Time for Password Expiration to Die

*By Lance Spitzner*

Password expiration is a dying concept. Essentially, it’s when an organization requires their workforce to change their passwords every 60, 90 or XX number of days. And while there are several reasons behind the password expiration policy, most at this point seem obsolete.

The first reason? History. Years ago (decades, even) it was estimated that it would take the average computer approximately 90 days to ‘crack’ the average password hash. In other words, if an attacker hacked into a website and was able to copy all the password hashes, (passwords are not secured via encryption, [but instead one-way hashes](https://en.wikipedia.org/wiki/Cryptographic_hash_function)) hackers could attempt to automate the process of guessing the passwords. So, the thinking was if the average password could be cracked in 90 days, people should get into the habit of changing their passwords every 90 days. Over time, this guideline became a requirement for many different standards and became embedded in security folklore. If you did not advocate the regular changing of passwords, you were *obviously*an incompetent security professional.

Fast forward to today. Things have radically changed. Password expiration is no longer relevant. In fact, if you conduct a risk-based analysis, you will quickly determine that password expiration does far more harm than good and actually *increases*your risk exposure. The problem is that organizations and security standards (looking at you, PCI-DSS) have not kept up and continue to promote outdated and harmful practices simply because that is how it has always been done. Let’s take a look at why this is the case.

There has been a community effort to kill password expiration for years, this is not something new. People like [Per Thorsheim](http://passwordscon.org/), [Microsoft's Dr. Cormac Herley](https://www.microsoft.com/en-us/research/people/cormac/), [Gene Spafford of Purdue](https://www.cerias.purdue.edu/site/blog/post/password-change-myths/) and the [Chief Technologist at FTC](https://www.ftc.gov/news-events/blogs/techftc/2016/03/time-rethink-mandatory-password-changes), to name just a few, have been working hard to kill password expiration. Here are the reasons why:

**Outdated Threat Model**: In the past twenty plus years, both technology and the threat model have radically changed. First, most of today's "average" or "bad" passwords can be quickly cracked in the cloud. Passwords that would have taken your average cyber attacker 90 days to crack twenty years ago now takes literal seconds, thanks to solutions like AWS.

Also, the greatest risk to your password is no longer cracking, but password *harvesting*. Cyber criminals infect your computer with keystroke loggers, data harvesting via phishing websites, people sharing or reusing passwords, social engineering attacks over the phone, SMS texting, or a number of other methods. Basically, since the threat model has changed, if your password is compromised, it will almost certainly be collected in seconds, not months. And when the bad guy gets your password, they are not going to wait the required "90 days", [they are going to leverage it within hours.](https://enterprise.verizon.com/resources/reports/dbir/) So by the time you get around to changing your passwords the bad guys are long gone. Regular password changing only makes you *feel*more secure. It does not do anything to actually secure you.

**Behavioral Cost**: It always amazes me how people in our field always look at security from a risk mitigation perspective, but often forget the cost perspective. There is a huge cost to organizations for a password expiration program. As [Dr. Angela Sasse](http://sec.cs.ucl.ac.uk/people/m_angela_sasse/) at University of College London has documented, every behavior has a cost and having every employee change X number of passwords every X number of months is a big one. I’m not talking about just lost employee time and help desk tickets, but I’m talking about the cost to your *culture*. Ever wonder why people hate your security program? Ever wonder why employees have to constantly write down their passwords on sticky notes and post them everywhere? This is why. Don’t annoy your employees with outdated security practices. They’re less likely to buy into the program, rendering adverse results.

**Increasing Risk**: Think you are mitigating risk by requiring a password expiration at your workplace? Think again. First, think this through**.**The only behavior you are really promoting in your workforce is people are simply increasing that number 1 at the end of their password to a number 2.

You know this.
I know this.
The bad guys know this.

If you keep forcing people to change their passwords, they are going to come up with some system where it’s easy for them to remember their new passwords (or force them to repeatedly write them down on sticky notes). What’s that you say? You keep password history to ensure that every password is truly unique for every password change? The challenge is you are now providing the cyber attacker not just *one*password hash to break instead of multiple password hashes to break. Password history exponentially increases the likelihood of cracking the passwords as they now have multiple passwords to crack.

Finally, go to any pentester you know and ask them if password expiration ever stopped them. I discussed password expiration with several of top SANS instructors, including [Jake Williams](https://www.sans.org/instructors/jake-williams) and [Rob M. Lee](https://www.sans.org/instructors/robert-m-lee). Both used to work at the NSA TAO group, where they were responsible for hacking other countries and their systems. Both said in their years of service, not *once*did password expiration ever slow them or their team down.

Password expiration had its time and place, but now it’s time for it to fade out of our security awareness practices. But there is an even bigger lesson to be learned here. Essentially, whenever you enforce a security behavior at your workplace, you should have a good reason as to *why*. Far too often policies, processes or requirements become folklore. Never be afraid to ask ‘why? Worst case scenario you will learn something. As for passwords, what should we be doing to protect our data instead of password expiration? How do we address the risks of passwords but at minimal cost? Here are a few tips:

* Encourage the use of long passphrases. Length, not complexity, is the new entropy. Long passphrases are easier to remember AND easier to type (we forget that need too often).
* Ensure every account has a unique password. That way, if an account is compromised, all of the other accounts are safe. However, if you encourage this behavior at your workplace, support it with password managers. Ensure people have a way to easily and securely store all of their unique passwords.
* If you have a key account you need to secure, use Multi-Factor Authentication (MFA). Hands down, this is one of the simplest, most effective ways to secure any authentication requirement.
* Have a compliance standard that requires password expiration? Consider implementing compensating controls, where you document the reason for eliminating password expiration (\**sigh*\* once again looking at PCI DSS for this one).
* When it comes to password expiration, only require people to change their passwords if they have reason to believe it has been compromised. If you really just can’t let the password expiration go gracefully, consider a policy where the longer the password is, the less frequently people have to change it.

In this day and age, changing passwords every 90 days gives you the *illusion*of stronger security while inflicting needless pain, cost, and ultimately additional risk to your organization. Fortunately, the tide has turned. The UK government [published new password guidelines](https://www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach) that recommends killing password expiration, and the [NIST SP800-63b password guidance](https://pages.nist.gov/800-63-3/) has stated the same.

Now if we could just get people to [stop inflicting password complexity on their workforce](https://www.sans.org/security-awareness-training/blog/nist-has-spoken-death-complexity-long-live-passphrase)...