computer dimensions

520.743.7554
computerdimensions.net
business it solutions

Does Your Password Pass the Test?

30% of people have been the victims of a security breach caused by a weak password. By employing a few password best practices, you can avoid being one of them. In the 1990s animated series “Futurama,” a villain and her henchmen are forced to stage an elaborate ruse to obtain the main character’s passcode. While we’re still a long way from the year 3000, they were a bit overly optimistic about the future’s commitment to securing our online presence. Instead, today’s credentials too often include passwords like the one used to destroy a planet in the movie “Spaceballs” (12345). Even back in 1987, we knew that “12345” is less a secure password and more “the kind of thing an idiot would have on his luggage.” So why are so many people still securing their identities, finances and more passwords like this in 2022?

The Passwords That Don’t Pass Muster

In a study conducted by Google and Harris Poll, a full quarter of respondents had used one of the following passwords, or a variation thereof:

- abc123
- password
- 123456
- Iloveyou
- 111111
- qwerty
- admin
- welcome

These sorts of passwords can not only make you vulnerable to hackers — who with a bit of social engineering or a cursory search on social media can find out enough about you to guess your password — but also to the merely nosy. That same survey found that 27% of respondents admitted to having tried to guess another person’s password. And of those, 17%, or nearly 1 in 5, were successful.

But even people with good passwords undermine their security with bad decisions. In a Harris Poll, 78% of Gen Z, 67% of Millennials and Gen X’ers, and 60% of Baby Boomers admitted to using the same password for multiple online accounts. Worse, when security firm SpyCloud compared 1.7 billion username and password combos gathered from more than 750 leaked sources, they discovered that nearly two-thirds of people were using a password exposed in a breach for other accounts.

Don’t Pass on these Password Tips

Because anti-malware and other security measures often cannot detect threat actors who have gained access using legitimate credentials, poor password hygiene can create a nearly indetectable pathway into your network. So how do you prevent this? Luckily, there are several ways to ensure your password earns a passing grade:

1. Don’t reuse passwords! Reusing passwords can turn stolen credentials from one of your accounts into stolen credentials for ALL of your accounts. Very few things sting as badly as having your bank account compromised because you bought a pair of sneakers in 2016.

2. Don't give passwords away, either. If someone has control of your password, they have control of your account — and they can cancel it, offer access to others and more.

3. Don't use personal information in your passwords. Things like family members' names, birthdates, favorite sports teams or city of residence are known to those close to you and can be figured out through social media.

4. Check to see if your password has been involved in a breach. If you're using a well-constructed password that's been widely exposed, it isn't much better than just using one of these. Go here to see if your password has been pwned, and if it has, change it everywhere it has been used and forget about it forever.

5. Passwords should be at least 12 characters long, regardless of what combination of numbers, letters and characters is used.

6. Complex to you isn't necessarily complex to an attacker. People assume a password like T3Dl@55o will be hard to guess. And it will — for a human. But a password cracker will make quick work of it (it'll only take about 39 minutes). You're better off choosing a long passphrase than a short but complicated password. A passphrase that's at least 15 characters long, as in the well-known example CorrectHorseBatteryStaple, is significantly harder for crackers to guess (it'll take hundreds of billions of years … unless you actually use "CorrectHorseBatteryStaple," in which case it'll likely take much less time.)

7. The best passwords of all are long; include a variety of numbers, characters and special symbols; and don't make use of ordinary words. But these, understandably, can be hard to remember, so …

8. Consider using a password manager. These services can create and store long, secure and unique passwords, so you only ever have to remember one — eliminating the need to ever again deal with the "Forgot Your Password?" link.

Now that you've ditched "p@ssw0rd!" and the like for truly secure credentials, you're totally protected, right? Not necessarily — if the email provider, bank, etc., is compromised, attackers may still be able to get into your account. Utilize multifactor authentication to further help unauthorized access.

- Amber Wolff