

Sicherheit im Internet - darauf soltest DU achten!

Das Internet ist ein täglicher Begleiter. Egal ob Onlineshopping, Social Media oder Paketverfolgung - alles können wir im Internet erledigen. Dabei gibt es einige Sicherheitslücken und Gefahren.

Anlässlich des europäischen Tages des Datenschutzes haben wir 10 Tipps für Dich zusammengefasst, die Dir helfen, im World Wide Web sicherer unterwegs zu sein.



1

Privates sollte privat bleiben

Wahrscheinlich würdest Du wildfremden Personen nicht Deine Adresse oder Deinen vollständigen Namen verraten. Im Internet fällt es vielleicht nicht so schnell auf, dass diese Daten für so gut wie jede*n frei zugänglich sind und es besteht schnell die Gefahr, dass Du zu viel von Dir preis gibst. Hier gilt: weniger ist mehr. Bevor Du also Deine persönlichen Daten bei der X. Website für die Registrierung angibst, wäge ab, ob dies wirklich notwendig ist.

2

Sichere Passwörter

Bei der Wahl Deines Passwortes solltest Du kreativ sein und nicht auf unsichere wie „123456“ zurückgreifen. Am besten ist eine Kombination aus großen und kleinen Buchstaben, Zahlen und Sonderzeichen. Diese solltest Du außerdem nicht schriftlich festhalten, sondern z. B. Programme für die Kennwortverwaltung nutzen.

3

Datenlecks überprüfen

Kennst Du schon die Website von HPI? Hier kannst Du kostenlos checken, ob Deine E-Mail Adresse in bestehenden Datenveröffentlichungen verwickelt ist oder ob Deine Daten im Internet schon frei zugänglich sind. Unternehmen können gegen eine Gebühr regelmäßig Listen mit erhalten, die zeigen, welche E-Mail-Adressen von einem Datenleck betroffen sind.

4

Vorsicht bei E-Mails und Nachrichten

Bei E-Mails und Nachrichten, die Links oder Anhänge enthalten, solltest Du immer besonders vorsichtig sein. Oft verbergen sich hinter solchen E-Mails Betrüger, die sich unter falschem Namen verstecken. Wenn Du keinen Link oder Dateien vom Absender erwartest, solltest Du also immer lieber telefonisch nachhaken. Wenn der Absender sagt, er habe Dir keine Dateien geschickt, handelt es sich um eine Betrugsmasche.



5

Zwei-Faktoren-Verifizierung

Vielleicht kennst Du Sicherheitscodes, die Dir per SMS geschickt werden, damit Du Dich an Deinem Laptop für z. B. Onlinebanking anmelden kannst. Solche Zwei-Faktoren-Verifizierungen schützen vor Hackerangriffen auf Deine Passwörter und werden bei diversen Anbietern angeboten.

6

Nicht alles gehört ins Internet

Würdest Du einer fremden Person auf der Straße Fotos von Dir am Strand im Bikini zeigen? Oder von Deinen persönlichen Problemen erzählen? Wahrscheinlich nicht. Im Internet ist die Verlockung allerdings oft groß, solche sensiblen Inhalte zu teilen. Gerade Jugendlichen ist meist nicht bewusst, dass Millionen Menschen Zugriff auf diese Daten haben und auch potenzielle Arbeitgeber diese finden können.

7

Keine Fotos von Finanzinformationen

Es würden wohl jede*r zustimmen, dass man Fotos von Bank- oder Kreditkarten nicht im Internet veröffentlichen sollte. Allerdings kommt es immer noch oft vor, dass solche sensiblen Informationen online zu finden sind. Achte also genau darauf, was sich noch alles auf Deinem Schreibtisch befindet und welche Browserfenster Du geöffnet hast, bevor Du ein Bild von Deinem neuen Laptop postest. Durch die geöffnete Onlinebanking Homepage oder das Herumliegen Deiner Bankkarten können sonst schnell Informationen wie Kontonummern, Sicherheitscodes und Ablaufdaten von (Kredit-)Karten im Internet landen.

8

Back-Ups

E-Mails, Dokumente, Fotos - alles, was Dir wichtig ist, solltest Du mit einem Back-Up sichern. Es gibt sowohl online Backups (Cloud) als auch offline Back-Ups. Egal, wo für Du dich entscheidest, das Backup sollte in jedem Fall verschlüsselt abgespeichert werden. Bei offline Backups solltest Du zu externen Speichermedien greifen, die an einem anderen Ort aufbewahrt werden. So sind Deine Daten auch dann noch geschützt, wenn z. B. durch einen Brand das komplette Büro und somit die kompletten Daten zerstört werden.

9

HTTP und SSL

Das Hypertext Transfer Protocol Secure (https) oder die Datenübertragung über einen Sicherheitsserver wie Secure Sockets Layer (SSL) zeigen Dir, dass es sich um eine vertrauenswürdige Internetseite handelt. Wenn Du darauf achtest, kannst Du ohne Bedenken auch in neuen Online-Shops einkaufen.

10

Schutz für Deinen PC

Es gibt Programme, auf die Du getrost verzichten kannst - Virenschutz gehört nicht dazu! Um Deinen PC und damit Deine Daten bestmöglich zu schützen, solltest Du Dir regelmäßig Zeit für Updates und Virenschutz nehmen.

