Why we choose terrible passwords, and how to fix them

May 2 2017, by Megan Squire

Credit: Andres Ayrton from Pexels

The first Thursday in May is World Password Day, but don't buy a cake or send cards. Computer chip maker Intel created the event as an annual reminder that, for most of us, our password habits are nothing to

celebrate. Instead, they – and computer professionals like me – hope we will use this day to say our final goodbyes to "qwerty" and "123456," which are still the most popular passwords.

The problem with short, predictable passwords

The purpose of a password is to limit access to information. Having a very common or simple one like "abcdef" or "letmein," or even normal words like "password" or "dragon," is barely any security at all, like closing a door but not actually locking it.

Hackers' password cracking tools take advantage of this lack of creativity. When hackers find – or buy – stolen credentials, they will likely find that the passwords have been stored not as the text of the passwords themselves but as unique fingerprints, called "hashes," of the actual passwords. A hash function mathematically transforms each password into an encoded, fixed-size version of itself. Hashing the same original password will give the same result every time, but it's computationally nearly impossible to reverse the process, to derive a plaintext password from a specific hash.

Instead, the cracking software computes the hash values for large numbers of possible passwords and compares the results to the hashed passwords in the stolen file. If any match, the hacker's in. The first place these programs start is with known hash values for popular passwords.

More savvy users who choose a less common password might still fall prey to what is called a "dictionary attack." The cracking software tries each of the 171,000 words in the English dictionary. Then the program tries combined words (such as "qwertypassword"), doubled sequences ("qwertyqwerty"), and words followed by numbers ("qwerty123").

Moving on to blind guessing

Only if the dictionary attack fails will the attacker reluctantly move to what is called a "brute-force attack," guessing arbitrary sequences of numbers, letters and characters over and over until one matches.

Mathematics tells us that a longer password is less guessable than a shorter password. That's true even if the shorter password is made from a larger set of possible characters.

For example, a six-character password made up of the 95 different symbols on a standard American keyboard yields $95^{6,}$ or 735 billion, possible combinations. That sounds like a lot, but a 10-character password made from only lowercase English characters yields $26^{10,}$ 141 trillion, options. Of course, a 10-character password from the 95 symbols gives $95^{10,}$ or 59 quintillion, possibilities.

That's why some websites require passwords of certain lengths and with certain numbers of digits and special characters – they're designed to thwart the most common dictionary and brute-force attacks. Given enough time and computing power, though, any password is crackable.

And in any case, humans are terrible at memorizing long, unpredictable sequences. We sometimes use mnemonics to help, like the way "Every Good Boy Does Fine" reminds us of the notes indicated by the lines on sheet music. They can also help us remember a password like "freQ!9tY!juNC," which at first appears very mixed up.

Splitting the password into three chunks, "freQ!," "9tY!" and "juNC," reveals what might be remembered as three short, pronounceable words: "freak," "ninety" and "junk." People are better at memorizing passwords that can be chunked, either because they find meaning in the chunks or because they can more easily add their own meaning through

mnemonics.

Don't reuse passwords

Suppose we take all this advice to heart and resolve to make all our passwords at least 15 characters long and full of random numbers and letters. We invent clever mnemonic devices, commit a few of our favorites to memory, and start using those same passwords over and over on every website and application.

At first, this might seem harmless enough. But password-thieving hackers are everywhere. Recently, big companies including Yahoo, Adobe and LinkedIn have all been breached. Each of these breaches revealed the usernames and passwords for hundreds of millions of accounts. Hackers know that people commonly reuse passwords, so a cracked password on one site could make the same person vulnerable on a different site.

Beyond the password

Not only do we need long, unpredictable passwords, but we need different passwords for every site and program we use. The average internet user has 19 different passwords. It's easy to see why people write them down on sticky notes or just click the "I forgot my password" link.

Software can help! The job of password management software is to take care of generating and remembering unique, hard-to-crack passwords for each website and application.

Sometimes these programs themselves have vulnerabilities that can be exploited by attackers. And some websites block password managers

from functioning. And of course, an attacker could peek at the keyboard as we type in our passwords.

Multi-factor authentication was invented to solve these problems. This involves a code sent to a mobile phone, a fingerprint scan or a special USB hardware token. However, even though users know the multi-factor authentication is probably safer, they worry it might be more inconvenient or difficult. To make it easier, sites like Authy.com provide straightforward guides for enabling multi-factor authentication on popular websites.

So no more excuses. Let's put on our party hats and start changing those passwords. World Password Day would be a great time to ditch "qwerty" for good, try out a password manager and turn on multi-factor authentication. Once you're done, go ahead and have that cake, because you'll deserve it.

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

Provided by The Conversation