THE CONVERSATION

Academic rigour, journalistic flair

A secure relationship with passwords means not being attached to how you pick them

Published: February 14, 2019 11.47am GMT

Merrill Warkentin

James J. Rouse Endowed Professor of Information Systems, Mississippi State University

Karen Renaud

Professor of Cybersecurity, Abertay University

Robert Otondo

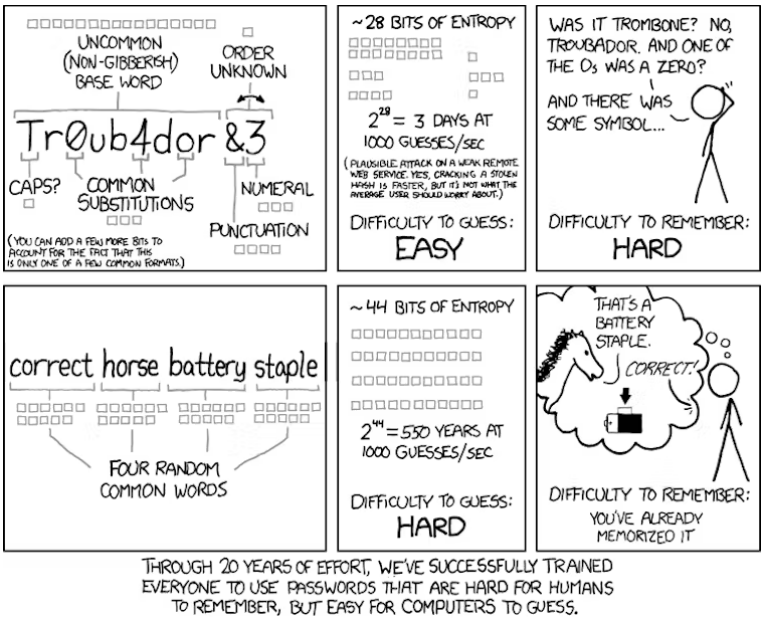
Associate Professor of Information Systems, Mississippi State University

Many people don’t want to let go of how they create passwords. Tono Balaguer/Shutterstock.com

When you are asked to create a password – either for a new online account or resetting login information for an existing account – you’re likely to choose a password you know you can remember. Many people use extremely basic passwords, or a more obscure one they reuse across many sites. Our research has found that others – even ones who use different passwords for each site – have a method of devising them, for instance basing them all on a familiar phrase and making site-specific tweaks.

In all those cases, the people are creating weak passwords that are easily guessed – especially when up against automated password-cracking software that can test thousands of possibilities a second. One reason for this weakness might well be their users' emotional connection to their preexisting password creation routine.

Cybersecurity efforts often encourage people to choose stronger passwords, but rarely acknowledge the idea that people have this feeling of attachment. They focus on the measurable improvement in security without realizing they're trying to persuade people to switch to a less personal method.



There's a better way to choose a secure password. XKCD, CC BY-SA

Insecure tendencies

Passwords are key to cybersecurity for people and companies. A single bad password can grant a hacker access to an entire network of computers and data-storage servers.

As a result, many computer systems force users to create new passwords regularly – say, every 30 or 45 days – and require every password to contain capital letters, numbers and punctuation characters even though federal experts advise against both of these practices. Regularly requiring people to choose new passwords that are hard to remember leads to unfortunate side effects. People could reuse a strong password on several sites, or they could write down the new password – which is safe only if you trust the other people who have access where you store the record.

Training people to create secure passwords hasn't made much of a difference to overall password security on the internet. People may not understand the risks related to weak passwords – though some experts blame character flaws, stupidity or just plain indifference.

The endowment effect

Our research has identified another explanation for why people choose weak passwords: People feel that they own, and are emotionally attached to, the way they usually create passwords. In behavioral economics, this kind of response is called the endowment effect, in which people so overvalue their existing possessions that they don't want to exchange them for other items – even if the new item is better or more valuable.

Seriously, it's time to replace this old clothes washer. Dja65/Shutterstock.com

The endowment effect is usually applied to physical goods – and may help explain why your grandmother doesn't want to get a new washing machine to replace her decades-old one. Our research suggests that the same psychological process influences how people contemplate their password creation routines.

In our study, we asked 419 participants how they created their passwords. Many used something they already knew, such as a pet name or their own birthday. Others had developed a personal system. They might have a root password and then personalize it for every different site, use a pattern on the keyboard or make up a silly sentence.

When we probed more deeply, we found that people felt a sense of ownership and personal pride about their password creation routine. One said "I think my way is a good system." In addition, we found that they overvalued their own method and felt threatened by suggestions that it was flawed.

We provided a scenario where "Terry" derides "Pat's" password creation routine, and then asked people how they thought Pat would react. The most popular responses were: becoming defensive, avoiding the conversation or withdrawing from it. All of these suggest that a critique of a personal password routine was perceived as an attack or a threat.

These answers we found lined up perfectly with the endowment effect, including finding that the participants labored under the illusion that their passwords provided more protection than they actually did.

More than just a habit

The attachment people feel to their password-choosing method is more than just a habit. Psychologically speaking, a habit is a behavior cued by an event or an item in the environment – like brushing teeth before bed, washing hands before meals or switching off lights when leaving a room. They're often nearly automatic, and don't require a deliberate decision or much thought. Something that's a habit seems to occur naturally, without any deliberate decision triggering its activation.

Choosing a password is different. It always requires deliberate and effortful cognition. That's what brings the endowment effect into play. Cybersecurity training programs should include information not only about how to choose more secure passwords, but also should acknowledge that users may feel a sense of loss about the change.

People won't pick stronger passwords just because they're asked to. If they feel their existing methods are being treated with disdain, they might perceive that as a personal attack, and become even less likely to adopt more secure practices.

Instead, security experts should find ways to minimize users' sense of loss – and perhaps even encourage them to find a new emotional connection to a more secure method of choosing.