With Omni present cyber space, criminals have become more desperate and sophisticated indulging in financial frauds through ATM/ Debit/ Credit card and Internet.

CYBER SAFETY IS OUR SHARED RESPONSIBILITY
#Never share your Username and Password.

#Avoid login from other Mobiles & Computers.

#Use a strong Password

#Change your Password at regular intervals.

#Use Antivirus & Antispyware

#Run Updates regularly

#Use Encryption

CYBER SAFETY IS OUR SHARED RESPONSIBILITY
Most popular Modus Operandi of Cyber Criminals in Jharkhand

Cyber criminal call the victim (Criminal call random mobile number Pan India)

Criminal pretend to be authentic authority of Bank, Investment Company etc and ask for victim ATM card number

As victim gives the same to cyber criminal, they transfer the money to the E-wallet

During the process of transferring the money to e-wallet OTP (One Time Password) generated which goes to victim mobile

As the OTP goes to Victim Mobile phone he/she find the criminal authentic person as result victim gives the highly sensitive OTP to the CYBER CRIMINAL

As soon as Cyber Criminal gets the OTP Money from Victim Account is transferred to e-wallet of the Criminal

Using their e-wallet criminal either perform online shopping or transfer the money to their own account

Note: e-wallet can be generated using registered mobile number
Second popular Modus Operandi of Cyber Criminals in Jharkhand

Develop Apps

Upload to Google Play Store

Person Using Smart phones download the app

If persons uses the internet banking through their smart phone their user Id & password goes to criminal email or website (criminal’s website) which he specifically created to store the credential of persons

User login to app **Bank website opens**, then user enter the user ID & Password for internet banking , the credential goes to criminal email or website (criminal’s website) which he specifically created to store the credential of persons

Using that credential cyber criminal transfer Amount from person account to their e-wallet (Digital wallet which can be used for mobile recharge, online shopping, etc/ any type of online transaction)

Using their e-wallet criminal either perform online shopping or transfer the money to their own account
This is Anjali,
Anjali is on Facebook
Anjali got a friend request from a stranger
Anjali didn't accept it
Anjali is SMART, be like Anjali

"NEVER ACCEPT OR SEND FRIEND REQUEST TO STRANGERS"

CYBER SAFETY IS OUR SHARED RESPONSIBILITY
Card security tips

Don't
- Seek help from strangers/Security Guards at ATMs
- Share your PIN number with anyone
- Give away your Debit Card details to anyone on incoming calls/emails
- Purchase from a company online should you have any doubts whatsoever
- Throw away your Card receipts without shredding them, they might contain your card information

Do
- Get your Debit card receipts and keep them for reconciliation
- Sign your new card as soon as you receive it
- Keep your card in sight all the time at Point of Sale
- Keep your card and PIN details separate
- Report to the bank immediately if your card is lost or stolen
- Check receipt slips against the amount reflected on the statement
Use a strong password (a combination of upper and lower case letters, symbols and numbers).

Don’t believe everything you read - make sure you know it’s coming from a reliable source.

Don’t give out any private information over the internet or through mobile phones about you, your family, friends or other people that you know.

Think before you send! You have to think about what you are saying and how the recipient/s may feel.

Don’t hide behind a computer screen, if you wouldn’t say it to their face, don’t say it at all!

Don’t post inappropriate or illegal content anywhere on the internet.

Make sure your social networking profile is set to private (check your security settings).

Only accept friend requests from people you actually know - even if it is a friend of a friend it’s not a good idea to add them unless you actually know them.

Tell your friends to ask for your permission before uploading and/or tagging a photo of you on their social networking profiles.

Don’t click on any links that are embedded in emails - type the URL into the browser and go from there.
Stay Safe Online

Remember the 5 SMART rules when using the internet and mobile phones.

S - Safe: Keep safe by being careful not to give out personal information – such as your full name, email address, phone number, home address, photos or school name – to people you are chatting with online.

M - Meet: Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents’ or carers’ permission and even then only when they can be present.

A - Accepting: Accepting emails, IM messages, or opening files, pictures or texts from people you don’t know or trust can lead to problems – they may contain viruses or nasty messages!

R - Reliable: Information you find on the internet may not be true, or someone online may be lying about who they are. Make sure you check information before you believe it.

T - Tell: Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.
“The term ‘Internet fraud’ refers generally to any type of fraud scheme that uses one or more components of the Internet - such as chat rooms, e-mail, message boards, or Web sites - to present fraudulent solicitations to prospective victims, to conduct fraudulent transactions, or to transmit the proceeds of fraud to financial institutions or to other connected with the scheme.”
TOOLS USED FOR INTERNET FRAUDS

- Email
- Chat rooms
- Websites
- Message Boards
- Portals
- Web Application
<table>
<thead>
<tr>
<th>Types of Internet Frauds</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credit/Debit Card Fraud</td>
</tr>
<tr>
<td>Business Deceit</td>
</tr>
<tr>
<td>Recruitment Deceit</td>
</tr>
<tr>
<td>Counterfeit Cheque Scam</td>
</tr>
<tr>
<td>Advance Fee Fraud</td>
</tr>
<tr>
<td>Non-Delivery of Goods/Service Fraud</td>
</tr>
</tbody>
</table>
TYPES OF INTERNET FRAUDS

- Spoofing/Phishing Scam
- Investment Rip-Off
- Identity Theft
- Ponzi/Pyramid Fraud
- Auction Fraud
- Nigerian 4-1-9 Scam
CREDIT/ DEBIT CARD FRAUD

This involves the use of credit/debit card to obtain money or acquire properties without appropriate authorization.

Fraudsters obtain credit/debit card numbers of victims from unsecured web media and use them carry out illegal or unethical transactions.
In this case, fraudsters masquerade themselves as genuine business people and attempt to collect personal information such as passwords, PIN numbers and date of birth from respondents, in order to use the data for purchasing goods which would most likely be transferred or shipped out of the country.
Generic public or private job or recruitment portals can be used for advertising spurious job openings with the intention to collect vital information from applicants, and deploy them for purchasing goods or use for some other illegal purposes.
COUNTERFEIT CHEQUE SCAMS

This entails the use of counterfeit cheque to pay for goods purchased online, such that the face value of the cheque would be far higher than the requirement; thus the seller would be instructed to return the overage amount to an account.
ADVANCE FEE FRAUD

This is popularly known as 4-1-9. It refers to the type of fraud in which a substantial amount would be demanded for payment of processing fees that stand as requirement for release of non-existing merchandise or large amount of money.

NON DELIVERY OF GOODS/ SERVICES FRAUD

This refers to scam in which people are encouraged to pay for goods and or service via a web portal, and thereafter nothing would be delivered to the buyers.
Spoofing is a type of fraud in which a fraudster masquerades as another person by using another person’s identity to transact business and obtain information such as bank account numbers, credit card numbers and associated passwords.

Phishing is a form of spoofing in which the webpage of a particular entity can be duplicated and positioned with URL for the purpose of luring people to divulge vital information.
IDENTITY THEFT

This entails the use of another’s personal information without appropriate consent, for the purpose of fraudulent practices.

Often personal information may even be leaked online or stolen during web surfing.
This is a system of luring investors to invest in a scheme in which the investment firm promises abnormally high returns, meanwhile the early investors shall be paid with investment capital obtained from successive investors. The payment chain would continue till the point of collapse.
AUCTION FRAUD

In this auction frauds, people are encouraged to participate in online auction and when money must has been paid for specific items, the fraudster would send either a lower standard item or counterfeit.
HOW TO BE SAFE FROM INTERNET FRAUDS?

1. Know who you’re dealing with.
2. Look for information about how complaints are handled.
3. Be aware that no complaints is no guarantee.
4. Don’t believe promises of easy money. Understand the offer.
5. Resist pressure.
Different types of scams

Investment scams
Generally targeted at the 55+ age group and are often sophisticated enough to lure in even experienced investors. Also called “boiler room” scams because they use high pressure sales to create a sense of urgency, they may offer shares, or a range of investment “opportunities.”
Different types of scams

Courier scams

Usually start with an unsolicited telephone call or text advising that a bank fraud has been detected. The scam is completed when the caller attends the victim’s home or uses an innocent courier to collect their bank card.
Different types of scams

Computer software service scam
Victims are cold called and told that there is a problem with their computer. They are talked through the logon steps so the fraudster can gain remote access to the computer, for which they charge “fees” and gain access to personal and financial information.
Different types of scams

Advance fee scams
Scammers get people to send money for a range of dodgy or non-existent goods and services - or to collect lottery “winnings”.
Key messages: Top tips to avoid scams

- If you haven’t bought a ticket - you can’t win it.
- You shouldn’t have to pay anything to get a prize.
- Contacted out of the blue - be suspicious.
- Don’t be rushed - resist pressure to make a decision straight away.
- Your bank will never phone you to ask for your PIN or your online banking password.
- Genuine computer firms do not make unsolicited phone calls to help you fix your computer.
ATM Frauds and Solutions
ATM FRAUDS

In general ATM fraud can include any deliberate 'criminal' technique which involves the use of an ATM to obtain something of value.

Attacks against ATMs may be classified as

ATM physical attacks (fraudulently ATM card is exchanged) and ATM fraud.
• More than 70 percent of financial institutions experienced an increase in ATM/debit card fraud claims in 2011

• The U.S. Secret Service reports $8.5B in annual U.S. credit card fraud losses, including ATM skimming.

• Ram raids are those threats when criminals physically break out ATMs from the wall at the institution.

• Criminals go through the financial institution’s telephone banking service to change PIN numbers.
Types of ATM frauds

- Card Theft
- PIN Compromise
- Card Skimming
- Cash Trapping
- Transaction Reversal
- Deposit Fraud.
What is ATM Skimming

- ATM skimming Device card reader which can be disguised to look like a part of the machine. The card reader saves the users’ card number and pin code, which is then replicated into a counterfeit copy for theft.

- It help criminals in
  a) Knowing Account information
  b) Pin compromise

- ATM card entry slot skimmers have various shapes and sizes
How PIN is Compromised

- It's obtaining debit card information by unauthorized individual.
- Shoulder surfing or using use of a miniature camera.
- Video surveillance
- Hidden video camera
- Overhead cell phone camera
- Remotely positioned cameras
- PIN pad overlay
ATM System Attacks

- Criminal attempts to penetrate ATM network, violate confidentiality, integrity, and/or authenticity of transaction data.

- Malicious software (i.e., viruses, worms, Trojans, rootkits, etc.) installed on ATM’s computer systems
How to avoid ATM Frauds

- Fraud Prevention
- Physical Protection
- System Security
- Intelligent Monitoring
- Consultancy
- Consumer Safety
Fraud Prevention

• Shield your hand when you enter in your PIN

• Ensure that no one is peeking or shoulder surfing while you are entering PIN.

• Avoid using ATMs in isolated locations

• Always prefer **ATM machines** near Bank Branch.
ATM Skimming

- Never follow a link in a bank email notice if you find it suspicious. Visit your bank's website and search for latest updates.

- Examine the ATMEquipment carefully for any skimming devices.

- Look for 'extra' cameras other than general ATM security camera.

- Check the ATM card slot properly before using it.
Do’s & Don’t’s

Safety Tips to avoid cybercrime

• Keep your operating systems up to date with critical security updates and patches.
• Don’t open emails or attachments from unknown sources.
• Read Privacy policy carefully when you submit the data through internet.
• Disable Remote Connectivity.
• Use hard-to-guess passwords. Don’t use words found in a dictionary. Remember that password cracking tools exist.
• Back-up your computer data on disks or CDs often.
• Use antivirus software and firewalls – keep them up to date.
**DOs & DON'Ts**

1. Do not give your phone number at public places or conduct transactions on public terminals.

2. If you change houses, inform the bank so that cards and statements are sent to the right address.

3. Check your bank and credit card statements. If you notice irregular charges, notify the bank.

4. Conduct ATM transactions preferably only at machines located inside bank branches.

5. Do not leave if ATM stalls. Report to security guard or bank official, or call up the bank.
Warning signs:

- 493 profile views

It requires extra steps to view (e.g. you must complete a survey and re-share a message first)

- The content is shocking or salacious (e.g. celebrity sex tapes)

- It promises something Facebook would never do (e.g. allows you to see profile views)

Avoid being a victim:

- Research apps or plugins before installing them (Google: 'app name' + 'scam')

- Be aware of the functionality limitations Facebook has (e.g. there's no 'dislike' button - no matter what you download)

- Check to see which Facebook apps you've granted permission to (Go to 'Settings', then select 'Apps') - remove any suspicious apps you don't recall downloading
Lets be alert ! & make the cyber Space safe

*Cyber Crime is a function of opportunities victims provide to the smart offenders*