(Approx. 391 words)

February 1 is National Change Your Password Day

Author: Dorothy Fitch*,*  Editor, GVR Computer Club, AZ

February 2020 issue Green Bytes

www.ccgvaz.org

dmfitch (at) cox.net

You know that you should pay attention to your passwords. You shouldn't reuse the same one on multiple sites, you should change them now and then, and you should use strong passwords.

But did you know that there is a special day that should inspire you to change your passwords? I just discovered that February 1 is National Change Your Password Day. (There is also a World Password Day on the first Thursday of May.)

According to an [inc.com article](https://ccgvaz.us16.list-manage.com/track/click?u=fc5b48c8cad5d194a77f4cb54&id=a53182a858&e=2857111c01), the top 10 passwords in use are:

1. 123456
2. password
3. 123456789
4. 12345678
5. 12345
6. 111111
7. 1234567
8. sunshine
9. qwerty
10. iloveyou

A different article cites ji32k7au4a83 as being a remarkably common password? Why? Because it translates to "mypassword" in English when typed on a bilingual keyboard in Mandarin Chinese. [Click to read this interesting article.](https://ccgvaz.us16.list-manage.com/track/click?u=fc5b48c8cad5d194a77f4cb54&id=d8c7627709&e=2857111c01)

So, as you head to your computer today to change your passwords in honor of this special day, keep in mind these password "best practices" from the [inc.com article](https://ccgvaz.us16.list-manage.com/track/click?u=fc5b48c8cad5d194a77f4cb54&id=12f5bf2470&e=2857111c01):

1. Don't use personal information in your password.
2. Make it memorable, but not simple.
3. Use longer passwords mixed with letters and numbers and symbols.
4. Don't re-use your passwords.
5. Use Two-Factor Authentication (when you are sent a code to your email address or phone to authenticate your identity)
6. Stategize Your Password Manager (Read [PC Magazine's article](https://ccgvaz.us16.list-manage.com/track/click?u=fc5b48c8cad5d194a77f4cb54&id=484a52c285&e=2857111c01) on Best Password Managers for 2020.)

Automated hacking systems use a "brute-force" method of simply trying random passwords to break into an account. [This analysis](https://ccgvaz.us16.list-manage.com/track/click?u=fc5b48c8cad5d194a77f4cb54&id=bab195403f&e=2857111c01) of how quickly (approximately) a password could be "guessed" using this method proves the importance of creating strong passwords. Here are some examples:

* 5 characters (3 lowercase letters, 2 numbers):  .03 seconds
* 7 characters (1 capital letter, 6 lowercase letters): 9 minutes
* 8 characters (4 lowercase letters, 2 special characters, 2 numbers): 2.6 days
* 9 characters (2 capital letters, 3 lowercase letters, 2 numbers, 2 special characters):  9.1 years

[Read the article](https://ccgvaz.us16.list-manage.com/track/click?u=fc5b48c8cad5d194a77f4cb54&id=696ec1e532&e=2857111c01) to find out a password type that would take approximately 7.5 million years to hack!

How strong is a password you have chosen? [Check it here](https://ccgvaz.us16.list-manage.com/track/click?u=fc5b48c8cad5d194a77f4cb54&id=71b7a5ac85&e=2857111c01).

So, go change your passwords. Now! (Even if is no longer Feb. 1.)