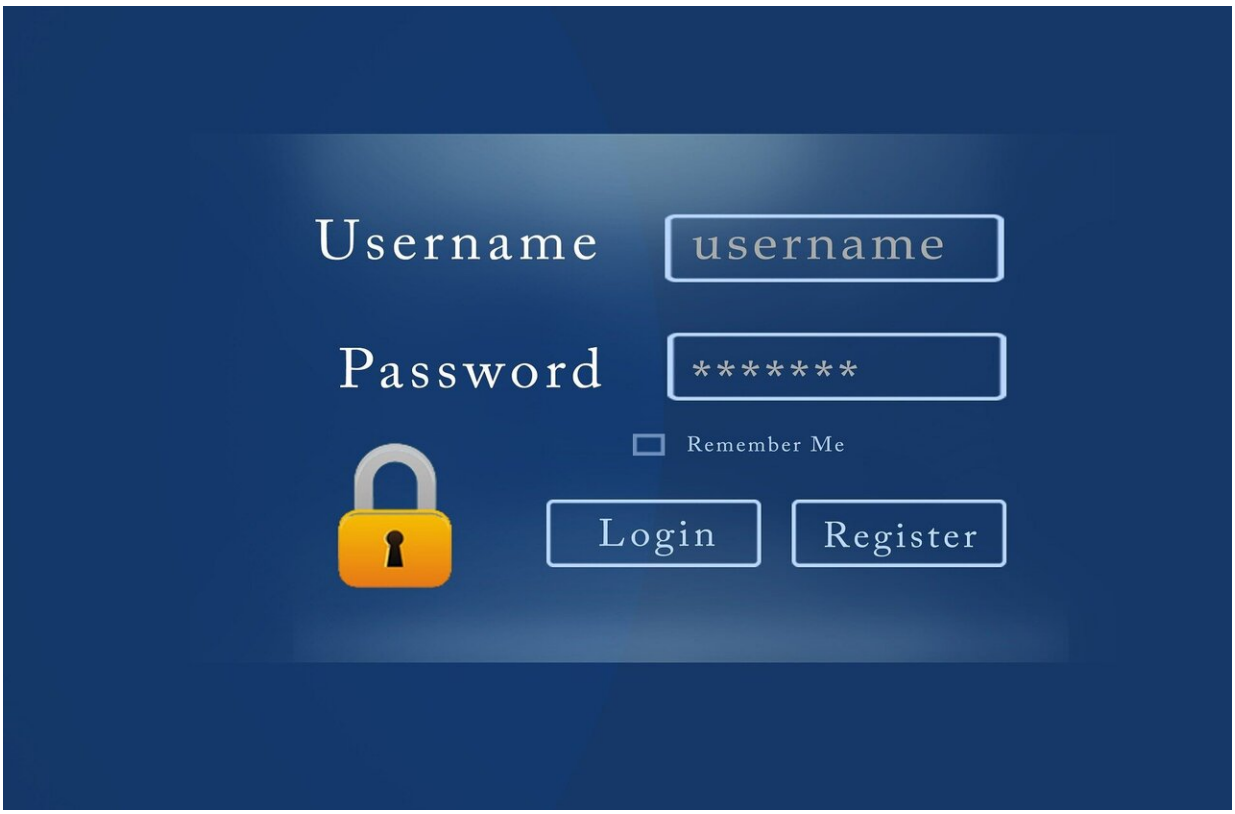
# Largest study of its kind shows outdated password practices are putting millions at risk

November 20 2023




Credit: CC0 Public Domain

Three out of four of the world's most popular websites are putting tens of millions of users and their data at risk by failing to meet minimum

password requirement standards.

The findings are part of a new Georgia Tech cybersecurity study that examines the current state of password policies across the internet.

Using a first-of-its-kind automated tool that can assess a website's password creation policies, researchers also discovered that 12% of websites completely lacked password length requirements.

Assistant Professor Frank Li and Ph.D. student Suood Al Roomi in Georgia Tech's School of Cybersecurity and Privacy created the automated assessment tool to explore the Google Chrome User Experience Report (CrUX), a database of 1 million websites and pages.

The study is based on 20,000 randomly sampled websites from the CrUX database and showed that many sites:

- Permit very short passwords.
- Do not block common passwords.
- Use outdated requirements like complex characters.

The researchers also discovered that only a few sites fully follow standard guidelines, while most stick to outdated guidelines from 2004. The project was 135 times larger than previous works that relied on manual methods and smaller sample sizes.

More than half of the websites in the study accepted passwords with six characters or less, with 75% failing to require the recommended eight-character minimum. About 12% had no length requirements, and 30% did not support spaces or special characters.

Only 12% of the websites studied enforced a password block list, which means more than 17,000 sites were vulnerable to cyber criminals who

might try to use common passwords to break into a user's account, also known as a password spraying attack.

"Both Professor Li and I were excited to take on the challenge," said Al Roomi. "With his guidance and our continuous work on both algorithm design and the measurement technique, we were able to fully develop an automated measurement of password creation policy and apply it at scale."

Al Roomi and Li designed an algorithm that automatically determines a website's password policy. With the help of machine learning, the pair could see the consistency of length requirements and restrictions for numbers, upper- and lower-case letters, special symbols, combinations, and starting letters. They could also see if sites permitted dictionary words or known breached passwords.

"As a security community, we've identified and developed various solutions and best practices for improving internet and web security," said Li. "It's crucial that we investigate whether those solutions or guidelines are actually adopted in practice to understand whether security is improving in reality."

The project began during the height of the pandemic when Al Roomi found a gap in the research literature surrounding website password policies. Through his reading, he discovered that a consensus of his peers did not think a large-scale survey of password policies was possible due to the variety of web design.

"It was exciting to see an identified challenge in the literature and to develop and apply a vision we turned into the measurement tool," said Al Roomi. "This research was my first in my Ph.D. program at Georgia Tech and SCP. It is one of the most challenging yet rewarding endeavors I've worked on."

The full report will be presented at the ACM Conference on Computer and Communications Security (CCS) in Copenhagen, Denmark, later this month. The article, "A Large-Scale Measurement of Website Login Policies" was also accepted to the 32nd USENIX Security Symposium earlier this year.

**More information:** A Large-Scale Measurement of Website Login Policies. www.usenix.org/conference/usen … resentation/al-roomi

Provided by Georgia Institute of Technology