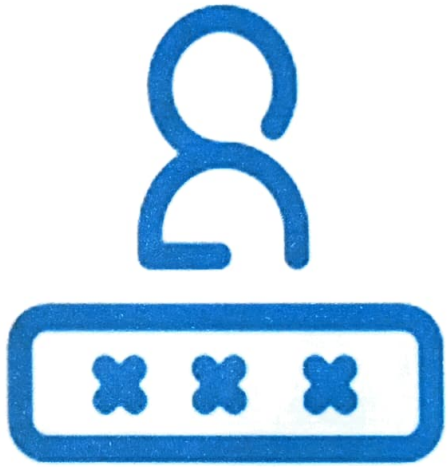
COFFEE AND PASSWORDS ARE BEST WHEN THEY ARE STRONG



Password Tips

Use atleast eight (8) characters

Make sure it contains alphabets, numbers and special characters

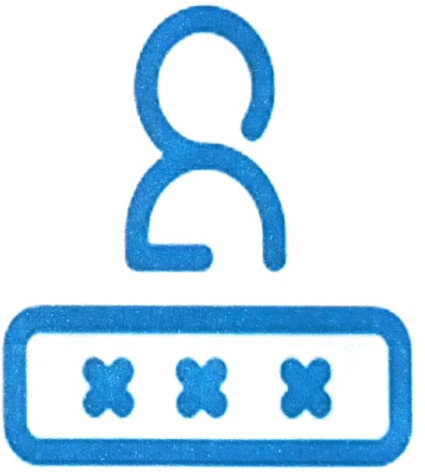
Change your passwords/ passphrases regularly.

Make sure no one watches when you enter your password

Give preference to passphrases instead of passwords e.g Up@1B2$Atm@7

M.Y. KICHLOO, SSP SECURITY CIVIL SECRETARIAT J&K

Coffee and passwords are best when they are **STRONG**



Password tips

Use atleast 8 characters

Make sure it contains alphabets, numbers and special characters

Be sure no one watches when you enter your password

Use short phases like (Up&Atm@7)

LARSEN & TOUBRO

CYBER THOUGHT:-

Dear netizens, we are gaga about smart phones and becoming Techno savvy/ Technobuff transforming our lives into nomo phobic world, an alarming signal as to playing second fiddle to human relations (Compassion/ sympathy/ empathy etc) by indulging willy-nilly into phubbing, paving a way towards dystopian society.

Can't we pledge techno camping for some hours a day to act as real humans?!!!

M.Y. KICHLOO, SSP SECURITY CIVIL SECRETARIAT J&K

PREVENTIVE MEASURES.

- Never share your Password with anyone.
- Never select "Remember My Password" option Many applications don't store them securely.
- Avoid creating common Password such as your name, your birthday etc.
- Use Passphrase instead of Password.
- Change your Password regularly.
- Include capital/small letter/No's in the beginning and in the end/special character etc to build a "Strong password"
- Please refrain from opening an e-mail attachment, even from someone you know unless you were expecting it.
- Never set your e-mail program to "automatic open" attachments.
- Do you know that most of the social media sites and e-mail service providers give you an option of two factor authentication to login into your account? You can go to setting and activate two factor authentications. This means you will need to type your password and One Time Password (OTP) received on your mobile to login to your account. It is a good safety feature and should be used for all your accounts.
- If your social media account is hacked/ compromised, send an alert e-mail or messages to all your contacts. Immediately ask your social media service provider to temporarily block your account. Try to retrieve your password and change your password immediately.
- If you notice that your fake account has been created, you can immediately inform social media service provider so that the account can be blocked. If Someone is bullying you or cyber-stalking or posting inappropriate comments or images or creating your fake account to damage your image, inform your parents or elders immediately so that they can support and guide you. With support from your parents, you can also register a complaint at your nearest police station or Cyber cell.
- Never purchase anything prompted in a spam message. Even if the offer is not a scam, you are only helping to finance and encourage spam.
- Don't give your Smartphone/Computer/laptop to anyone.
- Choose your friends & followers on social networking sites carefully. Give your access of yo2ur posts to your friends/followers only. Set your "settings" accordingly.
- Never attend phone calls of unknown persons.
- Never share your bank details/ aadharcard details/ OTP/ C.V.V of ATM/ credit card etc to anyone.
- There are phone calls/ SMS/ Whatsapp etc messages for winning of "Lottery"-never fall prey to these calls/messages. Don't reply. "Please inform Police".
- Don't share your details or documents with anyone.

- Make sure to stand by the photocopy machine to ensure that no extra copies are being printed.
- Always ask the shop owner to delete your scanned documents in front of you.
- If you are using public system to upload your documents online, make sure to delete the browser history and cache before leaving the place.
- Never share your details with any unverified lucky draw, contest, event organizer and other such people.
- Avoid using wifi at Public Places like Railway Station /Airport etc in case of emergency use VPN.
- Avoid using Pics in D.P/Profile and avoid sharing pics on social networking as morphing can damage your reputation.
- Avoid giving real-time location/updates/checkin on social networking particularly of children.
- Avoid video calls & chatting with unknown persons-never share any detail.
- Avoid dating with unknown persons as on social networking sites cybercriminals befriend and fix meeting at some place. This may lead to any harm.
- Avoid accepting friend request from unknown people. Before accepting a friend request try to see how many other people are following or are in friend's list of the requestor. Cybercriminals can create fake account of your known persons so be careful.
- Use Antivirus/Firewall etc.
- Clear all work you have done on computer as "scavenging" may give information to others.
- Don't charge your phone or use free wifi at Railway Station, Airport etc. as it may compromise your data. This crime is Juice Jacking.
- Don't attend video calls of unknown number, it may be a sextortion where a fraudester may be nude and can make short video recording to black mail you later.
- During Covid fraudesters start ponzi schemes of investment like power bank. Please do not fall prey to such schemes.
- Please don't share any information on phone, email, messenger etc.
- Cases of facebook hacking/ cloning are reported very often. Please lock profile pictures in settings and also go for double authentication of Facebook and whatsapp etc.

Police is at your service-please inform timely for action under law.

M.Y. KICHLOO, SSP SECURITY CIVIL SECRETARIAT J&K