Worauf kommt es an beim Datenschutz?

Was bedeutet Datenschutz?

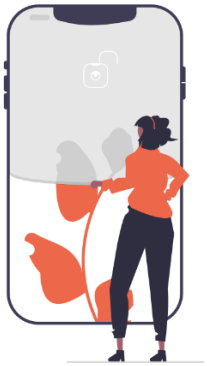
Der Begriff Datenschutz ist im späten 20ten Jahrhundert mit der Entstehung des Internets zum ersten Mal aufgekommen und wird seitdem ganz unterschiedlich definiert. Im Wesentlichen wird mit Datenschutz der Schutz der Persönlichkeitsrechte und der Privatsphäre jedes Menschen im Zuge von Datenverarbeitung gemeint.
Da wir mittlerweile alle auf die eine oder andere Weise mit dem Internet verbunden sind, sollten wir um die Möglichkeiten wissen, wie wir uns im Alltag, insbesondere beim Surfen im Internet und bei der Nutzung des Smartphones oder Computers, vor Angriffen und der missbräuchlichen Verwendung unsere persönlichen Daten schützen können.

Wie schützen wir unser Smartphone?

Wir sollten das Smartphone für andere unzugänglich machen, indem wir…

Unseren PIN-Code (Schlüssel zum Mobilfunkanbieter) geheim halten

Wenn wir ein Handy oder Smartphone nutzen, haben wir von unserem Mobilfunkanbieter eine kleine SIM-Karte und einen dazugehörigen PIN-Code bekommen.
Damit wir die Konditionen unseres Mobilfunkanbieters in Anspruch nehmen und somit telefonieren und ins Internet gehen können, muss die SIM-Karte in unser Smartphone eingesetzt werden. Wenn wir unser Smartphone einschalten, müssen wir die SIM-Karte mit dem PIN-Code entsperren. Der PIN-Code ist also der Schlüssel zu den Leistungen unseres Mobilfunkanbieters. Wir sollten den PIN-Code daher für andere unzugänglich aufbewahren und niemandem verraten.



Eine Bildschirmsperre (Schlüssel zum Smartphone) einrichten

Außerdem sollten wir eine Bildschirmsperre einrichten und damit auch unser Smartphone für andere verschließen. Wir können entweder einen Zahlencode, ein Passwort, ein Muster, unseren Fingerabdruck oder bei manchen Geräten auch eine Gesichtserkennung einrichten. Die Bildschirmsperre wird immer abgefragt, wenn wir den Bildschirm unseres Smartphones einschalten. So schützen wir unser Gerät nicht nur vor fremden Zugriffen, sondern auch vor der versehentlichen Benutzung, wenn wir das Gerät z.B. in der Hosentasche haben.

Wir sollten unser Smartphone auf dem neusten Stand halten, indem wir…

Updates (Aktualisierungen) durchführen

Das Wort Update bedeutet auf Deutsch Aktualisierung. Bei einem Update werden Sicherheitslücken geschlossen und neue Funktionen und Verbesserungen aktiviert. Im besten Fall prüfen wir regelmäßig, ob unser Smartphone und unsere Apps auf dem neusten Stand sind. Dies können wir entweder in der App Einstellungen auf unserem Smartphone oder über den Play Store oder App Store nachschauen. Wenn wir von unserem Smartphone gefragt werden, ob ein Update bzw. eine Aktualisierung durchgeführt werden soll, sollten wir dies möglichst zulassen. Da bei einem Update in der Regel größere Datenmengen benötigt werden, sollten wir bei der Durchführung des Updates mit unserem WLAN-Netz verbunden sein.

Wir sollten Zugriffsrechte und Verbindungen kontrollieren, indem wir…

Die Zugriffsberechtigungen unserer Apps prüfen

Damit wir unsere Apps auf dem Smartphone vollumfänglich nutzen können, müssen wir den Apps gewisse Zugriffsrechte auf Funktionen unseres Smartphones geben. Allerdings sind nicht immer alle Zugriffsrechte plausibel oder für das Funktionieren der App nötig. z.B. muss eine Taschenrechner-App nicht unseren Standort wissen, unsere Navigations-App aber schon.
Wir sollten daher gelegentlich die Zugriffrechte unserer Apps in den Einstellungen unseres Smartphones kontrollieren und ggf. anpassen. Hierfür tippen wir auf die App Einstellungen auf unserem Smartphone und suchen in den Einstellungen die Kategorie Datenschutz. Hier können wir die jeweiligen Zugriffsberechtigungen der Apps ein- und ausschalten.

Die Verbindungseinstellungen prüfen

Unser Smartphone bietet uns unterschiedliche Verbindungsmöglichkeiten. GPS ist beispielsweise eine Satelliten-Verbindung, die für die Navigation oder Routenplanung verwendet wird. Apps können allerdings über dauerhaft eingeschaltetes GPS oder Bluetooth unseren Standort ermitteln und auf diese Weise Bewegungsprofile erstellen, d.h. es kann nachvollzogen werden, wo wir überall gewesen sind. Über die Verbindungsdienste Bluetooth oder NFC können Daten ausgetauscht oder andere Geräte wie z.B. Kopfhörer kabellos mit unserem Smartphone verbunden werden. Haben wir diese Verbindungen dauerhaft aktiviert, ist das Risiko erhöht, dass sich jemand unerlaubt Zugriff zu den Daten auf unserem Smartphone verschafft. Wir sollten derartige Verbindungen also möglichst nur im Bedarfsfall einschalten. Wir finden die Verbindungseinstellungen in der App Einstellungen und können die Verbindungen hier ein- und ausschalten.

Tipps für die sichere Smartphone-Nutzung

1. Apps nur aus dem Playstore oder App-Store herunterladen

Wir sollten Apps nur aus dem Google Play Store oder dem Apple App Store auf unser Smartphone herunterladen. Im Google Play Store wird jede App, durch das sogenannte Play Protect System auf Schadprogramme und Viren geprüft.

2. Apps nur begrenzte Zugriffsrechte erlauben

Wir sollten Apps bei der Abfrage der Zugriffsberechtigung möglichst nur begrenzte Zugriffsrechte erteilen. Hier wählen wir, wenn möglich „nur dieses Mal“ oder „bei Nutzung der App“ aus.

3. Vorsichtige Nutzung von öffentlichen WLAN-Netzten

Wir vermeiden öffentliche oder fremde WLAN-Netze, wie in Hotels oder Cafés, wenn wir z.B. über einen Messenger sensible Daten oder Informationen austauschen oder Online-Banking nutzen wollen.

4. Die Seriennummer (IMEI-Nummer) unseres Smartphones

Wir sollten uns die Seriennummer (IMEI-Nummer) unseres Smartphones notieren. Die Nummer wird im Falle eines Diebstahls für eine Anzeige bei der Polizei benötigt.

Android: Einstellungen → Über das Telefon

Bei Android Smartphones finden wir die Seriennummer (IMEI-Nummer) in der APP Einstellungen unter dem Punkt „Über das Telefon“.

IOS: Einstellungen → Allgemein → Info

Bei Apple Smartphones finden wir die Seriennummer (IMEI-Nummer) in der App Einstellungen unter dem Punkt „Allgemein“ und dem Unterpunkt „Info“.

5. Passwörter und Zugangsdaten geheim halten

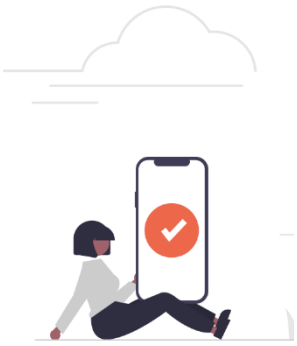
Wir sollten es unbedingt vermeiden, unsere Zugangsdaten und Passwörter dauerhaft auf einem Zettel in unserer Tasche oder unserem Portemonnaie aufzubewahren. Wir sollten diese Daten auch nicht auf dem Smartphone notieren.

Wie sichern wir unsere Daten?

Wir sollten unsere Daten gelegentlich sichern, indem wir…

Regelmäßige Backup´s erstellen

Das Wort Backup heißt auf Deutsch Sicherungskopie. Wir sollten für den Fall, dass unser Smartphone gestohlen wird oder verloren geht, eine Kopie von unseren Daten und Fotos auf einem anderen Speichermedium erstellen. Unsere Daten können wir z.B. auf einer sogenannten **SD-Speicherkarte** sichern. Diese wird in das Smartphone eingelegt und wir können unsere Daten und Fotos auf die Karte kopieren. Alternativ können wir unser Smartphone mit einem sogenannten USB-Kabel an **unseren Computer** anschließen und die Daten dorthin kopieren.



Eine unkomplizierte und praktische Lösung ist die Nutzung **einer Cloud**, wie Google Drive, Apple iCloud oder Microsoft OneDrive. Den Zugang zur Cloud finden wir als App auf unserem Smartphone. Wenn wir unsere Daten in einer Cloud speichern, befinden sich die Daten auf einem riesigen Speicher-Computer des Cloud-Anbieters. Wir können uns die Cloud wie eine riesige Lagerhalle vorstellen, in der wir unsere Daten lagern können. Der große Vorteil ist, dass wir jederzeit und von egal welchem Gerät mit einem Passwort auf die Cloud und damit auf unsere gespeicherten Daten zugreifen können.

Welche Schadprogramme gibt es?

Doch was kann passieren, wenn wir uns nicht schützen? Hierfür schauen wir uns zunächst an welche…

Der Wurm: Ein Wurm oder Virus ist eine versteckte Schadkomponente die z.B. im Anhang einer E-Mail, SMS oder Messenger-Nachricht lauert. Der Wurm gelangt in der Regel durch das Öffnen von Dateien oder das Antippen eines Links auf das Gerät und kann sich von dort aus wie ein Virus verbreiten.

Der Trojaner: Ein Trojaner dient häufig als ein Transportmittel für Schadkomponenten und wird z.B. unbemerkt beim Herunterladen von kostenlosen Software- und App-Angeboten auf dem Smartphone oder Computer installiert. Trojaner können auch Hintertüren auf dem Computer öffnen, damit Kriminelle darauf zugreifen und private Informationen stehlen können.

Was können Schadprogramme verursachen?

Der Überbegriff für Schadprogramme und deren Auswirkungen ist Malware. Der Begriff ist Englisch und heißt so viel wie böses Computerprogramm oder böse Software.

Es gibt unterschiedliche Arten von Malware. Wir schauen uns vier Arten mal etwas genauer an:

Spyware

Das englische Wort spy heißt auf Deutsch spionieren. Die Spyware gelangt durch einen Wurm oder Trojaner auf den Computer oder das Smartphone und spioniert die Nutzerinnen und Nutzer aus.

Ransomware

Das englische Wort ransom heißt auf Deutsch Lösegeld. Die Ransomware blockiert das Gerät und sperrt die Zugänge und Daten. Nicht selten fordern die Urheber im Anschluss Lösegeld von den betroffenen Personen für die Freischaltung des Geräts. Hier sollten wir uns an die Polizei wenden und uns Hilfe von IT-Experten holen.

Adware

Ad ist die Kurzform für Advertisement was auf Deutsch Werbung bedeutet. Die Adware überhäuft das betroffene System mit sogenannten Pop-Up´s und Werbeanzeigen. Pop-up ist Englisch und heißt auf Deutsch plötzlich aufgehen oder auftauchen. Wie Popcorn ploppen entsprechende Werbeanzeigen auf dem Bildschirm auf, nachdem man einen Link angeklickt oder eine Internetseite geöffnet hat.

Bot

Bots sind Computerprogramme, die Aufgaben automatisiert erledigen. Bot ist die Abkürzung für das Wort Roboter.
Es gibt nützliche und schädliche Bots. Bei schädlichen Bots handelt es sich um Malware, die sich unerlaubt auf vernetzten Computern befindet und diesen fernsteuert, meistens ohne, dass der Nutzer oder die Nutzerin dies bemerkt. Schädliche Bots können z.B. Falschnachrichten verbreiten, falsche Produkt-Bewertungen und Kommentare im Internet verfassen oder mit dem ferngesteuerten Computer anderen Schaden anrichten.

Wie können wir uns davor schützen?

Hier ein paar Tipps:

Regelmäßig Updates durchführen

Wir führen regelmäßig Updates durch und Aktualisieren unser System und alle Programme, um Sicherheitslücken zu schließen

Virenschutzprogramm und Firewall nutzen

Wir nutzen ein Virenschutzprogramm und eine Firewall**,** um Schadprogramme bereits beim ungewollten Download oder öffnen von E-Mail-Anhängen ertappen zu können

Vorsicht beim Umgang mit E-Mails

Wir sollten achtsam beim Lesen von E-Mails sein, insbesondere beim Anklicken von Links und öffnen von E-Mail-Anhängen, vor allem wenn es sich um eine Nachricht eines unbekannten Absenders handelt

Vertrauenswürdige Quellen nutzen

Wir sollten Programme und Apps nur von seriösen und vertrauenswürdigen Quellen herunterladen

Kamera (Webcam) abdecken

Wir verdecken unsere Kamera am Computer oder Laptop, wenn wir sie nicht benutzen. Sollte sich ein Schadprogramm Zugang zu unserer Webcam verschafft haben, kann es auf diese Weise trotzdem nichts sehen

Regelmäßig Back-Up´s erstellen

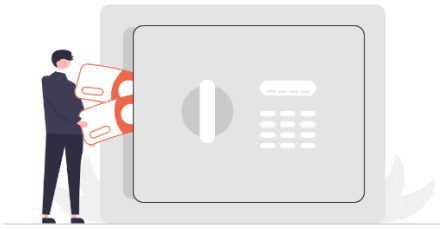
Wir sollten regelmäßig Sicherungskopien wichtiger Daten erstellen, um durch ein Schadprogramm gesperrte Daten nach einer Bereinigung oder Neuinstallation des Systems selbst wiederherstellen zu können. Hierfür können wir z.B. SD-Speicherkarten, externe Festplatten, USB-Speichersticks oder eine Cloud nutzen.

Sichere Passwörter verwenden

Wir verwenden für alle Geräte, Benutzerkonten und Zugänge sichere und ausreichend komplexe Passwörter und halten diese geheim.

*Hinweis: Wir sollten insbesondere **den Zugang zu unserem E-Mail-Programm** mit einem starken Passwort schützen. Denn überall, wo wir uns mit einem Passwort anmelden, wird uns für den Fall, dass wir unser Passwort vergessen haben, die Möglichkeit angeboten, über den Punkt „Passwort vergessen“ ein neues Passwort festzulegen. In diesem Fall wird uns in der Regel eine E-Mail zum Zurücksetzen und Neuerstellen des Passworts zugesendet. Damit niemand außer uns diese Funktion nutzen und so unsere Passwörter ändern kann, muss unser E-Mail-Passwort ganz besonders stark sein!*

Tipps zur Erstellung eines guten Passwortes



Unsere privaten Lebensbereiche schützen wir durch Schloss und Schlüssel. Wir verschließen unsere Wohnungstür, unser Auto und sichern unser Fahrrad mit einem Schloss. Ähnlich wie diese Schlösser, schützen sichere Passwörter unser digitales Eigentum und unsere Privatsphäre. Dabei gehen wir häufig zu sorglos mit der Erstellung unserer Passwörter um.

Hier ein paar Beispiel-Passwörter, die wir so oder ähnlich dringend vermeiden sollten:

- × 123456
- × passwort
- × abc123
- × qwertz
- × hallo
- × fußball
- × willkommen
- × 111111

Kurz gesagt sollten wir folgendes beachten:

- × Wir vermeiden Wiederholungen und Tastaturmuster
- × Wir nehmen keinen Namen als Passwort, auch nicht von Haustieren
- × Wir verwenden keine Buchstaben- oder Zahlenfolgen wie 1234
- × Wir verwenden keine Geburtsdaten, Telefonnummern oder Postleitzahlen

…und auf folgendes sollten wir Wert legen:

- ✓ Wir wählen ein möglichst langes Passwort (über 8 Zeichen)
- ✓ Wir erstellen ein möglichst komplexes, kryptisches Passwort
- ✓ Wir verwenden Groß- und Kleinschreibung
- ✓ Wir verwenden einen Mix aus Buchstaben, Zahlen und Zeichen

Mehr Infos und Tipps zur Erstellung eines sicheren Passworts, finden wir auf der Seite des Landeskriminalamts NRW – www.mach-dein-passwort-stark.de und in den in diesem Modul zur Verfügung gestellten Unterlagen.

Abschluss:

Auch wenn der Schutz unserer Daten ein wichtiges Thema ist, sollten wir uns nicht entmutigen lassen das Internet und digitale Technik wie das Smartphone oder den Computer für uns zu nutzen. Um unsere Daten zu schützen, können wir schon mit einigen wenigen Vorsichtsmaßnahmen viel bewirken. Indem wir unsere Geräte und Apps durch Updates immer auf dem neusten Stand halten, achtsam im Umgang mit E-Mails sind und unsere Geräte, Daten und Zugänge mit sicheren Passwörtern schützen, haben wir schon viel für den Schutz unserer Daten getan.