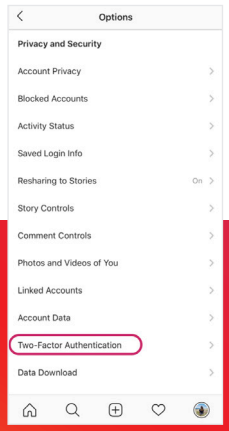
INSTAGRAM ACCOUNT MANAGEMENT BEST PRACTICES

Social media managers often reach out to us asking for guidance on how to manage their Instagram accounts. Instagram partnered with the Facebook Security teams to put together this set of best practices with clear, easy-to-follow instructions. While we cannot guarantee bad actors will not attempt to access your account, we highly recommend putting these practices in place to help ensure that your account is secure.

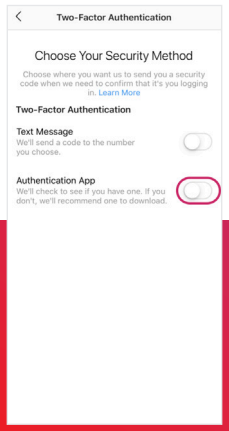
1. ENSURE TWO-FACTOR AUTHENTICATION IS IN PLACE.

Third-party authentication is a process to better protect your account by adding a third-party app to verify your login credentials before logging into your accounts. These third-party authentication apps make it significantly harder for bad actors to hack accounts and make it easier for you and your team to keep your account safe. You can also use SMS authentication, but note that third-party authentication reduces friction in sharing an account with multiple team members. Follow the steps below to set up two-factor authentication. There are multiple apps that you can use, including Duo Mobile or Google Authenticator.

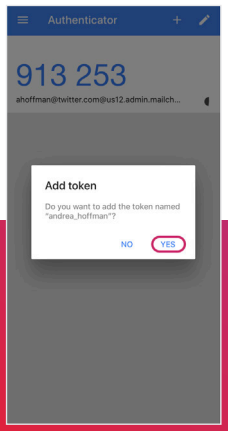
Set up third party authentication for a single device



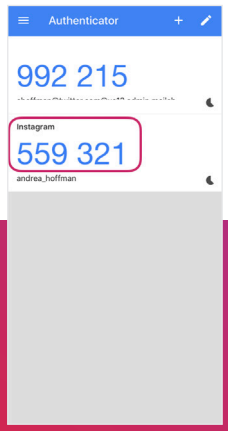
STEP 1
Go to Settings and tap on Two-Factor Authentication.



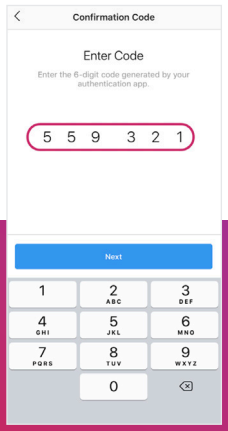
STEP 2
Toggle the Authentication App switch and tap next.



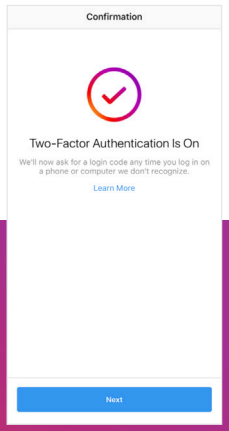
STEP 3
If you have installed Duo Mobile or Google Authenticator, tap on Yes to add token. You may need to go back to the previous page and tap "Set Up Manually" if this message does not appear.



STEP 4
A code for Instagram will be sent to your authenticator app. If you have selected "Set Up Manually," tap the "+" in your authenticator app and add your key. Copy the 6-digit code provided and go back to your Instagram app.

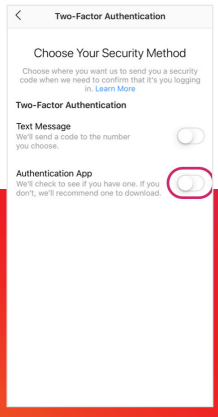


STEP 5
Enter the code from your authenticator app and tap Next to verify.

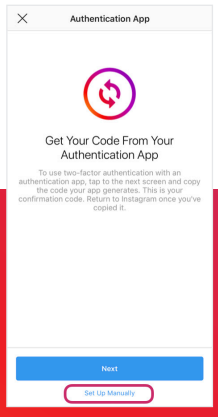


STEP 6
If you see this screen, then you've set up your third-party authenticator app correctly! Tap on Next to complete.

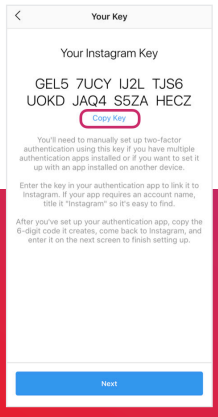
Set up third party authentication for multiple devices



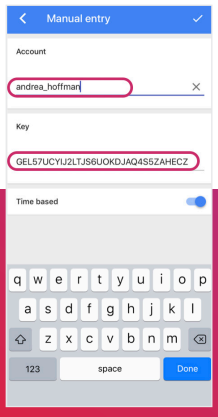
STEP 1
Go to Settings and tap on Two-Factor Authentication.



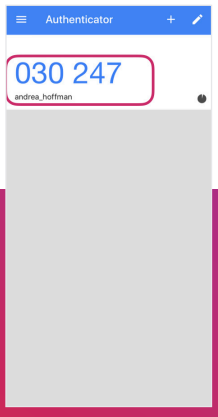
STEP 2
Toggle the Authentication App switch and tap on Set Up Manually to continue.



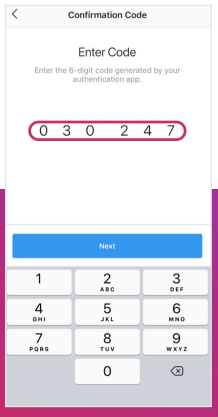
STEP 3
Copy the key provided and save it. Send your Instagram key to your other devices.



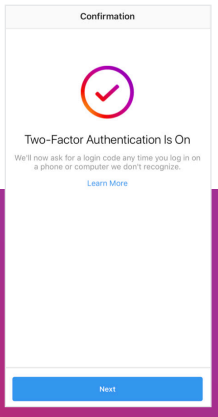
STEP 4
Add the key to your authenticator app by tapping on the "+" button and/or selecting "manual entry." Enter your Instagram account name into your authenticator app, paste the Instagram generated key and tap Done.



STEP 5
Your authenticator app will generate a new code for you. Copy this code and go back to your Instagram app.



STEP 6
Enter the authenticator generated code into your Instagram app and tap Next.



STEP 7
Replicate this process for each device that needs access to your account, using the same Instagram key.

2. PICK A STRONG PASSWORD.

We recommend that you pick a password that is not easy for others to guess. For example, do not use your phone number, email, username or other easy-to-guess passwords such as “password 123” and “1234567.” We recommend that you create a password of at least 8 characters in length—ideally around 10 to 12. If you decide to create a shorter password, we recommend making it more complex by including special characters and variance in casing (capital letters).

3. ROTATE PASSWORDS WHEN TEAM MEMBERS LEAVE.

It can be common practice at work for multiple people on a team to have access to a shared social media account. However, if a team member leaves the team or company, remember that it is important to change the password, so that only people who should continue to log into the account have access. Limiting the number of people who have access to an account to only those who absolutely need it is an important practice for keeping an account secure.

4. NEVER SHARE YOUR LOGIN CREDENTIALS WITH A THIRD-PARTY APP OR BUSINESS.

Many social media managers work with third parties that help them to manage their Instagram accounts. However, make sure that the third-party you work with properly uses Instagram or Facebook official authentication to access your account. Any third-party that asks you for your Instagram account password is in violation of Instagram Terms of Use. While a third-party might claim to use your credentials for a service that will benefit you, the unfortunate reality is that you never know what a third-party might do with your credentials once they have access, and this puts your account security at risk.

5. DO NOT GRANT THIRD-PARTY ACCESS TO WEBSITES OR APPS THAT DON'T FOLLOW OUR COMMUNITY GUIDELINES OR TERMS OF USE.

This includes websites that sell or promise free followers or likes. These websites and apps are likely attempts to use your account in an inappropriate way. Click these links to review our community guidelines or terms of use.

6. AVOID TYING A BUSINESS ACCOUNT TO ANY PERSONAL INFORMATION.

Always register any business social media accounts to a corporate email and corporate phone number. Do not register business social media accounts to your personal email or a personal phone number. Not linking to personal accounts can protect the business account, in the event that your personal email becomes compromised.

7. LOG OUT OF INSTAGRAM ON ANY DEVICES THAT BELONG TO SOMEONE ELSE.

If you need to log into your Instagram account on a device that does not belong to you, make sure to log out from Instagram after usage. This can protect your account from other third-parties continuing to have access.

8. BE WARY OF ANY COMMUNICATION ALLEGING TO COME FROM INSTAGRAM THAT MIGHT BE A SCAM.

Know that Instagram will never call you, and that any Instagram account that direct messages you will be verified. Beyond ads, Instagram does not sell any products or services and will not make any offers to you. Instagram will never sell you verification.

WHILE FOLLOWING THESE BEST PRACTICES CAN ENSURE YOUR ACCOUNT IS SECURE, WE CANNOT GUARANTEE THAT BAD ACTORS WILL NOT ATTEMPT TO ACCESS YOUR ACCOUNT.

If your account appears to post unauthorized content, we recommend that you change your password and also revoke access to suspicious third-party apps. You can do this here.

If your account has been hacked, there are a couple of ways to regain entry.

- **Emails to help you regain access:**
  If we detect unauthorized changes have been made to your account, we will send an email to notify you of these changes. This email is sent to the original email address associated with the account—not the updated or changed email address. If you did not initiate this change, please click the link marked 'revert this change' in the email, and then change your password. We will not ask you to share your login information in this email, and we will never ask you to pay to recover your account.

- **In-app support form:**
  If someone gains access through a compromised email account, people can follow the steps detailed on Instagram's Help Center to use our in-app support form to recover their accounts.