

## Einfache und sichere PIN und Passwortverwaltung

### Folgende Situationen müssen berücksichtigt werden:

1. Für jedes Kreditinstitut sollte eine separate PIN verwendet werden, um die Sicherheit zu erhöhen.
2. Für jeden Internetlieferanten, bei dem Sie eine Kundenbeziehung eingerichtet haben, muss ein separates Passwort benutzt werden. Etliche Internetshops, z.B. Ihre Energielieferanten, speichern Ihre Kontoverbindung - im Falle des Diebstahls von Passwort und Kontoverbindung wäre Tür und Tor für Manipulationen geöffnet. Wenn dies nicht gewollt ist, bleibt man besser immer Gast und gibt seine Daten jeweils neu ein. Auch von einem Trojaner in Ihrem PC kann eine solche Manipulation ausgehen, wenn Sie dafür keinen ausreichenden Schutz aufgebaut haben.
3. Auf jeden Fall muss verhindert werden, dass der Internetlieferant die Kontodaten abspeichert. Deshalb sollten bei jeder Aktion mindestens die Kontodaten neu eingegeben werden. Im persönlichen Bereich des Käufers ist anschließend zu prüfen, ob der Lieferant nicht doch die Kontodaten abspeichert. Sie sollten dann unmittelbar danach gelöscht werden.
4. Die PINs und die Passwörter sollten so gewählt werden, dass man sich diese merken kann.

### Vorschlag für eine sichere und leicht merkfähige PIN- und Passwort-Syntax:

1. Für die **PIN** wählt man für die ersten vier numerischen Zeichen zum Beispiel ein Geburtsdatum (Tag, Monat) vom Großvater bzw. von der Großmutter, das nirgendwo in Unterlagen im Haus verzeichnet ist, aber allen Beteiligten bekannt ist. Die Zeichen danach wählt man aus dem Namen des Kreditinstituts und übersetzt diese anhand der Telefontastatur in numerische Zeichen, also z.B. Commerzbank, zweites und drittes Zeichen = 66 (aus mno)
2. Die **Passwörter-Syntax** besteht aus alphanumerischen Zeichen mit Grossbuchstaben, mindestens achtstellig. Da viele Anbieter inzwischen aus Sicherheitsgründen bis zu zwei Grossbuchstaben verlangen, sollten die ersten beiden Buchstaben GROSS sein. Für die ersten vier Alphazeichen wählt man einheitlich einen im Benutzerkreis bekannten Begriff, z.B. einen Nicknamen. Für die Stellen 5 – 7 wählt man aus den ersten vier Stellen des Internet-Lieferanten drei Stellen aus und übersetzt diese Alphazeichen ebenfalls anhand der Telefontastatur in numerische Zeichen, also z.B. Amazon zweites bis viertes Zeichen = 629. Als achttes Zeichen wählt man einen festen Großbuchstaben, um die Sicherheit des Passwortes weiter zu erhöhen.

3. Die Passwortsyntax kann mit Hilfe des Portals <https://wiesicheristmeinpasswort.de/> getestet werden. Reicht die Sicherheit nicht aus, sollten weitere feste Begriffe im Wechsel zwischen numerischen Zeichen und Grossbuchstaben angefügt werden – aber Achtung, man muss diese Werte auch im Kopf behalten können, um die Grundidee dieses Vorschlages nicht zu verlassen.
4. Die Regeln sind – verschlüsselt natürlich – zu dokumentieren, damit im Krankheitsfall Familienangehörige in der Lage sind, z.B. Rechnungen zu bezahlen bzw. bei Lieferanten – Energieversorger – online Aktionen durchzuführen.