Cyber Security Awareness Presentation

RBI guidelines on CyberSecurity

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

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.

Dont's List

- 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 version /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 hot-spots from devices used to store and process official data

Do's List

- 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 Anti-virus / Anti-Malware application installed and is up to date
- Do report to IT department if any unusual behavior is observed on your system
- Do apply security updates on laptops / mobiles

- 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.