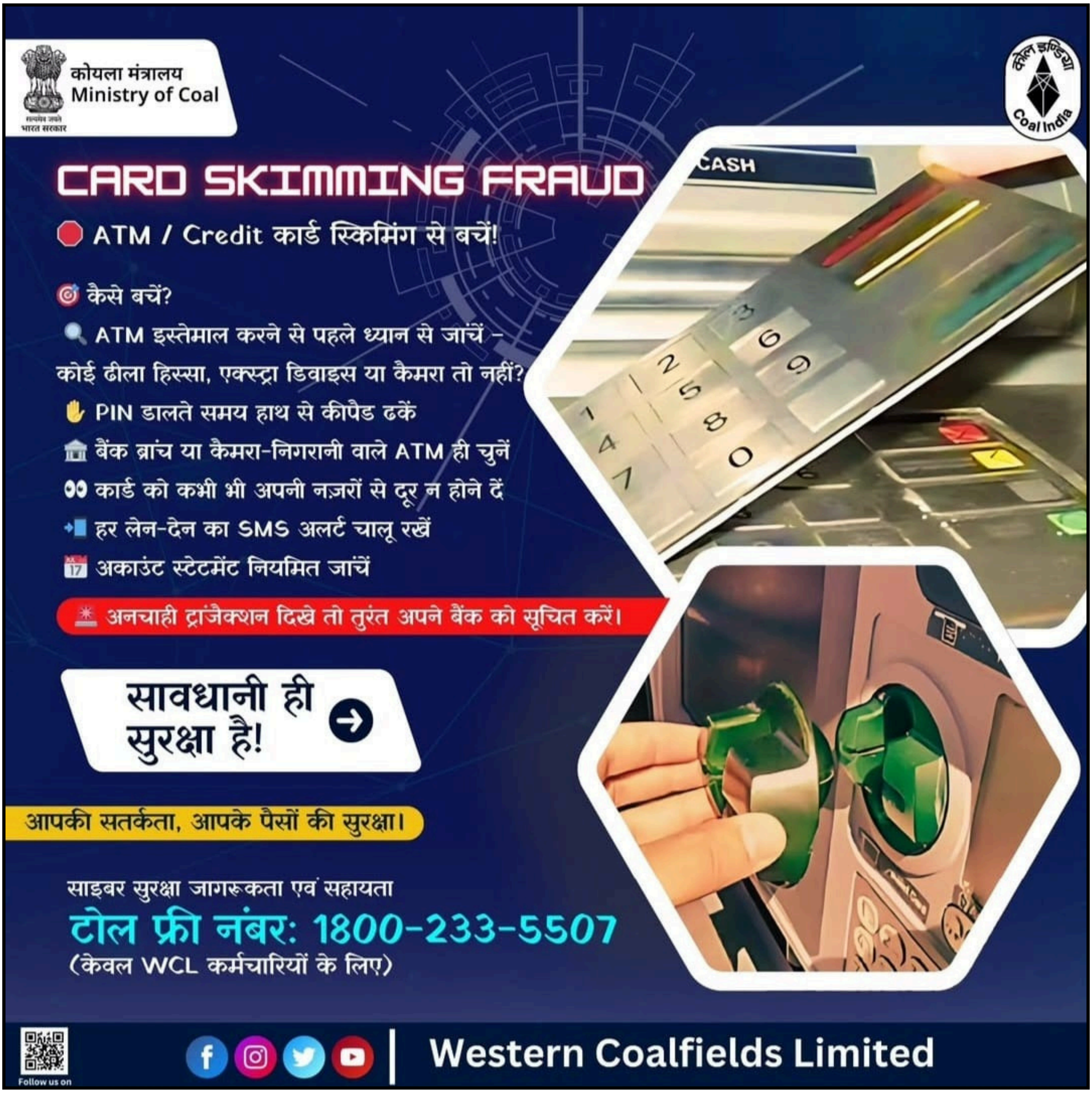
आपकी सतर्कता, आपके पैसों की सुरक्षा।

साइबर सुरक्षा जागरूकता एवं सहायता

टोल फ्री नंबर: 1800-233-5507
(केवल WCL कर्मचारियों के लिए)

Follow us on
linktr.ee/TEAM_WCL

Western Coalfields Limited



सत्यमेव जयते
भारत सरकार

कोयला मंत्रालय
Ministry of Coal

कोल इण्डिया
Coal India

CARD SKIMMING FRAUD

🛑 ATM / Credit कार्ड स्किमिंग से बचें!

🎯 कैसे बचें?

🔍 ATM इस्तेमाल करने से पहले ध्यान से जांचें – कोई ढीला हिस्सा, एक्स्ट्रा डिवाइस या कैमरा तो नहीं?

✋ PIN डालते समय हाथ से कीपैड ढकें

🏛 बैंक ब्रांच या कैमरा-निगरानी वाले ATM ही चुनें

👀 कार्ड को कभी भी अपनी नज़रों से दूर न होने दें

📲 हर लेन-देन का SMS अलर्ट चालू रखें

📅 अकाउंट स्टेटमेंट नियमित जांचें

🚨 अनचाही ट्रांजैक्शन दिखे तो तुरंत अपने बैंक को सूचित करें।

सावधानी ही सुरक्षा है! ➔

आपकी सतर्कता, आपके पैसों की सुरक्षा।

साइबर सुरक्षा जागरूकता एवं सहायता

टोल फ्री नंबर: 1800-233-5507

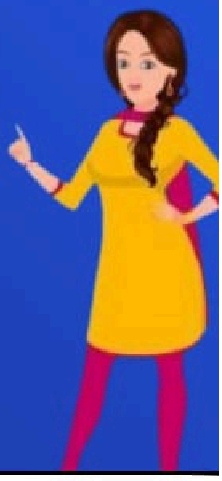
(केवल WCL कर्मचारियों के लिए)

Follow us on

Western Coalfields Limited

सुरक्षा विभाग
सक्षम सर्वोत्तम सर्वज्ञ

"OTP
कभी शेयर
न करे"



DO NOT SHARE YOUR OTP

with a stranger or a person asking for a verification code for any purpose. It could be a fraud.

OTP FRAUD

आप भी हो सकते है इसके शिकार

अगर कोई OTP मांगे
समझिये फ्रॉड है

किसी भी कॉल, मैसेज या लिंक पर अपना OTP न दे।
"बैंक , कंपनी या एप्लीकेशन आपसे OTP नहीं मांगते|

"सतर्क रहे ,सुरक्षित रहे।"

PLEASE CALL FOR
ANY QUERY

18002335506

सुरक्षा विभाग
सक्षम सर्वोत्तम सर्वज्ञ

FAKE JOB OFFER SCAM

"आसान नौकरी के झासे मे ना आए"!!!!

नकली जॉब ऑफर्स से बचाव ही सुरक्षा है। जल्दी नौकरी, ज़्यादा सैलरी ये हो सकता है धोखा.!!!!!

"सावधान! ये संकेत हो सकते हैं नकली जॉब के"

1. प्रोसेसिंग फीस या सिक्योरिटी डिपॉजिट की मांग!
2. इंटरव्यू के बिना सीधा ऑफर!
3. संदिग्ध वेबसाइट या ईमेल आईडी!
4. सरकारी नौकरी का वादा निजी एजेंसी द्वारा!

Please Call For Any Query
18002335506

"सतर्क रहें, सुरक्षित रहें!"

Follow us on

Western Coalfields Limited

वे.को.लि.

सुरक्षा विभाग

(सक्षम, सर्वोत्तम, सर्वज्ञ)

WESTERN COALFIELDS LIMITED

Coal Estate, Civil Lines, Nagpur