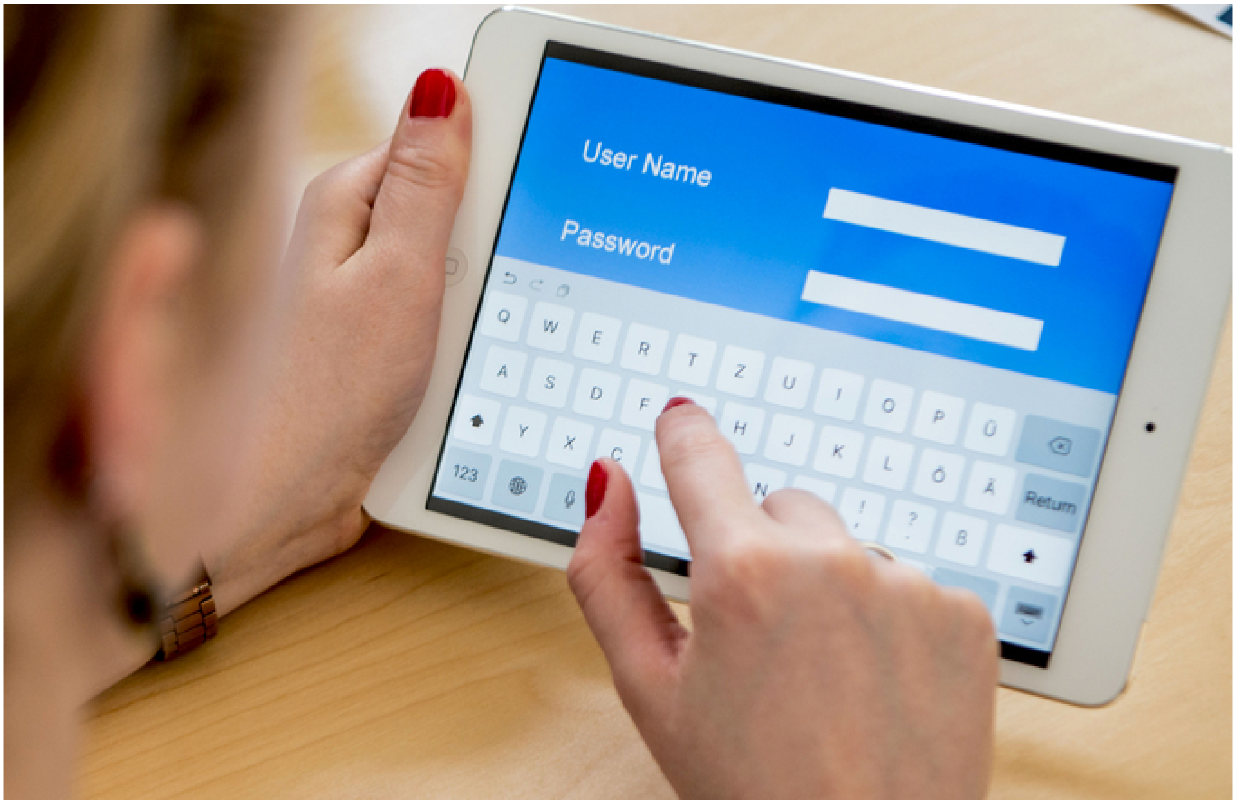
Securely resetting passwords

June 23 2016



On mobile devices, entering passwords is a fairly laborious task. Credit: Ruhr-Universitaet-Bochum

The number of passwords that each of us has to memorise is continuously on the increase. A password is easily forgotten. But watch out: if a new password is generated after the old one was lost, the information might be intercepted by third parties.

With a bit of luck, attackers can guess the correct answers

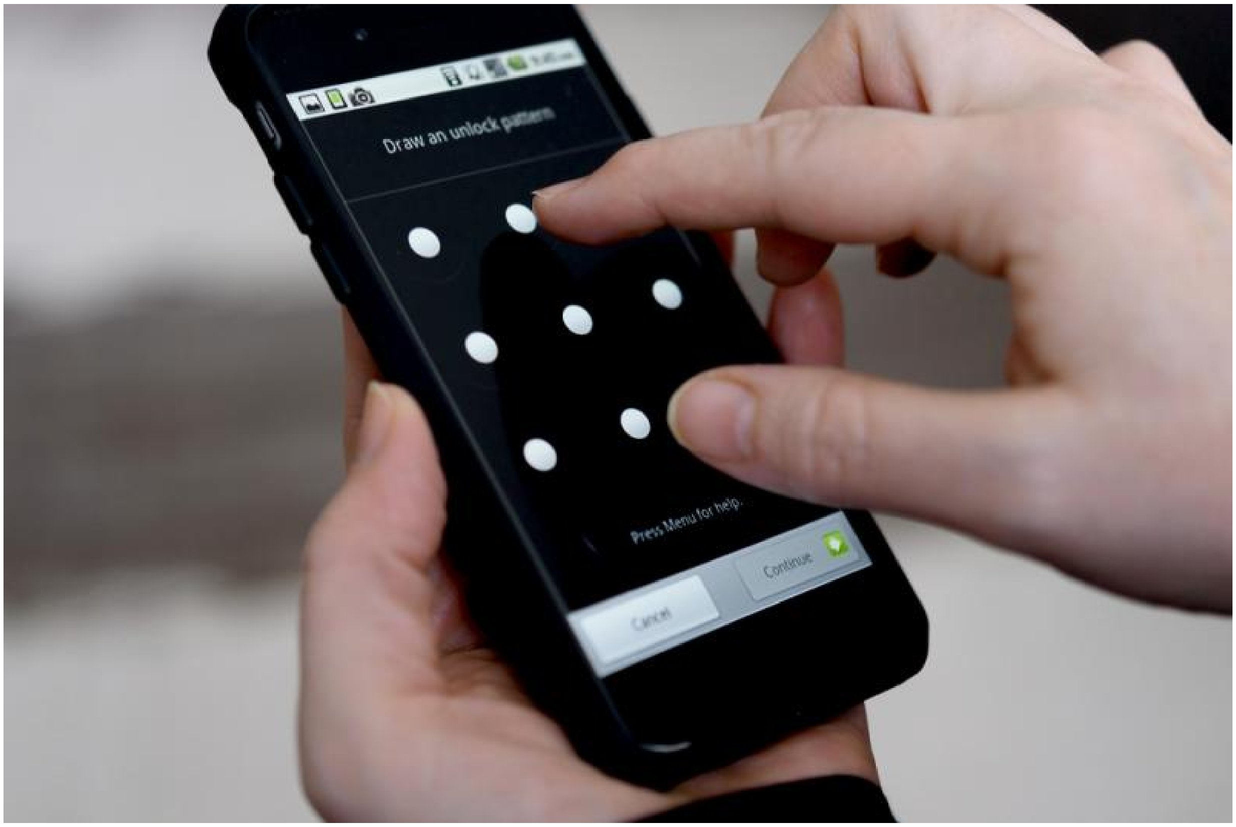
On the whole, losing a password is not a great problem: the Internet user will be sent a new one by email, or he will have to provide a correct answer to a security question to be assigned a new password.

Both methods have certain drawbacks, as Prof Dr Markus Dürmuth, Head of the research group Mobile Security at Ruhr-Universität Bochum (RUB), elaborates: "Emails are usually not encrypted and can be easily intercepted. Whereas correct answers to security questions can be guessed with a bit of luck and some research."

Not discernible at first glance

Together with colleagues from the University of California, Berkeley, and the Institut national de recherche en informatique et en automatique (INRIA), Grenoble, Dürmuth has developed an alternative to the methods described above. To this end, they use so-called Mooney images. This term refers to black-and-white images that were edited using a special filter.

At first glance, it is impossible to tell what a Mooney image is showing. Only after viewing the original picture, a user will be able to recognise the motive – an effect that lasts a long time. This is referred to as priming for a picture.



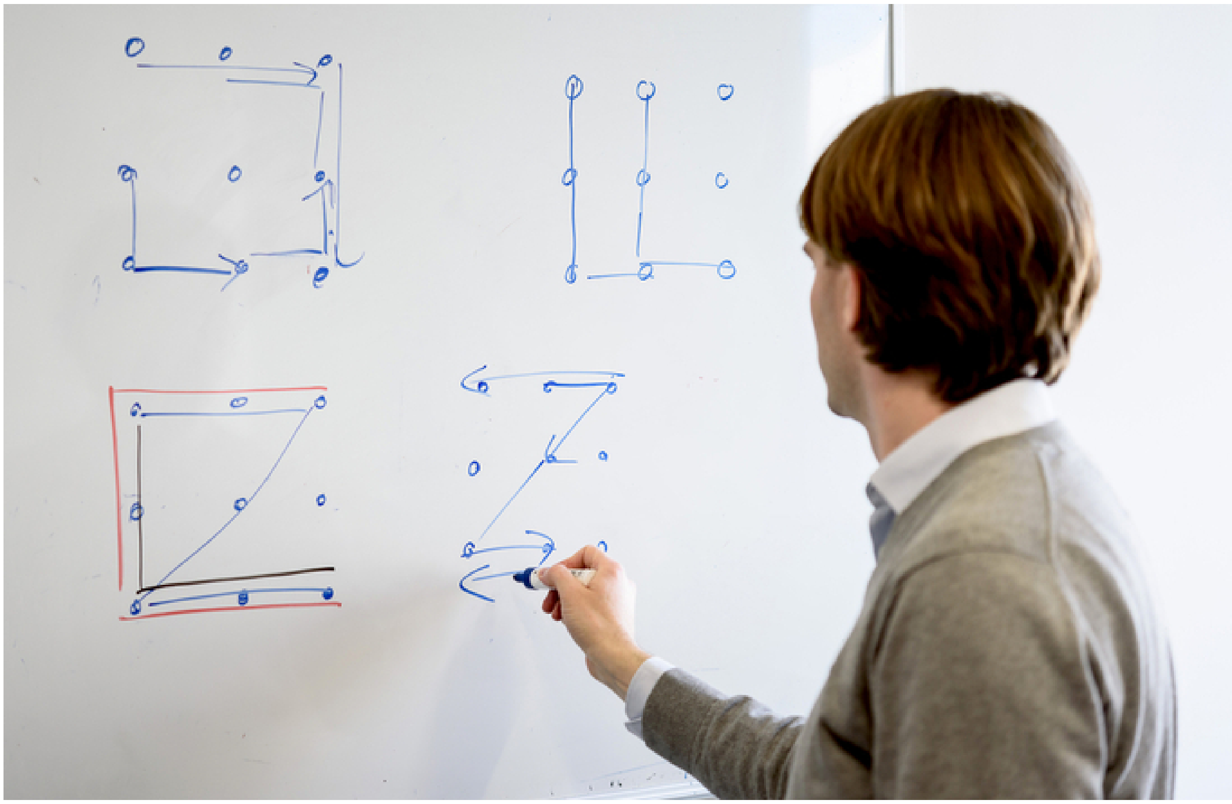
Credit: Ruhr-Universitaet-Bochum

The images originated in the field of brain research. In the 1950s, they were deployed by the psychologist Craig Mooney for examining the so-called aha! effect with the aid of MRI.

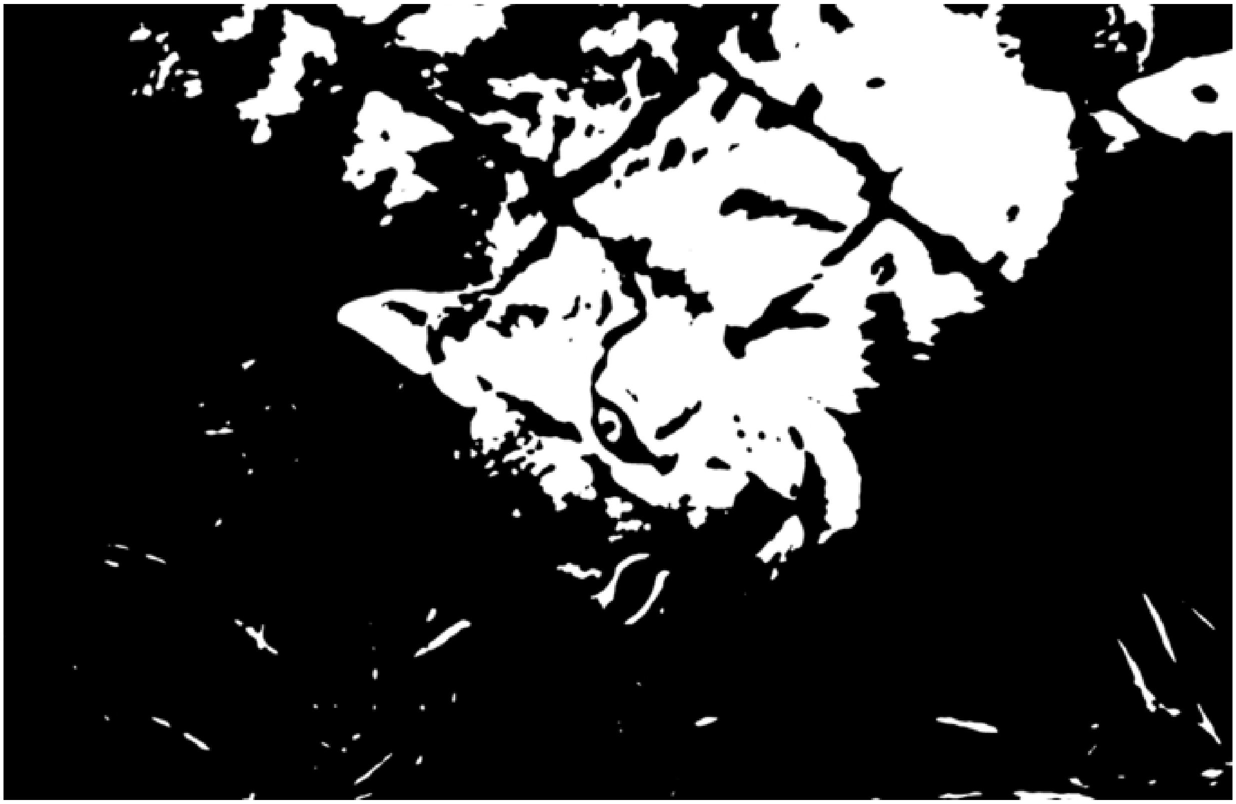
Hackers betray themselves by knowing too much

This is how Dürmuth uses the mechanism: rather than coming up with a security question and answer to prepare for the worst-case scenario, the user is presented ten Mooney images and the respective original pictures during the priming phase. Should he forget his password one day, he will be shown 20 Mooney images and will have to state what he has recognised.

"The true account holder will recognise the ten Mooney images for which he had been primed," explains Dürmuth. "But he won't be able to identify the other ten. Subsequently, he will be assigned a new password ." A hacker would betray himself either by not recognising any Mooney images at all, or recognising those that the true user is not familiar with.



Prof Dr Markus Dürmuth heads the research group Mobile Security at Ruhr-Universität Bochum. Credit: Ruhr-Universitaet-Bochum



Mooney images such as this one may be deployed in future to help users retrieve their forgotten passwords. Credit: Ruhr-Universitaet-Bochum

The original picture to the Mooney image above. A person who had seen it will instantly recognise the Mooney image. Credit: Ruhr-Universitaet-Bochum

Provided by Ruhr-Universitaet-Bochum

Citation: Securely resetting passwords (2016, June 23) retrieved 15 May 2024 from https://phys.org/news/2016-06-resetting-passwords.html