DAY 4

Protect Your Laptop

You've lost your laptop. Great. Now you have to spend $1,000 on a new one, but worse, your personal information is accessible to whomever happens to find it. To prevent this nightmare, take a few minutes to encrypt your hard drive right now. It sounds terribly complicated, like something a spy would do, but it's really quite simple.

Once the encryption is set up, nobody can access your laptop without the password and nothing about your day-to-day use of your laptop will change.

If you have a Windows laptop:

Windows laptops have a few options for encryption, but most versions of Windows include free software to encrypt your storage drive. Here's how to check if you can do it:

1. Click the Start Menu and select "Settings."
2. Click on "System."
3. Click on "Update & Security."
4. Look for the "Device Encryption" tab and click on it.
5. If the laptop supports encryption through a Microsoft account, or you have Windows 10 Professional, Student or Enterprise, you'll see an option to turn on BitLocker. When you do so, you'll get a recovery key. Store this code in a safe place (and not on your computer).

Unfortunately, if you have a version of Windows 10 Home that doesn't support the Microsoft account method of encryption above, the best free third-party option is VeraCrypt, but VeraCrypt can be difficult to use. If it's your only option, it's worth looking into, but it's a headache to get it set up.

If you have a MacBook:

Every Mac includes free encryption software:

1. Click the Apple logo in the top left of your screen and then click “System Preferences.”
2. Click “Security & Privacy.”
3. Select the “FileVault” tab.
4. Click “Turn on FileVault.” You'll be prompted to choose to unlock your account with iCloud or with a recovery key. A recovery key is more secure, but iCloud ensures you can't lose it. If you choose the recovery key, store the key the software shows you in a safe place (and not on your computer). If you do not get a prompt at all, your computer may have been set up by an institution like a company or school.

With both Windows and Mac, it’s important that you DO NOT lose the password or the key. If you set up a password manager earlier this week, store the key in the password manager. Otherwise, print it out and lock it up somewhere safe at home. Encrypting a laptop keeps a bad actor out, but you can also lock yourself out.

Have you completed this?
Mark this task complete

Bonus

Encrypting a lost or stolen laptop so no one can get your data is great, but what if you could find your lost laptop? Both Mac and Windows have free software to track a lost laptop.

On a Windows computer, you can enable Find My Device on the laptop and configure it with a Microsoft account:

1. Sign in to your Microsoft account. (If you don't have a Microsoft account, it's worth creating one for this feature.)
2. Click the Start Menu and click on "Settings."
3. Click "Update & Security."
4. Select "Find my device" and turn it on.

On Mac you'll use Find My Mac:

1. Click the Apple menu.
2. Click "System Preferences."
3. Click "iCloud." You may need to sign into your Apple account if you haven't already. (If you don't have an Apple ID, it's worth creating one for this feature.)
4. Check the box next to "Find My Mac."

Once you turn these services on, you will get an alert when your laptop connects to a Wi-Fi network. You can then see approximately where the laptop is (using the Wi-Fi network's location, not GPS) and, if you don't think you can get it back, remotely wipe the storage drive. .

Why Am I Doing This?

Even if you don't store anything important on your laptop, picture a stranger rummaging through your browser history, your notes or your to-do lists. It's terrifying, right? If you have a login password, a dedicated person can still access a good majority of the files on your laptop. Encryption takes all the data on your laptop, then jumbles it up with a mathematical process that can be unjumbled

only by a special key that only you have. Your day-to-day use of your computer won’t be affected at all. Just don’t lose the recovery key. Without this key, you may lose access to your laptop entirely.

We can’t say this enough: Make sure you save that key in a safe place — somewhere not on your laptop — in case anything goes wrong.