31 Days

Cyber Safety Challenge

Day 1	Day 2	Day 3	Day 4	Day 5
Ensure that every critical login accounts which you are using have Multi Factor Authentication Enabled	Make sure your operating system, application and software patches including anti-virus software are up to date; and Auto updates are turned on in your computer.	Remove unnecessary programs or services from computer Which are not required for day-to-day operation with the help of Systems Administrator.	Ensure that Malware / Antivirus Protection is enabled and updated in your system.	Ensure strong and unique passwords for each login account.
Day 6	**Day 7**	**Day 8**	**Day 9**	**Day 10**
Ensure that your critical files are being backed-up in an automated way and being tested for its successful restoration in case of disaster.	Ensure that you are not using any non-bank specific domain email IDs (ex. Gmail, yahoo, rediff mail, etc.) for any official communication.	Ensure that you are not storing any usernames and passwords on the Internet browser.	Ensure that you are using only Standard User (Non-Administrator) account for accessing the computer/ laptops for regular work.	Ensure that your all login accounts must use complex passwords with a minimum length of 8 characters.
Day 11	**Day 12**	**Day 13**	**Day 14**	**Day 15**
Ensure that no classified information of government / bank should be stored on Private cloud services (Google drive, Dropbox, iCloud etc.).	Ensure that you are not disclosing any official information on social media or social Networking portals or applications.	Ensure that a password-protected screen saver is enabled with a timeout period of 2 minutes to ensure that computers that were left Unsecured will be protected.	Ensure that you are not giving any remote access, file and print sharing option to Other computers.	Ensure that the Auto run/ Auto play feature must be disabled for all Removable media (including Pen Drives, Portable Hard Disks etc.)
Day 16	**Day 17**	**Day 18**	**Day 19**	**Day 20**
Review social media accounts and remove personal sensitive information.	Secure your android phones by installing free antivirus provided by the CERT-In If it is	Check for any passwords/ PIN written on paper and discard them.	Remove Remote Access Tool from Desktop/ Mobile.	Learn about Browser Privacy settings (Incognito-InPrivate Mode in web browsers)

	not installed already. Link			
Day 21	**Day 22**	**Day 23**	**Day 24**	**Day 25**
Learn about phishing, vishing and privacy risks.	Learn to use website filtering settings in web browser.	Learn how and where to report Cyber Incidents / Cyber Crime.	Learn to identify and detect malicious URLs/Links. Eg:nabạrd.org is not same as nabard.org	Disable international transactions on payment channels, if not needed.
Day 26	**Day 27**	**Day 28**	**Day 29**	**Day 30/31**
Review apps permission in your mobile and limit.	Learn about secure email use.	Remove extra-unused apps / programs from smartphone/ Any other Mobile Devices.	Configure pop-up blocker for the browser.	Spread cyber security awareness among the colleagues and friends.