LA Cyber Lab Special Report

PUBLIC SECURITY ANNOUNCEMENT #1

January 19, 2018

Worst Passwords of 2017

These are the Top 20 Worst Passwords from 2017 as reported by Tech Republic[1]. Avoid them and protect your data.

1. 123456
2. Password
3. 12345678
4. qwerty (the first 6 letters on the top of the keyboard and also a convenient combo on some mobile devices)
5. 12345
6. 123456789
7. letmein
8. 1234567
9. football
10. iloveyou
11. admin
12. welcome
13. monkey
14. login
15. abc123
16. starwars (an example of popular social themes influencing user behavior)
17. 123123
18. dragon
19. passw0rd (because some sites were alphanumeric passwords)
20. master

Passwords remain a security issues because they are part of the identity and authentication process used to protect information. User behaviors and human nature lend themselves to poorly crafted passwords. Let's face it, entering a 20 character password every time your computer locks isn't the definition of convenience. Criminals and hacking tools know users

[1] Tech Republic (2017) www.techrepublic.com/article/the-20-worst-passwords-of-2017-did-yours-make-the-list/

tendencies and exploit them. A well-known hacking tool, John the Ripper, allows hackers to employ searches of every word in the dictionary, including foreign language dictionaries plus commonly used examples like those from the list above. Password strategies have changed over the past 15 years. Generally, good password management requires frequent changes of passwords and enforcement of quality passwords which are at least eight characters or more. Passwords with less than eight characters are often defeated by hacking tools in less than five minutes. Educating employees and users is a constant struggle but is still worth the effort. Today, experts recommend the following practices to both avoid and to employ:

GOOD PASSWORD PRACTICES[2]

- Use passwords with more than 8 characters
- Randomize the use of capital and lowercase characters
- Use special symbols such as #,&,%,$
- Change passwords every 6 months
- Include a number in your password
- Educate employees
- Change the default password for devices and accounts

BAD PASSWORD PRACTICES

- Don't use *password* or any other form of *passw0rd* as your password or any of the worst passwords listed above
- Don't use common information that can be easily guessed (such as first/middle/last names or birthdays)
- Don't use the same password for multiple accounts (admin and user accounts need different passwords; HR and Financial records systems need different passwords, too)
- Don't write down passwords and leave them in an easy to find places (like under your keyboard)
- Don't share your passwords with anyone

[2] Harris, S. (2013). *CISSP, All In One Exam Guide, Sixth Edition.* United States of America: McGraw-Hill.