

10 Mobile Security Do's & Don'ts



1. Do

Embrace BYOD adoption to boost productivity

1. Don't

Allow users to download corporate data to unmanaged phones



2. Do

Support a variety of mobile operating systems and apps



2. Don't

Restrict which personal apps users can install on their devices

3. Do

Require strong authentication before accessing corporate apps

3. Don't

Make it difficult for users to access their personal apps



4. Do

Ensure that lost or stolen phones don't expose corporate data

4. Don't

Wipe users' personal data after a security violation, such as multiple failed logins



5. Do

Protect data in transit and at rest from snooping and theft

5. Don't

Assume that all mobile apps use strong ciphers to encrypt traffic