



# Cyber Risk Aware's: Do's and Don'ts



Below are the most important **Do's and Don'ts** to keep you safe from cyber threats

## DO'S

**Install only licensed anti-virus/software on PC, Laptop, Server, Tablet and Smartphone.**

*Update them regularly with latest patches to address security holes in your OS/applications.*

**Always keep back-up of your important documents.**

*Avoid cyber cafes for financial transactions.*

**Note:legitimate financial institutions will never ask you for your account information via e-mail or chat.**

*Download files from trustworthy websites only*

**Configure your e-mail to display messages only in plain text. Users can decide to view blocked images only from trusted sources.**

*Disable java-script for e-mail in your browser.*

**Disable automatic opening of attachments in your outlook e-mail client.**

*Personal e-mail IDs should be used only for personal communication & not for aofficial communication.*

**Manage your Financial Passwords i.e., change passwords every 15day.**

*Activate two-step authentication for online services.*

**Assign a separate useame for your family members. They should have their own account on a PC.**

*Check social network configuration of your family members. Personal data shared poses risk to security of family members.*

**Monitor browsing records. If you observe that these records are deleted, then the family member may need your counseling.**

*Regularly advise family members on pros and cons of using internet.*



## DON'TS

**Use pirated anti-virus or software, as it may contain Trojan viruses and malware**

*Ignore updates, offered by Microsoft Windows update Service (WSUS) & software vendors*

**Leave your pen-drive, portable HDD or CD / DVD with important data in open-space**

*Click suspicious or unknown links*

**Send/reveal confidential information, especially your PIN, over the internet through email or chat**

*Open suspicious emails / their attachments & those from unknown people*

**Reply to spam messages**

*Publish your e-mail address on internet when not needed*

**Share your e-mail address with unknown individuals**

*Use simple passwords for different accounts*

**Install or share info with third party applications until you check their authenticity**

*Allow family members to view / browse websites that may contain potentially offensive information*

**Keep webcam connected to PC while not in use**

*Ignore conversations with your colleagues / family members if you feel they are depressed or worried after spending time on internet*