



Medien und Informatik für PS

Frag Fred

Was ist ein sicheres Passwort?

7:46 Minuten

Hacker 01:00 Es gibt verschiedene Methoden, um Passwörter zu knacken. Die einfachste Methode ist eine Person dabei zu beobachten, wie sie ihr Passwort eingibt. Hacker gehen meist systematischer vor: Sie klauen Passwort-Tabellen von Servern und entschlüsseln sie. Diese verkaufen sie im Dark Web oder nutzen sie, um an Bank- und Kreditkartendaten zu gelangen. Erpressung ist ebenfalls ein gängiges Mittel, um an Geld zu gelangen.

Sichere Passwörter 02:15 Damit ein Account nicht gehackt werden kann, braucht es ein sicheres Passwort. Kurze Passwörter, die nur aus Zahlen bestehen, sind schnell geknackt. Besteht ein Passwort aus Zahlen, Gross- und Kleinbuchstaben und Sonderzeichen, dauert es länger, bis es geknackt werden kann. Grundsätzlich gilt: Je länger, desto sicherer.

Unsichere Passwörter 03:49 Hacker kennen die am häufigsten benutzten Passwörter und probieren diese in der Regel als Erstes aus. Unsicher sind Begriffe, die im Wörterbuch stehen, bekannte Namen und Orte, Jahreszahlen oder das eigene Geburtsdatum. Deshalb sollte man sich möglichst ein Fantasiewort ausdenken und dieses mit Zahlen und Sonderzeichen kombinieren.

Merksatz 05:13 Längere Passwörter kann man sich nicht gut merken. Abhilfe kann ein Merksatz schaffen. Die Anfangsbuchstaben der einzelnen Wörter werden mit Zahlen und Sonderzeichen ergänzt.

Passwort aufschreiben 05:35 Um sich ein Passwort merken zu können, darf man dieses auf einen Zettel schreiben. Diesen sollte man jedoch an einem sicheren Ort aufbewahren und vernichten, sobald man das Passwort auswendig kennt. Keinesfalls sollte man das Passwort ungesichert in eine Textdatei etc. schreiben.

Zwei-Faktor-Authentifizierung 06:50 Die Zwei-Faktor-Authentifizierung bietet zusätzliche Sicherheit und besteht aus zwei Eingaben