



# Cybersecurity Awareness Primer

Security, safety and hygiene



# Background to the CoE



IISc is the Anchor institute



**K-tech**

Initiative of GoK, Department of  
IT, BT, S&T and Karnataka  
Innovation and Technology  
Society



KSCST is the Implementation  
Agency



# CySecK Programme structure



## Awareness

- Cybersecurity awareness to citizens
- Cybersecurity awareness to school students
- Cybersecurity awareness for GoK staff



## Skill building

- Technology community (students / working professionals)
- Faculty development programme
- Create a marketplace for cybersecurity courses
- Community cyber lab



## Research Collaboration

- Research Grant Programme – for top institutes
- Research Development Programme for Tier 2 institutes



## Industry and startups

- Cybersecurity startup accelerator
- Development of standard specifications / best practices / reference architectures
- Cybersecurity awareness to MSME sector
- Policy advocacy for enabling industry



## Government

- Provide cybersecurity assistance / guidance to state government entities
- Support the Dept with actionising Cyber Security Strategy
- Provide technical support to K-CSIRT



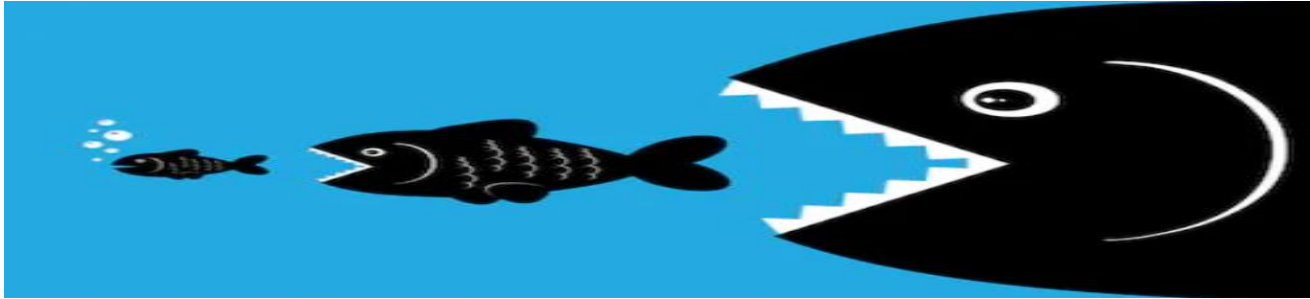


# Why is Cybersecurity important?

A philosophical view



# What story connects the two images?





# Why is it easy to commit cyber crime?



Anonymity



# Why is it easy to commit cyber crime?



IaaS  
PaaS  
SaaS  
CaaS

Anonymity

Crumbling barriers



# Why is it easy to commit cyber crime?



Anonymity

Crumbling barriers

Lack of jurisdiction



# Why is it easy to commit cyber crime?



Anonymity

Crumbling barriers

Lack of jurisdiction

Ease of laundering



# Why is it easy to commit cyber crime?



Anonymity

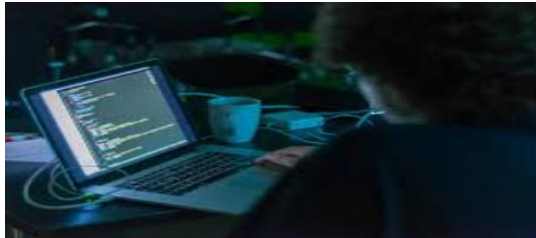
Crumbling barriers

Lack of jurisdiction

Ease of laundering



# The varied threat actors...



Script kiddies



Hobby hackers



Hacktivists



Nation-state actors

Classification: Public

Syndicates



Insider



# Cybersecurity during Covid19



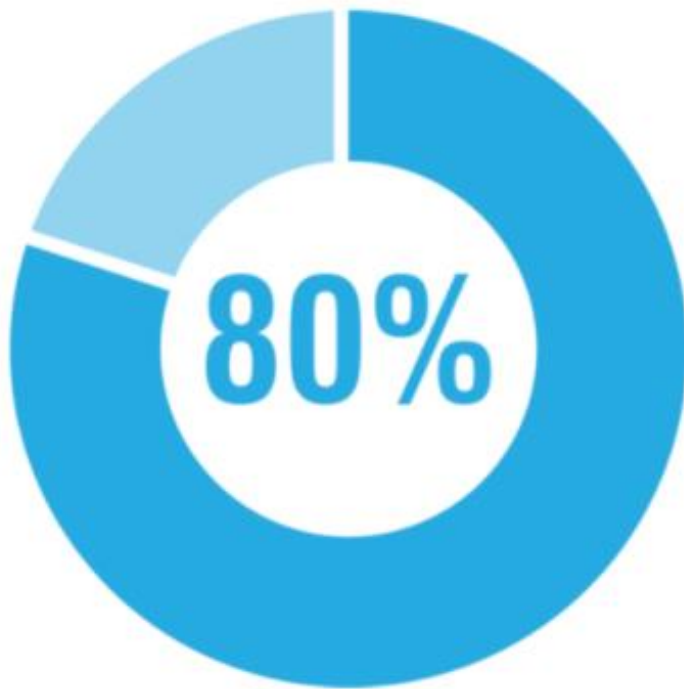
31% of companies around the world are attacked at least once a day. India reported almost twice as many attacks per day as any other country. 9% of all companies are targeted by cyberattacks at least once an hour.

## Covid-19 leads to sharp increase in phishing attacks

Phishing incidents rose 220% YoY at the height of the Covid-19, F5 Labs report says



# Importance of cyber hygiene



“ 80% of the problem can be solved by getting the cyber hygiene correct, rather than chasing the latest advanced technology. \* ”

Source- [cyber-observer.com](https://cyber-observer.com)





# ***CYBER THREATS***



# Phishing



## Pre-email era

### URGENT BUSINESS PROPOSAL

WE HAVE THIRTY MILLION U.S. DOLLARS WHICH WE GOT FROM OVER INFLATED CONTRACT FROM CRUDE OIL CONTRACT AWARDED TO FOREIGN CONTRACTORS IN THE NIGERIAN NATIONAL PETROLEUM CORPORATION (NNPC). WE ARE SEEKING YOUR ASSISANCE AND PERMISSION TO REMIT THIS AMOUNT INTO YOUR ACCOUNT. YOUR COMMISSION IS THIRTY PERCENT OF THE MONEY.

PLEASE NOTIFY ME YOUR ACCEPTANCE TO DO THIS BUSINESS URGENTLY. THE MEN INVOLVED ARE MEN IN GOVERNMENT. MORE DETAILS WILL BE SENT TO YOU BY FAX AS SOON AS WE HEAR FROM YOU. FOR THE PURPOSE OF COMMUNICATION IN THIS MATTER, MAY WE HAVE YOUR TELEFAX, TELEX AND TELEPHONE NUMBERS INCLUDING YOUR PRIVATE HOME TELEPHONE NUMBER.

CONTACT ME URGENTLY THROUGH THE FAX NUMBER ABOVE.

PLEASE TREAT AS MOST CONFIDENTIAL, ALL REPLIES STRICTLY BY DHL COURIER, OR THROUGH ABOVE FAX NUMBER.

THANKS FOR YOUR CO-OPERATION.

YOURS FAITHFULLY,

3/23/95  
PRINCE JONES DIMKA

3-4-95

## Email era



Dear Customer,

Greetings from ICICI Bank.

At ICICI Bank it is our constant endeavour to ensure the safety of your Netbanking account. We are working round the clock to provide our customers with up to date security during their Netbanking session.

Therefore we are requestion you to update your Netbanking details with our database by downloading the Mandatory ICICI Form attached Below this email.

Please Download the Mandatory Form Attached Below and Update Your Details

Looking forward to more opportunities to be of service to you.

Warm Regards,

ICICI Bank Online

Now banking is more convenient with:

More than 5300 ICICI Bank Branches	24x7 ATM Services	ICICI Bank Customer Care	ICICI Bank Internet Banking	Mobile Banking Services
---------------------------------------	----------------------	-----------------------------	--------------------------------	----------------------------

The products, services and offers referred to herein are subject to the terms and conditions governing them as specified by ICICI Bank / third party from time to time and are offered at the sole discretion of ICICI Bank / third party. ICICI Bank is not responsible for the goods/services provided by third parties. Nothing contained herein shall constitute or be deemed to constitute an advice, invitation or solicitation to purchase any products/ services of ICICI Bank.

If you do not wish to receive further marketing e-mails, please register under 'Do Not Call' registry on [www.kicibank.com](http://www.kicibank.com)



# Phishing identification cheat sheet



- Did you expect this?
- Did it identify you? Or is it asking you to identify yourself?
- Are there spelling / grammatical mistakes
- Observe the email id – both displayed as well as actual email id
- Do not trust URL text; see the URL carefully by hovering over
- Do not click on the URL; login to the legitimate site directly
- Do not go by look and feel
- Check full URL of shortened URLs
- Be wary of unsolicited attachments
- Is it trying to bait you with urgency?

<http://www.karnataka.gov.in/>



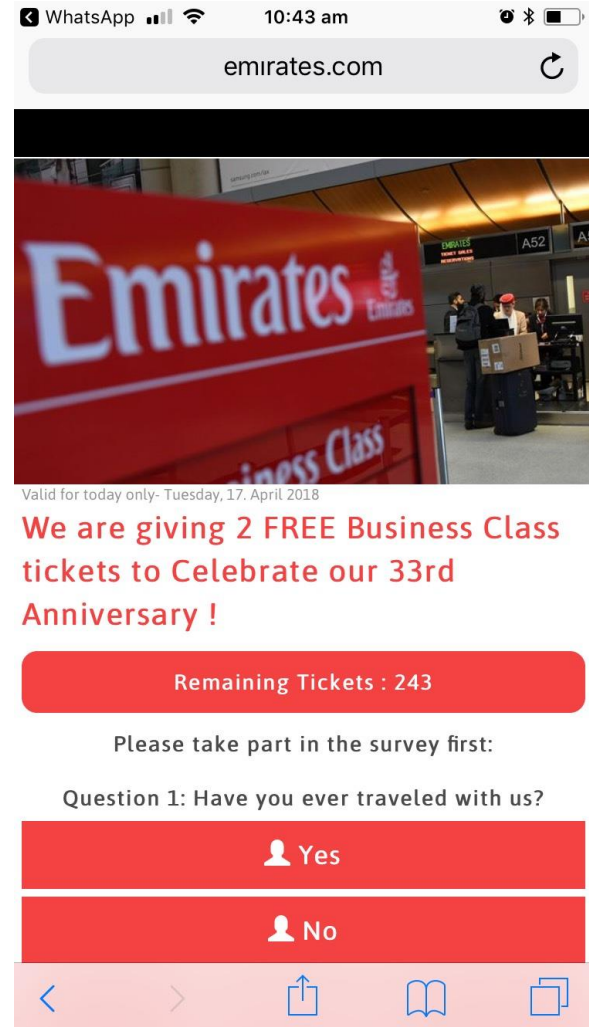
# Case Study

You receive this message on WhatsApp.

Emirates Airline is giving away 2 Free Business class Tickets to everyone on it's 33rd anniversary, Get your Free Tickets : <http://www.emirates.com/mytickets>  
Enjoy your flight !

This is a very smartly done phishing attack, the web address looks authentic, its spelled correctly but if you notice closely the dot on the alphabet i is missing. Phishing attacks are pretty easy to detect, its just you have to be a little extra alert.

Make sure you stay away from such forward links !!! There is No Free Food in this world !!!





# Click Email Links with caution



## Examples of when to click

- You just ordered something from Flipkart. Feel free to click the shipment tracking link in the email they send you. Just make sure it's exactly what you're expecting. If you get a tracking link that you weren't expecting, or for a product you don't recognize, delete the email right away.
- You just signed up for an account on a website. If they send you a link to confirm your email address, it's okay to click it. But again, make sure it's exactly what you're expecting, and you remember requesting it.

## Examples of when NOT to click

- You get an unexpected email from your Organization. Maybe it says that you need to log in and take care of something important. Don't click the link they give you. If you didn't know it was coming, there's no guarantee it's a legitimate email.
- Your friend sends you a link that you weren't expecting. Don't click it. Remember, the sender's address can be spoofed or their account hacked. Yeah, I know, this is all awfully annoying, so is there anything else we can do?



## Other types of phishing attacks



Vishing



Voice phishing

Smishing

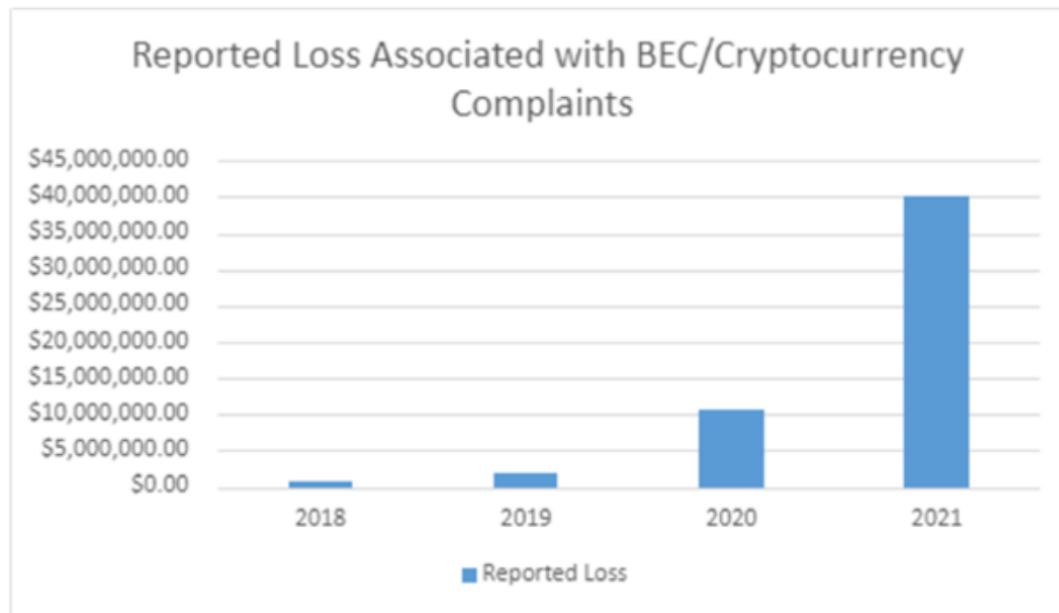


SMS phishing





## Targeted phishing attack!







# Nykaa Loses 62Lakh To Cyber Fraud

Fraudsters tricked Nykaa by spoofed emails which redirected Nykaa's payment intended for one of its Italian suppliers to their own bank accounts. How did this spoofed email work? The criminals imitated a valid supplier's email address. Emails from such an address would've appeared as authentic, as the



# Whaling



- Whaling is also a type of phishing attack where a high-profile target is attacked.
- The objective of whaling?
  - Target a senior person in the organisation
  - Get money transferred by masquerading as the senior person
  - Steal sensitive information like intellectual property





# Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case

Scams using artificial intelligence are a new challenge for companies

## **Austria's FACC, hit by cyber fraud, fires CEO**

FACC, whose customers include Airbus and Boeing, said on Jan. 19 it had been hit by a cyber fraud in which hackers stole around 50 million euros by posing as Stephan in an email.

The hoax email asked an employee to transfer money to an account for a fake acquisition project - a kind of scam known as a “fake president incident”.



# Socially Engineered attacks



- Socially Engineered Attacks aim at taking advantage of human trust and using psychological manipulation to deceive users to gain access to sensitive information or to conduct fraud.
- Stages in a socially engineered attack







# BrahMos Engineer Arrested For Spying, "Chatted On Facebook With Pak IDs"

Nishant Agrawal has worked in the technical research section of the missile centre for four years. He studied at the National Institute of Technology in Kurukshetra, was a gold medalist and is described as a very bright engineer

## Group Captain Arun Marwah was honey-trapped, blackmailed by ISI

*Indian Air Force officer Arun Marwah, who was arrested by Delhi Police for leaking classified information to a woman, fell for the oldest trick of Pakistan's ISI.*

The officer, according to the police, was super active on social media especially Facebook. Posting the photographs and videos of his work in Indian Air Force and family gatherings was routine for Marwah. But, this super activeness proved fatal six months back when he received two friend requests on Facebook. Suspecting no foul play, he accepted both the friend requests which were created by the ISI. Sources say, the friend requests were in the name of Kiran Randhawa and Mahima Patel.

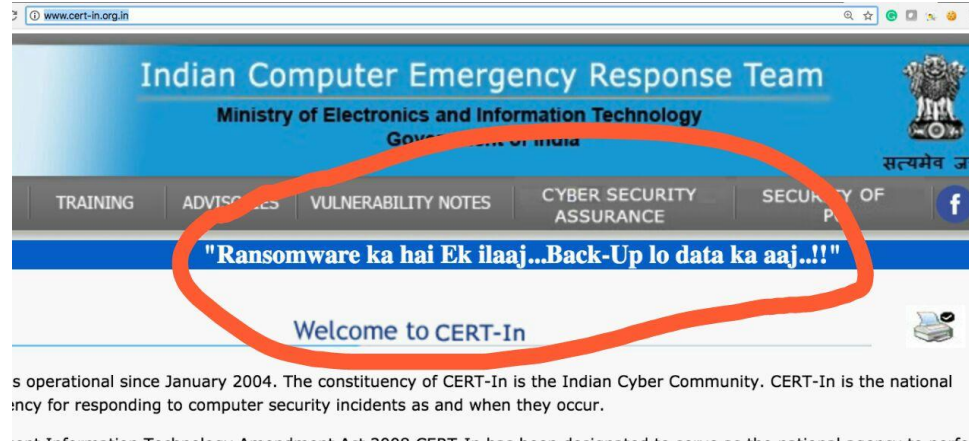


# Ransomware





# Prevention



- Keep anti-virus on your machine always running and updated
- Do regular backups – and make sure those have added protection or are stored offline
- Be wary of unexpected emails especially if they contain links and/or attachments
- Users should be especially careful of any Microsoft Office email attachment that advises enabling macros to view content



# Cryptojacking



## WHAT?

Using someone else's computer resources for crypto-mining!

## WHY

1. Crypto-mining is lucrative
2. Crypto-mining needs huge resources

## HOW

### Malware

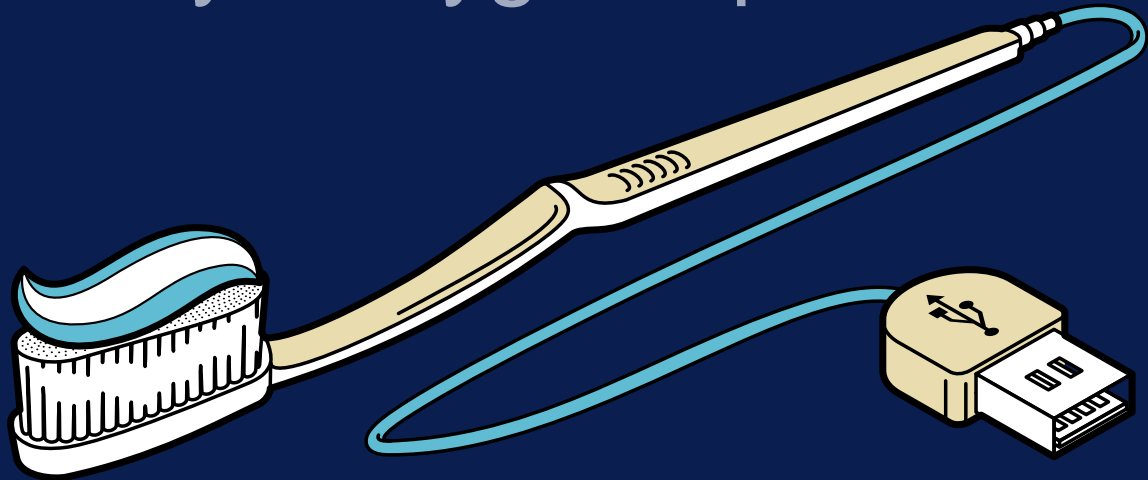
Malware installed on the system

### Website scripts

1. Also called drive-by cryptomining
2. When you visit a website, scripts get loaded
3. Sometimes hidden window are placed to ensure mining even after you close the web page

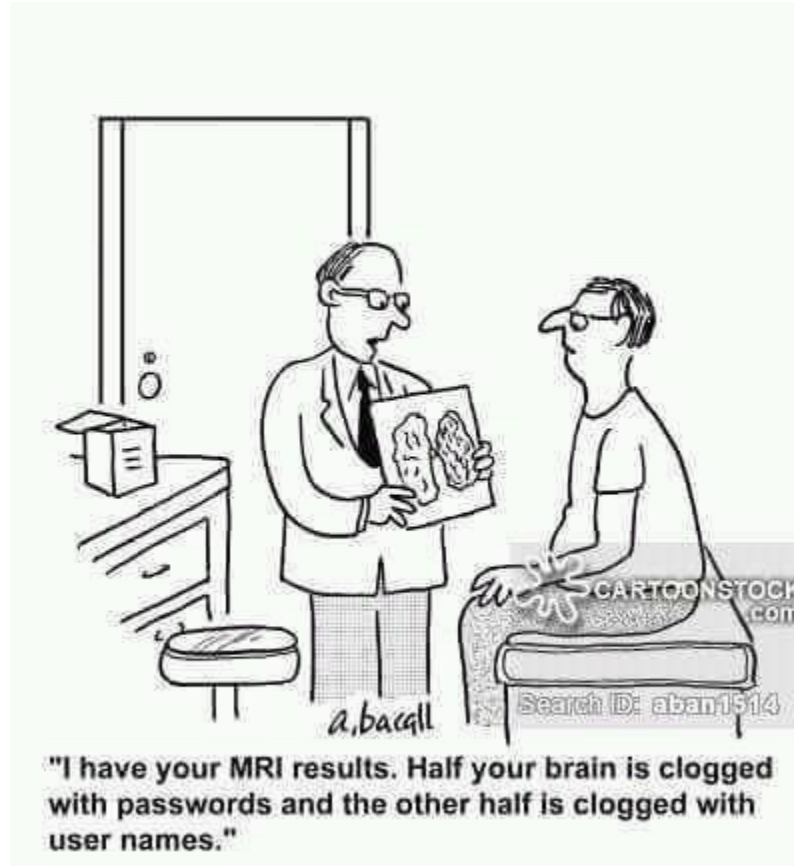


# Cyber hygiene practices





# Secure Passwords







# How hackers gain access to your passwords?

- **Password guessing-**

Don't be predictable. Resist the urge make passwords based on name of family / friends, birthdays, anniversaries, pet name, etc.

- **Shoulder surfing-**

Watch out when entering password in presence of others. Do not be embarrassed to ask to step back.

- **Keyloggers and other malware**

Keep your computer virus-free.

- **Brute Force – Full frontal attack**

Create long, complex, unique passwords.

- **Access to written passwords**

Keep your passwords in your head or encrypted on your computer

- **Phishing – Dangling the tasty bait**

Don't bite the bait. Don't ever click on links in emails or pop-ups that say they need you to log in somewhere, even if they say it's an emergency.

- **Hacking password databases**

Do not reuse passwords



# Password Security



Don't give out your passwords: if someone else knows your password, then it's no longer under your control

- It was Benjamin Franklin who said, "Three may keep a secret, if two of them are dead."

Don't reuse important passwords

Don't write them down

Don't create passwords based on personal information like name, date of birth, Address, etc



Use a reliable password manager

OR

Develop a method for password creation



# Method for password creation



J<sub>o</sub> J<sub>o</sub> L<sub>a</sub>ali N<sub>a</sub>a H<sub>a</sub>aaduve C<sub>h</sub>inna N<sub>i</sub>inna M<sub>u</sub>ddaduve



JJLNHCCNM



\$JLNHC1m

Instagram

\$JLNH1m

HDFC Bank

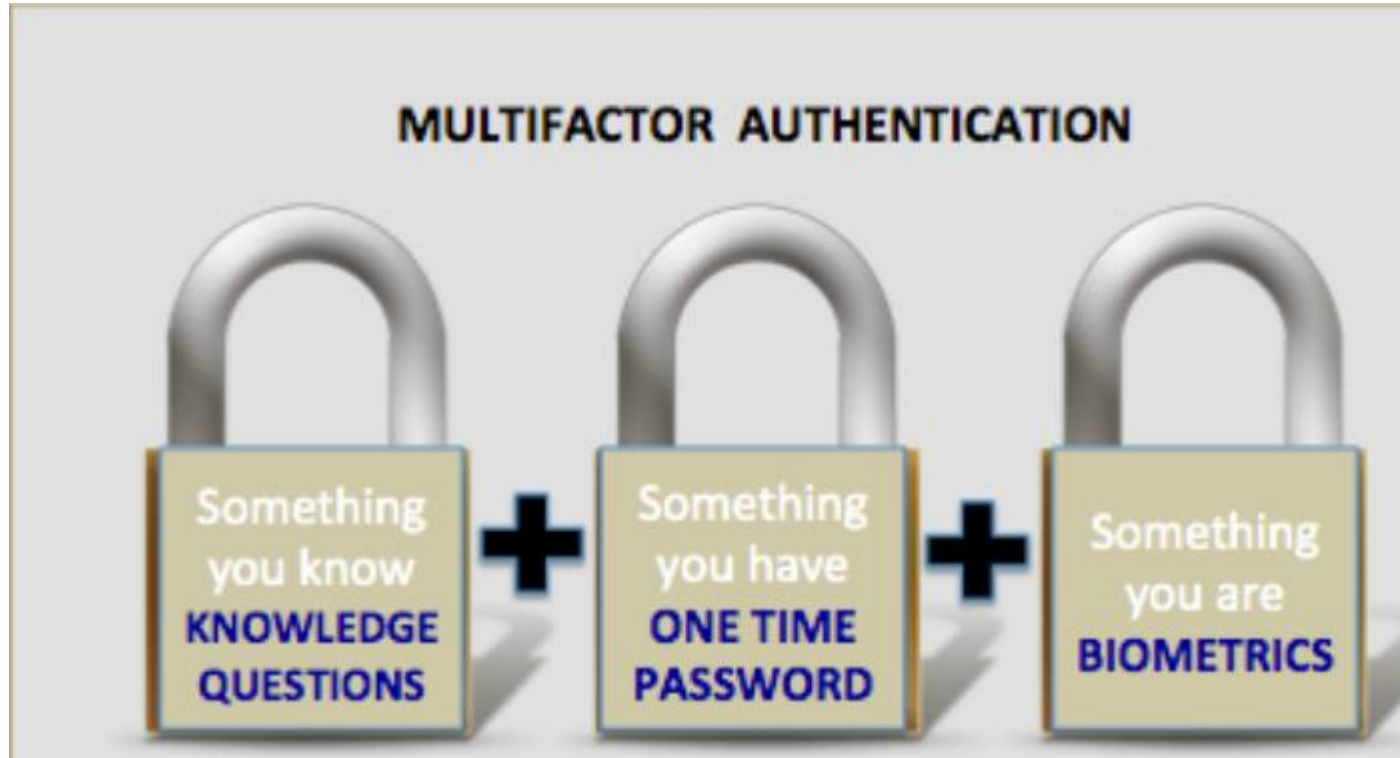
\$JLNHH1m

Paytm

\$JLNHP1m



# Multi Factor Authentication












# How to enable MFA? – Gmail



## Manage your Google Account

-  Home
-  Personal info
-  Data and privacy
-  **Security**
-  People and sharing
-  Payments and subscriptions
-  About

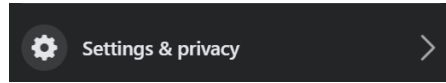
### Signing in to Google



Password	Last changed 19 May 2017	>
2-Step Verification	<input checked="" type="checkbox"/> On	>
App passwords	None	>



# How to enable MFA? - Facebook



General

**Security and Login**

Privacy

Timeline and Tagging

Blocking

Language

Notifications

Mobile

Public Posts

Apps

Ads

Payments

Support Inbox

Videos

## Security and Login



We reorganized a few things. Legacy contacts and account deactivation are now under [General](#).



### Recommended



#### Choose friends to contact if you get locked out

Nominate 3 to 5 friends to help if you get locked out of your account. We recommend this to everyone.

Edit

### Where You're Logged In



**Windows PC · Mumbai,**

Edge · [Active now](#)



**iPad 3rd gen · Mumbai,**

Messenger · 13 hours ago

### Setting Up Extra Security



#### Get alerts about unrecognized logins

We'll let you know if anyone logs in from a device or browser you don't usually use

Edit



#### Use two-factor authentication

Log in with a code from your phone as well as a password

Edit



#### Choose 3 to 5 friends to contact if you get locked out

Your trusted contacts can send a code and URL from Facebook to help you log back in

Edit

### Advanced



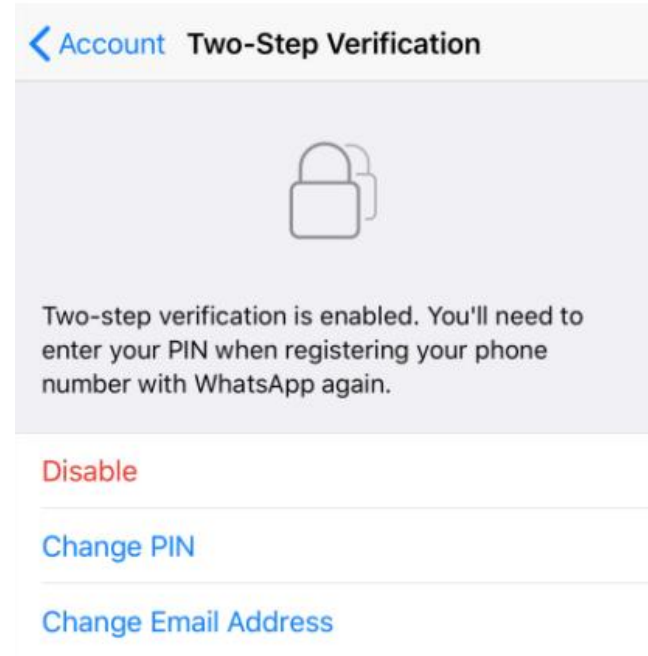
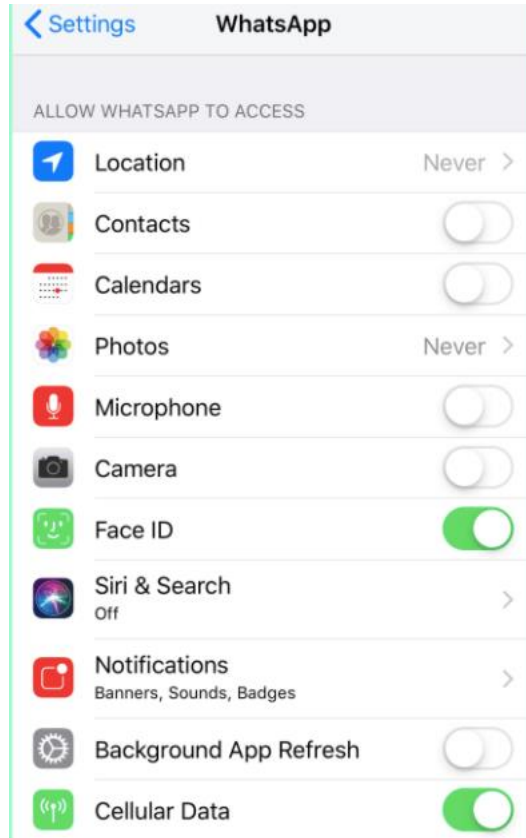
#### Encrypted notification emails

Add extra security to notification emails from Facebook (only you can decrypt these emails)

Edit




# MFA on WhatsApp





# User best practices



- 
- Careful when downloading files from internet
  - Install programs only from trusted sources
  - Avoid usage of unknown USB drives
  - Keep all software updated
  - Lock your system when not in use



# Ensure regular backups

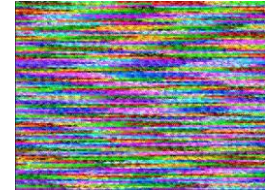


TO OBTAIN  
PROTECTION  
FROM...

- Ransomware



- Data corruption



- Device damage / loss / theft





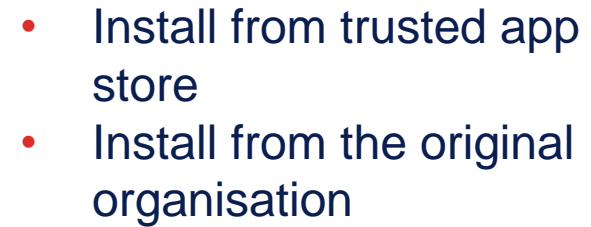
# Mobile security risks



- Inadequate OR poor OS patching
- No PIN or Password protection
- Fake apps / app stores
- Excess permissions given to Apps
- Malicious / shortened URLs
- Poor WiFi / Hotspot passwords
- Jailbroken Or Rooted devices

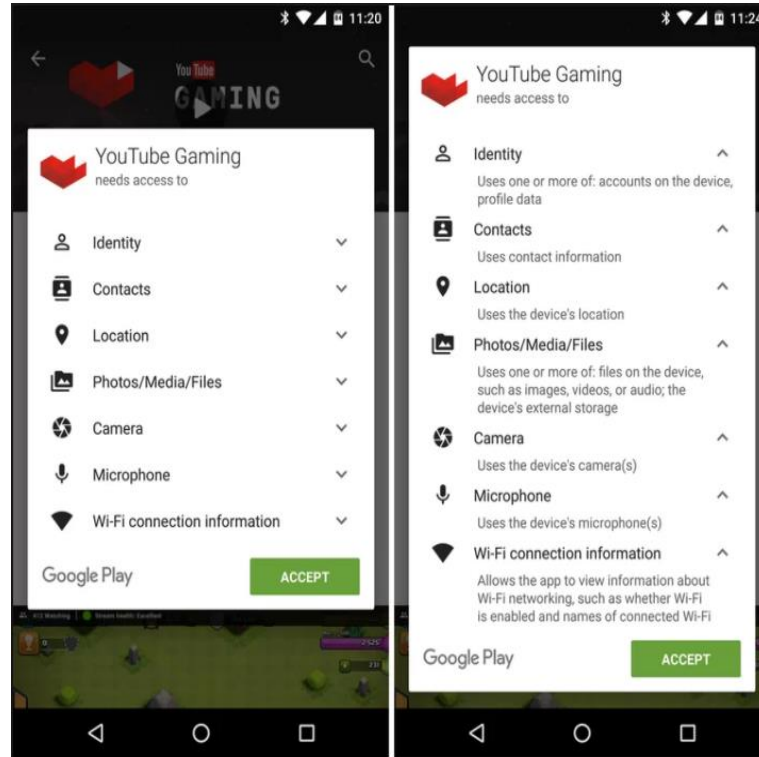








# Careful about already installed apps





# Share minimum data on social media



Careful with PII and social data -

- Date of birth
  - Living address
  - Phone number
  - Email address
  - Vacation plans
- Websites that want you to sign in with your social networking accounts are only mining you for advertising potential
- Reasons Why Linking Sites Is a Bad Idea
  - Decreased security
  - Decreased privacy
  - Decreased professional reputation



# Online Shopping



- Investigate credibility - Be wary of fraud websites; they are promoted using digital marketing and SEO
- Investigate free offers / high discounts
- Websites asking for refundable payments



# Digital Citizenship





# Responsible use of technology



## Digital citizenship is about responsible use of technology

Value  
privacy

Be  
sceptical

Be civil

Keep  
yourself  
updated

Do not fall  
for  
distractions

Avoid  
information  
overload

Report bad  
behaviour



# Responsible use of technology



Value  
privacy

Be  
sceptical

Be civil

Keep  
yourself  
updated

Do not fall  
for  
distractions

Avoid  
information  
overload

Report bad  
behaviour

## Be aware

- Know what is personal data
- Name, address, date of birth
  - Aadhar number, PAN, Passport number, Driving license number, etc
  - Medical or financial data
  - Biometric data

## Be careful

- When sharing personal data
- How securely do they handle it?
  - Will they share with anyone else?

## Be updated

- Follow those who study privacy policies and explain in simple terms
- Take privacy related news seriously

## Be wary

- Automated recommendations
- Keep an open mind
- Follow accounts providing differing views
- Be always in pursuit of truth



# Responsible use of technology



Value  
privacy

Be  
sceptical

Be civil

Keep  
yourself  
updated

Do not fall  
for  
distractions

Avoid  
information  
overload

Report bad  
behaviour

Do not trust easily

Remember that  
anonymity is easy in  
the cyber space

Anybody can  
publish anything.  
Everything  
published need not  
be true.

Verify authenticity  
before sharing  
information.



# Responsible use of technology



Value  
privacy

Be  
sceptical

Be civil

Keep  
yourself  
updated

Do not fall  
for  
distractions

Avoid  
information  
overload

Report bad  
behaviour

Maintain good  
citizenship  
practices in cyber  
world as well

Be civil when  
interacting with  
others

Do not let  
remoteness and  
anonymity bring  
out negativity



Report bad  
behaviour

## Don't just update yourself; update your devices!

50



# Responsible use of technology



Value  
privacy

Be  
sceptical

Be civil

Keep  
yourself  
updated

Do not fall  
for  
distractions

Avoid  
information  
overload

Report bad  
behaviour

Cyber world  
runs on  
clickbaits!

Big tech also  
want you to be  
glued in all the  
time.

Infinite scrolling  
content

Easy to access  
inappropriate  
content



# Responsible use of technology



Value  
privacy

Be  
sceptical

Be civil

Keep  
yourself  
updated

Do not fall  
for  
distractions

Avoid  
information  
overload

Report bad  
behaviour

The world contains far more information than any single person can learn in their lifetime.

The question is not whether you are ignorant, but what you choose to be ignorant about.

Few topics are worth your precious time. Choose what you pay attention to with great care.

**- James Clear**



# Responsible use of technology



Value  
privacy

Be  
sceptical

Be civil

Keep  
yourself  
updated

Do not fall  
for  
distractions

Avoid  
information  
overload

Report bad  
behaviour

The greatest tragedy is not the strident clamor of the bad people, but the appalling silence of the good people.

**- Martin Luther King Jr**



# How to report?



Report on the platform

Report to government agencies

Twitter

Instagram

WhatsApp

Facebook

Pinterest

Discord

Report on  
[cybercrime.gov.in](https://cybercrime.gov.in)

Ministry of Women &  
Child Development  
Email:  
[complaint-mwcd@gov.in](mailto:complaint-mwcd@gov.in)

Karnataka  
Call 112

Profiles

Posts

DMs

Allows even  
anonymous  
reporting

Sexual abuse towards  
women / children

Can file  
Cyber Crime  
Incident  
Report



# Thank you



<https://www.linkedin.com/company/cyseck/>



<https://twitter.com/CySecKCoE>



<https://www.facebook.com/CoECySecK/>



<https://cs-coe.iisc.ac.in/>