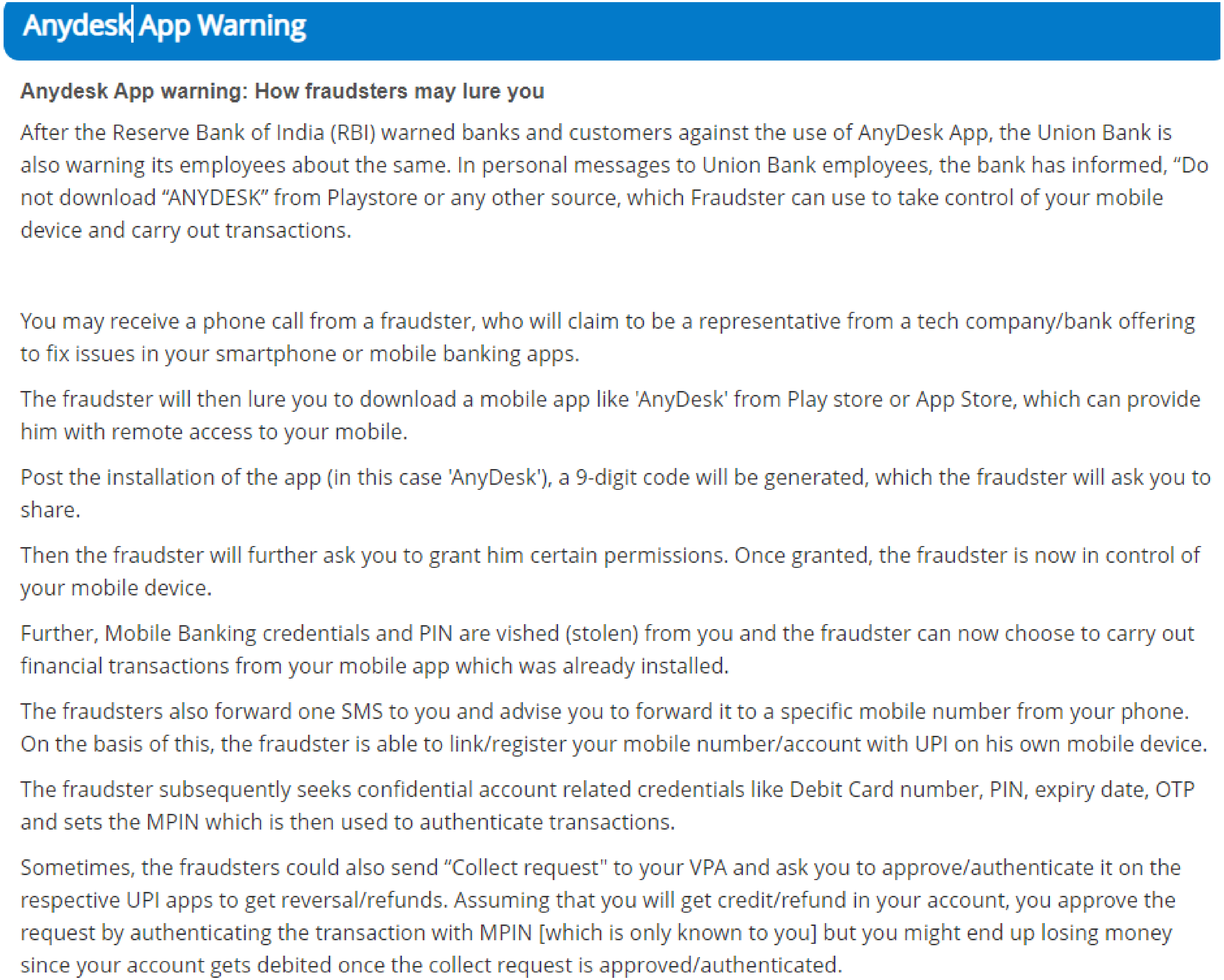
JANATHA SEVA CO-OPERATIVE BANK LTD.,
NO24 , RAJATHA BHAVANA , 1ST MAIN
ROAD,VIJAYANAGARA , BENGALURU-560104

CYBER SECURITY TIPS TO EMPLOYEES

CYBER SECURITY - CYBER SECURITY - CYBER SECURITY - CYBER SECURITY - CYBER SECURITY



Anydesk App Warning

Anydesk App warning: How fraudsters may lure you

After the Reserve Bank of India (RBI) warned banks and customers against the use of AnyDesk App, the Union Bank is also warning its employees about the same. In personal messages to Union Bank employees, the bank has informed, “Do not download “ANYDESK” from Playstore or any other source, which Fraudster can use to take control of your mobile device and carry out transactions.

You may receive a phone call from a fraudster, who will claim to be a representative from a tech company/bank offering to fix issues in your smartphone or mobile banking apps.

The fraudster will then lure you to download a mobile app like 'AnyDesk' from Play store or App Store, which can provide him with remote access to your mobile.

Post the installation of the app (in this case 'AnyDesk'), a 9-digit code will be generated, which the fraudster will ask you to share.

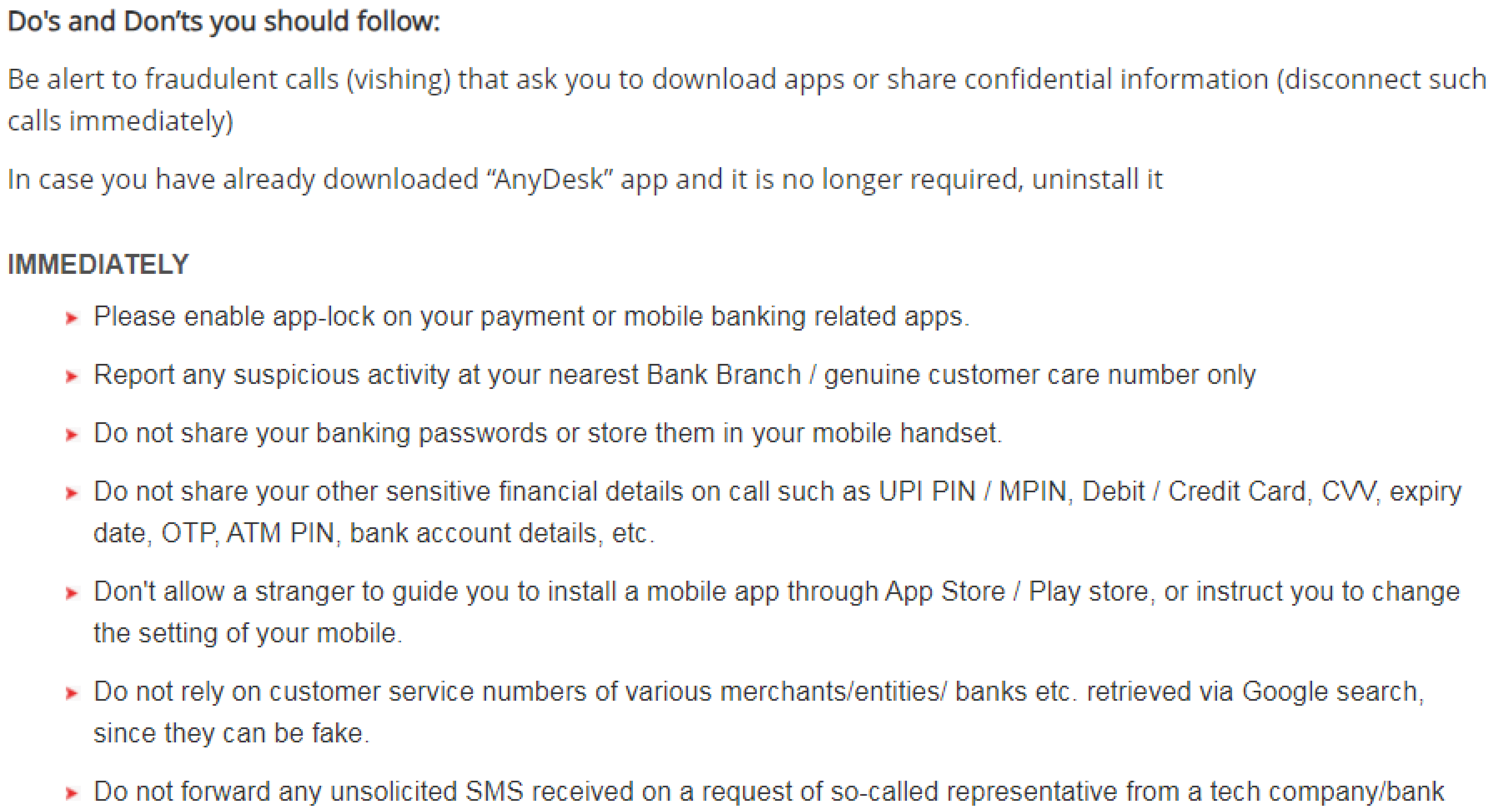
Then the fraudster will further ask you to grant him certain permissions. Once granted, the fraudster is now in control of your mobile device.

Further, Mobile Banking credentials and PIN are vished (stolen) from you and the fraudster can now choose to carry out financial transactions from your mobile app which was already installed.

The fraudsters also forward one SMS to you and advise you to forward it to a specific mobile number from your phone. On the basis of this, the fraudster is able to link/register your mobile number/account with UPI on his own mobile device.

The fraudster subsequently seeks confidential account related credentials like Debit Card number, PIN, expiry date, OTP and sets the MPIN which is then used to authenticate transactions.

Sometimes, the fraudsters could also send “Collect request" to your VPA and ask you to approve/authenticate it on the respective UPI apps to get reversal/refunds. Assuming that you will get credit/refund in your account, you approve the request by authenticating the transaction with MPIN [which is only known to you] but you might end up losing money since your account gets debited once the collect request is approved/authenticated.



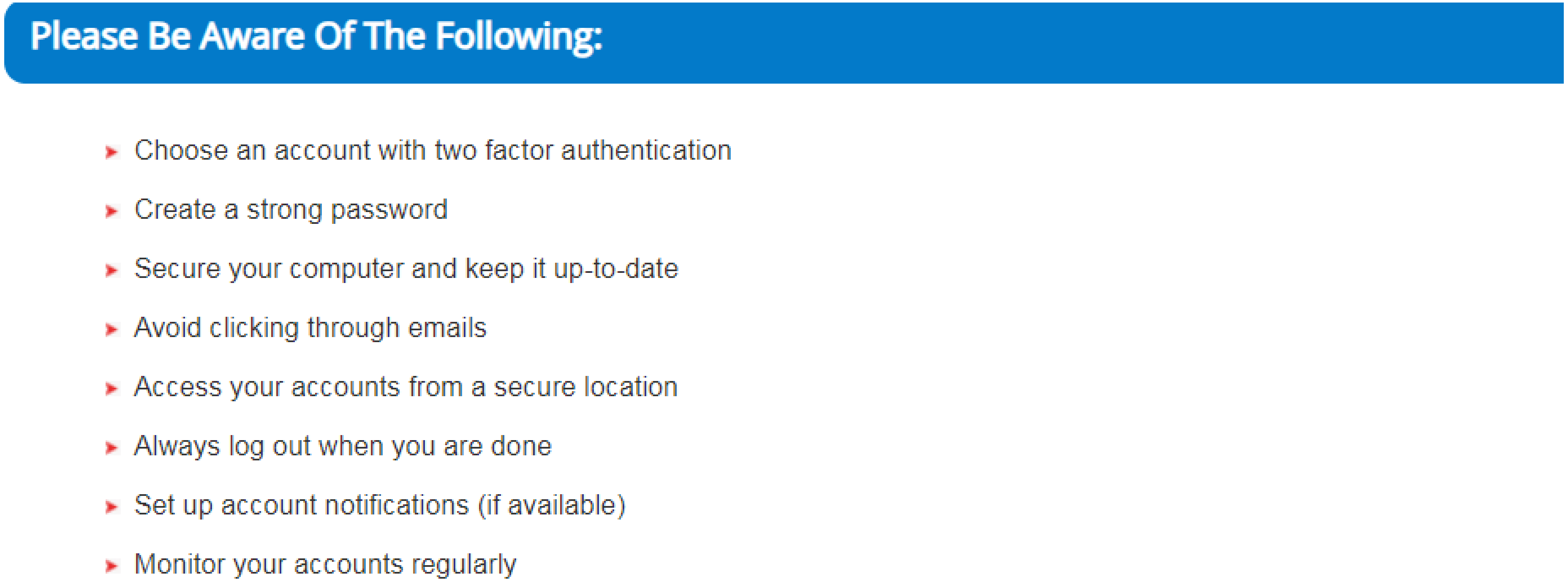
Do's and Don'ts you should follow:

Be alert to fraudulent calls (vishing) that ask you to download apps or share confidential information (disconnect such calls immediately)

In case you have already downloaded "AnyDesk" app and it is no longer required, uninstall it

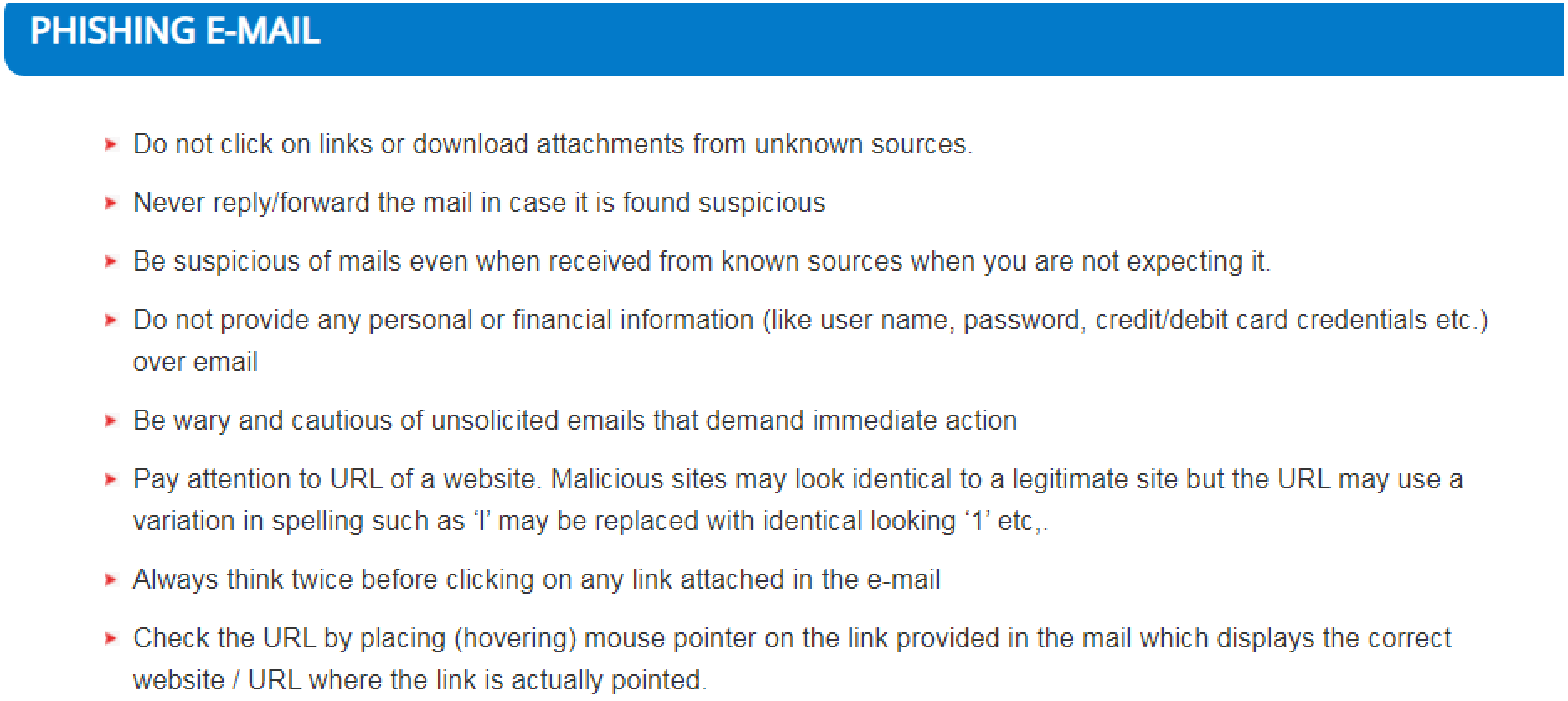
IMMEDIATELY

- Please enable app-lock on your payment or mobile banking related apps.
- Report any suspicious activity at your nearest Bank Branch / genuine customer care number only
- Do not share your banking passwords or store them in your mobile handset.
- Do not share your other sensitive financial details on call such as UPI PIN / MPIN, Debit / Credit Card, CVV, expiry date, OTP, ATM PIN, bank account details, etc.
- Don't allow a stranger to guide you to install a mobile app through App Store / Play store, or instruct you to change the setting of your mobile.
- Do not rely on customer service numbers of various merchants/entities/ banks etc. retrieved via Google search, since they can be fake.
- Do not forward any unsolicited SMS received on a request of so-called representative from a tech company/bank



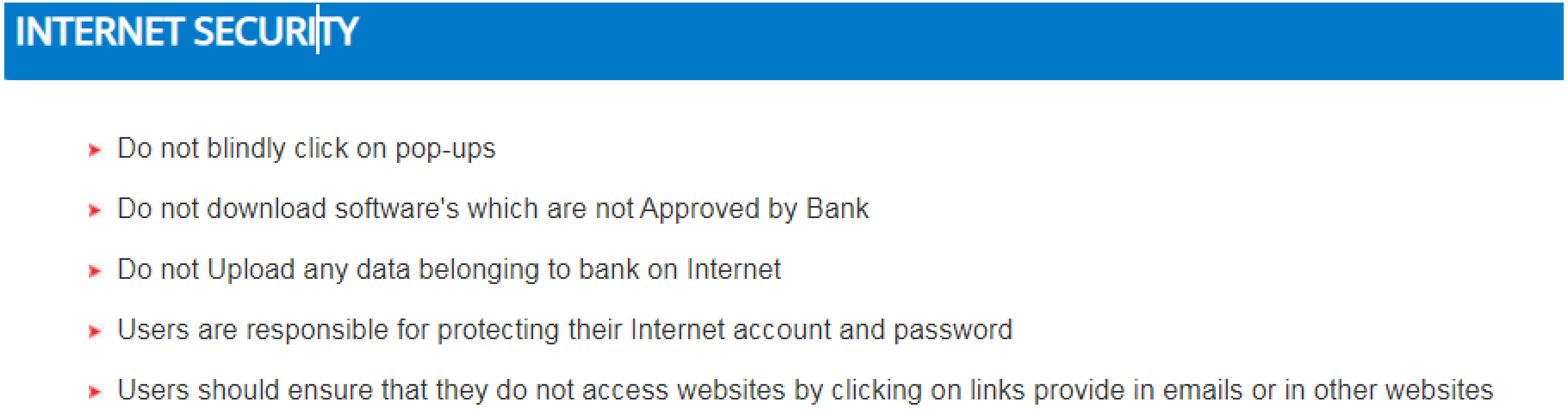
Please Be Aware Of The Following:

- Choose an account with two factor authentication
- Create a strong password
- Secure your computer and keep it up-to-date
- Avoid clicking through emails
- Access your accounts from a secure location
- Always log out when you are done
- Set up account notifications (if available)
- Monitor your accounts regularly



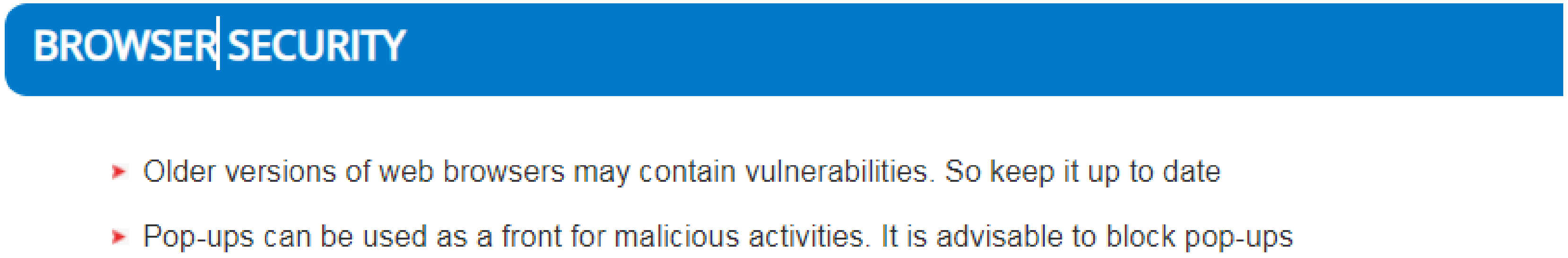
PHISHING E-MAIL

- Do not click on links or download attachments from unknown sources.
- Never reply/forward the mail in case it is found suspicious
- Be suspicious of mails even when received from known sources when you are not expecting it.
- Do not provide any personal or financial information (like user name, password, credit/debit card credentials etc.) over email
- Be wary and cautious of unsolicited emails that demand immediate action
- Pay attention to URL of a website. Malicious sites may look identical to a legitimate site but the URL may use a variation in spelling such as ‘l’ may be replaced with identical looking ‘1’ etc,.
- Always think twice before clicking on any link attached in the e-mail
- Check the URL by placing (hovering) mouse pointer on the link provided in the mail which displays the correct website / URL where the link is actually pointed.



INTERNET SECURITY

- Do not blindly click on pop-ups
- Do not download software's which are not Approved by Bank
- Do not Upload any data belonging to bank on Internet
- Users are responsible for protecting their Internet account and password
- Users should ensure that they do not access websites by clicking on links provide in emails or in other websites

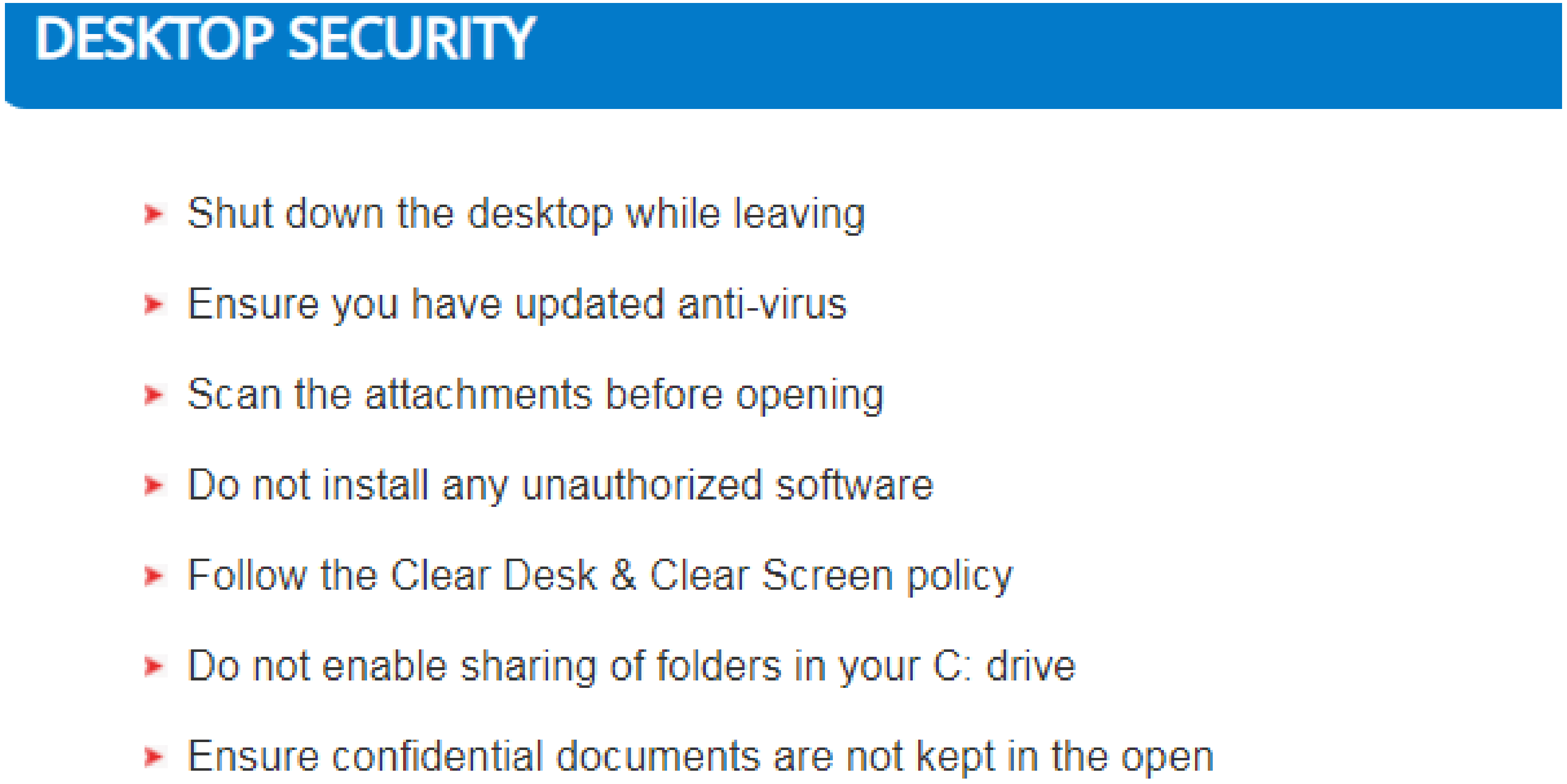


BROWSER SECURITY

- Older versions of web browsers may contain vulnerabilities. So keep it up to date
- Pop-ups can be used as a front for malicious activities. It is advisable to block pop-ups

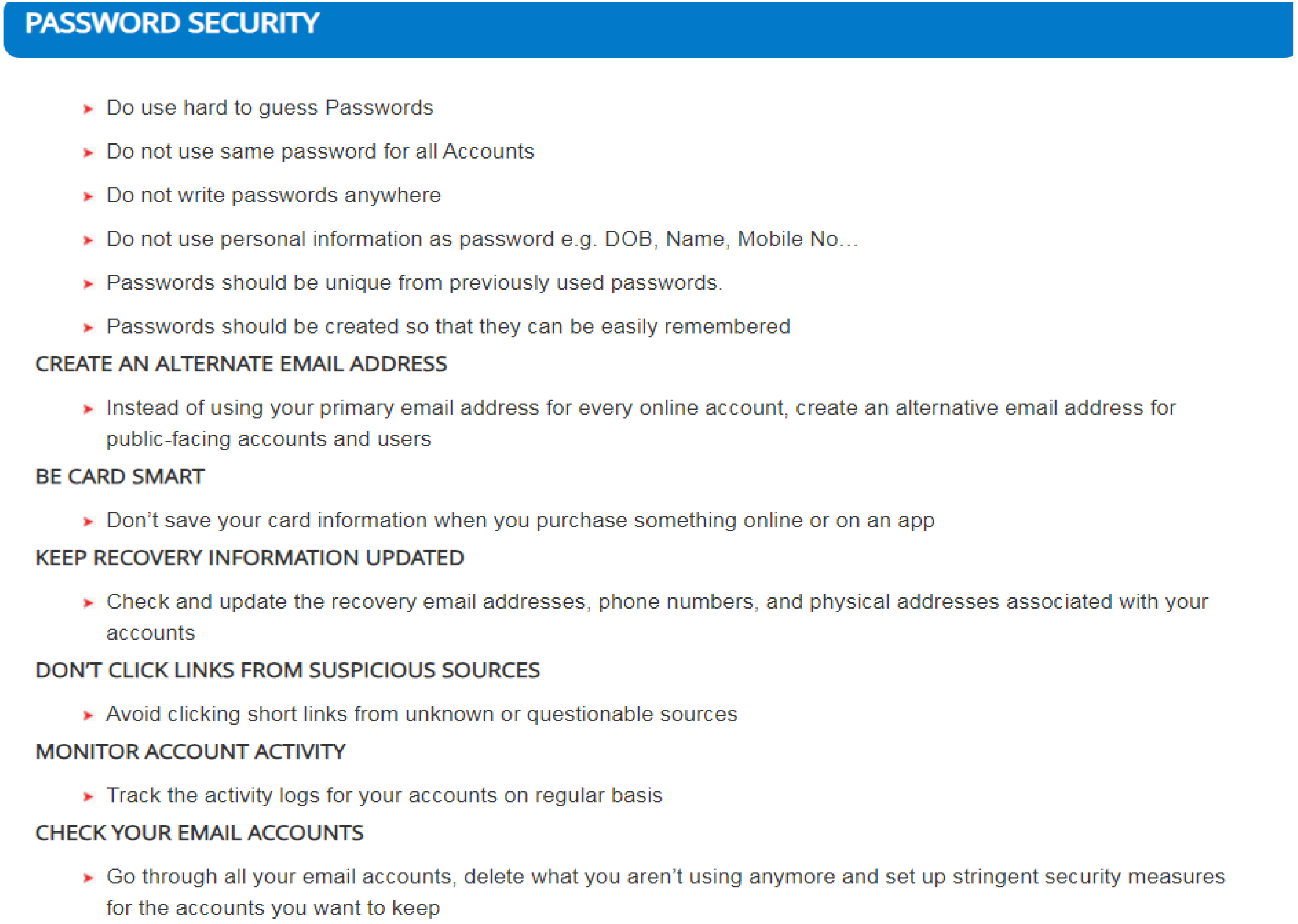
WI-FI SECURITY

- Don’t enable Auto-Connect to open Wi-Fi Networks
- Don’t leave broadband connectivity open when it is not utilized
- Don’t connect to unknown Wi-Fi network at office or public place
- Change Default Administrator Passwords and User names



DESKTOP SECURITY

- Shut down the desktop while leaving
- Ensure you have updated anti-virus
- Scan the attachments before opening
- Do not install any unauthorized software
- Follow the Clear Desk & Clear Screen policy
- Do not enable sharing of folders in your C: drive
- Ensure confidential documents are not kept in the open



PASSWORD SECURITY

- Do use hard to guess Passwords
- Do not use same password for all Accounts
- Do not write passwords anywhere
- Do not use personal information as password e.g. DOB, Name, Mobile No…
- Passwords should be unique from previously used passwords.
- Passwords should be created so that they can be easily remembered

CREATE AN ALTERNATE EMAIL ADDRESS

- Instead of using your primary email address for every online account, create an alternative email address for public-facing accounts and users

BE CARD SMART

- Don’t save your card information when you purchase something online or on an app

KEEP RECOVERY INFORMATION UPDATED

- Check and update the recovery email addresses, phone numbers, and physical addresses associated with your accounts

DON’T CLICK LINKS FROM SUSPICIOUS SOURCES

- Avoid clicking short links from unknown or questionable sources

MONITOR ACCOUNT ACTIVITY

- Track the activity logs for your accounts on regular basis

CHECK YOUR EMAIL ACCOUNTS

- Go through all your email accounts, delete what you aren’t using anymore and set up stringent security measures for the accounts you want to keep for the accounts you want to keep

BACK UP YOUR DATA

- Back up your data frequently and in multiple locations to protect your critical information

UPDATE YOUR SOFTWARE

- Make sure any software you use on your personal computer is updated regularly.

DISABLE AUTO-CONNECT

- Make sure your Wi-Fi auto discovery functions and Bluetooth is off when you are travelling or in public.

CONTROL MOBILE APP ACCESS

- Get into the habit of not installing any app unless they come from the official app store

REVIEW YOUR PASSWORDS PERIODICALLY

- Make sure they are strong and contain an assortment of characters and change them regularly.

REGULARLY UPDATE YOUR BROWSER

- Make sure you're using the latest versions of your Internet browsers and any related plug-in.

PROTECT YOUR SYSTEMS

- Take care that antivirus, firewall, and ad-blocker solutions are patched and updated on regular basis

SET UP 2FA (TWO FACTOR AUTHENTICATION)

- Make sure to link your accounts to your phone number and/or emails address to verify your identity when you sign in

Thank You