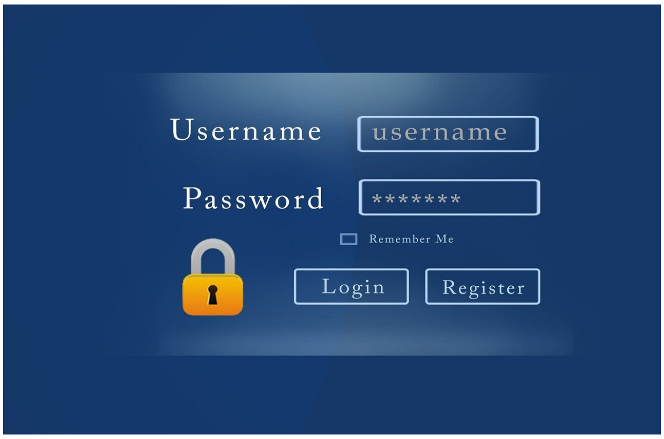
After a breach, users rarely change their passwords, and when they do, they're often weaker

27 May 2020, by Daniel Tkacik



Credit: CC0 Public Domain

Have you been pwned?

In other words, have any of your username / password combinations been stolen during any of the many data breaches in recent years? Chances are, they probably have, and it's also likely you didn't take the proper precaution of changing your password to a more secure one. That's not necessarily your fault.

Those are the findings in a recent study out of Carnegie Mellon University's CyLab. The findings were presented last week at the 2020 Workshop on Technology and Consumer Protection.

"In our study, only one in three people who had accounts on breached domains changed their passwords," says CyLab's Sruti Bhagavatula, a Ph.D. student in the School of Computer Science. "Only 13 percent of people with accounts on these domains changed their password within three months of the breach announcement."

Many may find these findings alarming, given the ubiquity and growing number of corporate data breaches in recent years. In January 2019, for example, a collection of over 700 million email addresses alongside passwords, referred to as "Collection #1" had been distributed on a popular hacking forum.

To reach their findings, the authors of the study observed the security practices of 249 willing participants through the Security Behavior Observatory (SBO), a group of participants consenting to have their daily computing behaviors observed. The researchers focused on nine breaches, and observed the behaviors of users who were in the SBO at the time of those breaches.

One of the breaches they focused on was the Yahoo breach that occurred in 2017, in which every single Yahoo account–all 3 billion of them–was hacked.

"We wanted to check whether or not they changed their Yahoo password after either of its two breach announcements," says Bhagavatula. "And if they changed their password, how good was the change?"

While one in three users affected by the breach changed their passwords, their new passwords were often weaker than their previous passwords, although a small number of new passwords were significantly stronger than the original. To make things worse, users' new passwords were overall more similar to passwords they use on other accounts.

"Breach notifications almost never tell people to reset their similar—or identical—passwords on other accounts," says CyLab's Lujo Bauer, a co-author on the paper and a professor in the Electrical & Computer Engineering department and in the Institute for Software Research. "Yet the participants whose data we studied had, on average, 30 other passwords that were similar to the breached password. On average, those who changed a breached password changed less than three of these 30 similar passwords."

Given these findings, the researchers recommend that companies take a more direct approach towards their customers who are affected by breaches.

"For the people who were affected, they should force password resets, for example, by preventing the customer from logging in until they've changed their password," Bhagavatula says. "Companies need to make it clear that even if users change the password on their site, they're still vulnerable on other sites if similar passwords are being used."

Apu Kapadia, an associate professor at Indiana University, was a third author on the study.

Provided by Carnegie Mellon University

APA citation: After a breach, users rarely change their passwords, and when they do, they're often weaker (2020, May 27) retrieved 28 November 2022 from https://techxplore.com/news/2020-05-breach-users-rarely-passwords-theyre.html