portswigger.net

U2F nowhere near ready for prime time

John Leyden @jleyden

15-19 minutes

Anti-phishing tech is anything but universal

The use of hardware security keys to secure online accounts against phishing is being heavily promoted by the industry, but tests by The Daily Swig have shown that the technology remains poorly supported by websites and browsers.

Even some consumer-focused services that support U2F-based authentication – such as Facebook and Twitter – fall back to supporting less secure app or SMS-based authentication in the absence of a hardware key, undermining most of the extra security protections the tech might otherwise offer.

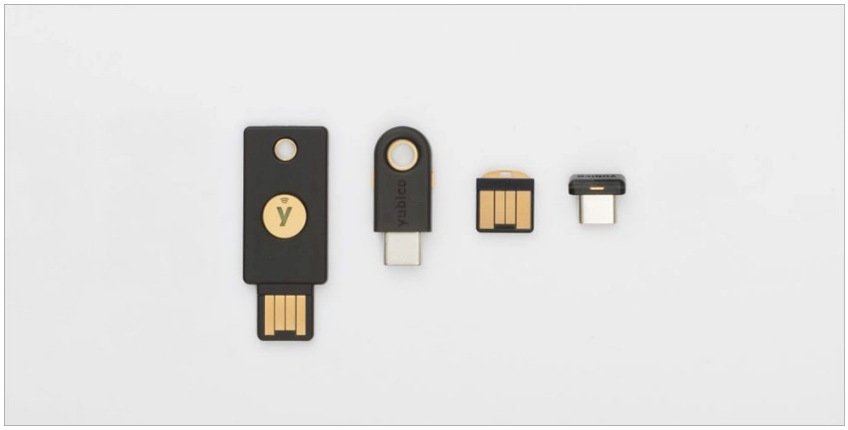
Life, the Universe, and Authentication

U2F (Universal 2nd Factor) is an open authentication standard designed to strengthen two-factor authentication (2FA). The technology, managed by the FIDO Alliance, makes use of USB or near-field communication (NFC) technology, and is similar to that widely found in smart cards.

Two-factor authentication renders a password and login ID alone not enough to log into an online account.

The second factor typically comes in the form of a six-digit number sent by a service provider to a user's pre-registered mobile phone, either via an SMS message or by an app.

After setup, a one-time 2FA code sent via SMS needs to be confirmed before access is granted.



Fly in the ointment

The growing prevalence of SIM-swap scams has rendered this approach perilous. Using either an SMS message or automated phone call to receive a one-time code is less secure than using a mobile authentication app such as Google Authenticator or Authy to generate codes.

More sophisticated approaches to phishing that incorporate man-in-the-middle attacks can circumvent these protections through schemes geared towards tricking users into handing over their codes as well as their passwords.

Either approach – more accurately described as two-step rather than two-factor authentication – is much better than relying on a password alone, even though it's far from bullet-proof.

The threat is far from academic. Various forms of malware-based attacks targeting 2FA have already been developed.

Hackers have even developed web-based attack tools to dumb down the process of circumventing 2FA, such as the recently uncovered Modlishka utility.

More secure forms of authentication involve "something that you know" alongside "something that you have" (a token) or "something that you are" (biometrics).

This is where U2F comes in.

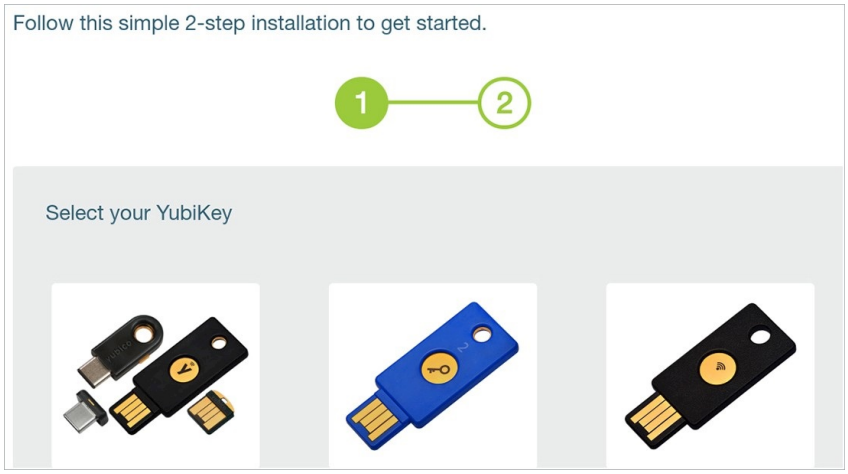
Google proudly states that it has avoided a successful phishing attack against any of its workers since the mandatory introduction of U2F back in 2017.

The tech firm's Advanced Protection Program is also built on the foundation of U2F tech. The program is aimed at journalists, activists, and political campaign teams, but isn't available for

business-focused G Suite accounts.

Google is by far the only organization to promote U2F hardware key authentication tech. Last month, the Committee to Protect Journalists started actively encouraging reporters to use security keys to access online accounts.

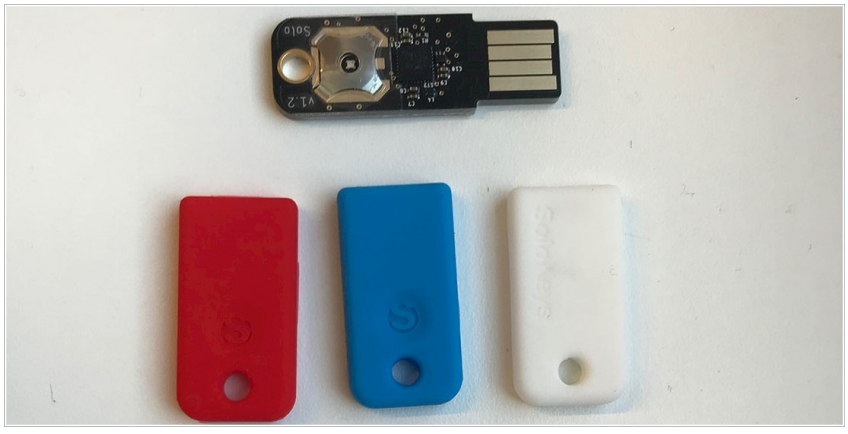
U2F hardware keys are hot right now. The devices cost from just $20, they clearly fulfill a need, and their promise is enticing.



Select your YubiKey

Recently, The Daily Swig sourced samples of the tech. We obtained a YubiKey from Yubico – probably the best-known brand in the market – as well as U2F security keys from Nitrokey and start-up SoloKey.

We would have also liked to have gotten our hands on Google's Titan security key, but these are not yet available in Europe, thwarting our ambitions in that direction.

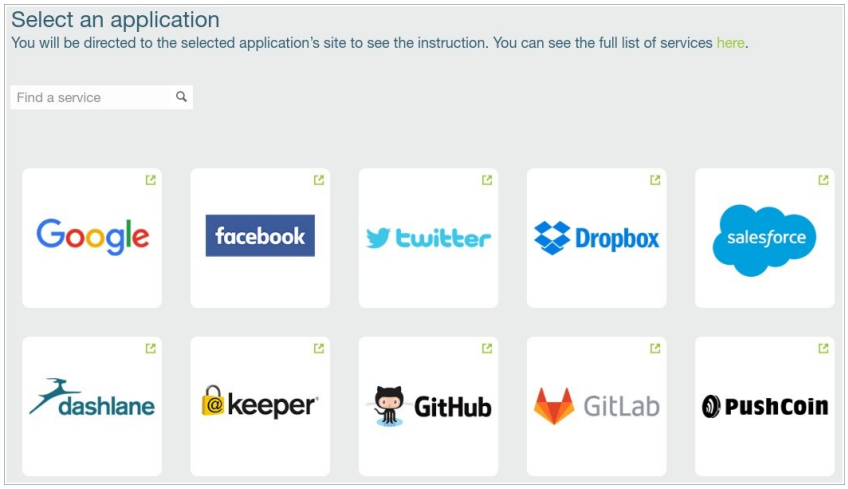


SoloKeys and sheaths

We set off wanting to do a comparative review, but it quickly became apparent that, at this point, support for U2F technology among web services in general was a much bigger issue than the competitive features of different devices.

Accordingly, we decided to explore this technology, rather than writing a straight product review.

As the dongleauth.info tracker site notes, consumer-facing sites that support U2F include Twitter, Facebook, and Dropbox, as well as Google and its various properties (including, but not limited to, Gmail). The websites and web services of both Apple and Microsoft are yet to support U2F.



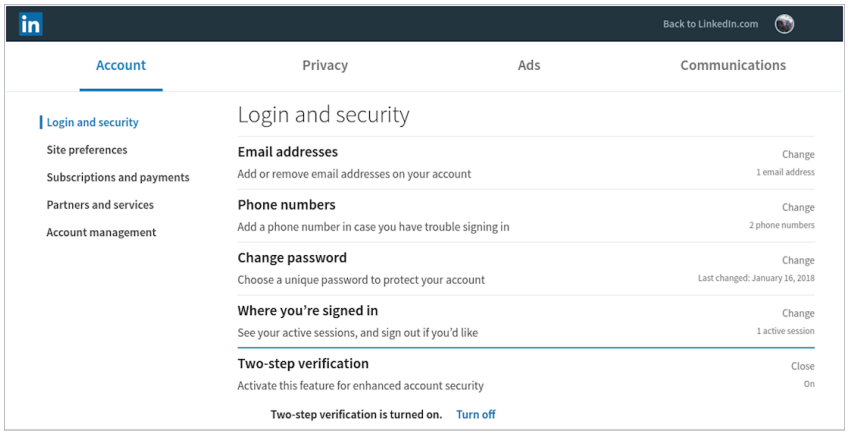
U2F supported sites

In the financial services sector, an obvious arena for the application of U2F and the stronger authentication it promises, the picture is even more patchy.

For example, online payment technology Stripe supports U2F, but PayPal does not. PayPal is a particularly striking omission since it's a member of the FIDO2 Project alliance. Likewise, eBay's adoption has yet to materialize.

U2F is a technology well suited to the requirement of enterprise-focused services. GitLab and BitBucket support its use by software developers, the main users of both services.

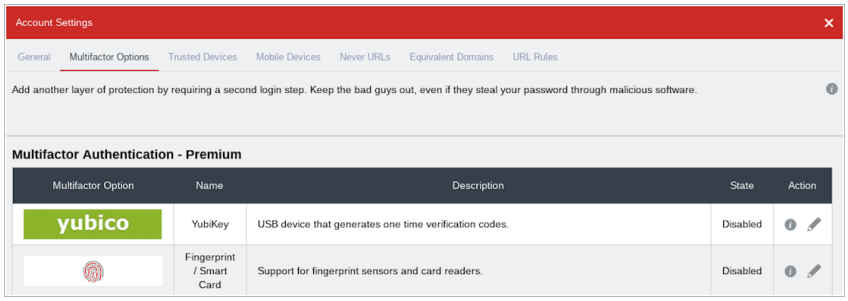
Support for U2F is also found in Amazon Web Services, if not on the e-commerce side of Amazon's business.



LinkedIn only supports two-step verification

If there's one area where you'd expect U2F technology to be encouraged, it's among password managers. Here again, though, matters are lacking.

LastPass endorses U2F, but only in the premium version of its product.



LastPass only supports U2F with the premium version of its service

It's a similar story with Dashlane. We found adding a security key to a Windows installation of the Dashlane app to be a cumbersome process.

Another major player, 1Password, only supports YubiKey for hardware key-based authentication.

Four-squared

With a limited list of (consumer-focused) targets, we decided to focus on signing up to use U2F for Google (Gmail), social media (Twitter and Facebook), and Dropbox accounts. We used a Chromebook and Windows 7 machine in our testing.

Phase one of enrolment generally involves associating an account with a mobile phone and sending a code via text to confirm it. Users can then switch to the more convenient route of receiving their codes through an app.

Our testing failed to uncover any example of jumping straight to using U2F hardware keys without preliminaries – you had to enroll for SMS or app-based authentication first.

During the process of adding a hardware key, you'll be asked to log back into an account. It's a good idea to sign up with a backup key at the same time, just in case you lose your main one.

One of these keys should be NFC compatible so that it works with your smartphone. If you lose one of your keys you can use the other to login, un-enroll the lost key, and sign up with a new one.

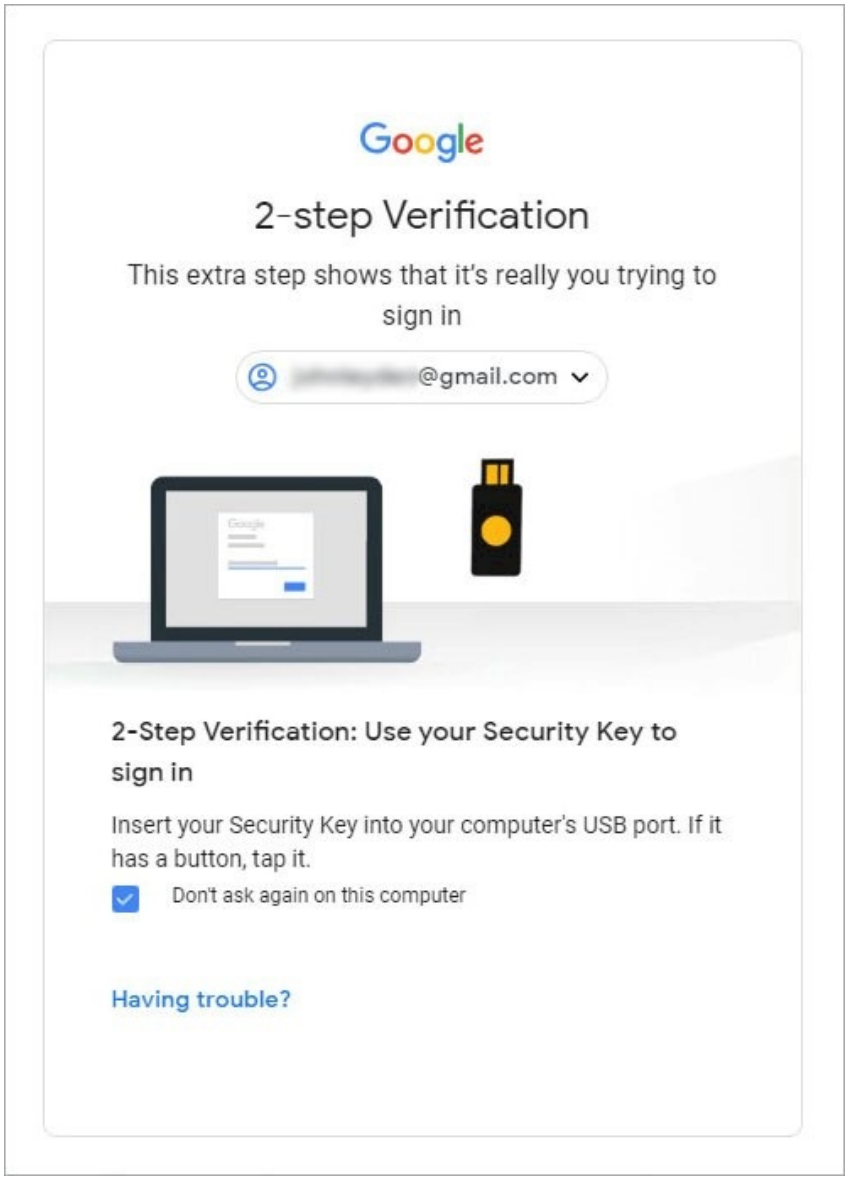
If you're unfortunate enough to somehow lose both your hardware keys, then you'll be locked out of your account. That's why it's a

good idea to a set of emergency access backup codes, which you're able to either store digitally or print – either way, keep them in a safe place.

Backup codes aren't an option for Google Advanced Protection, which has a more stringent account recovery regime.

The enrollment process for various sites is multi-stage, but not especially difficult. In the case of Google, once you jump through a few hoops (as explained in some depth in a blog post by Troy Hunt), you'll be able to login with security keys as default.

Google's multi-stage process is quite well designed, and this might be partly because its web services align naturally with its Chrome browser.

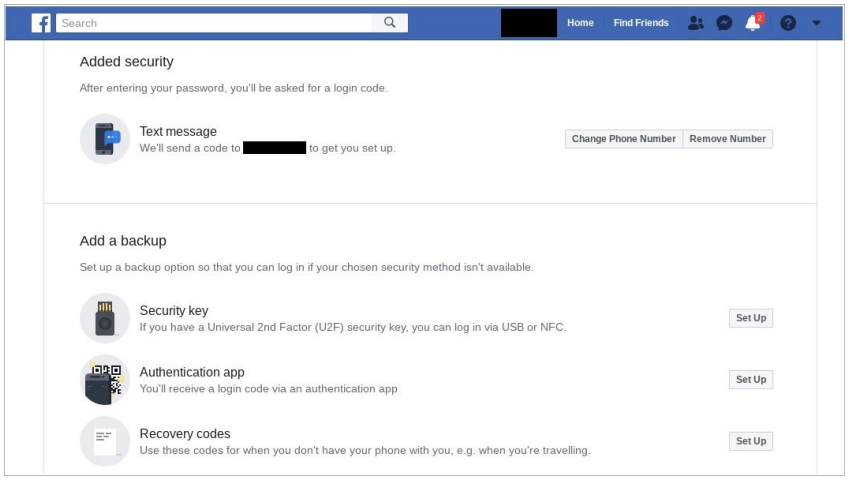


Gmail login with hardware security key enabled

In the case of Facebook, by contrast, hardware security keys are only supported as backup. Users cannot establish the security key

as the default option, even after you've enrolled a device.

We found that if you attempted to remove verification via an authenticator app, or dissociate an account from a mobile phone number, then the system would disable 2FA as a whole and you'd be back to square one.



Adding a security key to Facebook

Facebook explains that this is a deliberate design choice, prompted by what it describes as a lack of support for U2F within some browsers and by some (unnamed) mobile devices.

"Security keys for Facebook logins currently only work with certain web browsers and mobile devices, so we'll ask you to also register an additional login approval method, such as your mobile phone or Code Generator," the company said.

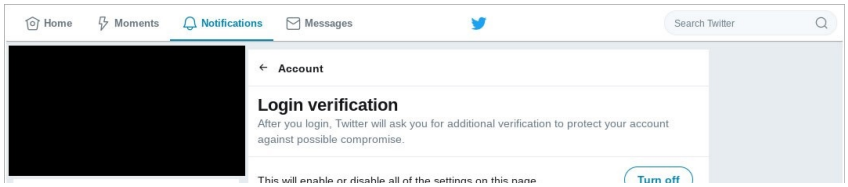
U2F vendor Nitrokey has acknowledged this browser compatibility problem in its setup documentation.

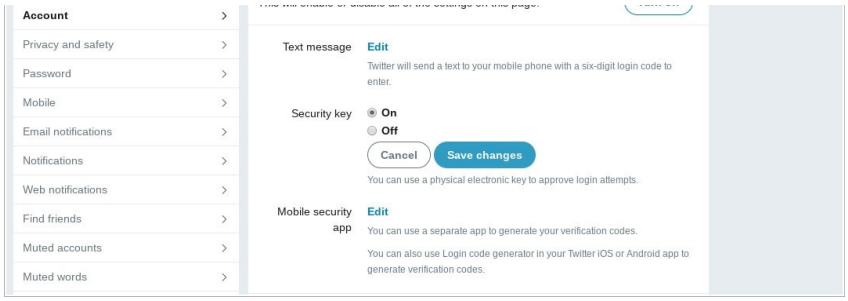
Twitter, which introduced U2F compatibility last June, doesn't let you select hardware-based security keys as the default authentication option, either.

If you disable both the mobile security app and Time-based One-time Password (TOTP) options, then you disable login verification. Establishing hardware security keys as the default option isn't possible, according to our tests.

Twitter itself confirms this, again telling users they need to have a phone number associated with your account for 'account recovery'.

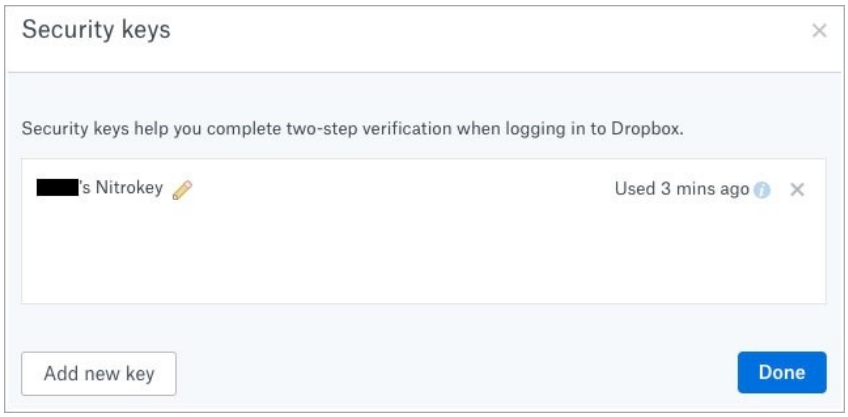
Keys alone aren't an option.





Twitter account with hardware security key authentication enabled

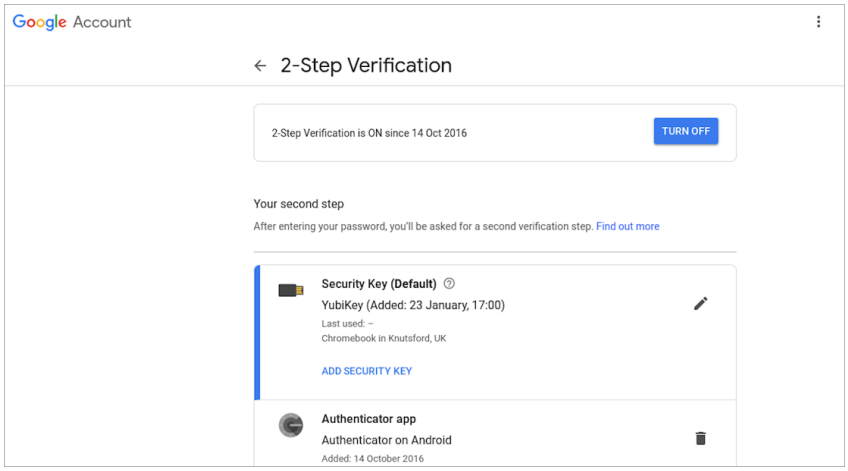
It's the same story with Dropbox. You have to have an alternate second factor system set up first before adding a hardware key as an additional authentication option. Even when you add a hardware security key, your U2F device can only be set up as a backup and not enforced as the default option.



Dropbox security key added

In the case of Gmail, our tests found that if you've only enrolled with one U2F hardware key, and that hardware wasn't present on a system, the process would fall back to accepting codes from an app.

This happens even when using a PC that hadn't been previously used to log in.



YubiKey selected as the default option on a Gmail account, but

other options can't be disallowed

The above U2F fallback mechanisms partially frustrate the purpose of using stronger hardware-based authentication. We say partially because there are still some ancillary benefits.

If you associate a hardware key with an online account, then you avoid the hassle of having to manually enter an authentication code yourself, while the hardware token provides cryptographic proof to a web service that it's in your machine.

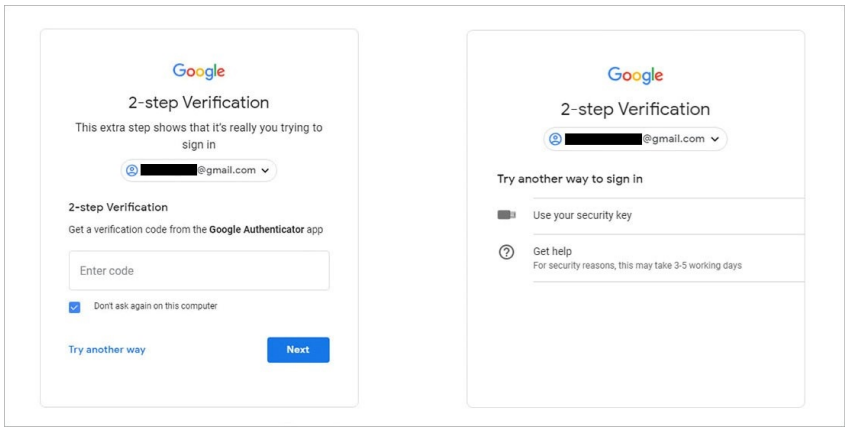
You'd simply tap a small hardware device that goes in the USB drive of your computer – less hassle than using a code generated via an app or (yet more trouble) an SMS message.

This falls short of ensuring your login is immune to phishing because of backward support for less sophisticated authentication schemes, as with Facebook and Twitter.

Google Advanced Protection, however, goes the extra mile to lock down accounts. Once an account is enrolled, using a hardware security key is mandated, as our tests confirmed.

This approach defends against man-in-the middle phishing attacks designed to capture both login details and authentication codes, Google explains.

Additional security measures in Advanced Protection mean only Google and select third-party apps retain the ability to access an enrolled user's emails and Drive files – an inconvenience for some, if not many.



Google's Advanced Protection does not offer a fallback to weaker SMS authentication

Two-step

In conclusion, we found that multi-factor authentication (2FA, but more accurately described) through a mobile app is much easier to set up, and more widely supported than hardware token-based

U2F.

Consumer-focused web-services – with the important exception of Google's Advanced Protection program – only support hardware token-based authentication as a backup, limiting the utility of the technology as things stand.

This assessment isn't far out of line with what other experts have found.

"Password and soft token is probably the best balance of security, usability and cost we have going for us today," Hunt notes in his blog post on U2F and Google Advanced Protection.

While Google's Advanced Protection scheme works, it isn't really ready for mainstream use. This is disappointing given U2F technology is needed, especially at a time when attacks against 2FA are growing in sophistication.

Hacker Luke Berner, for example, recently demonstrated how he was able to abuse app-based 2FA to maintain persistence even after a password change.

Google, Microsoft, and Instagram accounts were all potentially vulnerable, Berner discovered.

Back to the U2Future

Suppliers of U2F-compatible tokens admit that the utility of their technology is limited by partial or yet-to-arrive support by websites.

Despite this, they are still hopeful that change is in the air.

"U2F support is very disappointing," Nicolas Stalder of SoloKeys told The Daily Swig. "The hope is that with FIDO2… approaching a standard, this will improve."

U2F over NFC is even less supported than U2F on desktop or laptop, Stalder observed.

"U2F should be dead simple, for some reason it is shrouded in

mystery, or at least obscurity to the wider audience," he added.

Usability studies sponsored by Yubico provide further evidence that consumers find enrolling a U2F key and associating it with their account problematic.

Different web services also have broadly similar, but inconsistent enrollment schemes, tests by The Daily Swig found.

This may be a reason for the mediocre usability of what is otherwise a promising and useful technology, one that fulfills a growing need to fend off phishing – a form of attack that is growing in impact, according to a Google-sponsored study and other sources.

Stalder offered The Daily Swig a prescription to ease these woes.

U2F would be so easy if sites supported things properly:

• Have a visible invitation to register keys (instead of hiding behind multiple submenus)
• Suggest that users register at least two, or better, three keys
• Offer 'one-time use codes' as a backup, advising users to print them out and store them in a safe place
• If a [hardware security] key gets lost, a thief is probably not going to be able to use it immediately (either does not know the username, or has to crack password), so upon noticing this the user just logs in with a backup key and removes the stolen key from the whitelist/registered list

Part of the problem is that sites don't want to handle out-of-band verification of ownership to re-enable login of users in cases where problems occur, according to Stalder.

"I think the reason why sites often don't allow 'U2F only' is that it's actually secure – if a user loses [all] the key[s], they won't get in! Or as some say, if they still can get in, it was all a 'security theatre'," he said

We asked the FIDO Alliance, as backers of the technology, to comment on our findings.

Chief marketing officer Andrew Shikiar declined to comment on specific implementations of U2F, although he did offer an explanation of how the FIDO2 specification will move authentication technology forward, ultimately leading onto more widespread adoption of stronger login security technology.

"FIDO2 includes the W3C Web Authentication API (Webauthn) and CTAP (Client-to-Authenticator Protocols) from the FIDO Alliance,"

Shikiar explained.

“The specs enable FIDO Authentication support to be built directly into browsers and platforms, and will greatly expand the addressable market for FIDO as these browsers and operating systems push out updates to billions of devices.”

In developing FIDO2, the FIDO Alliance partnered with the World Wide Web Consortium on how to standardize FIDO across the web. The collaboration is designed to expand the addressable user base, as well as the available authentication use cases.

“The specs were announced only nine months ago, and FIDO2 technologies are already built into the latest versions of Windows 10, Google Play Services on Android, and the Chrome, Firefox, and Edge web browsers,” said Shikiar.

“WebKit, the technology behind Apple’s Safari web browser, is also previewing support for FIDO2. Native support across browsers and platforms eliminates a lot of the complexity of building strong authentication into apps, so we do believe it will lead to broad FIDO adoption.”

Greater usability for U2F is certainly desirable, but even that may not be enough to ensure widespread uptake –early last year, seven years after Google introduced less stringent 2FA, a Google engineer admitted that take-up was still under 10%.