Following tips may be adhered for safe online transactions:

Never disclose your net banking password, One Time Password (OTP), ATM or phone banking PIN, CVV number, expiry date to anyone, even if they claim to be from your bank. Also, never respond to mails asking for above details which seem to have received from your bank.

No bank or its employees will ever call or email you requesting for your net banking password, One Time Password (OTP), ATM or phone banking PIN, CVV number, etc. Such cases should be immediately reported to your bank.

Always use strong passwords and prefer separate ID/password combinations for different accounts to prevent anyone from guessing them.

Periodically change passwords of your online banking accounts.

To make passwords strong, use alphabets in upper case and lower case, numbers and special characters. Do not use passwords such as Jan@2018, admin@123, password@123, your date of birth etc.

Always use virtual keyboards while logging into online banking services. This is specially adhered in-case you need to access net banking facility from a public computer/ cyber café or a shared computer.

Do not make financial transaction over shared public computers or while using public Wi-Fi networks. These computers might have key loggers installed which are designed to capture input from keyboards and could enable fraudsters to steal your username and password.

Always remember to log off from your online banking portal/ website after completing an online transaction with your credit/ debit card.

Always delete the browsing data of your web browser (Internet Explorer, Chrome, Firefox etc.) after completing your online banking activity.

To make passwords strong, use alphabets in upper case and lower case, numbers and special characters. Do not use passwords such as Jan@2018, admin@123, password@123, your date of birth etc.

Always use virtual keyboards while logging into online banking services. This is specially adhered in-case you need to access net banking facility from a public computer/ cyber café or a shared computer.

Do not make financial transaction over shared public computers or while using public Wi-Fi networks. These computers might have key loggers installed which are designed to capture input from keyboards and could enable fraudsters to steal your username and password.

Always delete the browsing data of your web browser (Internet Explorer, Chrome, Firefox etc.) after completing your online banking activity.

Always remember to log off from your online banking portal/ website after completing an online transaction with your credit/ debit card.

Always be sure about the correct address of the bank website and look for the ‘‘lock’’ icon on the browser’s status bar while visiting your bank’s website or conducting an online transaction. Always be sure ‘‘https’’ appears in the website’s address bar before making an online transaction. The ‘‘s’’ stands for ‘‘secure’’ and indicates that the communication with the webpage is encrypted.

Login and view your bank account activity regularly to make sure that there are no unexpected transactions. Report any discrepancies in your account to your bank immediately.

Always be sure about the correct address of the bank website and look for the ‘‘lock’’ icon on the browser’s status bar while visiting your bank’s website or conducting an online transaction.

Always be sure ‘‘https’’ appears in the website’s address bar before making an online transaction. The ‘‘s’’ stands for ‘‘secure’’ and indicates that the communication with the webpage is encrypted.

It is easy for cyber criminals to send convincing emails which appear to be from your bank. Don’t click on the links provided in such emails even if they look genuine. They could lead you to malicious websites.

Keep your bank’s customer care number handy so that you can report any suspicious or unauthorized transactions on your account immediately.

Keep an eye on the people around you while transacting at an ATM. Make sure that no one is standing too close to you while you transact at an ATM.

Always review transaction alert received on your registered mobile number and ensure that your transaction is billed according to your purchase.

Register your personal phone number with your bank and subscribe to mobile notifications. These notifications will alert you quickly of any suspicious transaction and the unsuccessful login attempts to your netbanking account.

Check for latest updates of your Smartphones operating system if you are using your mobile phone for online banking. Do install an antivirus as well and keep it up-to date by enabling the automatic update feature.

Fraudsters may call your family members posing as hospital staff and may request for money transfer saying that you have met an accident and you are in urgent need of money. This could be a spam. Before entertaining any such request, contact your family member to confirm their whereabouts and check authenticity of the phone call.

Always ignore an advertisement if it claims that you can earn money with little or no work or you can make money on an investment with little or no risk. It could be a scam. These offers seem, too good to be true, and you may end up losing money.

Always verify and install authentic e-wallet apps directly from the app store on your smartphone. Do not follow links shared over email, SMS or social media to install e-wallet apps.

Do not save your card or bank account details in your e-wallet as it increases the risk of theft or fraudulent transactions in case of a security breach.

Always type the information in online forms and not use the auto-fill option on your web-browser to fill your online forms they may store your personal information such as card number, CVV number, bank account number etc.