Facebook Adds FIDO U2F Security Keys Feature For Secure Logins

---

Posted by Hermes 02/19/2017

Hacking password for a Facebook account is not easy, but also not impossible.

We have always been advising you to enable two-factor authentication — or 2FA — to secure your online accounts, a process that requires users to manually enter, typically a six-digit secret code generated by an authenticator app or received via SMS or email.

So even if somehow hackers steal your login credentials, they would not be able to access your account without one-time password sent to you.

But, Are SMS-based one-time passwords Secure?

US National Institute of Standards and Technology (NIST) is also no longer recommending SMS-based two-factor authentication systems, and it's not a reliable solution mainly because of two reasons:

- Users outside the network coverage can face issues
- Growing number of sophisticated attacks against OTP schemes

So, to beef up the security of your account, Facebook now support Fido-compliant Universal 2nd Factor Authentication (U2F), allows users to log into their Facebook account using a physical security key, such as the YubiKey, instead of relying on a one-time passcode sent via text message or email.

Compared with the traditional authentication protocols, Universal 2nd Factor Authentication (U2F) is a hardware-based authentication aims to simplify, fasten and secure two-factor authentication process.

U2F standard as a security feature has already been implemented by major companies including Google, Dropbox, GitHub, Salesforce and supported by Chrome and Opera web browsers.

The best thing about this standard is that one tiny little device can be used to authenticate with any number of online services and no mobile connection or batteries are required.

These hardware-based security keys are easy to use and deploy. You just need to simply plug-in the inexpensive USB device (which starts at about $10) into your computer's USB port to get into your Facebook account from any computer anywhere.

Ready to activate your security key for your Facebook account?

- Go to Security settings of your Facebook account.
- Open Login Approval and Click "Add Key" shown in front of 'Security Key.'
- 'Add Key ' and Facebook will ask you to "Insert your security key into a USB port."

Note: Hardware-based Security Key will only work if you're using the Chrome or Opera browser.

For more detailed instructions on setting up a security key, you can head on to this page.

How to Authenticate to your Account using the Fido-compliant U2F device? Simple, whenever next time you log into your Facebook account you'll be asked to plug your security key into the USB slot.

Once you plug in, the tiny device generates an encrypted, one-time security passcode for use in two-factor authentication (2FA) systems and logs you into your Facebook account.

These hardware-based security keys are thought to be more efficient at preventing phishing, man-in-the-middle (MITM) and other types of account-takeover attacks than 2FA via SMS, as even if your credentials are compromised, account login is impossible without that physical key.

> "By adding FIDO authentication to its security portfolio, Facebook gives their users the option to enable unphishable strong authentication that is no longer vulnerable to social engineering and replay attacks using stolen 'shared secrets' like passwords and one-time-passcodes," said Brett McDowell, executive director of the FIDO Alliance.

At this moment, security key logins for the mobile Facebook app is not supported, but users with NFC-capable Android device and the latest version of Chrome and Google Authenticator installed can use a security key to log in from their mobile website.
