

Sichere Passwörter

ICH BIN'S, *****



... und die Moral von der Geschichte...

Passwortschutz fängt bei Ihnen zu Hause an. Sie selbst können dazu beitragen, Ihr System und Ihre privaten Daten vor Unbefugten zu schützen. Sie lassen ja auch nicht jeden in Ihre Wohnung, oder? Verhindern Sie den Diebstahl, die Veränderung und den Missbrauch Ihrer Daten.

Nachfolgend ein paar Regeln, die Ihnen die Erstellung von sicheren Passwörtern und deren Umgang erleichtern sollen:

Geheime Passwörter

Geben Sie Ihre Passwörter nicht an Freunde, Bekannte oder Fremde weiter. Bewahren Sie Passwörter verdeckt auf und nicht an Orten wie der Pinnwand oder am Monitor. Speichern Sie auch nicht die Passwörter im Computer (z. B. im Browser, in Textdateien oder Tabellen).

Zeichenmix

Verwenden Sie keine bekannten Wörter, Namen und Zahlenkombinationen. Tier- und Spitznamen, Geburtsdaten und Vergleichbares sind tabu! Nutzen Sie scheinbar unvorhersehbare Kombinationen aus Buchstaben, Zeichen, Sonderzeichen, Zahlen. Verwenden Sie z. B. die Anfangsbuchstaben einer Liedzeile mit Satzzeichen und ergänzen diese um weitere Sonderzeichen und Zahlen. Ersetzen Sie auch Buchstaben durch Zahlen (z. B. „3“ für „E“). Aus der Liedzeile „Ein Männlein steht im Walde ganz still und stumm, Es hat von lauter Purpur ein Mäntlein um.“ wird z. B. das Passwort „EMSiWgsus,3hvlPeMu.“ (Dieses Beispiel nicht verwenden.) Verwenden Sie diese Methode auch bei der Beantwortung von Sicherheitsfragen, die diverse Dienste als zweiten Schutz vorgeben.

Unterschiedliche Passwörter / kein Passwortrecycling

Verwenden Sie für jeden Zugang ein neues sicheres Passwort und niemals dasselbe. Benutzen Sie keine alten Passwörter erneut. Bedenken Sie auch Verbindungen von z. B. Mailaccount zu Shoppingaccount, wobei oft die Mailadresse schon der Nutzername ist.

Voreingestellte Passwörter ändern

Voreingestellte Passwörter dienen lediglich zum ersten Schutz. Diese stehen jedoch oft in Handbüchern, auf Klebeetiketten am Gerät oder Sie haben diese per Mail erhalten. Fremde können diese Daten ablesen oder abgefangen haben, möglicherweise sind diese sogar noch im Mailpostfach unter den Mails abgelegt. Denken Sie daran, sämtliche Hardware (Internetrouter/DSL-Modem/Repeater/Powerline), sowie die Datenübertragung (z. B. WLAN) mit sicheren Passwörtern zu versehen.