Chola

Enter a better life

IS YOUR PHONE BEING SPIED ON?

FACTORS INDICATING THAT A PHONE IS BEING SPIED

- Unfamiliar applications are being downloaded on the phone.

- There is a faster than usual draining of phone battery.

- A phone turning hot may be a sign of someone spying by running spyware in the background.

- An unusual surge in the amount of data consumption can sometimes be a sign that spyware is running in the background.

- Spyware apps might sometimes interfere with a phone’s shutdown process so that the device fails to turn off properly or takes an unusually long time to do so.

- Note that text messages can be used by spyware and malware to send and receive data

BEWARE OF SPYWARE!

Chola
Enter a better life

Swipe WITH CARE!

Though plastic money has brought us a lot of convenience, it has also opened a gateway to Debit/Credit Card fraud. It is very crucial to use your cards carefully to stay away from fraudulent traps.

Precautions to take while using Debit/Credit Cards:

- You should deactivate various features of credit/debit cards, viz., online transactions both for domestic and international transactions, in case you are not going to use the card for a while and activate the same only when the card usage is required.
- Similarly, the Near Field Communication (NFC) feature should be deactivated, if the card is not to be used.
- Before entering a PIN at any Point of Sale (POS) site or while using the card at an NFC reader, you must carefully check the amount displayed on the POS machine screen and NFC reader.
- Never let the merchant take the card away from your sight for swiping while making a transaction.
- Cover the keypad with your other hand while entering the PIN at a POS site / ATM.

Chola
Enter a better life

STAY SAFE ONLINE!

KNOW WHO YOU'RE TALKING TO!
Keep yourself safe from people who hack your privacy!

KNOW WHAT YOU ARE POSTING!
Limit what you share and post online.

DON'T CLICK ON UNKNOWN LINKS!
There are many links online that can hack your devices instantly.

KEEP YOUR PASSWORDS PROTECTED!
Ensure your passwords are strong and change passwords often to stay safe.

DON'T SHARE YOUR OTP!
Never share your One Time Passwords to anyone – not even your bank agents.

KEEP YOUR ANTI-VIRUS UPDATED!
Invest in a good anti-virus scheme – it is worth it!

KEEP YOUR DATA PROTECTED!
Don't share your personal data to unknown or unauthorized sources.

STAY SAFE USING PUBLIC INTERNET ACCESS!
Browse the internet using known sources.

Chola
Enter a better life

ONLINE FRAUD USING CASHBACK OFFERS

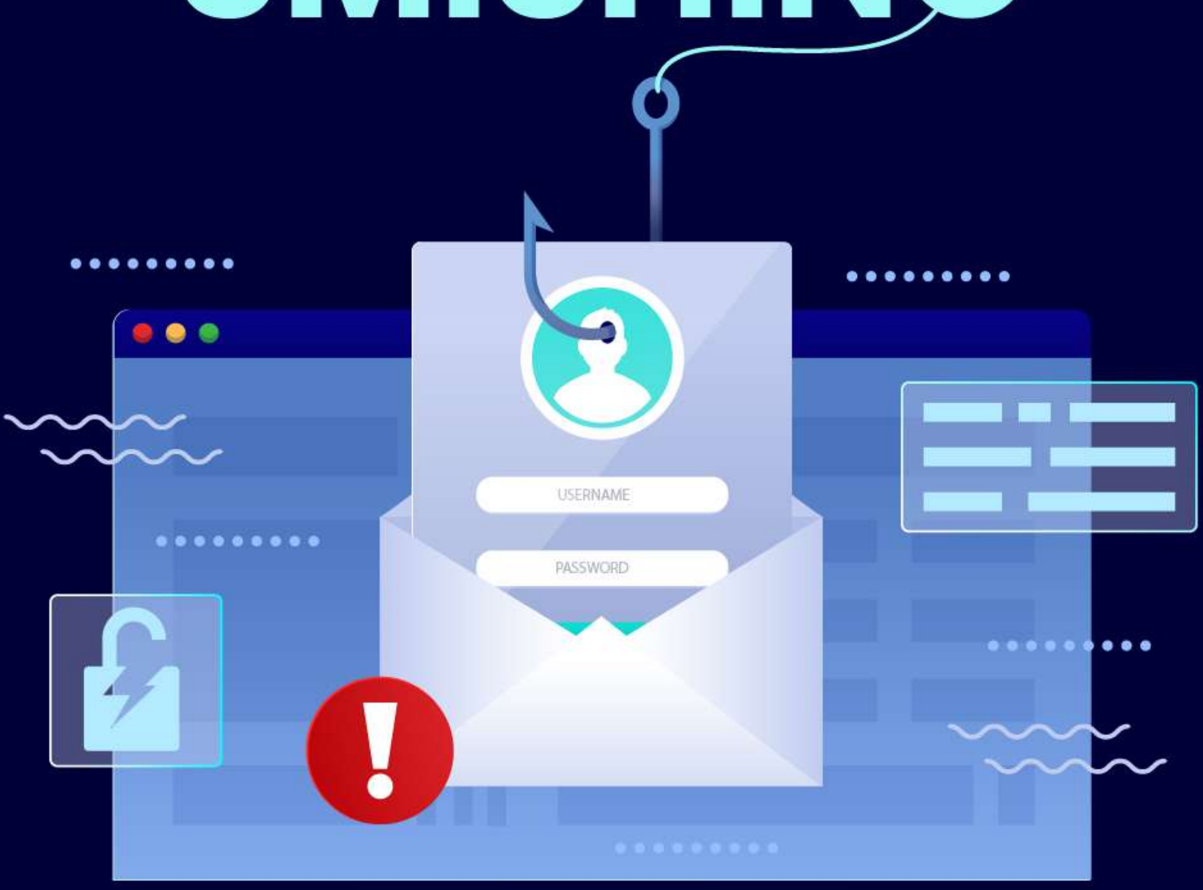
TIPS TO STAY AWAY FROM ONLINE FRAUD USING CASHBACK OFFERS

- Inform your home branch and block your account to prevent further financial loss.
- Don't believe e caller blindly: should verify the company's official website to check the authenticity of the offer.
- Don't enter or share UPI PIN for receiving payments as it is required only for sending payments.
- Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal.

STAY SAFE, STAY VIGIL!

Chola
Enter a better life

BEWARE OF SMISHING



Smishing, or SMS phishing, is a cybercriminal activity that combines SMS (Short Message Service) with phishing to deceive individuals into divulging sensitive information, such as login credentials, financial data, or personal identification information. This technique typically involves the perpetrator sending a seemingly legitimate and urgent SMS message, often containing links or phone numbers, to prompt the recipient to act immediately.

PROTECT YOURSELF FROM SMS PHISHING:

Don't Click on Links
Avoid clicking on links in unsolicited messages.

Verify the Sender
Double-check the sender's number and legitimacy.

Don't Share Personal Information
Never provide personal details in response to a text message.

Install Security Software
Use security apps that can detect and block malicious messages.

STAY ALERT, STAY SAFE!

Chola
Enter a better life

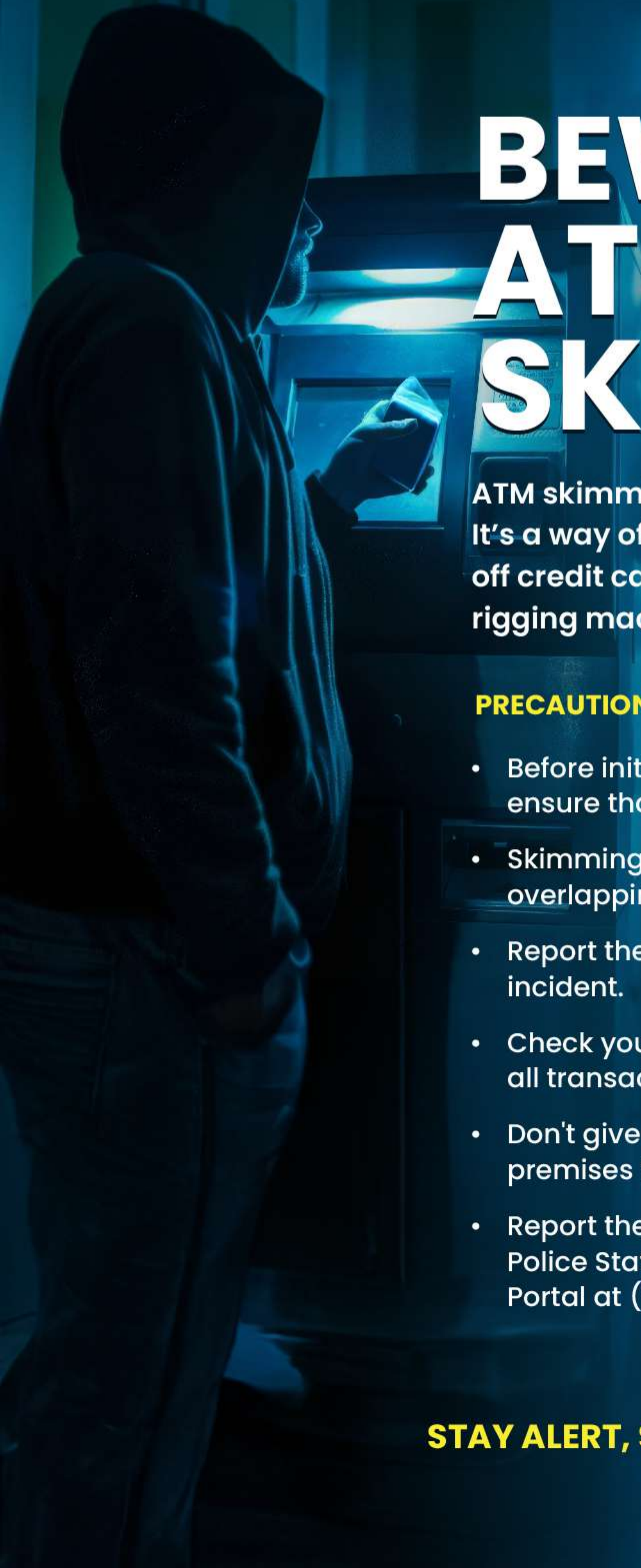
ENSURE SAFE INTERNET SURFING!

Though the internet is a vast ocean of information, it can also be a dangerous place if you're not careful. It's important to stay safe from cybersecurity threats and breaches.

TIPS FOR SAFE INTERNET BROWSING

1. Change passwords at regular intervals.
2. Install antivirus on your devices and install updates whenever available.
3. Always scan unknown Universal Serial Bus (USB) drives/devices before usage.
4. Do not leave your device unlocked.
5. Configure auto-lock of the device after a specified time.
6. Do not install any unknown applications or software on your phone/laptop.
7. Do not store passwords or confidential information on devices.
8. Do not share private information with anyone, particularly unknown persons on social media.
9. Always verify the security of any webpage (https:// - URL with a padlock symbol), more so when an email or SMS link is redirected to such pages.

Chola
Enter a better life



BEWARE OF ATM CARD SKIMMING

ATM skimming is a type of payment card fraud. It's a way of stealing PINs and other information off credit cards, ATM cards, and debit cards by rigging machines with hidden recording devices.

PRECAUTIONS TO STAY AWAY FROM ATM FRAUD:

- Before initiating any transaction in the ATMs, ensure that skimming devices are not present.
- Skimming devices are hidden by fraudsters by overlapping them with the card insertion slot.
- Report the fraud within 3 days of the card cloning incident.
- Check your transaction history frequently to verify all transactions.
- Don't give your ATM card to anyone on the ATM premises to transact on your behalf
- Report the incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at (https://cybercrime.gov.in)

STAY ALERT, STAY SAFE!

Chola
Enter a better life

Don't fall prey to **KYC Frauds!**

Be aware of scammers impersonating bank/NBFC officials and coercing unsuspecting individuals into sharing their KYC details under the guise of urgency

Dos and Don'ts to Prevent Yourself from KYC Frauds

DOs

- In the event of receiving any request for KYC updation, i.e., your data or any document details like PAN, Driving Licence, Aadhar, etc. please contact the financial institution for confirmation/ assistance. Do not divulge this especially if the call seems suspicious!
- Obtain the contact number/ customer care phone number of the bank/ financial institution only through its official website/ sources. Do not entertain any other mode.
- Inform your bank/ financial institution immediately in case of any cyber fraud incident. Enquire with the branch to ascertain available modes/ options for updating KYC details.
- For additional information on the requirements and channels for updation/periodic updation of KYC, please read paragraph 38 of the RBI Master Direction on KYC dated February 25, 2016, as amended from time to time.

DON'Ts

- Do not share account login credentials, card information, PINs, passwords, or OTPs with anyone.
- Do not share KYC documents or copies of KYC documents with unknown or unidentified individuals or organizations.
- Do not share any sensitive data/ information through unverified/ unauthorized websites or applications.
- Do not click on suspicious or unverified links received on mobile or email.

Stay Vigil, Stay Safe!

Chola
Enter a better life

Think Twice Before You Use a Public Wi-Fi

Refrain from using public Wi-Fi, especially while doing financial transactions. It is easy to hack into a laptop or mobile device that is on a public Wi-Fi connection with no protection. Hackers can read your emails, steal passwords and other credentials.

Precautions to stay safe from Public Wi-Fi Frauds

- One should always use a secured Wi-Fi network.
- Report fraud incident to the nearest Cyber Crime Police Station and National Cyber Crime Reporting Portal at https://cybercrime.gov.in
- Use a virtual private network (VPN) solution to ensure your privacy and anonymity are protected when you use public Wi-Fi.

Stay Alert, Stay Safe!