The problems with forcing regular password expiry

Why the NCSC decided to advise against this long-established security guideline.

Emma W

Regular password expiry is a common requirement in many security policies. However, in the Password Guidance published in 2015, we explicitly advised against it. This article explains why we made this (for many) unexpected recommendation, and why we think it's the right way forward.

Let's consider how we might limit the harm that comes from an attacker who knows a user's password. The obvious answer is to make the compromised password useless by forcing the legitimate user to replace it with a new one that the attacker doesn't know. This advice seems straightforward enough.

The problem is that this doesn't take into account the inconvenience to users - the 'usability costs' - of forcing users to frequently change their passwords. The majority of password policies force us to use passwords that we find hard to remember. Our passwords have to be as long as possible and as 'random' as possible. And while we can manage this for a *handful* of passwords, we can't do this for the *dozens* of passwords we now use in our online lives.

To make matters worse, most password policies insist that we have to keep changing them. And when *forced* to change one, the chances are that the new password will be similar to the old one.

Attackers can exploit this weakness.

The new password may have been used elsewhere, and attackers can exploit this too. The new password is also more likely to be written down, which represents *another* vulnerability. New passwords are also more likely to be forgotten, and this carries the productivity costs of users being locked out of their accounts, and service desks having to reset passwords.

It's one of those counter-intuitive security scenarios; the more often users are forced to change passwords, the greater the overall vulnerability to attack. What

appeared to be a perfectly sensible, long-established piece of advice doesn't, it turns out, stand up to a rigorous, whole-system analysis.

The NCSC now recommend organisations do **not** force regular password expiry. We believe this reduces the vulnerabilities associated with regularly expiring passwords (described above) while doing little to increase the risk of long-term password exploitation. Attackers can often work out the new password, if they have the old one. And users, forced to change another password, will often choose a 'weaker' one that they won't forget.

At the NCSC, we want administrators to think about alternative, more effective system defences they might implement in order to detect and prevent unauthorised account use. For instance, we recommend using system monitoring tools that present users with information about the last login attempt, so they can see if they're responsible for failed login attempts. If they're not, this may be a sign that someone has attempted to access their account, and users should be able to easily report this for investigation. Initiatives such as this are far more likely to help keep systems safe, and much more manageable for the user.

For more information, please refer to our Password Guidance: Simplifying Your Approach.

Emma W
People-Centred Security Lead, Sociotechnical Security Group, NCSC

WRITTEN BY

Emma W
Head of Cyber Essentials and Cyber Advisor

PUBLISHED

5 October 2016

WRITTEN FOR

Small & medium sized organisations

Large organisations

Public sector

Cyber security professionals

PART OF BLOG

NCSC publications