Cyber Security Awareness

Mar-2022

RBI guidelines on Cyber Security

24 baseline controls on Cybersecurity

- Inventory management of business IT assets
- Installation of Software
- Environmental controls
- Network management and security
- Secure configuration
- Application security life cycle
- Patch/vulnerability& change management process
- User access control/management
- Authentication framework for customers
- Secure mail and messaging systems
- Vendor risk management
- Removable media
- Real-time threat-defense & management
- Anti-Phishing, Anti Rogue services
- Data-leak prevention strategy
- Maintenance, monitoring & analysis of audit logs
- Audit log settings
- Vulnerability assessment and penetration testing
- Incident response & management,
- Risk based transaction monitoring,
- Metrics
- Forensics
- User/employee/management awareness
- Customer education & awareness

Cyber Security Awareness Campaign 2022

1 . Contactless Payments

2. Sim Swapping and Sim Cloning Frauds

3. Dangers of Instant Personal Loan Apps

4. Online Scams through online classified market place

5. Broadband internet security

6. ATM Threats

7. Guidelines to report financial frauds in India

8. Loan Frauds

9. AePS

10. Online shopping safety measures

11. PoS safety

12. Digital Transactions/Credit and Debit Cards

13. UPI

14. Online Banking

15. Micro ATMs

16. Online Scams

17. BHIM

18. Credit card scams

19. ATM Risks/Tips

20. E-wallets

21. Mobile Banking

Cyber Security Awareness Objectives :

1) Increase and reinforce awareness of cybersecurity, including the risks and threats and provide solutions for the people
2) To promote and launch a comprehensive **awareness** program on security of cyberspace
3) To sustain security literacy awareness and publicity campaign through electronic media to help people beware of challenges of **cyber security**

For Information on Cyber Security Awareness Objectives for 2022, please click on Document below :

Microsoft Word Document

Emerging Cyber threats…

Phishing is the **attempt** to obtain sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication

Spear-Phishing is a pinpoint attack against a subset of people (eg employees of a company), by knowing your name, email address and other information about you, to undermine that company or organization.

Ransomware is an exploit or malware in which the attacker encrypts the victim's data and demands payment for the decryption key. Ransomware spreads through e-mail attachments, infected programs and compromised websites.

Vishing is phishing attacks on cell-phones usually smart-phones/PDA

Denial of Service attacks (DoS) and Distributed DoS (DDoS) are attacks involving bombarding bogus packets on your public network or public facing systems to slow them and making services unavailable

Advanced Persistent Threats (APT) are advanced targeted attacks on specific organizations.

Work-from-home Attacks : Staff using home broadband connections for both personal use and their jobs, the corporate attack surface has increased by a lot. Use of broadband while WFH should be controlled and disciplined

Fileless malware and ransomware attacks: A typical fileless attack might start with an **emailed link to a malicious website**. Social engineering tricks on that site can launch system tools, such as PowerShell, which retrieve and execute additional payloads directly in system memory. Avoid

Cloud and Remote Service Attacks: Data on cloud is susceptible to loss, breach, or damage as the result of human actions, application vulnerabilities, and unforeseen emergencies. It can be protected by applying modern encryption algorithms to ensure the integrity of data in transit from the user to the cloud.

Dont's

- Do not open mails or attachments from an untrusted sources
- Do not click on links from an unknown or untrusted source as it maybe a trap from cyber-attackers into visiting malicious sites
- Do not respond to suspicious phone calls or emails requesting confidential data such as CVV number, PIN,OTP, Expiry period etc. of the Credit / Debit or any other cards used for financial transactions
- Do not install un-authorized / unlicensed / crack versions /unknown programs on your computers as well as on mobiles
- Do not access office emails on personnel mobiles and download official files
- Do not use public /free Wi-Fi hotspots from devices used to store and process official data
- Do not forward official Data to personal email ids

- Do not register on social sites with personal /office details such as DOB, Residential address, Office email id, Designation etc. social sites
- Avoid saving your credit/debit card information on websites and web browsers.
- Avoid checking ‘Keep me logged in’ or ‘Remember me’ options on websites, especially on public computers.
- Do not use office laptops to surf on an open internet for entertainment purpose
- Do not visit any untrusted website to download unauthorized / free software. It could be malware / spyware
- Do not install and configure Office VPN software on personal laptops / systems

Do's

- Do lock your computer and mobile phone when not in use
- Do use hard to guess password or pass-phrases on mobiles and computers
- Do pay attention to phishing traps in emails
- Do pay attention to fraudulent calls, messages
- Do report to your IT team if office provided laptop or mobile is lost/ stolen
- Do inform your IT dept. to take regular backup of your important data
- Do make sure your system has Licensed Anti-virus / Anti-Malware application installed and is up to date
- Do apply security updates regularly on computers / mobiles

- Delete old accounts that you do not use anymore
- Always log out of online accounts when you are done. This is especially important when you are using a public computer
- Use 2FA authentication for connecting to office network over VPN connectivity
- Use only dedicated Wi-Fi connection for connecting to office VPN

- Do not leave wireless or Bluetooth connections turned ON handheld devices when not in use
- Do not leave mobile devices, office laptops / Desktops unattended
- Do not connect any removable media such as USB drive, mobiles (in File Transfer mode), USB CD drives etc. to office systems.

Thank You ☺