PASSWORTSCHUTZ

Online-Dienste, Rechner und vieles mehr sind mit Benutzername und Passwort geschützt. Um sich die vielen verschiedenen Logins zu merken, tendieren Anwenderinnen und Anwender dazu, vier bis fünf nicht allzu komplexe Passwörter abwechselnd zu nutzen. Um potenziellen Angriffen entgegenzuwirken, empfehlen wir für jedes digitale Konto sein eigenes, starkes Passwort. Denn nur so wird das Sicherheitsrisiko, gehackt zu werden, minimiert. Welche Parameter starke Passwörter haben und wie diese verwaltet werden, lesen Sie in den folgenden 9 Merkmalen:

9 Merkmale für starke und sichere Passwörter

1. **Richtig starkes Passwort** ist mehr als 12 Zeichen lang und beinhaltet Zahlen, Sonderzeichen, Gross- und Kleinbuchstaben.

2. **Zwei-Faktor-Authentifizierung:** Ein zweiter Faktor bei der Authentifizierung erhöht massiv die Sicherheit. Dieser zusätzliche Faktor ist für einen Angreifer nicht leicht zu erlangen und erhöht den Aufwand für den Angriff enorm.

3. **«Passphrase»** statt Passwort, denn dies ist sicherer aber einfach zu merken; «Meine Mutter wurde am 24. März 61 in St. Gallen geboren» wäre als Passphrase «MMwa24M61iSGg».

4. **Grundregeln zur Passworterstellung:**
   - Keine Wörter aus dem Wörterbuch
   - Keine Substitution wie «o» durch «0» oder «e» durch «3»
   - Keine Haustiernamen oder ähnliche Informationen, die aus sozialen Medien entnommen werden können
   - Wenn Sicherheitsfragen zur Auswahl stehen, schwer zu erratene Optionen nehmen, auf die nur ich die Antwort kenne.

5. Ich melde mich regelmässig von den Webseiten ab und schalte meinen Computer abends aus, so dass **keine aktiven Verbindungen bestehen** bleiben.

6. **Umgang mit meinen Passwörtern:**
   - Jedes Konto hat sein eigenes Passwort
   - Ich behalte die Passwörter für mich und sage sie niemandem
   - Ich schreibe die Passwörter nicht auf
   - Ich ändere meine Passwörter regelmässig
   - Keine Varianten desselben Passworts für verschiedene Konten

7. Ich nutze eine **Passwort Security Software** (z.B. 1Password, Password Safe, SecureSafe, Keepass, etc.). So muss ich mir nur ein starkes Passwort merken und kann mir von der App komplexe Passwörter generieren lassen und abspeichern. Regelmässiges und sicheres Backup nicht vergessen ☺

8. Ich prüfe regelmässig, ob meine Login-Daten bei einem Angriff gestohlen wurden (**https://haveibeenpwned.com**).

9. **Wenn meine Login-Daten gestohlen wurden:**
   - Passwort bei den betroffenen Konten ändern
   - Hilfe holen, wenn Sie Schwierigkeiten haben
   - Zwei-Faktor-Authentifizierung aktivieren
   - Bei Kontomissbrauch alle relevanten Kontakte benachrichtigen
   - Update aller Geräte mit den letzten Hotfixes

Benötigen Sie Hilfe? Erfahren Sie mehr über unsere Cyber Defence Services und melden Sie sich: **cdc@netcloud.ch**

NETCLOUD ICT PROFESSIONALS
BERN WINTERTHUR BASEL