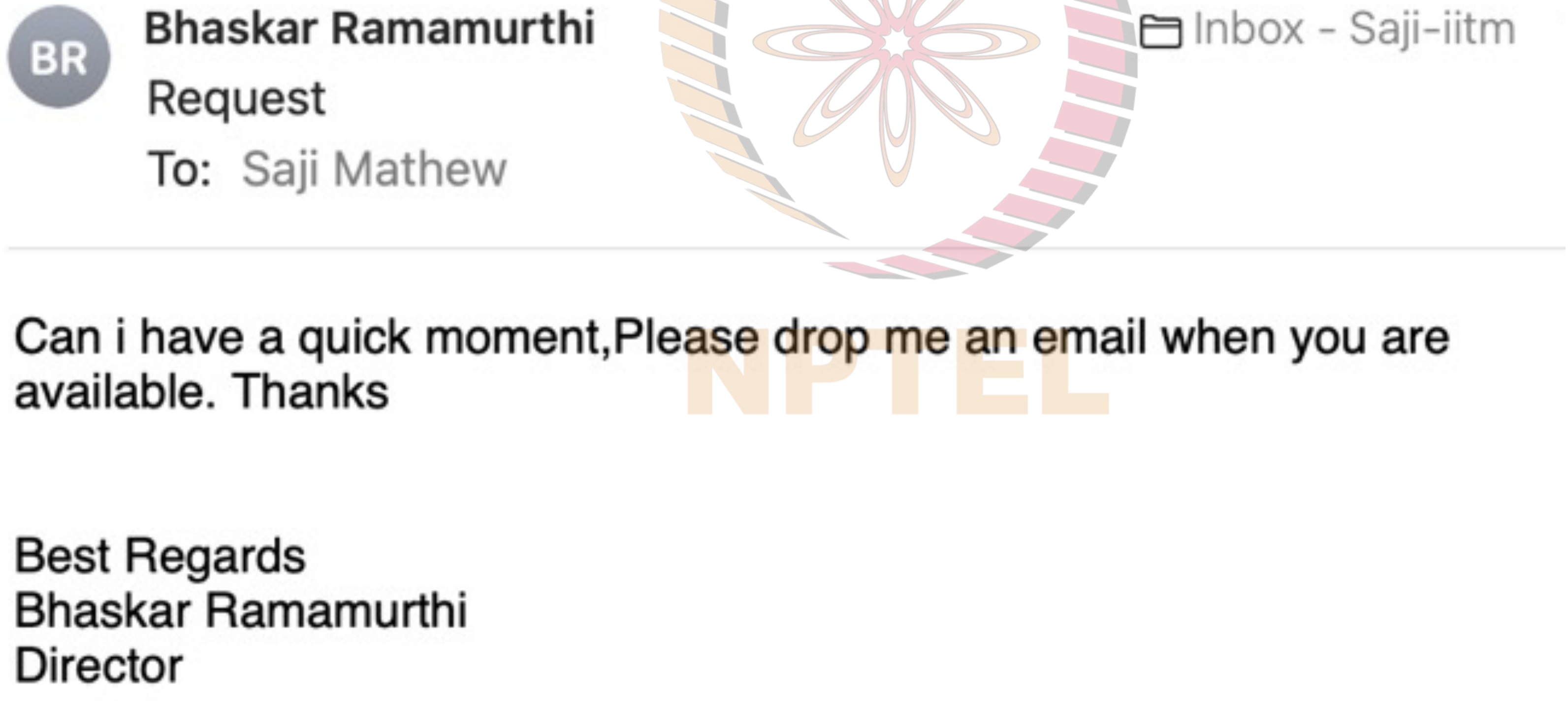
Cyber Security and Privacy
MS6880

Introduction

Saji K Mathew, PhD
Professor, Management Studies
INDIAN INTITUTE OF TECHNOLOGY MADRAS

Are cyber attacks real?



Bhaskar Ramamurthi

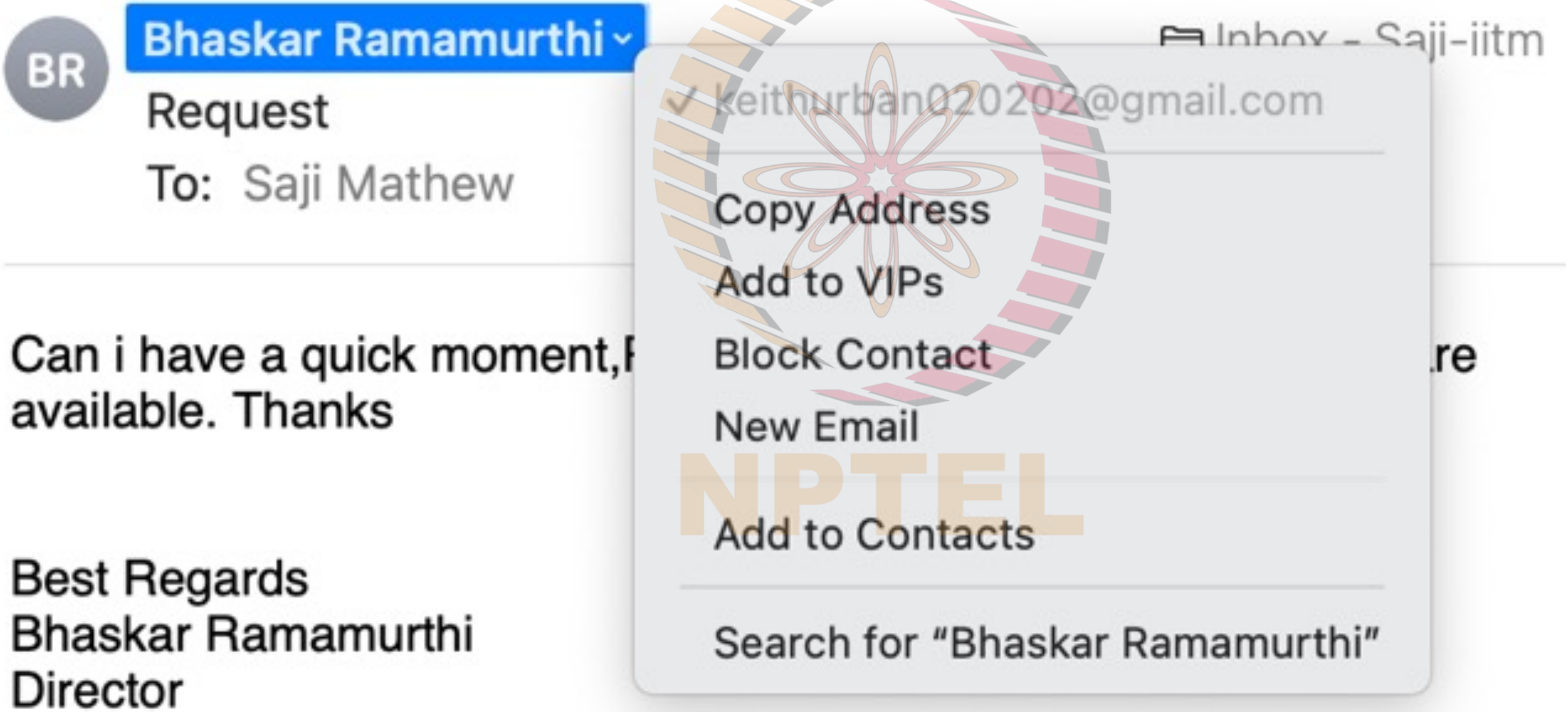
Inbox - Saji-iitm

Request

To: Saji Mathew

Can i have a quick moment,Please drop me an email when you are available. Thanks

Best Regards
Bhaskar Ramamurthi
Director

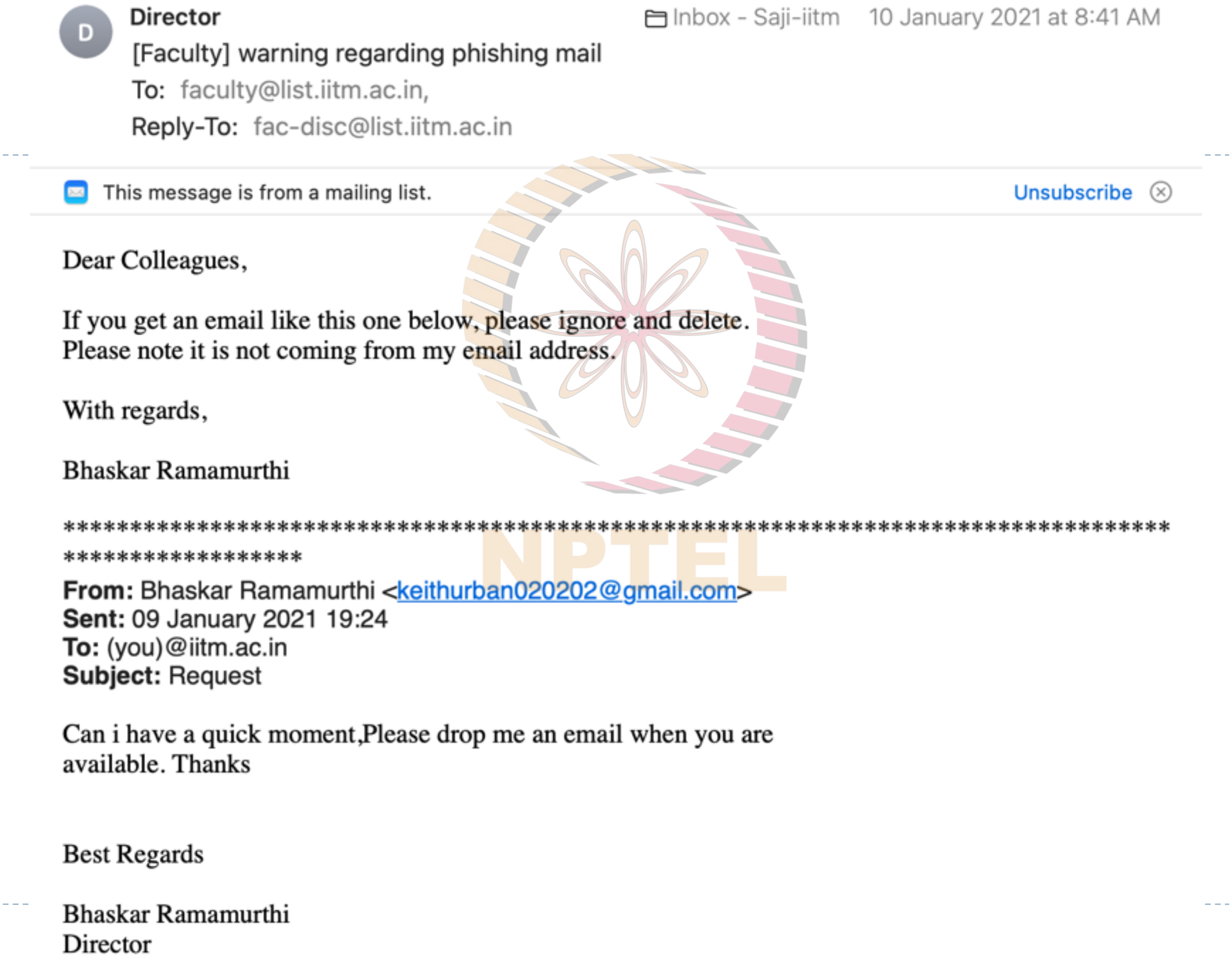


Request

To: Saji Mathew

Can i have a quick moment,F re
available. Thanks

Best Regards
Bhaskar Ramamurthi
Director



Director

Inbox - Saji-iitm 10 January 2021 at 8:41 AM

[Faculty] warning regarding phishing mail

To: faculty@list.iitm.ac.in,

Reply-To: fac-disc@list.iitm.ac.in

This message is from a mailing list.

Dear Colleagues,

If you get an email like this one below, please ignore and delete.
Please note it is not coming from my email address.

With regards,

Bhaskar Ramamurthi

****
****

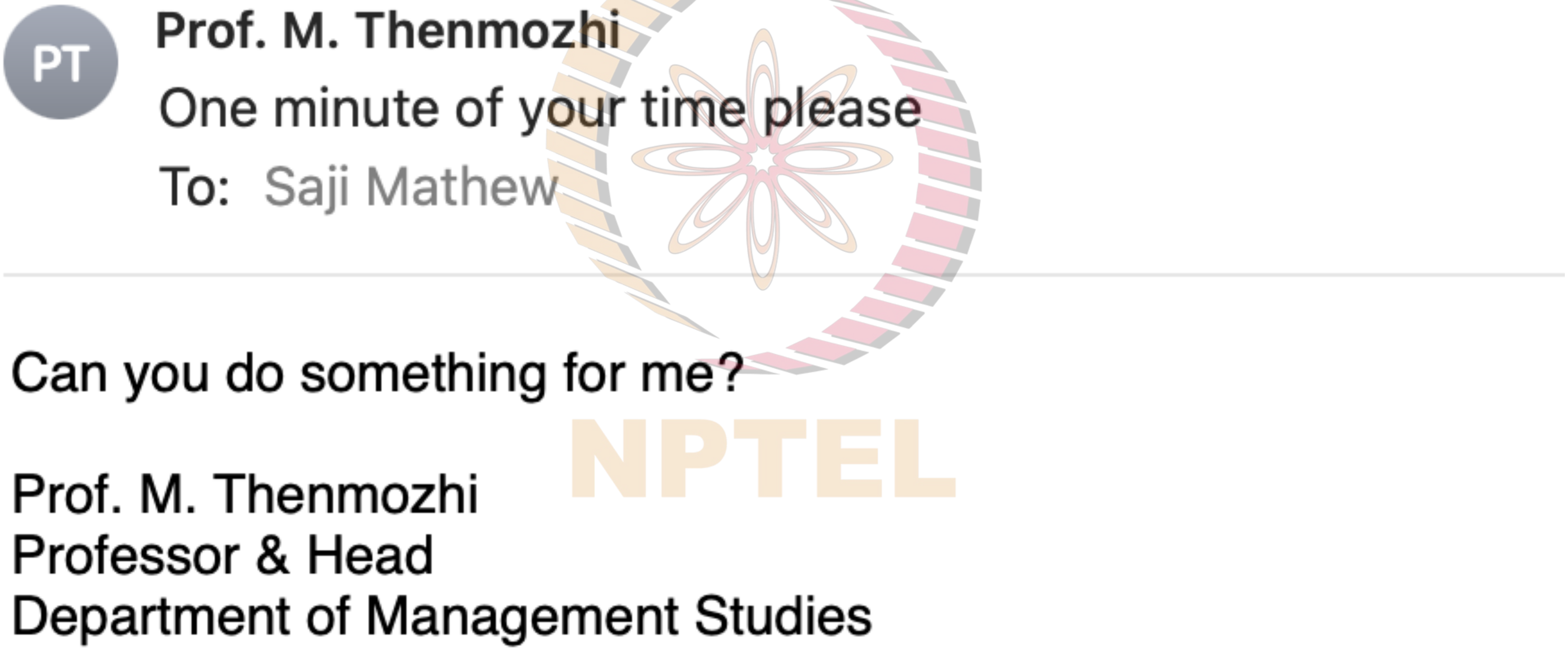
From: Bhaskar Ramamurthi <keithurban020202@gmail.com>
Sent: 09 January 2021 19:24
To: (you)@iitm.ac.in
Subject: Request

Can i have a quick moment,Please drop me an email when you are
available. Thanks

Best Regards

Bhaskar Ramamurthi
Director

What should I do?



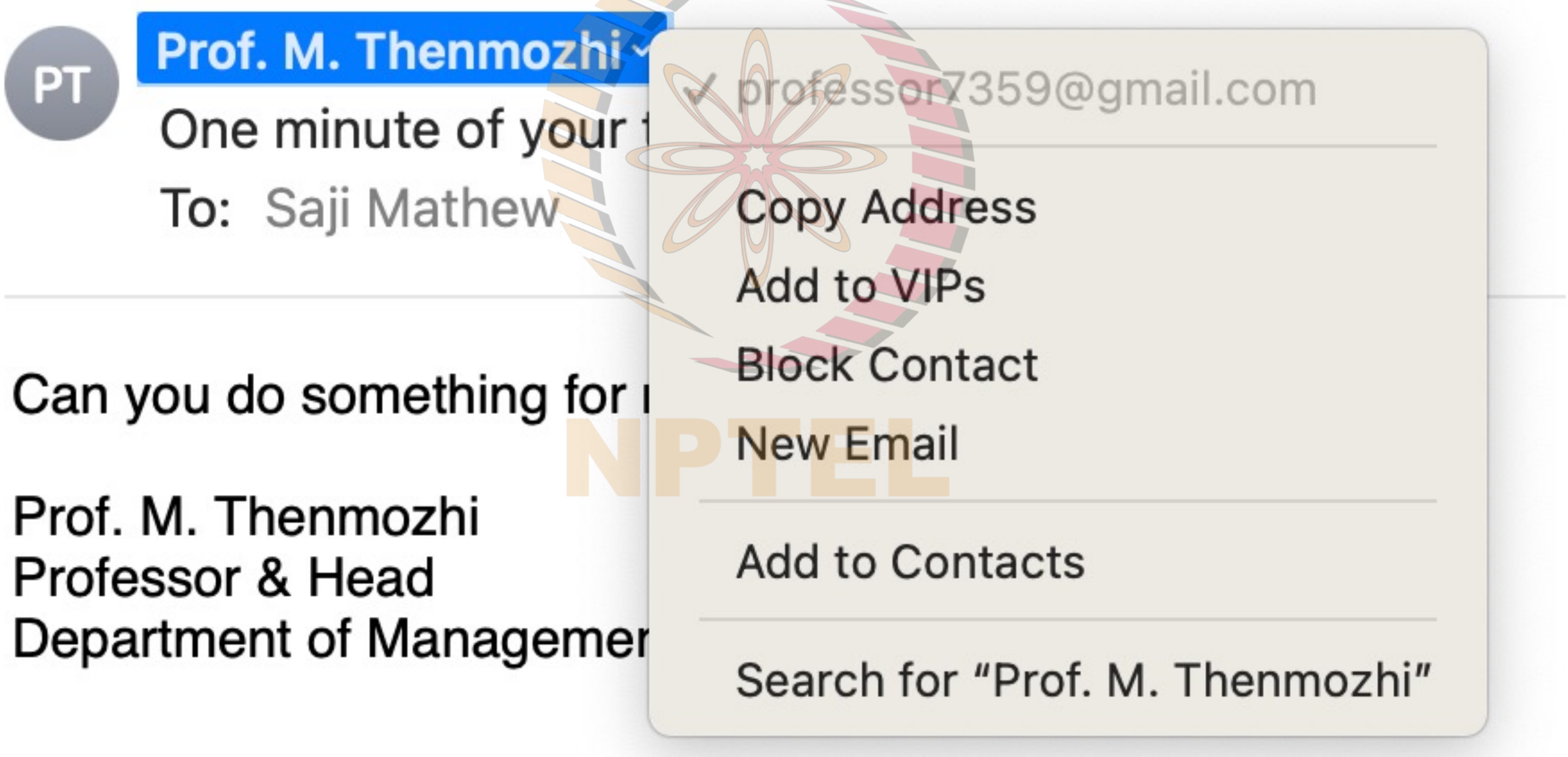
Prof. M. Thenmozhi

One minute of your time please

To: Saji Mathew

Can you do something for me?

Prof. M. Thenmozhi
Professor & Head
Department of Management Studies



PT

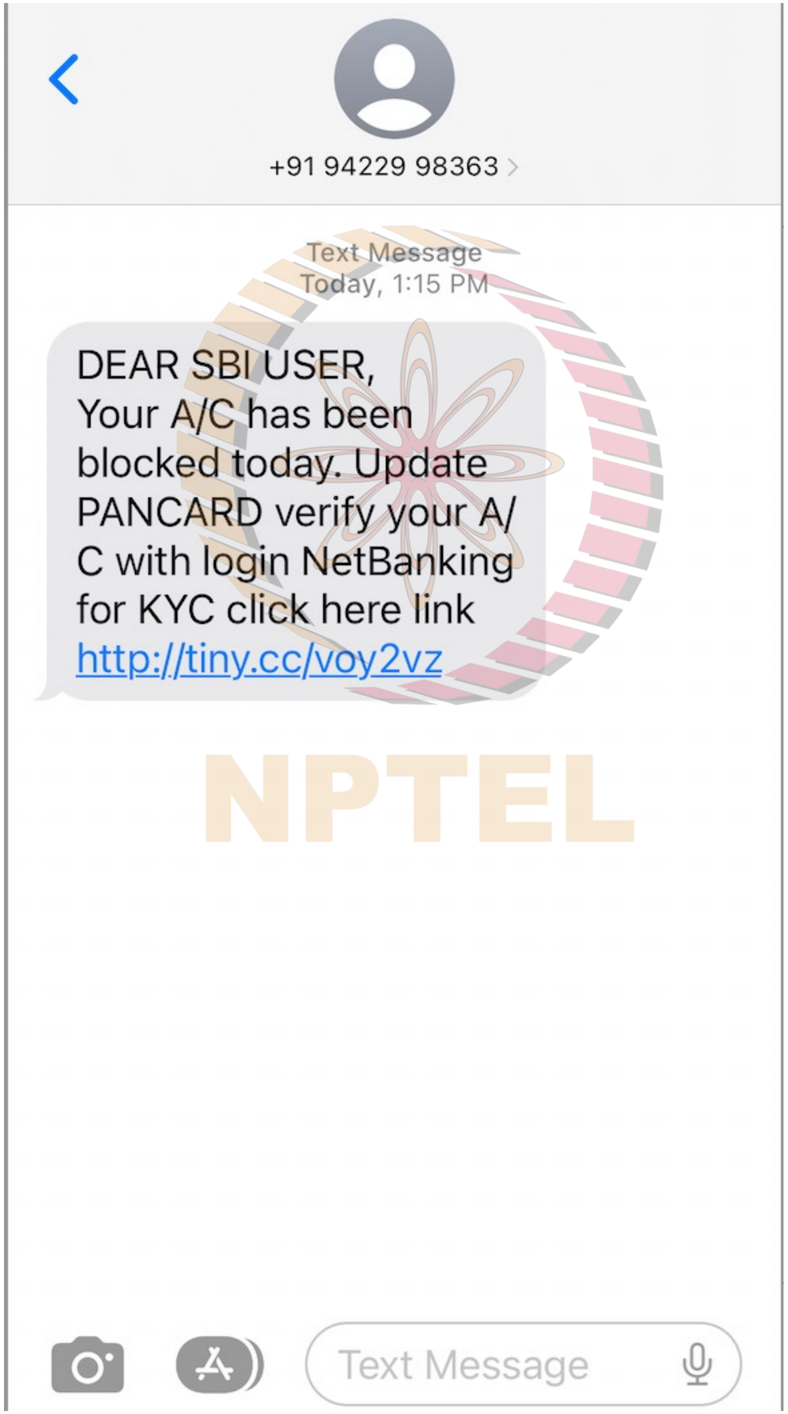
Prof. M. Thenmozhi

One minute of your t

To: Saji Mathew

Can you do something for r

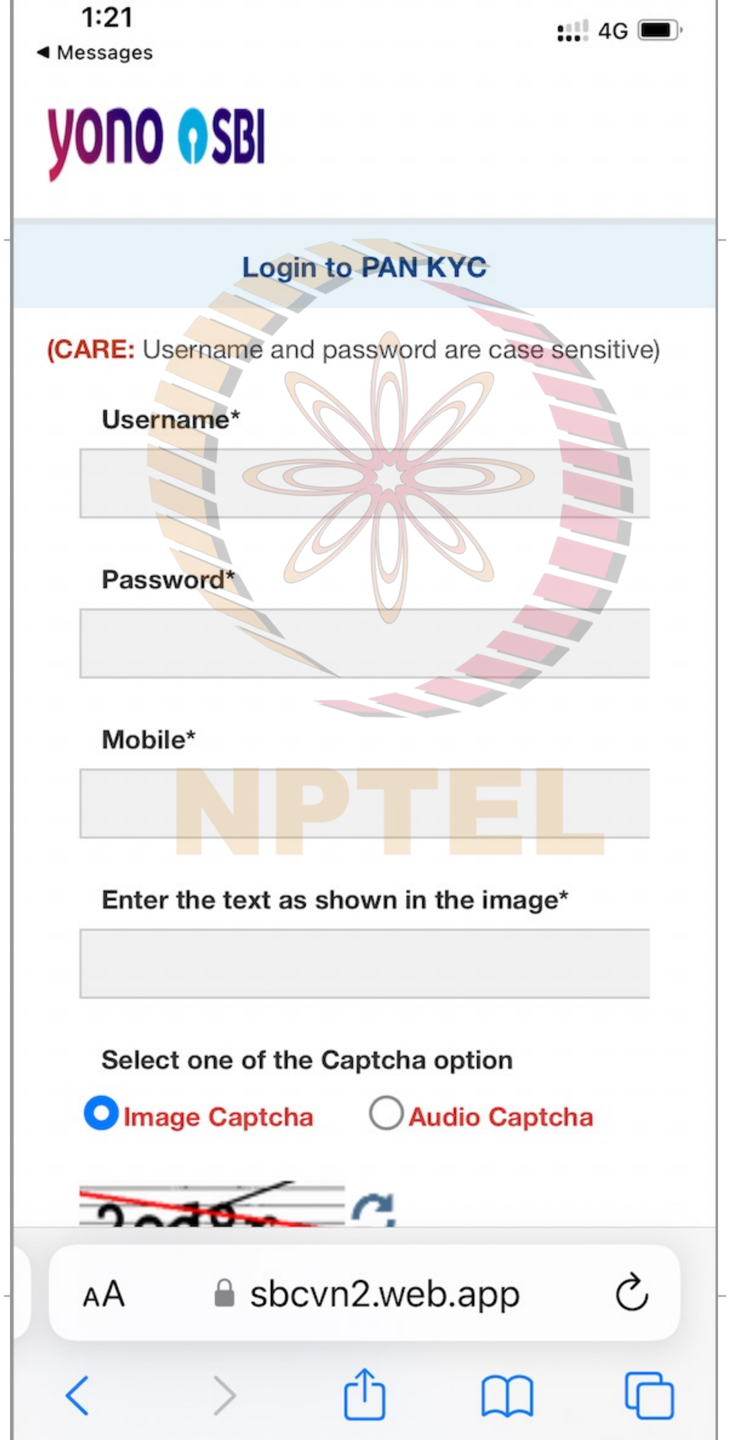
Prof. M. Thenmozhi
Professor & Head
Department of Managemer



+91 94229 98363

Text Message
Today, 1:15 PM

DEAR SBI USER,
Your A/C has been blocked today. Update PANCARD verify your A/C with login NetBanking for KYC click here link http://tiny.cc/voy2vz



Login to PAN KYC

(CARE: Username and password are case sensitive)

Username*

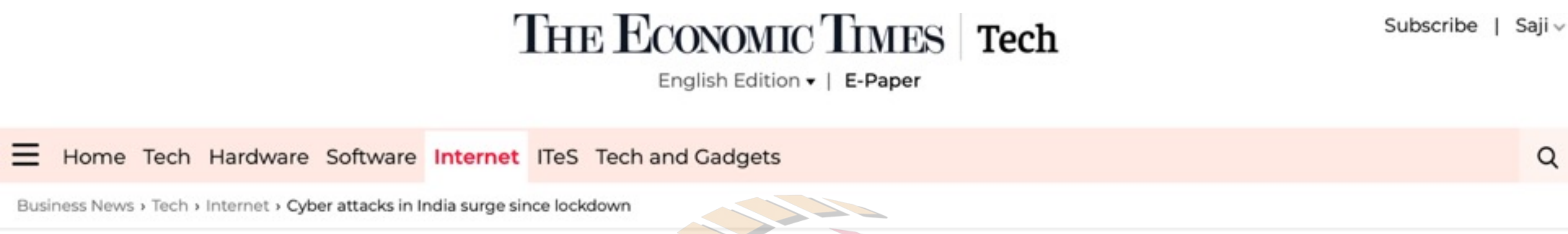
Password*

Mobile*

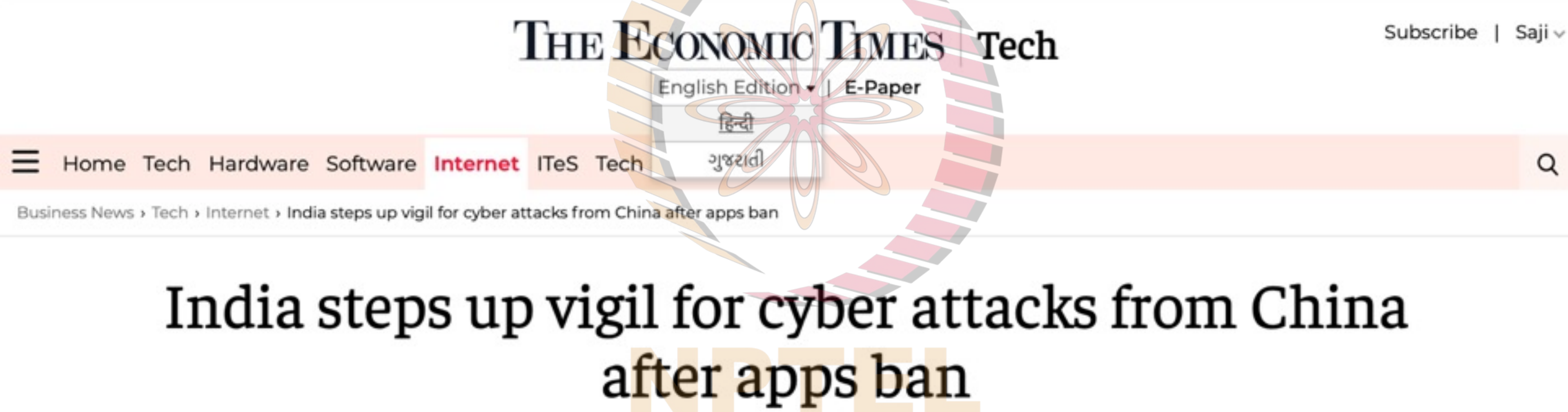
Enter the text as shown in the image*

Select one of the Captcha option

● Image Captcha ○ Audio Captcha

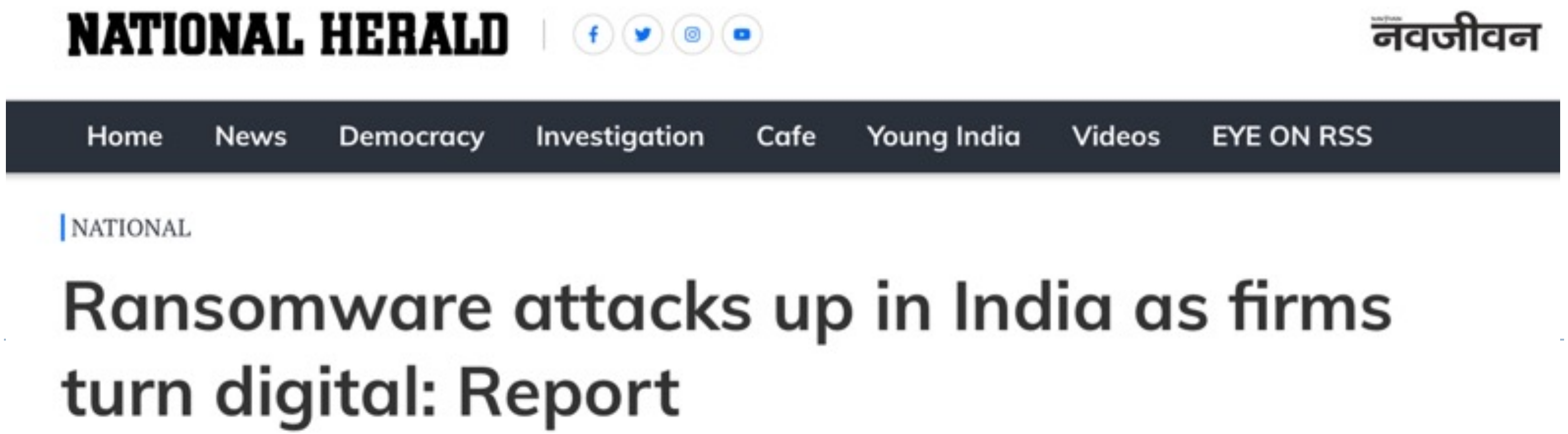

The Economic Times | Tech
English Edition | E-Paper
Subscribe | Saji
Home Tech Hardware Software Internet ITeS Tech and Gadgets

Business News › Tech › Internet › Cyber attacks in India surge since lockdown


The Economic Times | Tech
English Edition | E-Paper
हिन्दी
ગુજરાતી
Subscribe | Saji
Home Tech Hardware Software Internet ITeS Tech

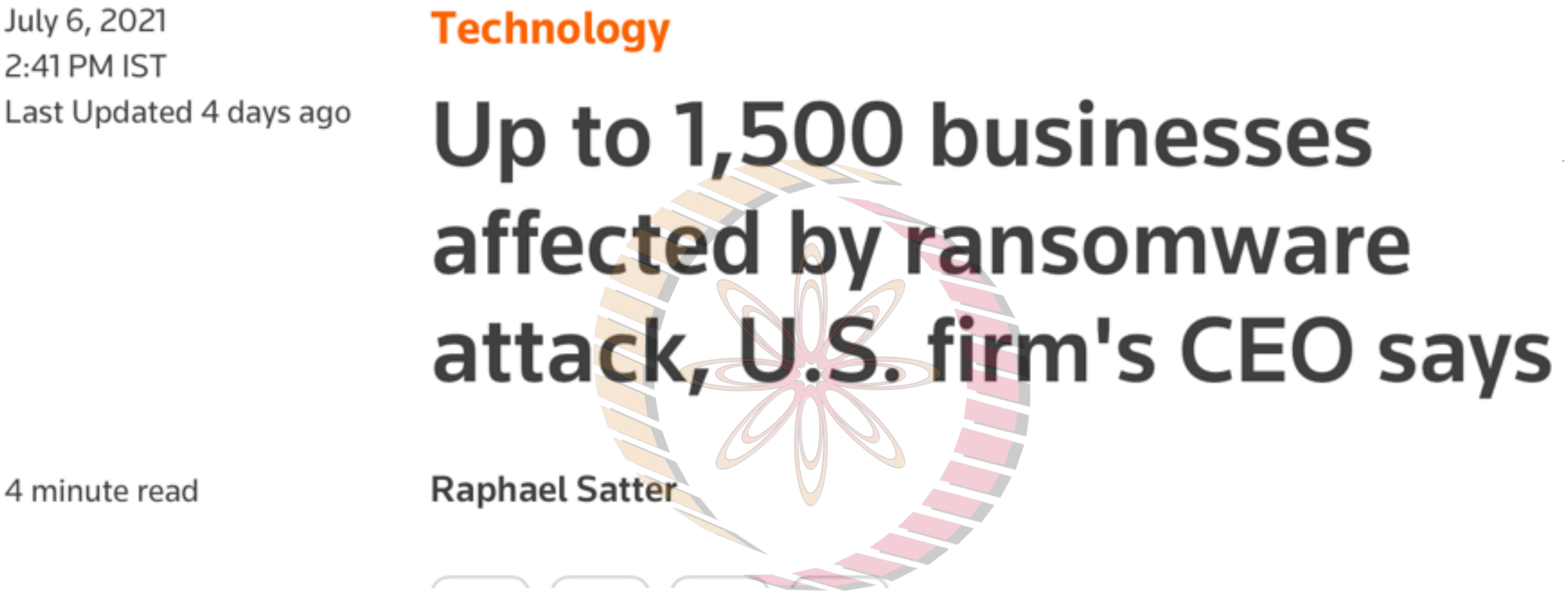
Business News › Tech › Internet › India steps up vigil for cyber attacks from China after apps ban

India steps up vigil for cyber attacks from China after apps ban


NATIONAL HERALD
नवजीवन
Home News Democracy Investigation Cafe Young India Videos EYE ON RSS

NATIONAL

Ransomware attacks up in India as firms turn digital: Report



July 6, 2021
2:41 PM IST
Last Updated 4 days ago

Technology

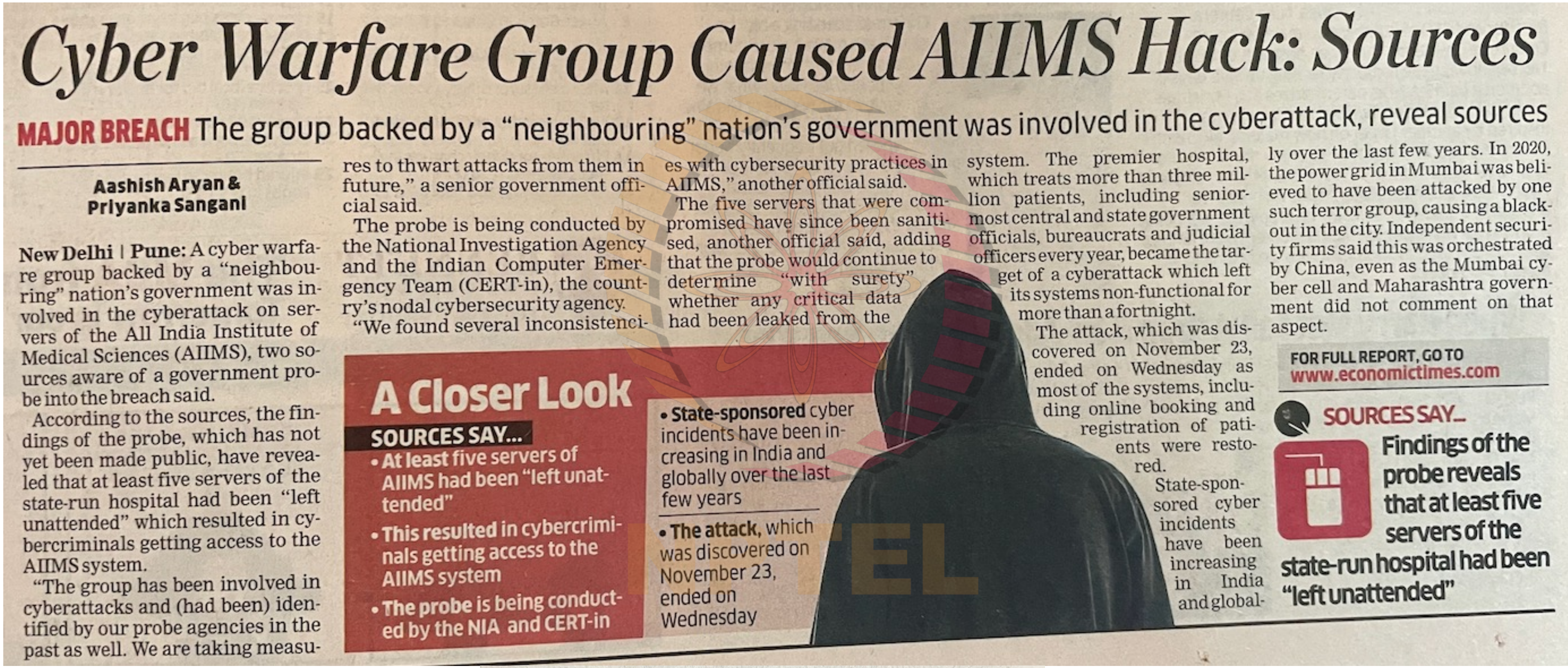
Up to 1,500 businesses affected by ransomware attack, U.S. firm's CEO says

4 minute read

Raphael Satter

- Kaseya is a company which provides software tools for IT outsourcing
- One of those tools was subverted
- The hackers who claimed responsibility for the breach have demanded $70 million to restore all the affected businesses

Nov-Dec'22



Cyber Warfare Group Caused AIIMS Hack: Sources

MAJOR BREACH The group backed by a "neighbouring" nation's government was involved in the cyberattack, reveal sources

Aashish Aryan & Priyanka Sangani

New Delhi | Pune: A cyber warfare group backed by a "neighbouring" nation's government was involved in the cyberattack on servers of the All India Institute of Medical Sciences (AIIMS), two sources aware of a government probe into the breach said.

According to the sources, the findings of the probe, which has not yet been made public, have revealed that at least five servers of the state-run hospital had been "left unattended" which resulted in cybercriminals getting access to the AIIMS system.

"The group has been involved in cyberattacks and (had been) identified by our probe agencies in the past as well. We are taking measures to thwart attacks from them in future," a senior government official said.

The probe is being conducted by the National Investigation Agency and the Indian Computer Emergency Team (CERT-in), the country's nodal cybersecurity agency.

"We found several inconsistencies with cybersecurity practices in AIIMS," another official said.

The five servers that were compromised have since been sanitised, another official said, adding that the probe would continue to determine "with surety" whether any critical data had been leaked from the system. The premier hospital, which treats more than three million patients, including senior-most central and state government officials, bureaucrats and judicial officers every year, became the target of a cyberattack which left its systems non-functional for more than a fortnight.

The attack, which was discovered on November 23, ended on Wednesday as most of the systems, including online booking and registration of patients were restored.

State-sponsored cyber incidents have been increasing in India and globally over the last few years. In 2020, the power grid in Mumbai was believed to have been attacked by one such terror group, causing a blackout in the city. Independent security firms said this was orchestrated by China, even as the Mumbai cyber cell and Maharashtra government did not comment on that aspect.

FOR FULL REPORT, GO TO www.economictimes.com

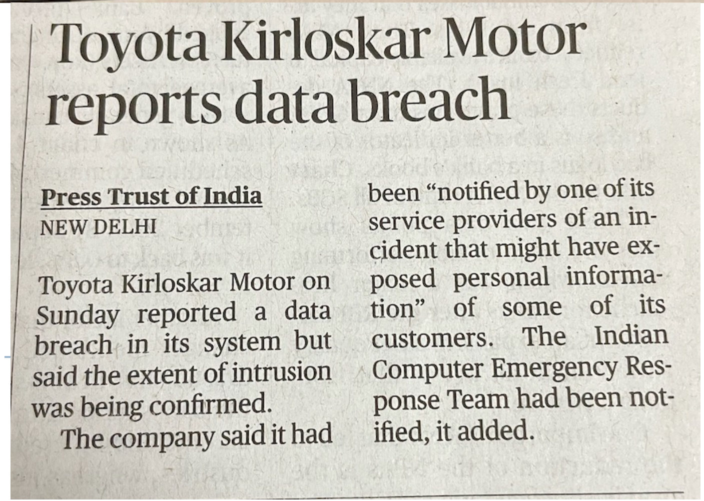
A Closer Look

SOURCES SAY...

- **At least five servers of AIIMS had been "left unattended"**
- **This resulted in cybercriminals getting access to the AIIMS system**
- **The probe is being conducted by the NIA and CERT-in**
- **State-sponsored** cyber incidents have been increasing in India and globally over the last few years
- **The attack,** which was discovered on November 23, ended on Wednesday

SOURCES SAY...

Findings of the probe reveals that at least five servers of the state-run hospital had been "left unattended"

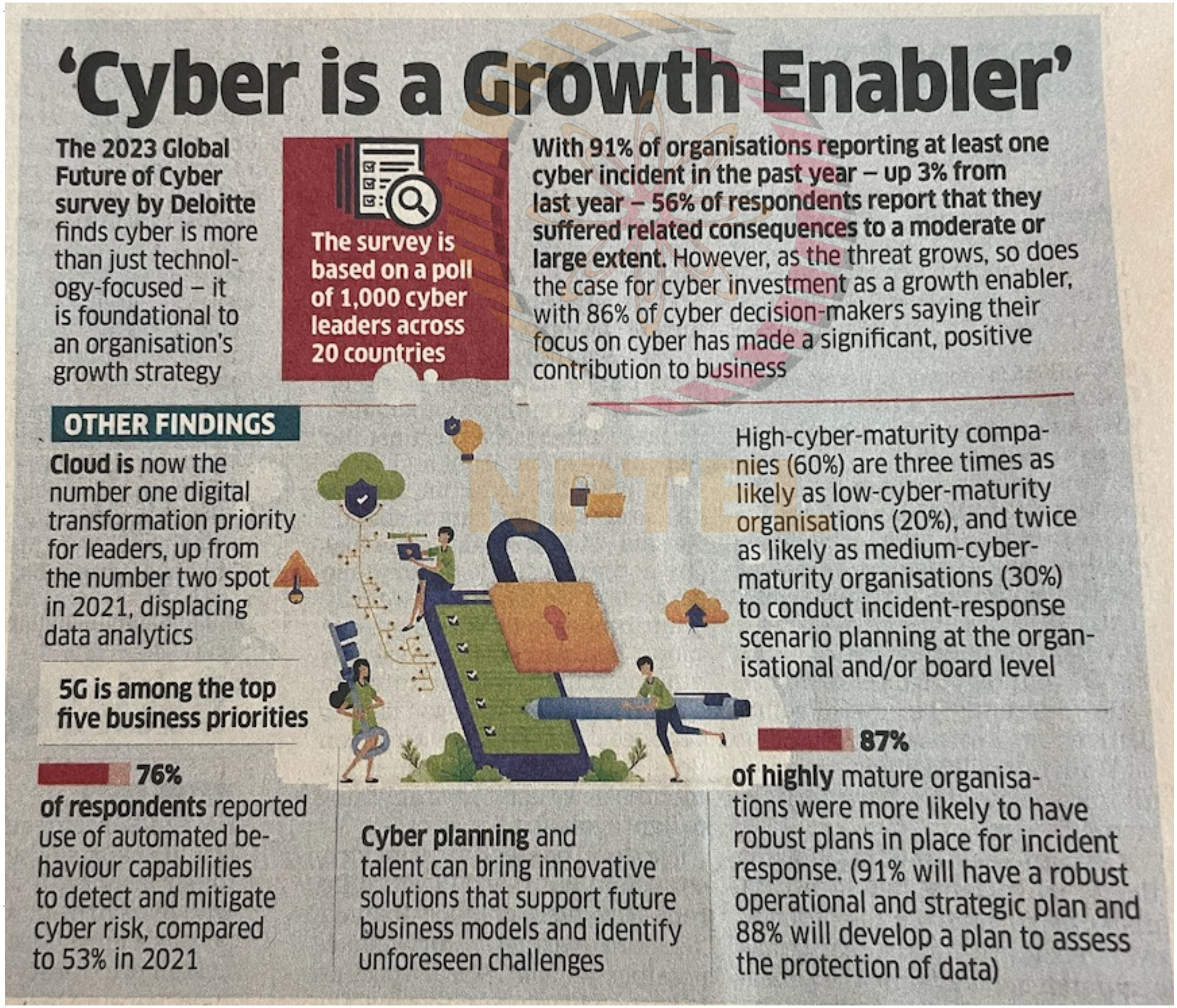


Toyota Kirloskar Motor reports data breach

Press Trust of India
NEW DELHI

Toyota Kirloskar Motor on Sunday reported a data breach in its system but said the extent of intrusion was being confirmed.

The company said it had been "notified by one of its service providers of an incident that might have exposed personal information" of some of its customers. The Indian Computer Emergency Response Team had been notified, it added.



‘Cyber is a Growth Enabler’

The 2023 Global Future of Cyber survey by Deloitte finds cyber is more than just technology-focused – it is foundational to an organisation's growth strategy

The survey is based on a poll of 1,000 cyber leaders across 20 countries

With 91% of organisations reporting at least one cyber incident in the past year – up 3% from last year – 56% of respondents report that they suffered related consequences to a moderate or large extent. However, as the threat grows, so does the case for cyber investment as a growth enabler, with 86% of cyber decision-makers saying their focus on cyber has made a significant, positive contribution to business

OTHER FINDINGS

Cloud is now the number one digital transformation priority for leaders, up from the number two spot in 2021, displacing data analytics

5G is among the top five business priorities

76%

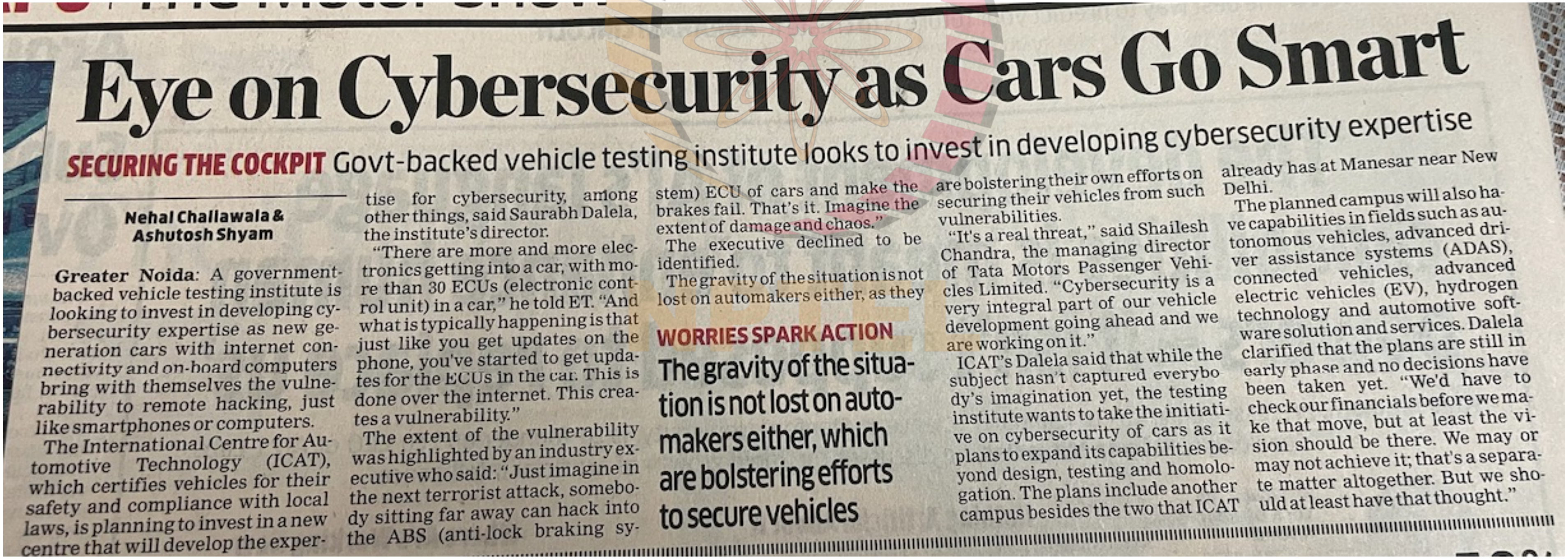
of respondents reported use of automated behaviour capabilities to detect and mitigate cyber risk, compared to 53% in 2021

Cyber planning and talent can bring innovative solutions that support future business models and identify unforeseen challenges

High-cyber-maturity companies (60%) are three times as likely as low-cyber-maturity organisations (20%), and twice as likely as medium-cyber-maturity organisations (30%) to conduct incident-response scenario planning at the organisational and/or board level

87%

of highly mature organisations were more likely to have robust plans in place for incident response. (91% will have a robust operational and strategic plan and 88% will develop a plan to assess the protection of data)



Eye on Cybersecurity as Cars Go Smart

SECURING THE COCKPIT Govt-backed vehicle testing institute looks to invest in developing cybersecurity expertise

Nehal Challawala & Ashutosh Shyam

Greater Noida: A government-backed vehicle testing institute is looking to invest in developing cybersecurity expertise as new generation cars with internet connectivity and on-board computers bring with themselves the vulnerability to remote hacking, just like smartphones or computers.

The International Centre for Automotive Technology (ICAT), which certifies vehicles for their safety and compliance with local laws, is planning to invest in a new centre that will develop the expertise for cybersecurity, among other things, said Saurabh Dalela, the institute's director.

"There are more and more electronics getting into a car, with more than 30 ECUs (electronic control unit) in a car," he told ET. "And what is typically happening is that just like you get updates on the phone, you've started to get updates for the ECUs in the car. This is done over the internet. This creates a vulnerability."

The extent of the vulnerability was highlighted by an industry executive who said: "Just imagine in the next terrorist attack, somebody sitting far away can hack into the ABS (anti-lock braking system) ECU of cars and make the brakes fail. That's it. Imagine the extent of damage and chaos."

The executive declined to be identified.

The gravity of the situation is not lost on automakers either, as they are bolstering their own efforts on securing their vehicles from such vulnerabilities.

WORRIES SPARK ACTION

The gravity of the situation is not lost on automakers either, which are bolstering efforts to secure vehicles

"It's a real threat," said Shailesh Chandra, the managing director of Tata Motors Passenger Vehicles Limited. "Cybersecurity is a very integral part of our vehicle development going ahead and we are working on it."

ICAT's Dalela said that while the subject hasn't captured everybody's imagination yet, the testing institute wants to take the initiative on cybersecurity of cars as it plans to expand its capabilities beyond design, testing and homologation. The plans include another campus besides the two that ICAT already has at Manesar near New Delhi.

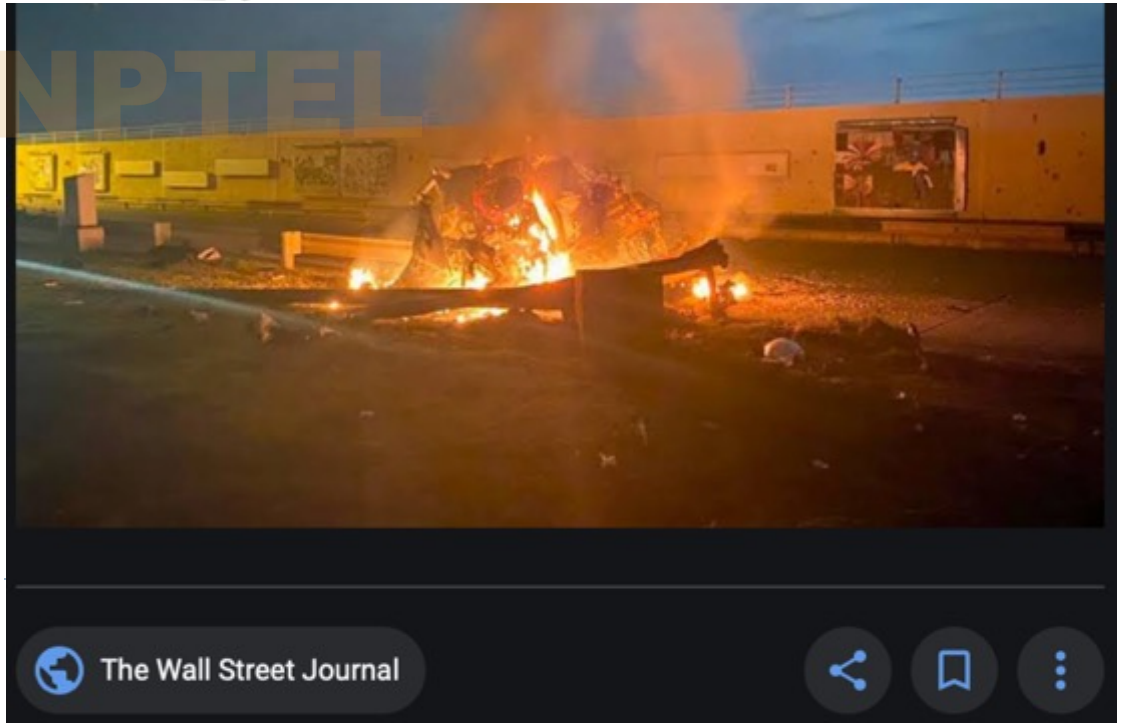
The planned campus will also have capabilities in fields such as autonomous vehicles, advanced driver assistance systems (ADAS), connected vehicles, advanced electric vehicles (EV), hydrogen technology and automotive software solution and services. Dalela clarified that the plans are still in early phase and no decisions have been taken yet. "We'd have to check our financials before we make that move, but at least the vision should be there. We may or may not achieve it; that's a separate matter altogether. But we should at least have that thought."

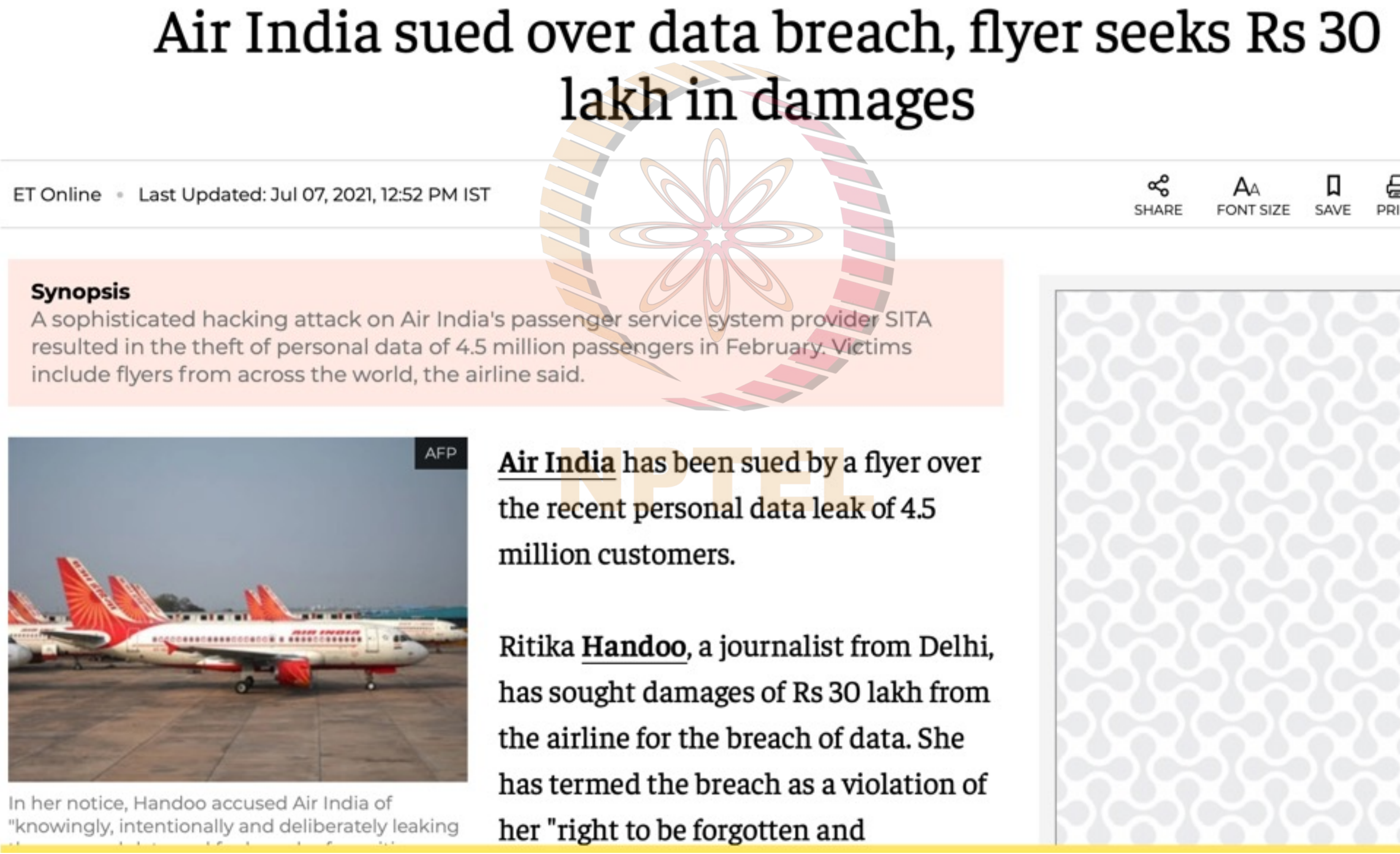
Drones attack Saudi oil refinery (Sept 16, 2019)

- Aramco was being listed in stock market
- Attack begins at 4:00AM
- Shutting down production around 5% of the world's daily crude oil production causing oil prices to surge up to 20%
- US said Iran behind Saudi oil attacks
- 17 hits identified on the Abqaiq refinery with dozen cruise missiles and more than 20 drones.

Jan 3, 2020, ~ 1:00 am

A US drone strike on a Baghdad airport killed Qasem Soleimani.





Air India sued over data breach, flyer seeks Rs 30 lakh in damages

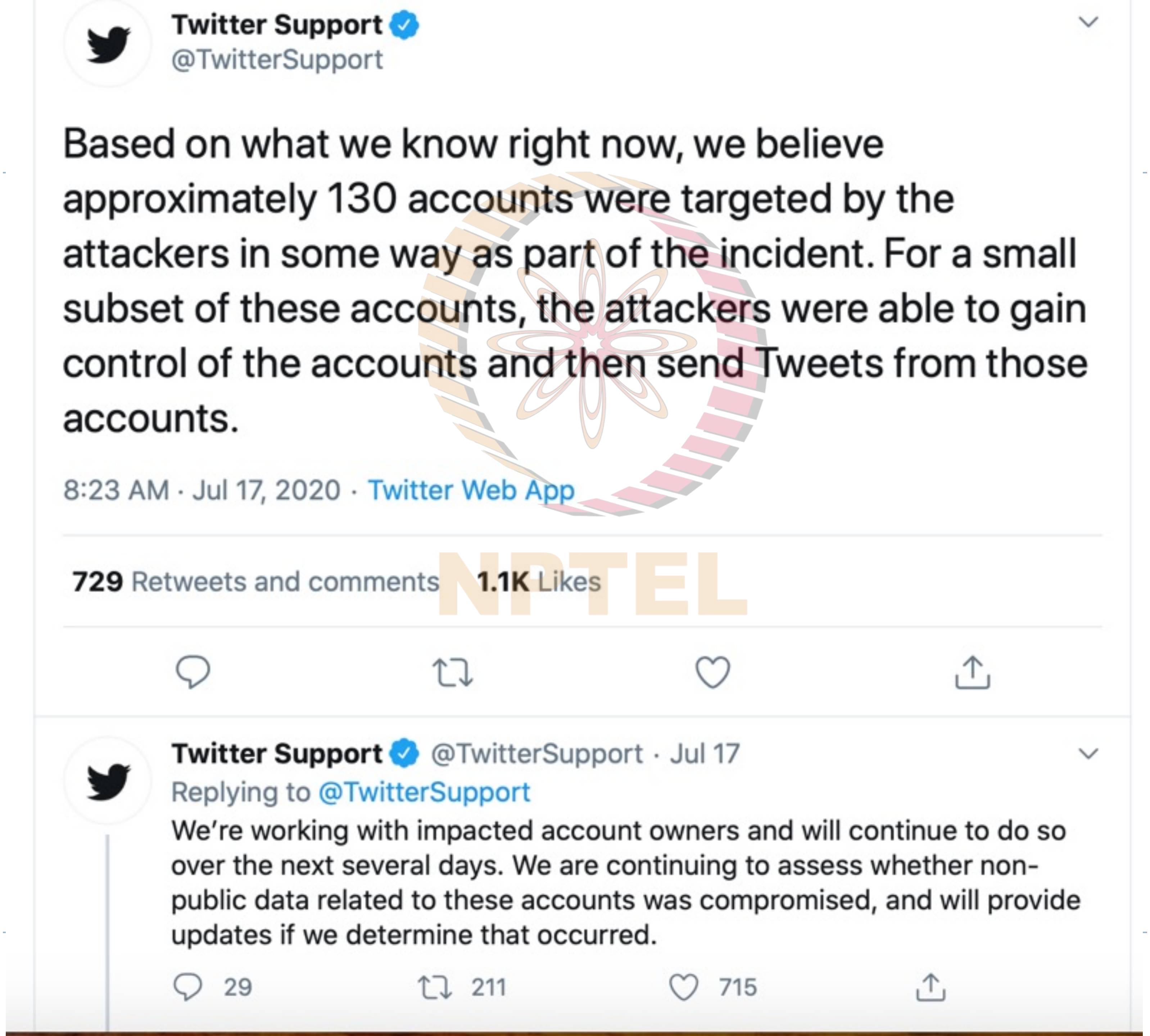
ET Online • Last Updated: Jul 07, 2021, 12:52 PM IST

Synopsis
A sophisticated hacking attack on Air India's passenger service system provider SITA resulted in the theft of personal data of 4.5 million passengers in February. Victims include flyers from across the world, the airline said.

In her notice, Handoo accused Air India of "knowingly, intentionally and deliberately leaking

Air India has been sued by a flyer over the recent personal data leak of 4.5 million customers.

Ritika Handoo, a journalist from Delhi, has sought damages of Rs 30 lakh from the airline for the breach of data. She has termed the breach as a violation of her "right to be forgotten and



Twitter Support
@TwitterSupport

Based on what we know right now, we believe approximately 130 accounts were targeted by the attackers in some way as part of the incident. For a small subset of these accounts, the attackers were able to gain control of the accounts and then send Tweets from those accounts.

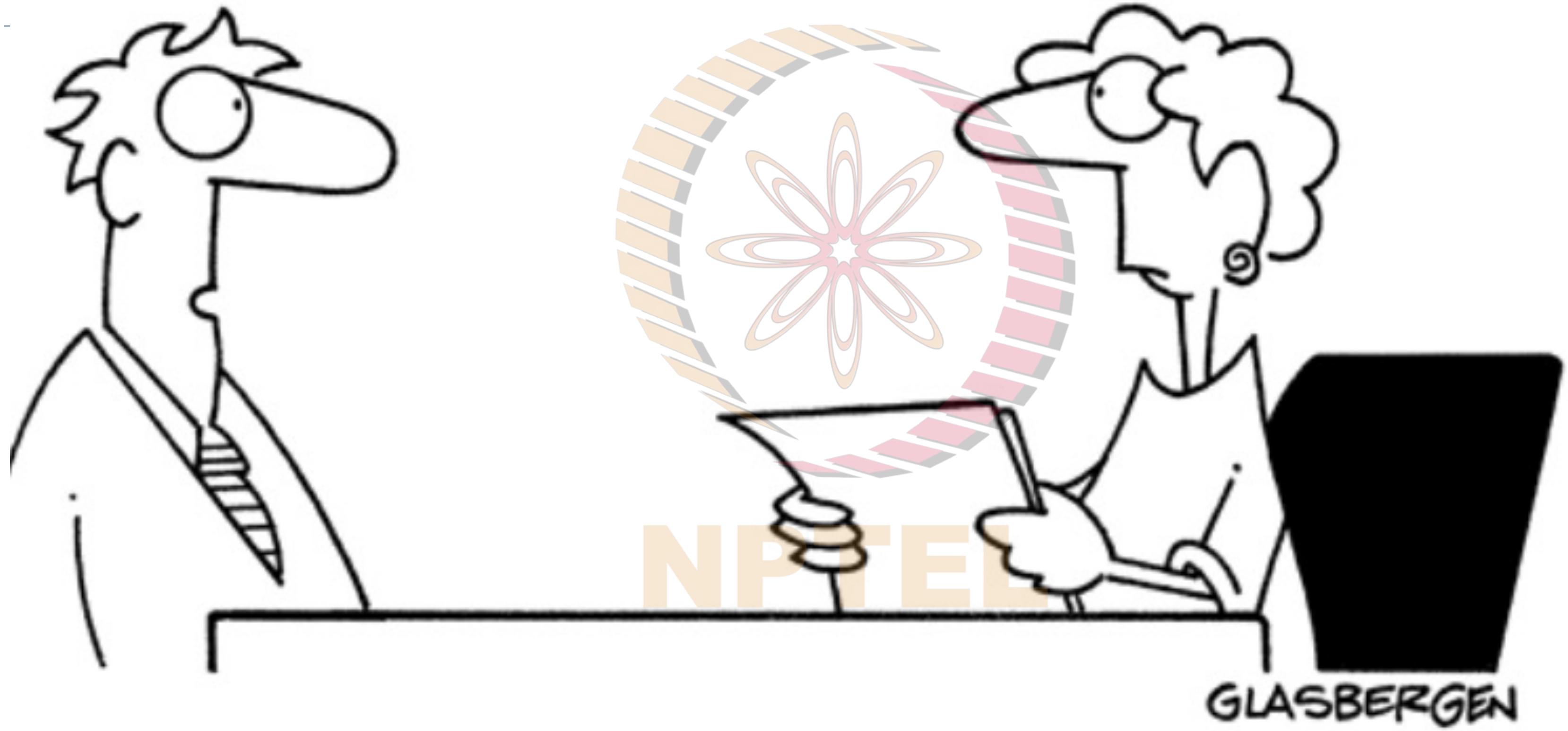
8:23 AM · Jul 17, 2020 · Twitter Web App

729 Retweets and comments 1.1K Likes

Twitter Support @TwitterSupport · Jul 17
Replying to @TwitterSupport
We're working with impacted account owners and will continue to do so over the next several days. We are continuing to assess whether non-public data related to these accounts was compromised, and will provide updates if we determine that occurred.

Summary

- Cyber security is a current and serious problem
  - Open a newspaper or business magazine
  - Pervasive digital technologies
- Cyber security affects individuals, organizations, society and government
  - The landscape of threats spread across units
- Privacy issues, data protection issues
  - policy angles, operational and management angles, as well as technology angles
- Triple role of technology
  - Source of threat, asset to protect and defense weapon



“For the sake of information security, everything on my résumé is false.”

What is security?

- "The quality or state of being secure--to be free from danger"
- To be protected from adversaries
- A successful organization should have multiple layers of security in place:
  - Physical security-areas of organization from unauthorized access and misuse.
  - Personal security- protection of individual or group.
  - Operations security – Focus protection of particular operation.
  - Communications security – Protect org. media, tech, content.
  - Network security – Components, connections, contents.
  - Information security- databases, analytics, insights

Cyber confusion

Which is correct?

A. cyber security

B. cyber-security

C. cybersecurity

- Cyber security form is common in Europe
- Cybersecurity form common in the America’s

- Cyber is borrowed from cybernetics, which implies control (Greek *steer man*)
- When applied to IT, it refers to the online world
- Often used as a stylized pre-fix
  - Cyber space, cyber koolies, cyber bullies etc.
- This course has no preferred spelling

Cyber security

- Cyber security often used interchangeably with the term information security.
- However, incidents of cyber-bullying, damage to equipment, media piracy, or cyber terrorism etc occur in cyber space, beyond information assets—ie. it includes humans as sources and targets of security

Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following: Availability, Integrity, which may include authenticity and non-repudiation and Confidentiality (ITU, 2008)

Information security

- Information security is the preservation of the *Confidentiality, Integrity and Availability (CIA)* of information (ISO/IEC 27002, 2005, p. 1)
- The protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information" (Whitman and Mattord, 2009)." 2018
  - Information security is not a product or a technology, but a process
  - Definitions is that information security is commonly defined in terms of the properties or characteristics that secure information should have. These usually include the confidentiality, integrity and availability of information, but can include additional characteristics.