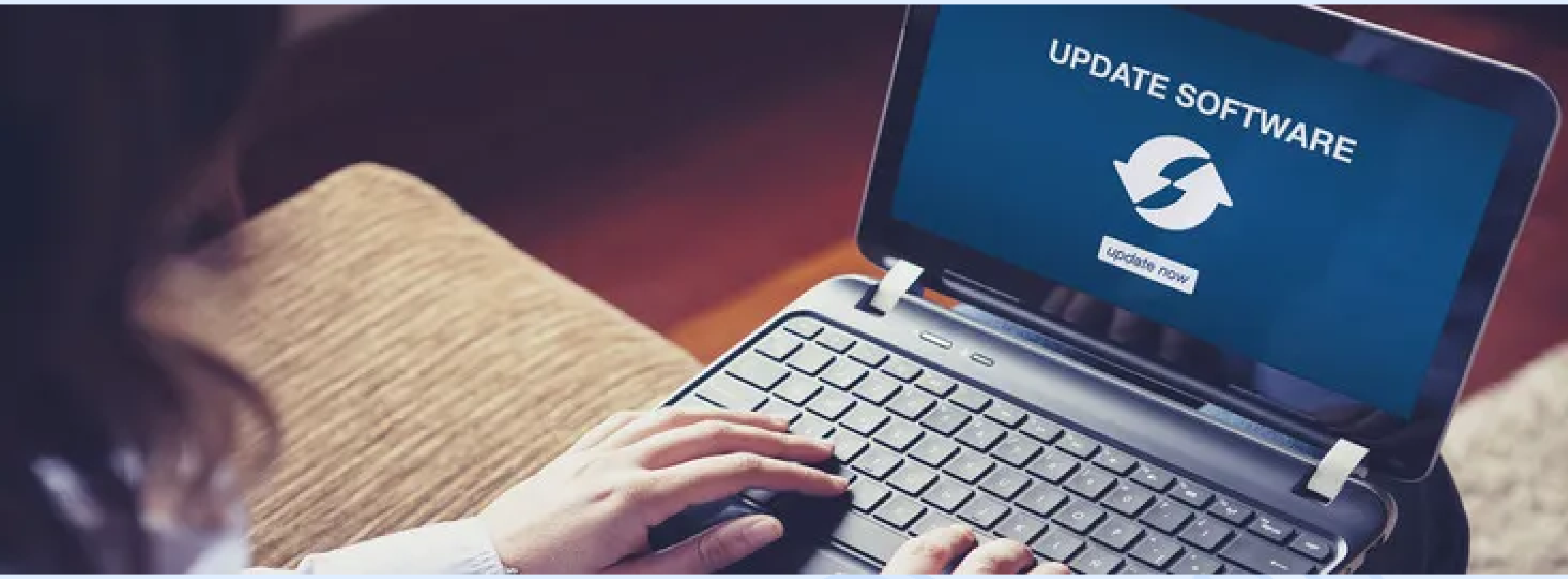

In our previous blog post, we discussed the new updates of iOS and Android platforms and the opportunities they bring to users. Today we would like to touch upon another vital issue related to system updates - virtual security. How important is it to timely upgrade your operating system, and what risks do outdated versions involve? Let’s check this out.

Keep Up with the Changing Digital Environment

In the fast growing digital world, mobile platforms face security threats at every turn. Mobile developers are in an endless struggle with hackers, who are tirelessly searching for new ways to compromise OS and gain access to valuable user data through mobile malware.

Don’t Be Caught Off-Guard

In this battle against hackers, you should know your enemy and take measures to avoid their tactics.

Android devices are vulnerable to Stagefright

Stagefright penetrates into your devices via a malicious multimedia message. You don’t even need to open it - just receiving it alone infects the device and manages to steal access into your data, camera, microphone. It performs like spyware, hijacking everything within its grasp.

XcodeGhost hits iOS devices

XcodeGhoste distributes thousands of accidentally infected apps, built in the Xcode SDK downloaded from a malicious website. If you install such an app to a personal or corporate device, your data is at serious risk. The malware can provide attackers with remote command and control (CnC), open web pages, and steal credentials.

Keyraider can steal data from Apple accounts

Keyraider targets jailbroken iPhones and iPads to get access to corporate documents and emails. It can also steal passwords, usernames, and other valuable data.

YiSpecter steals user data

YiSpecter uses private Apple iOS APIs to infect iPhones and iPads. It can also be distributed through offline app installation, ISPs or when pairing with Windows. This malware can install, change, replace and launch iOS applications without your permission, show full-screen ads, and also upload your data to the CnC server.

Protect Your Data Efficiently

Any malware can jeopardize your corporate security and make a cyber breach. To protect your enterprise and personal data, follow the simple steps:

- Avoid suspicious emails, messages, links, and downloads.
- Use app security testing to check the quality and reliability of your apps.
- Choose special programs that enable you to manage software security, don’t neglect antiviruses.
- Make sure you have the latest version of the operating system and perform timely updates.
- If you are the app owner, assign your developers to introduce regular updates for the platform it is built on or upgrade your app to work with the functionality of the latest OS version to provide access to the new features and the most secure solutions.

Many malware programs can hit only older operating systems, making regular updates an integral part of your data protection strategy. The latest iOS and Android updates will bring you, and your app users not only new features but also additional security and a peace of mind. If you need to test or upgrade your current apps in compliance with the latest system requirements, our experienced developers are always ready to help.