DAY 7

Lock Down Your Most Important Accounts

By setting up two-factor authentication, all your important accounts get locked behind two doors, requiring two sets of keys: a password and a special one-time use code. Once this is set up, it's much more difficult for nefarious people to get into the account because even if they learn a password, they can't pretend to be you unless they have physical access to your phone.

Setting up two-factor authentication isn't technical, but it can take a lot of time to enable if you have a lot of accounts. Give yourself 30 minutes to an hour to complete this task.

Two-factor authentication comes in two primary forms:

- Text message verification: A numerical code is sent to you as a text message.
- Application authentication: An authentication app constantly generates new codes valid for 30 seconds each.

Security experts recommend using an authenticator app over text messages wherever possible because it's easier to intercept a text message than to spoof the numbers generated by an app. But not all accounts support authentication apps, so chances are you will use both text messages and an app during this process. Yes, it gets a bit confusing, but the security benefits are really worth it.

Setting up two-factor authentication is a two-step process. First, you need to choose an authentication app. Second, you need to enable two-factor authentication for each individual online account.

Step 1 of 2: Choose an Authentication App:

For an authentication app, Authy is the easiest to use. It's free and available on Android, iPhone, Chrome, Windows and Mac(though most people will need only the smartphone app). You can lock Authy behind a fingerprint scan or a PIN, and you can store a backup of your security key online, so if you lose a phone you're not totally locked out from all your accounts. Once you download the app on your smartphone, set-up is easy:

1. Open the app. Enter your phone number and email address.
2. Authy will send you a PIN; enter it in the app.
3. If you want to sync Authy to a computer, first open the Authy app on your phone, then tap Accounts.
4. Tap "Authenticator Backups" to enable it. Choose a password. Now, if you lose your phone, you will still be able to access your Authy account.

Step 2 of 2: Enable Two-Factor Authentication

With the authentication app taken care of, it's time to enable two-factor authentication on each account. The most important accounts to secure are the ones that include personal information. So, email, bank accounts, your password manager and social networks are all must-do. For a list of every single place you can enable two-factor authentication and how to do it, check out Authy's guides or twofactorauth.org.

To give you an idea of how this process works, here's how to enable it on Facebook, which happens to be one of the more complicated ones:

1. Log into Facebook, click the drop-down menu on the right side and select "Settings."
2. Click the "Security" tab.
3. Click the "Edit" box next to "Login Approvals."

4. Click “Enable” next to “Two-Factor Authentication,” click enable again when the prompt pops up, then click “Close.”

5. Scroll down to the “Code Generator” section and click the link for “Third party app.”

6. A QR code will pop up on the screen. Open the Authy app on your phone, then click “Add Account” and “Scan QR Code.” Use your phone’s camera to scan the QR code from Facebook. Follow the on-screen prompts to finish the process.

Now, the next time you log into Facebook, you’ll log in as usual, using your username and password. After you log in, Facebook will ask for a code. Open the Authy app, tap Facebook and enter the six-digit code from the app into the field on Facebook.

The first few times you log into an account using two-factor authentication, it feels cumbersome and annoying. As you get used to the process, it quickly becomes second nature.

So set up two-factor authentication wherever you need to. Be patient. It will take awhile to get through your major accounts, but once it’s done you’re extra protected forever.

Have you completed this?
Mark this task complete

Why Am I Doing This?

When you set up a password manager earlier this week, you took the first step to cleaning out overused, simple passwords. Two-factor authentication is the next step to locking digital security down tight. Because getting into your important

accounts now requires two factors, a password and an authentication token, it’s much more difficult for any bad people to get in.

Two-factor authentication does create some problems. For one, when it adds an extra step for a hacker, it also adds a step for you. This means logging into accounts will take longer. If you lose your phone and you didn’t save the backup codes properly, getting back into an account is more complicated than clicking the “I forgot my password” link on a login page. In some cases, you’ll even need to call a company directly to regain access to the account. So set up two-factor authentication and then don’t lose the backup codes you get. (Put them in the same safe place your put your recovery key from Day 4.)