How to secure your Twitter account

Twitter just revealed that it made a monumental security blunder by exposing the passwords of users in plain text. The company says there's been no indication of a security breach tied to the log that contained those login credentials, but let's not kid ourselves. It's 2018. You need to change your password — on Twitter and with any other account where you might've repeated that password — and secure your Twitter account immediately. The full scope of what happened here isn't yet clear (or how many users were directly affected), but there's no downside to taking immediate action.

Change your Twitter password

On the web: Go to Twitter.com, **click your profile image** in the upper right, choose **Settings and privacy** and then when the next page loads, select **Password** in the list running down the left side. Twitter will ask for your existing password and then your new one. Use a strong, unique password. And never repeat them between multiple services, apps, and online accounts.

From the mobile app: Tap your profile photo at the upper left and choose **Settings and privacy.** Then **Account**, followed by **Change password**. Again, ensure that your new password is used exclusively for your Twitter account.

Illustration by Alex Castro / The Verge

Enable login verification (two-factor

authentication)

A password alone isn’t enough of a wall between you and people with tech smarts and bad intentions. Aside from changing your Twitter password, locking down your account to the fullest extent possible requires enabling the company’s login verification feature.

This two-factor authentication process can either send a code to your mobile phone number whenever a new device attempts signing into your account with the correct password. Or you can generate your own code within a third-party app made for that specific purpose – like Authy. The latter approach is safer since SMS itself can be compromised.

Turning on login verification from the web:

- Click your **profile** icon, then click **Settings and privacy**.
- Choose **Account** and then **Set up login verification**. On mobile, there’s an extra step here where you’ll have to tap on the **Security** section inside Settings and privacy.
- Read the overview instructions, then click **Start**.
- Enter your password and click **Verify**.
- Click **Send code** to add your phone number if that’s the verification method you want.
- Enter the verification code sent to your phone, hit **Submit**, and login verification will then be enabled.

Using a third-party app to generate secure login codes:

- Click or tap your **profile** icon, then click **Settings and privacy**.
- Choose the **Account** tab.
- Under **Security** and next to **Login verification**, click the **Review your login verification methods** button to get

started.
- Enter your password and click **Confirm**.
- Look for **Mobile security app** and you should see a **Set up** next to it.
- Read the instructions and then hit **Start**.
- **Verify** your password if asked to.
- You'll then be shown a **QR code that you'll scan with the app that will generate your Twitter login code. Once that's done, you should see the app automatically generate a six-digit code.** The code changes every 30 seconds.
- Enter the currently active code in the **Security code** text field and click **Done**.

Which apps should I use to generate login codes?

Some password managers, including 1Password, offer built-in code generators for two-factor authentication. Other apps meant specifically for two-factor codes include:

Authy (/ Android)

Google Authenticator (/ Android)

Microsoft Authenticator (/ Android)

LastPass Authenticator (/ Android)

https://www.theverge.com/2018/5/3/17316846/how-to-secure-twitter-change-password-two-factor-authentication