by Shelly Palmer, CEO, The Palmer Group

Every time there's a notable cybersecurity breach, someone (even me) writes a comprehensive primer on the proper way to create "secure" passwords. Lather, rinse, repeat. Until a few years ago, everyone (including me) based their password advice on a 2003 paper from the National Institute of Standards and Technology (NIST), with the catchy title "NIST Special Publication 800-63." The paper recommended that passwords be cryptic, contain special characters, and be as close to nonsense as possible.

I was in a camp I called "How to Make a Cryptic Password You Can Easily Remember." The short version was this: take a phrase you know, such as a favorite quote from a movie, and use the first letter of each word. For example, Sheriff Brody's famous line from Jaws, "I think we're gonna need a bigger boat," becomes 1twgn@bb. The trick was using Leet (a technique where letters are replaced by numbers and symbols; see my post from July 2012, "Yahoo! Hacked: What You Need To Do Now") to add the numbers and special characters. But as you can see from the example, a password made in this way is total nonsense to everyone but you – unless you forget your favorite quote.

That Was Then

Right after the Sony Hack became public knowledge (circa November 2014), cybersecurity paranoia set in and everyone started grasping for ways to enhance their cyberdefenses.

Once again, passwords were in the spotlight, but two strategic camps had evolved. Camp one was advocating the creation of more-cryptic passwords and changing them often (like monthly), and camp two began advocating for the longest passwords possible, made from any words you like and left alone until there was a reason to change them. All my cybersecurity friends fell squarely into the second camp, advocating for the longest passwords possible. My thinking evolved and I fell into line with camp two.

Fast Forward to Today

According to the Wall Street Journal, Bill Burr (the man who wrote the NIST memo back in 2003 that recommended the cryptic craziness and frequent replacement guidelines) has had an epiphany. “Much of what I did I now regret,” said Mr. Burr, 72 years old, who is now retired. If the reporting is accurate, he had very little evidence upon which to base the NIST’s recommendations. (Sort of makes me think about the USDA Food Chart I grew up with. But that’s for another article.) Why were Mr. Burr’s assumptions wrong?

The Math

This very widely circulated cartoon from XKCD tells the story beautifully.

The key takeaway is that the longer the password is, no matter its complexity, the harder it is for a computer to guess.

Now What?

The good news is that Mr. Burr’s old memo has been discarded and the NIST has published new Digital Identity Guidelines. The bad news is that it is going to take quite a while for these new guidelines to become widely adopted. Many sites limit the length of your password to “8-12 characters.” If that’s the case, you can’t use a password that is long enough to be considered safe under the new guidelines. As you know, many sites (especially government sites) require a

special character and a number for a password to be considered strong. In practice, it may be years before the Internet catches up. By then, we may not be using passwords at all.

No Passwords

For consumers, passwords are just a way to validate that you are who you say you are. If you forget your password, you can request an email, a txt, or in some cases a phone call to obtain a temporary replacement. So if there's another valid way to authenticate you, passwords really aren't necessary. Google, Facebook, and several other sites can be easily used to verify that you are who you say you are. If proper authentication protocols are used, any site could determine you are you by checking to see if you are properly logged in to Facebook or Gmail. Lots of sites already do this, and there are a host of biometric and multifactor identification and authentication schemas fighting to be the new new thing in secure Internet living. Password science is evolving quickly, but it's likely to be a hot mess for the foreseeable future.

So What Do I Do?

Do what the experts are now telling you to do. Start using the longest passwords possible. I would not use correcthorsebatterystaple, but "passwordswedontneednostinkinpasswords" will absolutely do the job.

+++

About Shelly Palmer

Named one of LinkedIn Top 10 Voices in Technology, Shelly Palmer is President & CEO of The Palmer Group, a strategic advisory and business development practice focused at the nexus of technology, media and marketing with a special emphasis on data science and data-driven decision making. He is Fox 5 New York's on-air tech and digital media expert and a regular commentator on CNBC and CNN. Shelly Palmer also presented the Opening Keynote for CEDIA 2016, America's leading event for residential installers.

Go Shelly Palmer