

Easy to Use or Easy to Lose? How to Protect Mobile Devices

Mobile devices like the BlackBerry and Palm Treo have become indispensable tools for many lawyers. Compact and easy to use, these devices offer quick access to calendars, contacts, e-mail, documents, and other sensitive personal and client information. Unfortunately, the portability of such devices also makes them highly prone to loss or theft. If you or members of your firm use a PDA, smartphone, or similar device, take appropriate steps to protect client confidentiality:

1. Limit Use. Restrict the type of information stored on a handheld device to reduce your exposure.

2. Standardize. If more than one handheld device is used, everyone in the firm should use the same type of device. Do not allow outside devices. In the event of a problem, it will be easier to implement a firm-wide solution if everyone is using the same product.

3. Password Protect. Use “power-on” passwords. If the device is lost or stolen, data on the device cannot be accessed without the password.

4. Use the Lock-out Feature. Set devices to lock out users after a specified number of incorrect log-in attempts. Use “sleep” settings to lock devices after 10 or 15 minutes of inactivity.

5. Consider Encryption or Biometrics. Products like SafeGuard PDA from Utimaco go beyond password protection and lockouts to protect data by using encryption and biometrics. Biometrics protect data by requiring signature, voice, or fingerprint authentication. If the device doesn’t recognize the user, it can’t be accessed. Visit http://americas.utimaco.com/safeguard_pda for more information.

6. Explore Data Wiping. Research in Motion’s BlackBerry Enterprise Server, as an example, comes with a feature that wipes all data from the device’s memory once a certain number of failed log-in attempts are exceeded. The current version of Microsoft Exchange provides for a remote wipe of a lost or stolen Windows PDA. Remember that if you have regularly synchronized your device, the destroyed data can be easily restored to a replacement device.

7. Starve the Virus. Virus attacks on handheld devices are rare but potentially devastating if a compromised mobile device is synched to a desktop or network. All the major antivirus vendors, including Symantec (Norton Smartphone Security) and McAfee (McAfee Mobile Security), offer security products designed for mobile platforms. Visit www.symantec.com and www.mcafee.com for more information.

8. Learn More. To learn more about mobile devices, visit resources like the PDA Learning Center at http://palmtops.about.com/od/pda-learningcenter/PDA_Learning_Center.htm or www.pdatoday.com.

BEVERLY A. MICHAELIS
PLF PRACTICE MANAGEMENT ADVISOR

DISCLAIMER

IN BRIEF includes claim prevention information that helps you to minimize the likelihood of being sued for legal malpractice. The material presented does not establish, report, or create the standard of care for attorneys. The articles do not represent a complete analysis of the topics presented, and readers should conduct their own appropriate research.