

## SMARTPHONE SECURITY TO-DO LIST

### Protection against theft or loss of the device:

- Consider a smartphone with a PIN feature to deter unauthorized use.
- Consider a smartphone with a fingerprint authentication feature (Michael L. Kasavana, "Cell Phones: A Key Player in Proximity Payment Systems," *Automatic Merchandiser*, May 2006).
- Use secure sync interfaces to back up the data in case the device fails or is lost.
- Always be vigilant.

### Protection against malware:

- Download files only from trusted websites.
- Do not open e-mail attachments from unknown senders.
- Turn off the Bluetooth feature when it's not in use.
- Purchase and install anti-malware programs.

### Protection against data theft and hacking:

- Install firewalls on the enterprise server. (This should already be a standard practice.)
- Use encryption software to protect sensitive data.
- Use WPA2 (Wi-Fi Protected Access 2.0, a stronger encryption than WPA) to stay safe at "hot spots" (if both the smartphone and the mobile service are WPA2-compatible).