Should You Really Change Your Password Every 90 Days?

If you've worked a job that requires you to have login credentials, you're probably familiar with the common "90 day rule" for passwords. The rule being: change your password every 90 days (or 45 days, depending on the workplace). It's a security best practice that will keep your accounts—and your organization—secure from hackers and nosy coworkers.

The "90 day rule" has been around for years, and no matter how each individual company decides to enforce it (some are encouraged to change it around the three month mark; others receive emails or warnings that count down the days until the current password expires), the outcome remains the same. Employees around the world stop what they're doing, think up a new, *hopefully strong* password, and apply it as quickly as possible so they can get back to work.

This is the way it's always been done. Changing your password makes the network secure and thwarts evildoers, right? And the good outweighs the inconvenience. Why fix what isn't broken?

Unless it is broken.

Emerging studies from University of North Carolina at Chapel Hill and Carleton University report that requiring password changes every 90 days may not actually be the best way to protect your company data and user accounts. In fact, some big organizations are actively starting to question this practice: in 2016, the National Institute of Standards and Technology (NIST) put out new guidelines that recommend removing routine password change requirements.

So, should you really change your password every 90 days? There's no absolute consensus in the IT industry yet, but there are good arguments on both sides. To help keep you informed, we compiled information about each perspective. Here's what we found:

The "No" Camp

On one side of the ring, we have the "no" camp, the organizations and thought leaders that are talking about how outdated mandatory password rotation policies are.

The main theory for the 90 day naysayers? Requiring frequent changes causes users to create weak passwords—or simply slightly modify their current one.

Lorrie Cranor, computer science professor at Carnegie Mellon University, spent a year with the U.S. Federal Trade Commission as a Chief Technologist. During this time, she wrote on the FTC blog: "There is a lot of evidence to suggest that users who are required to change their passwords frequently select weaker passwords to begin with, and then change them in predictable ways that attackers can easily guess."

Think about the passwords you create. In the frustration of the moment, have you ever created a new password similar to your last one, just with different punctuation or capitals? A majority of users probably have at least once. According to a study by University of North Carolina, Cranor writers, the people whose credentials they had access to "tended to create passwords that followed predictable patterns … such as incrementing a number, changing a letter to a similar-looking symbol…, adding or deleting a special character…, or switching the order of digits or special characters."

Troy Hunt, author at Pluralsight and Microsoft Regional Director, also addressed the "90 day rule" in our recent project, Cybersecurity Myths Debunked. His thoughts? The myth about password rotation is "really interesting because we have this mix of opinions at the moment where most organizations say 'you must rotate your password every 90 days in order to keep it secure' and on the other side you have The National Cyber Security Centre of the British government and NIST saying 'don't do this because it makes it worse!' And I love the rationale that they use, it's just so pragmatic: If someone gets your password, they're not going to wait 90 days to use it, they're going to use it now!"

Hunt's point is an important one. If a hacker has access to your password, changing it to something different is unlikely to be effective. Chances are, they've already peered into your account, maybe even installed a keylogger to cull your future credentials. The fix to a compromised account isn't to update your password; the fix is to create a unique password for each account, then tighten your security through measures like multi-factor authentication and slow hashing.

The "Yes" Camp

On the other side of the ring, we have the "yes" camp, the organizations and thought leaders that are talking about how important the "90 day rule" is for IT security. The main theory for the 90 day hype? If you change your password every three months, a hacker that has access to an old password (say through a data breach) won't be able to use it forever, and won't be able to use it across your accounts.

Many data breaches have happened over the years. In May 2017, 560 million email credentials were leaked, which included "a collection of data from previous breaches at LinkedIn, Dropbox, LastFM, MySpace, Adobe, Neopets, Tumblr and others," reports this article from LifeHacker. If you change your passwords frequently and use *strong/unique* passwords that aren't similar to your previous ones, your data is likely safe. But if you rarely change your password, have an account with an

organization affected by a leak, or use the same password across multiple accounts? Well, you may be out of luck.

As an aside: You can check to see if any of your accounts were leaked in the breach using Have I Been Pwned, a tool created by Troy Hunt that scans for your email account in a list of data that's been publically released. The results may surprise you, and inspire you to update your account security.

No matter which camp you personally fall in, it's critical to use almost-impossible-to-crack passwords and enable multi-factor authentication, especially for accounts you have with financial institutions, medical institutions, and email providers. To ease this burden, many thought leaders recommend using a password manager, like LastPass or 1Password, that allows you to create original passwords for your accounts without having to remember them all … or inevitably stick a colorful post-it note under your keyboard (hint: don't do that).

Do you subscribe to the 90 day rule? Join the conversation on Twitter with the hashtag #SecurityMyth.