Mobile devices are computers, too!

Protect them like you would any computer:

- Use a complex password and set it to automatically lock
- Keep it with you or lock it up securely before you step away
- Encrypt restricted data and passwords (or the entire device)
- Run current versions of the operating system and apps
- Beware of phishing: Don't open files, click links, or call numbers in unsolicited emails, text messages or IMs
- Use anti-virus/anti-malware software, if available
- Use known, encrypted networks whenever possible
- Securely delete all contents before disposing of a device

All devices connecting to UCSC's network or services must meet UC & UCSC security requirements

More tips for protecting mobile devices:
its.ucsc.edu/security/stay-secure/minreq/mobile.html

UC SANTA CRUZ Information Technology Services