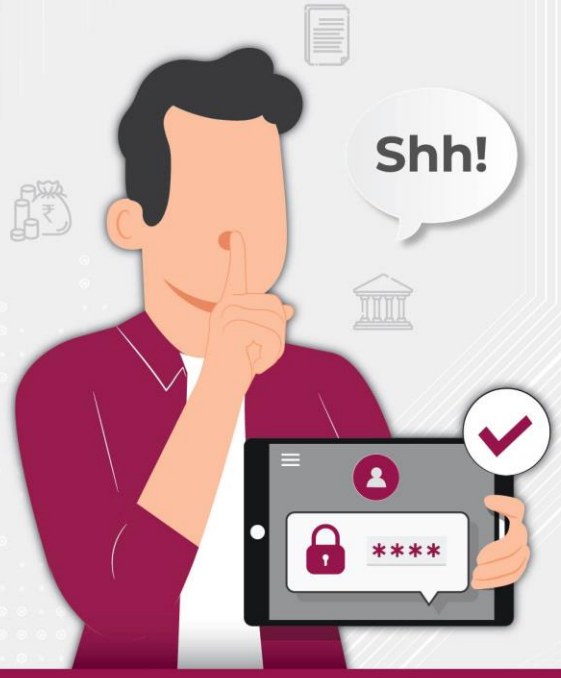
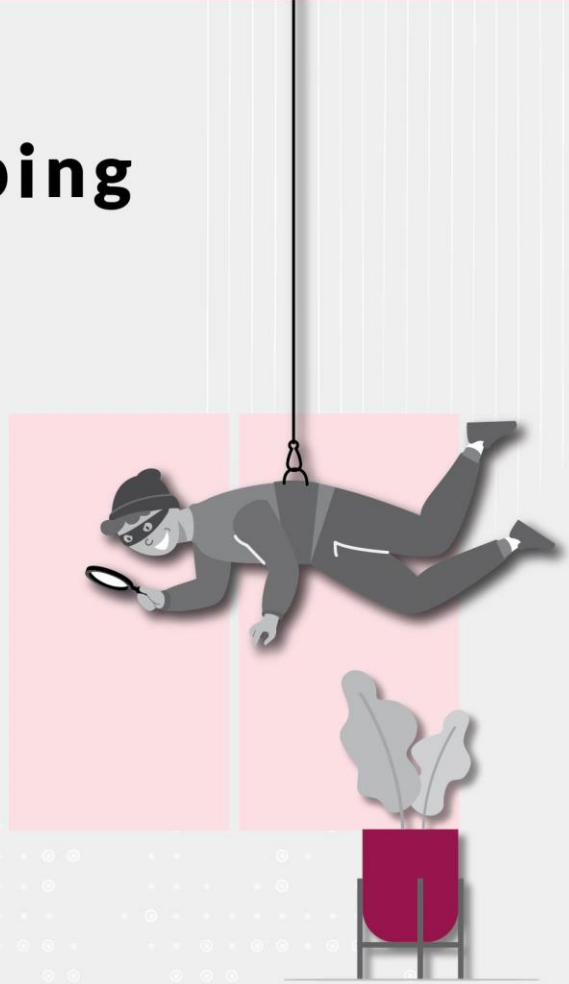
Some secrets are worth keeping

Just like your banking credentials

Presenting

Safe Digital Banking Tips by Axis Bank

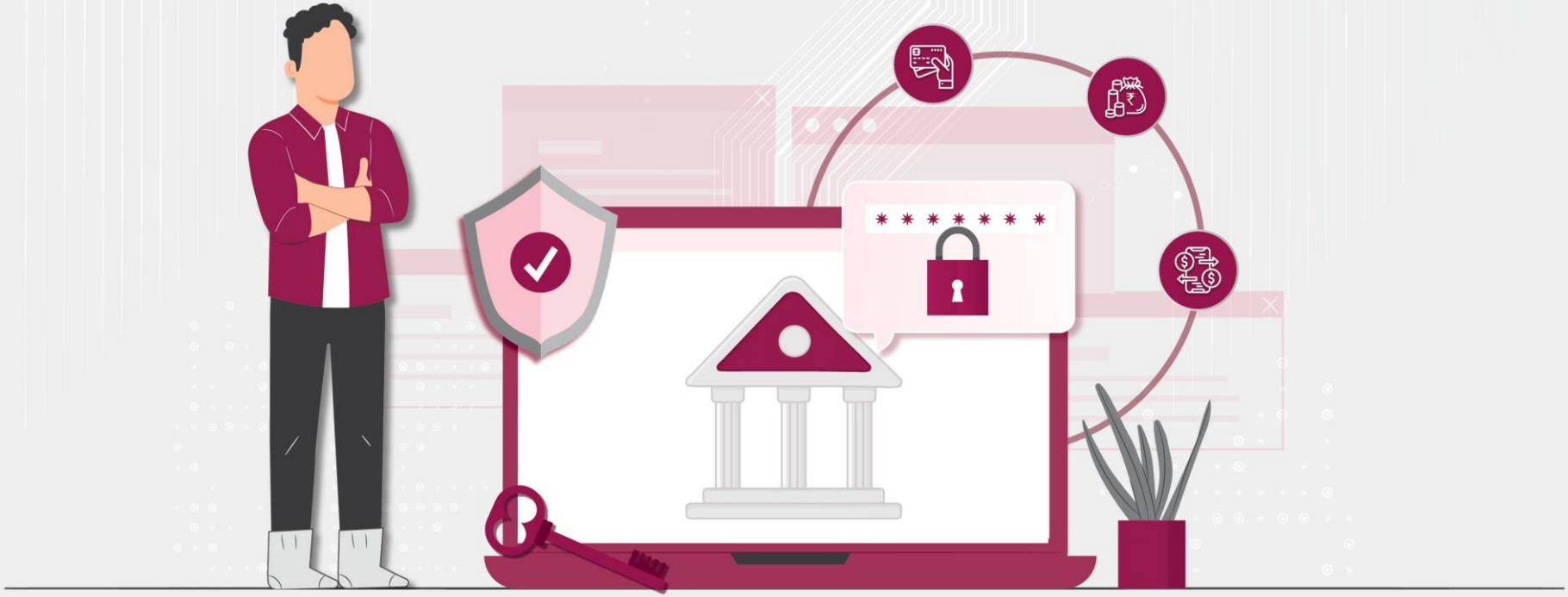




AXIS BANK

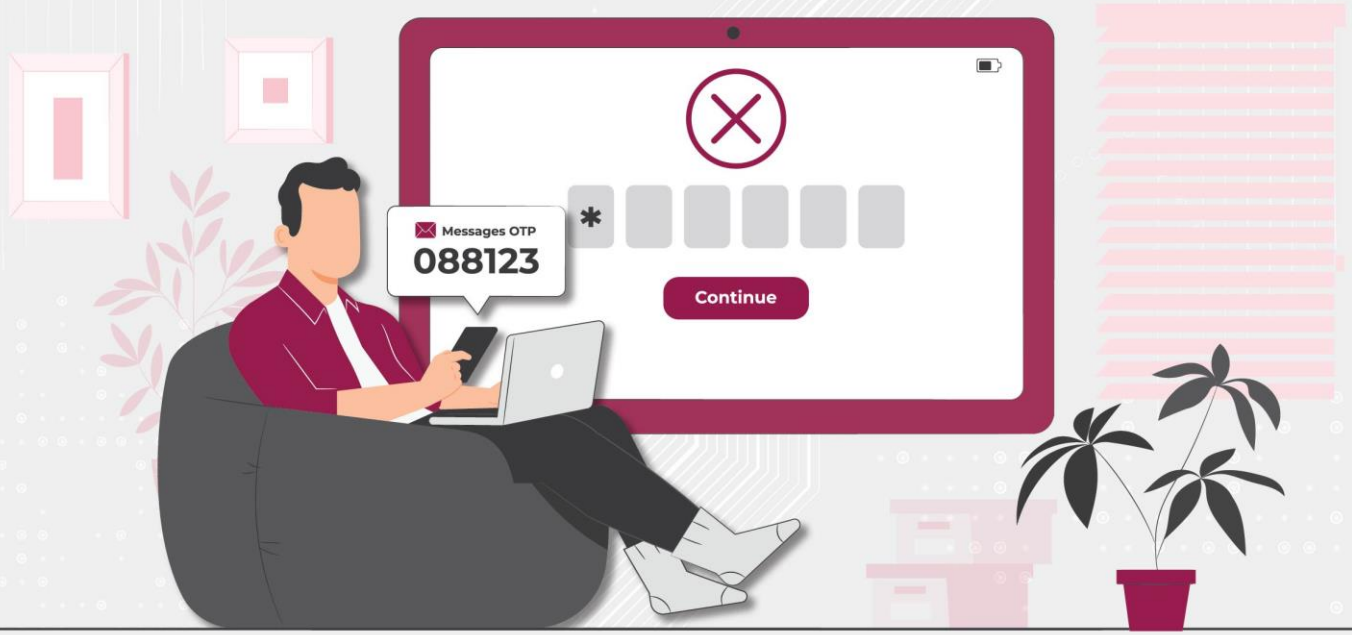
A gist to ways you can be safe from being a victim to fraudsters:

01 Keep a strong password and change it regularly



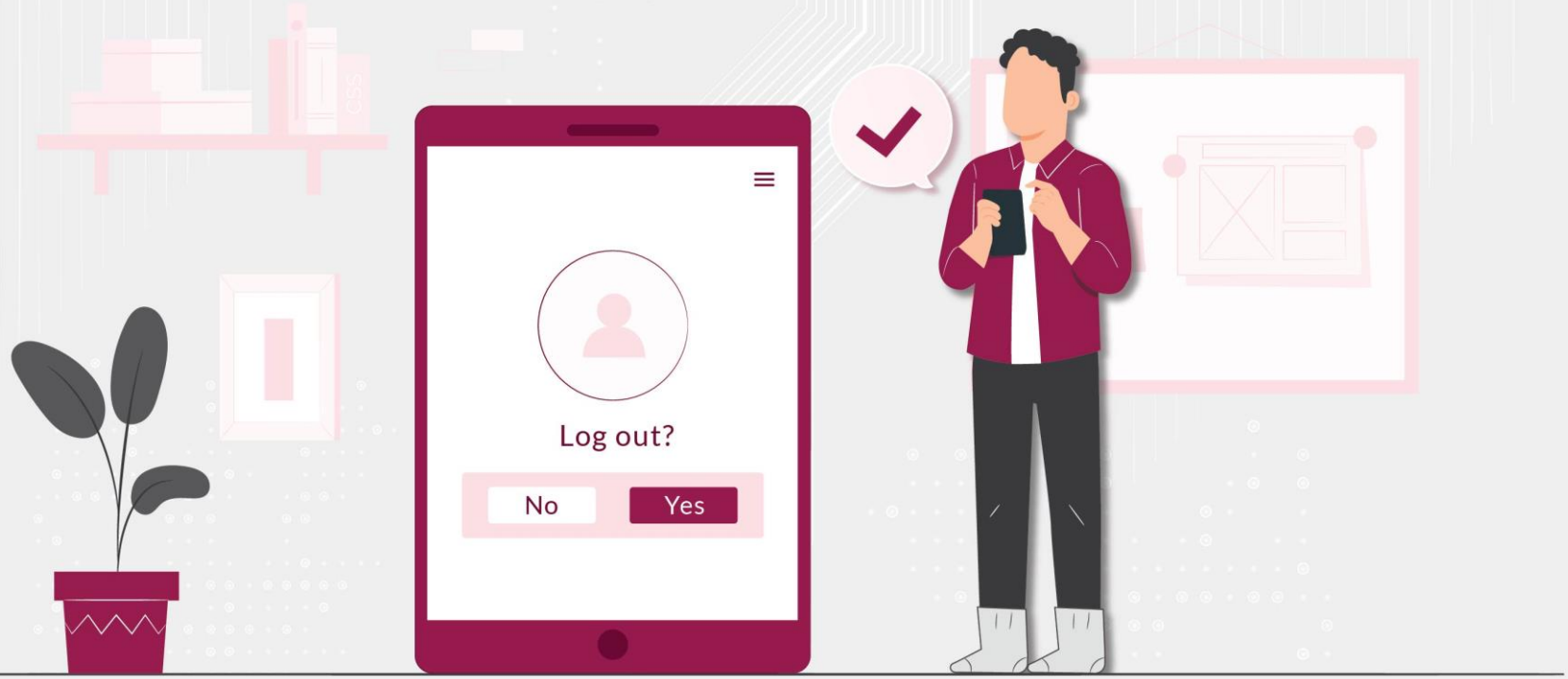
- Just like a bodyguard, your password – the bodyguard to your financials, needs to be strong! Your password should be a good mix of upper and lower-case alphabets, numbers and symbols.
- Make sure to keep changing your passwords at regular intervals.
- Please Note: As there cannot be a single key to different locks, please keep different passwords for all your online accounts.

02 Do not share your details with anyone



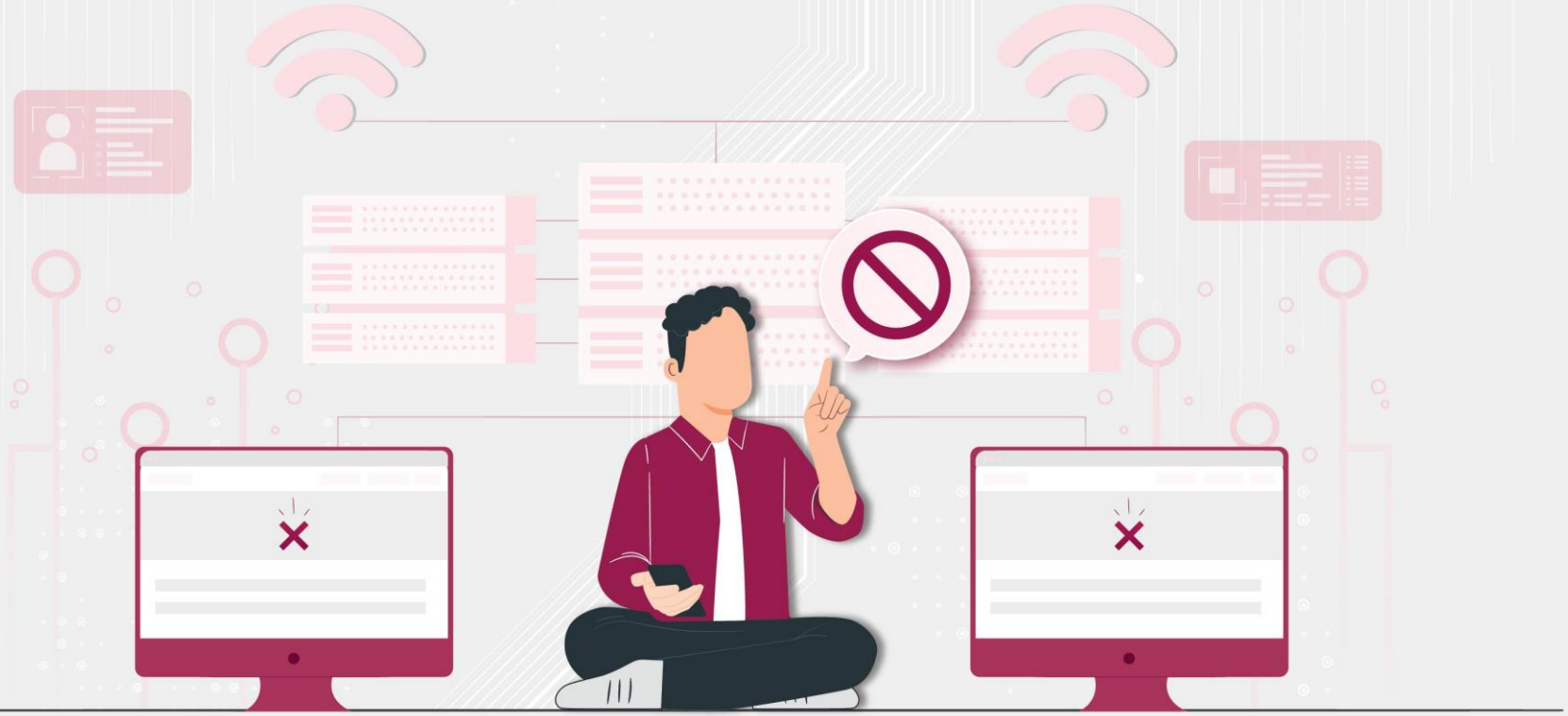
- Your details belong to you and you alone.
- Remember, the Bank does not ask you for any private details pertaining to your account like CVV, OTP, PIN, etc. If anyone calls and asks you these details, do not divulge this information, or any information pertaining to your accounts before confirming the identity of the caller.

03 Always logout from your accounts when ending a digital banking session



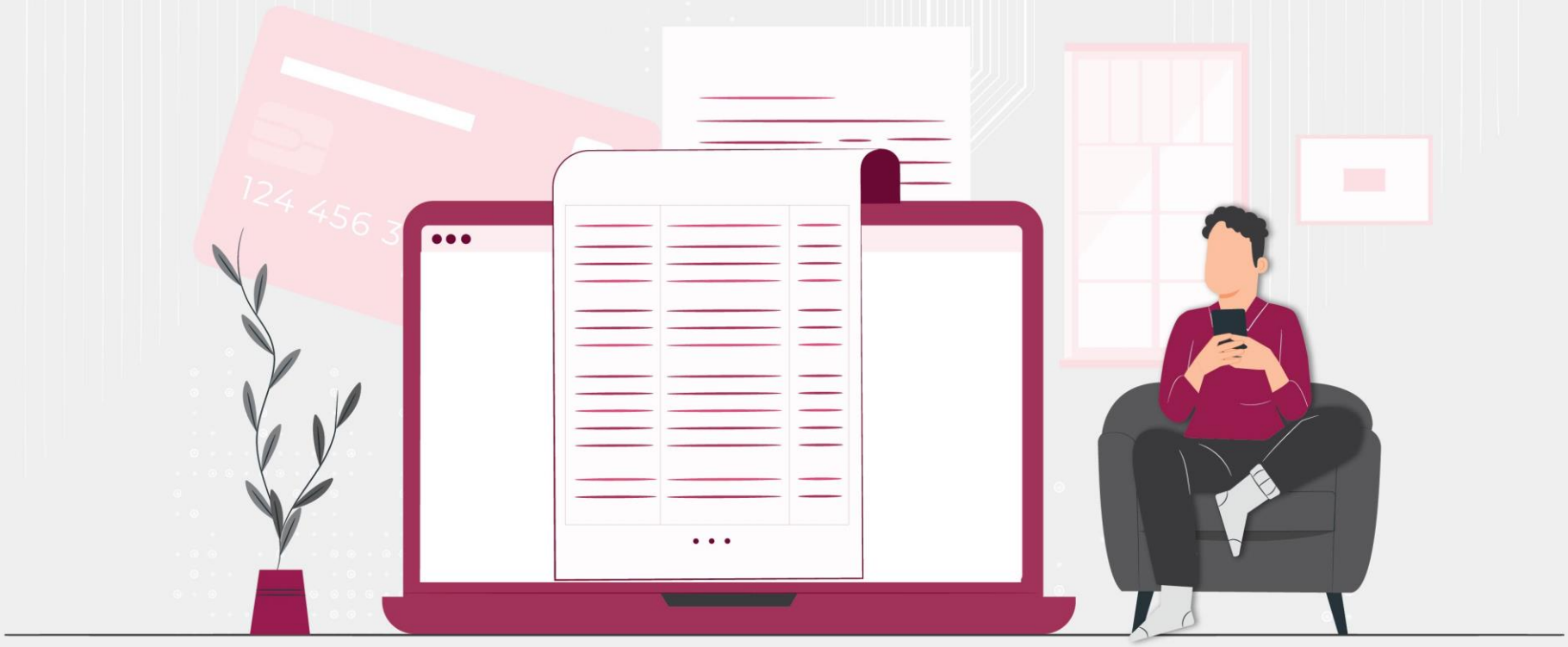
- Don’t forget to lock the doors of your house before leaving home? Similarly, do not leave any digital banking session without logging out of your account.
- This ensures that if your system (Laptop / Desktop) ends up in other hands, your life savings do not come at risk.

04 Avoid using public computers and Wi-Fi connections



- The biggest threat of an open Wi-Fi network is that the hacker can sit in between the end user and the hotspot and can trace all the data without any difficulty.
- Hackers see unsecured connection as an opportunity to introduce malware into your device.
- Usage of public Wi-Fi hotspots for internet or mobile banking and making payments on ecommerce sites should be avoided.

05 Periodically check your Account and Credit Card Statements



- You must check your Bank Account statement and Credit Card statement every month to identify any unauthorised or suspicious transaction.
- If there is some transaction that was not authorized by you, inform your bank immediately.

06 Install an established and reliable anti-virus on your devices

- Install genuine anti-virus and anti-malware software on your computer / mobile and keep it up to date.
- To protect your computer from phishing, malware, and other security threats, always use genuine anti-virus software.
- Anti-virus helps in detecting and removing spyware that can steal your sensitive information.

AXIS BANK

Need to report a fraud?

Click Here

to watch the video on ***How to report a Fraudulent Transaction?***