

# World Safer Internet Day

WORLD SAFER INTERNET DAY – 11 Feb. 2025



TOGETHER FOR BETTER INTERNET

## WORKSHOP

- **World Safer Internet Day** is celebrated world wide on second Tuesday of February. This year's theme is **Together for a Better Internet**
- **Purpose:**
  - Fraudsters try to commit fraud such as swindling money, stealing personal information, and online bullying etc.
  - These fraudsters are targeting innocent and gullible internet users in new ways..
  - There are various types of frauds taking place. Through awareness on kinds of frauds and the ways to mitigate them would help protect ourselves and our loved ones.

# What is the Internet?



- The Internet is a global network of computers and devices connected to each other to share information and communicate with each other.
- It allows for data exchange, access to websites and communication through various digital means.
- The Internet is not owned by anyone. Everyone participates and uses it..



# Internet in the day to day life



WORLD SAFER INTERNET DAY – 11 Feb. 2025

# Risks of the Internet



**Virus Threats**

**Financial Frauds**

**Theft of Personal Information**

**Mis-Information**

**Hatred & Fake News**

**Trolls, Bullying & Stalking**

**Work – Life Imbalance**

**Health Issues**

**Internet Addiction**

**Lack of Focus**

**Spams**

**Uncontrolled Expenses**

WORLD SAFER INTERNET DAY – 11 Feb. 2025

# Personally Identifiable Information-PII



WORLD SAFER INTERNET DAY - 11 Feb. 2025



Never share any of these critical information with anyone.

# Digital Arrest



“Your parcel has been seized by customs for containing illegal items. You are now being interrogated online and you have been placed under digital arrest. You are not allowed to contact anyone.”

“Your mobile number has been reported to be used for illegal purposes. The Crime Branch police will interrogate you online. You are under digital arrest. You are not allowed to communicate with anyone, including your family..”

- Fraudsters may initiate the conversations like this
- They may connect to a fake police officer through video conference. They may threaten with dire consequences. They may lure you to transfer huge amount to drop the case
- They may try with newer and newer ways to trap the victims.

Never entertain such calls. If in doubt, may contact the respective agencies with the details. May report to the Cyber Crime Police Station

# Scam Calls

WORLD SAFER INTERNET DAY - 11 Feb. 2025

Calling from XYZ Bank. Please share the OTP you have received.





# Scam Calls

WORLD SAFER INTERNET DAY – 11 Feb. 2025



“Your bank account will be closed within the next 15 minutes. Press 1 to speak to a customer service executive”

“Your mobile number's services will be revoked within the next 30 minutes. To avoid disconnection, press 1.”

“You have a criminal case in the High Court. You have not been responding. Press 1 for further details”

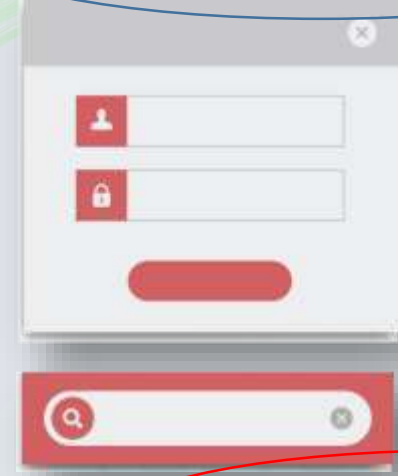
- Fraudsters may call and play this type of recorded messages. In addition, fraudsters may try newer methods.
- Next, they talk to you and force you to give them your important personal information. Using these details, they steal money from your bank account..
- Do not entertain these scam calls. If in doubt, contact the actual organization and get clarification.

# Phishing Attacks



WORLD SAFER INTERNET DAY - 11 Feb. 2025





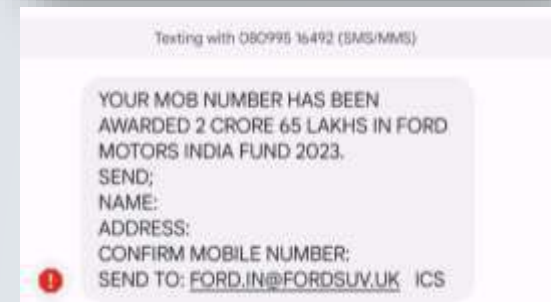
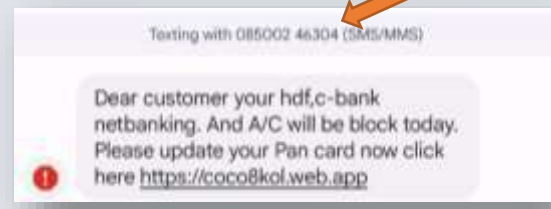
Actual URL: [www.original.com](http://www.original.com)



Phishing URL: [www.Original1.com](http://www.Original1.com)

 Do not click the URL links received through eMails, Messages etc. from unknown person 

 Type the correct URLs in the address bar of the browser 



# Phishing

WORLD SAFER INTERNET DAY – 11 Feb. 2025

Received from a normal mobile number

← CP-KAJGRO ?

**Why this looks like spam**  
Similar messages that you received were identified as spam. Google keeps your personal information private, safe and secure.

Not spam

Unread  
Friday, 3 May • 11:17

Dear Union Bank Customer Your Gift Union Reward Point Rs.6577 Please Collect Now Visit <https://s.id/vyomreword> Reg.KAAJ GROUP

11:17

Can't reply to this short code. [Learn more](#)

← 082908 30194

**Blocked**  
Unblock to receive messages from this sender.

Unblock

Saturday • 19:44

Texting with 082908 30194 (SMS/MMS)

Dear friends, congratulations your resume being hired you will receive a daily income of Rs 31500. contact: <https://wa.me/917060134996>

RCS chat with 082908 30194

← 094928 91464

**Why this looks like spam**  
Similar messages that you received were identified as spam. Google keeps your personal information private, safe and secure.

Not spam

Friday, 26 Jul • 06:03

Texting with 094928 91464 (SMS/MMS)

Unread

**AXIS BANK UPDATE!**

DEAR-USER  
Your REWARD\_Points RS:- 8799 expired\_by Today. Claim cash-voucher On Your A/C now. <https://rb.gy/ukoxmh>  
Axis Bank team

06:03

Text message

← 069090 45732

**Why this looks like spam**  
Similar messages that you received were identified as spam. Google keeps your personal information private, safe and secure.

Not spam

Thursday, 7 Mar • 10:33

Texting with 069090 45732 (SMS/MMS)

Unread

Your Mobile No Have Wins 2,65,00,000.00/- Inr From WhatsApp PrOmO Award"  
Send Full Name  
Mobile NO  
Age  
Addss  
Occup  
Reply To ( [wwaccessibility@gmail.com](mailto:wwaccessibility@gmail.com) )

10:33

Text message

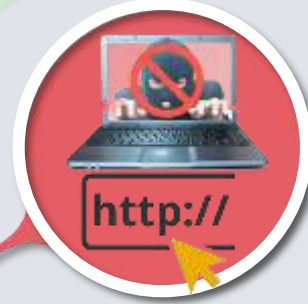
# Safer Internet

Security in the digital world is just as important as in the real world.



WORLD SAFER INTERNET DAY – 11 Feb. 2025

Never befriend strangers or share personal details on social media.



Never trust or click on links from unknown sources in messages/emails. Type URLs yourself.

Never use untrusted public computers and networks for critical transactions.



Do not share passwords, OTP and personal information with anyone.



Never trust attachments and applications from unknown sources.

# Passwords & OTPs

Do not share your password and OTP with anyone.

Wherever facility is available, enable Multi Factor Authentication



Keep strong passwords and change them regularly.

Make sure to keep passwords for computers and mobile phones.

Do not use the same password for different purposes.

Don't use passwords that are easy to guess.

# Safer social media presence



WORLD SAFER INTERNET DAY - 11 Feb. 2025



Be careful about your presence on social media.



Do not share personal and unnecessary information.



Check the authenticity of the content. There will be a lot of fake and unreliable information.



Don't fall prey to hate messages and don't spread it.



Remember that once something is posted online, it can be difficult to completely remove it.



Don't click on unknown links, don't download unknown apps.



Do not accept friend requests from unknown people, verify the authenticity of the requester.



Lock your profile from unknown people



# Social Media : Fake Profiles

WORLD SAFER INTERNET DAY - 11 Feb. 2025



Fake social media accounts can be created using the profile photo and other details of some individuals and impersonate that person to commit fraud.

11h ...  
It has come to my notice that some fraudsters have created a fake account using my name on social media and demanding money. This is totally false and intended to deceive people. Please don't fall prey to such fraudsters.

ಕೆಲವು ಕಿಡಿಗೇಡಿಗಳು ಸಾಮಾಜಿಕ ಜಾಲತಾಣದಲ್ಲಿ ನನ್ನ ಹೆಸರು ದುರ್ಬಳಕೆ ಮಾಡಿಕೊಂಡು ನಕಲಿ ಖಾತೆ ಸೃಷ್ಟಿಸಿ ನಾನು ಹಣದ ಸಹಾಯ ಕೇಳುತ್ತಿದ್ದೇನೆಂದು ಸುಳ್ಳು ವದಂತಿ ಹಬ್ಬಿಸಿದ್ದಾರೆ. ಇದು ಸಂಪೂರ್ಣವಾಗಿ ಸುಳ್ಳು. ಯಾರೊಬ್ಬರೂ ಇಂತಹ ವಂಚನೆಗೆ ಒಳಗಾಗಬೇಡಿ. ಈ ಕುರಿತು ಸೈಬರ್ ಕ್ರೈಮ್ ಗೆ ದೂರು ನೀಡುವ ಬಗ್ಗೆ ಚಿಂತನೆ ನಡೆಸಿದ್ದೇನೆ.

Protect your profile details from unknown people

Don't befriend strangers. Check before accepting requests.

# Unsafe Links, Applications and Files

Never trust or click on links from unknown sources in messages/emails. Type URLs yourself.

WORLD SAFER INTERNET DAY - 11 Feb. 2025



Fraudsters can take control of your device and steal personal data.



Can track all your activities on the device and commit other frauds.



Data can be deleted or data can be encrypted and ransom can be demanded to decrypt the data.




Your data can be sold to competitors




# Maintaining Digital Hygiene




WORLD SAFER INTERNET DAY – 11 Feb. 2025




Use only licensed and trusted software




Never give access through remote desktop




Have one good Antivirus Software



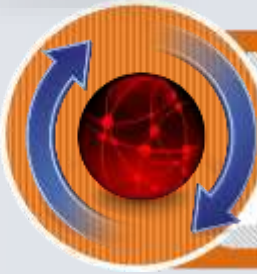
Never use out-dated Software and Hardware




Buy or Download Software only from the trusted sources



When not in use, lock the screens and set password to unlock



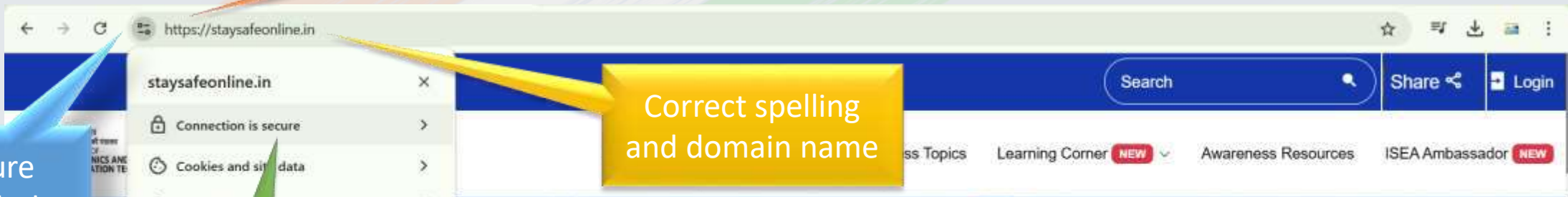
Keep all the Software & Antiviruses up-to-date



Do not use Super user / Admin user account for regular use

# Safe Browsing

Presence of "https"



Secure Symbol

Correct spelling and domain name

"Connection is Secure"



WORLD SAFER INTERNET DAY - 11 Feb. 2025

# Safe Messaging with WhatsApp



WORLD SAFER INTERNET DAY – 11 Feb. 2025



## WhatsApp

- 01 Set your profile photo and status to only be visible to people in your contacts.
- 02 Set a password to open the WhatsApp app.
- 03 Enable two-step verification
- 04 Report and block dangerous messages. Do not respond to unknown video calls.
- 05 Do not install applications received from strangers, do not click on links received.



ಸ್ವಾಮಿನ್ಯ ಶಾಸನ ಕರ್ನಾಟಕ ಸರ್ಕಾರ

# Officer's Responsibility



- Do not share your User ID, Password, and OTP with anyone.
- Never share your Digital Signature Token and password..
- Your account may have higher privileges due to Role Based Access. So do not share your account details with others.
- Do not register apps installed on other people's devices with your details.
- If you are authorized to share data, the data should only be shared with password-protected files. The password should be shared separately.
- Make sure that the personally identifiable information of others is not shared in any way in the public domain.

WORLD SAFER INTERNET DAY – 11 Feb. 2025

# In-case of fraud

- Citizens can register their complaints through the helpline number 1930.
- Complainants can call the helpline number 1930 and provide some mandatory details like name, mobile number, address, transaction details etc.
- After receiving the acknowledgement number in the SMS, the complainant will have to file a formal complaint on the portal (<https://cybercrime.gov.in/>) within 24 hours





Report a  
Cybercrime on  
**1930**

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



If it is financial fraud, contact the bank immediately and report the details.

If you lose your mobile, contact the service provider immediately, block the number and get another SIM with the same number.



Contact the nearest cybercrime police station immediately.

# For additional information and awareness



## Indian Cybercrime Coordination Centre (I4C)

- To create a safer cyber space for the citizens of India.
- To create an effective framework and ecosystem for the prevention, detection, investigation, and prosecution of Cybercrime in the country

<https://i4c.mha.gov.in/>



## Stay Safe Online

- Promoting Cyber awareness through cyber fitness app, social media and workshops / Webinars
- Interactive programs to engage users - Cyber Quizzes/ competitions/ Games
- Cyber Schooling through role-based learning

<https://www.staysafeonline.in/>



WORLD SAFER INTERNET DAY – 11 Feb. 2025



# Thank you