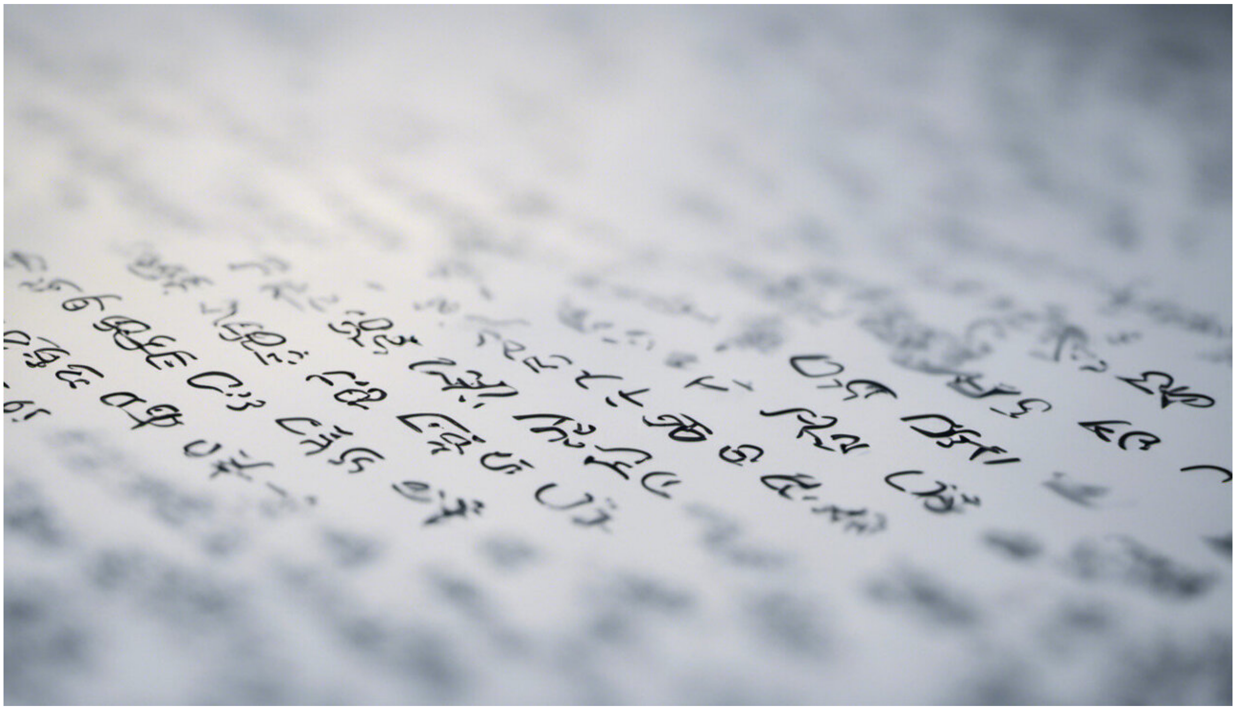
TechXplore

Choose better passwords with the help of science

August 30 2017, by Lorrie Cranor, Blase Ur, Lujo Bauer, Michelle Mazurek And Nicolas Christin



Credit: AI-generated image (disclaimer)

For years, computer users have been told they should have complicated passwords, including numbers, punctuation marks and other symbols, and upper- and lowercase letters. Despite those being hard to remember, people were told not to write their passwords down, and forced to make up new ones quite frequently. Users dutifully complied – by capitalizing the first letter of their passwords, adding a "1" or their birth year, or perhaps ending their password with an exclamation point.

Most people couldn't actually remember lots of passwords without writing them down, so instead they reused a small number of passwords over and over again. And when they were required to change their passwords, they incremented that "1" to a "2" or added another exclamation point. These simple steps to deal with complicated passwords are so common that they actually make it easier for attackers.

As researchers into password security, we've known for years that most password advice was not actually based on scientific knowledge. To address this, we have been conducting experiments about the effects of password requirements on security and usability. The federal government recently changed its password recommendations in ways that echo some of our research findings.

Defending passwords from computers

We spent years modeling how different password-cracking approaches work to better understand how attackers guess passwords and to develop an accurate measure of password strength. People who are trying to break into online accounts don't just sit down at a computer and make a few guesses. Many attackers have been able to steal the entire database of passwords from large companies – for example, this has happened to Yahoo, LinkedIn, Adobe, Ashley Madison and many others. The passwords are scrambled for security, so attackers have to make lots of guesses to unscramble them. But computer programs let them make millions or billions of guesses in just a few hours.

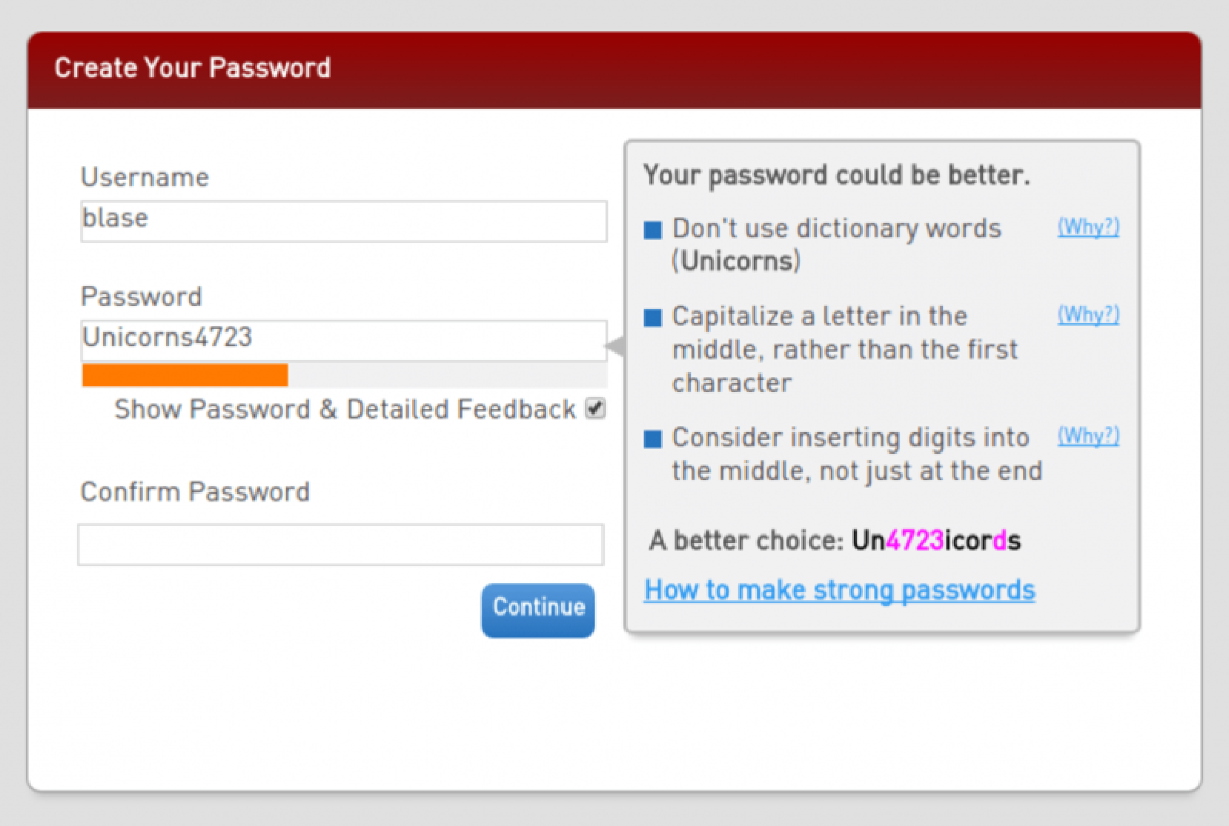
They may start by guessing all the most popular passwords and words in the dictionary, then adding "1" to each of these, and then again with every other digit and symbol, and then with the first letter capitalized, and so on. The end result is that all the complicated password policies don't prevent – or even really slow down – cracking of many users' passwords.

Even worse, once an attacker guesses a user's password for one account, he will often try using that same password on the user's other accounts. Since users tend to reuse passwords, this can be very successful. An attacker who cracks the password for some website you registered with eight years ago and forgot about may now be able to access your email, your social network account and your bank account.

All this computing power being applied to cracking passwords means users need to go beyond choosing passwords that are hard for a human to guess: Passwords need to be difficult for a computer to figure out.

Testing perceptions of password strength

Our research has informed efforts to teach people how to use this new understanding of password security. More than 50,000 people participated in our online experiments, each creating a password that complied with randomly assigned requirements: for example, "minimum of 12 characters long" or "must include lowercase and uppercase letters, digits and symbols." We measured the actual strength of the password, a participant's ability to remember a password a few days later and other metrics. We also analyzed real passwords created by students, faculty and staff at our university.



Create Your Password

Username

blase

Password

Unicorns4723

Show Password & Detailed Feedback ☑

Confirm Password

Your password could be better.

- Don't use dictionary words (Unicorns) (Why?)
- Capitalize a letter in the middle, rather than the first character (Why?)
- Consider inserting digits into the middle, not just at the end (Why?)

A better choice: Un4723icords

How to make strong passwords

A password meter provides an opportunity for advice that helps people improve their passwords. Credit: CyLab Usable Privacy and Security Laboratory, Carnegie Mellon University, CC BY-ND

Our data have shown us that people hold many misconceptions about passwords, such as believing that adding a digit or exclamation point to the end of their password will make it much stronger. This problem is widespread enough that we created an online quiz game to help dispel some of these misconceptions.

In addition, our data have shown us that it is more important to encourage longer passwords (at least 12 characters) than complicated passwords. At the same time, we've learned that some users create long passwords that are still predictable – like "passwordpassword" or "xxxxxxxxxxxx."

We also learned that giving people feedback at the moment they're creating new passwords can help. Most often this takes the form of what are called "password meters" – color-coded signals that indicate whether a person has chosen a weak password or one that's very strong.

While most password meters on the internet provide inaccurate scores and sometimes questionable advice, we developed a password meter that uses an artificial neural network to compute the strength of those passwords based on an analysis of millions of other passwords. In addition, when it identifies a weak password, our meter provides immediate advice on what would make it stronger. For example, if a person puts all the digits at the end of a password, our system might suggest moving them to the middle.

Creating strong passwords

Our research has led us to develop some specific recommendations for choosing passwords that provide good protection for online accounts and the data they contain. A crucial aid in this process is to use a password manager to generate long, random passwords – and remember them for you.

If you're making your own passwords:

- Make your password at least 12 characters, and mix it up with at least two or three different types of characters (lowercase letters, uppercase letters, digits and symbols), put in unpredictable places.
- Don't put your capital letters at the beginning or your digits or symbols at the end.Avoid including names of people or pets,

places you have lived, sports teams, stuff you like or birth dates.
- Avoid common phrases (especially anything related to "love" in any language) and song lyrics. Don't use patterns ("abc," "123"), including patterns on the keyboard ("1qazxsw2").
- One way to make a strong password is to create a sentence that no one's ever said before and use the first letter or two of each word as your password, mixing in other types of characters.

It may be tempting to reuse your existing passwords, but don't do it for any accounts you care about. It is better to write your passwords down in a secure place if you have more passwords than you can remember, or better yet, use a password manager.

You can also protect your account without making your password more complicated by using two-factor authentication when it is offered – it's easier than most people think.

Passwords are an annoying part of online life, but they aren't going away soon. While the password policies of the past decade have caused more user pain than security gain, our research is helping find ways to create passwords that actually work for regular people while keeping us more secure.

This article was originally published on The Conversation. Read the original article.

Provided by The Conversation

Citation: Choose better passwords with the help of science (2017, August 30) retrieved 23 April 2024 from https://techxplore.com/news/2017-08-passwords-science.html