ENABLE MULTI-FACTOR AUTHENTICATION

Authentication

- Authentication is the process of verifying the identity of user.
- The most common technique to authenticate a user is to use username and passwords

Two factor Authentication

- It is an approach to authentication which requires the presentation of two different kinds of evidence that someone is who they say they are.

USE STRONG PASSWORDS

Passwords should be:

- At least 8 characters long
- Contain at least one number
- Contain at least one capital letter
- Contain at least one symbol (like #, %, &)
- Not be a real word, name or anything that would be relatively easy to guess

Change your passwords if & when:

- There has been any type of security breach on the site or your system
- You have lost a device that has the password stored
- Someone else gets hold of your password

- And even if none of this happens, change them every few months

Use a very strong passwords for:

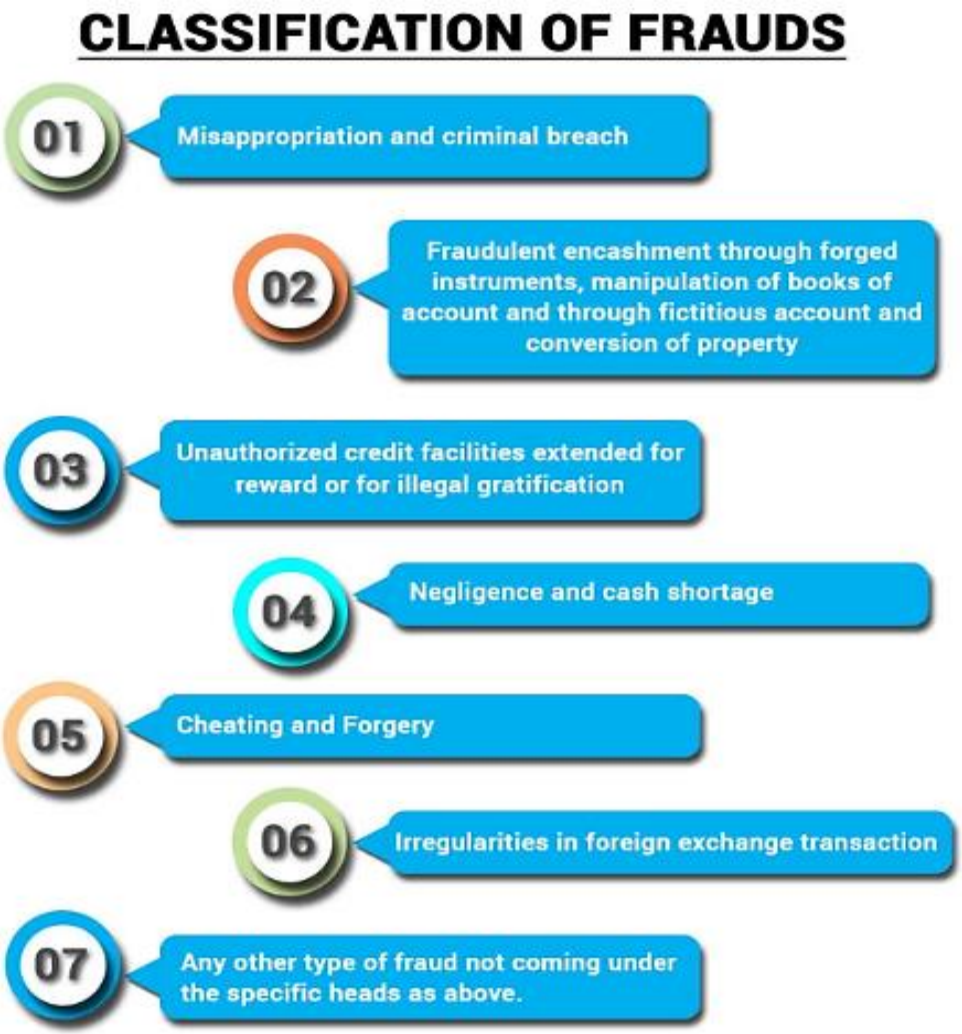
- Email:
  - Many sites will send your password to your email address so it's important that it be very secure
- Social network sites
  - Your reputation can be affected if someone posts negative and abuse material in your name
- Banking
  - Pretty much goes without saying that you want a strong lock on your bank account
- E-commerce sites
  - Don't let anyone go on a shopping free with your money

RECOGNIZE AND REPORT PHISHING/VISHING/SMISHING

- It is always good advice to be wary of unexpected emails. If you were not anticipating a message or attachment, you should review the email very carefully. Most phishing emails are designed to send you to a bad website to steal your username and password or to visit a hacked website. However, attackers may also entice you to open an attachment. It is important to not open questionable attachments. Also, be on the lookout for common executable file attachments such as; .exe, .com, .jar, .msi, .bat, .scr and more. These attachments are known for being malicious and containing malware. Documents may also have malicious code embedded within them that take advantage of a weakness on your system such as unpatched software. These attachments may install ransomware or other malicious programs on your computer. Mistakes are bound to happen, and eventually, you may fall for one of these attacks. It is vital that you know your organizations' process for reporting this type of incident, as time is critical to stop the spread and further infection of machines.

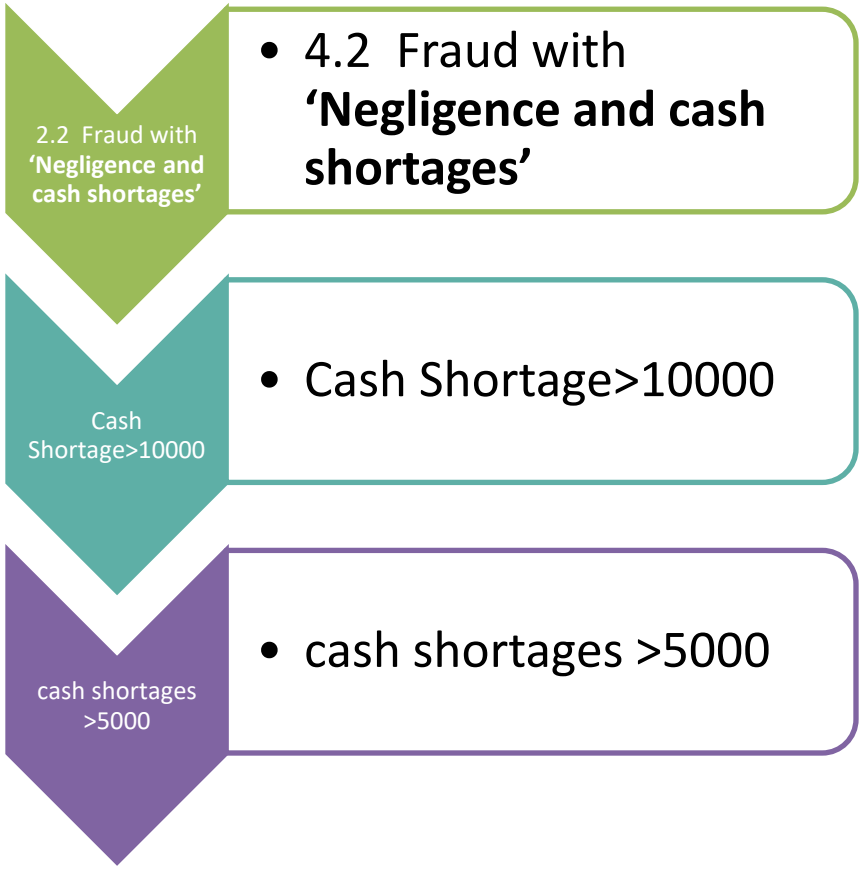
CLASSIFICATION OF FRAUDS

- 4.1 In order to have uniformity in reporting, frauds have been classified as under, based mainly on the provisions of the Indian Penal Code (IPC)

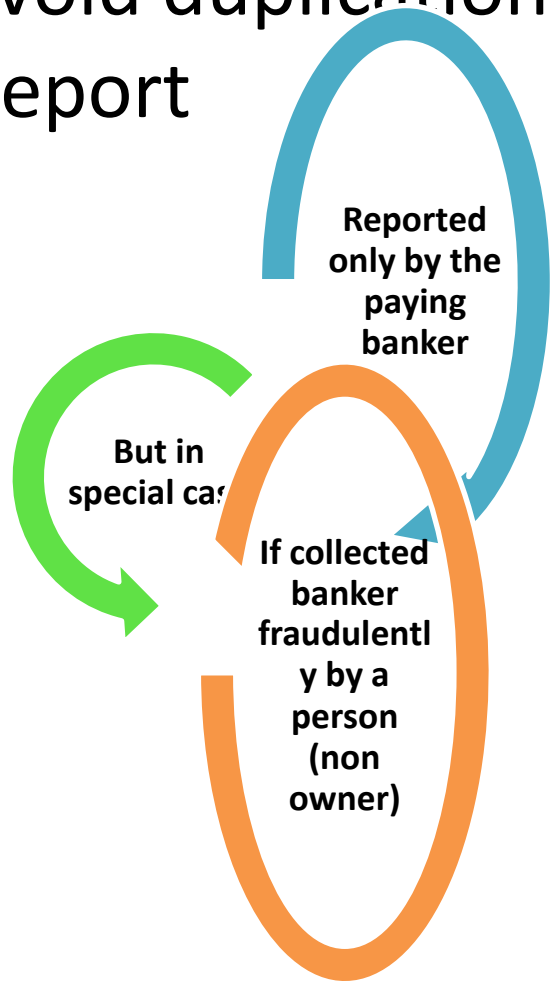


Classification of frauds

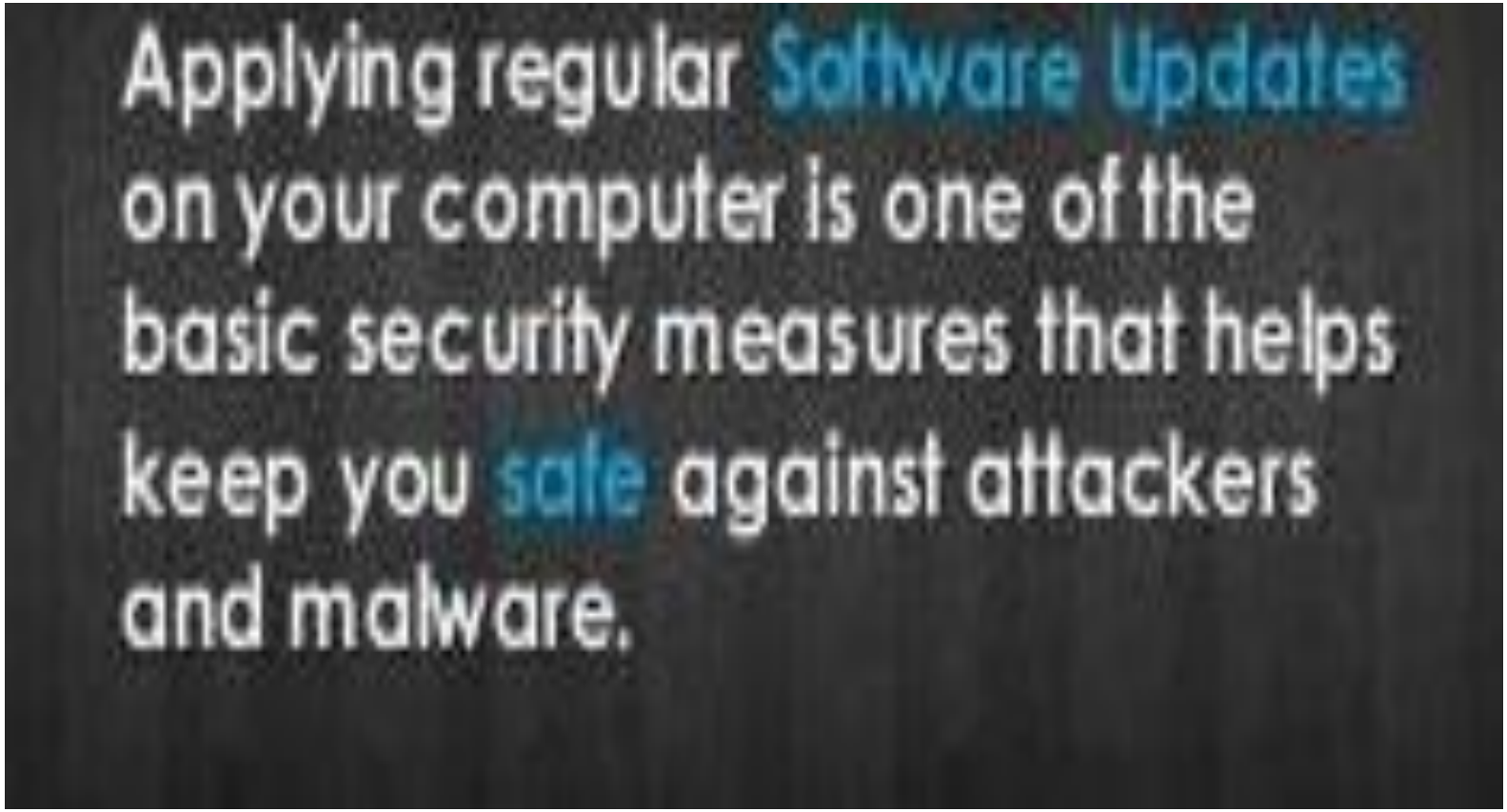
- 4.2 This will be treated as fraud and reported accordingly.



- 4.3 To ensure uniformity and to avoid duplication and Report



UPDATE YOUR SOFTWARE



BE CYBER SECURE AWARE ON SOCIAL MEDIA

- Social media has become a prime target for cyber-crime. All People should take appropriate measures to be cyber-crime safe, and users, too, shall protect their personal information to avoid any misuse. Cyberspace is becoming a significant area for crimes, so there is a need for comprehensive collaboration and combat these social network security and social media cyber attacks

BE CYBER SECURE AWARE ON SOCIAL MEDIA

- Privacy of Data
- Virus and Malware Attacks
- Issues involving the use of 3rd Party Applications
- Identity Theft
- Romance Scams
- Whistle-blower