‘Apple Picking:’ 5 Ways to Lose (& Retrieve) Mac Data

Apple platforms are far from invincible, as these common loss scenarios demonstrate.

When iPhones, iPads, and other Apple devices like Macbooks became popular, thieves saw stealing them as an easy way to make a quick buck. Now they're after much more -- data. Today's Apple devices store quality data -- contacts, credit card transactions, passwords -- of interest to criminals. Worse, BYOC and BYOD are increasingly making Macs repositories for sensitive corporate intellectual property, which further attracts both cyber-criminals and disgruntled or dishonest employees.

This story will educate IT managers and end users about the threat to data from "Apple picking" and how to reduce the risk of data loss through policy, practices, and free and market-based security tools and solutions such as data loss protection (DLP) and mobile device management (MDM). Full disclosure: My company provides such solutions.

The best way to protect your users from Apple picking is simple, but often not enforced. Train your employees to be religiously aware of their surroundings. Teach them not to leave devices (iPhone, iPad, Macbook) unattended or in plain sight of coworkers or the public. However, should an employee become a victim, here are five tips to help keep your company's confidential data safe.

Tip 1: Use the password protection and encryption already in the device
Both computers and mobile devices come with built-in security features. Ensure your users create a password and enable encryption to add another layer of protection. For Macs and iPads, FileVault is a great full disk encryption solution. For iPads, ensure that Screen Control Center, Notifications, and Today View are locked, as well.

Tip 2: Always use Apple's device tracking and locating features
If you have to, these features will enable you to wipe data off any device if it gets lost or stolen. Apple provides a guide for activating and using these cloud-based features. They're easy to set up, so why run the risk of someday needing to wipe data off a user's device, only to learn the user didn't activate device tracking and locating? The downside to wiping the device is the data is gone forever, along with options to control the device remotely. If an employee's device has been stolen, the tracking features can help you pinpoint its location, so you can alert authorities to help recover it.

Now, let's get a bit more creative and give you information that's not as commonly known.

Tip 3: Applock makes things harder for the Apple picker
Applock is a feature that allows users to set their iPhone or iPad to access only a specific application if it's stolen, adding yet another obstacle for anyone who tries to take a mobile device. For example, the app can be a media player, which can be set to play a specific song if the device is lost or stolen. Applock can also be programmed to sound an alarm or siren to annoy or scare a thief into discarding it.

Tip 4: Applock combinations: video capturing and/or voiceover apps
Through the Applock feature, an MDM solution can remotely "wake up" the phone and launch the device's video camera or a voiceover app. The camera can record everything around it, which could provide clues about who has your device. You can use the voiceover app to start talking to the person who has your phone, too. Though this may not directly avoid data loss, it can help you recover your stolen phone or gather information to decide whether to wipe away its data or not.

Tip 5: Stay hopeful
Not everyone has bad intentions. Sometimes employees simply forget their device "somewhere," and a well-intentioned person finds it. You can put the device on "Lost Mode" to set a four-digit passcode to protect it, and to display an onscreen message stating the device has been lost or stolen, along with an alternate phone number.

Because the device is locked, the person has only one option: Call the number.

Roman Foeckl leads CoSoSys. The company is a leading developer of mobile device management (MDM), data loss prevention (DLP), device control, network endpoint security, and portable storage encryption solutions for Windows, Mac OS X, and Linux. It has ...