



Newsletter zum Datenschutz

Sicherheitslücke Passwörter

In einer zunehmenden digitalisierten Welt spielen Passwörter eine wichtige Rolle. Die vierstellige PIN einer EC Karte kann ein herkömmlicher PC in 0.0000025000 Sekunden knacken. Umso erstaunlicher ist, dass „123456“ das beliebteste Passwort 2014 war. Viele verwenden ein Passwort für alle ihre Anwendungen. Das macht das Hacken von Passwörtern sehr lukrativ. Hier einige Tipps für den richtigen Umgang mit Passwörtern:

- Testen Sie Ihre Passwörter bei <https://checkdeinpasswort.de> oder <http://www.passwortliebe.de>. Hier erhalten Sie sämtliche Informationen, wie ein sicheres Passwort aussehen muss.
- Verwenden Sie für jede Anwendung verschiedene Passwörter. Passwort-Container wie „KeePass“ oder „1Password“ sind empfehlenswert (siehe Kasten).
- Ändern Sie Ihre Passwörter in regelmäßigen Abständen.
- Schreiben Sie sich Passwörter nur auf Papier auf, wenn Sie es auch sicher absperren können. Lassen Sie ein solches Dokument niemals unbeaufsichtigt!

Passwort-Container

Stellen Sie sich so einen Container wie einen Passwort Manager vor. Alle Passwörter werden in einer Datenbank gespeichert und durch ein „gutes“ Masterpasswort geschützt. Sie müssen sich also nur noch **ein** Passwort merken. Abhängig vom verwendeten Programm sind weitere Sicherheitsmaßnahmen möglich, wie z.B. der Fingerabdruck.

Wichtige Regeln im Schulalltag

- **USB-Sticks** auf denen personenbezogene Daten gespeichert sind, müssen verschlüsselt werden.
- Die **Präsentation einer Notenliste** vor der ganzen Klasse ist nicht zulässig.
- **Papierdokumente**, die personenbezogene Daten enthalten, dürfen für Schüler nicht zugänglich sein. Beispielsweise ist es unzulässig, Dokumente auf dem Lehrertisch abzulegen und das Klassenzimmer zu verlassen. Ein im Schulhaus ausreichender Schutz ist gewährleistet, wenn die Dokumente in einer geschlossenen (nicht verschlossenen) Tasche aufbewahrt werden.
- Bei Verdacht, dass ein Schüler während des Unterrichts mit seinem Handy Filme bzw. Fotos vom Lehrer erstellt hat, ist eine **Durchsicht des Handys** nicht zulässig.
- Lehrer, die sich an einem Computer angemeldet haben, müssen beim Verlassen des Arbeitsplatzes das Betriebssystem sperren oder sich abmelden (**Zugangsschutz an Computer**).
- **Entsorgen von Dokumenten** mit personenbezogenen Inhalten: Die Dokumente nie in einen Papierkorb werfen, sondern in den Schredder oder in die Datenschutzbox geben. Datenträger müssen mechanisch zerstört werden. Dies gilt auch beim Ausmustern von privaten Rechnern, wenn auf ihnen schulische Daten abgelegt wurden.
- Das **Versenden von E-Mails** mit personenbezogenen Daten ohne SSL-Verschlüsselung ist nicht zulässig.

„Datenschutz-Tipps für Jugendliche - So sind Deine Daten im Internet sicher!“

Dieser Flyer klärt Jugendliche darüber auf, welche Folgen die unbedachte Weitergabe und Verbreitung persönlicher Daten im Internet haben kann. Neben grundlegenden rechtlichen Rahmenbedingungen werden Sicherheits-Tipps vorgestellt. Außerdem zeigt der Flyer auf, wie man sich als „Datenprofi“ in Sozialen Netzwerken verhält. Auch der faire Umgang mit den Daten anderer wird behandelt. Konkrete Tipps, wie man bei Datenschutzverletzungen reagieren sollte, einschließlich der Nennung kompetenter Ansprechpartner für alle Fragen zum Thema Datenschutz runden den Flyer ab. Kostenlos als download + kostenfreie Flyer unter: www.klicksafe.de

