

INVESTMENT ADVISER

# CYBER SECURITY AWARENESS CAMPAIGN

For contemporary awareness by Investment Adviser  
(In pursuance of SEBI / BASL compliances initiative)

2022 - 23



© Infosec Partner  
**SANJAY KADEL** & CO.  
chartered accountants



EXCLUSIVELY FOR MEMBERS

# ARIA Partners

Platinum  
Partners..



Gold  
Partners..



Silver  
Partners..



Investment Advisers | Cyber Security Awareness Campaign (2022-23)

Exclusively for members of ARIA by Sanjay Kadel & Co. Infosec Partner



# Introduction & Agenda

*"Our intention creates our reality." – Wayne Dyer*



## 1. Intent [↗](#)

Establish the knowledge, importance and need for Cyber Security, and commitment towards it.

*Build awareness of cyber security*



## 2. Practices [↗](#)

Secured Practices / Process related

**For contemporary awareness by Investment Adviser**  
(In pursuance of SEBI / BASL compliances initiative)

2022 - 23



© Infosec Partner  
**SANJAY KADEL** & CO.  
chartered accountants



EXCLUSIVELY FOR MEMBERS



# Part 1. Intent

Establish the knowledge, importance and need for Cyber Security, and commitment towards it.

[Go to Index page](#) 



Investment Advisers | Cyber Security Awareness Campaign (2022-23)

Exclusively for members of ARIA by Sanjay Kadel & Co. Infosec Partner



# It's a digital world

[Part 1. Intent]

- Extensive reliance on computer systems and network to process / manage '**Information**'
- Inevitable spread of digital transformation, that has exposed our sensitive data to potential jeopardy.



Investment Advisers | Cyber Security Awareness Campaign (2022-23)

Exclusively for members of ARIA by Sanjay Kadel & Co. Infosec Partner



# Information!

[Part 1. Intent]

- **'Information'** is the most valuable asset
- It affects the behavior, decision, an outcome, and the destiny of the Organisation
- To be valuable, Information has to be ...
  - meaningful
  - relevant
  - accurate
  - timely
  - specific
  - organized
  - for a purpose
  - enhance understanding
  - reduce uncertainty



Investment Advisers | Cyber Security Awareness Campaign (2022-23)

Exclusively for members of ARIA by Sanjay Kadel & Co. Infosec Partner





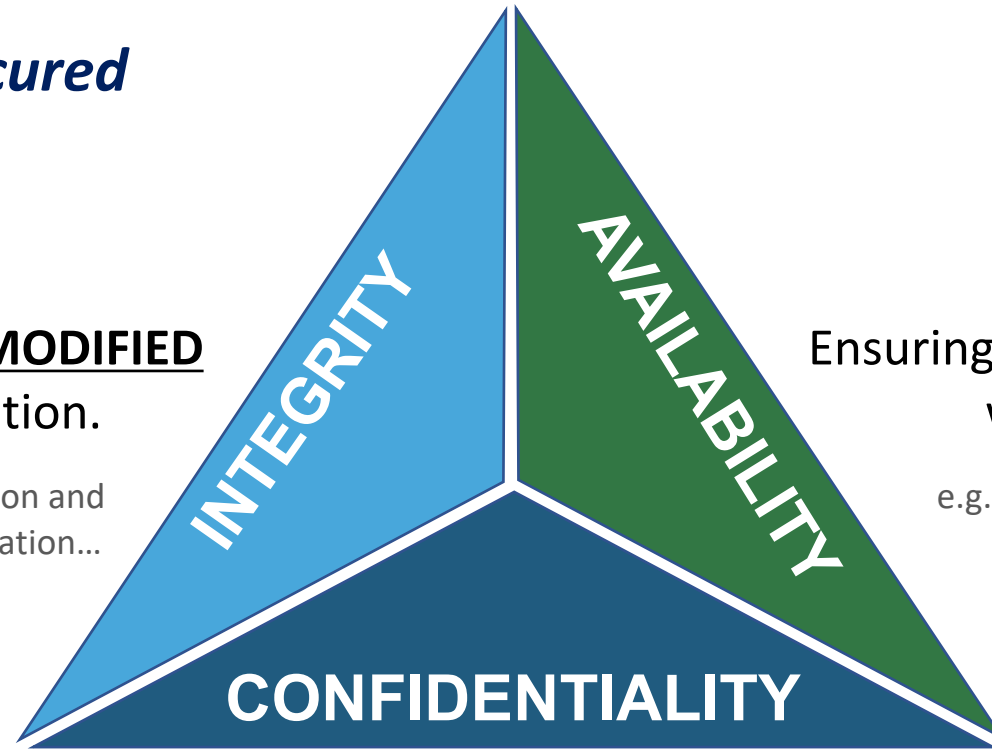
# Information Security – CIA

[Part 1. Intent]

*Information need to be secured by ensuring CIA*

Ensuring data is **NOT MODIFIED** without authorization.

e.g. Modifying critical field values, virus infection and manipulation of numbers, website mis-information...



Ensuring Information is **AVAILABLE** when it is needed.

e.g. Power outages, DOS attacks...

Ensuring Information is not **DISCLOSED** to unauthorized individuals / systems.

e.g. Credit Card info theft, Password breach, Accidental access to sensitive data



Investment Advisers | Cyber Security Awareness Campaign (2022-23)

Exclusively for members of ARIA by Sanjay Kadel & Co. Infosec Partner



# Impact of security violations

[Part 1. Intent]

Such '**Information**' if not secured, would lead to serious consequences!

- Financial... Non-Financial...
- Physical... Logical...
- Legal... Ethical/Moral...
- Short-Term... Long-Term...
- Serious... Non-Serious...
- To Organization / Employees / all...
- Loss of Business
- Loss of operational continuity
- Loss of business information
- Loss of Customers
- Loss of Trusts of Employees, Customers, Public, Stakeholders
- Embarrassment
- Bad publicity
- Internal disciplinary action;
- Termination
- Penalties / Prosecution
- ... ..



Investment Advisers | Cyber Security Awareness Campaign (2022-23)

Exclusively for members of ARIA by Sanjay Kadel & Co. Infosec Partner

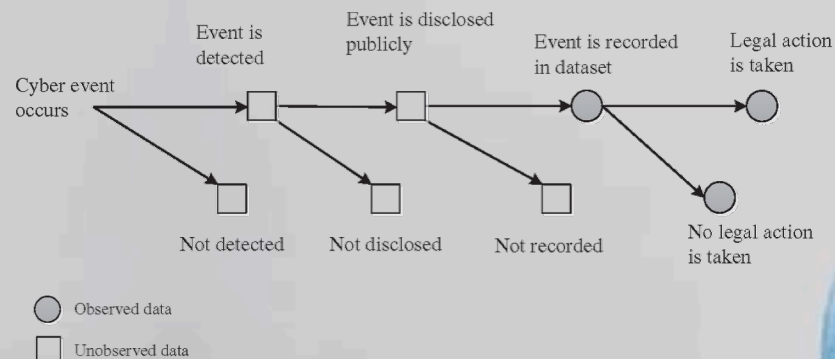


# Extent of Impact

[Part 1. Intent]

- In the year 2021, Indian Computer Emergency Response Team (CERT-In) handled 14,02,809 incidents. **Almost 4,000 incidents every day!**
- According to IBM Security, the average total cost of a data breach in India was INR 14 crores in 2020. **Almost INR 4,00,000 every day!**

**Note: This number is far-lesser than actual occurrence.**



Investment Advisers | Cyber Security Awareness Campaign (2022-23)

Exclusively for members of ARIA by Sanjay Kadel & Co. Infosec Partner



# Cyber security Incidents

[Part 1. Intent]

| Mumbai, was hit by a massive power outage prompting the cancellation of train services which brought the whole city to its knees.

| Indian SMEs lost yearly INR 7 Cr in cyber attacks

| Hackers stole the personal data of 4.5 Mn Air India passengers

| Personal and financial information of nearly 180 Mn PNB customers was left exposed for 7 months.

Oct. 2020

Feb. 2021

Sep. 2021

Nov. 2021



Investment Advisers | Cyber Security Awareness Campaign (2022-23)

Exclusively for members of ARIA by Sanjay Kadel & Co. Infosec Partner



★★★★★

# Cyber security Incidents

[Part 1. Intent]

- July 2022 | SEBI faced Cyber **security incident** involving its email system.

As per SEBI, no sensitive data was lost. Further, FIR is lodged and CERT-In is looped in.

- July 2022 | Hacker groups from Malaysia and Indonesia initiated a **cyber war** against India, following Nupur Sharma's recent controversial comments.

The hacker groups targeted more than 2,000 websites and leaked the database of Andhra Pradesh police as well as PAN card and Aadhaar details of many Indians.

***and it continues...***



Investment Advisers | Cyber Security Awareness Campaign (2022-23)

Exclusively for members of ARIA by Sanjay Kadel & Co. Infosec Partner



# The need

[Part 1. Intent]

Hence, considering the importance of information as an asset, its security, and the potential / extent of impact, if it is not secured,

*logical & obvious*  
*there is a <sup>^</sup>need to establish **awareness** of Cyber security and related practices with all stakeholders!*

---

**You! are RESPONSIBLE for your action and inaction.**

You may affect others! and may be affected by others!



Investment Advisers | Cyber Security Awareness Campaign (2022-23)

Exclusively for members of ARIA by Sanjay Kadel & Co. Infosec Partner



★★★★★

## The commitment

[Part 1. Intent]

### Cyber Security Pledge to build safe digital environment

*Let's commit ourselves, to be cyber aware and alert in safeguarding self, organisation and others, against all possible cyber attacks, by implementing secured infrastructure and following secured practices.*



Investment Advisers | Cyber Security Awareness Campaign (2022-23)

Exclusively for members of ARIA by Sanjay Kadel & Co. Infosec Partner





## Part 2. Practices

Awareness → Secured Practices / Process related

[Go to Index page](#) ↗



Investment Advisers | Cyber Security Awareness Campaign (2022-23)

Exclusively for members of ARIA by Sanjay Kadel & Co. Infosec Partner



# Secured Practices / Process

[Part 2. Practices]

## *Information Security is an IT Problem?*

- 10% of security safeguards are Technical.
- Whereas 90% rely on users (You) to adhere to secured practices / best practices / process.



The lock on the door..... is 10%

Remembering to lock – checking to see if it is closed –  
Ensuring others do not prop the door open – Keeping control  
of keys..... is the 90%



Investment Advisers | Cyber Security Awareness Campaign (2022-23)

Exclusively for members of ARIA by Sanjay Kadel & Co. Infosec Partner



# Secured Practices / Process

[Part 2. Practices]

**Adopting best practices and technologies can help you and your organization implement strong cybersecurity that reduces vulnerability to cyber attacks and protects critical information systems.**



***Certain areas of Secured Practices / Process are as follows:***

1. Password practices
2. Workstation security
3. Laptop security
4. Mobiles security
5. Mobile App practices
6. Email practices
7. Internet use practices
8. Antivirus use practices
9. Backup practices
10. Security Incidents reporting practices
11. Social media practices
12. Financial Transactions practices
13. Social Engineering safeguard practices



Investment Advisers | Cyber Security Awareness Campaign (2022-23)

Exclusively for members of ARIA by Sanjay Kadel & Co. Infosec Partner





★★★★★

# 1. Password practices

[Part 2. Practices]

## *Framing Passwords*

- Don't use a word that can be found in a dictionary
- Use min. atleast 8 characters length
- Passwords should include alphabets + numerics + special chars
- Don't frame same passwords for all applications
- Don't make it easily guessable based on your public infos
- Don't make it guessable based on your user id
- Don't repeat the passwords on change
- When framing Passwords, also ensure that the Hints, the Secret questions and answers meet the strength and complexities
- Don't use sequences of keys in keyboards or order of alphabets



Investment Advisers | Cyber Security Awareness Campaign (2022-23)

Exclusively for members of ARIA by Sanjay Kadel & Co. Infosec Partner



# 1. Password practices (contd.)

[Part 2. Practices]

## *Using Passwords*

- Don't visibly type in front of others
- Use virtual keyboard, if available
- Don't let browsers or softwares or websites remember the password
- Don't use on un-official or friend's or public computers
- Don't share with others and change immediately, if shared
- Don't use passwords on suspicious websites



Investment Advisers | Cyber Security Awareness Campaign (2022-23)

Exclusively for members of ARIA by Sanjay Kadel & Co. Infosec Partner



# 1. Password practices (contd.)

[Part 2. Practices]

## ***Maintaining Passwords***

- Don't store / note passwords in clear text.
- Don't write down as to be easily accessible or visible to others
- Don't make post-it notes of your passwords
- Change them immediately upon first receipt
- Change the default passwords immediately in new h/w or s/w
- Change them frequently – 45 days
- Change them immediately upon suspicion
- Ensure strength of the password of passwords
- Don't share the secret questions or answers with anyone
- Don't store passwords in (mostly untrusted) mobile apps or s/ws



Investment Advisers | Cyber Security Awareness Campaign (2022-23)

Exclusively for members of ARIA by Sanjay Kadel & Co. Infosec Partner

## 2. Workstation security

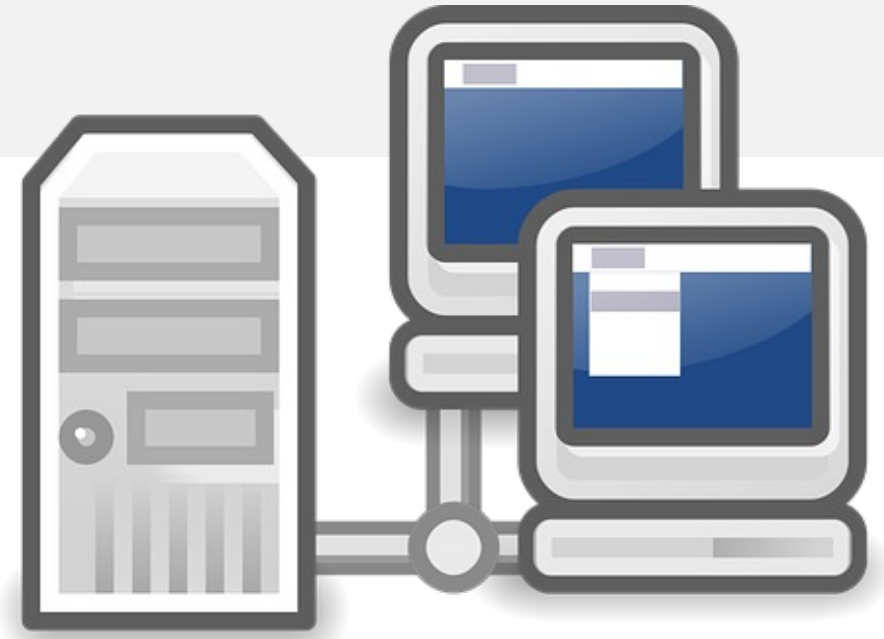
[Part 2. Practices]

### ***Controls for the period when it's attended by You***

- Sharing – Share folders /files only if necessary
- Sharing – Cancel sharing once requirement is met
- Sharing – Provide only required permissions (read / write)
- Ensure non-visibility by people around

### ***Controls for the period when it's un-attended***

- Log-off before leaving the device
- Set a 5-minute screen-saver with password protection
- Have a boot password / power-on password
- Have a operating system logon password
- Encrypt & Password Protect it



Investment Advisers | Cyber Security Awareness Campaign (2022-23)

Exclusively for members of ARIA by Sanjay Kadel & Co. Infosec Partner

## 3. Laptop security

[Part 2. Practices]

*In addition to Workstation controls...*

### *Controls for the period when it's attended by You*

- Have a personal firewall for the Laptops
- Ensure proper ergonomics and house-keeping around else it might be dropped / damaged
- Ensure non-visibility by people around

### *Controls for the period when it's un-attended*

- Never leave it un-attended at places other than home/office
- Physically secure it to the desk / grill-window with a lock-down cable
- Have the name and address of the user labelled, to facilitate its return in the event of a loss



## 4. Mobiles security

[Part 2. Practices]

### *Controls for the period when it's attended by You*

- Ensure non-visibility by people around
- Ensure proper ergonomics and house-keeping around else it might be dropped / damaged
- Turn off wireless interfaces when not necessary
- Install anti-virus software
- Do not share phone-device with kids, naive users and others
- Lock keypad / touch when not required to avoid accidental calls or deletion of data



Investment Advisers | Cyber Security Awareness Campaign (2022-23)

Exclusively for members of ARIA by Sanjay Kadel & Co. Infosec Partner

## 4. Mobiles security (contd.)

[Part 2. Practices]

### *Controls for the period when it's un-attended*

- Never leave it un-attended at any place
- Have the name and address of the user labelled, to facilitate its return in the event of a loss
- Enable mobile tracking facility, Remote-wipe facility
- Lock Keypad / touch before leaving the device
- Set auto lock every 2-minutes with password protection
- Have a power-on password
- Encrypt & Password Protect it



Investment Advisers | Cyber Security Awareness Campaign (2022-23)

Exclusively for members of ARIA by Sanjay Kadel & Co. Infosec Partner

## 5. Mobile App Practices

[Part 2. Practices]

**First and Last Rule: Install only needed apps! ABSOLUTELY NEEDED APPS!  
Which app to use! Which to not! Decide that first.**

- Install only trusted apps!
- Don't give access to apps to access for everything. Be selective. Be careful.
- Secure access to – Microphone / Camera / Phone book.
- Secure access to – Photos / Message logs / Root.
- Apply MFA
- Don't allow to store card info.
- Keep apps updated.
- Change app login credentials at least 45 days once.

***Many more.. stay vigilant.***



Investment Advisers | Cyber Security Awareness Campaign (2022-23)

Exclusively for members of ARIA by Sanjay Kadel & Co. Infosec Partner



## 6. Email practices

[Part 2. Practices]



### ***Controls related to Receiving***

- Do not open or reply to spam messages.
- Do not open or reply to suspicious e-mails.
- Do not open un-solicited emails from strangers whatever subject line may read.
- Do not open attachments with macros or executable files unless it is from very very very trusted source
- Do not read or waste time on un-official messages during official time (vice versa is encouraged though!)
- Do check personally or through other modes of communication, in cases where an email requires critical action
- Beware of Phishing Emails, Spoofed emails



Investment Advisers | Cyber Security Awareness Campaign (2022-23)

Exclusively for members of ARIA by Sanjay Kadel & Co. Infosec Partner



## 6. Email practices (contd.)

[Part 2. Practices]



### ***Controls related to Sending***

- Use the mailing system for official purposes only
- Send file attachments only if absolutely necessary
- Do not reply / forward spam messages.
- Do not forward chain letters. It's the same as spamming!
- Do not send confidential / critical business information without encryption & password
- Double-check the Email Address of Recipients before sending
- Check whether you have attached the proper files and not those belonging to others or those infected with virus
- Do not send 'very-large' attachments. Use hyperlinks instead.
- Use Official Disclaimers with Email-signatures



Investment Advisers | Cyber Security Awareness Campaign (2022-23)

Exclusively for members of ARIA by Sanjay Kadel & Co. Infosec Partner

## 6. Email practices (contd.)

[Part 2. Practices]



### ***Controls related to Maintenance / Usage***

- Periodically backup your email folder
- Password Protect the Email-Client and Email-Client-Folder
- Do not treat Emails as a data storage but only as communication tool. Take out necessary attachments and store in usual file-structure of organization.
- When using web-mail on un-official devices, be sure to log off after use
- Use Emails on Mobiles and other Mobile devices only upon authorisation from the organization



Investment Advisers | Cyber Security Awareness Campaign (2022-23)

Exclusively for members of ARIA by Sanjay Kadel & Co. Infosec Partner

# 7. Internet use practices

[Part 2. Practices]

- Visit only trusted websites
- While surfing beware of bad-waters!
- Use internet for official purpose only during official time
- Pay attention to warnings from your browser – read in your interest!
- Employees may be monitored for any internet activities
- Not everything on Internet is authenticated information and hence, double-check before using such information
- There's no free lunch in the world and hence, beware of free softwares, songs, videos, images and other information.
- Use Internet security and firewalls and do not open infected webpages
- Beware of real-looking fake web pages



## 8. Antivirus use practices

[Part 2. Practices]

- Use only approved Anti-virus software
- Do not turn off or disable scheduled & real-time virus-scan
- Run full scan of your system once in 7 days
- Run anti-virus updates if not automatically set and running
- User possession or development of viruses or other malicious software is prohibited and punishable as per IT Laws.
- Inform / Report the Virus or Infection warnings
- Do not use USB drives, external media without scanning



Investment Advisers | Cyber Security Awareness Campaign (2022-23)

Exclusively for members of ARIA by Sanjay Kadel & Co. Infosec Partner



# 9. Backup practices

[Part 2. Practices]

- Desktop backup is the responsibility of the end-user
- End user to identify critical data that needs to be backed & frequency
- Include email files in your list of critical files for backup
- Ensure before Backup that the data is virus-free
- Ensure encryption / password for backup media
- Ensure safe custody of backup media
- Ensure off-site backup as per ISMS at your organization
- Test Backup restoration at regular intervals
- Ensure Backup logs are maintained in system or manually
- Ensure approved methodology for backup and authority for backup
- While Disposal – ensure shredding, destruction, erasure



Investment Advisers | Cyber Security Awareness Campaign (2022-23)

Exclusively for members of ARIA by Sanjay Kadel & Co. Infosec Partner

# 10. Security Incidents reporting practices

[Part 2. Practices]

- Report security incidents & breaches to HoD or IS Manager
- Report & respond to security incidents & security breaches

***An incident may relate to –***

- Suspected hacking attempts,
- Loss of information,
- Hardware resources and components,
- Virus incidents, Failure / crash of IT equipment,
- Power problems and
- Loss of data,
- Natural calamity or disaster,
- Software and Operational failure / errors



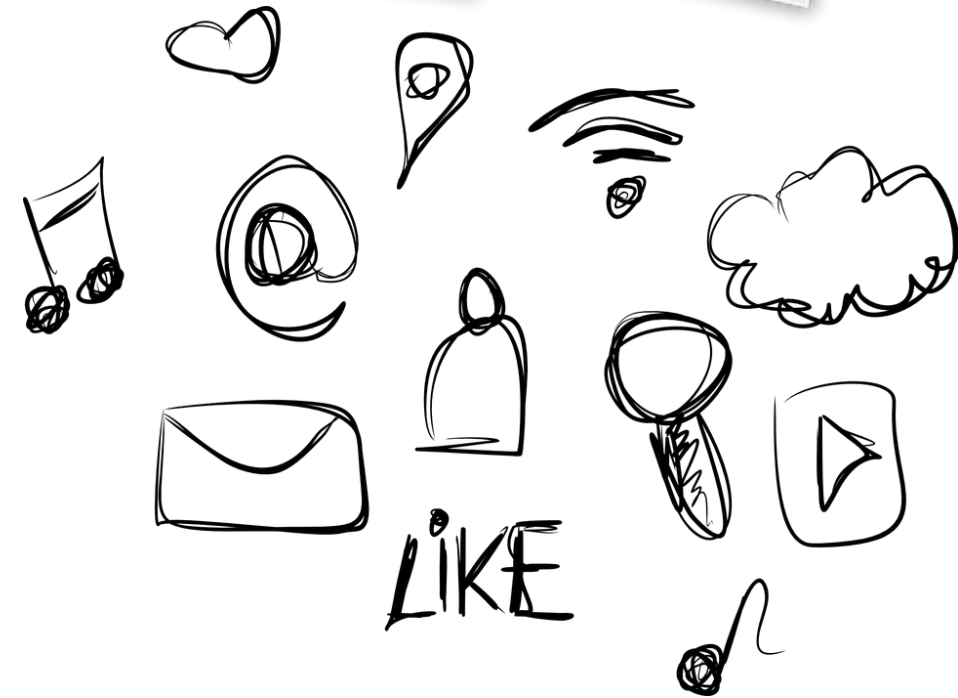
Investment Advisers | Cyber Security Awareness Campaign (2022-23)

Exclusively for members of ARIA by Sanjay Kadel & Co. Infosec Partner

# 11. Social media practices

[Part 2. Practices]

- Don't reveal too much – photos, personal updates, etc. Be careful!
- Avoid "FOMO"
- Configure privacy settings properly
- Don't go friend-shopping. Not 'entire world' is your friend. Add friends who are really known to you..
- Don't interact too much. Block all – Allow some!
- Opt-out of targeted advertisements. Beware of **adware-malware!**
- Don't scatter social media accounts on all devices unnecessarily
- **Build a positive online reputation..**
- Think before you 'post'





# 12. Financial Transactions practices

[Part 2. Practices]

- Don't fall to urgent / phishing communication – call, sms, email, etc.
- Don't enable "remember password"
- Don't search for the financial platforms or services like banks, etc. through google. It will be phished!
- Don't store card information – while online purchases, etc.
- Don't enter password before your nearby people.
- Ensure https is enabled.
- Beware of keyloggers. Use virtual keyboard wherever available.
- Now-a-days 'Secure message' is very helpful. Enable that in the bank site.
- Don't keep common password for all financial transaction platform.
- Enable MFA.
- Configure daily transaction limits, wherever possible.
- Wherever using card details – ensure they are PCI-DSS certified.



Investment Advisers | Cyber Security Awareness Campaign (2022-23)

Exclusively for members of ARIA by Sanjay Kadel & Co. Infosec Partner

# 13. Social Engineering safeguard practices

[Part 2. Practices]

**“The Clever Manipulation of the natural human tendency to trust.”**

- Social engineering is the practice of obtaining confidential information by manipulation of legitimate users.
- A social engineer will usually use the telephone / email / Internet / Social Networking Messaging / sometimes personal interaction....

to trick people into revealing sensitive information, or getting them to do something that is against typical secured practices.



Investment Advisers | Cyber Security Awareness Campaign (2022-23)

Exclusively for members of ARIA by Sanjay Kadel & Co. Infosec Partner

# 13. Social Engineering safeguard practices (contd.)

[Part 2. Practices]

## ***Signs of social engineering attacks to recognize:***

- Shoulder Surfing, Dumpster Diving, New house-keeping
- Sudden Trustworthiness, Charm, Attraction and Closeness
- Refusal to give contact information
- Rushing by the Social engineer
- Requesting forbidden information
- Name-dropping
- Intimidation / coercion / threatening
- Very high dreams and higher promises
- Asking for immediate action and rushing towards it
- Small mistakes (misspellings, misnomers, odd questions)



Investment Advisers | Cyber Security Awareness Campaign (2022-23)

Exclusively for members of ARIA by Sanjay Kadel & Co. Infosec Partner

# Caveat

[Part 2. Practices]

***The design of controls and extent of cyber security best practices, to be adopted for the organisation / user, should be based on business requirements (nature and size), risk assessment and feasibility (technical, financial and operational), and compliance requirements! arising from policies, contractual obligations, legal & regulatory mandates.***

**For contemporary awareness by Investment Adviser**  
(In pursuance of SEBI / BASL compliances initiative)



2022 - 23

© Infosec Partner  
**SANJAY KADEL** & CO.  
chartered accountants



EXCLUSIVELY FOR MEMBERS

# Disclaimer

## Terms of use of this presentation

- Information contained in the **cyber security awareness campaign**, and related notes / documents / guidelines / interpretations / publication provided in connection to such awareness campaign, for RIA's compliance to cyber security awareness campaign, are intended for use, primarily by the relevant members of ARIA only, to the extent suitable to their situation / case. If you are not the intended audience of these publication or artefacts, an agent of the intended audience or a person responsible for delivering the information to the named entities, you are notified that any use, distribution, transmission, printing, copying or dissemination of this information in any way or in any manner is strictly prohibited.
- Every effort has been made to avoid errors or omissions in these publications and artefacts. In spite of this, errors may creep in. Any mistake, error or discrepancy noted may be brought to our notice at [membership@aria.org.in](mailto:membership@aria.org.in) (more contact details at <https://aria.org.in>) which shall be taken care of in the next update and release.
- Though, we may provide, to the best extent possible, a reasonably proper publication or artefact, there may be, alternative approaches / interpretations / improvisation possible.
- It is notified that neither ARIA nor the authors, including, members of Sanjay Kadel & Co. Chartered Accountants, or anyone connected herewith will be responsible for any damage or loss of action to any one, of any kind, in any manner, therefrom. It is suggested that to avoid any doubt the reader, receiver, or user of the information contained in these publications or artefacts, should cross-check all the facts, law and contents of the publication with original source, publication or notifications.



INVESTMENT ADVISER

# CYBER SECURITY AWARENESS CAMPAIGN



*Wishing you <secured> digital star! in work and life.*

For contemporary awareness by Investment Adviser  
(In pursuance of SEBI / BASL compliances initiative)



2022 - 23

© Infosec Partner  
**SANJAY KADEL** & CO.  
chartered accountants



EXCLUSIVELY FOR MEMBERS

# ARIA Partners

Platinum  
Partners..



Gold  
Partners..



Silver  
Partners..



Investment Advisers | Cyber Security Awareness Campaign (2022-23)

Exclusively for members of ARIA by Sanjay Kadel & Co. Infosec Partner

