What are zero-click attacks? Explain the measures that are required to prevent users from the possible threats.

The consequence of malicious malware cyber-attacks have been constantly raising. With improvements, advanced-technological inputs these malware attacks the user's privacy. From the spear phishing methods to zero-click attacks, the malware cyber attacks have come far way.

Zero-click attacks:

The malicious malware which performs the spying attacking and transfering data even without the target's engagement or knowledge. This spyware is more potent and impossible to detect or stop sending to importer's server. This remotely operated spyware would exercise grass root privelige from the targets device to control everything from camera, GPS to sending private data. These type of spyware's are load by over-the-air methods and can be controlled remotely.

Issues:

The target may become vulnerable in many sensitive information data the device has. The spyware even gets unnoticed by antivirus and thus evade forensic analysis. Further it can be removed remotely by the hacker. As, it uses network injection, no body would know when the spyware

has been loaded to the device (target). The spyware transmits more data controlling all the information ie GPS, contacts, passwords, Camera etc. The way of attack after loading is very simple. With just a message or call through whatsapp is sufficient to start the malicious spying action. With radio proximity and wireless the possibility of being target to attacks is more.

Measures:

1) Update the apps and operating system regularly.

2) Avoiding opening anonymous / malicious message which may / might could carry the spyware load.

3) Avoid downloading applications from browser which could potentially have a malware patch in it.

4) Avoid connecting to public networks which would increase changes of attacks.

5) Avoid keeping sensitive informations in devices, which could prove fatal to your privacy