

# MAKING SOCIAL CARE TECHNOLOGIES ACCESSIBLE TO ALL

## Topic 1.4. Sichere und einfache Nutzung mobiler Geräte

*Gefördert durch die Europäische Union. Die geäußerten Ansichten und Meinungen sind jedoch ausschließlich die der Autor:innen und spiegeln nicht unbedingt die der Europäischen Union oder der Europäischen Exekutivagentur für Bildung und Kultur (EACEA) wider. Weder die Europäische Union noch die EACEA können dafür verantwortlich gemacht werden.*

# Inhalt

1. Einführung
2. Einfache Nutzung mobiler Geräte
3. Sichere Nutzung mobile Geräte

# 1. Einführung

- 1.1. Überblick
- 1.2. Zielgruppe
- 1.3. Ausbildungsziele
- 1.4. Format und Indikatoren

# 1. Einführung



## 1.1. Überblick

### Worum geht es in diesem Training?

Das Training zielt darauf ab, die Fähigkeiten und Kenntnisse von Pflegefachkräften für den sicheren und effektiven Einsatz mobiler Geräte bei der täglichen Arbeit zu verbessern. Es bietet ihnen einfach umsetzbare Maßnahmen, Tools und Best Practices. Um eine möglichst effektive Nutzung des erworbenen Wissens in der Praxis zu gewährleisten, ist es unerlässlich, auf Erfahrungen und vorhandenen Ressourcen der Zielgruppe aufzubauen und etablierte Tools zu nutzen/vertiefen.

### Warum ist das notwendig?

Die transnationale Erhebung des SociALL-Projekts hat gezeigt, dass mobile Geräte in allen Ländern zu einem wichtigen Thema geworden sind. Die meisten Pflegefachkräfte nutzen sie bereits für den persönlichen Gebrauch und sind mit deren Funktionalität, Betriebssystem, Anwendungen etc. weitgehend vertraut. Dieses Training bietet ihnen die Möglichkeit, Aufgaben im Arbeitsalltag schneller und einfacher zu erledigen, sich sicherer zu fühlen und somit produktiver zu werden.

# 1. Einführung

## 1.2. Zielgruppe



### Für wen ist dieses Training?

Zielgruppe sind alle im Pflegebereich tätigen Fachkräfte, aber auch Management und Hilfspersonal. Diese Personen engagieren sich in der Bereitstellung von Pflegediensten und können ihre Fähigkeiten zur Zusammenarbeit und Kommunikation mithilfe digitaler Tools zum Nutzen ihrer Patient:innen verbessern.

### Was sind die Voraussetzungen?

Teilnehmende sollten mobile Geräte regelmäßig nutzen, zumindest für den persönlichen Gebrauch, und über grundlegende praktische Erfahrungen mit Basisfunktionen und -befehlen verfügen. Um den Zugang zum digitalen Lernen und idealerweise zur eigenständigen Weiterbildung zu schaffen, werden sie durch Präsenzworkshops begleitet. Zur Vertiefung und Festigung werden Online-Workshops, Online-Coachings und Lernmaterialien in verschiedenen Formen angeboten.

# 1. Einführung

## 1.3. Ausbildungsziele

### Was kann mit diesem Training erreicht werden?

- Verständnis der **Bedeutung der Nutzung mobiler Geräte** im Pflegebereich
- Gezielte Anwendung von **Tipps und Tricks** speziell für den **Einsatz mobiler Geräte vor Ort**
- Erlernen und Umsetzen **grundlegender Sicherheitsmaßnahmen** , um die digitale Sicherheit zu erhöhen

### Was wird sich ändern?

- **Produktivitätssteigerung** bei der Umsetzung von Aufgaben durch **gezielten Einsatz mobiler Geräte** im Arbeitsbereich
- **Erhöhen** des **Ausmaßes** der über mobile Geräte realisierten **Aufgaben und Kommunikation**
- **Vertrauen in die eigene Fähigkeit gewinnen**, komplexe Probleme lösen und über mobile Geräte zusammenarbeiten
- **Verbessern der digitale Sicherheit** auf Mobilgeräten und Reduktion des Risikos von Sicherheitsvorfällen

# 1. Einführung

## 1.4. Format und Indikatoren

### Wie wird das Training durchgeführt?

Um einen Zugang zu digitalem Lernen und im Idealfall in weiterer Folge selbständiger Weiterbildung zu schaffen, braucht es ein Hinführen und eine Aktivierung der Teilnehmenden über Präsenz-Workshops. In weiterer Folge ist es sehr sinnvoll Online-Workshops, Online Coachings Lernunterlagen in unterschiedlicher Form zur Vertiefung und Festigung digital/online zur Verfügung zu stellen.

### Wie ist das Training organisiert?

- **Zwei Präsenz-Workshops** a 3-4 Einheiten
- Max. **10 Teilnehmende**/Workshop
- Eine **Teilnahme an allen Workshops** wird empfohlen, um **Kontinuität** und **maximalen Lernerfolg** zu erzielen

## 2. Workshop Einfache Nutzung mobiler Geräte

- 2.1. Einführung und allgemeine Informationen
- 2.2. Praktische Anwendung, hilfreiche Tipps and Tricks



# 2. Einfache Nutzung mobiler Geräte

## 2.1. Einführung und allgemeine Informationen

### Gerätehersteller und Betriebssysteme

#### Betriebssystem

Das Betriebssystem ist die Basissoftware, mit der ein Computer, Smartphone oder Tablet gesteuert wird. k

Die gängigsten Betriebssysteme sind



Android - Google, Samsung, LG, HTC, Huawei, etc.

iOS - Apple, iPhone, iPad

Windows - Nokia, Microsoft

# 2. Einfache Nutzung mobiler Geräte



## 2.1. Einführung und allgemeine Informationen

### Begriffserklärungen

#### **Android**

Android ist das Betriebssystem von Google.

#### **Apps**

„Apps“ (engl. Kurzform für „Applications“ = Anwendungen) sind Programme für Smartphones und Tablets, die den Alltag erleichtern oder der Unterhaltung dienen. Es gibt kostenlose und kostenpflichtige Apps.

#### **App Shop**

Shop (Geschäft) für Apps.

Die wichtigsten App Shops: App Store (Apple), Play Store (Android), Phone Store (Windows).

#### **Backup**

Sicherungskopie

#### **Bildschirmsperre**

Die Bildschirmsperre verhindert den Zugriff auf das Smartphone und schaltet sich automatisch nach einer bestimmten Zeit ein, wenn das Gerät nicht benutzt wurde. Zum Entsperren existieren unterschiedliche Möglichkeiten: PIN-Eingabe, Musterentsperrung, Fingerabdruckscanner, Gesichtserkennung.

# 2. Einfache Nutzung mobiler Geräte



## 2.1. Einführung und allgemeine Informationen

### Begriffserklärungen

#### **Bluetooth**

Bluetooth bezeichnet eine kabellose Übertragungstechnik zwischen Geräten über kurze Distanz per Funk.

#### **Cloud Dienste**

Unter Cloud-Dienste versteht man Dienste, welche über das Internet zur Verfügung gestellt werden, z.B. Speicherplatz, Rechenleistung oder Anwendersoftware.

#### **GPS**

GPS steht für Globales Positionsbestimmungssystem, welches mit Hilfe von Satellitensignalen zur Navigation oder Standortbestimmung genutzt wird.

#### **IMEI Nummer**

15-stellige internationale Seriennummer des Smartphones (IMEI-Nummer: International Mobile Station Equipment Identity).

#### **iOS**

iOS ist das Betriebssystem von Apple.

# 2. Einfache Nutzung mobiler Geräte



## 2.1. Einführung und allgemeine Informationen

### Begriffserklärungen

#### **Online Banking**

Die Abwicklung von Bankgeschäften über das Internet wird Online-Banking oder Electronic Banking (eBanking) genannt.

#### **Phishing**

Versuch auf betrügerische Weise per E-Mail oder über Websites an persönlichen Daten, Kontodaten oder Geld zu gelangen.

#### **PIN**

Persönliche Identifikationsnummer.

#### **SIM Karte**

Chipkarte in verschiedenen Formaten, die in das Smartphone oder Tablet eingelegt wird. Dadurch ist die eindeutige Identifikation möglich, ähnlich wie ein Mitgliedsausweis.

# 2. Einfache Nutzung mobiler Geräte

## 2.1. Einführung und allgemeine Informationen

### Begriffserklärungen

#### **Smartphone**

Ein Smartphone (ugs. manchmal auch „Wischhandy“ genannt) ist ein Mobiltelefon zum Telefonieren, Versenden und Empfangen von Kurznachrichten. Darüber hinaus bietet ein Smartphone aber noch weitere Funktionen mit Hilfe von Apps, wie z.B. E-Mail-Zugriff, Internet, Fotos, etc.

#### **Tablet**

Ein Tablet ist ein mobiles Gerät ähnlich einem Smartphone, jedoch mit einem größeren Display. Ein weiterer wesentlicher Unterschied besteht darin, dass nicht immer eine SIM-Karte verwendet wird, sondern dass für die Nutzung des Internets WLAN erforderlich ist.

#### **Updates**

Ein Update ist eine Aktualisierung einer gespeicherten Programmversion.

#### **WLAN / WiFi**

WLAN steht für „Wireless Local Area Network“, auch Wifi genannt. Ein lokales drahtloses Funknetz, das den Zugang zum Internet ermöglicht.

# 2. Einfache Nutzung mobiler Geräte

## 2.1. Einführung und allgemeine Informationen

### Einstellungen App

Die App mit dem Zahnradsymbol bietet viele Einstellungen für Mobilgeräte



- ✓ Das Gerät besser einrichten (z.B. Anzeigeneinstellungen, Ton , einfache Bedienung)
- ✓ Verbindungseinstellungen (WLAN, Bluetooth, Hotspot... verwenden)

## 2. Einfache Nutzung mobiler Geräte

### 2.1. Einführung und allgemeine Informationen

#### Mitteilungszentrale und Schnellzugriff



# 2. Einfache Nutzung mobiler Geräte

## 2.1. Einführung und allgemeine Informationen

### Mitteilungszentrale und Schnellzugriff

Auf der rechten Seite:

- Zeit
- Akku-Stand
- Aktuelle Verbindungen (Mobilfunkempfang, WLAN, Bluetooth...)

Auf der linken Seite werden Symbole angezeigt, wenn das Betriebssystem oder einzelne Apps Benachrichtigungen bereithalten.

Zum Beispiel:

- Google Play Store: App-Updates sind verfügbar oder wurden installiert
- WhatsApp / Email: Sie haben eine neue Nachricht
- Phone: Entgangener Anruf
- Android System: Betriebssystem-Update ist verfügbar
- ...



# 2. Einfache Nutzung mobiler Geräte

## 2.1. Einführung und allgemeine Informationen

### Zugang zur Mitteilungszentrale



Um auf das Benachrichtigungscenter zugreifen zu können, muss der Bildschirm entsperrt sein. Wischen Sie dann von oben nach unten, beginnend außerhalb des Touchscreens. Möglicherweise müssen Sie ein zweites Mal wischen, um das Benachrichtigungscenter vollständig anzuzeigen.

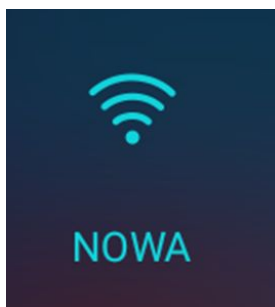
## 2. Einfache Nutzung mobiler Geräte

### 2.1. Einführung und allgemeine Informationen

#### Symbole der Mitteilungszentrale

Je nach Gerätehersteller und Versionsnummer des Betriebssystems sind hier unterschiedliche Symbole zu sehen und Funktionen ein- und ausschaltbar. Wird eine Funktion aktiviert, verändert sich das Symbol entweder in der Farbe oder in der Helligkeit.

#### Hier einige Beispiele:



#### WLAN

In diesem Fall ist der Verbindungstyp WLAN aktiv und das Gerät ist mit dem WLAN-Netzwerk „NOWA“ verbunden. WLAN steht für „Wireless Local Area Network“. lokale (Internet-)Verbindung“. Ein solcher Internetzugang ist oft in Geschäften, Bars und Hotels verfügbar; Für den Zugriff benötigen Sie häufig ein Passwort.

# 2. Einfache Nutzung mobiler Geräte

## 2.1. Einführung und allgemeine Informationen

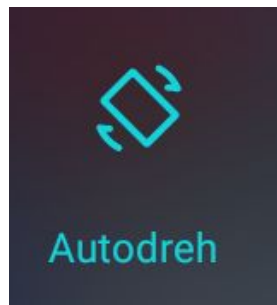
### Symbole des Mitteilungszentrale



#### Bluetooth

Auf diesem Bild ist Bluetooth deaktiviert.

Bluetooth ist ebenfalls eine Art Funkverbindung, allerdings zwischen zwei „Bluetooth-fähigen“ Geräten (zum Beispiel einem Kopfhörer mit einem Smartphone).



#### Automatische (Bildschirm-)Rotation

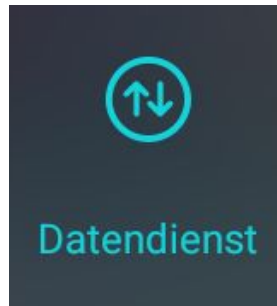
Wenn diese Funktion aktiviert ist, dreht sich der Bildschirm vom Hoch- ins Querformat, wenn Sie Ihr Gerät horizontal halten, und umgekehrt.

Sollte dies störend sein, kann man die Ansicht durch Deaktivieren sperren, dann erscheint „Portrait“ für den Portraitmodus.

# 2. Einfache Nutzung mobiler Geräte

## 2.1. Einführung und allgemeine Informationen

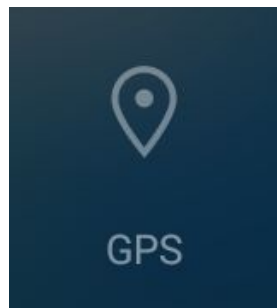
### Symbole des Mitteilungszentrale



#### **Mobile Daten**

Wenn eine SIM-Karte eines Mobilfunkanbieters in Ihr Gerät eingelegt ist, wird dieses Symbol angezeigt.

In Nicht-EU-Ländern oder wenn Ihr Datenguthaben bereits aufgebraucht ist, ist es wahrscheinlich besser, diese Funktion zu deaktivieren. Sie erhalten dann weiterhin Anrufe und SMS, jedoch keine E-Mails und Nachrichten von Messenger-Apps wie WhatsApp mehr.



#### **GPS (global positioning system)**

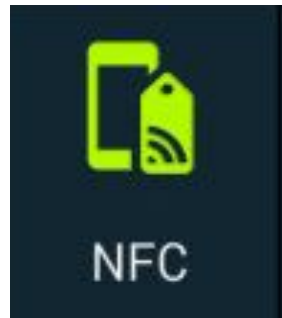
Wenn diese Funktion aktiviert ist, kann Ihr Gerät mithilfe von Satelliten seine Position bestimmen. Dies kann hilfreich sein, wenn Sie mit einer Karten-App durch eine unbekannte Region navigieren.

Auch ohne GPS wird die Position Ihres Geräts immer ermittelt, beispielsweise durch die Nähe zu verschiedenen Funktürmen Ihres Providers.

# 2. Einfache Nutzung mobiler Geräte

## 2.1. Einführung und allgemeine Informationen

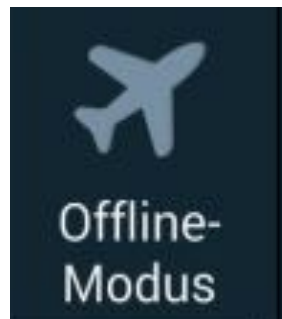
### Symbole des Mitteilungszentrale



#### **NFC (near field communication - Nahfeldkommunikation)**

Bei dieser Art der Verbindung handelt es sich um eine relativ neue Technologie, die Sie aus dem Alltag bereits von Geldautomatenkassen kennen: Bei kleinen Beträgen kann die Bankomatkarte zum Bezahlen einfach auf das Lesegerät gelegt werden.

Auch ein neues Smartphone oder Tablet verfügt mittlerweile über einen Chip, der, verbunden mit einem geeigneten Empfangsgerät, durch einfaches Berühren Informationen austauschen kann.



#### **Flugmodus**

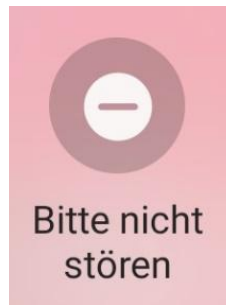
Wenn Sie diesen Modus aktivieren, werden die Mobilfunk- und Datenverbindungen getrennt. Das bedeutet, dass Sie weder Anrufe noch neue Nachrichten erhalten und nicht im Internet surfen können. Es ist weiterhin möglich, die „Offline“-Funktionen Ihres Geräts zu nutzen (Notizen, Musik hören, viele Apps und Spiele nutzen).

Bei Flugreisen werden Sie aus Sicherheitsgründen gebeten, diese Maßnahme zu nutzen.

# 2. Einfache Nutzung mobiler Geräte

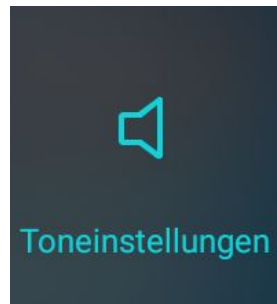
## 2.1. Einführung und allgemeine Informationen

### Symbole des Mitteilungszentrale



#### **Bitte nicht stören**

Wenn Sie diesen Modus aktivieren, werden Anrufe und Nachrichten (SMS, WhatsApp, ...) stummgeschaltet. Anrufer werden direkt an die Voicemail weitergeleitet und erscheinen als verpasste Anrufe. In den Einstellungen können Sie Ausnahmen (wer durchkommt) und einen Tagesplan festlegen.



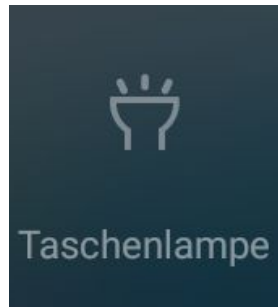
#### **Toneinstellungen**

Wenn Sie auf dieses Symbol tippen, wird Ihr Klingelton stummgeschaltet. Durch erneutes Tippen wird auch die Vibration deaktiviert. Ideal für einen Konzert- oder Kinobesuch sowie für einen ungestörten Schlaf!

Durch langes Tippen gelangen Sie direkt zu allen Lautstärkeinstellungen. Beispielsweise können Videos und Musik (Medien) stummgeschaltet werden, während eingehende Anrufe weiterhin klingeln.

## 2. Einfache Nutzung mobiler Geräte

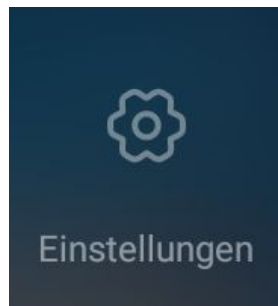
### Symbole des Mitteilungszentrale



#### **Taschenlampe**

Dieses Symbol aktiviert die Blitzfunktion Ihrer Telefonkamera, bis Sie erneut darauf tippen.

Mit einem Smartphone hat man immer eine Taschenlampe dabei, um im Dunkeln ein Schlüsselloch zu finden oder einen Weg besser auszuleuchten.



#### **Einstellungen**

Obwohl Sie die Einstellungen-App Ihres Geräts woanders finden können, ist der schnelle Zugriff über das Benachrichtigungscenter dennoch praktisch.

## 2. Einfache Nutzung mobiler Geräte

### 2.2. Praktische Anwendung, hilfreiche Tipps and Tricks

#### Nutzen Sie die Spracheingabe (Speech-to-Text) und den Sprachassistenten

Das Mikrofonsymbol befindet sich auf der Tastatur oder an anderer Stelle in Apps und ermöglicht es Ihnen, Texte zu diktieren, anstatt sie einzutippen.





# 2. Einfache Nutzung mobiler Geräte



## 2.2. Praktische Anwendung, hilfreiche Tipps and Tricks

### App Installation

Voraussetzung: Google-Konto (Android) oder Apple-ID

- Entsperren Sie Ihr Gerät und öffnen Sie den Desktop
- Tippen Sie auf den Play Store (Android) oder App Store (Apple)
- Bei der Eröffnung des Stores werden zunächst aktuelle und neue Apps in verschiedenen Kategorien empfohlen
- Um nach einer bestimmten App zu suchen, tippen Sie auf das Suchsymbol (Android: Suchfeld oben, Apple: Suche unten)
- Geben Sie den App-Namen oder einen Suchbegriff ein

# 2. Einfache Nutzung mobiler Geräte



## 2.2. Praktische Anwendung, hilfreiche Tipps and Tricks

### App Installation

- Wenn Sie einen allgemeinen Suchbegriff eingegeben haben (z. B.: Memory-Spiel), erscheint eine Ergebnisliste und Sie können anhand von Sternebewertungen und Beschreibungen der Apps entscheiden, welche Ihnen gefällt
- Wenn Sie sich für eine App entschieden haben, tippen Sie auf „Installieren“ (Android) oder „Herunterladen“ und geben Sie dann Ihr Apple-ID-Passwort (Apple) ein
- Anschließend wird die App installiert. Sobald dies abgeschlossen ist, kann die App geöffnet werden
- Wenn Sie eine App zum ersten Mal starten, werden Sie möglicherweise aufgefordert, bestimmte Berechtigungen zu erteilen. Nehmen Sie sich einen Moment Zeit, um dies durchzulesen, um zu verstehen, welche Informationen die App von Ihrem Tablet verwendet oder auf welche Gerätesensoren sie zugreifen möchte

# 2. Einfache Nutzung mobiler Geräte

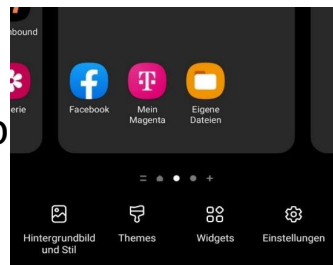
## 2.2. Praktische Anwendung, hilfreiche Tipps and Tricks

### Widgets

Der englische Begriff „Widget“ ist ein Begriff, der sich aus „window“ für Fenster und „gadget“ für Zubehörgerät zusammensetzt. Dabei handelt es sich um grafische Fenster auf dem Startbildschirm des Smartphones, die einen Link zu einer App enthalten.

Im Gegensatz zu den App-Icons ist die grafische Form variabel. Darüber hinaus bietet ein Widget immer „mehr“ Informationen. Das Wetter-Widget zeigt beispielsweise die aktuelle Wetterlage und Temperatur am eingestellten Standort an.

Um ein neues Widget hinzuzufügen, wischen Sie mit zwei Fingern auf Ihrem entsperrten Bildschirm nach innen, als würden Sie ein Bild verkleinern. Unten erscheint nun eine Schaltfläche, die Ihnen alle auf dem Gerät verfügbaren Widgets anzeigt:



Widget tippen o

Ihrem Gerät müssen Sie lediglich auf das gewünschte

Widget tippen o gewünschte Stelle auf dem Bildschirm

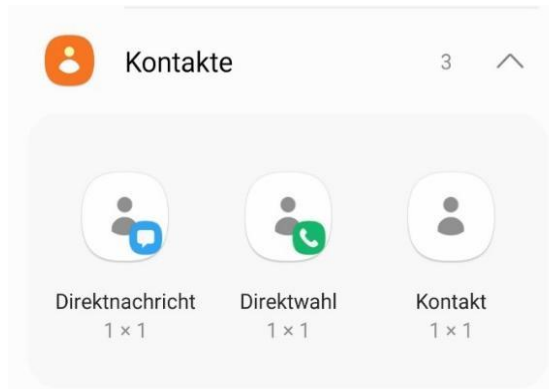
ziehen.

# 2. Einfache Nutzung mobiler Geräte

## 2.2. Praktische Anwendung, hilfreiche Tipps and Tricks

### Widgets

Zu den praktischen Widgets gehören neben dem Wetter, der Suchleiste und



-Widgets:

n Sie Personen aus Ihrem Adressbuch direkt auf dem

ntweder als Kurzwahl (ein Tipp darauf startet den

Anruf sofort), als

Person startet) oder als

Verknüpfung

zum

Kontakt

in der

Einige Widgets sind beim Kauf des Geräts verfügbar. Weitere können Sie über den Playstore installieren.

Dazu installieren Sie einfach die zugehörige App.

# 2. Einfache Nutzung mobiler Geräte

## 2.2. Praktische Anwendung, hilfreiche Tipps and Tricks

### Routenplanung und Navigation mit Ihrem Smartphone per Karten-App (für Pkw und öffentliche Verkehrsmittel)

#### Batterie



- ✓ Verbrauch prüfen (Stromfresser-Apps deinstallieren)
- ✓ Bei Bedarf Energiesparmodus aktivieren, Powerbank nutzen

#### Benachrichtigungen verwalten



- ✓ Entfernen Sie ggf. App-Berechtigungen

## 3. Workshop Sichere Nutzung mobile Geräte

- 3.1. Browser Einstellungen
- 3.2. Cookies
- 3.3. Viren und Trojaner
- 3.4. Tipps, um Mobilgeräte sicher zu machen
- 3.5. Hilfreiche Links

# 3. Sichere Nutzung mobile Geräte



**Mobile Geräte sind mittlerweile treue Begleiter in vielen Lebenslagen.**

**Wir speichern private Kontaktinformationen, unsere Termine, halten unsere Erlebnisse in Bild und Ton fest, kommunizieren über verschiedene Apps und erledigen unsere Bankgeschäfte online.**

**Viele persönliche Daten sind auf unseren Geräten gespeichert und diese gilt es zu schützen.**

# 3. Sichere Nutzung mobile Geräte

## 3.1. Browser Einstellungen

In vielen Apps kann man Einstellungen für die verschiedensten Funktionen treffen, in einem Browser können Sie zum Beispiel die Startseite ändern, Cookies aktivieren oder deaktivieren und gespeicherte Passwörter löschen.

Die Einstellungen der Browser App finden Sie vermutlich in dem Menü das hinter dem Symbol drei Striche oder drei Punkte versteckt ist.





# 3. Sichere Nutzung mobile Geräte

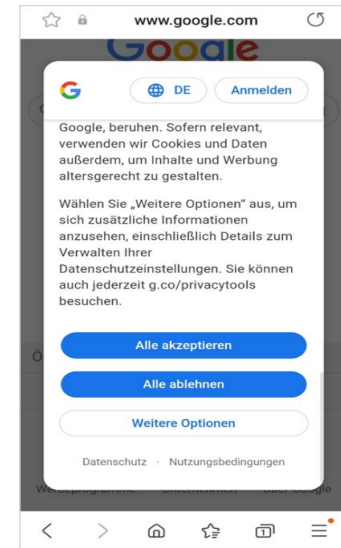
## 3.2. Cookies

### Cookies

Ein Cookie ist in seiner ursprünglichen Form eine Textdatei auf einem Computer. Sie enthält typischerweise Daten über besuchte Webseiten, die die Browser-Software beim Surfen im Internet speichert. Da hier etwas auf Ihrem Gerät abgespeichert wird, werden Sie über lästige Pop-Up-Fenster darüber informiert.



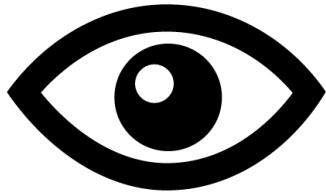
- ✓ Wenn die Option besteht, alle Cookies abzulehnen, können Sie diese auswählen. Alle wesentlichen Funktionen der Website bleiben weiterhin aktiv.



# 3. Sichere Nutzung mobile Geräte

## 3.2. Cookies

### Cookies



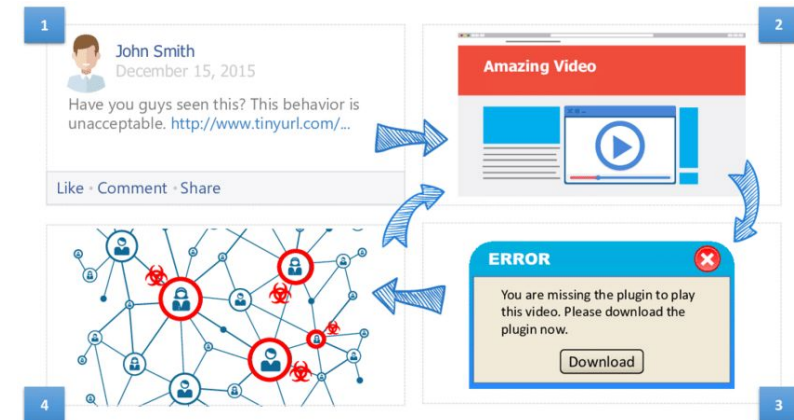
- Es gibt funktionelle Cookies, die zum Beispiel dazu dienen, dass man sich beim wiederholten Besuch einer verschlüsselten Seite nicht erneut anmelden muss. Solche Cookies helfen Internetseiten auch, sich Informationen über Ihren Besuch zu merken wie beispielsweise Ihre bevorzugte Sprache und andere Einstellungen. So finden Sie sich auf der Website schneller zurecht und nutzen sie effektiver, wenn Sie sie das nächste Mal aufrufen.
- Andere Cookies werden für die Statistik der besuchten Internetseite und für Marketing und PR-Zwecke verwendet. Diese haben für Sie persönlich keinen Nutzen.
- Darüber hinaus gibt es auch Tracking-Cookies, die sich nicht auf eine bestimmte Internetseite beschränken, sondern Ihr Verhalten beim Surfen verfolgen um daraus Informationen über Sie zu sammeln und Sie besser als Konsument:in einschätzen zu können. Zum Schutz Ihrer Privatsphäre können Sie, wo möglich, diese ablehnen.

# 3. Sichere Nutzung mobile Geräte

## 3.3. Viren and Trojaner

### Internetseiten / Google / Social Media

- Um sich vor Schadsoftware zu schützen, besuchen Sie keine unseriösen Websites, die Ihnen mit zahlreichen Pop-up-Fenstern dubiose Apps verkaufen oder Sie zur Teilnahme an Gewinnspielen verleiten wollen. Ziel ist es oft, Schadsoftware zu installieren oder Ihre persönlichen Daten auszuspionieren.
- Seien Sie vorsichtig in sozialen Netzwerken wie Facebook und WhatsApp. Tippen Sie nicht vorschnell auf Links oder Anwendungen, die Ihnen besonders spektakuläre Videos oder Fotos, Schnäppchen oder Gutscheine versprechen.



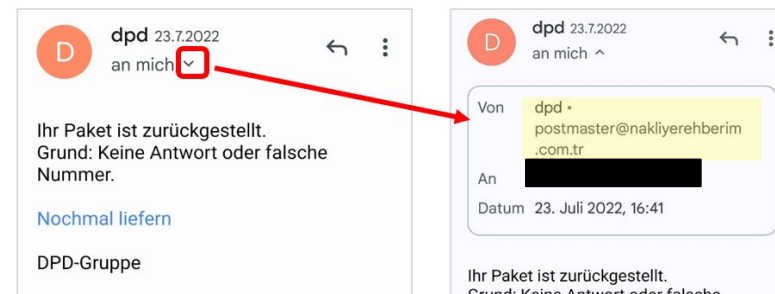
# 3. Sichere Nutzung mobile Geräte

## 3.3. Viren and Trojaner

### E-Mail

Ebenso wichtig ist es, keine Dateianhänge in E-Mails oder Chatnachrichten von Personen oder Unternehmen zu öffnen, die Sie nicht kennen. Kriminelle versuchen häufig mit betrügerischen E-Mails (z. B. gefälschten Rechnungen), an Ihr Geld oder Ihre Kontoinformationen zu gelangen – **Phishing**.

- ✓ Überprüfen Sie immer die E-Mail-Adresse des/der Absender:in, bevor Sie auf Schaltflächen oder Links in der E-Mail klicken oder Anhänge öffnen.



- ✓ Markieren Sie betrügerische E-Mails als Spam und löschen Sie sie sofort

# 3. Sichere Nutzung mobile Geräte



## 3.3. Viren and Trojaner

### E-Mail

Für Registrierungen, Bestellungen etc. im Internet können Sie anstelle Ihrer Hauptadresse eine zusätzliche E-Mail-Adresse verwenden. Erstellen Sie dazu eine kostenlose E-Mail-Adresse bei Anbietern wie Gmail oder gmx, bei der es nicht so störend ist, wenn Ihr Posteingang mit dubiosen E-Mails überschwemmt wird.

**Jedes Mal, wenn Sie Ihre E-Mail-Adresse online angeben, erhöht sich das Risiko, unerwünschte und damit betrügerische E-Mails zu erhalten.**

# 3. Sichere Nutzung mobile Geräte

## 3.3. Viren and Trojaner

### Betriebssystem und Apps aktuell halten

- Generell sollten Sie Apps nur aus dem Playstore installieren, da andernfalls nicht ausgeschlossen werden kann, dass es sich um versteckte Schadsoftware handelt.
- Viele Kriminelle nutzen Sicherheitslücken in Betriebssystemen und Apps aus, um gezielte Attacken gegen ihre Opfer zu starten. Dabei spielt ihnen in die Hand, dass viele Internetnutzer:innen ihre Software nicht aktuell halten. Das obwohl es bereits Aktualisierungen gibt, die die Sicherheitsmängel beheben.

# 3. Sichere Nutzung mobile Geräte

## 3.3. Viren and Trojaner

### Betriebssystem und Apps aktuell halten

Manche Apps sind wahre Datenspione – seien Sie skeptisch, wenn etwa eine simple Taschenlampen-App Zugriffsberechtigungen auf Ihren aktuellen Standort, Ihr Telefonbuch etc. haben möchte. Diese Informationen sollten für die Nutzung einer Taschenlampe nicht relevant sein!



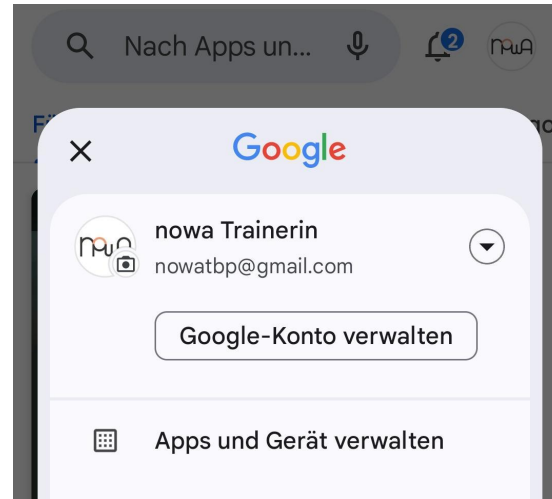
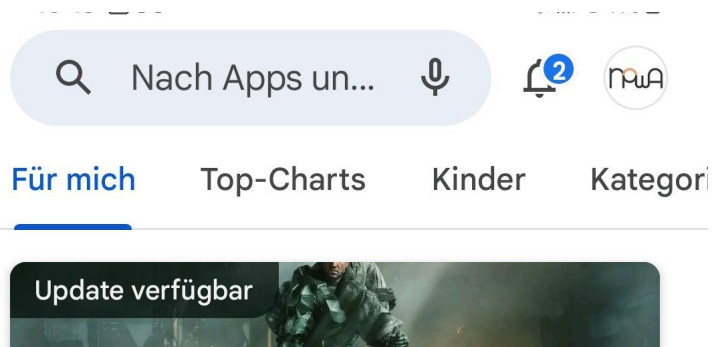
- ✓ Führen Sie regelmäßige App-Updates durch/löschen Sie nicht mehr verwendete Apps
- ✓ Normalerweise sendet Ihr Betriebssystem eine Benachrichtigung, sobald Updates verfügbar sind


Um Apps manuell zu aktualisieren, öffnen Sie den Play Store (Android) oder den App Store (iOS).

# 3. Sichere Nutzung mobile Geräte

## 3.3. Viren and Trojaner

### Manuelles Aktualisieren von Apps im PlayStore



 Updates verfügbar  
⚠️ 10 ausstehende Updates  
[Alle aktualisieren](#) [Details anse](#)



# 3. Sichere Nutzung mobile Geräte

## 3.3. Viren and Trojaner

### Anti-Viren-App benutzen

Um Schadsoftware entdecken und beseitigen zu können, ist es empfehlenswert, ein Anti-Viren-App zu installieren oder in den Einstellungen zu aktivieren. Das hat den Vorteil, dass durch dieses im Hintergrund sämtliche Prozesse untersucht und Gefahren erkannt sowie beseitigt werden können. Alle Virenschutz-Apps bieten eine automatische Aktualisierung an, die Sie unbedingt nutzen sollten.



# 3. Sichere Nutzung mobile Geräte

## 3.4. Tipps, um Mobilgeräte sicher zu machen

### Mobilgerät sperren (Einstellungen App)



- ✓ Durch die Verwendung von PIN-Passwörtern, -mustern oder biometrischen Entsperroptionen werden die Daten auf Ihrem Mobilgerät geschützt
- ✓ Installieren Sie eine Bildschirmsperre, um Ihr Gerät vor unbefugtem Zugriff auf Einstellungen und Anwendungen zu schützen

### Sichere Passwörter verwenden



- ✓ Sichere Passwörter bestehen aus einer Kombination aus Buchstaben (vorzugsweise Groß- und Kleinbuchstaben), Zahlen und Sonderzeichen
- ✓ Je länger das Passwort, desto sicherer ist es (besser 14 als 8 Zeichen)
- ✓ Verwenden Sie mindestens zwei verschiedene: ein sehr sicheres Passwort zum Schutz Ihres E-Mail-Kontos und eines oder mehrere für alle anderen Anwendungen
- ✓ Verwenden Sie eine Passwort-Manager-App, um mehrere Passwörter sicher zu verwalten und sich diese nicht merken zu müssen

# 3. Sichere Nutzung mobile Geräte

## 3.4. Tipps, um Mobilgeräte sicher zu machen

**Halten Sie Ihre persönlichen Zugangsdaten (z. B. PIN, Passwörter) geheim**

**Seien Sie vorsichtig, wenn Sie öffentliche Geräte verwenden**



- ✓ Wenn Sie sich auf dem Gerät einer anderen Person bei einer bestimmten Website (z. B. E-Mail-Anbieter, soziales Netzwerk) angemeldet haben, sollten Sie sich immer abmelden
- ✓ Lassen Sie sich bei der Eingabe persönlicher Daten nicht von Fremden über die Schulter schauen

**Updates installieren**

Updates liefern neue Funktionen und schließen Sicherheitslücken, das Betriebssystem benachrichtigt Sie, wenn Updates verfügbar sind.



- ✓ Installieren Sie Updates sofort oder
- ✓ Aktivieren Sie automatische Updates auf dem Gerät

# 3. Sichere Nutzung mobile Geräte

## 3.4. Tipps, um Mobilgeräte sicher zu machen

Laden Sie Apps nur aus dem offiziellen App-Shop Ihres Anbieters herunter

### Überprüfen Sie die Berechtigungen

Apps benötigen unterschiedliche Berechtigungen (z. B.: Zugriff auf Mikrofon, Kontakte, Internet)



✓ Überprüfen und passen Sie die Berechtigung für Ihre Apps an

### Dienste deaktivieren

Mobile Geräte können über verschiedene Dienste Daten austauschen. Apps können beispielsweise über GPS- und WLAN-Netzwerke den Standort bestimmen und Bewegungsprofile erstellen.



✓ Aktivieren Sie WLAN, Bluetooth und GPS nur bei Bedarf

# 3. Sichere Nutzung mobile Geräte

## 3.4. Tipps, um Mobilgeräte sicher zu machen

### Gehen Sie sorgfältig mit den Daten Ihrer Patient:innen und Ihrer Organisation um



- ✓ Übertragen Sie keine Daten über öffentliche WLAN-Netzwerke (z. B. Gesundheits-Apps).
- ✓ Berücksichtigen Sie die DSGVO und handeln Sie entsprechend

### Regelmäßige Backups

Wenn Sie Ihr Mobilgerät verlieren, es gestohlen wird oder kaputt geht, sind alle Ihre Daten verloren – es sei denn, Sie sichern es regelmäßig.



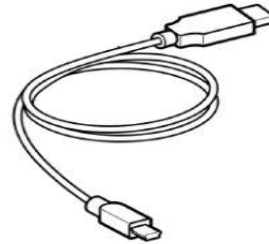
- ✓ Übertragen Sie Ihre Daten per Kabel auf einen Computer
- ✓ Nutzen Sie einen Cloud-Dienst zur Datensicherung und aktivieren Sie die automatische Synchronisierung für kritische Daten/Ordner

# 3. Sichere Nutzung mobile Geräte

## 3.4. Tipps, um Mobilgeräte sicher zu machen

### Regelmäßige Backups

Wenn Sie Ihr Mobilgerät verlieren, es gestohlen wird oder kaputt geht, sind alle Ihre Daten verloren – es sei denn, Sie sichern es regelmäßig.



**Tipps**

- ✓ Übertragen Sie Ihre Daten per Kabel (USB) auf einen Computer. Die Einstellungen werden auf dem Bildschirm des Mobilgeräts angezeigt – erlauben Sie den Zugriff per Computer
- ✓ Nutzen Sie einen Cloud-Dienst zur Datensicherung und aktivieren Sie die automatische Synchronisierung für kritische Daten/Ordner (Anbieter: Dropbox, Google, Apple, Microsoft,...)

# 3. Sichere Nutzung mobile Geräte

## 3.4. Tipps, um Mobilgeräte sicher zu machen

### Installieren von Anti-Virus Software



- ✓ Halten Sie die Antiviren-App stets auf dem neuesten Stand, da neue Bedrohungen sonst nicht erkannt und abgewehrt werden können

### Aktivieren des Diebstahlschutzes

Es gibt keine App, die Ihr Mobilgerät vor Diebstahl schützt, aber es gibt Programme, die Ihnen dabei helfen, es leichter zu finden. Diese „Anti-Diebstahl-App“ kann das verlorene oder gestohlene Gerät aus der Ferne orten, sperren oder sogar die Daten löschen. Es ist häufig in Antivirensoftware enthalten.



- ✓ Installieren oder aktivieren Sie die Anti-Diebstahl-App/-Funktion und aktivieren Sie GPS auf dem Gerät
- ✓ Notieren Sie sich die Seriennummer (IMEI-Nummer) Ihres Smartphones, im Falle eines Diebstahls müssen Sie eine Anzeige bei der Polizei erstatten

# 3. Sichere Nutzung mobile Geräte

## 3.4. Tipps, um Mobilgeräte sicher zu machen

### So finden Sie die Seriennummer Ihres Smartphones (IMEI-Nummer)



- ✓ Android Smartphone - Einstellungen → am Telefon
- ✓ iPhone - Einstellungen → Allgemein → Info
- ✓ *Oder:* Geben Sie den folgenden Code auf dem Ziffernblock des Telefons ein:  
\*#06#



# 3. Sichere Nutzung mobile Geräte

## 3.5. Hilfreiche Links

Diese Linksammlung dient als Beispiel und muss im jeweiligen Partnerland angepasst werden.

<a href="http://www.saferinternet.at">www.saferinternet.at</a>	Tipps und Broschüren für verschiedene Zielgruppen
<a href="http://www.watchlistinternet.at">www.watchlistinternet.at</a>	Informationsplattform zu Internet-Betrug und betrugsähnlichen Online-Fallen aus Österreich
<a href="http://www.ombudsstelle.at">www.ombudsstelle.at</a>	Hilft Ihnen kostenlos, wenn Sie eine Beschwerde zu einem bestimmten Unternehmen oder eine allgemeine Anfrage rund um das Einkaufen im Internet haben
<a href="http://checkdeinpasswort.de">checkdeinpasswort.de</a>	Finden Sie heraus, wie man ein sicheres Passwort aussucht (Seite und Grundlage der Sicherheits-Einschätzung aus Deutschland)

# Vielen Dank für Ihre Teilnahme und Ihre Ideen!

