

Account Security on Twitter

Login and security

We encourage you to confirm that the [email address](#) and [phone number](#) associated with your account are correct. If not, update please them.

Use a strong password

We encourage you to [use a strong password](#) that you do not reuse on other websites. You should also create an equally strong and unique password for the email address associated with your Twitter account.

Two-factor authentication

We recommend you enable [Two-factor authentication](#) (2FA). 2FA provides an additional layer of security to protect accounts from unauthorized logins.

Password reset

We encourage you to enable [password reset protection](#) for your accounts. This is a setting that helps prevent unauthorized password changes by requiring an account to confirm its email address or phone number to initiate a password reset.

Connected apps

As a best practice, we encourage you to [check your connected apps](#) and revoke access from any apps that you no longer need or don't recognize.

Tip

Be cautious of suspicious links (including those received in emails, text messages or DMs), and always make sure you're on [twitter.com](#) or in our app before you enter your login information.

Two-factor authentication

Two-factor authentication >

Protect your account from unauthorized access by requiring a second authentication method in addition to your Twitter password. You can choose text message, authentication app, or security key. [Learn more](#)

Additional password protection

Password reset protect

For added protection, you'll need to confirm your email address or phone number to reset your Twitter password.

Help Center

To learn more about security best practices check out our [Help Center](#).