Mobile Device Security: Prevent Others from Accessing Confidential Information

Americans are relying more and more on mobile devices to store sensitive personal and business information. A number of new applications also involve the storage and transition of personally identifiable medical information between consumers, vendors and health care and insurance providers. The stakes are getting very high - and the technology arms race between service providers and would-be hackers and data thieves is getting intense, indeed.

Consumers have long been encouraged to use "strong" passwords that include a combination of numbers, letters and alpha-numerics that make it much more difficult for hackers to break into their devices and communications and steal data. But this doesn't deter the most determined and sophisticated threats - as the State Department recently learned.

The constantly evolving threat has forced corporations and government entities alike to develop a number of additional safeguards and protocols to protect the integrity of mobile devices.

Vendor-Specific Encryption

Apple's latest iPhone software, iOS 8, includes an automatic encryption feature that applies to FaceTime and iMessage transmissions. Even Apple can't decrypt these messages. However, iPhone and other mobile users are vulnerable to data hackers if they back up their data to the iCloud - as a number of very embarrassed celebrities found out to their chagrin last year. To eliminate the possibility of your iCloud data being stolen, turn off iCloud backup of iMessage and SMS messages.

iPhone Procedure

iPhones have come with a PIN-access option for years. What's new is this: Activating your PIN number functionality on your iPhone also enables Apple's encryption protocols that lock hackers out of your most sensitive data. To get started, open the Settings application, scroll to Touch ID & Passcode (or, on older models, simply 'Passcode') and turn the Passcode function on.

Android users can find specific instructions to enable encryption on their phones here.

'Something You Have + Something You Know'

This is the key to the evolving 'multi-factor' systems gaining an increasing foothold in the mobile security industry: Users must have something physically in their possession, plus enter a password or PIN known (presumably), only to them.

Multi-factor protocols aren't just twice as effective as single-factor systems like passwords. They're exponentially more effective. The downside: You have to make the effort to enable them! The logistics of actually enabling multi-factor encryption on all devices and accounts can be daunting, but there's a convenient resource available: The website Turnon2fa.com contains detailed instructions on scores of prominent sites and services.
You can also download apps to your mobile device, like BioMetric Security (a fingerprint reader) and Eyeprint ID (an iris scanner), among others.

**Future Rollouts**

Look for more effective and affordable biometric apps that use Iris-scanning, fingerprint scanning or voice-recognition to help secure your mobile devices. The technology has been out there for a while, but just hasn't caught on. As consumers become more acutely aware of the benefits of this kind of technology, however, we may see it becoming more common.

One promising development: Next Generation PIV cards and readers that are adopted to mobile devices. The PIV card includes a microchip that includes a photo of the card/device owner or user, PIN number, fingerprint and other information locally stored on the card - and only on the card, in a method called 'on-card biometric comparison.'

*Publication was created by a third party for the representative’s use*