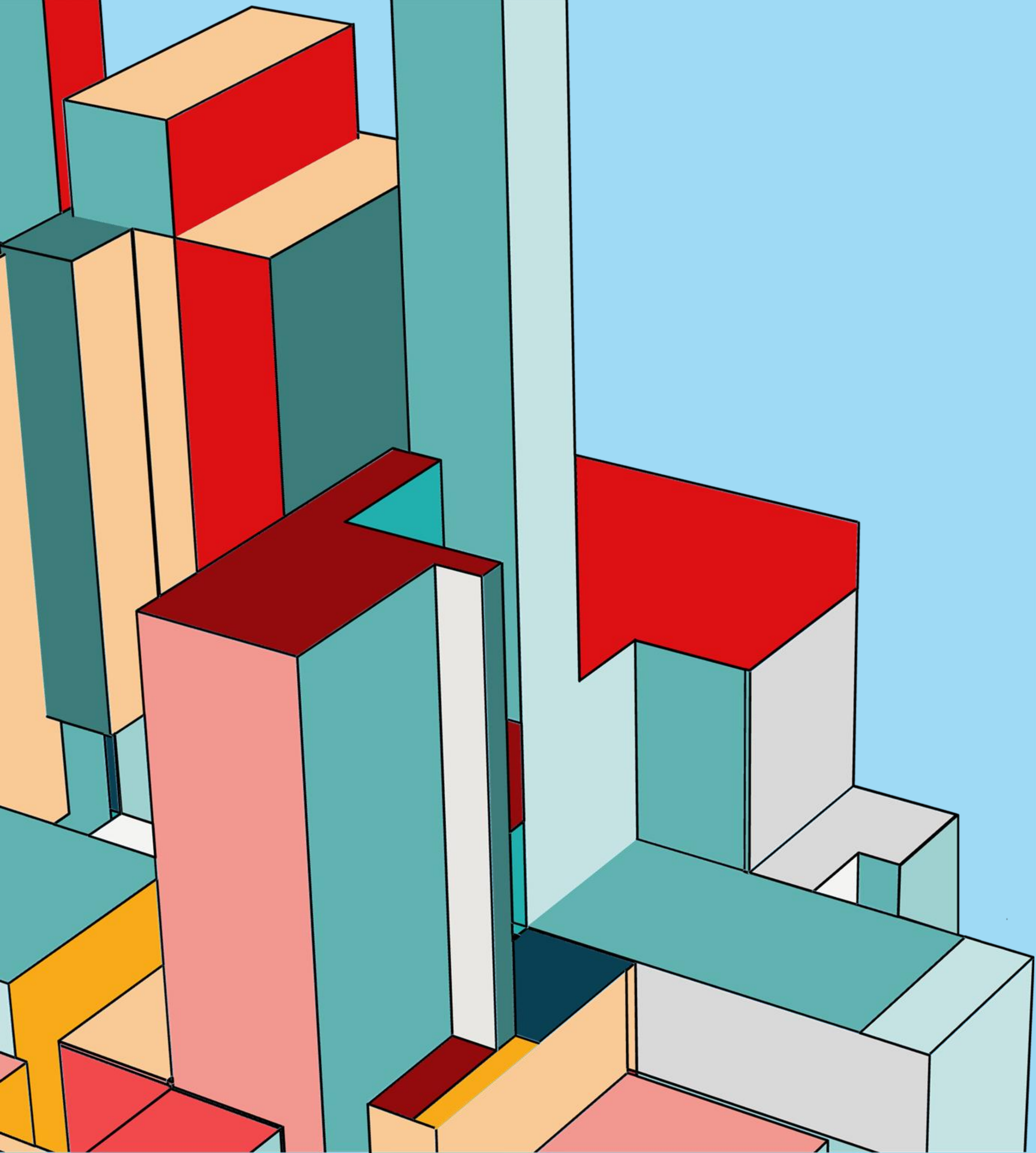
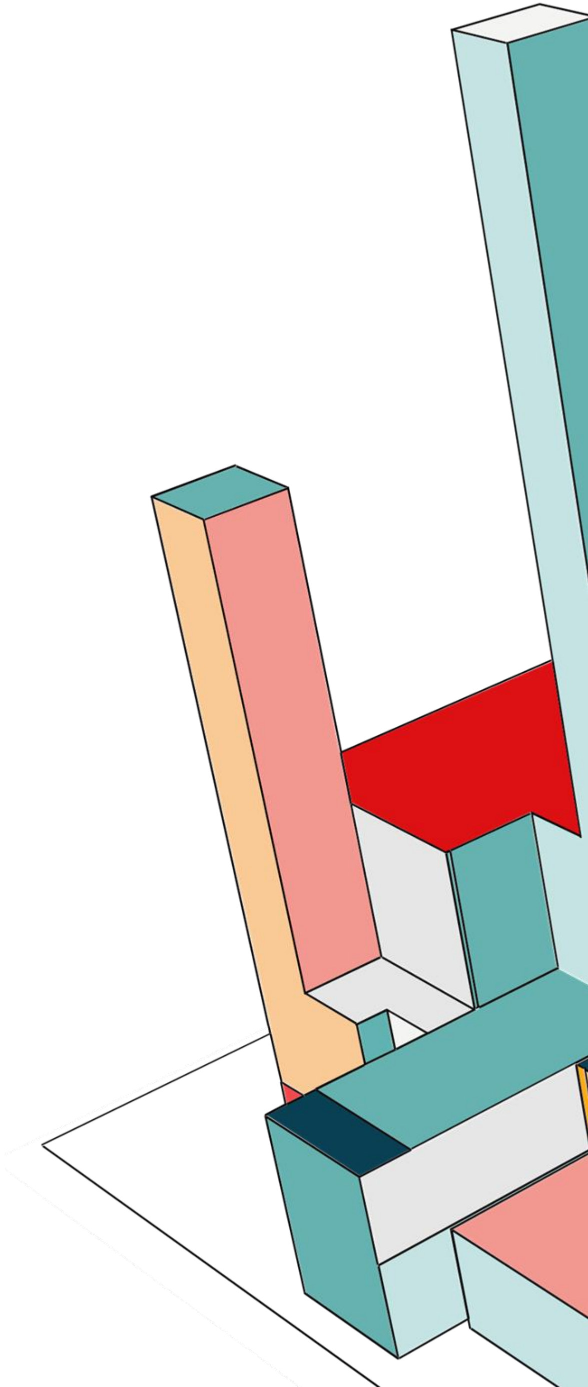


CYBER SECURITY AWARENESS SESSION

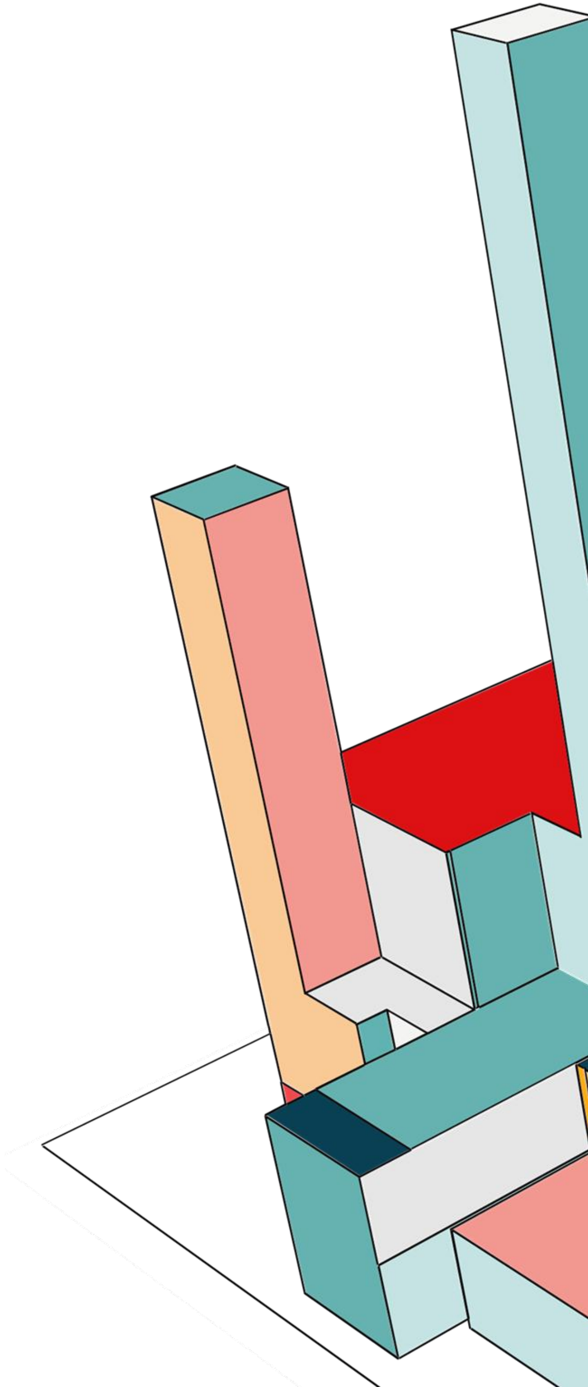
AGENDA

- Introduction
- Some common cyber threats seen in educational organization
- Known Cyber Attack currently taking more concern
- Some Important SoPs
- Incident Reporting



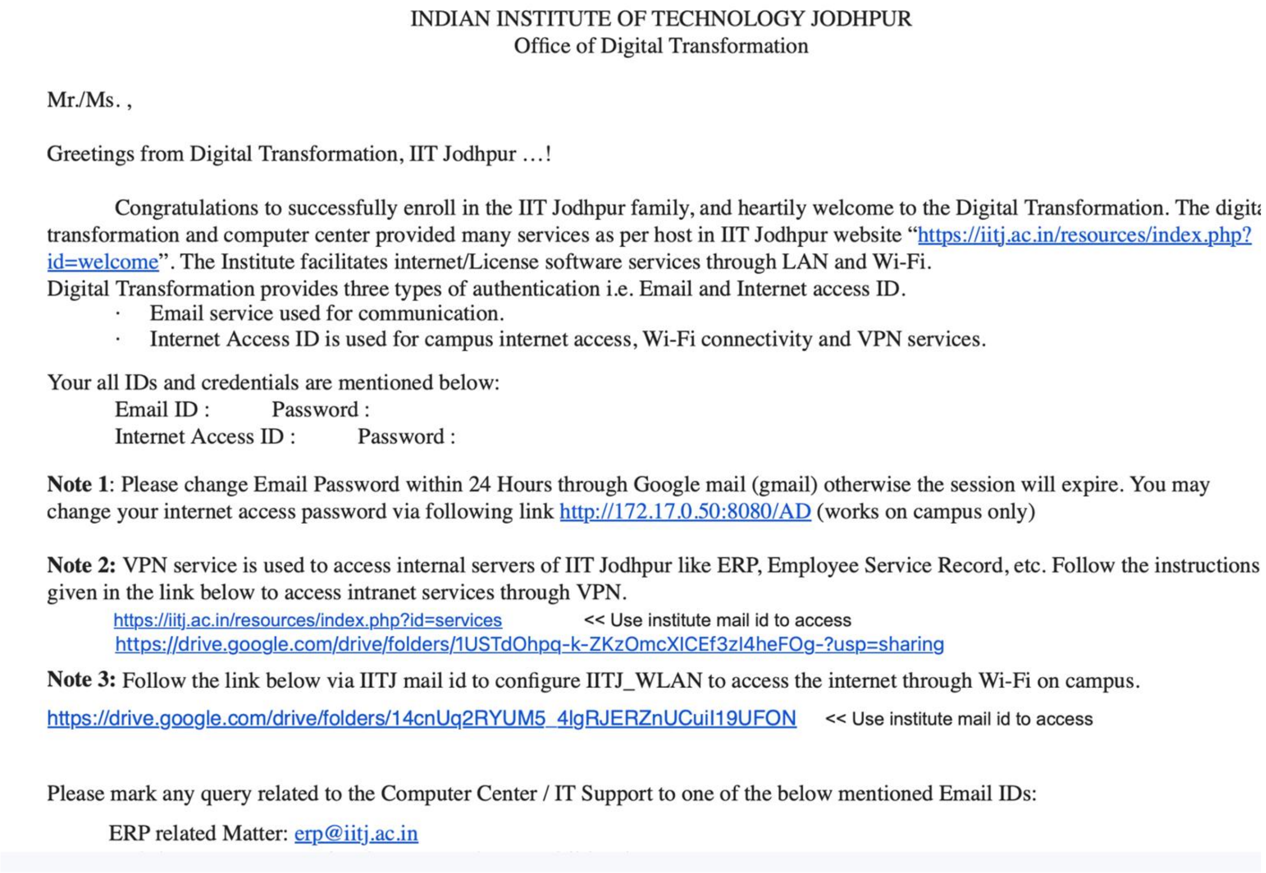
WHAT IS CYBER THREAT

- A cyber or cybersecurity threat is a malicious act that seeks to damage data, steal data, or disrupt digital life in general.
- Educational institutions are one of the most vulnerable targets for cybercrimes as they involve a huge amount of information and personal data of students.
- That’s why we need to implement strong cybersecurity measures and to make sure that our students are aware of the main rules on how to secure themselves and their data on the Internet



SOME COMMON CYBER THREATS SEEN IN EDUCATIONAL ORGANIZATION

Changing your default/welcome credentials immediately



INDIAN INSTITUTE OF TECHNOLOGY JODHPUR
Office of Digital Transformation

Mr./Ms. ,

Greetings from Digital Transformation, IIT Jodhpur …!

Congratulations to successfully enroll in the IIT Jodhpur family, and heartily welcome to the Digital Transformation. The digita transformation and computer center provided many services as per host in IIT Jodhpur website "https://iitj.ac.in/resources/index.php?id=welcome". The Institute facilitates internet/License software services through LAN and Wi-Fi.
Digital Transformation provides three types of authentication i.e. Email and Internet access ID.

- Email service used for communication.
- Internet Access ID is used for campus internet access, Wi-Fi connectivity and VPN services.

Your all IDs and credentials are mentioned below:
Email ID : Password :
Internet Access ID : Password :

Note 1: Please change Email Password within 24 Hours through Google mail (gmail) otherwise the session will expire. You may change your internet access password via following link http://172.17.0.50:8080/AD (works on campus only)

Note 2: VPN service is used to access internal servers of IIT Jodhpur like ERP, Employee Service Record, etc. Follow the instructions given in the link below to access intranet services through VPN.
https://iitj.ac.in/resources/index.php?id=services << Use institute mail id to access
https://drive.google.com/drive/folders/1USTdOhpq-k-ZKzOmcXICEf3zl4heFOg-?usp=sharing

Note 3: Follow the link below via IITJ mail id to configure IITJ_WLAN to access the internet through Wi-Fi on campus.

https://drive.google.com/drive/folders/14cnUq2RYUM5_4lgRJERZnUCuil19UFON << Use institute mail id to access

Please mark any query related to the Computer Center / IT Support to one of the below mentioned Email IDs:

ERP related Matter: erp@iitj.ac.in

What to do by user ?

- As soon as you receive similar email, kindly change your password immediately.

Main three password you generally need to reset

- Internet Access Password **(http://172.17.0.50:8080/AD from inside the campus)**
- Email Password (i.e your gmail account)
- ERP Password.

PHISHING EMAILS

A phishing email is a type of social engineering attacks where an attacker tricks target victims into opening a malicious file or link or providing personal or confidential information, such as passwords, credit/debit card number etc.

How to be cautious against Phishing Attacks?

- Be suspicious of any email with urgent request for personal information.
- Never Share passwords, personal information or financial information over email.
- Don’t click links in email messages if you suspect the message might not be authentic or if you don’t know the sender.
- Don’t trust offers that seem too good to be true. (if somebody pretending your relative want to send money to you, winning lottery etc.

PHISHING EMAILS

E.G.

Phishing Example: Library Account

Dear Student, Your access to your library account is expiring soon due to inactivity. To continue to have access to the library services, you must reactivate your account. For this purpose, click the web address below or copy and paste it into your web browser. A successful login will activate your account and you will be redirected to your library profile. https://lib@iitj.com

How to be cautious against Phishing Attacks?

- Here we have to check the link provided in the email
- Our domain is **@iitj.ac.in**, if any link or url received to reset password related IIT Jodhpur, mostly come from our domain only.

EMAIL FRAUD (GIFT CARD SCAMS)

Gift card scams are on the rise and can result in a victim losing hundreds or thousands of rupees.

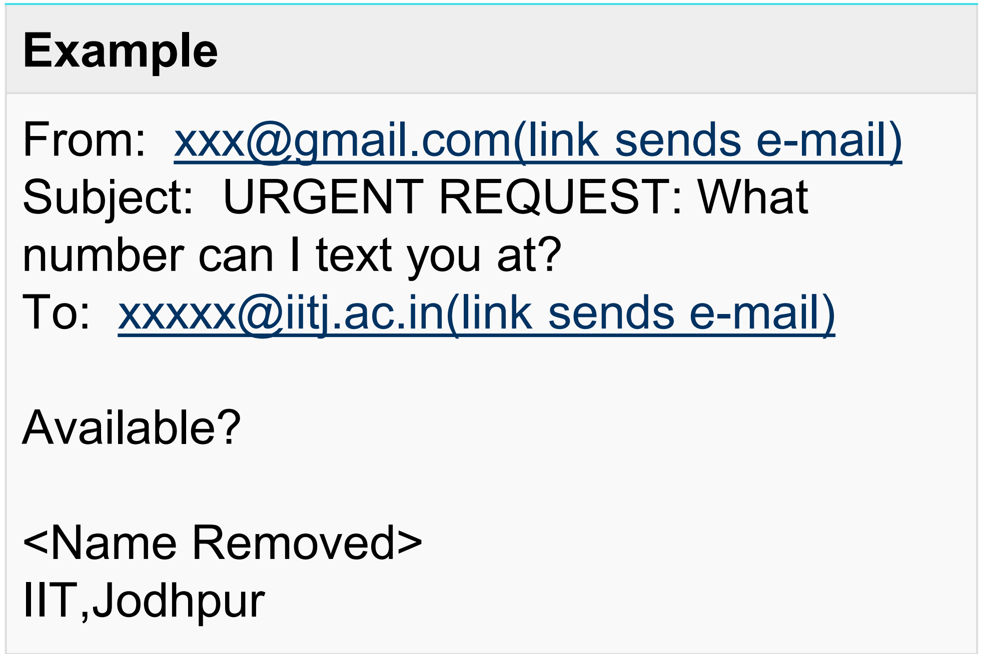
In a typical scam, an employee/student receives an email or a text message that pretends to be from their co-student, faculty members, or another senior figure or person of authority. It asks them to buy gift cards and send them photos.

The scammer may ask you to communicate with them via text message or email only, unable to take calls.

How to Spot a Gift Card Scam ?

- Inspect the sender's email address to confirm it's actually coming from that person. Scammers will often send the email from a random email account and change the Display Name of the email address.
- If the sender’s address ends in @gmail.com, @outlook.com, or anything other than @iitj.ac.in, the request is most likely a scam.

EMAIL FRAUD (GIFT CARD SCAMS)



Example

From: xxx@gmail.com(link sends e-mail)
Subject: URGENT REQUEST: What number can I text you at?
To: xxxxx@iitj.ac.in(link sends e-mail)

Available?

<Name Removed>
IIT,Jodhpur

Identifying Gift card scam email messages :-

- Indicate some level of urgency, such as indicating they are currently busy or are heading into a meeting and need your help ASAP
- Possibly include a subject line of "are you are available?" or "URGENT REQUEST“
- Ask you to do them a "favor“, promise of Reimbursement..
- Possibly have typos and grammatical errors.

What should I do?

1. If you get an email from a colleague asking if you "are available?" or asking for you to only "text them", before responding, **reach out to the sender in a separate email or call them** to check if they actually sent the request.
2. Don't reply to the email or use any contact information provided in the email - attackers often provide fake numbers or email addresses that they control.
3. If you find the email is a phish, report it! (cybersec@iitj.ac.in)

BLACKMAIL OR SEXTORTION EMAILS

Its an email scam where an attacker claims to have compromised victims' machine, sensitive data including sexual content and picture.

The attacker demands payment, bitcoins, gift cards or more photos, and threatens to publish the data to the internet.

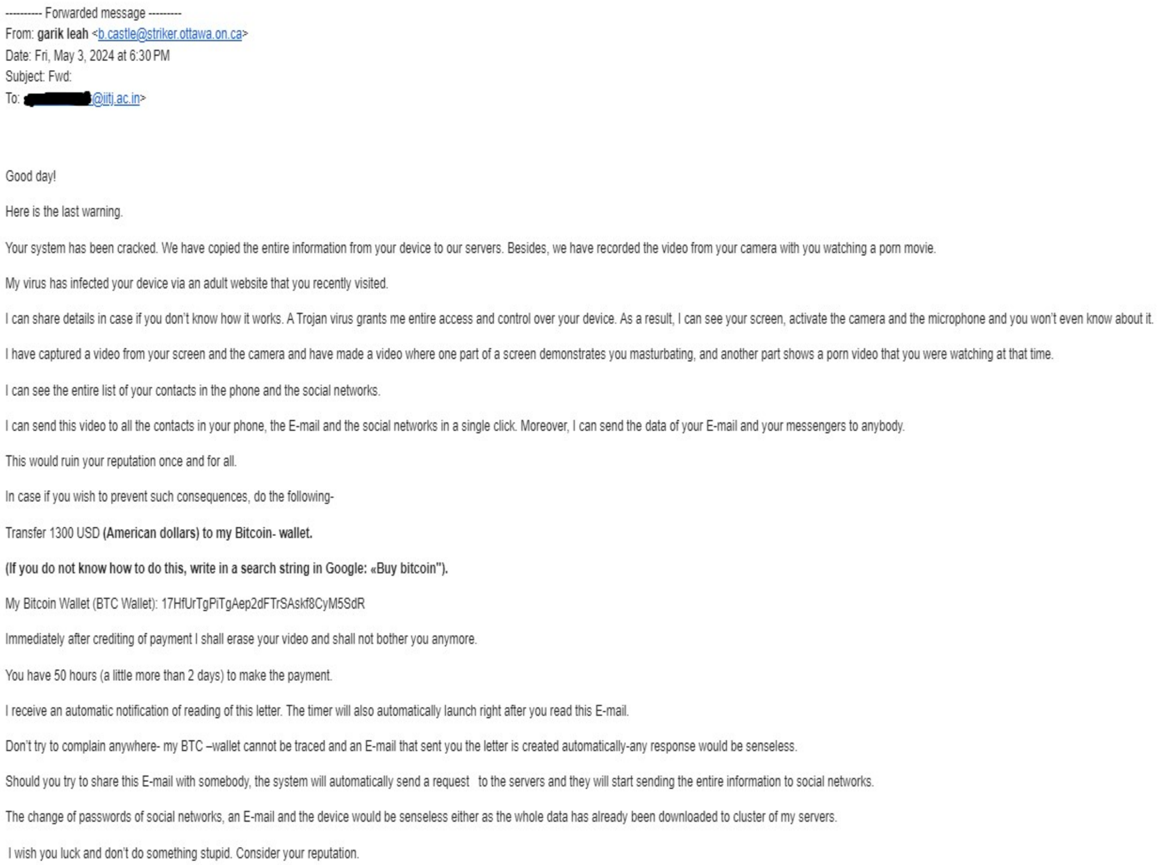
Example:-

the emails claim to have video of users watching "adult sites" and demanding $900 if they don't want the video shared with all of their contacts.

How to respond to sextortion ?

- Stop responding and do not pay.
- Talk with someone you trust, like a close friend, teacher or parent. Otherwise reach IITJ student wellbeing committee and alo report to us at **cybersec@iitj.ac.in**
- Report tech companies, report any threats and images to help center of Facebook, Instagram etc. to remove if shared.
- Do not worry if the phish includes your password; likely this has been obtained from historic breaches of personal data. If the phish includes a password you still use then change it immediately,
- Keep your personal details private.

BLACKMAIL OR SEXTORTION EMAILS



---------- Forwarded message ---------
From: **garik leah** <b.castle@striker.ottawa.on.ca>
Date: Fri, May 3, 2024 at 6:30 PM
Subject: Fwd:
To: [redacted]@iitj.ac.in>

Good day!

Here is the last warning.

Your system has been cracked. We have copied the entire information from your device to our servers. Besides, we have recorded the video from your camera with you watching a porn movie.

My virus has infected your device via an adult website that you recently visited.

I can share details in case if you don't know how it works. A Trojan virus grants me entire access and control over your device. As a result, I can see your screen, activate the camera and the microphone and you won't even know about it.

I have captured a video from your screen and the camera and have made a video where one part of a screen demonstrates you masturbating, and another part shows a porn video that you were watching at that time.

I can see the entire list of your contacts in the phone and the social networks.

I can send this video to all the contacts in your phone, the E-mail and the social networks in a single click. Moreover, I can send the data of your E-mail and your messengers to anybody.

This would ruin your reputation once and for all.

In case if you wish to prevent such consequences, do the following-

Transfer 1300 USD **(American dollars) to my Bitcoin- wallet.**

(If you do not know how to do this, write in a search string in Google: «Buy bitcoin").

My Bitcoin Wallet (BTC Wallet): 17HfUrTgPiTgAep2dFTrSAskf8CyM5SdR

Immediately after crediting of payment I shall erase your video and shall not bother you anymore.

You have 50 hours (a little more than 2 days) to make the payment.

I receive an automatic notification of reading of this letter. The timer will also automatically launch right after you read this E-mail.

Don't try to complain anywhere- my BTC –wallet cannot be traced and an E-mail that sent you the letter is created automatically-any response would be senseless.

Should you try to share this E-mail with somebody, the system will automatically send a request to the servers and they will start sending the entire information to social networks.

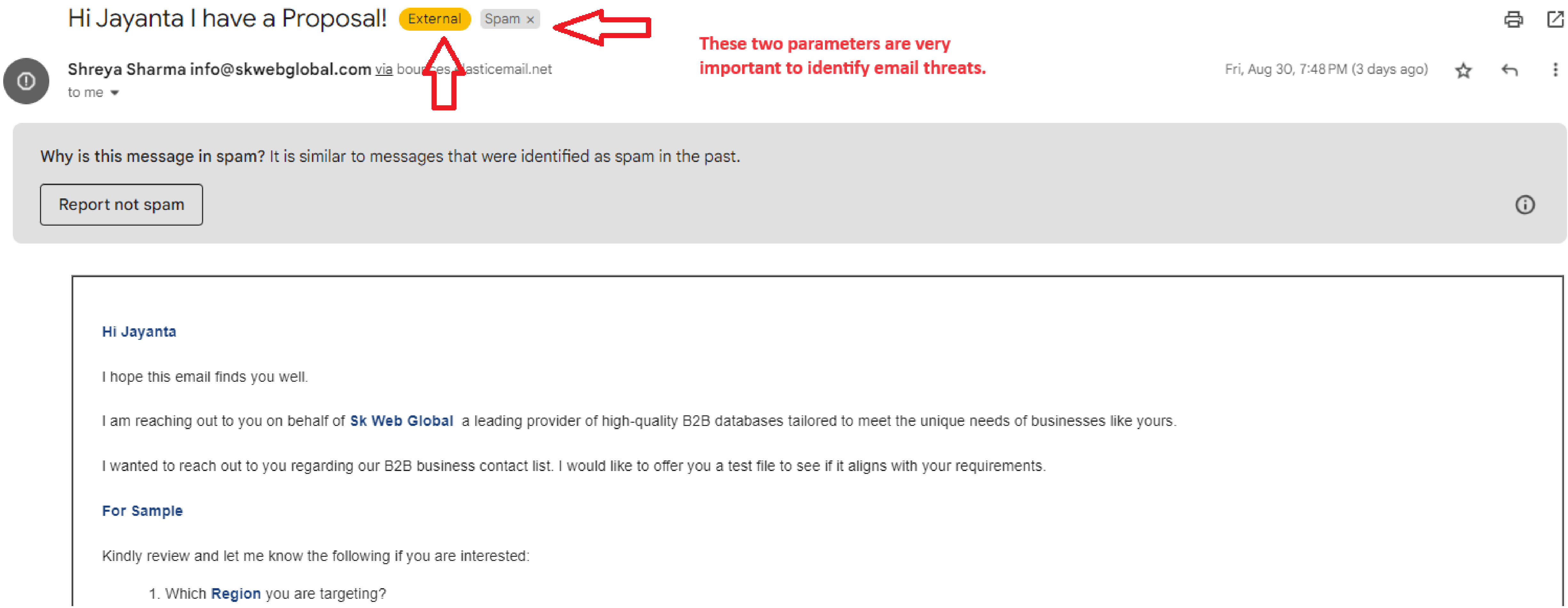
The change of passwords of social networks, an E-mail and the device would be senseless either as the whole data has already been downloaded to cluster of my servers.

I wish you luck and don't do something stupid. Consider your reputation.

What to do by user ?

- First of all, don't panic.
- We recommend you to ignore this type of communication. Its a type of blackmail email also known as "Sextortion"
- However, if you download any attachment or click any links from this email or suspect that your PC or mobile might be infected with malware you can scan your device for malware.
- Some notable free antivirus like Sophos home premium, hitman pro, Bitdefender you can use.

EMAILS IDENTIFICATIONS



Hi Jayanta I have a Proposal! External Spam ×

These two parameters are very important to identify email threats.

Shreya Sharma info@skwebglobal.com via bounces.elasticemail.net

to me

Fri, Aug 30, 7:48 PM (3 days ago)

Why is this message in spam? It is similar to messages that were identified as spam in the past.

Report not spam

Hi Jayanta

I hope this email finds you well.

I am reaching out to you on behalf of **Sk Web Global** a leading provider of high-quality B2B databases tailored to meet the unique needs of businesses like yours.

I wanted to reach out to you regarding our B2B business contact list. I would like to offer you a test file to see if it aligns with your requirements.

For Sample

Kindly review and let me know the following if you are interested:

1. Which **Region** you are targeting?

RANSOMWARE

Ransomware is a type of malware that encrypts a victim’s files and demands payment, usually in cryptocurrency, in exchange for the decryption key.

Ransomware attacks are typically carried out through phishing emails, malicious downloads, or exploiting vulnerabilities in software.

In recent years, educational institutions have become larger prime targets for ransomware attacks.

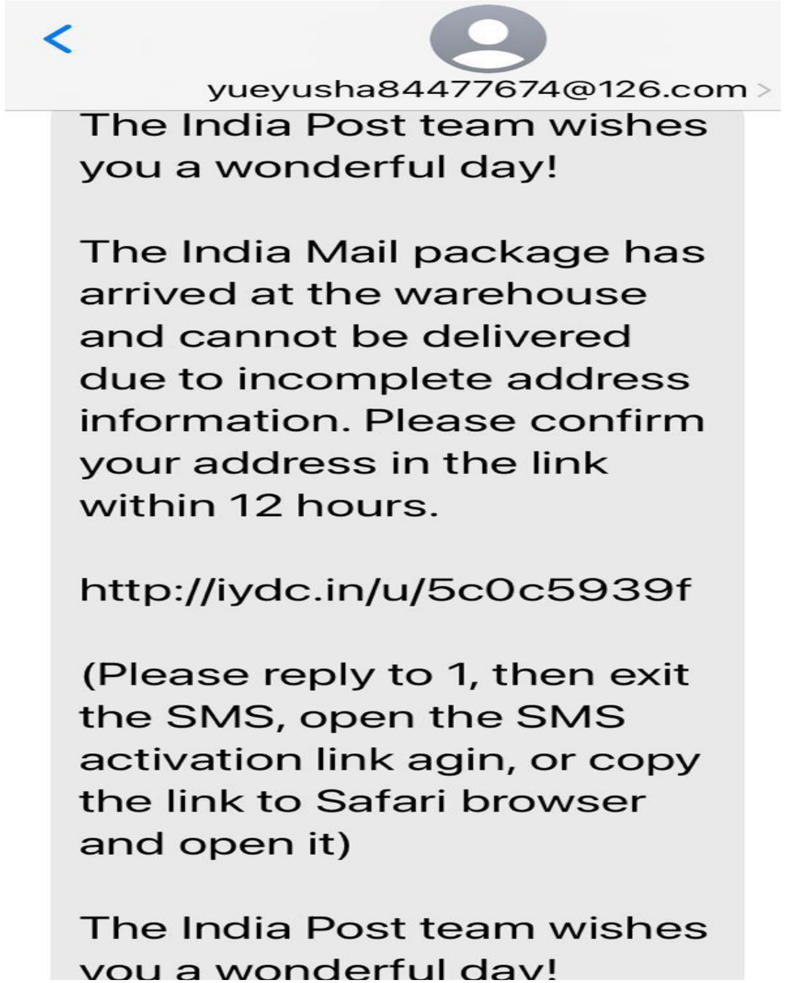
How to protect yourself from Ransomware threats:-

- Don’t open unexpected email attachments.
- Make backups of your data and keep them separate.
- Install and use endpoint protection software like antivirus/EDR
- Update with latest OS and patches regularly.
- Don’t click links in email if sender is unknown.

SOME OTHER KNOWN CYBER ATTACK CURRENTLY TAKING MORE CONCERN

Fake India Post delivery Scam

- The fraudsters send an SMS stating the status of delivery of an India Mail package which could not be delivered due to incomplete address information.
- They provide a deadline of 12 hours for recipients to confirm their address by clicking on the given link (http://iydc[.]in/u/5c0c5939f).
- This misleading message seeks to fool people into disclosing personal information or compromising the security of their device.
- Don’t click these link, if required verify with Indian Post.



yueyusha84477674@126.com

The India Post team wishes you a wonderful day!

The India Mail package has arrived at the warehouse and cannot be delivered due to incomplete address information. Please confirm your address in the link within 12 hours.

http://iydc.in/u/5c0c5939f

(Please reply to 1, then exit the SMS, open the SMS activation link agin, or copy the link to Safari browser and open it)

The India Post team wishes you a wonderful day!

SOME OTHER KNOWN CYBER ATTACK CURRENTLY TAKING MORE CONCERN

New parcel fraud:'Drug was found in your parcel, will inform police';

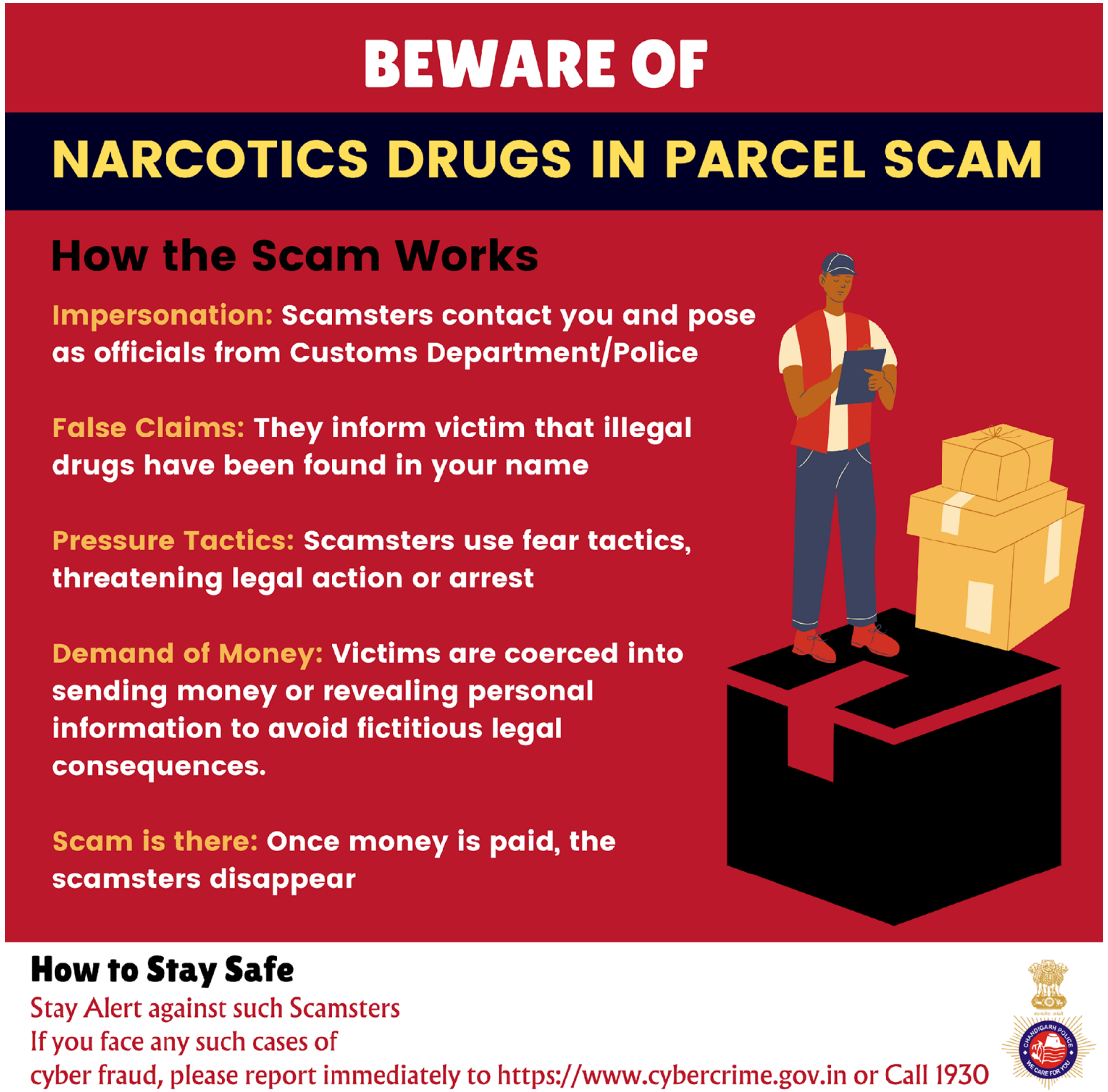
- Fraudsters are posing as fake courier staff or customs officers to scam you.
- They call you to inform that the customs department under the Central Board of Indirect Taxes & Customs (CBIC) has intercepted a parcel/package in your name.
- Now they demand you to pay customs duty or tax on it.
- Sometimes the scamsters with an aim to build a more convincing narrative, say that drugs have been found in such parcels/packages and you need to pay a bribe to get this parcel destroyed along with other evidence.

- **How can you recognise the parcel scam and protect yourself?**

a. You should first verify and cross-check the information.

b. Don't rush into making a transaction or provide any personal or financial details.

c. For instance, all communications from Indian Customs consist of a document identification number (DIN), which can be verified on the CBIC website- https://esanchar.cbic.gov.in/DIN/DINSearch



BEWARE OF

NARCOTICS DRUGS IN PARCEL SCAM

How the Scam Works

Impersonation: Scamsters contact you and pose as officials from Customs Department/Police

False Claims: They inform victim that illegal drugs have been found in your name

Pressure Tactics: Scamsters use fear tactics, threatening legal action or arrest

Demand of Money: Victims are coerced into sending money or revealing personal information to avoid fictitious legal consequences.

Scam is there: Once money is paid, the scamsters disappear

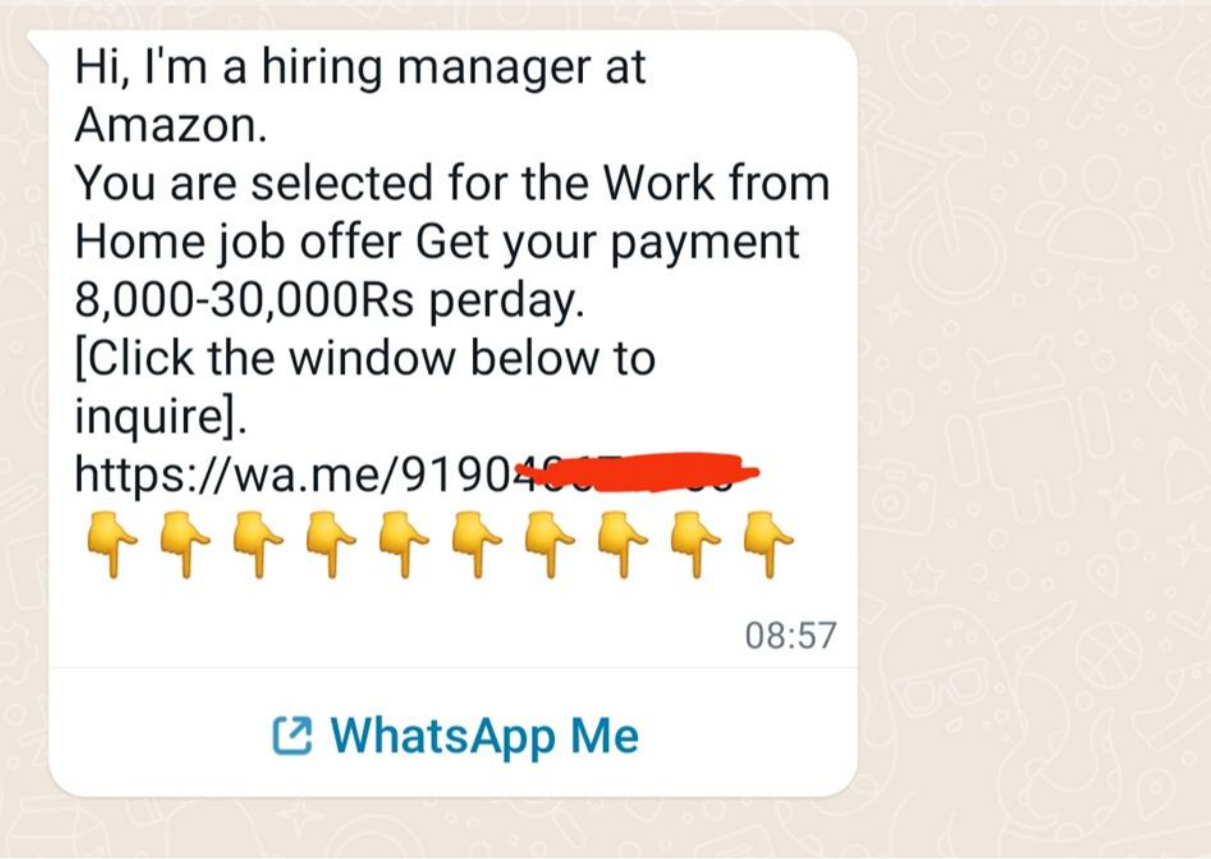
How to Stay Safe

Stay Alert against such Scamsters
If you face any such cases of
cyber fraud, please report immediately to https://www.cybercrime.gov.in or Call 1930

SOME OTHER KNOWN CYBER ATTACK CURRENTLY TAKING MORE CONCERN

Work-From-Home Job Scam:-

- User received the text on his WhatsApp number that user can do a work-from-home job in which he/she need to rate hotels on Google Maps and will receive money in return as rewards.
- User was then added to a Telegram group with about 100 members, where he/she started performing the rating tasks, the tasks soon included investment activities.
- User later unable to withdraw his investment money and requesting additional money as a TAX.
- Therefore, be cautious when accepting work from home tasks and disclose information only after thorough verification.



Hi, I'm a hiring manager at Amazon.
You are selected for the Work from Home job offer Get your payment 8,000-30,000Rs perday.
[Click the window below to inquire].
https://wa.me/9190[redacted]
👇👇👇👇👇👇👇👇👇👇

08:57

UPI Frauds and Tips to Prevent it?

UPI (Unified Payment Interface) is an instant payment system created by the National Payments Corporation of India (NPCI). It facilitates instant money transfers between the bank accounts of the two parties.

Types of UPI Fraud

- **Impersonating Sellers Fraud :-** Often, fraudsters use a seller's number to receive orders from customers. In such a situation, they will take the order and ask the customer to make the payment using UPI. Thus, the fraudster will get the money and not deliver the product.

- **UPI Fraud via Authorized Access to Screen Mirroring Apps:-** In this case, fraudsters posing as bank employees will try to connect with you or list customer care numbers online that are actually fake. If you try to connect on this number for any complaints, the fraudster will ask you to download 3rd party apps, which are screen mirroring apps. These apps provide complete access to your device through which they carry out unapproved financial transactions.

- **OTP or PIN Fraud:-** This is one of the most common types of **UPI transaction fraud**. Many individuals share their OTPs or PIN with fraudsters unknowingly. After that, these fraudsters gain access to the individual's account and make unauthorised transactions using UPI.

- **UPI Fraud via Collection Request:-** A collection request scam is quite common with UPI Payment Apps. Scammers committing this fraud usually provide a reason of a refund or debit reversal and then compel you to click on 'Collect Request'. Once you click on it, you will be asked to provide your UPI PIN. As soon as you enter the PIN, scammers immediately debit the money from your bank account.

Tips to prevent UPI Fraud

- **Don't Share UPI PIN**
- **Avoid Downloading Apps You Don't Trust**
- **Check the Credibility of the UPI ID before Scanning**
- **You must follow some security measures, like:**
  - **Install anti-virus software on your device.**
  - **Install biometric recognition software on your device.**
  - **Don't open links from unreliable sources.**

Some Important SoPs

- Don't Share password with anyone.
- Always use 2FA whenever possible with complex passwords.
- Keep all your systems (Laptop/Desktop/Mobile) always updated with latest versions.
- Its recommended to use an antivirus software in your systems.
- Scan the removable media with Antivirus software before accessing.
- Internet Surfing:- Do Not use proxy or other sites to bypass campus firewall security.
    - Don’t install any network switches and Wi-Fi Access point/router without informing DIA.
- Limit and control the use/exposure of personal information while accessing social media and networking sites.
- Always check the authenticity of the person before accepting a request as friend/contact.

INCIDENT REPORTING

- **If you suspect a cybersecurity incident or data breach, report it by sending an email to our Cyber Security team immediately at (cybersec@iitj.ac.in).**
- **Remember that cybersecurity is a shared responsibility, and your actions are crucial in maintaining a secure academic environment.**
- **Stay vigilant, stay informed, and help protect your institutes digital assets and personal information.**
- **Always follows the SoP’s and Cyber Security policies of the institute.**

THANK YOU