Google Security Blog

The latest news and insights from Google on security and safety on the Internet

So long passwords, thanks for all the phish

May 3, 2023

By: Arnar Birgisson and Diana K Smetters, Identity Ecosystems and Google Account Security and Safety teams

Starting today, you can create and use passkeys on your personal Google Account. When you do, Google will not ask for your password or 2-Step Verification (2SV) when you sign in.

Passkeys are a more convenient and safer alternative to passwords. They work on all major platforms and browsers, and allow users to sign in by unlocking their computer or mobile device with their fingerprint, face recognition or a local PIN.

Using passwords puts a lot of responsibility on users. Choosing strong passwords and remembering them across various accounts can be hard. In addition, even the most savvy users are often misled into giving them up during phishing attempts. 2SV (2FA/MFA) helps, but again puts strain on the user with additional, unwanted friction and still doesn't fully protect against phishing attacks and targeted attacks like "SIM swaps" for SMS verification. Passkeys help address all these issues.

Creating passkeys on your Google Account

When you add a passkey to your Google Account, we will start asking for it when you sign in or perform sensitive actions on your account. The passkey itself is stored on your local computer or mobile device, which will ask for your screen lock biometrics or PIN to confirm it's really you. Biometric data is never shared with Google or any other third party – the screen lock only unlocks the passkey locally.

Unlike passwords, passkeys can only exist on your devices. They cannot be written down or accidentally given to a bad actor. When you use a passkey to sign in to your Google Account, it proves to Google that you have access to your device and are able to unlock it. Together, this means that passkeys protect you against phishing and any accidental mishandling that passwords are prone to, such as being reused or exposed in a data breach. This is stronger protection than most 2SV (2FA/MFA) methods offer today, which is why we allow you to skip not only the password but also

2SV when you use a passkey. In fact, passkeys are strong enough that they can stand in for security keys for users enrolled in our Advanced Protection Program.

Creating a passkey on your Google Account makes it an option for sign-in. Existing methods, including your password, will still work in case you need them, for example when using devices that don't support passkeys yet. Passkeys are still new and it will take some time before they work everywhere. However, creating a passkey today still comes with security benefits as it allows us to pay closer attention to the sign-ins that fall back to passwords. Over time, we'll increasingly scrutinize these as passkeys gain broader support and familiarity.

Using passkeys to sign in to your Google Account

Using passkeys does not mean that you have to use your phone every time you sign in. If you use multiple devices, e.g. a laptop, a PC or a tablet, you can create a passkey for each one. In addition, some platforms securely back your passkeys up and sync them to other devices you own. For example, if you create a passkey on your iPhone, that passkey will also be available on your other Apple devices if they are signed in to the same iCloud account. This protects you from being locked out of your account in case you lose your devices, and makes it easier for you to upgrade from one device to another.

If you want to sign in on a new device for the first time, or temporarily use someone else's device, you can use a passkey stored on your phone to do so. On the new device, you'd just select the option to "use a passkey from another device" and follow the prompts. This does not automatically transfer the passkey to the new device, it only uses your phone's screen lock and proximity to approve a one-time sign-in. If the new device supports storing its own passkeys, we will ask separately if you want to create one there.

In fact, if you sign in on a device shared with others, you should not create a passkey there. When you create a passkey on a device, anyone with access to that device and the ability to unlock it, can sign in to your Google Account. While that might sound a bit alarming, most people will find it easier to control access to their devices rather than maintaining good security posture with passwords and having to be on constant lookout for phishing attempts.

If you lose a device with a passkey for your Google Account and believe someone else can unlock it, you can immediately revoke the passkey in your account settings. If your device supports the option

to remotely wipe it, consider doing that as well, especially if it also has passkeys for other services. We always recommend having a recovery phone and email on your account, as it increases your chance of recovering it in case someone gains access.

To start using passkeys on your personal Google Account today, visit g.co/passkeys.

How does this work under the hood?

The main ingredient of a passkey is a cryptographic private key – this is what is stored on your devices. When you create one, the corresponding public key is uploaded to Google. When you sign in, we ask your device to sign a unique challenge with the private key. Your device only does so if you approve this, which requires unlocking the device. We then verify the signature with your public key.

Your device also ensures the signature can only be shared with Google websites and apps, and not with malicious phishing intermediaries. This means you don't have to be as watchful with where you use passkeys as you would with passwords, SMS verification codes, etc. The signature proves to us that the device is yours since it has the private key, that you were there to unlock it, and that you are actually trying to sign in to Google and not some intermediary phishing site. The only data shared with Google for this to work is the public key and the signature. Neither contains any information about your biometrics.

The private key behind the passkey lives on your devices and in some cases, it stays only on the device it was created on. In other cases, your operating system or an app similar to a password manager may sync it to other devices you own. Passkey sync providers like the Google Password Manager and iCloud Keychain use end-to-end encryption to keep your passkeys private.

Since each passkey can only be used for a single account, there is no risk of reusing them across services. This means that your Google Account is safe from data breaches across your other accounts, and vice versa.

When you do need to use a passkey from your phone to sign in on another device, the first step is usually to scan a QR code displayed by that device. The device then verifies that your phone is in proximity using a small anonymous Bluetooth message and sets up an end-to-end encrypted connection to the phone through the internet. The phone uses this connection to deliver your one-time passkey signature, which requires your approval and the biometric or screen lock step on the phone.

Neither the passkey itself nor the screen lock information is sent to the new device. The Bluetooth proximity check ensures remote attackers can't trick you into releasing a passkey signature, for example by sending you a screenshot of a QR code from their own device.

Passkeys are built on the protocols and standards Google helped create in the FIDO Alliance and W3C WebAuthn working group. This means passkey support works across all platforms and browsers that adopt these standards. You can store the passkeys for your Google Account on any compatible device or service.

The same standards and protocols power security keys, our strongest offering for high risk accounts. Passkeys inherit many of their strong account protections from security keys, but with convenience that is suitable for everyone.

Today's launch is a big step in a cross-industry effort that we helped start more than 10 years ago, and we are committed to passkeys as the future of secure sign-in, for everyone. We hope that other web and app developers adopt passkeys and are able to use our deployment as a model. Developers can learn more about passkey support on our Chrome and Android platforms here.

No comments :

Post a Comment