Sicherheit geht vor

Downloads, Passwörter und Daten

Heutzutage sind Smartphones und Tablets ständig mit dem Internet verbunden, sei es im eigenen WLAN, in einem öffentlichem oder fremden oder über mobiles Internet. Mit diesen tollen Möglichkeiten gehen aber auch Risiken einher, die Sie vorbeugen können, denn: Sicherheit geht vor.

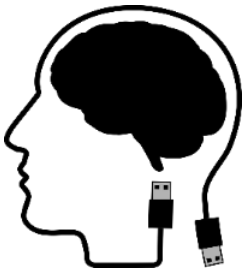
Daten

Bei der Nutzung von Smartphone und Tablet fallen eine Menge Daten an. Zum einen, weil Sie selber Daten erstellen (bspw. Fotos machen) und zum anderen, weil Apps Daten verarbeiten. Und das unabhängig davon, ob Sie sie nutzen oder nicht. Deswegen müssen Ihre Daten geschützt werden – vor Verlust und ungewünschter Weitergabe.

Datensicherung - Regelmäßige Sicherungen (Backups)

Es empfiehlt sich, in regelmäßigen Abständen die Daten Ihres Smartphones, wie bspw. Dokumente, Fotos und Videos, zusätzlich auf einem Computer, auf einem externen Speichermedium (bspw. Festplatte oder USB-Stick) oder in einer Cloud zu sichern. Auf diese Weise schützen Sie sich vor einem kompletten Datenverlust, sollte Ihr Smartphone einmal verloren oder kaputtgehen. Schließlich besitzen aufgenommene Bilder oftmals einen hohen emotionalen Wert und ein Verlust wäre bedauernswert. Das Video über den QR-Code gibt ihn ebenfalls einen Einblick.

Bei der Sicherung Ihrer Daten über Ihren Computer via USB-Kabel können Sie wie folgt vorgehen:



- Gehen Sie bei einer Datensicherung via **USB-Kabel** folgendermaßen vor:

1. Schließen Sie das USB-Kabel an Ihr Smartphone an.
2. Das Ende des Kabels mit dem USB-Stecker schieben Sie nicht in das Netzteil, sondern in den USB-Anschluss Ihres Computers.
3. Schauen Sie auf den Bildschirm Ihres Smartphones. In den meisten Fällen müssen Sie nun den Entsperrungs-Code (mit welchem Sie Ihr Gerät an- und abmelden) eingeben, damit der Computer auf Ihr Smartphone zugreifen darf.
4. Wenden Sie sich nun Ihrem Computer zu. Erstellen Sie an einer gewünschten Stelle (wie z. B. auf dem Desktop) einen neuen Ordner, in welchem die Dateien (Fotos etc.) Ihres Smartphones gespeichert werden sollen (iPhone: über die Synchronisation).
5. Öffnen Sie die Ordnerstruktur auf Ihrem Computer. Gehen Sie nun auf „Computer“ (früher „Arbeitsplatz“), um zur Übersicht der Festplatten zu gelangen. Ihr Smartphone wird hier als externes Gerät angezeigt.
6. Klicken Sie auf dem PC nun das Symbol Ihres Smartphones an, damit Sie alle Dateien einsehen können, die sich auf Ihrem Gerät befinden.
7. Wählen Sie die gewünschten Dateien zum Kopieren aus.

Diese Maßnahme wird mitfinanziert durch Steuermittel auf der Grundlage des von den Abgeordneten des Sächsischen Landtags beschlossenen Haushaltes.
SMS SACHSEN

8. Tippen Sie die rechte Maustaste einmal an und klicken Sie auf „kopieren“. (Achtung! Wenn Sie „Ausschneiden“ wählen, entfernen Sie die Bilder von Ihrem Smartphone. Beim Kopiervorgang bleiben diese erhalten.)
9. Speichern Sie die Dateien nun auf Ihrem PC. Wählen Sie den gewünschten Ordner aus, klicken Sie anschließend erneut die rechte Maustaste an und wählen Sie „einfügen“ aus.
10. Haben Sie alle gewünschten Dateien kopiert, entfernen Sie Ihr Smartphone vom Computer.

Alternativ gibt es folgende weitere Möglichkeiten der Datenübertragung:

- **Speicherkarte:** Falls Sie den Speicherplatz Ihres Gerätes mit einer Speicherkarte erweitert haben, können Sie diese entnehmen, in den Kartenslot Ihres Computers stecken und die Daten von dort aus kopieren.
- **Bluetooth:** Sie können damit Ihr Gerät kabellos mit einem anderen Gerät verbinden und Daten via Funk übertragen. Gern können Sie dazu das Tutorial über den QR-Code rechts verfolgen.
- **Cloud:** Mittels Internetverbindung können Sie Ihre Daten auch in eine Cloud (englisch für Wolke), also Speicherplatz auf Servern, hochladen.

Datenschutz

Neben vielen bekannten und seriösen Angeboten gibt es auch unseriöse und gefährliche Angebote, wie Internetseiten, Apps und E-Mails. Deswegen lohnt es sich, nicht alles sofort zu aktivieren oder auszuwählen. Bei Ihrer vorsichtigen Nutzung helfen Ihnen folgende Hinweise weiter.

- Gehen Sie mit Bedacht vor bei dem was Sie tun, so wie im echten Leben.
- Geben Sie nicht sofort überall Ihre Daten ein, da es auch viele unseriöse Angebote gibt. Überlegen Sie, ob Ihre Daten immer wirklich notwendig sind für das entsprechende Angebot.
- Fremde und öffentliche WLANs sollten Sie besonders vorsichtig nutzen, insb. in Hinblick auf sensible Daten.
- Passen Sie auf Ihr Gerät auch physisch auf und lassen Sie bei Verlust Ihre SIM-Karte sperren.
- Ihre E-Mail-Adresse sollten Sie nur bei vertrauenswürdigen und bekannten Stellen angeben.
- Erstellen Sie eine extra E-Mail-Adresse nur für Anmeldevorgänge.

Datenspuren

- digitale Geräte sammeln eine Menge Daten und geben diese weiter

Welche Datenspuren gibt es?

- IP-Adressen / Cookies / Browserchroniken / Standortdaten / Tracking / Werbe-IDs

Wie können Sie sich datensparsam verhalten?

- gespeicherte Nachverfolgung (Cookies und Tracking) beschränken
- Standortdaten ausschalten
- pseudonyme verwenden und wenig Daten preisgeben
- Wegwerf-E-Mail-Adressen für unpersönliche Zugänge nutzen → *Müllmail*

Identitätsmissbrauch

- prüfen Sie, ob Ihre E-Mail geknackt wurde → *E-Mail-Sicherheit prüfen*

Passwörter

Ein Anmeldevorgang ist für viele Angebote im Internet notwendig. Damit verbunden ist die Erstellung eines Passwortes. Dieses müssen Sie nicht nur sicher aufbewahren, sondern auch sicher auswählen.

Einstellungen und Knacken

Passwörter lassen sich knacken. Umso einfacher das Passwort gestaltet ist, umso schneller lässt es sich knacken. Andersrum gesagt: Umso schwerer Sie sich das Passwort merken können, umso sicherer ist es. Es gibt aber einige Möglichkeiten, wie Ihr Passwort sicher und merkbar gestaltet werden kann.

- Das sollte Ihr Passwort alles können
  - Nutzen Sie überall ein anderes Passwort.
  - Ihr Passwort sollte mindestens 8 Zeichen lang sein.
  - Ein sicheres Passwort muss Groß- und Kleinbuchstaben, Zahlen, Sonderzeichen enthalten.
  - Dabei sollten Sie keine Tastatur- oder Zeichenfolgen, Wörter und private Daten (bspw. Geburtstage, Kosenamen) verwenden.
  - Nur Sie sollten Ihr Passwort kennen.
- Schützen Sie auch Ihr Gerät mit einem Passwort, einer PIN, einem Muster, einem Fingerabdruck und/oder Gesichtserkennung (unterschiedliche Vor- und Nachteile sowie geräteabhängig), iPhone: Touch ID, Face ID und → *Schlüsselbundfunktion beim iPhone*

Aufgabe

Was ist kritisch an den folgenden Passwörtern?
1) qwertz123456 2) j!-7A. 3) Hallo-Welt!1

Aufgabe

Erstellen Sie ein Passwort, welches in diesem Jahrzehnt nicht geknackt werden kann!
→ www.checkdeinpasswort.de

Tipp

Um sich viele Passwörter zu merken, hilft eine Variation, die an den Dienst angelehnt ist, bspw. ein a für Amazon (8uT,w.7-fKH_a) oder ein g für Google (8uT,w.7-fKH_g). Bei sehr vielen Passwörtern unterstützt Sie auch ein Passwortmanager

Ihre Notizen

Apps

Apps sind die Programme auf Smartphones und Tablets. Sie können helfen und das Leben einfacher machen. Sie können aber auch Schaden anrichten und private Informationen einholen. Mit einigen Hinweisen können Sie dafür sorgen, die Vorteile zu nutzen und Nachteile zu vermeiden.

App-Downloads

- Laden Sie Apps nur von offiziellen Stellen herunterladen (iPhone: App Store/Android: Google Play/Hersteller:inseite).
- Dabei werden die Apps auf Viren und Schadsoftware geprüft.
- Viele Apps gibt es kostenlos und Nutzende „bezahlen“ mit ihren Daten wie Kontakten, Standorten, Konsum- und Nutzungsverhalten sowie Werbung.

Updates

Von Zeit zu Zeit wird es vorkommen, dass Ihr Gerät ein verfügbares Update anzeigt. Ein Update ist die Überarbeitung eines Programmes und fungiert als eine neuere und verbesserte Version. Daher ist es äußerst sinnvoll, die Aktualisierung zuzulassen, damit Ihr Gerät auf dem neusten Stand ist, einwandfrei funktioniert und eventuelle Sicherheitslücken geschlossen werden.

- Updates (englisch für Aktualisierung) können sowohl das Betriebssystem als auch einzelne Programme (Apps) betreffen.
- Ist ein neues Update verfügbar, wird Ihnen eine entsprechende Meldung auf Ihrem Benachrichtigungsfeld (Statusleiste) angezeigt. Tippen Sie die entsprechende Nachricht an, um die Aktualisierung durchzuführen.
- Installieren Sie Updates, sobald sie Ihnen angeboten werden. Diesbezüglich ist die Voreinstellung meist, dass dies nur im WLAN erfolgt. Beachten Sie dies, falls Sie nur mobile Daten nutzen.
- Bei einem Software-Update schaltet sich Ihr Telefon kurzzeitig aus, um die Installation vorzunehmen. Halten Sie daher unbedingt Ihren Entsperrungs-Code (Bildschirmsperre) sowie die Zahlenkombination Ihrer SIM-PIN bereit, um das Gerät danach wieder benutzen zu können.

Einstellungen

- Smartphones und Tablets sowie die darauf installierten Apps haben teilweise tiefe Einblicke in Ihre Privatsphäre.
- Die standardmäßigen aktiven erlauben den Apps meist viel.
- Diese Datenschutzeinstellungen können Sie anpassen und selbst entscheiden, welche Daten wie verarbeitet werden dürfen.

Aufgabe

Prüfen Sie die Datenschutzeinstellungen gleich selber: Gehen Sie in eine App Ihrer Wahl und suchen Sie in den Einstellungen nach dem Bereich Datenschutz. Was können Sie hier einstellen? Sind Sie mit den aktuellen Einstellungen einverstanden?

TECHNISCHE UNIVERSITÄT DRESDEN
gemeinsam digital
LERNEN VOR ORT - GEMEINSAM INS NETZ
Diese Maßnahme wird mitfinanziert durch Steuermittel auf der Grundlage des von den Abgeordneten des Sächsischen Landtags beschlossenen Haushaltes.
SACHSEN

Am besten erledigen Sie dies bei der Installation einer neuen App sofort. Dann ist es erledigt und von vornherein Ihren Bedürfnissen angepasst.

Kurz und knapp

- Betriebssysteme und Programme aktuell halten
- Apps aus seriösen Quellen beziehen
- keine unseriösen Nachrichten öffnen und Dateien herunterladen
- überall ein anderes Passwort, mind. 8 gemischte Zeichen
- wichtige Daten regelmäßig sichern

Weiterführende Informationen

Thema	Link
Ganz aktuell: Basistipps zur IT-Sicherheit vom Bundesamt für Sicherheit in der Informationstechnik	https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/cyber-sicherheitsempfehlungen_node.html
Sichere Passwörter – so geht's von der Verbraucherzentrale	https://www.verbraucherzentrale.de/wissen/digitale-welt/datenschutz/sichere-passwoerter-so-gehts-11672
Ausführlich: Digitale Kompetenzen in der CYBERfibel	https://www.cyberfibel.de/digitale-kompetenzen
Für Neugierige: DsiNSicherheitsIndex 2021. Digitale Sicherheitslage von Verbraucher:innen in Deutschland	https://www.sicher-im-netz.de/file/13161/download?token=se3us1Mq
Für Checker:innen: DsiN-Computercheck	https://www.sicher-im-netz.de/dsin-computercheck
Video: Sichere Passwörter knacken mit Tobias Schrödel	https://www.youtube.com/watch?app=desktop&v=ZJtWZIuU_jk
Passwörter. Informationen für Erwachsene in leicht lesbarer Sprache.	https://www.digitaleseniorinnen.at/fileadmin/redakteure/Downloads/Passwoerter_Informationen_in_leichter_Sprache.pdf
Müllmail / Wegwerfemailseiten	https://muellmail.com / https://praxistipps.chip.de/wegwerf-email-adressen-diese-anbieter-gibts_1674
E-Mail-Sicherheit prüfen	https://sec.hpi.de/ilc
Schlüsselbundfunktion iPhone	https://support.apple.com/de-de/HT204085

Quellen

Dieses Cover wurde unter Verwendung von Ressourcen von pixabay.com erstellt.
'Bild: Freepik.com'. Dieses Cover wurde unter Verwendung von Ressourcen von Flaticon.com erstellt.
'Bild: Flaticon.com'. Dieses Cover wurde unter Verwendung von Ressourcen von Flaticon.com erstellt.