BANK

CYBER DOST

SECURE ONLINE
Financial services!

Be
Cautious...

With the growth of information and communication technology, the structure and nature of financial services delivery has also changed. Online banking or internet banking has emerged as a new and convenient way for using financial services like funds transfer, viewing account statement, bill payment, use of e-wallets etc.

An upsurge in the use of devices connected with the internet and the convenience of online financial services has increased the risk of our hard-earned money being duped by cybercriminals of our hard-earned money.

Follow us on Twitter Handle @*CyberDost* to get cyber safety tips
National Cyber Crime Reporting Portal
www.cybercrime.gov.in

Hello....
May I have your
Account details
Sir !!!

Bank Employee

B A N K

Card

1234 5678
01/11
CARD HOLDER

CVV

Expiry date
of card

CVV

ATM
passwords

Never
Disclose

CYBER
C D
DOST

Following tips may be adhered
for safe online transactions:

1. 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.

2. 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.

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

4. Periodically change passwords of your online banking accounts.

Follow us on Twitter Handle **@CyberDost** to get cyber safety tips
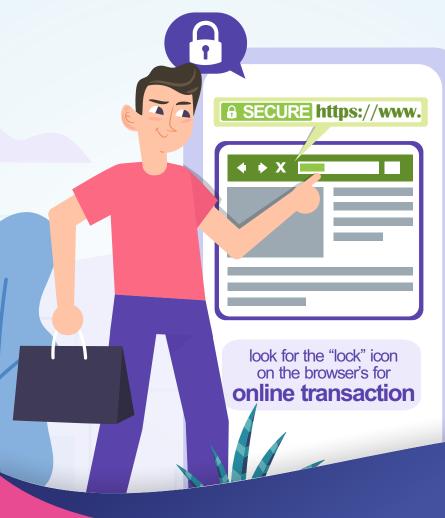**National Cyber Crime Reporting Portal**
www.cybercrime.gov.in

5. 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.

6. 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.

7. 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.

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

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

Follow us on Twitter Handle *@CyberDost* to get cyber safety tips
National Cyber Crime Reporting Portal
www.cybercrime.gov.in

use passwords such as Jan@2018, admin@123

5. 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.

6. 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.

7. 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.

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

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

look for the "lock" icon
on the browser's for
online transaction

10. 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.

11. 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.

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

13. 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.

Follow us on Twitter Handle **@CyberDost** to get cyber safety tips
National Cyber Crime Reporting Portal
www.cybercrime.gov.in

14. Whenever you receive a credit/ debit card from the bank, make sure the letter is not damaged and it is sealed properly. In-case, there are any signs of tampering with the package, please notify your bank immediately.

15. Make sure to change the PIN of credit/ debit card after receiving a new card from your bank. The PIN can be changed online by visiting your bank's website or at your nearest ATM machine.

16. Always ensure that credit or debit card swipes at point of sale are done in your presence to avoid cloning/unauthorized copying of your card information. Do not let the sales person take your card away to swipe for the transaction.

17. Take extra precaution while typing your password/PIN so that no one sees it. Try to cover the key-pad with your other hand while you type your PIN to avoid the number being picked up by someone monitoring CCTV footage.

Follow us on Twitter Handle *@CyberDost* to get cyber safety tips
National Cyber Crime Reporting Portal
www.cybercrime.gov.in

BANK

NOTIFICATION

ATM

CYBER DOST

18. 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 net-banking account.

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

20. 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.

21. It is necessary that you keep your PIN secret and close your transaction completelybefore walking away from the ATM machine. If there is anything suspicious, cancel your transaction and walk away immediately.

Follow us on Twitter Handle *@CyberDost* to get cyber safety tips
National Cyber Crime Reporting Portal
www.cybercrime.gov.in

22. Enable international transaction option on your credit card only when you are travelling abroad. Always ensure to disable international transaction option on your card upon return to your country.

23. 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.

24. 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.

25. 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.

Follow us on Twitter Handle *@CyberDost* to get cyber safety tips
National Cyber Crime Reporting Portal
www.cybercrime.gov.in

गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS

50% OFF

SHOP NOW

50% OFF

BUY OUT

CYBER DOST

26. Always use familiar websites for online shopping rather than shopping by searching products on search engines. Search results can be misleading and may lead to malicious websites.

27. Avoid using third-party extensions, plugins or add-ons for your web browser as it may secretly track your activity and steal your personal details.

28. 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.

29. 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.

30. 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.

Follow us on Twitter Handle *@CyberDost* to get cyber safety tips
National Cyber Crime Reporting Portal
www.cybercrime.gov.in

About Us

An initiative of Government of India to facilitate victims/complainants to report all types of cybercrime complaints online.Complaints reported National Cyber Crime Reporting Portal are dealt by respective police authorities of States/ UTs based on the information provided by the complainants.

If you want to report something other than Cybercrime cases or in case of an emergency please contact your local police by dialing 100.

National Cyber Crime Reporting Portal

www.cybercrime.gov.in

@CyberDost

Follow us on Twitter Handle **@CyberDost** to get cyber safety tips
National Cyber Crime Reporting Portal
www.cybercrime.gov.in