

# Axians-Regeln für einen sicheren Umgang mit Passwörter

## VERWENDEN SIE STARKE PASSWÖRTER



Ein sicheres Passwort muss lang und komplex sein, beispielsweise ungefähr 10 Zeichen mit mindestens einem Klein- und einem Grossbuchstaben, einer Zahl und wenn möglich mit einem Sonderzeichen.

Es ist schwierig, eine Vielzahl von starken Passwörtern im Kopf zu behalten. Darum versuchen viele dem Gedächtnis zu helfen, indem auf persönliche Daten zurück gegriffen wird. Solche Passwörter können mit Hilfe öffentlich verfügbaren Informationen, Sozialen Medien herausgefunden und somit erraten werden. Darum achten Sie sich darauf, keine ganzen und richtigen Wörter von z. B. Namen, Ort, ... aufzuschreiben.

## PASSWÖRTER REGELMÄSSIG ÄNDERN



Auch wenn Sie ein sicheres und starkes Passwort verwenden, ist es äusserst wichtig es regelmässig zu ändern. Leider dauert es manchmal eine gewisse Zeit bis festgestellt wurde, dass das Konto mit dem dazugehörigen Passwort kompromittiert worden ist. Deshalb ist es von Vorteil einen Zeitplan für das Wechseln der Passwörter zu erstellen.

## PASSWÖRTER NIE AUFSCHREIBEN



Notieren Sie keine Passwörter! Weder auf Papier, auf dem Smartphone, oder sonst wo. Es sei denn, Sie haben ein Passwort-Tool, wo sehr gut gesichert ist!

## VERWENDEN SIE IHRE PASSWÖRTER NICHT MEHRFACH



Wichtig ist nicht für mehrere Konten dasselbe Passwort zu verwenden. Im Idealfall sollte jedes Konto mit einem einzigartigen Passwort geschützt sein, egal ob Nachrichtendienst, E-Banking, Forum, oder Buchungs-Website. Zudem muss man sicherstellen, dass die Passwörter auf den Routern und anderen Peripherie-Geräten regelmässig aktualisiert werden. Die Passwörter an den Geräten und Arbeitsplätzen der Mitarbeitenden sollten in regelmässigen Abständen aktualisiert werden.

## BEHALTEN SIE IHRE PASSWÖRTER FÜR SICH



Die Sicherheit des stark erstellten Passwortes ist (höchstens) nur so lange gewahrt, wie das Passwort geheim bleibt. Per Definition ist ein Passwort ein geheimes Wort oder eine geheime Formulierung, die stets geheim bleiben soll, das heisst, es Dritten nicht bekannt ist. Darum müssen Sie stets vorsichtig mit Passwörtern umgehen!