THE VERGE

WEB TL;DR TECH

50

Best practices for passwords updated after original author regrets his advice

Fourteen years later, Bill Burr says his tips were misguided

By Nick Statt | @nickstatt | Aug 7, 2017, 3:53pm EDT

Photo by Amelia Holowaty Krales / The Verge

A vast majority of the trusted tips and tricks we employ when crafting a custom password actually make us more vulnerable to hackers, according to the expert who popularized the tips back in 2003. In an interview with *The Wall Street Journal*, former National Institute of Standards and Technology manager Bill Burr admitted that a document he authored on crafting strong passwords was misguided. “Much of what I did I now regret,” says Burr, who is 72 years old and now retired.

The problem wasn't that Burr was advising people to make passwords that are inherently easy to crack, but that his advice steered everyday computer users toward lazy mistakes and easy-to-predict practices. Burr's eight-page password document, titled "NIST Special Publication 800-63. Appendix A," advised people to use irregular capitalization, special characters, and at least one numeral. That might result in a password like "P@ssW0rd123!" While that may make it seem secure on the surface (neglecting, of course, that "password" is a bad password), the issue is that most people tend to use the same exact techniques when crafting these digital combo locks. That results in strings of characters and numbers that hackers could easily predict and algorithms that specifically target those weaknesses.

BURR'S PASSWORD ADVICE PUSHED USERS TOWARD LAZY AND EASY-TO-PREDICT PRACTICES

Even worse, Burr suggested people should change passwords regularly, at least every 90 days. This advice, which was then adopted by academic institutions, government bodies, and large corporations, pushed users to make easy-to-crack passwords. Most people can probably point to a password they've created that was deemed strong simply because it had a special character like the "!" or "?" symbol and a numeric string like "123." And when prompted to change a password, who hasn't altered it only slightly to avoid the hassle of coming up with an all-new code?

A popular xkcd comic from cartoonist Randall Munroe, published back in August 2011, poked a hole in this common logic by pointing out how the password "Tr0ub4dor&3" could be cracked in about three days with standard techniques, due to its predictable capitalization, numeric substitutions, and special character use. The password "correct horse battery staple," written as a single phrase, would take 550 years. (Security experts have confirmed Munroe's math, according to the *WSJ*.) "Through 20 years of effort, we have correctly trained everyone to use passwords that are hard for humans to remember, but easy for computers to guess," Munroe wrote at the bottom.

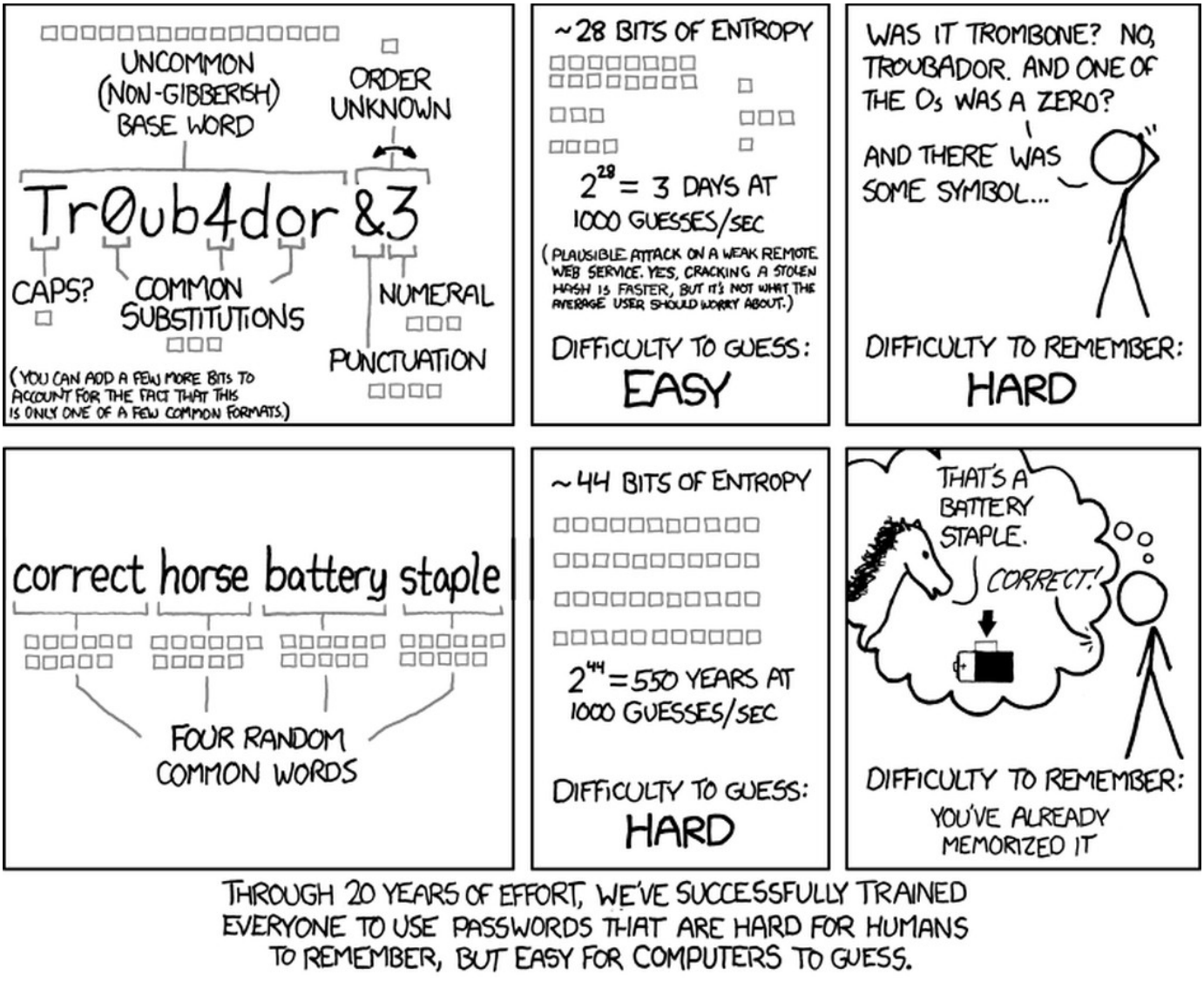

Image: xkcd

In other words, the passwords you should be using are obscure, almost unexplainable phrases full of human randomness that make them easy to commit to memory and yet almost impossible for an automated system to make sense of. Of course, for those who use password managers like LastPass, you can generate cryptographically secure passwords on the fly. But it's still important to have a hard-to-crack master password.

"In the end, it was probably too complicated for a lot of folks to understand very well, and the truth is, it was barking up the wrong tree," Burr admits of his advice. The new NIST standards that were published in June, authored by technical advisor Paul Grassi, did away with much of Burr's advice.

“We ended up starting from scratch,” Grassi tells the *WSJ*. But Burr might be exaggerating the negative effects of his password advice, Grassi adds: “He wrote a security document that held up for 10 to 15 years. I only hope to be able to have a document hold up that long.”