Passwords
Like You Never Knew Them Before!

Per Thorsheim
Twitter: @thorsheim
Phone: +47 90 99 92 59 (Use Signal!)
Password recommendations

• Make your password a sentence
• Unique account, unique password
• Write down your passwords
• Use 2-factor authentication
About gamification...
What is the risk analysis behind your password policy?
Where did you get those password recommendations?
Don’t blame users for bad passwords
Whenever I see a bad password policy...
PasswordsCon.org
«Making security better by making it easier.»
PINs

1234
Choose your pins (17yr olds, fall 2013)

Girls
1996

Boys
1337
1996
Creating a long & memorable PIN:

Johansen 56426736
Lock Patterns
10% uses a letter from standard English alphabet

«On User Choice for Android Unlock Patterns»
Loge, Duermuth, Rostad
Password change frequencies
The problems with forcing regular password expiry

Version: 1
Created: 11 April 2016
Updated: 15 April 2016
Topics: Passwords, Best Practice

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

Regular password expiry is a common requirement in many security policies. However, in CESG’s 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 a handful of words, we can’t use keywords, we can’t use our birthdays, we can’t use our dog’s name, we’re not allowed to use ‘123456’ or ‘password’. In short: they’re difficult to remember.

If you’re required to change your passwords each month or each quarter, you need to write them down somewhere. This is a common practice, agreed by most security professionals, in order to remember complex passwords. But in a review of online password policies in the US, it was found that 80% of passwords were created by following the rules of password policies, with a consistent pattern of using a small number of words, adding a number or symbol, and then adding a number or symbol to the end of it. This is a classic example of a self-defeating security measure.

https://www.cesg.gov.uk/articles/problems-forcing-regular-password-expiry
Time to rethink mandatory password changes

By: Lorrie Cranor, Chief Technologist | Mar 2, 2016 10:55AM

Data security is a process that evolves over time as new threats emerge and new countermeasures are developed. The FTC's longstanding advice to companies has been to conduct risk assessments, taking into account factors such as the sensitivity of information they collect and the availability of low-cost measures to mitigate risks. The FTC has also advised companies to keep abreast of security research and advice affecting their sector, as that advice may change. What was reasonable in 2006 may not be reasonable thought.

https://www.ftc.gov/news-events/blogs/techftc/2016/03/time-rethink-mandatory-password-changes
Complexity
The password you entered is not valid

Please note that the password must respect the following rules:

- It must contain between 7 and 32 characters. Use only characters from the following set: !#$%&()'*+,./0123456789:<=>@ABCDEFGHIJKLMNOPQRSTUVWXYZ\_ `abcdefghijklmnopqrstuvwxyz{ | }~
- It must contain at least 1 lowercase letter(s) (abcdefghijklmnopqrstuvwxyz).
- It must contain at least 1 capital letter(s) (ABCDEFGHIJKLMNOPQRSTUVWXYZ).
- It must contain at least 1 numeric character(s) (0123456789).
- It must not contain more than 2 identical consecutive characters (AAA, iii, $$ $$ ...).
- It must not contain your user name.
- It must not contain your email address.
- It must not contain your first name.
- It must not contain your last name.
«Your password contains invalid characters.»

NO, your startup contains incompetent engineers.

@harribellthomas
Usability: masking passwords?
Username

One truly amazing passphrase!
Password recommendations

• Make your password a sentence
• Unique account, unique password
• Write down your passwords
• Use 2-factor authentication
COMPARE & COMPLAIN
And a personal story at the end

Why you should write down your passwords.
per@thorsheim.net
+47 90 99 92 59 (Use Signal!)
@thorsheim