

**Department of Computer Engineering**

**LMS Assignment 4**

Q. 1 Explain the various methods how we can prevent risk. [5M]

Make sure you've got a superstrong, unique password. In other words, ensure that your password is difficult to guess. One way to come up with a creative password is to brainstorm a random sentence. Take the first letter of each word in that sentence and use that acronym as the base for your password.

Don't use the same password for multiple services. Using the same term for all of your passwords leaves your entire digital life vulnerable to attack. This means that if a hacker has one password, he or she has all of your passwords.

Enable two-factor authentication. Many services, including Google, offer two-factor authentication for logging into your account. Instead of simply entering a username and password to log in, the website will prompt you to enter a code sent to your smartphone to verify your identity.

Apply software updates when necessary. Apple, Google, and Microsoft typically include security bug fixes and patches in their most recent software updates. So don't ignore those annoying prompts and keep your software up-to-date.

Carefully read the permissions before installing apps. This is one of the most prominent ways in which malicious apps can gain access to your personal information. These types of issues have been especially present in the Google Play store. A lot of apps ask for a lengthy list of permissions, and that doesn't mean they're all ill-intentioned. But it's important to be aware of the types of information your apps are accessing, which can include your contacts, location, and even your phone's camera.

Check the app publisher before installing. There have been numerous instances in which scammers have published apps in the Google Play store posing as another popular app. For example, in late 2012 an illegitimate developer posted an imposter app in Google Play pretending to be "Temple Run." A quick look at the publisher shows that the app comes from a developer named "apkdeveloper," not the game's true publisher Imangi Studios.

Avoid inserting hard drives and thumbdrives you don't trust into your computer. If you find a random USB stick, don't let your curiosity tempt you to plug it in. Someone could have loaded malware onto it hoping that an interested person was careless enough to insert it into their device. If you don't trust the source, you're better off not putting your computer at risk.