Compliance Today - June 2022
Password conundrum

By Jan Elezian, MS, RHIA, CHC, CHPS

Jan Elezian (jan.elezian@sunhawkconsulting.com) is a consultant and Director at SunHawk Consulting, LLC.

- linkedin.com/in/jan-elezian-30821011/

Jan Elezian

There's an app for just about everything these days. Online banking, games, email, services, shopping, and even accessing your health records require a password to enter. Each application asks you to supply a secret password that stops other people from entering without your permission. The Cybersecurity & Infrastructure Security Agency experts guide us to create a strong, complex password that is difficult for others (hackers) to guess.[1] Every application has rules for creating what it construes to be a strong and complex password. Some dictate at least eight characters but fewer than 12. Others ask for at least one capital letter, a number, and a symbol. Some have a combination of each. Added to the recommendation that passwords are unique, the user has the conundrum of remembering and storing potentially dozens of passwords.

This document is only available to members. Please log in or become a member.

Become a Member Login