Hinweise zu Aktivitätsphase II: Informationsflyer zu Datenschutztipps für den Alltag (1/2)

Tipps für den Datenschutz-Flyer könnten sein …

- Bevor du ein Gerät kaufst, kannst du dich über den Anbieter informieren. Legt der Hersteller Wert auf Datenschutz? Unabhängige Testseiten im Internet können dir bei der Recherche helfen.
- Wo werden die erhobenen Daten gespeichert? Werden die Daten von Anbieter-/Herstellerseite mit Dritten geteilt oder in eine Cloud geladen? Wird eine Cloud gehackt, kommen Unbefugte schnell an deine Daten. Am besten ist es, wenn deine Informationen lokal auf dem Gerät gespeichert werden.
- Überprüfe, welchen Berechtigungen du für die Nutzung von Smartphone-Apps zustimmen musst. Wollen sie z. B. auf Smartphone-Daten zugreifen, die für eine Nutzung der jeweiligen App nicht wirklich erforderlich ist, dann überleg dir noch einmal genau, ob es dir das wert ist.
- Wäge ab, ob die Funktion des Geräts und die Preisgabe deiner persönlichen Daten in einem ausgewogenen Verhältnis zueinander stehen. Schütz dich und gib deine privaten Informationen nicht leichtfertig an die Hersteller der jeweiligen Geräte oder Apps.
- Lies, bevor du Cookie-Einstellungen zustimmst! Du kannst auswählen, ob du allen zustimmst oder nur den Cookies, die für die Funktion der jeweiligen Internetseite notwendig sind. Eine persönliche Auswahl kannst du unter „Einstellungen“ treffen. So kannst du dich vor personalisierter Werbung schützen und davor, dass mehr Daten als notwendig von dir gesammelt und an Dritte weitergebeben werden.
- Lösche regelmäßig deine Cookies! Du kannst in den Privatsphäreeinstellungen deines Browsers auch festlegen, dass alle Cookies gelöscht werden, wenn du deinen Browser schließt. Gleiches gilt auch für Suchverläufe und besuchte Internetseiten.
- Browser-Add-ons helfen dir dabei, Cookies und Werbung zu blockieren. Leider funktionieren manche Internetseiten nur mit Cookies.
- Für Smartphone und Computer gibt es kleine Apps und Programme, die dir dabei helfen „aufzuräumen“: Browserverläufe, ungenutzte Daten sowie Cookies zu verwalten und zu löschen, z. B. CCleaner.
- Hast du Cookies einmal zugestimmt, kannst du deine Erlaubnis in den Datenschutz-Einstellungen der jeweiligen Internetseite auch widerrufen oder ändern!
- Achte auf sichere Passwörter und ändere Passwörter sofort nach dem Kauf eines Geräts. Nutze zudem unterschiedliche Passwörter.
- Regelmäßige Updates schützen auch deine Daten. Bring deine Geräte und Apps auf den neuesten Stand, damit weniger Sicherheitslücken entstehen können.
- Du musst nicht immer deinen richtigen Namen, dein korrektes Geburtsdatum oder deine meistverwendete E-Mail-Adresse angeben, wenn du im Internet ein Konto erstellst.
- Nutze verschiedene E-Mail-Adressen für unterschiedliche Angebote im Netz. Du kannst dir bspw. eine E-Mail-Adresse ohne deinen richtigen Namen nur für Social Media einrichten.
- Melde dich nicht mit deinem Google Account oder Konten sozialer Medien wie Facebook bei anderen Seiten an! Sonst können noch mehr Daten über dich zusammengeführt werden.
- Gönn dir offline-Zeit, schalte auch mal dein Smartphone aus oder lass es zu Hause! Auch dein Fitness-Tracker muss nicht immer dabei sein. Setz ihn gezielt beim Sport ein.

Hinweise zu Aktivitätsphase II: Informationsflyer zu Datenschutztipps für den Alltag (2/2)

- Überprüfe die Einstellungen von Google-Maps. Diese App zeichnet deine Bewegungsverläufe auf, wenn du es nicht bewusst ausschaltest. Es gibt Alternativen, z. B. OpenStreetMap oder Maps.me, die mit offenem Kartenmaterial arbeiten und offline funktionieren.
- Schalte Sprachassistent:innen und Smart Speaker aus, wenn du sie nicht benutzt, damit diese nicht immer zuhören können.
- Überlege dir, wo dein Smart Speaker überall dabei sein darf. Dein:e Sprachassistent:in lernt auch, weil echte Menschen die Sprachbefehle verschriftlichen und korrigieren. Möchtest du, dass dein Smart Speaker theoretisch jedes private Gespräch mit deinen Freund:innen mithören kann?
- Wäge ab, welche Standort-Informationen, Tracking- und Fitnessdaten du in sozialen Netzwerken teilen willst und welche du lieber für dich behältst.
- Es gibt Suchmaschinen, die deine Privatsphäre besser schützen als Google. Sie erlauben dir z. B. anonym und ohne Tracking-Cookies im Internet zu suchen. Beispiele sind: startpage, duckduckgo, metaGer oder die umweltfreundliche Suchmaschine ecosia.
- Probier unterschiedliche Browser aus! Chrome, Internet Explorer und Safari schützen deine persönlichen Daten nicht so gut wie z. B. Mozilla Firefox, Opera, Tor, Comodo „Dragon“ und „Ice Dragon“ sowie Brave. Sie lassen dich anonym surfen.
- Achte auf die Adresszeile deines Browsers. Dort sollte immer https:// vor der Adresse stehen statt http://. Dafür gibt es auch extra Browser-Add-ons.
- Die Datenschutzbestimmungen und AGBs kannst du auch in Ruhe nachlesen. Internetseiten müssen sie bereitstellen. Ist dir etwas unklar, schau doch mal auf datenschutz.org, klicksafe.de, handysektor.de oder verbraucherzentrale.de vorbei.