Using 1Password for Two-Factor Authentication (2FA)

First published: April 2021.

Introduction

1Password is the password management software that I have been using for some time now to help me manage passwords for the many online accounts that I use. 1Password makes the creation, storage and use of complicated and lengthy “strong” passwords a straightforward and efficient process.

1Password

Although the use of a strong password can protect an online account much better than a weak or reused password, given the frequent reports of leaking user account data by various websites, the use of strong passwords alone probably isn’t “good enough” security any longer.

Two-factor authentication (hereinafter referred to as “2FA”) is a method of logging into a website account with a greater degree of security than merely using your username and password. When using your password as the first factor for authentication of your login, the second factor can be provided by one of several options: a text message (SMS), an authenticator application, a Bluetooth/USB/NFC-based hardware security key, or biometrics (such as fingerprint or FaceID recognition).

Having investigated and considered implementing 2FA for some of my online accounts, of the various second-factor options, I’ve concluded that the use of authenticator software would likely offer the best combination of convenience and security. Given the huge privacy/security sensitivity of my 1Password account, I felt that the addition of 2FA security to that account should be prioritized.

I’ve also concluded that I ought to add 2FA security to at least some of my other online accounts. My ProtonMail encrypted email account heads that list, since it seems imprudent to me to enable and use encrypted email services and yet not bother to secure the account for that service to the fullest extent as is practical.

Setting up 2FA for 1Password via Authy - Round #1

To use 2FA as noted above, my plan was to use another 2FA service to provide 2FA security for my 1Password account and then have 1Password provide 2FA services to my other online accounts. Thus, a single application would be efficiently handling the secure login functions of pretty much all of my on-line accounts, enabling and implementing added 2FA security for those accounts for which it is supported.

Indeed, the 1Password support website notes that the account of the authenticator application, 1Password, needs itself to be secured via 2FA:

> Although 1Password can be used to store one-time passwords for other services where you use two-factor authentication, **it's important to use a different authenticator app to store the authentication codes for your 1Password account.** Storing them in 1Password would be like putting the key to a safe inside the safe itself.
>
> (from https://support.1password.com/two-factor-authentication/)
> (bold emphasis added by me)

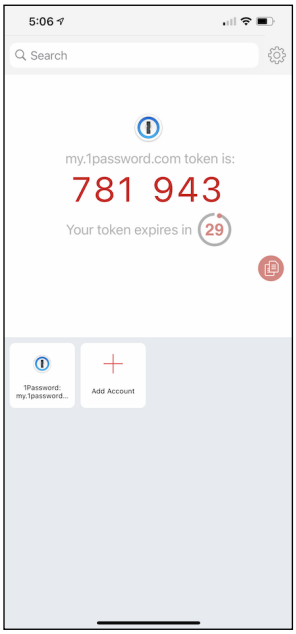
So, you need a different 2FA software utility to provide 2FA login security for your own 1Password account. Based on the several reviews that I have read, the Authy application seems well-suited for this purpose. Authy is free, well-respected and can be installed on mobile devices and computers.

Thus, my first action was to enable 2FA for my 1Password account via Authy. I installed Authy on my iPhone and performed the basic account setup for it: entered my phone number, entered a password for secure online backup of my Authy account, and verified my phone number via a text (SMS) message from the Authy server. Now Authy was ready to receive a new 2FA "account token" from my 1Password account.

Authy

On my computer, I logged in to my 1Password account via its website and started the process of adding 2FA to 1Password, following the 1Password directions for enabling 2FA for the account. A QR code was shown with the instruction to scan it with my 2FA application, i.e. Authy.

Switching to my iPhone, I started the process of adding a new account to the Authy app. Authy requested access to the iPhone camera, instructing me to use the camera to capture the QR code that had been generated by the 1Password website. Using the iPhone, I scanned the QR code (on the computer screen) that was presented to me on the 1Password 2FA setup page.



Having captured the data, the Authy app recognized that I was setting up 2FA for a 1Password account, created an icon for 1Password on the app's main screen, and then displayed a 6-digit authentication code. Back on the computer, I entered the code on the 1Password website, completing the process of turning on 2FA for my 1Password account.

To test that the newly set 2FA was working, I logged out of the 1Password account and then started to log back in. Sure enough, in addition to my login name and password, the 1Password website login process asked me to enter my 2FA code. Picking up my iPhone, I touched the 1Password icon in Authy and a 6-digit code was displayed with a 30-second count-down timer. Back on the computer, I entered the 6-digit code on the 1Password login page (with 5 seconds to spare!) and completed my first 2FA login to my account on the 1Password website.

Great! I've added more security to my 1Password account. It felt gratifying, but then I started to over-think things!

Second thoughts…

I had read on some other websites that supported 2FA that, during the setup for 2FA, the website would display some "recovery keys/codes." These are unique passcodes that are provided for the potential situation in which your software or hardware 2FA utility cannot provide a 2FA code for you to use to log into the site. For example, here is what ProtonMail notes about enabling 2FA and using recovery codes:

> ProtonMail will also provide you with several one-time use recovery codes. Please save these codes in a secure place and do NOT lose them. **If you ever misplace or lose your authentication device (mobile phone, etc.), these codes will be the only way to log in to your account.** If you ever lose your second-factor device, you can enter these codes instead of the six-digit authenticator code. Note, each code can only be used once, so please save all the codes.
>
> (from https://protonmail.com/support/knowledge-base/two-factor-authentication/)
> (bold emphasis added by me)

Thus, recovery codes are an "emergency" entry to the account on a 2FA-enabled website than can be used if you can't provide a 2FA code during the login process on the website.

The problem that occurred to me was that, during the process of enabling 2FA for my 1Password account, I was not provided any recovery keys or codes by the 1Password website. With no recovery capability, I was concerned that I could be locked out or my 1Password account if I had a 2FA "glitch" of some kind.
So, under an over-abundance of caution, I logged back into my 1Password account and turned off the 2FA option that I had just enabled an hour earlier!

Setting up 2FA for 1Password via Authy - Round #2

The next morning I started to further investigate this situation. I found it hard to believe that 1Password's security experts had overlooked the potential need for recovery keys. Indeed, my perusal of the 1Password support pages was leading me to believe that I already had the credentials to access my 1Password account even if I couldn't provide a proper 2FA token during login.

To confirm this, I emailed 1Password support about my concerns. I received a quick response and they verified that one can use the 1Password application to disable a 2FA login requirement that had been set. So my "over-thinking" was indeed just that.

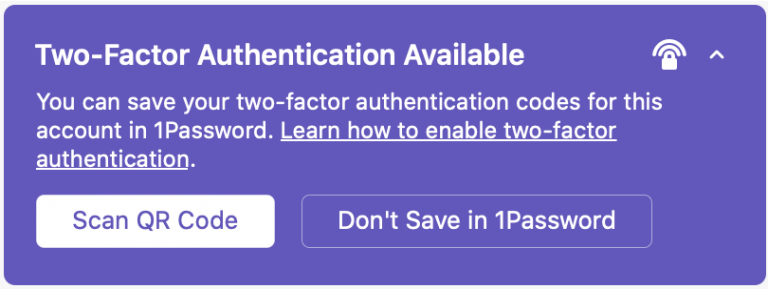
Now that I was reassured, I reenabled 2FA for my 1Password account, again registering the account info in Authy. Testing the newly enabled 1Password 2FA login was successful.

Setting up 2FA for other accounts via 1Password

OK, now the real fun begins: using 1Password to set up another account to utilize 2FA login security, thereby enabling 1Password to provide all the required login/authentication info for that account, i.e. my user name, password and 2FA token.

"Use 1Password as an authenticator for sites with two-factor authentication" is the 1Password web page that provides instructions on how to do this. Several options are available; I chose to follow the directions "To save your QR code in the apps." Thus, I would be using the 1Password application on my Mac to set up and save the 2FA login functionality for another website.

Following is what I experienced as I enabled 2FA for my ProtonMail account. (This differs a little bit from the process described in the instructions on the 1Password support web page.)



I opened up the 1Password application on my iMac and found the entry for my ProtonMail account. At the top of that window a purple box noted "Two-Factor Authentication Available." Clicking on the disclosure arrow in that box revealed the link "Learn how to enable two-factor authentication." Clicking on that link opened Safari and loaded the ProtonMail support web page about how to set up 2FA for ProtonMail. (I was impressed that 1Password

conveniently provided that direct link.) I arranged the Safari and 1Password windows so that I could see both on my iMac's display at the same time.

The ProtonMail page directed me to log into my ProtonMail account, go to the security tab within the settings section for my account and click on the "enable two-factor authentication" button. I did this and then a QR code appeared onscreen with the instruction to scan it with my two factor authentication device.

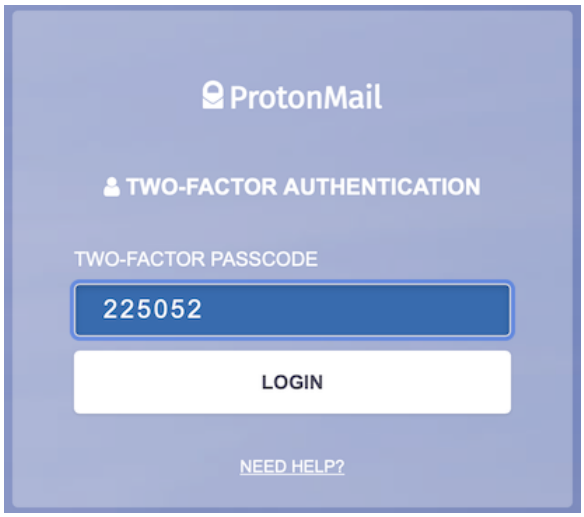
Next I went back to the 1Password application and clicked on the "Scan QR Code" button in the purple box of my ProtonMail entry. This brought up a draggable window with the instruction to move the scanner outline in the window over the QR code to be scanned. I did so and 1Password recognized the QR code and imported the info.

Then, back on the ProtonMail web page that showed the QR code, I clicked on the "Next" button and was asked to reenter my ProtonMail account password and to enter "the two-factor passcode which you will see in the authenticator application you are using." Indeed, back in the 1Password application, my ProtonMail entry was now showing a 6-digit 2FA passcode with a 30 second count-down timer. Back in the ProtonMail web page, I entered my password and the 2FA passcode and they were accepted.

Next, the ProtonMail web page showed a list of one-time use recovery codes, to be used "if you ever misplace or lose your authentication device" in order to login to the ProtonMail account. (These were the type of codes that I had expected to see when I set up 2FA via Authy for my 1Password account login.) I downloaded the codes and securely saved them in my Mac user account's keychain should I ever need them.

OK, now to test my new 2FA-secured login for ProtonMail! I logged out of the ProtonMail website and, on the login page for ProtonMail, clicked on the login pop-up generated by 1Password to auto-enter my ProtonMail account name and password. 1Password filled in the info and a small pop-up notification window produced by 1Password noted "One-Time Password copied to the clipboard." This confirmed that a 2FA code generated by 1Password was now on my Mac's clipboard.

With the ProtonMail username and password fields filled in, I clicked on the “Login” button and another login box was now shown, asking for the two-factor passcode. The 2FA passcode code field was already auto-filled by 1Password. Clicking on the Login button now completed the 2FA login process for my ProtonMail account. Another small pop-up notification window (produced by 1Password) soon followed, stating that the Mac’s clipboard contents were restored. Nice!



I’ve subsequently added 2FA to another online account of mine. For that account, only one recovery code was provided after I had enabled 2FA.

Summary

Adding and using 2FA login security for a website account is an easily-accomplished and satisfying process when done via 1Password. Once enabled, 1Password handles the 2FA login process for a website both seamlessly and elegantly. It’s very gratifying to have one utility completely manage secure logins the way 1Password does.

I strongly urge you to enable 2FA to enhance your login security of your important website accounts and I heartily recommend 1Password for your use as a password/2FA utility.