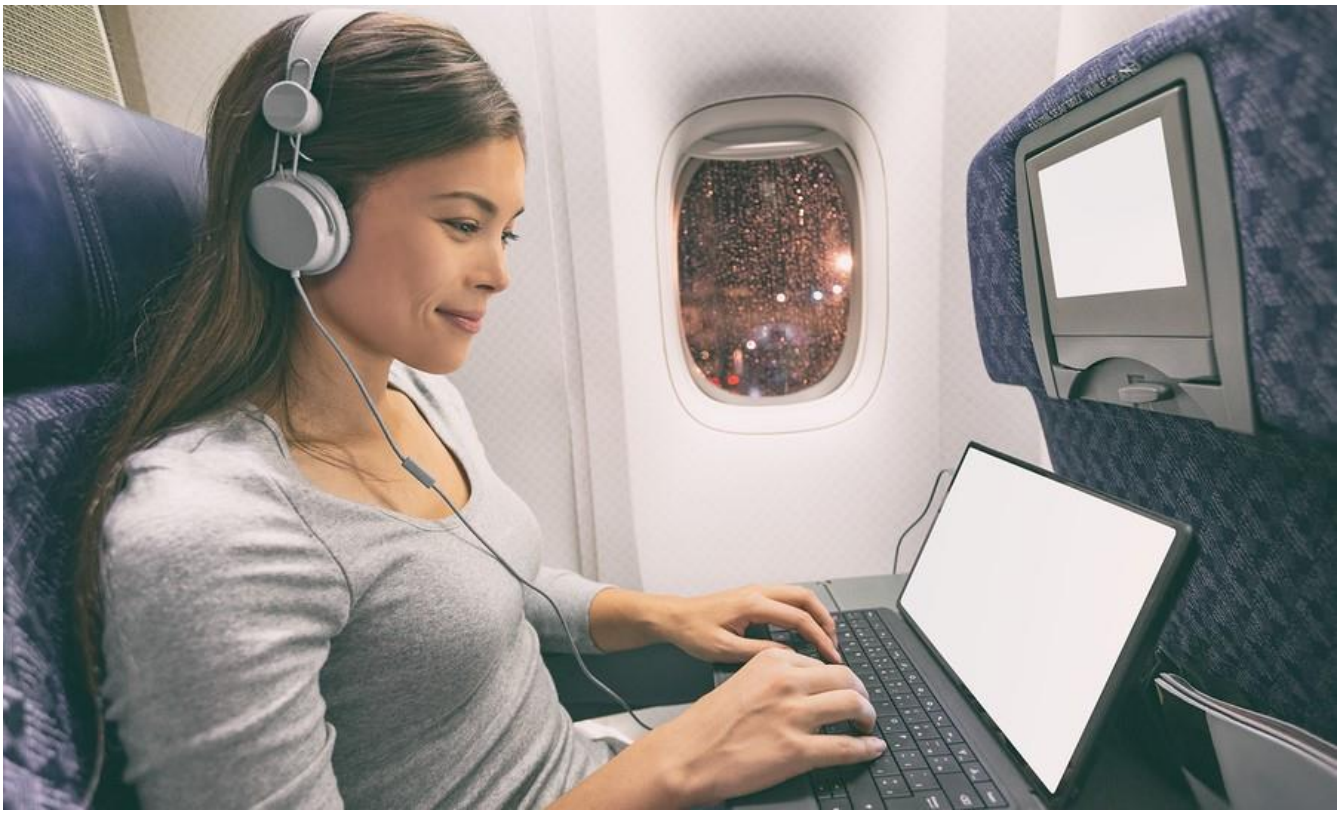
Safeguard Vital Assets with Mobile Workforce Security



With a myriad of advantages for both employees and the companies they work for, it should come as no surprise that forecasters predict that by 2023, mobile workers will account for over 43 percent of the global workforce. Employees gain the flexibility of working from anywhere at any time. Businesses also benefit from increased productivity and decreased response times.

At the same time, the mobile environment opens the door for increasing cyber-attacks. For instance, a hacker who gains access to an employee phone can potentially reach sensitive data inside the enterprise network. Organizations therefore need to address mobile workforce security from multiple levels, including both individual devices and the network.

Understand the Mobile Threat Landscape

In the old days, employees split work between desktop computers at the office and laptops that connected to the office network. Today's employee, however, may work variously on a smartphone, a laptop and a tablet, in addition to a desktop computer. And organizations that operate with bring-your-own-device (BYOD) policies have little control over the devices used.

Mobile threats cover a wide territory. Workers using personal cell phones and tablets may use unprotected devices. Compromised apps spread dangerous malware that can steal data or render a device unusable. And phishing attacks on mobile devices have increased 85 percent annually over the past eight years.

Device-Level Security

An effective multi-layered approach to mobile workforce security addresses security at the device level. The device itself needs comprehensive, up-to-date virus protection. In addition, the security strategy must determine how the device accesses the network and what happens should a device become lost or stolen.

The industry offers several options for mobile device management (MDM). With a good MDM system, administrators can specify which devices can access the network. The MDM system should define access for applications and provide end-to-end encryption. It should also allow for remote configuration and the ability to remotely wipe a device in the case of theft.

Essential Policies for Mobile Workforce Security

From the perspective of the IT department, the safest approach to mobile access involves restricting employees to devices owned and managed by the company. This scenario gives the organization the greatest control over what applications employees download and use.

However, many small to medium businesses instead opt for a BYOD environment. This can reduce overhead costs and even increase productivity. But it greatly increases the security risks. To offset those risks, organizations need to define and enforce comprehensive policies for mobile device usage. Policies should include requirements such as the following:

- **Never use public Wi-Fi** – That free internet access at the local café may sound convenient, but cybercriminals love it. Use cellular data instead, or keep data safe with a virtual private network (VPN).
- **Stay current on updates** – Those updates often include patches for known software vulnerabilities, in addition to enhanced features.
- **Run frequent backups** – Employees should adhere to a regular backup schedule to protect against data loss.

- **Mandatory passcodes or biometrics** – On all devices.

- **Download only approved apps** – Through the MDM system, create a whitelist of official apps that employees can download and use. Unofficial apps provide a haven for viruses and other malware.

Security in the Cloud

Another critical element of multi-layer security involves implementing protections on the network side. First, you need to understand your network, including all points where data enters or leaves the organization. At a minimum, this includes email and cloud storage areas, as well as any additional cloud-based applications.

Second, define policies for data access and retention, encryption, naming conventions, passwords and regulatory compliance. These policies should cover how employees create, store and share data. For organizations using Office 365 for mobile workers, Microsoft includes the ability to automate many of those policies within the software.

Finally, run regular security audits to assess ongoing data safety. Employees come and go, and every new application changes the landscape. Audits will flag employees not adhering to policies and provide ongoing identification of vulnerabilities.

Don’t Leave Security to Chance

Mobile devices play an essential role in modern business, providing efficiencies and connections we cannot imagine living without. That convenience and flexibility brings increased challenges to securing vital intellectual assets. Organizations must know the risks and implement defense in depth strategies to secure both individual devices and the network.

The staff at Messaging Architects bring extensive expertise at building comprehensive mobile workforce security. From e-policy review and consulting to security audits, we can help you implement multi-level protections to ensure data security and privacy.