Cyber Security Awareness

RBI guidelines on CyberSecurity
24 baseline controls

- Inventory management of business IT assets
- Installation of Softwares
- 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.

Email Spoofing is an type of hacking in which sender address that is forged to make it look as if it came from someone else. This is a common technique used by phishing attacks, spam, and malware to make their **emails** appear to be coming from legitimate sources, such as governmental authorities, insurance companies, and banks.

For E.g. rathinakumar.k@**dccsbank**.com instead of @dcbbank.com

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.

Shoulder Surfing is an attempt in spying your data, credentials, PIN etc. while operating it on devices such as Mobiles, laptops at crowded places

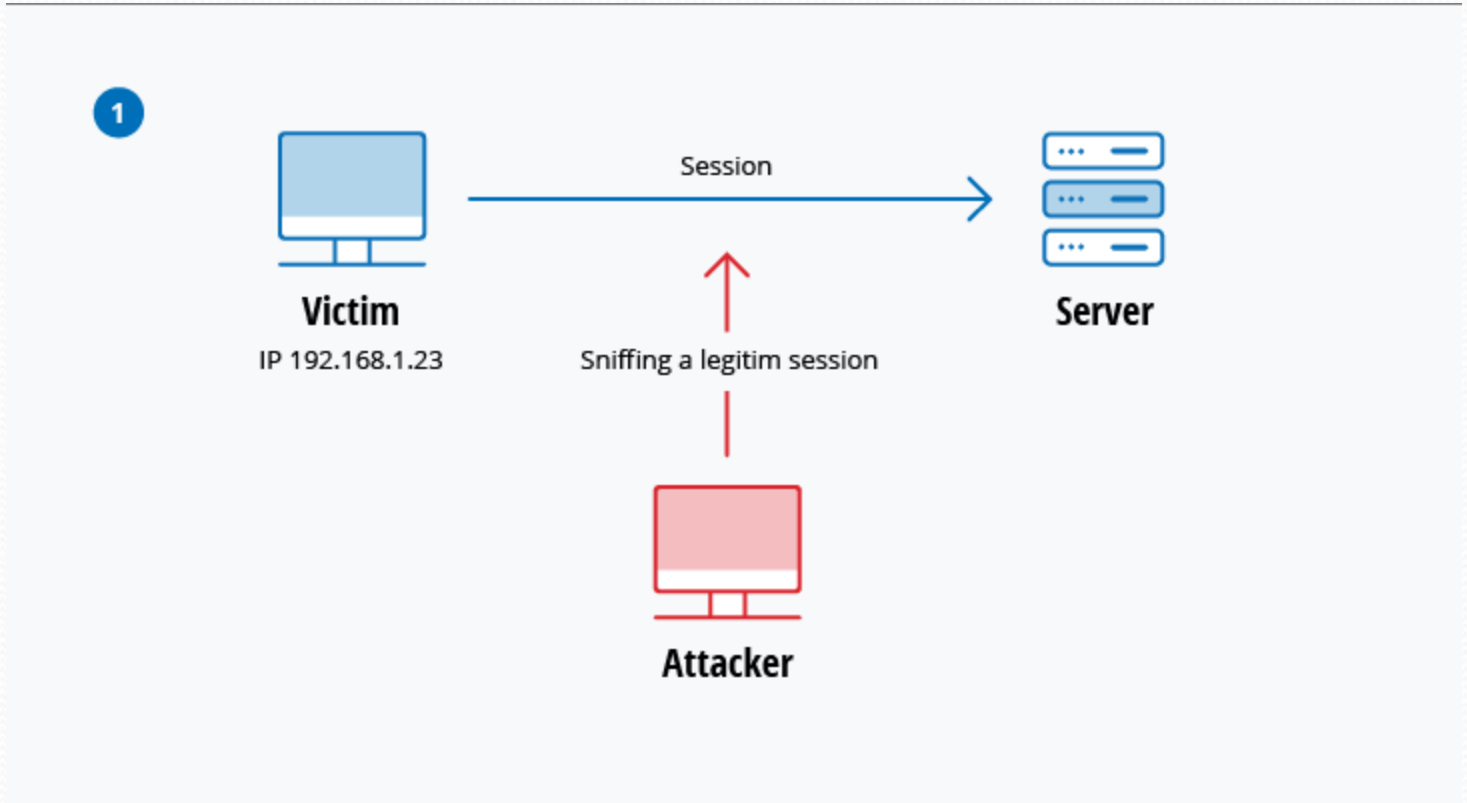
(MitM) attack

A MitM attack occurs when a hacker inserts itself between the communications of a client and a server.

For e.g. **Session hijacking**

In this type of MitM attack, an attacker hijacks a session between a trusted client and network server. The attacking computer substitutes its IP address for the trusted client while the server continues the session, believing it is communicating with the client. For instance, the attack might unfold like this:

- A client connects to a server.
- The attacker's computer gains control of the client.
- The attacker's computer disconnects the client from the server
- The attacker's computer replaces the client's IP address with its own IP address and spoofs the client's sequence numbers
- The attacker's computer continues dialog with the server and the server believes it is still communicating with the client


1
Session
Victim
IP 192.168.1.23
Sniffing a legitim session
Server
Attacker

Juice Jacking : Juice Jacking is a type of fraud involving a charging port typically over USB. This often involves either installing malware or copying sensitive data from a smart phone, tablet, or laptop of the victim with malicious intentions.

For e.g. Unsecured mobile charging points at railway platforms, hotels etc.

To Avoid any Juice Jacking incidence you may follow simple steps as below :

- **Go to settings and Disable Data Transfer while charging**
- **Switch off Handset before recharging**
- **Always carry your own power bank while going out of station**
- **Avoid opening password pattern tool**

Why Cyber Security Awareness sessions are necessary?

Security awareness session is all about teaching your colleagues and employees to understand the risks and threats around the ever evolving cyber world. Security awareness training also ensures that employees are aware of the consequences of failing to protect the organisation from outside attackers.

There are few general practises which can be followed by all employees of the organization to protect themselves at individual level as well as at an organization level from any possible Cyber attack.

Do use hard to guess password or pass-phrases on mobiles and computers :

- Don't share your passwords and avoid writing them down.
- Characteristics of good, cryptic passwords:
  - Contain a mixture of upper and lower case letters, numbers, and symbols
  - At least 8 characters in length (or longer if they're less complex)
  - Difficult to guess (e.g. don't include real words or personal information like user name, names of family members, places, pets, birthdays, addresses, hobbies, etc.)
  - Easy to remember (so you don't have to write them down)
- Enable Password protect all of your devices.

Beware of scams

- **Never reveal your password(s) or click on unknown links or attachments. Be careful who you share your private information with.**
  Don't respond to email, instant messages (IM), texts, phone calls, etc., asking you for your password of any account(s). You should never disclose your password to anyone, even if they say they work for organizations such as Banks, Charity, Financial firms etc.
- Only click on links from trusted sources. Never click on an unfamiliar link unless you have a way to independently verify that it is safe. This includes tiny URLs and any link where you can't tell where it will take you.
- Don't open unsolicited or unexpected attachments. If you can't verify an attachment is legitimate, delete it immediately as well as inform IT team to take further action
- Don't give private information to anyone you don't know or who doesn't have a legitimate need for it -- in person, over the phone calls, via e-mail, IM, text or on social sites such as Facebook, Twitter, etc.
- Beware telephonic support scams. These are usually over the phone and threaten serious consequences if you don't act immediately. **For. e.g**. Fake executive will call on your mobile number. He will tell you that Your debit card of xxxx bank has been blocked. To Issue a new card you will have to tell us the details of OLD card and the CVV. Once you give these details to them your account will be hacked and amount will be debited from your bank account

Secure laptop computers and mobile devices at all times: Lock them up or carry them with you

- In your office, at coffee shops, meetings, conferences, etc.
  Remember: Phones and laptops get stolen from cars, houses, and offices all the time.
- Make sure these devices are locked / Auto locked.
- May use lockdown cables for laptops and or follow Clean desk policy

Protect information when using the Internet and email

- Look for **https://** (not http://) in the URL to indicate that there is a secure connection.
- Be especially careful about what you do over wireless. Information and passwords sent via standard, unencrypted wireless are especially easy for hackers to intercept **(Note : most public access wireless is unencrypted).**
- Check your wireless preferences/settings to make sure your devices aren't set up to auto-connect to any wireless network they detect. Auto-connecting to unknown networks could put your device and data at risk.
- Don't send restricted data / official files via public email applications, text or instant message (IM). These are not generally secure methods of communication.
- Be extremely careful with 3rd party, Free file sharing software. Filesharing applications opens your computer to the risk of malicious files and attackers. Also, if you share copyrighted files, you risk being disconnected from the office network.

Make sure your computer is protected with well known anti-virus and all necessary security "patches" and updates are latest ones

- Shut down or restart your computer / laptop at least weekly -- and whenever your programs tell you to in order to install updates. This helps to make sure software and security updates are properly installed.
- Contact IT team desktop / laptop for updating your desktops / laptops.
- If you get an antivirus alert that there is malware on your computer, contact the IT team for assistance.

Shut down, lock, log off, or put your computer and other devices to sleep before leaving them unattended, and make sure they require a secure password to start up or wake-up

- Use <ctrl><alt><delete> or <Windows><L> on windows system and Apple menu or power button on a Mac.
- Also set your computer and portable devices to automatically lock when they're not being used.

Don't install or download unknown or unsolicited programs/apps to your computer, phone, or other devices

- These can harbour behind-the-scenes viruses / malwares or open a "back door" to hackers giving them direct or indirect access to your devices without your knowledge.

Secure your area before leaving it unattended.

- Lock the drawers and take keys and never share your access cards or keys.

Make backup copies of files or data you are not willing to lose and store the copies very securely.

As a safety precaution, make more than 1 copy of your important data

Shut down, lock, log off, or put your computer and other devices to sleep before leaving them unattended, and make sure they require a secure password to start up or wake-up

- Use <ctrl><alt><delete> or <Windows><L> on windows system and Apple menu or power button on a Mac.
- Also set your computer and portable devices to automatically lock when they're not being used.

Don't install or download unknown or unsolicited programs/apps to your computer, phone, or other devices

- These can harbour behind-the-scenes viruses / malwares or open a "back door" to hackers giving them direct or indirect access to your devices without your knowledge.

Cyber Security Basics while WFH

Cyber Criminals can target companies, Financial Institutions etc. of All Sizes, so it is very important to keep ourselves safe and secured from any such cyber attack.

Knowing some cyber security basics and putting them in practice will help you protect your business and reduce the risk of a cyber attack even when you are working from home.

- **Keep Work Data on Work Computers only**

Even though you are using personal laptops only for email access and sharing official files, please avoid saving official files on personal laptops**.** Please use office laptops only to save, work and sharing the files

- Avoid using personal laptops to connect to Bank's network

- Update your Operating systems / security applications

This includes your operating systems and Antivirus. Set updates to happen automatically wherever it is possible.

- Secure your files

Do not keep any official data on local pc/ laptop. Keep all official data on Shared drive only.

- **Use multi-factor authentication**

Enable 2 Factor Authentication to connect and use VPN. Do not allow an access to VPN without 2 Factor authentication

- **Secure your router / Mobile hotspot**

Change the default name and password, turn off remote management, and log out as the administrator once the Wi-Fi router is set up.

- **Use at least WPA2 encryption**

Make sure your home router or mobile hotspot offers WPA2 or WPA3 encryption, and that it's turned on. Encryption protects information sent over your network so it can't be read by outsiders.

- **Require strong passwords**

A strong password is at least 12 characters that are a mix of numbers, symbols, and capital lowercase letters. Never reuse passwords and don't share them on the phone, in texts, or by email. Limit the number of unsuccessful log-in attempts to limit password-guessing attacks.

Thank You