Stringent password policies help prevent fraud, study finds

October 11 2018

L. Jean Camp. Credit: Eric Rudd, Indiana University

The all-too-common practice of using the same email address/password combination to log into multiple websites can be damaging, especially for employers with many users and valuable assets protected by passwords, like universities.

"If someone uses their university email address and passphrase to sign up for, say, LinkedIn, and LinkedIn is breached by cybercriminals, that would mean their university password is sitting on the web for everyone to see," said Indiana University's Dan Calarco, co-author on a new paper that examines the practice of password reuse.

But researchers at IU have discovered a simple way to foil criminals intent on breaking into university data.

"We found that requiring longer and more complicated passwords resulted in a lower likelihood of password reuse," the authors write in the paper, Factors Influencing Password Reuse: A Case Study . The authors are Jacob Abbott, an IU Bloomington Ph.D. student; Daniel Calarco, chief of staff for the IU Office of the Vice President for IT and CIO; and L. Jean Camp, a professor in the IU Bloomington School of Informatics, Computing and Engineering. The group presented their findings Sept. 21 at the TPRC46: Research Conference on Communications, Information and Internet Policy in Washington, D.C.

To investigate the impact of policy on password reuse, the study analyzed password policies from 22 different U.S. universities, including their home institution, IU. Next, they extracted sets of emails and passwords from two large data sets that were published online and contained over 1.3 billion email addresses and password combinations. Based on email addresses belonging to a university's domain, passwords were compiled and compared against a university's official password policy.

The findings were clear: Stringent password rules significantly lower a university's risk of personal data breaches.

"Our paper shows that passphrase requirements such as a 15-character minimum length deter the vast majority of IU users (99.98 percent) from reusing passwords or passphrases on other sites," they write. "Other universities with fewer password requirements had reuse rates potentially as high as 40 percent." Their analysis found that IU performed the best of all 22 universities—and had the most extensive requirements. The authors could not legally test whether credentials were actually valid; instead they examined whether passwords could potentially be valid given public password requirements such as password length, complexity and other requirements.

"IU has worked with security and usability faculty to design our password policies, with the result being policies that value people's time while mitigating risk," Camp said. "The length and complexity are balanced by the extended period before new passwords must be generated and the use of a longer authentication time window for applications. Indiana University's rollout of two-factor authentication is similarly a model."

The authors offer the following recommendations to safeguard passwords:

1. Increase the minimum password length beyond 8 characters.
2. Increase maximum password length.
3. Disallow the user's name or username inside passwords.
4. Contemplate multi-factor authentication.

Multi-factor authentication is becoming more common and usable. IU, for example, employs Two-Step Login. With the potential benefits of reducing the risk of password reuse, multi-factor authentication may be a viable alternative to changing the length and/or complexity of password policies.

"Our recommendations are not only applicable for universities, but also can be used by other organizations, services or applications," they write.

Provided by Indiana University

Citation: Stringent password policies help prevent fraud, study finds (2018, October 11) retrieved 11 May 2024 from https://phys.org/news/2018-10-stringent-password-policies-fraud.html