**Scamsters again trying to call you ??**
Read more to avoid such call in the future through

**Be Aware while Using QR Code.**
Read more to learn about importance and usage of QR Code.

**Are you a victim of ATM Card Skimming Fraud ?**
Read more about frauds related to ATM cards and about Skimmings.

DSEU
Crafting Excellence

# THE FINANCIAL MINUTE

A Student Initiative of DSEU Dwarka

## Don't be a BABU RAO in Real life !!!

# ISSUE 05 *September 2022 Edition*

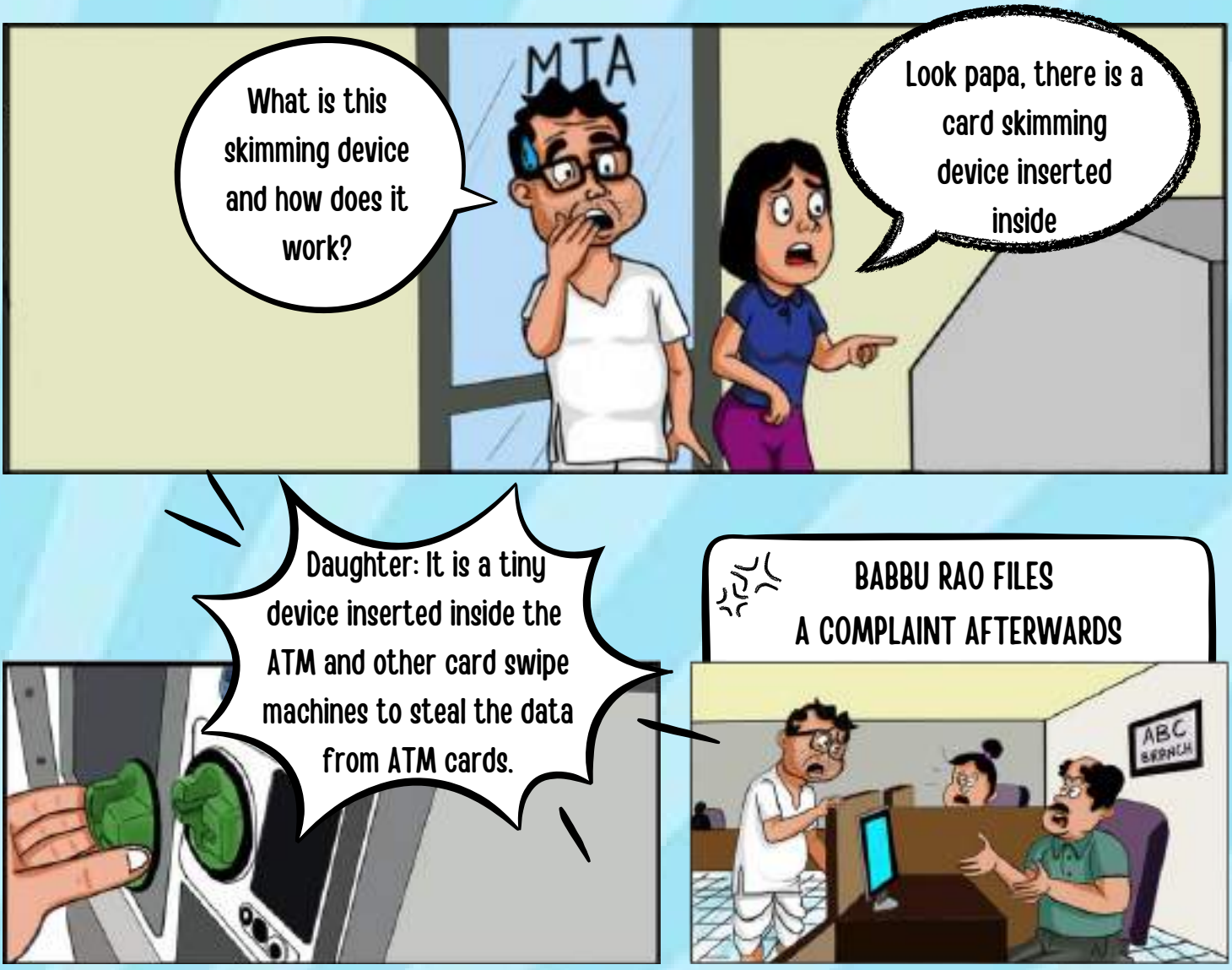
Delhi Skill and Entrepreneurship University
Govt. of NCT of Delhi

# ATM Card Skimming Fraud

## Babu Rao visits an ATM to withdraw money.


After an hour, he received SMS notifications about a few more extra debit transactions. (Rs. 14000 has been debited from your account, Rs. 8000 has been debited from your account). Babu Rao tells about the whole scene to his daughter.


# Both Of Them Went To ATM.




## DO'S

- Before inserting your cards inside the ATMs, make sure any skimming device is not present.
- Report the Fraud within 3 days after the incident takes place.

## DON'TS

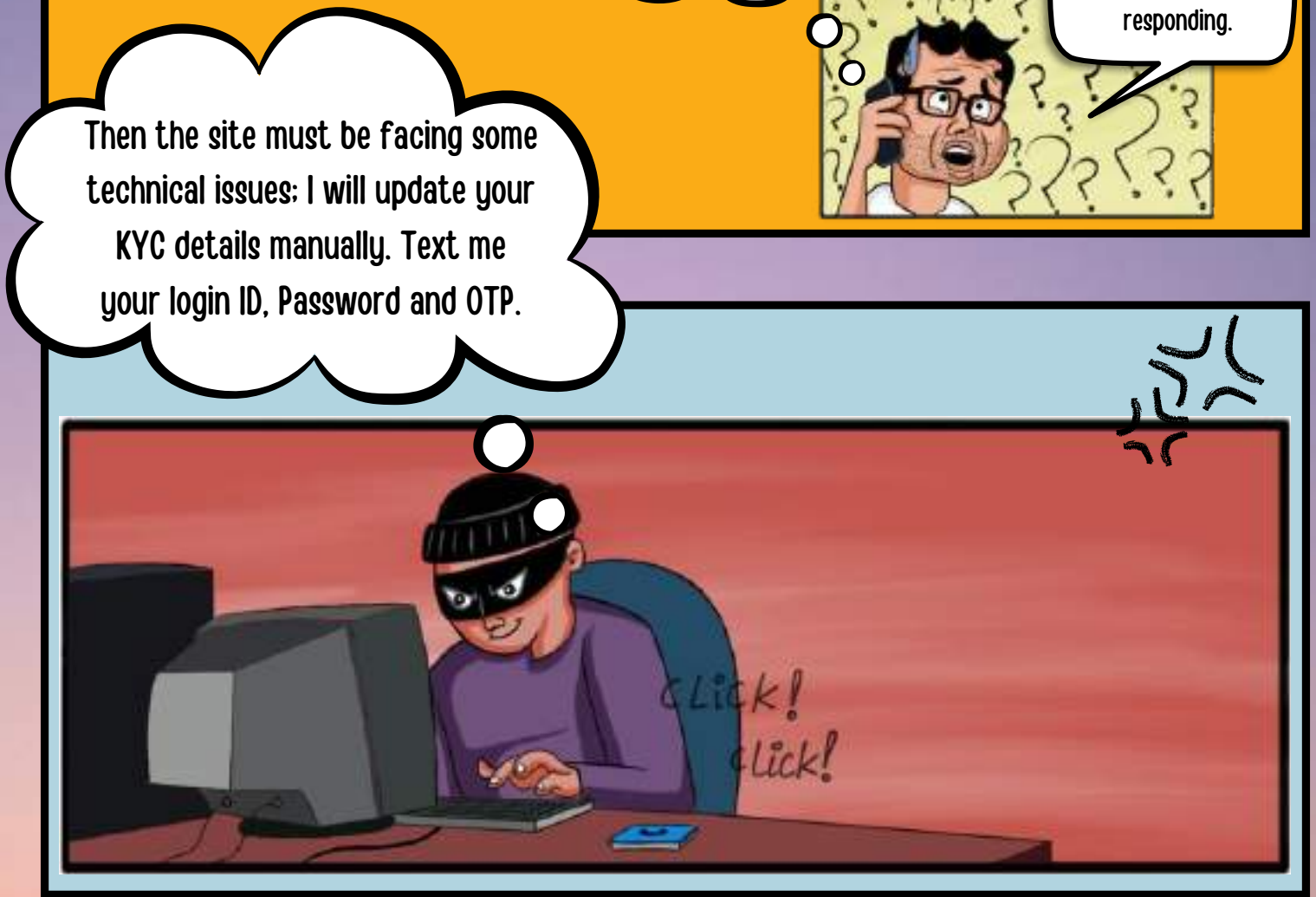
- Never give your ATM cards to anyone to withdraw money on your behalf.
- Never respond to messages or Emails asking for your card details or OTP.

# FRAUD THROUGH PHISHING LINKS

One day Babu Rao received a message on his mobile: Dear customer, your KYC details have not been updated. If not done within two days, the account shall be blocked. Click on the link below to update the details:


Babu Rao clicked on the link but it didn't work. After a few minutes, he gets a call.






After a few minutes, Babu Rao received a notification stating that Rs. 50,000 has been debited from his account.


Babu Rao tried to call the person again and no one responded. He immediately realized that he was a scammer and he should not have shared the details with him.

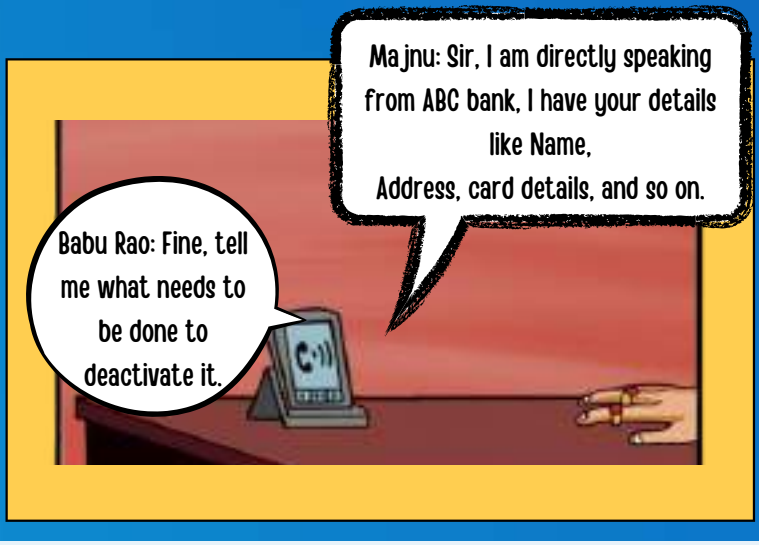


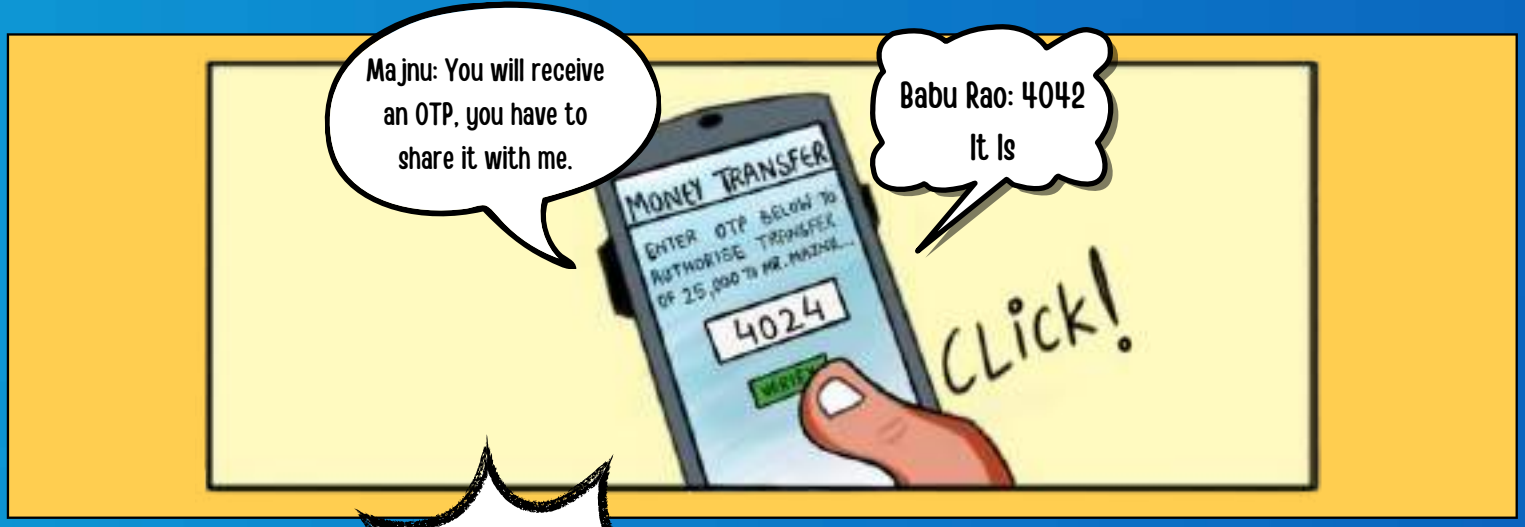
- If you receive any suspicious text, call, or message requesting you to update your KYC, always cross check it with your home branch or your relationship manager.

- Don't click on unknown links before verifying or cross-checking them.
- Don't disclose your confidential details to strangers

# PHISHING CALLS







After a few minutes, Babu Rao received a message stating that Rs. 25000 has been debited from your account

After that Babu Rao visited the bank branch and got to know that no such call had been made from their side. He immediately realized that he had been scammed.

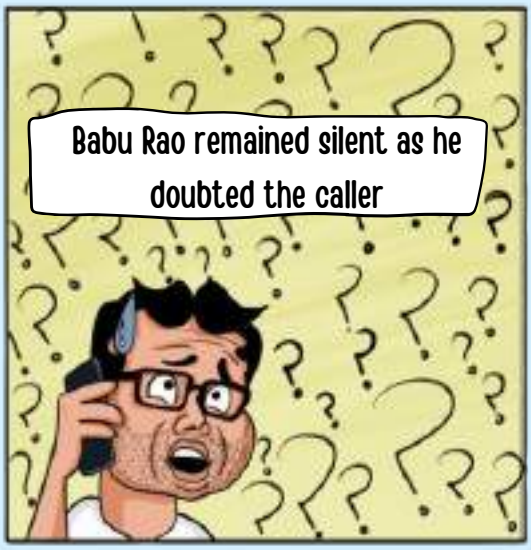

## DO'S

- Always cross-check with your bank before answering anyone regarding your details.
- At any cost never share your OTP

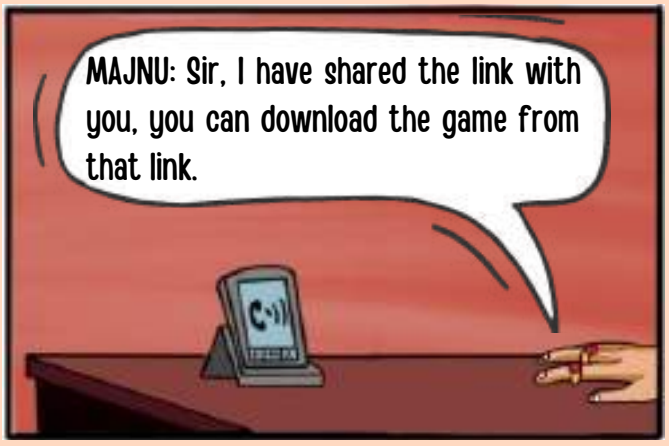
## DON'TS

- Don't trust anyone claiming to be a bank employee asking for personal details. Banks don't ask for confidential details over the phone.
- Never trust anyone without verifying him.

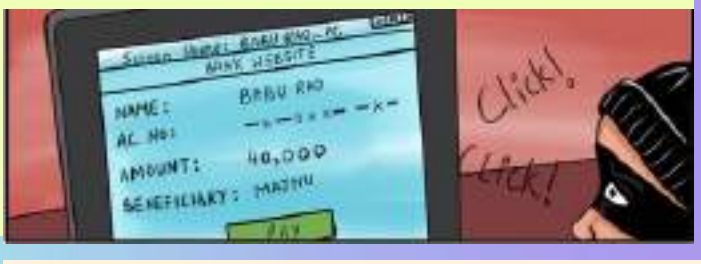
# FRAUD USING SCREEN SHARING APP/REMOTE ACCESS




MAJNU successfully installed the screen sharing app on Babu Rao's phone and now he can access his messages and even keep track of his keypad.




After the screen sharing app was installed, the fraudster had access to the net banking password entered by Babu Rao to make the payment of Rs. 10.


After sending Rs. 10, soon after, Babu Rao received three new debit messages of Rs. 25000, Rs. 13000, and Rs. 22000.


## DO'S

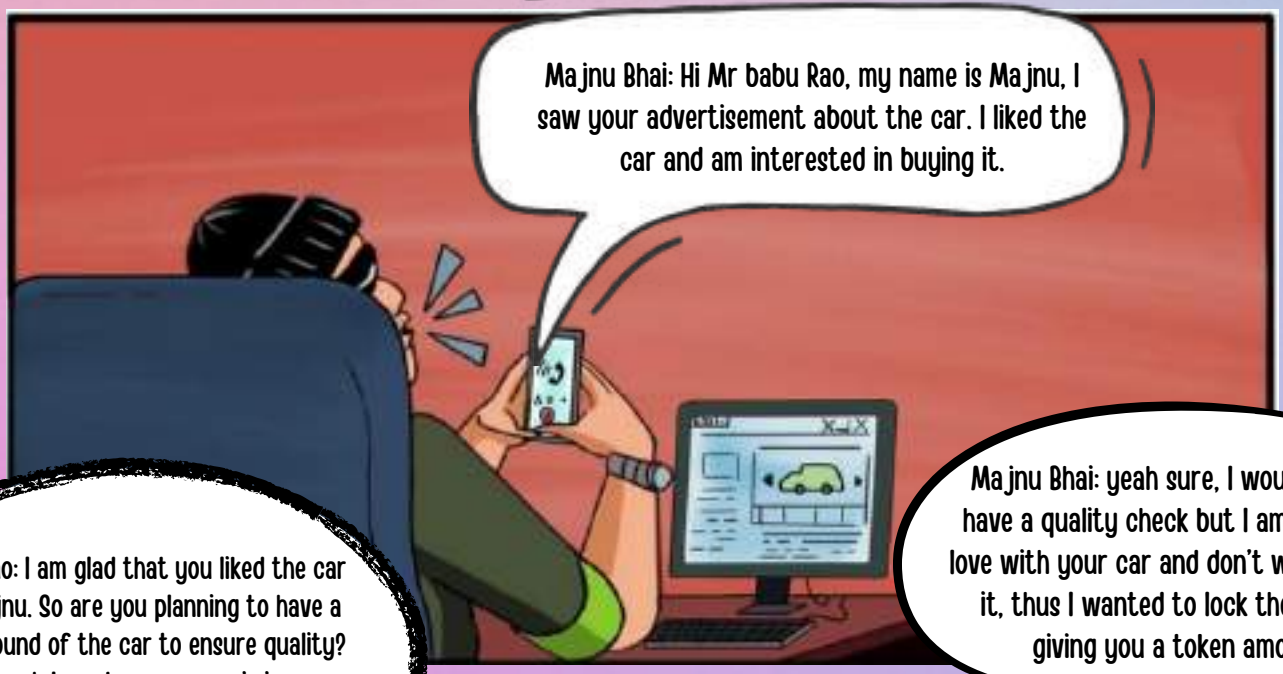
1. Verify the offer before availing it on the official site of the entity.
2. Download anti-virus/SPAM blocking apps.

## DON'TS

1. Never download any app through links sent through SMS, E-mails, or other messaging apps.
2. Don't download screen-sharing apps from unknown sources or links.

# QR CODE SCAN FRAUD

Babu Rao listed his old car on an online website, hoping to get a good price for it. Within a few hours of him uploading the details of the car. He was contacted by an unknown person acting like an interested buyer of the car.



Babu Rao: That would be great, I will send you my account details so that you could send me the token amount of INR 10,000.

Majnu Bhai: sure Mr Babu Rao, I will send you the amount as soon as possible.

Majnu Bhai : (again calling babu Rao after some time) hello Mr Rao, I am trying to send you the amount for the last 30 mins but it is not happening. I don't know if there is a problem with my server or any other issue. But I am sending you a QR code through Email which you could scan so that I can send the amount.

Babu Rao : ohk, no problem. I have just received the QR code. I am scanning it..... I have scanned the QR code but it is asking for my UPI passcode to complete the process. Is it safe?

Babu Rao entered the passcode and subsequently a message popped on his mobile phone informing him about the INR 1,00,000 that had just got debited from his bank account.

Mr majnu: yes yes it is safe, you must enter the pin so that could send you the INR 10,000.

Babu Rao started getting cold feet, he was not able to understand what had happened to him, he immediately called Majnu Bhai but his phone was switched off.

## DO'S

1. Be well informed about the QR codes before engaging in any transactions through them.
2. Report the transaction immediately to the bank.

## DON'TS

1. Never enter UPI passcodes for receiving payments. They are only used for making payments.
2. A QR code is to be scanned only while making the payment not while receiving it.


# Credits

## DESIGN TEAM

Abhishek Rawat
Alok Sahu
Mayank Sharma
Hardik Seth
( Students of BBA-BFSI )

## CONTENT TEAM

Tushar Bhardwaj
Archit Puri
Kavya Trivedi
( Students of BBA-BFSI )

## CO-ORDINATION

Kavya Trivedi
Archit Puri
*Founding Members, External Relations Committee*

## EDITOR

Dr. Parul Kumar
*Assistant Professor, BBA-BFSI Department*
*External Relations Incharge*

If you wish to contribute to
The Financial Minute, kindly reach out to us at
**newsletter_dwarka@dseu.ac.in.**

# Contact DSEU

www.dseu.ac.in
1800-309-3209
admissions@dseu.ac.in
G/Floor, Delhi Skill and Entrepreneurship University, Sector-9, Dwarka, New Delhi-110077

# Social Media

Youtube / dseu_official
LinkedIn / dseu_official
Twitter / dseu_official
Instagram / dseu_official