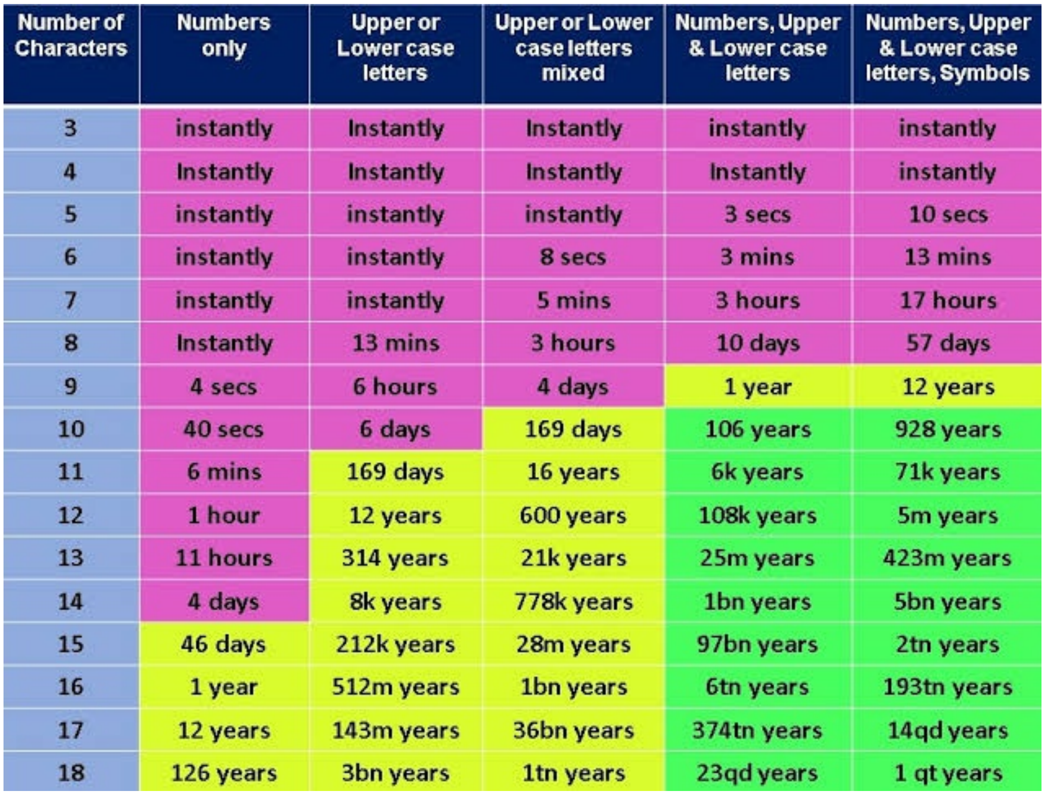
WRW LEGAL

FSI TRUST SOLUTIONS

Password Security for Funeral Homes and Cemeteries

One of the security measures FSI clients must remain aware of every day is password management. Passwords are intended to protect personal data from unauthorized access. A weak, common, re-used or easily guessed password all can create security issues and expose personal data to unauthorized users.

Weak passwords are short and lack a mix of letters, numbers, cases and punctuation. A weak password can be hacked by a computer in the amount of time based on the chart below. **Passwords of less than ten characters that use only numbers can be guessed instantly, while passwords of 14 characters that include numbers, uppercase letters and lowercase letters will take 2,000 years to hack.**



Number of Characters	Numbers only	Upper or Lower case letters	Upper or Lower case letters mixed	Numbers, Upper & Lower case letters	Numbers, Upper & Lower case letters, Symbols
3	instantly	Instantly	Instantly	instantly	instantly
4	Instantly	Instantly	Instantly	Instantly	instantly
5	instantly	instantly	instantly	3 secs	10 secs
6	instantly	instantly	8 secs	3 mins	13 mins
7	instantly	instantly	5 mins	3 hours	17 hours
8	Instantly	13 mins	3 hours	10 days	57 days
9	4 secs	6 hours	4 days	1 year	12 years
10	40 secs	6 days	169 days	106 years	928 years
11	6 mins	169 days	16 years	6k years	71k years
12	1 hour	12 years	600 years	108k years	5m years
13	11 hours	314 years	21k years	25m years	423m years
14	4 days	8k years	778k years	1bn years	5bn years
15	46 days	212k years	28m years	97bn years	2tn years
16	1 year	512m years	1bn years	6tn years	193tn years
17	12 years	143m years	36bn years	374tn years	14qd years
18	126 years	3bn years	1tn years	23qd years	1 qt years

According to Recode, people re-use passwords across websites up to 31% of the time. A password hack anywhere on the internet could expose data protected by that password.

Additionally, hackers will first turn to easily guessed passwords when trying to access personal data. Easily guessed passwords include:

- Sequential passwords: i.e., 12345, 1234, 1234567
- Password, password1 or admin
- Repeated numbers: i.e., 11111

The National Institute of Standards and Technology (NIST) state that passwords should:

- Be more than 8 characters
- Include a number, letter, and a punctuation mark
- Include both lowercase and uppercase letters
- Not be shared with any other website
- Not be easily guessed

In the past, experts have recommended changing your passwords every 90 days. That is no longer the case. As long as the password complies with the other guidelines, updates can be more periodic, such as every six months, as well as if or when breaches occur.

Lauren Pettine is an attorney at WRW Legal, PLLC. She can be reached at Lauren.Pettine@WRWLegal.com.