Die zehn Passwort-Gebote

1 “Verleihen” Sie Ihr Passwort auf keinen Fall an irgend jemanden!
Passwörter sind nur nützlich, solange sie geheim gehalten werden können.

2 Benutzen Sie niemals Begriffe, die im Wörterbuch stehen.
Organisierte Kriminelle benutzen automatisierte Programme, die jedes Wort mit Lichtgeschwindigkeit ausprobieren. Auch persönliche Daten wie Autokennzeichen, Geburtsdaten, Tiernamen, Sportteams oder Namen von Angehörigen mögen leicht zu merken sein, sind aber ebenso leicht zu erraten und eigenen sich deshalb nicht als Codes. Dasselbe gilt für Tastaturfolgen wie z.B. „12345678“ oder „qwertz“.

3 Benutzen Sie, sofern möglich, mindestens 11 Zeichen, besser mehr. Je länger das Passwort, um so schwerer ist es zu erraten. WLAN-Passwörter sollten eher 20 Zeichen umfassen.

4 Verwenden Sie eine Kombination aus Buchstaben und Zahlen, schließen Sie möglichst Sonderzeichen ein. Mischen Sie Groß- und Kleinbuchstaben. Das Passwort “lOx94Rv!”$gT3” ist schwieriger anzugreifen als “Darling”. Einfacher machen Sie es sich , wenn Sie aus Merksätzen ein Passwort ableiten:
„Am liebsten esse ich Pizza mit vier Zutaten und extra Käse!“ - „AleiPm4Z+eK!“

5 Notieren Sie Ihr Passwort nirgendwo, wo es gefunden werden könnte.
Bewahren Sie es nicht in Ihrer Brieftasche oder in Ihrem Portemonnaie auf. Bitte auch nicht in der Schublade in der Nähe Ihres Computers. Speichern Sie Passwörter nicht im Browser – auch wenn es bequem ist…

6 Nutzen Sie unterschiedliche Passwörter!
Falls Sie gehackt werden sollten, hat der Angreifer zumindest nicht Zugang zu allen accounts.

7 Verwalten Sie die Passwörter am besten in einem digitalen Passwortmanager, z.B. keepass!
Wenn Sie ein starkes Masterpasswort generieren, sind darin alle Passwörter sicher abgelegt.

8 Teilen Sie Ihr Passwort niemals fernmündlich mit.
Diebe, die sich am Telefon als Systembetreuer ausgaben, haben ausgesagt, erstaunlich viele Leute seien bereit, Fremden Ihr Passwort auszuplaudern.

9 Berichten Sie jeden ungewöhnlichen Vorgang, der Ihnen beim Einloggen ins Datennetzwerk auffällt, sofort Ihrem EDV Administrator.

10 Möchten Sie prüfen, ob Ihr E-Mail-Passwort geknackt wurde?
Das Hasso-Plattner-Institut (https://sec.hpi.de/ilc/) oder die Website „Have I been pwned?“ (https://haveibeenpwned.com/) geben Klarheit, ob Ihre persönlichen Identitätsdaten bereits im Internet veröffentlicht wurden.