HOW TO PROTECT AGAINST

COMPROMISED

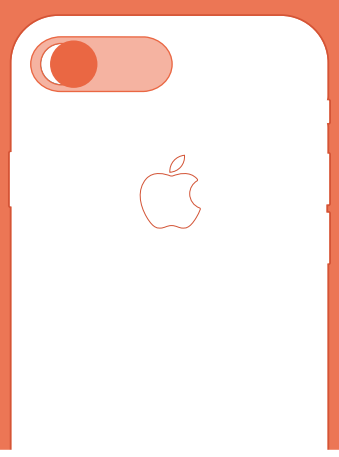
SMARTPHONE CAMERAS AND MICROPHONES

If you're concerned that your organization's sensitive conversations and visual details may be at risk of capture via hijacked smartphone cameras and microphones, consider the four options available for defending against this emerging breed of attack.

1

ENCOURAGE COVERS AND PLUGS

Urge users to utilize camera covers and microphone plugs at their discretion.



2

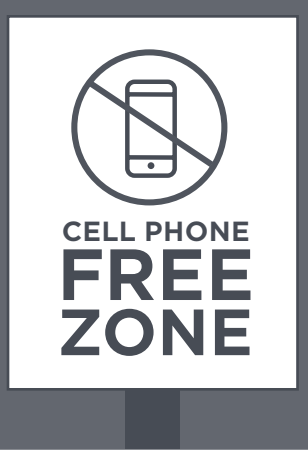
DISCONNECT CAMERAS AND MICROPHONES

Physically disconnect the cameras and microphones within a user's smartphone.

3

BAN SMARTPHONES ENTIRELY

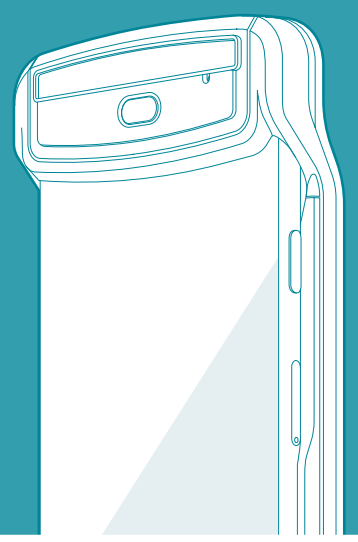
Establish policies for banning smartphones from sensitive work locations.



4

ADOPT THE SAFECASE

Procure a SafeCase for each user's smartphone.



HOW IT WORKS

A removable sticker or sliding camera cover can be used to block illicit image capture, while a microphone plug (such as a modified pair of earbuds) can be used to block some audio capture.

Some vendors, like mobile repair shops, may be able to disconnect a smartphone's cameras and microphones, either by snipping the pertinent cables or removing these components entirely.

Smartphone bans can be enforced through periodic security inspections. Designated storage areas (such as lockers) may be installed outside of the affected locations.

The SafeCase, an intelligent smartphone case, has built-in protections against audio and video surveillance. User compliance can be monitored and enforced through an administrator portal.

KEY DRAWBACKS

- Clunky user experience
- Lack of enforcement

- Permanent loss of functionality
- Voided warranty

- Lost productivity
- Lower personnel morale

- Hardware investment
- Administrator duties

TYPICAL USAGE

Organizations or units operating in low-risk environments

Rare circumstances in which internet use is permissible but audio/image capture is not

Locations where extremely high-risk information is shared

Security-conscious organizations or units dealing with sensitive information

PRIVORO®