



AUTONOMOUS

Permanently affiliated to JNTUA Ananthapuramu, Approved by AICTE,
Accorded 'A' grade by Govt. of AP, Recognized by UGC 2(f) & 12(B),
ISO 9001:2015 certified Institution, Approved with 'A+' Grade by NAAC

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

Report on "An Overview on the Securities Market"

The department of **Electronics and Communication Engineering** has conducted "Webinar on An Overview on the Securities Market" on behalf of "Securities and Exchange Board of India (SEBI) and National Stock Exchange (NSE)" on 28/10/2021. Students of II, III and IV Year B.Tech came forward to participate in this event.

In this competition world all the companies are looking for graduates who have higher education and have additional skills, career guidance cell is training the students by conducting this activity. Skills needed to succeed as entrepreneur and as a investor or as a startup are provided **Securities and Exchange Board of India (SEBI) and National Stock Exchange (NSE)** who are collaborating with Narayana Engineering college.

The incharges are given instructions regarding these sessions where the resource persons spoke on a the topic in length.

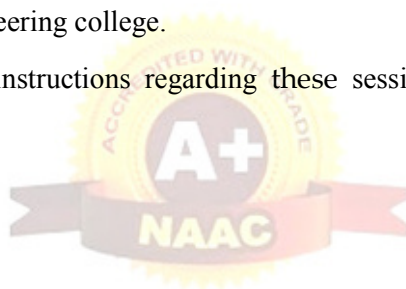
The resource person is

MR.Sanjay dhakite,

Deputy General Manager, SEBI.

MS.Saumya dube ,

Manager NSE.



**भारतीय प्रतिभूति और विनियम बोर्ड**
Securities and Exchange Board of India



Cordial invitation to an interactive webinar on

An Overview on the Securities Market

Date: Oct 28, 2021 **Time:** 11:00 am

Speakers

Mr. Sanjay Dhakite Deputy General Manager, SEBI	Ms. Saumya Dube Manager, NSE
---	--

Join at

Webinar Link: <https://bit.ly/3EneVf8>
Meeting Id: 2515 760 6064 Password: 1234

Webinar organised by National Stock Exchange of India Ltd





Faculty and students participation in the webinar



Students participation during webinar





Webinar explanation on hacking

REC

Biggest Data Breaches in 2021

91

	Data Breach	Size
1.	Dominos India	18 crore orders
2.	Mobikwik	10 crore users
3.	Facebook	60 lakh users
4.	Air India	45 lakh users
5.	Upstox	25 lakh users

10/29/2021
9

REC

RBI Phisher

The original website is bappedsumbawa.com

Select Bank

Resource person explaining on RBI Phisher

REC

World's Biggest Data Breaches & Hacks

Select losses greater than 30,000 records
Last updated: 1st April 2020

Filter: Colour YEAR DATA SENSITIVITY 2009 2020 Search...

10/29/2021 JRM 10

Next Gen Cyber Security's screen

REC

RANSOMWARE

Ransomware is a type of malware that restricts users from accessing the system and demands to pay ransom in order to regain access.

Modus Operandi

- Cybercriminals load malwares within email attachments, fake websites, offers, etc. which when clicked/accessed by users unknowingly get installed on their systems.
- The ransomware encrypts various file formats with different file extensions.
- They steal credentials/sensitive information and block the user out of the system.
- Advanced ransomwares are designed to evade anti VM or Sandbox, so they can't be analysed by security researchers.

How to Stay Safe

- Protect your personal/official devices with licensed Antivirus.
- Install ad blockers to combat exploit kits such as Fallout that are distributed via malicious advertising.
- Lock Remote Desktop Protocol, if not in use or follow RDP best practices such as rate limiting, MFA, etc.
- Configure strong firewalls & VPN must have capability to test basic security protocols before connection.
- Deploy effective backup strategies including keeping the backup safe, so that they can be used to recover lost data in the event of an infection.

10/29/2021 JRM 38

REC

REBOOT[®] CORPORATE DATA BREACHES STUDY

REBOOT Online surveyed 1,798 business owners and employees in the UK about their experience with data breaches and password security in the past year (2020/2021)

Percentage of ex-employees trying to access corporate apps or data

Before WFH	After WFH
37%	44%

Sector with the weakest protocols

% of businesses with weak or no security protocols in the past year	Sector
52%	Marketing / Digital Media
46%	Business / Consulting
41%	Healthcare
38%	Charity
36%	Hospitality
35%	HR / Recruitment
27%	Accountancy / Finance
22%	IT
21%	Leisure / Tourism

Role of ex-employees trying to access corporate apps or data

Role	Percentage
Executive	51%
Manager	34%
Director	9%
Junior	6%
Intern	4%

Most commonly accessed corporate apps or data by ex-employees

App/Data Type	Percentage
Private chats	56%
Learning resources	47%
Payroll	41%
Company data/information	33%
Internal reports	26%
Tools	19%

Do companies change ALL their security passwords after an employee departs?

Response	Percentage
NO	79%
YES	31%

10/29/2021 JRM 11

Resource person explaining on Data Breaches

