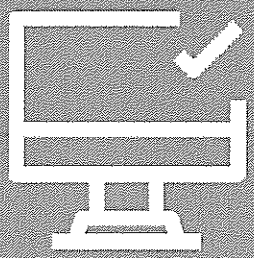
RSM

CYBER HYGIENCE CHECKLIST



Password Management

S/No	Description	Remarks
	Change passwords once every three months.	Set a calendar reminder.
	Change router password and SSID every three months.	Check with your local ISP.
	Use different login name and password for different websites. (Internet Banking, Social Media, Email, etc.)	Visit the official website for each service/account to find out how to change your password.
	Use complex passwords. (e.g. #S780218#03-82e)	A mix of upper case letters, lower case letters, numbers and symbols
	Use token for 2FA. Avoid using SMS for 2FA.	Obtain token from banks, government bodies and suppliers.

Device Security Management

S/No	Description	Remarks
	Avoid using free Wi-Fi hotspots in public areas. (Use your mobile data)	Turn off device Wi-Fi when in public areas.
	Switch off location services, Wi-Fi and Bluetooth on your device when not in use.	Develop a habit to check your device settings.
	Restart your mobile devices and computers regularly.	• Restart mobile device every night. • Turn off computers after use.
	Install the latest security patches for mobile devices, operating systems and applications.	Verify that automatic updates are genuine.
	Use WebCam cover (KISSclip) for laptops and mobile devices.	Some malwares can secretly activate device cameras.
	Change your CCTV camera's default password to a alternate password that is secured.	CCTV cameras using the default password are easily compromised.

Data Security Management

S/No	Description	Remarks
	Backup your valuable data on a regular basis.	Schedule a backup when you edit or add important data.
	Alternate backups using different hard drives.	Use different external USB Hard drives from different brands.
	Disconnect your external backup storage device when not in use.	To prevent malware (e.g. ransomware) from destroying valuable data.
	Password protect sensitive data files.	Refer to software documentation.
	Backup storage devices should be locked in a fire-rated safe or stored offsite (e.g. bank's deposit box).	Store in a cool area and in a locked cabinet.

Personal Security Management

S/No	Description	Remarks
	Change SMS alert for credit card transactions to $1 (Default is usually set at $1000).	Call your credit card company to find out how you can do this.
	Change "Mom", "Dear", "Wife", "Son" ... to the person's name on your contact list. Do not disclose your relationships.	• Mobile devices • Address books and contact lists • Social media accounts
	Do not share your login name or password with anyone.	Not even family members. Information may be leaked to criminals.
	Be wary of anonymous phone calls: • "I am calling from the police station ..." • "A kid crying ... help me dad ..." • "Your xxx met an accident ..." • "You have won $1 Million ..." • "You have a parcel ..."	• Stay calm and take down caller's particulars. • Verify dubious claims. • Make a police report if you suspect it is a scam.