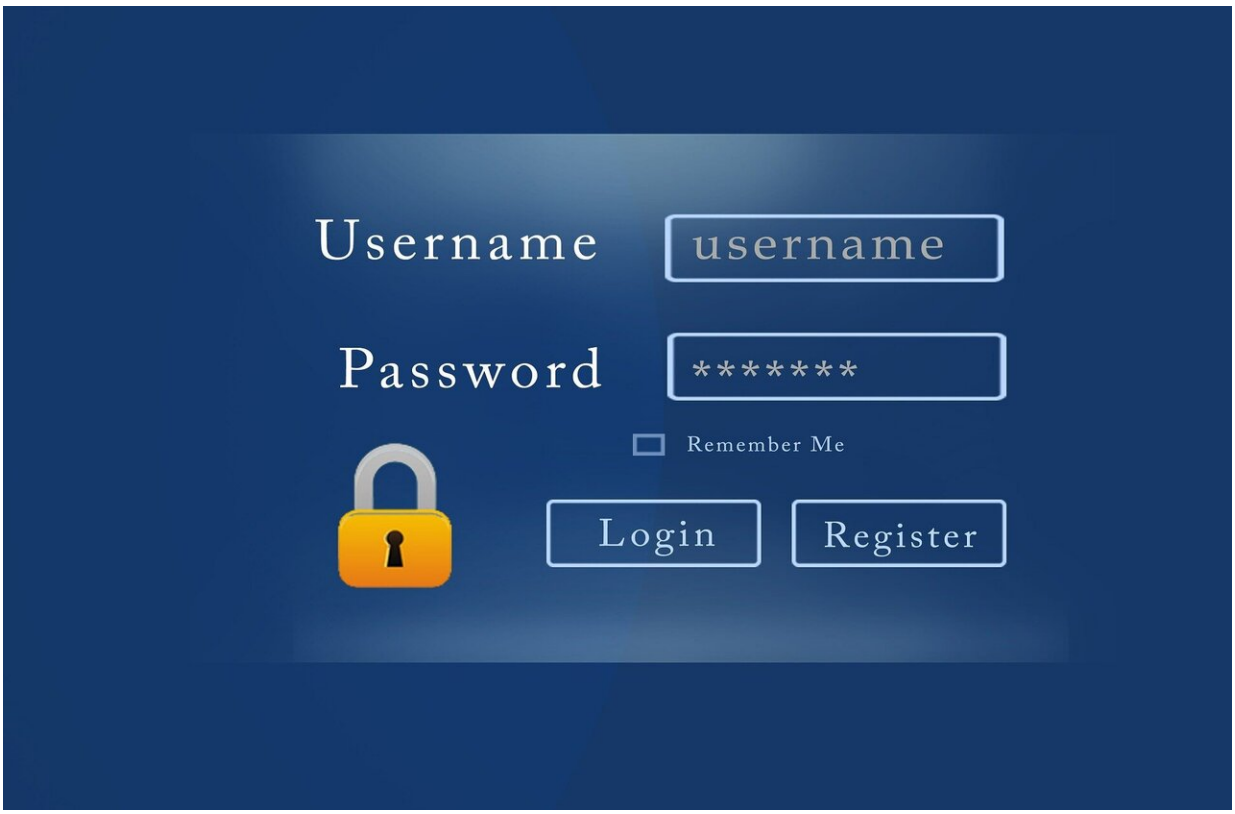
Computer scientists run a password update campaign efficiently and with minimal IT costs

February 1 2024, by Ioana Patringenaru



Credit: CC0 Public Domain

Updating passwords for all users of a company or institution's internal computer systems is stressful and disruptive to both users and IT

professionals. Many studies have looked at user struggles and password best practices. But very little research has been done to determine how a password update campaign can be conducted most efficiently and with minimal IT costs. Until now.

A team of computer scientists at the University of California San Diego partnered with the campus' Information Technology Services to analyze the messaging for a campus-wide mandatory password change impacting almost 10,000 faculty and staff members.

The team found that email notifications to update passwords potentially yielded diminishing returns after three messages. They also found that a prompt to update passwords while users were trying to log in was effective for those who had ignored email reminders.

Researchers also found that users whose jobs didn't require much computer use struggled the most with the update. The findings are published as part of the *Annual Computer Security Applications Conference*, where the team presented their work in December 2023.

To the team's knowledge, it's the first time an empirical analysis of a mandatory password update has been conducted at this large a scale and in the wild, rather than as part of a simulation or controlled experiment.

The research team hopes that lessons from their analysis will be helpful to IT professionals at other institutions and companies.

During the campaign, almost 10,000 faculty and staff at UC San Diego received four emails at about a weekly interval prompting them to change their single sign-on password. Users who still hadn't changed their password even after receiving four emails then got a prompt to do so as they logged in.

The emails were clearly effective, leading between 5% and 15% of users to update their passwords during each wave of emails. However, even after four such email prompts, a quarter of users had not completed the update procedure.

The finding contradicts a previous study that found 98% of participants changed their passwords after receiving multiple email messages. But that study had a much smaller sample size.

Remarkably, 80% of the remaining users who hadn't changed their passwords after the email campaign finally did so when they were prompted at log in.

"The active single sign on prompting was a big winner across the board," said Ariana Mirian, the paper's first author, who earned her Ph.D. in the UC San Diego Department of Computer Science and Engineering. "You managed to get people who are stubborn–and maybe not paying attention–to take action, and that's huge."

Researchers also noted that despite concerns from the campus, the campaign did not generate a significant increase in tickets to the IT help desk. Ticket volume did increase three to four times, but tickets related to the password update only represented 8% of all requests.

Not surprisingly, users who struggled the most work in areas where they're not required to log in to their computers regularly, such as maintenance, recreation and dining services.

"Targeting such users earlier, or forgoing email reminders and using login intercepts from the start, or even using a different notification mechanism such as text messages, may be more effective," the researchers write.

More information: Mirian Ariana et al, An Empirical Analysis of Enterprise-Wide Mandatory Password Updates, *Annual Computer Security Applications Conference* (2023). DOI: 10.1145/3627106.3627198