MOBILE COMPUTING - SECURITY ISSUES

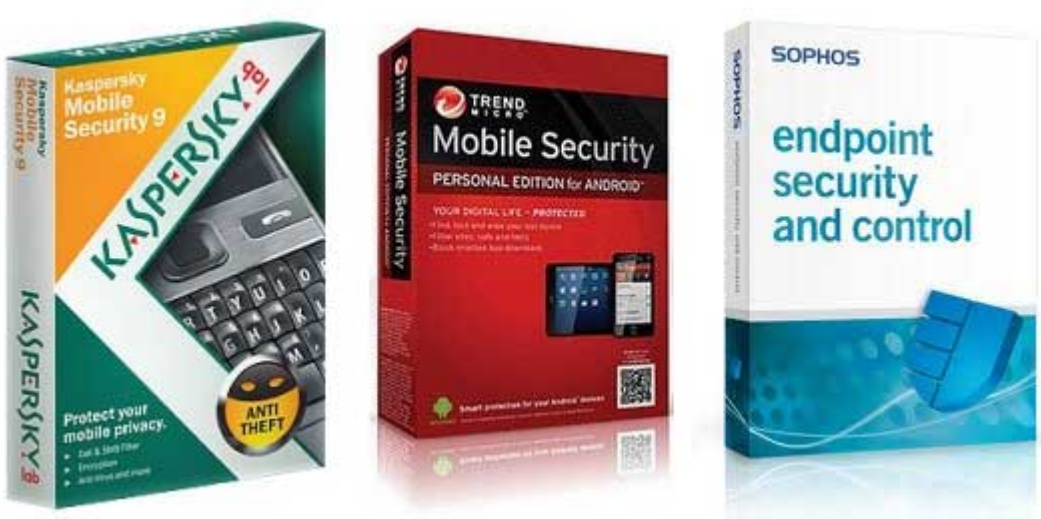
Mobile computing has its fair share of security concerns as any other technology. Due to their nomadic nature, it's not easy to monitor the proper usage. User might have different intentions on how to utilize this privilege. Improper and unethical practices such as hacking, industrial espionage, pirating, online fraud and malicious destruction are some but few of the problems experienced by mobile computing.

Another big problem plaguing mobile computing is credential verification. It's not possible to that the person using that person is the true barrier. Other users share username and passwords. This is also a major threat to security. This being a very sensitive issue, most companies are very reluctant to implement mobile computing to the dangers of misrepresentation.

The problem of identity theft is very difficult to contain or eradicate. Issues with unauthorized access to data and information by hackers, is also a plaguing problem. They gain access to steal vital data from companies. This problem has been a major headache and hindrance in rolling out mobile computing services.

No company wants to lay open their secrets to hacker and other intruders, who will in terms sell them to their competitors. It's also important to take the necessary precautions to minimize these threats from taking place. Some of those measures include −

- Hiring qualified personnel.
- Installing Security Hardware and Software.
- Educating the Users on proper Mobile computing ethics.
- Auditing and developing sound, effective policies to govern mobile computing.
- Enforcing proper access rights and permissions.



These are just but a few ways to help deter possible threats to any company planning to offer mobile computing. Since information is vital, all possible measures should be evaluated and implemented for safeguard purposes.

In the absence of such measures, it's possible for exploits and other unknown threats to infiltrate and cause irrefutable harm that would cost a huge of damage. These maybe in terms of reputation or financial penalties. In such cases, it's very easy to be misused in different unethical practices.

The other issue would be online security. If this factor isn't properly worked on, it might be an avenue for constant threat. Theft and Espionage can be also another fact limiting its full utilization. Various threats to security still exist in implementing this kind of technology.