Device Protection

In today’s hyper-connected world, device security is of utmost importance. Cyber criminals exploit the anonymity of the Internet to perpetrate an assortment of criminal activity. Their technology is neck-and-neck with the technological advancements of the security software industry. Fortunately, there are solutions to stay ahead of the game.

Protective technologies secure your internet-connected devices from cyber attack around-the-clock. In today’s post, we will discuss how these easy-to-use and highly affordable technologies can keep your personal and business data out of harm’s way.

Device security, that is; protecting the phone, laptop, tablet or anything else that is connected to the Internet from all cyber threats is of fundamental concern to risk management today. First, think about the electronic activities that take place on your internet-connected devices. We use these devices for shopping, banking, conducting all types of personal communications, and almost every element of our lives.

As deep and broad as our engagement with technology has become, we are just in the early innings of the Information Age. The level of personal data transmitted at the press of a fingertip is increasing at exponential rates. Good device security will protect all of it while being adaptive to the constantly evolving threat environment, automatically and preemptively.

Device Security Checklist

AntiVirus

The threat of malware is real. The consequences of infection can be severe, so your first step towards cybersecurity should be prevention. It can take years to recover from the ransomware and spyware damage a viral breach can incur. The antivirus service you choose should include automatic updates and fast responses to the confirmation of new threats. This is a 24/7 job, and it requires significant resources and commitment. Only the best providers should be considered to protect your devices from viruses.

Intruder Protection

Intruders are constantly attempting to connect to your computers and mobile devices. When successfully connected, they attack internally to steal information or hijack your device. In many cases, they can operate for months before being discovered, all the while collecting your personal information to engineer future attacks.

Rootkit Protection

A rootkit is a typically malicious assembly of software that enables unauthorized access while masking its existence from detection. Protection from concealed rootkits is essential to secure your computer and smart devices.

Firewall

In today's hostile online environment, advanced firewalls are required to stay abreast of the constantly evolving threats on the internet. The firewall should always be "on" even when the device is not connected. It is also good practice to update your database every time a connection is made.

Software Updater

One of the most effective measures against hacking is keeping the software on your device updated and current. Modern device security software will do this for you, regularly scanning your system for missing patches in the operating system and 3rd party software. Once the requirement for an update is recognized, the service will deploy the required updates automatically. The most important updates are those from Microsoft, Apple, Adobe, Java, OpenOffice, archive managers, media players and image viewers, all of which are especially prone to vulnerabilities. According to a leading study conducted by F-Secure, 83% of all malware breaches could have been avoided simply by having the latest updates and patches installed.