Cyber Security
Do's and Don'ts

The security of data and information in an electronic format is of utmost importance. The loss due to intrusion into the sensitive information by the intruders could be beyond imagination as it differs from the content and the sensitivity of the information and data. The loss could be financial as well as threats and security of the organization and the country sovernighity. Prevention is the best cure as the loss due to breach in the information and data could not be quantifiable and hence there is a need to take number of basic measures as suggested herein. However, there is no security which can be foolproof as people make mistakes, equipment fails and threats keep shifting thus constant review of such measures is essential. As consumers of the information economy each person has a responsibility to contribute to cyber security in his own way. One security hole could provide access to a scamester to the network. Thus ensuring cyber security is your responsibility and adherence to the Do's and Don'ts will be your contribution to the same.

Do's

- Do ensure physical security of your computer, laptop or mobile phone at all times, unattended hardware will provide ordinary as well as cyber criminals a lucrative opportunity for intrusion apart from loss of a valuable item in retrieving the system.
- Do ensure access control by incorporating appropriate identification and authentication mechanism like 'complex passwords' at different levels and ' dynamic log-in' by verifying users' magnetic strip cards, fingerprints and voice recognition, depending upon the nature and sensitivity of data. Combination of password with alphabets, numerals and special character could be a better password protection.
- Do use effective encryption techniques while communicating sensitive information over networks. Simple encryption software can be downloaded.
- Do ensure that you overwrite sensitive files with some junk data before deleting these. Antivirus software has facilities for file shredding. Use the same instead of simply deleting the file.
- Do ensure you have a back up copy of sensitive files and keep the same constantly updated. Antivirus software frequently has back up facilities bundled with the main package which can be availed of.
- Use original operating software like Windows, Office etc. The original software are expensive but will ensure security of your information.
- Be careful while installing software, criminals attempt to dupe users into downloading malicious software.
- Do update software regularly. Suppliers of PCs, software, and operating systems such as Windows frequently releases software updates (patches) to fix minor problems (bugs) or improve security. Keeping the computer up to date is important.

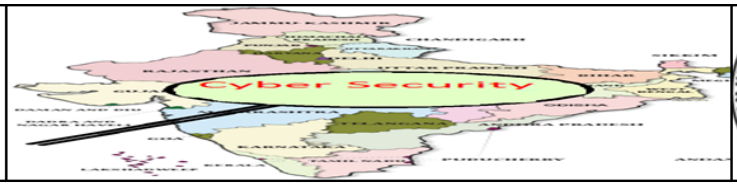
STATE CONSUMER HELPLINE
KNOWLEDGE RESOURCE MANAGEMENT PORTAL
Centre for Consumer Studies, Indian Institute of Public Administration, New Delhi
Phone - (011) 23705055 , TELEFAX - (011) 23705054
Email - schkrmp.iipa@gmail.com
Website - www.consumeradvice.in, www.consumereducation.in

- Update your anti-virus software regularly. The antivirus software update automatically in the background and continuously via the Internet.
- Do ensure that all removable media as CDs, pen drives and so on are in proper custody and regularly accounted for.
- Do test every removable hard disk, CD and pen drive for virus infection by running a scan on the system on insertion.
- Do destroy damaged and unusable CDs / pen drives by burning rather than dumping in the garbage in case these contain sensitive information.
- Do ensure that maintenance and repair is done by a competent person from an authorized agency and person does not pilfer data or manipulate the system
- Do use Uninterrupted Power Supply (UPS) with sufficient back up in case you have frequent power break downs which are normal in India.
- Do delete chain and junk emails rather than forwarding these mails.
- Do ensure software is loaded to delete all information on a laptop or mobile phone from remote locations to safeguard the same in case it is stolen.
- Do ensure that user name and pass words for a computer even if only one person is using the laptop or computer. As all files contain the user name, this will ensure that your identity is also secure in case of identity theft.
- All the important documents containing sensitive information may be secured with passwords
- Do make smart passwords a habit. This will include a combination of upper- and lower-case letters, numbers and symbols. Minimum length of a good password is eight characters which should be frequently changed by setting an expiry period.
- Do ensure security if you are using cloud computing services. Check level of security provided by cloud computing provider and as most of these are based outside India legal aspects need consideration.
- Do update Email list regularly and delete contacts who are unknown from time to time,
- Do log out of websites after accessing desired information.
- Do exercise caution when downloading files from the Internet. Ensure that the source is a legitimate and reputable one. Verify that an anti-virus program in the email checks the files on the download site.
- Do err on the side of caution when in doubt and do not open, download, or execute any files or email attachments.
- Do maintain logbook regarding all activities carried out on computer systems indicating the name of the user, duration for which a particular user used the computer, type of activity carried out etc. 'Audit Trail Concept' should be incorporated in the system where high security is essential.
- Do ensure that all financial transactions have multiple levels of security including a system of one time passwords and authentication of persons issuing instructions.
- Do always visit Internet Banking site through the bank's web site.
- Do verify domain name displayed on the site to avoid spoof websites.

- Do ensure a suitable firewall is installed in your PC to protect the contents from outsiders on the internet.
- Do enter User ID and Password only at the authenticated login page of the Bank and use virtual keyboard feature while logging into your Internet banking account.
- Do check account and transaction history regularly. Check your statements for any transactions that look suspicious.
- Do check the Last Log-in Date and Time on the top right hand corner to monitor any unauthorised logins.
- Do, "Log Out," after using the Internet Banking Service and not just close the window.
- Do close your Internet browser after logging out of each Internet Banking session.
- Do contact bank if you lose your pin number or card immediately on the Customer Service Number and by Email.
- Do change your password and pin number frequently.
- Do report any suspicious infringement immediately to bank's customer care telephone and through email.
- Do treat your smart phone like a wallet - keep it safe and on your person at all times.
- Do remember your smart phone is a computer, thus all security rules should apply to the same.
- Do use only reputed mobile applications (apps)
- Do turn on the security features of your phone, set a password or Personal Identification Number (PIN). Use the same rules for setting passwords as for computers.
- Do check for updates to phones operating system regularly. Install them as soon as they are available.
- Do use only encrypted networks for Wi-Fi.
- Do note down complete details of your phone in case of theft, in particular the unique International Mobile Station Equipment Identity (IMEI). Network provider can stop phone being used if it is stolen.
- Do report loss of telephone to network operator immediately so it can be disabled. If you find it the same can be easily re-enable the phone.
- Do check your phone bill details regularly, an infected phone will also lead to inflated bills.

Don'ts

- Do not use pirated software – including operating system, application and antivirus, as it is not just a security hazard but may also result in systems crash at a critical time.
- Do not download any files from Emails sent by strangers. Preferably use email services as Google which contains software that checks virus in attachments.
- Do not download files from the Internet directly without confirming the source. Use an antivirus program that checks files before downloading.
- Do not open files when in doubt even from known Email addresses. Some viruses can replicate themselves and spread through email. Confirm that your contact really sent an attachment.
- Do not open any files attached to an email if the subject line is questionable or unexpected.



- Don't let any un-authorised person use your computer system.
- Don't share your password with anyone, not even with your colleagues.
- Don’t have a, ‘family,’ password based on the names of members of the family as these are the easiest to break.
- Don't connect computers directly to mains. Also, no heavy electric load drawing machines like photo copier, shredder, A/C, cooler etc. should be connected to the source of power supply to the computer.
- Do not get carried away by Emails promising large sums of money through an inheritance or other sources like winning lottery tickets, prizes etc. These are invariably Spam.
- Do not make friend requests to strangers on Facebook or Twitter .
- Do not forward or reply to chain email. Delete chain emails and junk email.
- Do not save passwords or PINs as contacts on phone unless they are encrypted.
- Don’t turn on Bluetooth permanently, do so only when planning to use the same and then only in a safe environment.
- Do not open multimedia messages (MMS) or attachments in emails, or click on links in emails and SMS messages unless they are from a trusted source. They could contain malicious software or lead to a malicious website.
- Do not leave mobile phones, laptops,, tablets, digital cameras, and other devices that use lithium batteries on dash board of car during excessive heat with glasses rolled up as they are not only attractive targets for thieves but may also explode.
- Do not surf internet at cyber cafe for sensitive information.

STATE CONSUMER HELPLINES

Andhra Pradesh	1800-425-0082,1800-425-2977	Odisha	1800-345-6724,1800-3456760
Bihar	1800-345-6188	Puducherry	1800-425-1082,1800-425-1083,1800-425-1084,1800-425-1085
Gujarat	1800-233-0222,079-27489945,079-27489946	Rajasthan	1800-180-6030
Haryana	1800-180-2087	Tamilnadu	044-28592828
Himachal Pradesh	1800-180-8026	Telangana	1800-425-00333
Jharkhand	1800-3456-598	Tripura	1800-345-3665
Madhya Pradesh	155343,0755-2559778,0755-2559993	Uttar Pradesh	1800-1800-300
Maharashtra	1800-22-2262	Uttrakhand	1800-180-4188
Mizoram	1800-345-3891	West Bengal	1800-345-2808