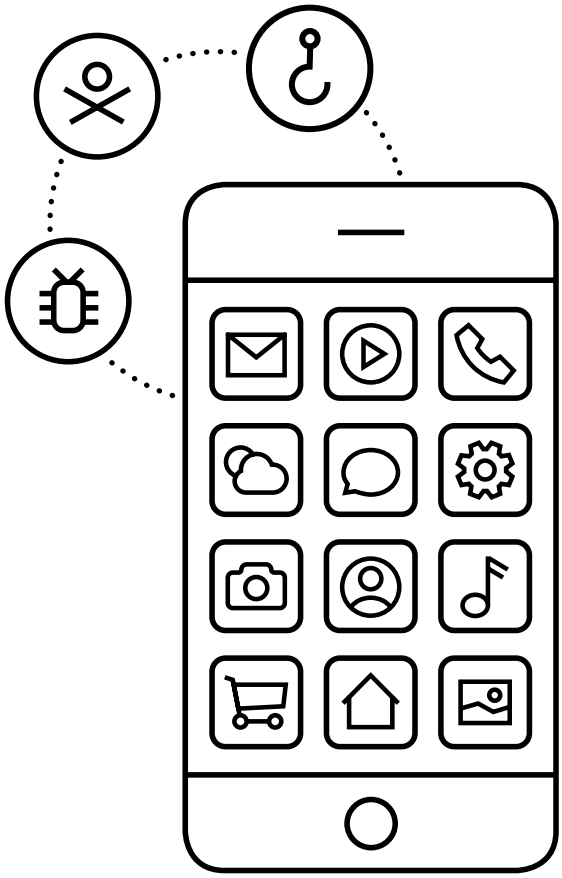
Acceptable Use Policy (AUP) Best Practices

Starting point...

An Acceptable Use Policy (AUP) is a necessary first line of defense for BYOD and corporate devices.

With AUP you can:

- Set criteria for access to websites
- Help secure mobile devices
- Promote LTE and limit use of Wi-Fi
- Curate company-approved apps
- Address mobility ecosystem risks
- Establish patch schedules and policies
- Define per-device data volumes
- Review user behaviors
- Guide employees on compliance
- Provide regular phishing simulations and training



It shouldn't take a compromise to step up your game.
Read the Rise of Social Engineering and Cost of Personal Devices: A Security Perspective white paper at verizon.com/business/resources/whitepapers/the-rise-of-social-engineering-and-the-cost-of-personal-devices.pdf

Learn more.
Contact your Verizon Business Account Manager to discover how Verizon can help protect your business. www.verizon.com/business/products/security/mobile-device-endpoint-security/

verizon business