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
- 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
- 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.

Do's

- Do lock your computer and mobile phone when not in use
- Do use hard to guess password or pass-phrases as per the Bank's policy
- Do pay attention to phishing traps in email
- Do report to IT team if office provided laptop or mobile is lost/ stolen
- Do take regular backups of your important data
- Do make sure your system has latest anti-virus
- Do report any unusual behavior on your system to the IT department as well as Head of Department
- Do keep up to-date on Bank's cyber security policy and practices

Dont's

- Don't open mail or attachments from an untrusted source
- Don't click on links from an unknown or untrusted source as it maybe a trap from cyber-attackers into visiting malicious sites
- Don't respond to suspicious phone calls or emails requesting confidential data such as card CVV number, PIN, Expiry period etc.
- Don't install un-authorized programs and games on your work computer as well as on mobiles having office email account configured
- Do not access office emails on personnel mobiles and download official files
- Don't use public Wi-Fi hot-spots from devices that store and process official data

- Don’t leave wireless or blue-tooth turned ON when not in use
- Don’t leave mobile devices unattended
- Do not connect any removable media such as USB drive, mobiles (in File Transfer mode), USB CD drives etc. to systems in office.