# All.Net Analyst Report and Newsletter

***Welcome to our Analyst Report and Newsletter***

## Change your password – Doe Si Done!

This is not an article about changing your password. It’s about the pace of change and innovation in cybersecurity. So let’s take a look back. In September of 1997, I wrote an article titled “Change Your Password - Do Si Do”. It said, in essence, that periodic password changes are a waste of time, reduce security effectiveness, are based on bad assumptions unrelated to passwords, and should not be done. Over the next 20 years, I have, in various ways, rallied against this practice in many forums, including the creation of an element in a widely reviewed standard of practice that indicated this was not appropriate. Finally, as of just about now, some 20 years later, NIST is apparently taking the approach in their standards of only changing passwords if there is a reason to do so (and there are good reasons to do so in various cases).

Obviously, I want to applaud NIST for taking what will be viewed by many as a bold step. The folks I know there are smart, hard working, honest, sincere, and trying to improve things.

## Good job. However… Mean time to change: 20 years

As a single data point (not the only one I am currently aware of), it takes about 20 years to remove a security constraint once it has been pointed out to be ineffective. But I have some more evidence in this arena:

- Antivirus efforts started in about 1983 when I first pointed out the issues in a paper that was ultimately published in the National Security Conference in 1984. The concept of integrity shells was due to Brian Cohen and written up by me with him as co-author along with optimization criteria in the 1988 time frame. It was eventually codified into the trusted platform module about 20 years later, when it became a standard hardware feature in computers and systems on a global basis.
- Deception for information protection as a subject of published studies in cybersecurity started in the mid to late 1990s. Cliff Stohl, Brian Chess, Bill Cheswick, and others started to apply these methods, and things like the deception toolkit appeared in the late 1990s. The first commercial solutions appeared in the 2000 time frame, but the field really started to catch on starting in the 2016 time frame as companies started to emerge (they were started a few years earlier in some cases). About 20 years!

I’m starting to detect a pattern. And I have more similar examples.

## Conclusion

Despite the claims of rapid innovation and the so-called dire need for innovative approaches to information protection (cybersecurity) it seems to take about 20 years to actually start to adopt new ideas.

- I am happy to announce the beginning of the end of unnecessary password changes
    - I also did my forced password change every 90 days today on a corporate account.
- I am saddened to see that it takes 20 years for change to start taking hold. Speed it up!