Forced Periodic Password Resets by the Numbers

Forced periodic password resets are widely used across industries throughout the world. But now some security experts are changing perspectives on them. The numbers below explain why.

HOW OFTEN DO SOME ORGANIZATIONS FORCE PASSWORD RESETS?

The typical organization forces users to **CHANGE** their **PASSWORD every 30, 60, or 90 days.**

77%
OF IT DEPARTMENTS expire passwords for all staff **quarterly.**[1]

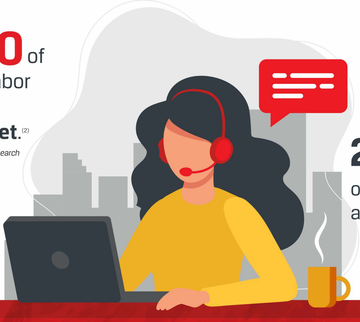
(1) Forrester Research

THE COST OF FORCED PERIODIC PASSWORD RESETS

IT departments spend large amounts of money to fund these password resets.

It costs **$70** of IT Help Desk labor for a single **password reset.**[2]

(2) Forrester Research



20% to 50%
of all Help Desk calls are for **password resets**

LOST TIME IS ALSO A SIGNIFICANT FACTOR IN WHY PASSWORD RESETS ARE SO EXPENSIVE FOR COMPANIES

Organizations spend an average of **2.5 months** a year on **password resets** alone.[3]

(3) OneLogin

Lost productivity is also a concern as **78% of people** had to **reset a password** they forgot in the **past 90 days.**[4]

(4) HYPR

Lost productivity due to password resets is estimated to cost companies **$420** per employee per year. [5]

(5) Widmeyer and Centrify

SIGNIFICANT ANNUAL COSTS

An organization with
500 employees

=

$210,000
per year in lost productivity

SECURITY LEADERS NOW RECOMMEND AGAINST FORCED PERIODIC PASSWORD RESETS

Microsoft claims that password expiration requirements do more harm than good because they make users select easier and more predictable passwords.

The National Institute of Standards and Technology updated the NIST password guidelines to reflect that passwords shouldn't periodically expire.

Other cybersecurity organizations and frameworks are starting to agree with NIST and Microsoft.

What can organizations do instead?

Password Monitoring

Passwords should be checked daily against a continually updated list of compromised or bad passwords.
In Active Directory, organizations can automate password policies and NIST password guidelines with a plugin that compares passwords against exposed, weak, and common passwords.

Summary

Forced periodic password resets are no longer necessary. Forced periodic password resets have high Help Desk costs and lost productivity costs, and they also encourage poor password practices.

Instead, password monitoring increases security, reduces employee friction, and reduce costs. Visit **www.enzoic.com** to learn more.

ENZOIC