Digital Transactions

CAREFUL WHAT YOU CLICK!

CAG
Citizen consumer and civic Action Group

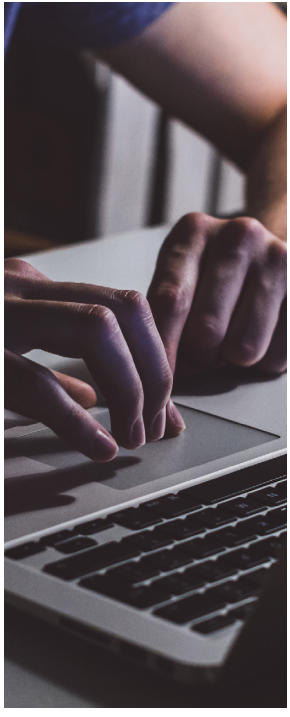
WCRD, 2022

The age of the internet

With the dawn of the internet, how banks and other financial institutions offer their services to consumers has undergone immense changes. Online banking, also known as internet banking, has become the quick and efficient way to access financial services such as money transfers, viewing account statements, bill payment, and the usage of e-wallets. But along with this convenience have come the cyber criminals.

Each week seems to bring in a newer and more cleverly disguised scam to make us part with our hard-earned money.

Know Your Terms



DIGITAL FINANCE

Using the internet to access financial services.

E-WALLETS

E-wallet is a digital wallet on an application (app) where money from the bank account can be transferred and stored to make purchase/transaction easy.

URL

URLs (Uniform Resource Locators) is the internet address that appears in the search bar.

Beware!

of fraudulent calls/messages/emails

1) Fraudsters may call/message/e-mail your family members posing as someone known to you or as calling on official business and request money transfers. Look out for alarming claims (like a family member is unwell / has been in an accident and is in need of immediate assistance). It's possible that this is a spam message. Before agreeing to any such request, check in with your family member to confirm their whereabouts and the call's validity.

2) Even if they pretend to be from your bank, never give out your online banking password, One Time Password (OTP), ATM or mobile banking PIN, CVV number, or expiration date. Remember that no bank or its staff will ever call or email you to ask for these details.

3) Never reply to emails claiming to be from your bank and requesting the above information. Such instances should be notified to your bank right away.

Don't fall for phishing

Disregard any advertisement you may get over email / SMS with claims that you can make money with little or no effort/ risk/ investment. It's possible that it's a trick. These deals appear to be too good to be true, and you may lose money as a result.

You may get emails/ messages with links that may appear to be legitimate. However do not click on the links if it appears unsolicited (ie, from an organisation or a service you have not contacted yourself). They will direct you to harmful websites and/or your data may be compromised.

Netbank safely!

Tips for safe and secure netbanking

When logging into online banking services, always utilise virtual keyboards. This is especially important if you need to use a public computer, a cyber café, or a shared computer to access your net banking account.

Make no financial transactions on public computers or when connected to public Wi-Fi networks. Keyloggers, which are designed to capture input from keyboards and allow fraudsters to obtain your username and password, may be installed on these machines.

After you've finished your online banking activity, always remove the browsing data from your web browser (Internet Explorer, Chrome, Firefox, etc.).

Netbank safely!

...CONTD

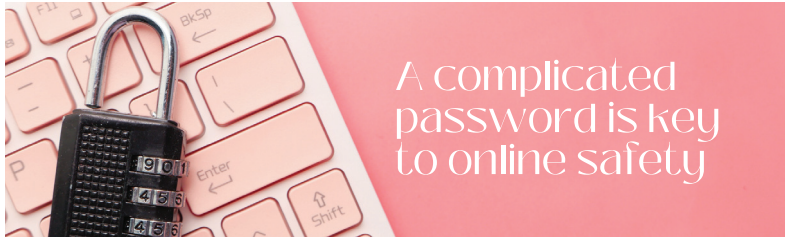
When visiting your bank's website or during an online transaction, make sure you have the correct URL address and look for the "lock" icon in the browser's status bar. Make sure the website's address bar says "https". The "s" stands for "secure," and denotes that the webpage's communication is encrypted. Cyber fraudsters can easily send convincing emails that look to be from your bank.

Create a difficult password

To prevent guessing passwords, always use strong passwords and unique ID/password combinations for various accounts.

Use upper and lower case alphabets, numbers, and special characters in your passwords to make them more secure. Passwords like Jan@2018, admin@123, password@123, or your date of birth should be avoided.

Change the passwords on your online banking accounts on a regular basis.



Never Do These

NEVER DISCLOSE

Expiry date of card
CVV
ATM PIN

NEVER SCAN

Unknown QR code (quick response code) for receiving money.

NEVER SHARE

identification numbers like Aadhar, PAN, drivers licence, ration card, passport, voters card, etc

Netbank safely!

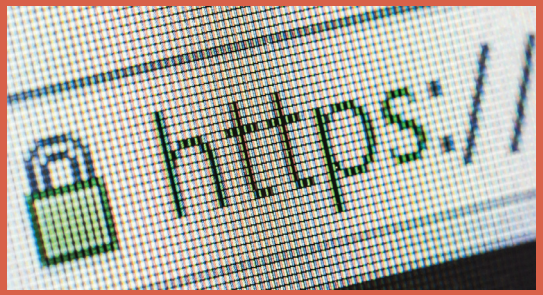
...CONTD

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

Regularly log in and check your bank account activity to ensure that no unexpected transactions have occurred.

Any inconsistencies in your account should be reported to your bank at once.

Always double-check the address and look for the "lock" indicator in the browser's status bar.



Protect Your PIN and CVV

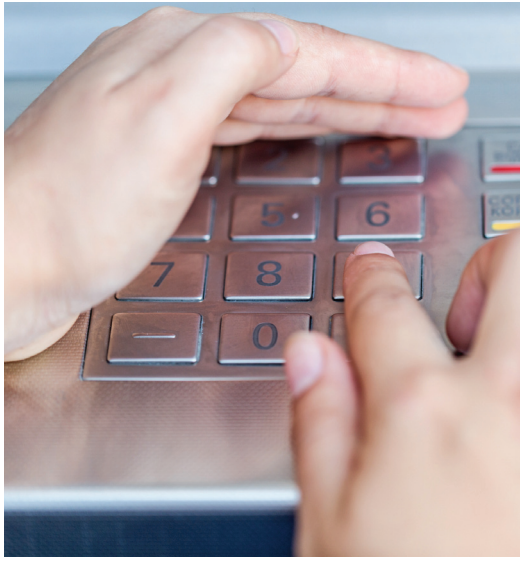
When your bank writes with your credit/debit card and associated information, make sure the envelope has not been tampered with. If it is, contact your bank immediately.

After receiving a new credit/debit card from your bank, make sure you change the PIN. PINs can be changed online at your bank's website or at an ATM machine near you.

To avoid cloning/unauthorised copying of your card information, make sure that credit or debit card swipes are done in your presence at the point of sale. Allowing the salesperson to swipe your card for the purchase is not a good idea.

Only use your credit card for overseas transactions while you are travelling abroad. When you return to your home country, make sure to turn off the international transaction option on your card.

ATM Safety



To ensure that no one sees your password/PIN, take extra precautions when typing it. To avoid the number being picked up by someone watching CCTV footage, try to cover the keypad with your other hand while typing your PIN.

While using an ATM, keep an eye on the individuals surrounding you and make sure no one is standing too near to you.

It is critical that you keep your PIN private and finish your transaction before leaving the ATM machine.

If you see anything strange, cancel your transaction and leave right away.

Avail Bank Services

Subscribe to mobile notifications and register your personal phone number with your bank. These alerts will notify you immediately of any suspicious transactions and failed login attempts to your accout.

Always check the transaction alert sent to your registered mobile number to make sure your transaction is billed correctly.

Update Your Gadgets

If you use your computer (or your smartphone) to conduct online banking, make sure your operating system is up to date.

Install an antivirus program on your device.

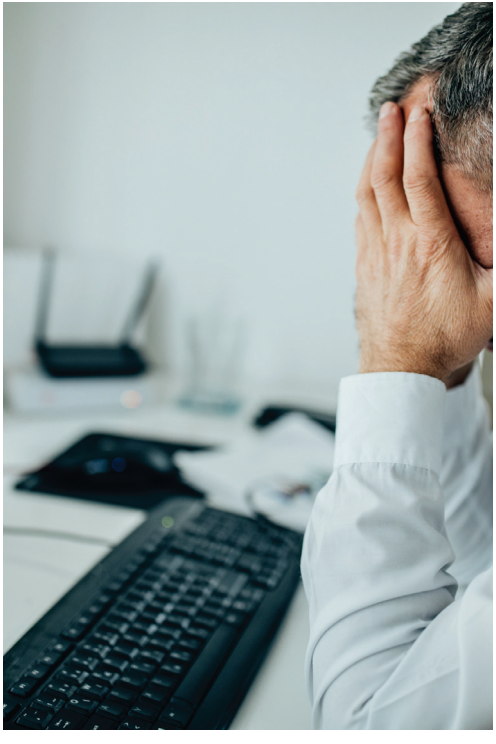
Use the automatic update mechanism to keep it up to date.

Shop Safely

When purchasing online, always visit established websites rather than searching for things on search engines. The results of a search can be deceiving, leading to dangerous websites.

Beware!
Don't go home with more than you bargained for!

So you got it wrong. What now?



ALWAYS

keep the customer service number for your bank ready so you can report any suspicious or unauthorised activity on your account right away.

In order to protect the interests of consumers by limiting their liability in case of unauthorised online transactions, the RBI issued a circular in 2017. Accordingly,

ZERO LIABILITY

in case of loss due to negligence by bank or third party breach and if the customer informs the bank within 3 days.

LIMITED LIABILITY

If the loss is due to customer negligence. The customer will be liable until he reports the unauthorised transaction to the bank. Any loss occurring after the reporting shall be borne by the bank.

In case of a delay in reporting fraudulent transactions (from 4-7 days), the liability of the customer shall be limited to the transaction value or the amount mentioned in table below, whichever is lower

LIABILITY BASED ON BANK'S BOARD APPROVED POLICY

If there is a third party breach and the customer informs the bank after 7 days. Policy details need to be shared with the customer at the opening of the account.

MAXIMUM LIABILITY OF A CUSTOMER

TYPE OF ACCOUNT	MAXIMUM LIABILITY
• BASIC SAVINGS BANK DIRECT ACCOUNTS	5000
• ALL OTHER SB ACCOUNTS • PRE-PAID PAYMENT INSTRUMENTS AND GIFT CARDS • CURRENT/ CASH CREDIT/ OVERDRAFT ACCOUNTS OF MSMES • CURRENT ACCOUNTS/ CASH CREDIT/ OVERDRAFT ACCOUNTS OF INDIVIDUALS WITH ANNUAL AVERAGE BALANCE (DURING 365 DAYS PRECEDING THE INCIDENCE OF FRAUD)/ LIMIT UP TO RS.25 LAKH • CREDIT CARDS WITH LIMIT UP TO RS.5 LAKHS	10,000
• ALL OTHER CURRENT/ CASH CREDIT/ OVERDRAFT ACCOUNTS • CREDIT CARDS WITH LIMIT ABOVE RS.5 LAKH	25,000

CAG
Citizen consumer and civic Action Group

Citizen consumer and civic Action Group
New #246 (Old #277B),
TTK Road (J.J. Road), Alwarpet,
Chennai, Tamil Nadu 600018
India
+91-44-2466 0387
+91-44-2499 4458
Email: helpdesk@cag.org.in

Find us on CAG Chennai