See word

Technology, Information Technology

Answer The most important lesson learnt from the opening case is to ensure that private and confidential information is not shared on the social network sites like Facebook, twitter etc. Moreover, it is also important that emails from unknown source should not be opened as it might be from some unscrupulous source and means of downloading malicious software like malware which could transfer whatever you type to the cyber criminals.

Answer 2

Some of the users' actions are unintentional threats to information security while they are using internet from their personal or professional computers. Sharing personal details and daily agenda on their social network can be hugely dangerous for them as cyber criminals can access them through hacking and exploit the same for their vested interests. Opening emails from unknown source and downloading information from non-trusted sites could seriously threaten the information security. Most importantly, as social network sites are most vulnerable to cyber-attacks, users must avoid using them through corporate setting as important corporate information could be leaked and go to unscrupulous hands.

Answer 3

When personal computers are turned into ' zombie computer' through the malicious software like malware by cyber criminals who have hacked the personal accounts of individuals, the users do not require any actions as they are unaware of the fact. This is a critical issue as users' not being aware that they are being tracked by cyber criminals, tend to work on computer and internet as normal, using passwords to log on to their individual/ corporate accounts on corporate site or sharing personal information on their social

network. Consequently, unintentionally they disclose their confidential passwords to attackers and allow them access to their private and confidential information, including corporate information.

(words: 286)

Reference

Source as provided.