BUZZ CHRONICLES > TECH
Saved by @zmbnski
See On Twitter

Twitter Thread by Paul Stamatiou ■

Paul Stamatiou ■
@Stammy

Just published 15,000+ words on security keys. ■■■

With SIM attacks at their highest, now is a great time to take a closer look at your online security.

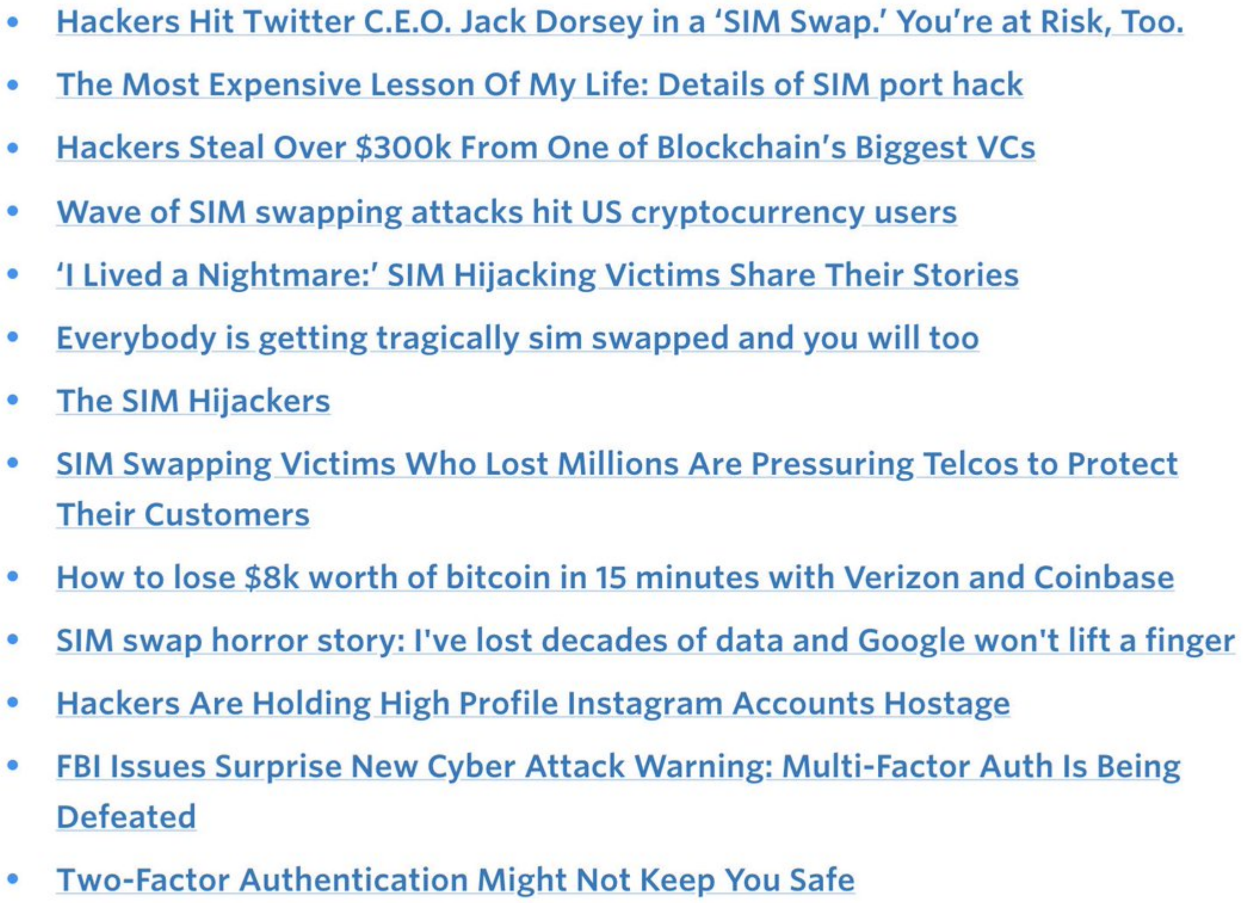
Removing SMS from your two-factor auth is a start, but authenticator apps have downsides too...

https://t.co/Dk0MPJHL2V

Just look at these headlines from recent SIM swap and port attacks.

It's all too established for attackers to find ways to socially engineer control of your phone number and start gaining control of your accounts.

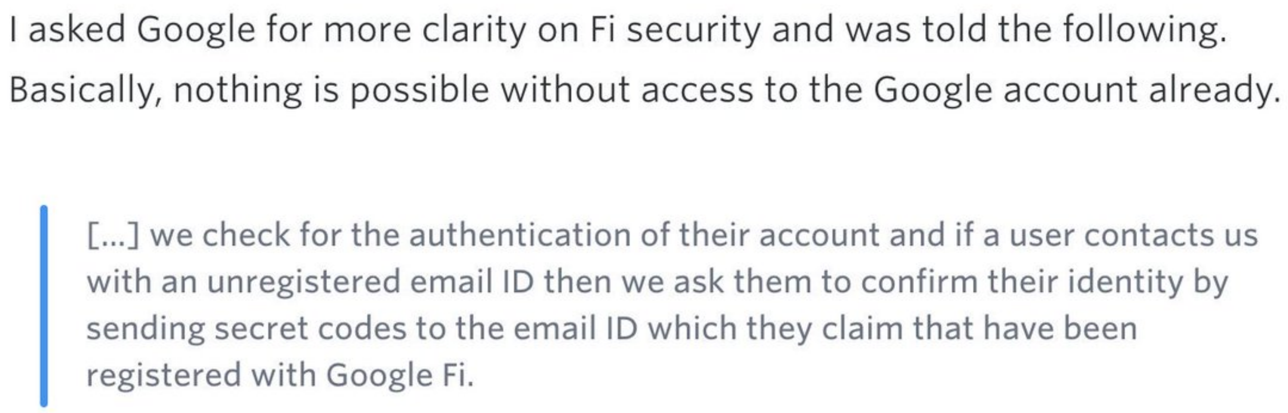
I first talk about some general security tips.



- Hackers Hit Twitter C.E.O. Jack Dorsey in a 'SIM Swap.' You're at Risk, Too.
- The Most Expensive Lesson Of My Life: Details of SIM port hack
- Hackers Steal Over $300k From One of Blockchain's Biggest VCs
- Wave of SIM swapping attacks hit US cryptocurrency users
- 'I Lived a Nightmare:' SIM Hijacking Victims Share Their Stories
- Everybody is getting tragically sim swapped and you will too
- The SIM Hijackers
- SIM Swapping Victims Who Lost Millions Are Pressuring Telcos to Protect Their Customers
- How to lose $8k worth of bitcoin in 15 minutes with Verizon and Coinbase
- SIM swap horror story: I've lost decades of data and Google won't lift a finger
- Hackers Are Holding High Profile Instagram Accounts Hostage
- FBI Issues Surprise New Cyber Attack Warning: Multi-Factor Auth Is Being Defeated
- Two-Factor Authentication Might Not Keep You Safe

Unfortunately not all websites let you remove your phone number from accounts.

You may consider migrating your phone carrier to @googlefi , which requires email account access to do anything (and can be locked down with security keys and even Advanced Protection)



I asked Google for more clarity on Fi security and was told the following. Basically, nothing is possible without access to the Google account already.

> [...] we check for the authentication of their account and if a user contacts us with an unregistered email ID then we ask them to confirm their identity by sending secret codes to the email ID which they claim that have been registered with Google Fi.

Beyond SMS, I talk about issues that TOTP authenticator apps (the code generators) have as a form of two-factor auth. They're so, so much better than relying on SMS for your second factor but they still have issues like utilizing shared secrets and lacking phishing prevention.

Enter security keys!

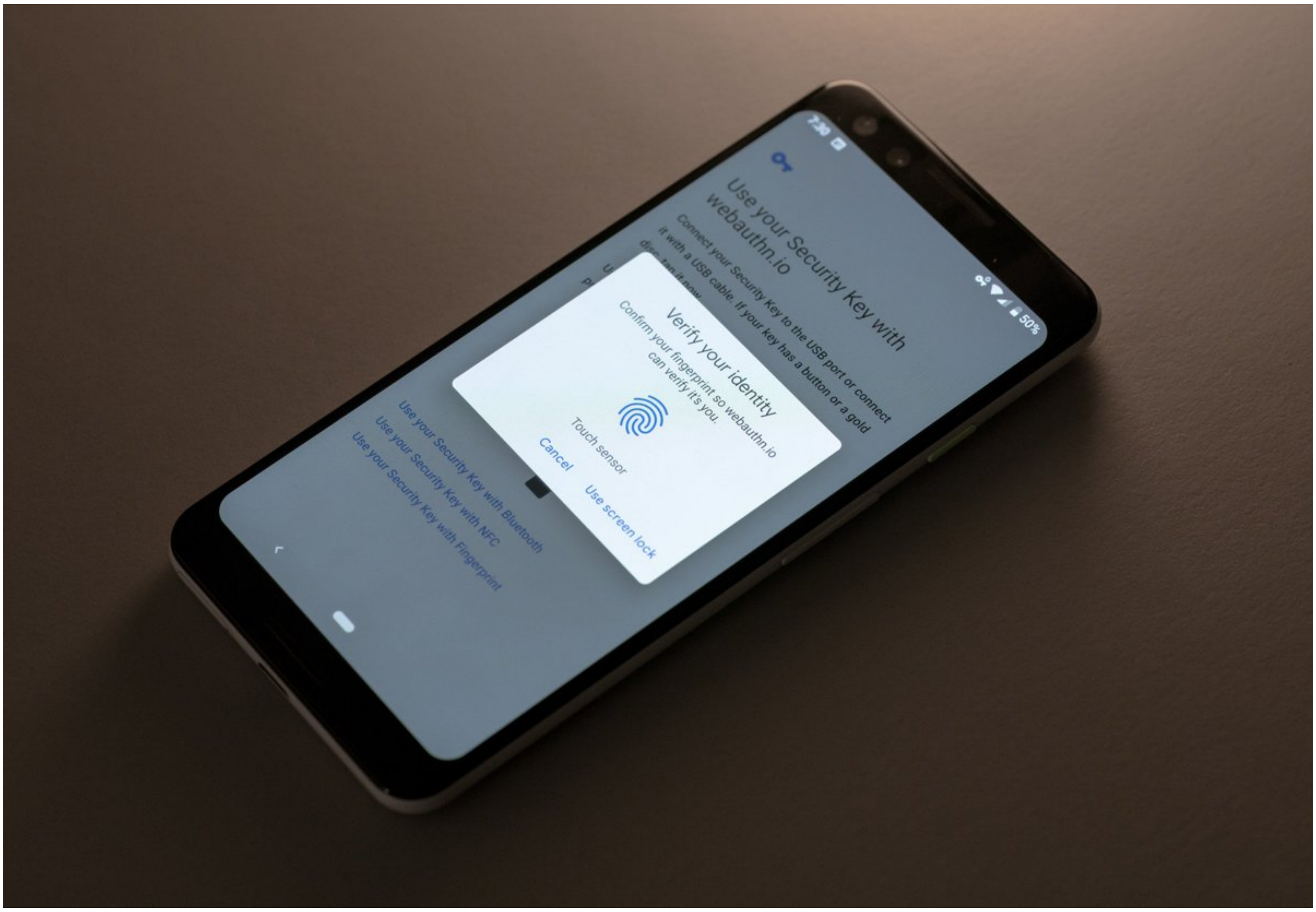
Utilizing public key cryptography they don't have any shared secret between the client and the server. They prevent phishing by taking the website domain into account.

Even if you get tricked by a clone phishing website, your key won't.

Keys have been around for a while under various names and technologies. Recently it was FIDO U2F + CTAP1 but now we have FIDO2 WebAuthn with CTAP2..

It's all very confusing...

Security keys are great for two-factor auth but FIDO2 has a vision for more: support for platform authenticators (like fingerprint readers and other biometrics) as well as being able to use them for "passwordless" authentication.
https://t.co/qHI8n8x8m6


Use your Security Key with webauthn.io
Connect your Security Key to the USB port or connect it with a USB cable. If your key has a button or a gold
Verify your identity
Confirm your fingerprint so webauthn.io can verify it's you.
Touch sensor
Cancel
Use screen lock
Use your Security Key with Bluetooth
Use your Security Key with NFC
Use your Security Key with Fingerprint
50%

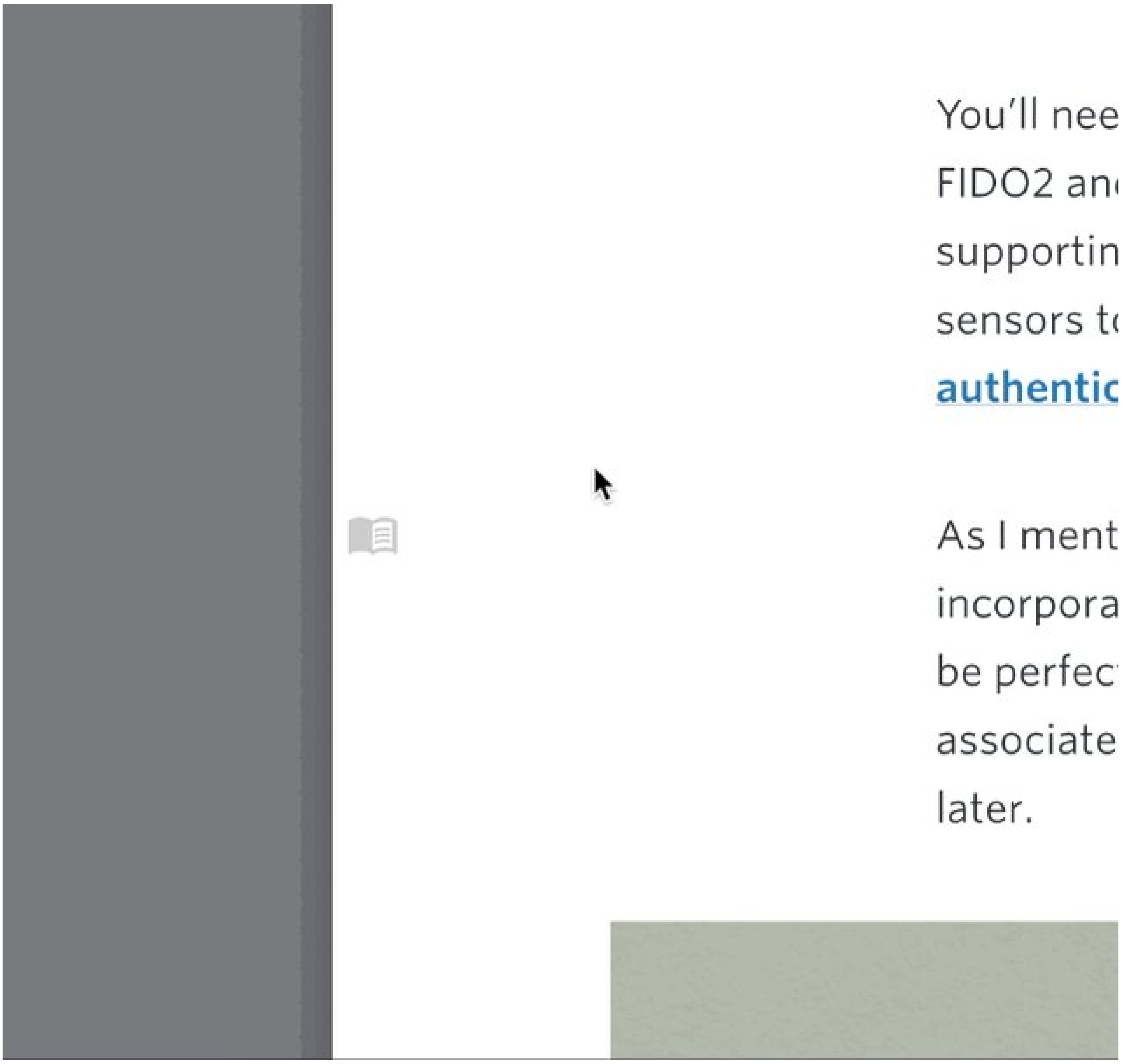
But this area is still nascent. Plagued by years of sub-par security key support across browsers. Things have been getting better in recent years with recently updated NFC support on iOS 13 but it's still a waiting game until things are made easier.

Which brings the question.. Why must I carry around an extra device just to be safe online?

You shouldn't. WebAuthn aims to change that.

But for now, security keys—combined with strong online security best practices—are a great way to fortify your regular online activities.

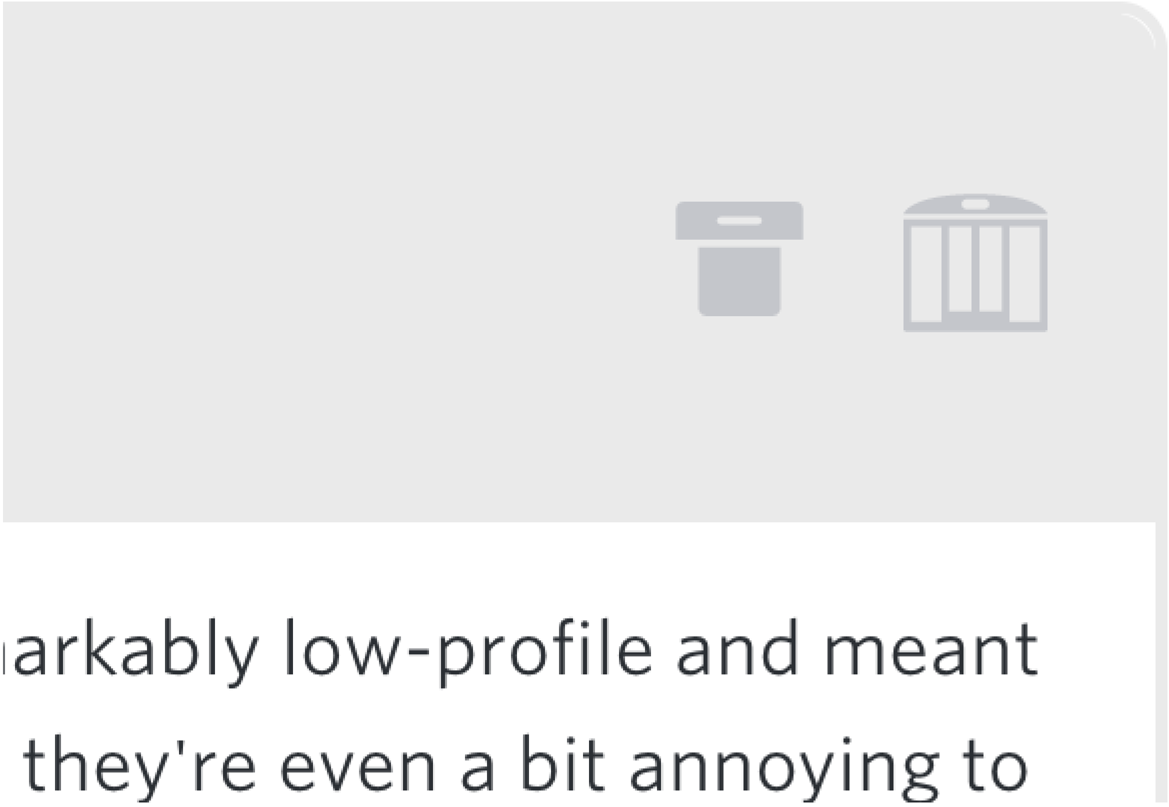
This article was so long (like all of mine) that I took the time to build this little fly-out table of contents browser ■



You'll nee
FIDO2 an
supportin
sensors t
authentic

As I ment
incorpora
be perfec
associate
later.

I also went out of my way to design these little security key icons in figma while I was writing this ■ cc @Yubico



arkably low-profile and meant
they're even a bit annoying to