Privatsphäre und Datenschutz im Internet

Immer mehr Daten werden heute im Internet abgespeichert – bewusst oder unbewusst. Aber wie sicher sind Ihre persönlichen Daten?

Schützen Sie sich und Ihre Daten im Internet:

- Verwenden Sie Ihren Browser sicher.
- Gehen Sie mit Passwörtern sorgsam um.
- Seien Sie im Umgang mit Sozialen Medien vorsichtig.
- Seien Sie im Umgang mit Cloud-Speichern vorsichtig.
- Konfigurieren Sie Ihr Betriebssystem sicher.

Verwenden Sie Ihren Browser sicher

Der Browser ist das Tor ins Internet. Betreffend Datenschutz sollten Sie einige relevante Einstellungen vornehmen.

Löschen oder verhindern Sie das Abspeichern von Cookies

Cookies sind Textdateien, welche Informationen über Ihr Surf-Verhalten speichern. Nach der Beendigung Ihrer Internet-Sitzung sollten Sie diese löschen (https://www.ebas.ch/browserverlauf-loeschen/). Alternativ können Sie auch im Inkognito- oder Privat-Modus surfen, damit Ihr Browser erst gar keine Daten speichert.

Speichern Sie keine Passwörter im Browser ab

Das Abspeichern von Passwörtern im Browser ist sehr unsicher. Verwenden Sie stattdessen einen Passwort-Manager (https://www.ebas.ch/4-schuetzen-der-online-zugaenge/).

Nutzen Sie sichere Suchmaschinen

Google ist die meistgenutzte Suchmaschine, sammelt aber sehr viele Daten über Sie und Ihr Surf-Verhalten. Verwenden Sie Alternativen wie «DuckDuckGo (https://duckduckgo.com/)», die keine persönlichen Daten analysieren oder speichern.

Verwenden Sie eine Anti-Tracking-Software

Erweiterungen für die gängigen Browser wie etwa «Ghostery (https://www.ghostery.com/)» blockieren beim Surfen versteckte Dienste, die im Hintergrund private Daten übermitteln. Weitere Informationen (https://www.ebas.ch/ad-blocker-und-anti-tracking-tools/)

Gehen Sie mit Passwörtern sorgsam um

Web-Shop, E-Mail-Konto, E-Banking etc.: Sichere Passwörter sind zur Identifikation des Benutzers unerlässlich.

Verwenden Sie sichere Passwörter

Wichtig dabei ist, nicht nur ein komplexes Passwort (http://www.ebas.ch/securepassword) zu wählen, sondern auch

überall verschiedene Passwörter zu verwenden.

Verwenden Sie einen Passwort-Manager
Kaum jemand kann sich all seine Passwörter merken. In einem Passwort-Manager (http://www.ebas.ch/securepassword) können Sie sämtliche Passwörter verschlüsselt abspeichern.

Seien Sie im Umgang mit Sozialen Medien vorsichtig

Soziale Medien wie Facebook, Twitter oder Instagram sind aus dem Alltag nicht mehr wegzudenken, erfordern aber einen verantwortungsvollen Umgang.

Kommunizieren Sie zurückhaltend
Veröffentlichen Sie nur Informationen, welche Sie auch einem wildfremden Menschen auf der Strasse erzählen würden. Weitere Informationen (http://www.ebas.ch/socialmedia)

Konfigurieren Sie Ihre verwendeten Social Media sicher
Schränken Sie den Zugriff auf Ihre veröffentlichten Informationen ein. Unsere Anleitungen unterstützen Sie bei der sicheren Konfiguration von Facebook (https://www.ebas.ch/facebook-einstellungen/), Twitter (https://www.ebas.ch/twitter-einstellungen/), Instagram (https://www.ebas.ch/instagram-einstellungen/) und LinkedIn (https://www.ebas.ch/linkedin-einstellungen/).

Seien Sie im Umgang mit Cloud-Speichern vorsichtig

Das Auslagern von Daten ins Internet mit beispielsweise Dropbox, OneDrive, Google Cloud oder iCloud ist bequem. Doch auch hier gilt es Aspekte zur Sicherheit zu beachten.

Wählen Sie einen geeigneten Cloud-Anbieter
Die grossen internationalen Anbieter speichern Ihre Daten in der Regel im Ausland, was zu einer Verletzung des hiesigen Datenschutzgesetzes führen kann. Wählen Sie daher nach Möglichkeit einen Schweizer Anbieter (https://www.ebas.ch/cloud-speicher/).

Verwenden Sie Cloud-Speicher sicher
Nutzen Sie wenn möglich eine Zwei-Faktor-Authentisierung (http://www.ebas.ch/securepassword), wie sie beim E-Banking eingesetzt wird, und erstellen Sie auch von Ihren Daten in der Cloud regelmässig lokale Backups (https://www.ebas.ch/1-sichern-der-daten/).

Konfigurieren Sie Ihr Betriebssystem sicher

Viele Betriebssysteme senden regelmässig Berichte über den Anwendenden an den Systembetreiber. Diese Funktion kann in der Regel zumindest teilweise unterbunden werden.

Schränken Sie in Windows die Datenübermittlung ein
Windows analysiert unter anderem personenbezogene Daten und übermittelt diese teilweise auch an Microsoft. Die Datenübermittelung lässt sich jedoch stark einschränken (https://www.ebas.ch/datenschutz-windows-10/).

Datenschutz und Informationspflicht

Gemäss schweizerischem Recht werden Website-Betreibern einige Pflichten auferlegt, um den Datenschutz zu gewährleisten. So sind ein Impressum sowie eine Datenschutzerklärung vorgeschrieben.

Jede Website muss die Besucher darüber informieren, welche personenbezogenen Daten erhoben und gespeichert werden und zu welchem Zweck. Zu den personenbezogenen Daten gehören auch Online-Kennungen, wie beispielsweise die IP-Adresse und das Klickverhalten. Also etwas, was fast jede Website speichert.

Zudem gilt die Auskunftspflicht: Möchten Sie erfahren, welche Daten über Sie gespeichert werden, haben Sie das Recht, kostenlos Auskunft darüber zu erhalten. Sind gespeicherte Daten falsch, müssen diese auf Ihren Wunsch hin berichtigt oder gelöscht werden.

Wie sicher sind Ihre Daten im Internet? Die Beantwortung dieser Frage ist nicht ganz einfach. Zum einen müssen Internet-Dienstleister gewisse Anforderungen erfüllen. Zum anderen können Sie selber aber auch Massnahmen ergreifen, um Ihre Daten im Internet zu schützen.