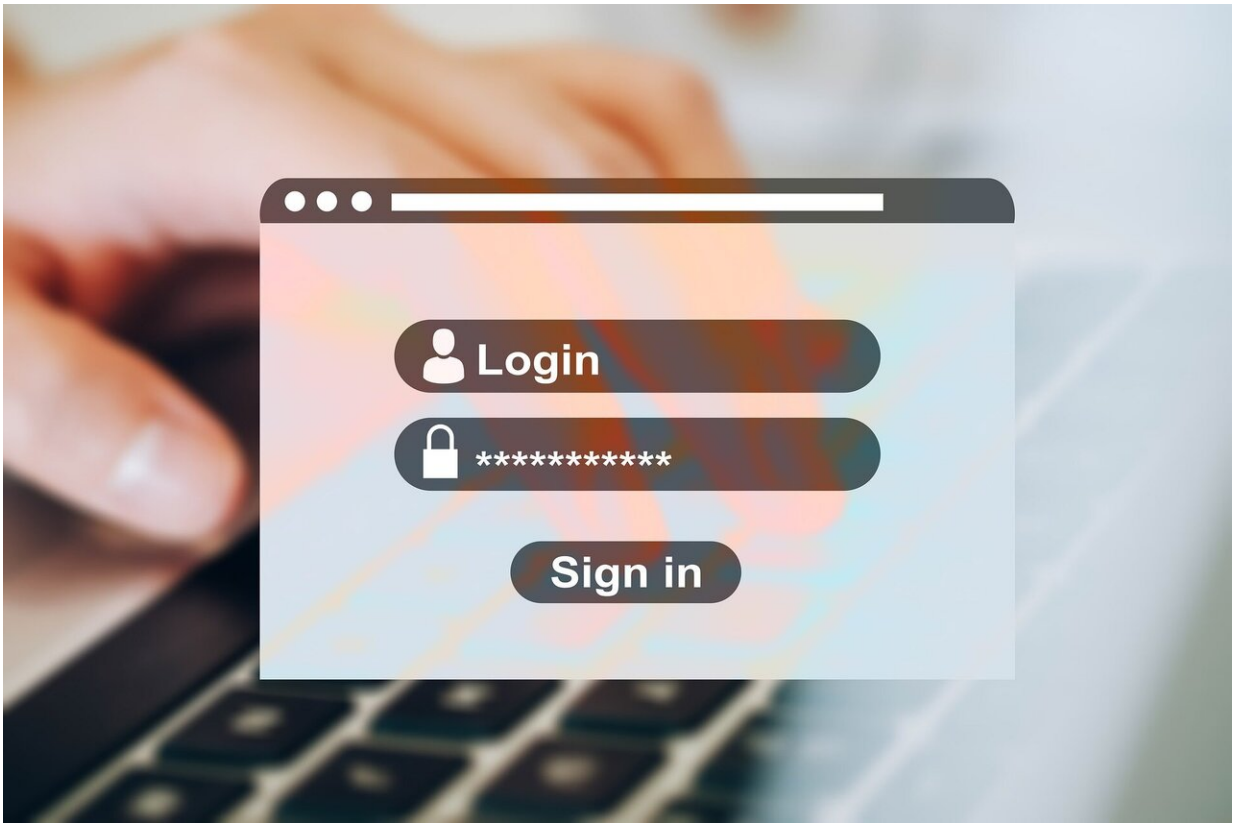
What are passkeys? A cybersecurity researcher explains how you can use your phone to make passwords a thing of the past

April 13 2023, by Sayonnha Mandal



Credit: Pixabay/CC0 Public Domain

Passwords could soon become passé.

Effective passwords are cumbersome, all the more so when reinforced by two-factor authentication. But the need for authentication and secure access to websites is as great as ever. Enter passkeys.

Passkeys are digital credentials stored on your phone or computer. They are analogous to physical keys. You access your passkey by signing in to your device using a personal identification number (PIN), swipe pattern or biometrics like fingerprint or face recognition. You set your online accounts to trust your phone or computer. To break into your accounts, a hacker would need to physically possess your device and have the means to sign in to it.

As a cybersecurity researcher, I believe that passkeys not only provide faster, easier and more secure sign-ins, they minimize human error in password security and authorization steps. You don't need to remember passwords for every account and don't need to use two-factor authentication.

How passkeys work

Passkeys are generated via public-key cryptography. They use a public-private key pair to ensure a mathematically protected private relationship between users' devices and the online accounts being accessed. It would be nearly impossible for a hacker to guess the passkey—hence the need to physically possess the device the passkey is accessed from.

Passkeys consist of a long private key—a long string of encrypted characters—created for a specific device. Websites cannot access the value of the passkey. Rather, the passkey verifies that a website possesses the corresponding public key. You can use the passkey from one device to access a website using another device. For example, you can use your laptop to access a website using the passkey on your phone by authorizing the login from your phone. And if you lose your phone,

the passkey can be stored securely in the cloud with the phone's other data, which can be restored to a new phone.

Why passkeys matter

Passwords can be guessed, phished or otherwise stolen. Security experts advise users to make their passwords longer with more characters, mixing alphanumeric and special symbols. A good password should not be in the dictionary or in phrases, have no consecutive letters or numbers, but be memorable. Users should not share them with anyone. Last but not least, users should change passwords every six months at minimum for all devices and accounts. Using a password manager to remember and update strong passwords helps but can still be a nuisance.

Even if you follow all of the best practices to keep your passwords safe, there is no guarantee of airtight security. Hackers are continuously developing and using software exploits, hardware tools and ever-advancing algorithms to break these defenses. Cybersecurity experts and malicious hackers are locked in an arms race.

Passkeys remove the onus from the user to create, remember and guard all their passwords. Apple, Google and Microsoft are supporting passkeys and encourage users to use them instead of passwords. As a result, passkeys are likely to soon overtake passwords and password managers in the cybersecurity battlefield.

However, it will take time for websites to add support for passkeys, so passwords aren't going to go extinct overnight. IT managers still recommend that people use a password manager like 1Password or Bitwarden. And even Apple, which is encouraging the adoption of passkeys, has its own password manager.

Commons license. Read the original article.

Provided by The Conversation