IHR SMARTPHONE IN DER FIRMA SICHER NUTZEN

Smartphones sind wesentlicher Teil unseres Arbeitsalltags. Dabei bringt der Einsatz auch einige Risiken mit sich. Mit überschaubarem Aufwand lassen sich jedoch wirksame Strategien entwickeln, um auf Vorfälle wie z.B. den Verlust eines Gerätes vorbereitet zu sein. **Wie Sie Ihr Smartphone absichern können, erfahren Sie hier!**

DIGITAL SICHER NRW
Kompetenzzentrum für Cybersicherheit in der Wirtschaft

Beauftragt vom Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen

DIGITAL SICHER NRW

WOZU SOLLTEN WIR UNSERE MOBILEN GERÄTE ABSICHERN?

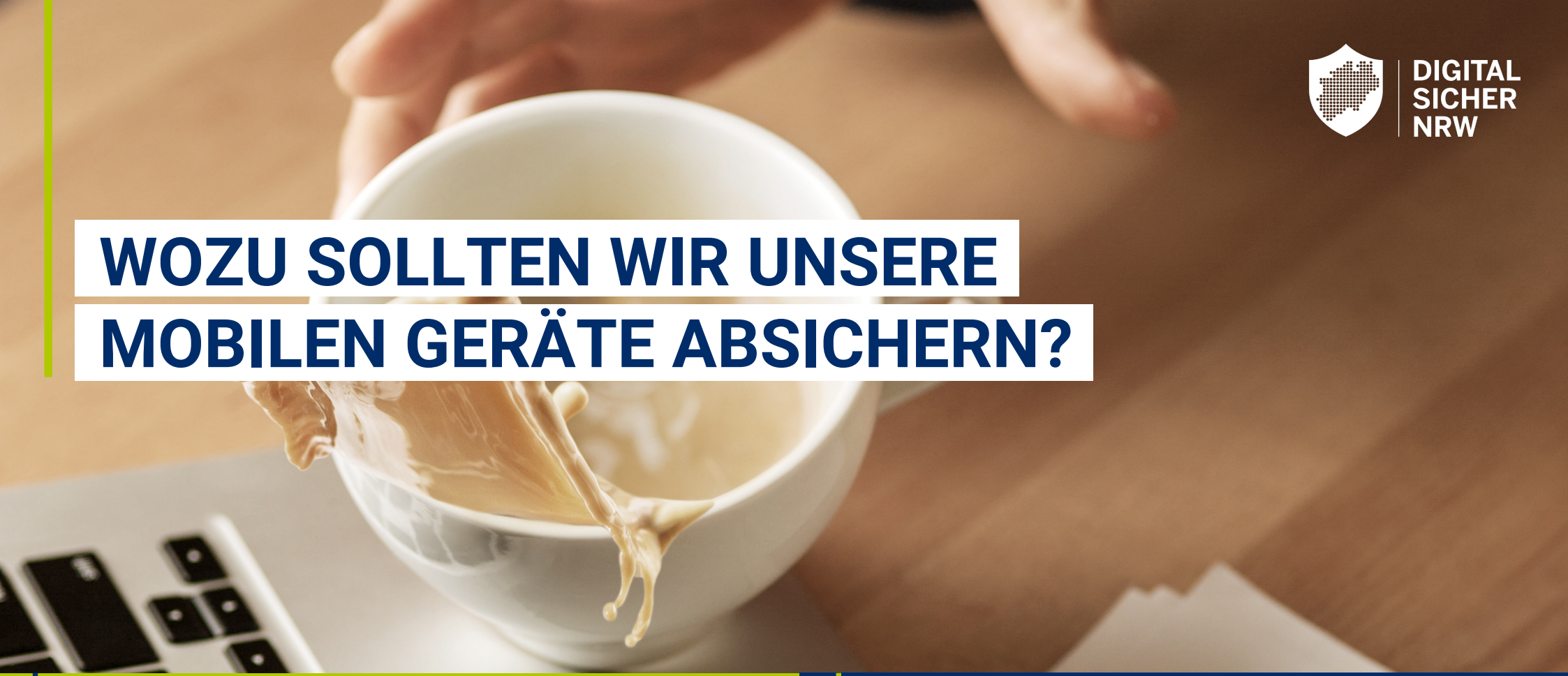
Smartphones werden in Bezug auf Sicherheit oft mehr als „bester Freund“ oder „treuer Begleiter“ und kaum auch als potentielles Sicherheitsrisiko wahrgenommen. Dies ist jedoch wesentlich, da die Geräte in den meisten Fällen voll von persönlichen Informationen und oft auch betrieblichen Daten sind. Ob privat oder beruflich, sind sie faktisch Geheimnisträger.
Welche Gefahren bestehen also im Umgang mit Smartphones?

GEFAHR 1: ÖFFENTLICHES W-LAN UND LADESTATIONEN

Die Nutzung öffentlicher „Hotspots“ oder frei zugänglicher Ladestationen kann zum Sicherheitsrisiko werden, denn von außen lässt sich nicht erkennen, wie diese jeweils funktionieren. Unbefugten Dritten kann so potenziell ein ungewollter Zugriff auf das Smartphone gegeben werden. So können bspw. Verkehrsdaten vom Betreiber der Hotspots oder von Angreifern mitgeschnitten und eingesehen oder über eine USB-Ladestation Schadsoftware übertragen werden.

GRUND 2: VERLORENES GERÄT

Ohne eine Absicherung (z.B. durch ein sicheres Passwort, den Fingerabdruck oder die Face-ID) können Dritte im Fall eines Geräteverlusts auf alle Unternehmensdaten – inklusive vertraulicher Mails, Bilder, Dateien, Kontaktdaten – zugreifen. Angreifern stehen dadurch alle Möglichkeiten offen, das Unternehmen zu gefährden.



DIGITAL SICHER NRW

WOZU SOLLTEN WIR UNSERE MOBILEN GERÄTE ABSICHERN?

GRUND 3: HACKING

Auch Smartphones können von schadhafter Software befallen sein oder in das Visier eines Angreifers rücken. Besonders durch Phishing-Mails können Kriminelle Login-Namen und Passwörter von Accounts oder andere sensible Informationen abgreifen.
Dies erfolgt in der Regel durch die Installation von Schadsoftware, durch die sich Hacker Zugriff zum Gerät verschaffen.
Hier können auch gefälschte Apps ein Risiko darstellen.

GRUND 4: TRACKING

„Tracking“ bedeutet auf Deutsch so viel wie „eine Spur aufnehmen“. Betreiber von Apps holen sich umfassende Berechtigungen, die Ihre Privatsphäre verletzten. Dazu verlangen die Apps verschiedene Zugriffe auf Ihr Gerät, damit die App im vollen Funktionsumfang genutzt werden kann. Hier ist stets Vorsicht geboten und jede angefragte Berechtigung sollte hinterfragt werden.

WIE SIE IHR SMARTPHONE SCHÜTZEN

DIGITAL SICHER NRW

Für den Umgang mit mobilen Geräten sollten Sie in Ihrem Unternehmen **verbindliche Regelungen** schaffen und **Verantwortlichkeiten festlegen**. Dabei sollte immer auch der **Umgang mit gestohlenen bzw. verlorenen Geräten** bedacht werden.

1. SICHERE GRUNDKONFIGURATION

- Deaktivieren Sie die feste Werbe-ID.
- Aktivieren Sie den Standort nur, wenn notwendig und schalten Sie Ihren Standortverlauf / Wichtige Orte aus.
- Deaktivieren Sie Roaming bei Reisen ins nicht EU-Ausland, um sich vor kostenpflichtigem SMS-Versand im Ausland zu schützen.
- Schränken Sie die Datenweitergabe / Telemetrie ein.

2. AUTHENTIFIZIERUNG

- Setzen Sie eine PIN oder besser ein Passwort. Tipp: Nutzen Sie einen Passwortmanager zur sicheren Verwaltung von Passwörtern und PINs.
- Ein Fingerabdruck bzw. eine Gesichtserkennung ermöglicht Ihnen ein komfortables entsperren und damit ein komplexes Passwort, PIN oder Muster.
- Nutzen Sie Zwei-Faktor-Authentifizierung, wo immer möglich.

3. EINSCHRÄNKEN VON APP-BERECHTIGUNGEN

- Hinterfragen Sie, welche App welche Berechtigungen wirklich benötigt!
- Nehmen Sie nicht notwendige Berechtigungen wieder zurück.
- Deinstallieren sie stets Apps, die Sie nicht mehr benötigen oder nicht nutzen

WIE SIE IHR SMARTPHONE SCHÜTZEN

DIGITAL SICHER NRW

4. UPDATES DURCHFÜHREN

- Aktivieren Sie die automatische Installation von Updates.
- Installieren Sie neue Updates immer zeitnah nach der Benachrichtigung.
- Stoßen Sie die Suche nach Updates zur Sicherheit regelmäßig selbstständig an.

5. NICHT-PERSONALISIERTE GERÄTENAMEN

- Achten Sie darauf, dass Firmengeräte keine Hinweise auf die Institution oder den Benutzenden enthalten.

6. SICHERE KOMMUNIKATION

- Nutzen Sie einen Messenger, über den die Kommunikation verschlüsselt abläuft, wie etwa Signal oder Threema

WIE SIE IHR SMARTPHONE SCHÜTZEN

DIGITAL SICHER NRW

7. VERWENDUNG VON WERBEBLOCKERN

- Auch angezeigte Werbung kann schadhaften Code enthalten. Davor können regelmäßig aktualisierte Werbeblocker schützen.
- Greifen Sie auch zum Schutz vor „Tracking“ auf Werbeblocker zurück.
- Werbeblocker leisten einen wichtigen Beitrag zum Schutz Ihrer Daten und Ihrer Geräte.

8. SENSIBILISIERUNG FÜR GEFÄHRDUNGEN

- Ermöglichen Sie Ihren Mitarbeitenden die regelmäßige Teilnahme an Schulungen zu Sicherheitsaspekten.

- Bleiben Sie stets achtsam!
- Seien Sie immer misstrauisch!

NUTZUNGSSZENARIEN – PRIVAT ODER DIENSTLICH?

DIGITAL SICHER NRW

VOM UNTERNEHMEN GESTELLTE GERÄTE

Vorteile:

- Das Unternehmen hat volle Kontrolle (bspw. bei Verlust) über die Smartphones.
- Rechtliche Fragestellungen werden stark vereinfacht.
- Software-Lizenzierung wird vereinfacht.

Nachteile:

- Anschaffungskosten und Verwaltungsaufwand
- Begrenzt geeignet für Externe

BRING YOU OWN DEVICE – DIE BETRIEBLICHE NUTZUNG PRIVATER GERÄTE

Vorteile:

- Die Flexibilität und Mobilität der Mitarbeitenden wird gesteigert.
- Es wird eine größere Auswahl an Gerätetypen ermöglicht.
- Die Kosten für Hard- und Software werden gesenkt.

Nachteile:

- Das Unternehmen hat keine oder nur eingeschränkte Kontrolle über Geräte.
- Die Sicherheit und DSGVO-Konformität der Firmen-Daten ist nur eingeschränkt gewährleistet.
- Das Risiko für Datenlecks ist höher.
- Die Geräte- und App-Sicherheit ist ggfs. nicht gegeben.

SICHERN SIE JETZT IHR SMARTPHONE AB!

Smartphones sind ein fester Bestandteil unserer alltäglichen Kommunikation. Auf ihnen werden persönliche Dokumente gespeichert und sie sind oft mit sensiblen Bereichen wie Bankkonten und Aktiendepots verknüpft. Sie sind im Grunde echte Geheimnisträger.

Wie Sie Ihr Smartphone sicher konfigurieren, zeigen wir Ihnen Schritt für Schritt in unserer Videoanleitung, die Sie über den QR-Code erreichen!

Erklärvideo Smartphone

DIGITAL SICHER NRW
Kompetenzzentrum für Cybersicherheit in der Wirtschaft

Beauftragt vom Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen