Sichere mobile Geräte

RUHR UNIVERSITÄT BOCHUM

Stabsstelle für Informationssicherheit

1. Gerät mit PIN, Passwort oder biometrischer Sperre schützen
Verwenden Sie eine starke Bildschirmsperre (PIN, Passwort, Fingerabdruck oder Gesichtserkennung), um unbefugten Zugriff zu verhindern.

2. Regelmäßige Updates durchführen
Halten Sie das Betriebssystem und alle Apps immer auf dem aktuellen Stand, um bekannte Sicherheitslücken zu schließen.

Aufgepasst bei Geräten, die von IT.SERVICES oder Ihrem Admin-Team betreut werden:

Bei gemanagten Geraten stehen Ihnen nicht alle Einstellungen direkt zur Verfügung.

Folgen Sie den Empfehlungen Ihres Admin-Teams. Fragen Sie nach, welche Sicherheits-Einstellungen bereits für Sie vorgenommen wurden.

3. Apps nur aus offiziellen Quellen installieren
Laden Sie Apps ausschließlich aus dem Google Play Store oder Apple App Store herunter.

4. App-Berechtigungen prüfen und einschränken
Überprüfen Sie, welche Berechtigungen Apps anfordern, und erlauben Sie nur das Nötigste (z. B. Zugriff auf Kamera, Standort, Kontakte).

5. Langes Drücken auf Links zeigt Ziel an
Auf Desktops zeigt die Maus das Ziel an, wenn man mit der Maus über den Link fährt . Auf mobilen Geräten hat das Gedrückthalten mit dem Finger oder Stift den gleichen Effekt.

6. Weiterleitung entlarvt Absender
E-Mail-Apps zeigen oft nur den Anzeigenamen, aber nicht die Mailadresse des Absenders. Durch die Weiterleitung wird die Mailadresse sichtbar.

7. Vorsicht bei öffentlichen WLANs
Meiden Sie öffentliche WLANs. Deaktivieren Sie das automatische Verbinden mit unbekannten WLANs.

8. Gerät verschlüsseln
Aktivieren Sie die Gerätespeicher-Verschlüsselung, damit Daten bei Verlust oder Diebstahl geschützt sind (bei modernen Geräten meist standardmäßig aktiviert). Verschlüsseln Sie zusätzliche Speicherkarten.

9. Gerät aus der Ferne orten und löschen können
Aktivieren Sie Funktionen wie „Mein Gerät finden“ (Android) oder „Wo ist?“ (iOS), um das Gerät bei Verlust zu orten oder zu löschen.

10. Bluetooth und NFC deaktivieren, wenn nicht benötigt
Schalten Sie drahtlose Schnittstellen wie Bluetooth oder NFC aus, wenn sie nicht gebraucht werden, um Angriffsflächen zu minimieren.

11. Keine sensiblen Daten unverschlüsselt speichern
Speichern Sie Passwörter, Bankdaten oder andere sensible Informationen nicht unverschlüsselt auf dem Gerät.