Modul 4: Sicherheit

DiA – Digital in Arbeit

Bayerisches Staatsministerium für Familie, Arbeit und Soziales

DiA wird gefördert aus Mitteln des Arbeitsmarktfonds des Bayerischen Staatsministeriums für Arbeit, Familie und Soziales

Forschungsinstitut Betriebliche Bildung

Level 2

Lernziel:

Ergreifen von einfachen Maßnahmen zum Schutz des eigenen Gerätes und zum Energiesparen

Kapitel 1: Maßnahmen zum Schutz des Computers und des Smartphones

Wie schütze ich meinen Computer?

„Viele nützliche und wichtige Dienstleistungen werden heute über das Internet in Anspruch genommen. Dazu zählen beispielsweise das Erledigen von Bankgeschäften oder Online-Einkäufe, aber auch der Austausch mit Freunden und Familie – zum Beispiel über Soziale Netzwerke oder Messenger. Neben den vielen Chancen, die das Netz bietet, gibt es aber auch Risiken, wie Schadsoftware oder Identitätsdiebstahl, vor denen Sie sich schützen sollten.“

Wie Sie das machen, können Sie u.a. in den folgenden
10 Handlungsempfehlungen,
die **Klicksafe** und das **Bundesamt für Sicherheit in der Informationstechnik** zusammengestellt haben, erfahren.

10 Tipps zum Schutz des Computers

- ✓ Verwenden Sie einen aktuellen Webbrowser.
- ✓ Halten Sie Ihre Software aktuell.
- ✓ Nutzen Sie Virenschutz und Firewall.
- ✓ Legen Sie unterschiedliche Benutzerkonten an.
- ✓ Nutzen Sie unterschiedliche Passwörter und ändern Sie sie bei Bedarf.
- ✓ Seien Sie vorsichtig bei E-Mails und deren Anhängen.
- ✓ Laden Sie Daten nur aus vertrauenswürdigen Quellen herunter.
- ✓ Seien Sie zurückhaltend mit der Weitergabe persönlicher Daten.
- ✓ Schützen Sie Ihre Daten durch Verschlüsselung.
- ✓ Fertigen Sie regelmäßig Sicherheitskopien an.

10 Tipps zum Schutz des Computers

Mehr dazu erfahren Sie auf den Seiten von Klicksafe und dem Bundesamt für Sicherheit in der Informationstechnik.

Surfen, aber sicher! Basisschutz leicht gemacht 10 Tipps für ein ungetrübtes Surf-Vergnügen. Bundesamt für Sicherheit in der Informationstechnik – BSI (Hrsg.)(2019).
Bürgerbroschüre - Das Internet sicher nutzen (bund.de)

Klicksafe: Den PC schützen.
Den PC schützen - klicksafe.de

Wie schütze ich mein Smartphone?

Das *Gerät* schützen **PIN** und **Bildschirmsperre** vor dem Zugriff durch Andere:

PIN (Persönliche Identifikationsnummer)

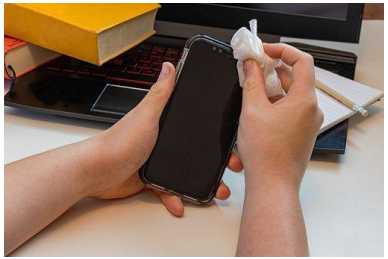
Die PIN schützt die SIM-Karte des Smartphones und damit alle auf ihm befindlichen Daten. Sie muss beim Neustart des Handys eingegeben werden.

Bildschirmsperre

Die Bildschirmsperre schützt vor dem fremden Zugriff auf Einstellungen und Anwendungen des Geräts. Sie muss bei jeder Nutzung eingegeben werden.

Möglichkeiten der Bildschirmsperre

- **Zahlenkombination:** unbedingt auf gängige Zahlenkombinationen wie z. B. „1234“, „1111“ oder dergleichen verzichten. Solche Kombinationen sind zu einfach zu knacken.
- **Mustersperre:** man kann sich ein eigenes Muster aus verschiedenen vorgegebenen Punkten zusammensetzen, z. B. ein Rechteck, Quadrat oder einen Buchstaben. Aber Vorsicht! Auf dem Touch-Display entstehen im Lauf der Zeit sichtbare Spuren durch Fingerabdrücke. Deshalb sollte das Display regelmäßig gesäubert werden, wenn eine Mustersperre verwendet wird. Die Mustersperre ist generell nicht zu empfehlen.



Möglichkeiten der Bildschirmsperre

- **Passwort**: Es sollte Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen enthalten. Je länger es ist, desto sicherer ist es oft.

- **„FaceUnlock“**: das Entsperren mittels Gesichtserkennung. Nicht sehr sicher, da man es einfach mittels eines Bildes des Besitzers/der Besitzerin austricksen kann.

- **Fingerabdruck**: Viele neuen Handys haben einen Fingerabdrucksensor. Beim Einrichten des Fingerabdrucks erfordert das Gerät meistens eine zweite Entsperr-Variante, für den Fall, dass der Abdruck mal nicht erkannt werden kann. Ziemlich fälschungssicher.

Sicherheit: Wie schütze ich das Smartphone? - klicksafe.de

Wie ändere ich PIN und Bildschirmsperre?

Bei Android-Geräten meist unter:

Einstellungen

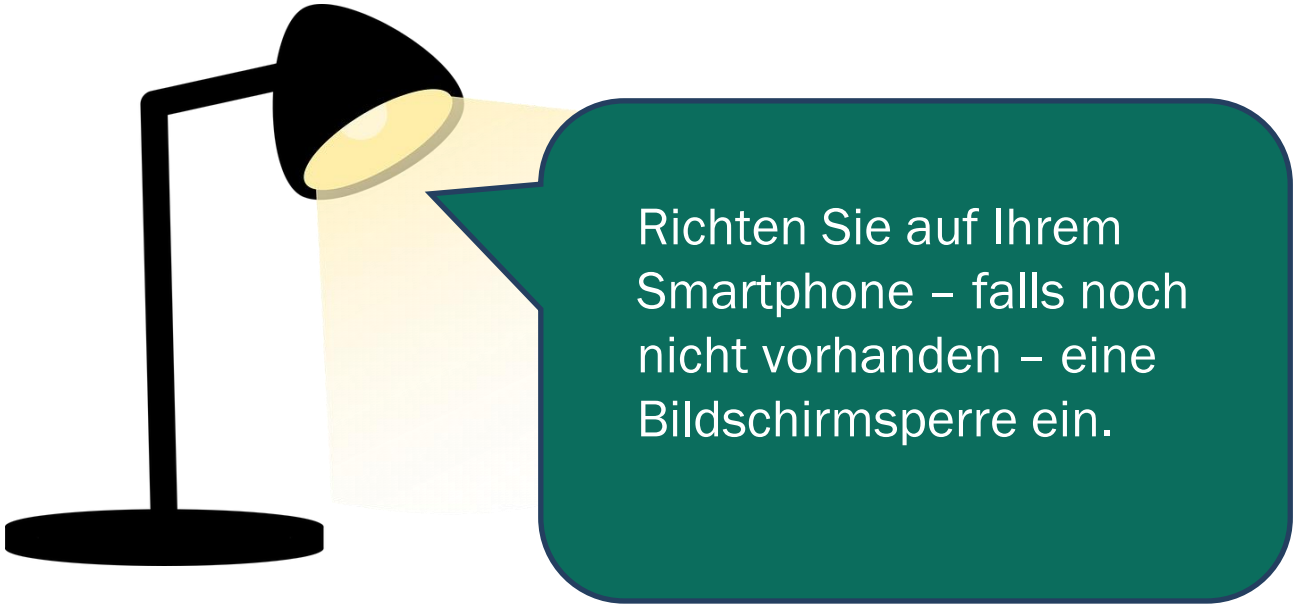
Sicherheit

Bei iOS meist unter:

Einstellungen

Touch ID & Code

Übung 1



Richten Sie auf Ihrem Smartphone – falls noch nicht vorhanden – eine Bildschirmsperre ein.

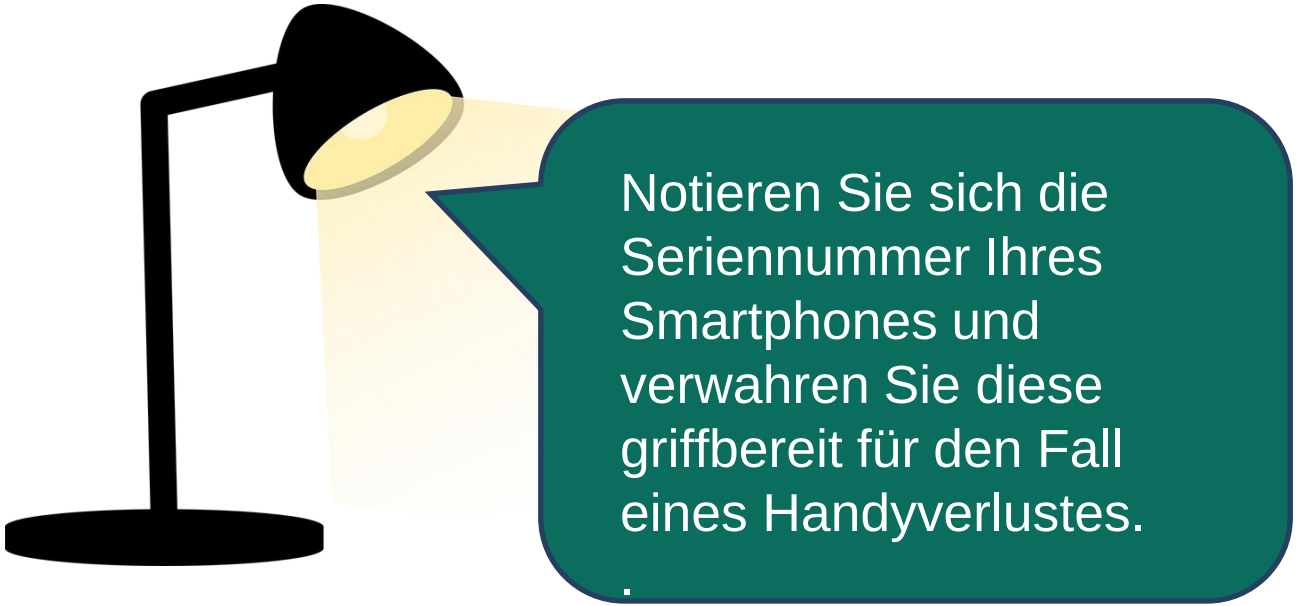
Diebstahlschutz

- Wird das Smartphone gestohlen, sollte man die **SIM-Karte** des Geräts beim Netzbetreiber (z.B. Telekom) unter Angabe der Telefonnummer sperren lassen. Ist diese gesperrt, kann kein Fremder/keine Fremde mehr damit telefonieren und hohe Kosten verursachen.

- Im Anschluss daran sollte Anzeige bei der Polizei erstattet werden. Hier ist auch die **„Seriennummer“** (IMEI-Nummer) des Smartphones anzugeben.
  Die Nummer findet sich unter dem Akku, auf der Originalverpackung oder der Rechnung zum Handykauf. Schreiben Sie diese auf jeden Fall auf, so dass Sie im Falle eines Handyverlusts schnell griffbereit ist.

Sicherheit: Wie schütze ich das Smartphone? - klicksafe.de

Übung 2



Notieren Sie sich die Seriennummer Ihres Smartphones und verwahren Sie diese griffbereit für den Fall eines Handyverlustes.

.

Schutz nach „außen“

Oft werden persönliche Daten (Kontakte, aktueller Standort,...) ganz unbemerkt und ungewollt gesammelt und übermittelt.

- Neben dem Betriebssystem sind dafür auch Apps verantwortlich. Daher ist es ratsam, Anwendungen, die gerade nicht gebraucht werden und aktiv sind, abzuschalten.
- Auch Bluetooth ist eine Schnittstelle nach „draußen". Ist Bluetooth eingeschaltet, steigt die Gefahr, dass andere ungewollt persönliche Daten vom Gerät abrufen. Deshalb sollte man Bluetooth nur einschalten, wenn es tatsächlich benötigt wird.
- Das gilt auch für die WLAN-Funktion. Hier sollte auch die automatische Einwahl in öffentliche WLAN-Netze deaktiviert sein.

Spionierende Apps

- Schutz vor allzu neugierigen Apps oder gar Schadprogrammen bietet eine **gesunde kritische Haltung** gegenüber Apps.
- Apps sollten nur von den **großen Plattformen** - *Apple App Store oder Google Play* – heruntergeladen werden, da diese zumindest oberflächlich mittels eines automatisierten Verfahrens überprüft werden.
- Außerdem sollte man immer die **Allgemeinen Geschäftsbedingungen** (AGBs) einer jeden App vor deren Installation kritisch lesen.
- Zudem sollte man in Erfahrung bringen, welche **Zugriffsrechte** sich die jeweilige App auf dem Smartphone oder Tablet-PC einräumen möchte.

Zugriffsrechte

Viele der Apps greifen, einmal installiert, auf Dateien und Programme auf dem Gerät zu.

- Vor der Installation sollte man überprüfen, ob die App auf den Standort oder auf andere persönliche Daten, wie z. B. Kontaktdaten oder Kalendererereignisse zugreifen kann. Apps sollten nicht installiert werden, wenn die Zugriffsrechte, die sie einfordern, **nicht zu den Funktionen der App passen**. Z. B. muss eine Taschenlampen-App nicht das Adressbuch auslesen dürfen.

- Eine App, die dabei helfen kann, ist z.B. **APEFS** = Android Permission Filter System (Android, kostenlos): Diese App fungiert als Filter zwischen App-Store und Endgerät. Bei der App-Suche zeigt APEFS an, welche Berechtigungen sich eine App beschaffen möchte. Auch bereits installierte Apps können nach diesen Berechtigungen durchsucht werden.

Apps & Datenschutz - klicksafe.de

Viel Erfolg beim Ausprobieren!

Bayerisches Staatsministerium für Familie, Arbeit und Soziales

DiA wird gefördert aus Mitteln des Arbeitsmarktfonds des Bayerischen Staatsministeriums für Arbeit, Familie und Soziales

f-bb Forschungsinstitut Betriebliche Bildung