Carolina
ALLIANCE BANK™

here for you. every day.

Let’s Start Taking Password Security More Seriously

New research released by SplashData reveals that many people are still making woefully poor decisions when it comes to the passwords they use to secure their online accounts.

As we all know, passwords often leak out onto the internet – which is clearly bad news for the people who own the accounts, and good news for malicious hackers who want to break into them. But another group who find leaked password databases fascinating are the security researchers interested in shining a light on the sometimes (poor) choices made by regular internet users when choosing a password.

SplashData’s chart of most commonly-chosen passwords (which thus makes them some of the very “worst” passwords you can choose) is based upon its examination of over five million passwords leaked by hackers. Truth be told, a lot more than five million passwords were grabbed by hackers in the course of 2017, but it’s still a helpful indicator of just how reckless computer users can be online.

Here’s a list of the top (i.e. worst) 30 passwords:

1. 123456
2. password
3. 12345678
4. qwerty
5. 12345
6. 123456789
7. letmein
8. 1234567
9. football
10. iloveyou
11. admin
12. welcome
13. monkey
14. login
15. abc123
16. starwars

17. *123123*
18. *dragon*
19. *passw0rd*
20. *master*
21. *hello*
22. *freedom*
23. *whatever*
24. *qazwsx*
25. *trustno1*
26. *654321*
27. *jordan23*
28. *harley*
29. *password1*
30. *1234*

Passwords like these are not only easily guessable, they're already in the password-cracking databases of any hacker worth his or her salt, alongside millions of other popular choices and dictionary words. If you, or someone you know, is using any of the passwords above online then you need to take a long hard look at yourself in the mirror. The good news is that better password security is not a hard resolution to keep, and with the right tips you have a much higher likelihood of achieving your goal than you will making the most of your gym membership.

I believe that the vast majority of computer users would benefit from running a good password manager – a program that not only securely stores your passwords, but can also generate hard-to-guess, complex passwords when you create an account on a website.

But maybe websites need to buck their ideas up as well. Not only do more websites need to do a better job of securing sensitive information (such as password databases) but they could also be more diligent in rejecting easy-to-crack passwords like those listed above or regular dictionary words.

For instance, wouldn't it be great if more sites blocked passwords that are frequently used, have been exposed in past data breaches, or if they at the very least "warned" users that they might be choosing a potentially unsafe password?

Troy Hunt's HaveIBeenPwned service makes hundreds of millions of passwords available for download for precisely this purpose. For advice on how the data might be best used to defend your website's users – be sure to check out his blog post.

Additionally, I'd love to see more website administrators make a New Year's Resolution to look into implementing two-factor authentication (2FA) – so even if login credentials do fall into the wrong hands, they won't be enough by themselves to allow a hacker to break into an account.

1
User name:
Password:

2
Your One-Time Password (OTP)

3
ESET Secure Authentication
Secure Login
958 906

Chances are that if you're a regular reader of We Live Security you have heard a lot of this advice before, and may even have (hopefully!) put it into practice. If that's the case, give yourself a pat on the back – but realize that you have your own special New Year's Resolution…

… and that's to spread the word. Tell your friends, colleagues, and loved ones how they can better defend themselves online by choosing complex, hard-to-guess, hard-to-crack passwords, and explain to them the benefits of two-factor authentication.