**The Dangers of a Software Monoculture:**

Monoculture is the term that is derived from agriculture. The actual definition of the monoculture is the agricultural practice of producing or growing a single crop or plant species over a wide area and for a large number of consecutive years. In the context of software and computers, monoculture means a group of computers or majority of computers are running on identical software. In present world, more than 80% computers are operated on Microsoft operating system. It indicates Microsoft is the major creator of monoculture in the software world. The prominent issue with a monoculture is that it is vulnerable to the same type of attack. In the context of agriculture if one virus can affect one variety of a crop, there is high probability for the same variety and conditions of crop getting affected. Computers exhibits almost similar behavior. If everyone is using similar OS or similar application or similar protocol to access a network, any security bug or risk is identified in that OS or Software or protocol, a single attack can affect everything. It points out the need heterogeneity in software industry. But the software monoculture suffers from three basic flaws. The first flaw is comparing software monoculture to agriculture monoculture. Whenever there is an active and powerful virus is in action, why not all the computers in the world using same OS are not getting affected? The reason is those computers may be having advanced updated antivirus software. Even two systems might be having same operating system or application software; they might have different antivirus software and different firewalls and different configurations. This is one of the reasons behind why popular viruses did not affect every system. The other reason is the security team capable to develop and deploy the security patches, new antivirus updates and configurations. The second flaw in the monoculture analysis is having heterogeneity factor. Achieving this factor needs large amount of money. Suppose a IT company have got few systems running on Windows, few other on Linux and other variants like sun solaris and unix variants; it costs more to hire experts in each domain. It might cost twice or thrice if we have different types of operating systems. A single operating system locked down by experts is far more secure than two operating systems configured by sysadmins who aren't so expert. The third flaw is that we may get a limited amount of diversity using two operating systems from three different manufacturers. In monoculture context, two is little better than one. In worst case, diverse network is less secure as it is easily affected to the attacks against one of it heterogeneous components. Some degree of monoculture is necessary in computer networks. Most of the times we communicate others in same terminology and trying to be different may not give much security. In conclusion, we can say monoculture is dangerous thing and is important. But analyzing all the factors such as time, cost and efforts to ensure our current infrastructure is more than important.

**When to Change Passwords:**