PRESS NOTE

Today on 15.03.2019, Chandigarh Police organized an awareness event with the help of Home Credit India Finance Pvt. Ltd. at Recruitment Training Centre, Police Lines Sector-26 for the awareness of police force regarding financial and cyber frauds and help in investigation of financial and Cyber frauds. The event was organized in the presence of W/SSP Nilambari Jagadale and SP/Hqrs, SP/Operations, DSP-Cybercrimes, SDPO-Central and SDPO-South were also present along with Sh. Manish Kaushik, Security Head of Home Credit India. In this awareness event more than 150 police officials of every rank from different units of Chandigarh Police attended this event. During the day long event, officials of Home Credit India conducts knowledge sharing sessions with Police officials across different levels on challenges, issues and measures relating to prevention of cybercrime, cyber bullying, online and financial frauds. These sessions highlight current trends through case studies and reference materials. During sessions, many topics like rising incidents of cyber stalking, web jacking, juice jacking, theft of online data, ATM frauds, phishing frauds etc. were discussed. The aim of event is assisting the police force in reducing/investigating cyber crime and financial frauds in the city, so that Chandigarh Police can provide the citizens a safe and friendly platform with technology for online banking to protect them from financial frauds and cyber crimes. The Chandigarh Police, Cyber Cell in assistance with Home Credit will train Police officials of all Police Stations in the city regarding financial frauds to enable Police Stations to deal with basic complaints of Cyber Crime. For general awareness regarding Cyber frauds, Do & Don'ts are as under:-

- A strong password shall make your venturing into cyber space safer.
- To stay away and not accept invites, as well as friend requests from unknown persons.
- Do not give/share your password with friends.
- Don't give common password for all social networking accounts and don't expose your passwords to un-trusted sites
- Change your current PIN from time to time to make it more difficult for fraudsters to guess.
- Never write down your personal identification number (PIN), especially on the back of your card. Memorize it.
- Don't lend or hand over your cards to anyone. The innocent looking bartender/petrol pump attendant/ restaurant waiter could be carrying a skimmer to skim your card. Report lost or stolen credit cards immediately to bank that issued you the card by calling the call center

- If you receive an email/phone calls asking for your credit/debit/ATM card details. Never respond to such emails/phone calls; even if they seem to official emails from your bank. Your bank will never ask you for confidential information via emails, calls or texts. If you do receive any such communication, report it to your bank.
- Don’t reply to the received SMS/MMS from strangers as it could be a Smshing/Vishing attack.
- Don’t share your internet as Hot spot to other/strangers.
- Don’t always keep turn on your location
- Don’t give your mobile numbers where chatting on internet to avoid “STALKING”
- Don’t handover your mobile phone to unauthorized service centre, to avoid “CLONING/MISUSE”
- MMS/SMS/links received should be checked before opening the message as there could be hidden attachments for fraud and remote access of your device.
- It is best to refrain form clicking on the pop-ups and unknown websites links.
- The mails which make claims about winning a prize money are malicious and must be ignored
- Verify about the company/organization when you applying for a job/VISA/ work permit online. Don’t deposit money in hurry.
- No IRDA agent can call/ discuss over phone for your Insurance policy or investment.
- Be vigilant when purchase any product from OLX/Quickr and do not deposit money in hurry.
- Avoid public charging points to charge your mobile phones as the data of your mobile phone can be fetch through data cables by fraudsters.