DAY 1

Set Up a Password Manager

Installing and setting up a password manager is a simple way to keep online accounts secure. A password manager is software that generates strong passwords and then securely stores them for all the websites you use. (Think complex passwords such as 4GFjsX4*34@!, as opposed to Password1234). With a password manager, you will never need to reuse the same password, and you will be notified to change a password if a website gets hacked.

Best of all? You'll never need to remember any of them.

The initial set-up process can take about 10 minutes, but you will get all your passwords changed gradually as you log into your accounts. It sounds tedious, but it's not, and it is worth it. This is the one thing you can do to protect your online security with the biggest impact. Bonus: Once you're done, a password manager makes logging into all your accounts faster and easier.

Step 1 of 4: Choose a password manager.

You have dozens of password managers to choose from, but Wirecutter recommends either:

- LastPass: Pros: Free; Cons: Has a higher learning curve, and it is not as good at telling you how to improve the security of your accounts, including notifying you when a site uses two-factor authentication (which we'll get to at the end of the week).

- 1Password: Pros: Intuitive to use, has security tutorials that are helpful to new users; Cons: Costs $36 a year.

Both password managers work on smartphones and computers in all major browsers.

If you're well-versed with computers and don't mind futzing with settings, then LastPass is an excellent free option. If you don't mind paying for the

convenience of better software that is easier to use, choose 1Password.

Step 2 of 4: Create an account with a strong master password.

Once you choose a password manager, it's time to create an account. Click these links to create an account at 1Password or LastPass.

When you create an account, you start by choosing a "master password." *This is the one password you need to remember to unlock the rest of your data*. The password should be memorable, but hard to guess, which rules out passwords that include birthdays, pet names or hometowns. Instead, the National Institute of Standards and Technology recommends using a series of randomized words, like "judge carver olympian globulin." 1Password has an online password generator for creating these types of memorable passwords.

After creating an account, 1Password displays a security key and a link to the Emergency Kit, which includes a QR code you will need in the next step. If you're using LastPass, you need only the master password.

Step 3 of 4: Download and install the applications and browser extensions.

If you chose to go with 1Password, here is how to set it up:

1. On your desktop, download 1Password for Windows or Macand sign into your account. This desktop application is where you will run security checks and edit passwords.

2. Download the 1Password browser extension for your browser (where you go to surf the web, such as Chrome, Firefox, Internet Explorer) and log in. If you use multiple browsers, you will need to install the extension for each one. This will autofill passwords when you log in and generate new passwords when you create accounts. This is how you will use 1Password most of the time.

3. On your phone, download the 1Password iPhone or Androidapp. On an iPhone, hop into the settings and allow Safari to access the password manager. It will work automatically on most versions of Android, though you may need to enable autofill in the app. When you launch the app for the first time, it will ask you to use the camera to scan the code from the Emergency Kit.

LastPass is a bit simpler:

1. On your desktop, download the LastPass browser extensionfor the browser you use (where you go to surf the web, such as Chrome, Firefox, Internet Explorer) and log in.

2. On your phone, download the iPhone or Android app and log in. Follow these instructions to access the passwords from the phone's browser.

Step 4 of 4: Start browsing and change passwords as you go.

The rest is easy: Browse the web and log into websites as you normally do. As you go, 1Password and LastPass will keep track of the passwords you use and prompt you to change weak or duplicated passwords. Follow the prompts, and soon most of your passwords will be updated and stored in the manager. When you create new accounts, the password manager will offer to generate a password for you.

Have you completed this?
Mark this task complete

Why Am I Doing This?

If you complete only one challenge for the week, this is the most important one. Setting up a password manager secures your digital accounts in ways that almost

nothing else can.

Nobody wants to (or can) remember dozens of complicated passwords, so most of us tend to reuse the same password across multiple websites. That means if one site gets hacked, your password for multiple sites can leak, which then gives a nefarious person access to your entire digital life, including bank accounts, emails, social media and more. With a password manager, all of your account passwords are unique, and you're notified if a site gets hacked so you can change the password on that account.

A good password manager syncs passwords between a computer and a smartphone, making it easy to access accounts no matter where you are. The best password managers aren't intrusive or annoying, and because they autofill passwords (after you unlock the manager with a fingerprint scan or a master password), they eventually make it easier to log into sites. They can also safely store other secure data you might need to gain access to on the go, like passport numbers, credit card numbers, bank account information and more.