WFG National Title

SAFE | Security Awareness for Everyone

TIP SHEET - JULY 2025

Protecting Your Identity, Finances, and Data in a Mobile-First World

Why Mobile Device Security Matters More Than Ever

Smartphones are no longer just communication tools; they have evolved into multifunctional platforms that support critical aspects of daily life. From managing finances and accessing sensitive business data to serving as digital keychains and identity hubs, their convenience is unmatched. However, this convenience comes at a cost: the more applications and capabilities added to these devices, the more attractive they become to attackers.

One fundamental principle of mobile devices is ease of use, which many consumers equate with security. Unfortunately, the opposite is often true. As functionality increases, so does risk exposure. Threat actors continue to develop advanced techniques to exploit mobile vulnerabilities, many of which don't require physical access to the device. Add the risk of leaving devices unattended, and the consequences for individuals and organizations can be severe, ranging from financial theft to unauthorized access to corporate systems.

To address this, it's critical to strike a balance between usability and security. For iOS and Android devices, several impactful configurations can fortify defenses without unduly undermining day-to-day functionality. This article outlines actionable steps to enhance mobile security, examines their usability implications, and highlights how strategic adjustments can effectively protect personal data and organizational information. The intent of these recommendations is not that you must apply all of them. You should understand the level of risk and choose the right amount of friction with these settings, understanding that increasing security decreases usability, and conversely, increasing usability (making things easier) decreases security.

Periodic Review of Security Settings is Essential

In the dynamic landscape of cybersecurity, static defenses are a liability. It is essential to recognize that security measures are not a one-time implementation, but an ongoing process that must continually adapt to emerging threats. As such, we recommend a disciplined approach to mobile security management, with a structured review every quarter. This reassessment is particularly crucial following operating system updates or the addition of new applications, both of which can introduce new vulnerabilities. By maintaining this regular cadence, you are better positioned to identify and mitigate risks proactively, thus reinforcing your organization's overall security posture.

Click the logo below to download a mobile security guide for your device.

iOS android