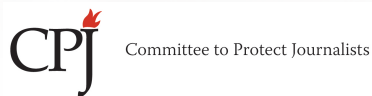


FACEBOOK SAFETY FOR

JOURNALISTS

Thanks to these partners for reviewing these safety guidelines:



**JAMES W. FOLEY
LEGACY FOUNDATION**

10 STEPS

TO KEEP YOURSELF SAFE

Journalists are using Facebook in innovative ways to do their jobs, tell stories, and connect directly with people. We want to make sure your information and accounts are secure so that you can stay safe online and protect your sources and contacts. Here are 10 steps to follow:

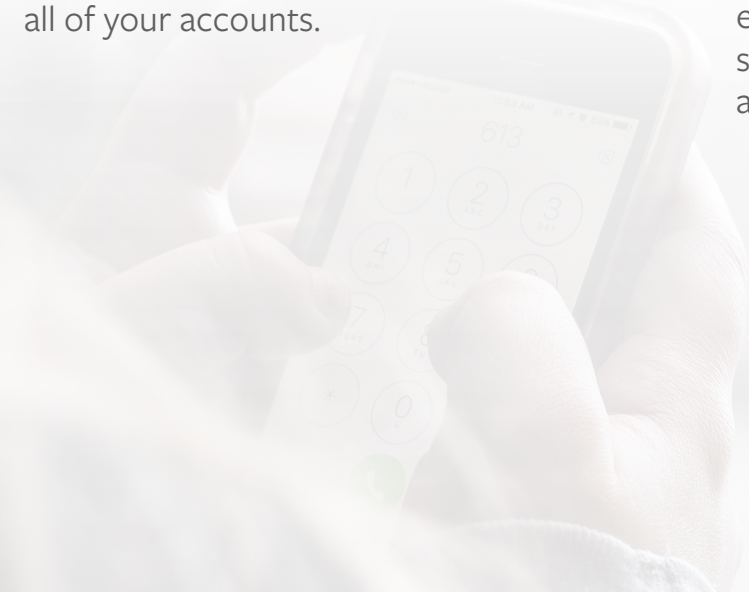
1 PROTECT YOUR PASSWORD

Your Facebook password should be unique, safe, and never shared with anyone or anywhere. Key information to avoid includes anything that's personally identifiable, like your name, phone number, birthdate and mailing address. One tip is to use a password manager that will save your passwords securely, as well as generate strong passwords for all of your accounts.

2 GET ALERTS ABOUT UNRECOGNIZED DEVICES

Use login alerts to get notifications any time someone attempts to get access to your account from a new or unrecognized device.

Turn on alerts about unrecognized logins by visiting the Security and Login section, under Settings. When alerts are turned on, you'll receive an email or notification any time someone logs into your account from an unrecognized device or browser.



3 TURN ON TWO-FACTOR AUTHENTICATION

Two-factor authentication is an extra layer of security for your account. This can be found in the Security and Login section under Settings. When you turn on two-factor authentication, you will enter a special security code each time you try to access your Facebook account from a new computer, phone or browser.

Here are options for retrieving your special security code:

- Use Code Generator if you have the Facebook app on your smartphone or tablet.
- If you are using the latest version of Chrome or Opera, register a physical security key to your account so that you'll simply use a small hardware device that fits in the USB drive of your computer. Security keys can be purchased through companies like Yubico, and the keys support the open Universal 2nd Factor (U2F) standard hosted by the FIDO Alliance.
- Facebook can also send you a text message (SMS; charges may apply) with a login code each time you need one.
- You can also get 10 recovery codes to print or write down. Save them in a safe place for when you need them, or share with a highly trusted friend or colleague as a backup option.

4 USE FACEBOOK CHECKUP TOOLS

Use Security Checkup to review and manage your profile's security settings. You can:

- View which browsers and apps you've used to log into Facebook in the past, but haven't used in over a month. You can quickly remove access from any you don't need anymore.
- Manage alerts for when your account is logged into from an unrecognized device or browser.
- Get tips on how to strengthen your password and how often to change it.

Use Privacy Checkup to make sure only the people you trust can see your information and posts, because sometimes you want to share publicly, and sometimes only with friends. You can review who can see your posts and information from your profile, like your phone number and email address. It also shows you your settings for apps that you've logged into using Facebook. You can use Privacy Checkup to review and adjust your privacy settings to help make sure that you are sharing your stories with the people you want to see them.



5

MANAGE YOUR PRESENCE ON PAGES AND PROFILES

You can be as public or as private as you want to be with your audience on Facebook. Here's advice on how to manage what you post.

Profile

- Use the Audience Selector tool to manage who can see your posts. You can choose to share with everyone, just your friends or even a customized audience. When you create a customized audience, you can selectively share with specific people.
- Control who sees what you post by updating Settings in the Timeline and Tagging tab. You can approve or dismiss tags that friends add to your posts. Once you approve a tag, the person tagged and their friends may see your post. Tag review can be found in Settings under "Timeline and Tagging."
- Use Timeline review to decide whether posts you're tagged in appear on your Timeline. When people you're not friends with tag you in a post, they automatically go to Timeline review. If you'd also like to review tags by friends, you can turn on Timeline review for tags from anyone. Timeline review can be found in Settings under "Timeline and Tagging."
- Manage how your profile appears to other people by using the "View As" tool. Simply go to your profile, click "View As" and see what your profile looks like to the public or to a specific person.

Page

Whether you are a social media editor, a journalist using a Page to reach your readers or viewers, or a Page moderator, there are multiple options to keep your Page safe. Selecting and assigning the right admin roles will help you manage your page without compromising passwords. Each person will log into their own personal account and work on the Page from there. It's important to assign Page roles accordingly because not everyone needs to have complete admin control over a page; some people only need editorial or advertiser responsibilities.

- Ensure Page admins use real accounts and have two-factor authentication turned on so they don't lose access to their accounts. Facebook removes fake and impersonating accounts when we become aware of them.
- Use Page moderation and filter tools, which are found under Page settings, to proactively moderate comments and posts by visitors. These tools will also block words and turn on the profanity filter for your Page. Don't forget to filter different variations of banned words. You can add periods or spaces in between and hashtags. For example, to filter out the word "gun," also include "g.u.n.," "#gun," and "g u n." While you can't disable comments on your Page's posts, you can hide or delete individual comments. When you hide a comment, the person who posted it will not know that it was hidden.

5 cont.

- You can choose to ban people who continually publish spam on your Page. You can remove the ban at any time. When you ban someone from your Page, they'll still be able to share content from your Page to other places on Facebook, but they'll no longer be able to publish to your Page, like or comment on your Page's posts, message your Page, or like your Page.
- If you want someone in a different location to broadcast live from your Facebook Page, consider giving them the "Live Contributor" role. This will give them the ability to go Live, but will limit access to other features on your Page.
- Facebook also allows you to delete any comments you wish to remove from your profile or Page, whether or not they're against our community standards.

6

CONTROL YOUR LOCATION IN POSTS

Facebook gives you the option to include a location in your posts. Facebook does not share location by default but it's always a good idea to update or turn off your phone's location services before posting from sensitive areas. You can update your location settings on your Android or iOS device.



7

PROTECT YOUR COMMUNICATION

Use messaging services like WhatsApp and Facebook Messenger for private communications with sources.

- WhatsApp offers end-to-end encryption by default for every message you send and call you make. When end-to-end encrypted, your messages and calls are secured so only you and the person you're communicating with can access them, and nobody in between, not even WhatsApp. For added protection, every message you send has its own unique lock and key. All of this happens automatically: there's no need to turn on settings or set up special secret chats to secure your messages. You can also show security notifications to receive notifications when a contact's security code has changed.
- You can send messages with end-to-end encryption within Messenger using your iOS or Android device. These 'secret conversations' are intended just for you and the other person. In Messenger, start a new conversation and tap either the switch with the padlock on Android or the word 'Secret' on iPhone to start a secret conversation with someone. Remember, you will need to follow these steps for each conversation partner..

Journalists can also use Facebook with the Tor browser to help conceal their IP address so Facebook, advertisers, local phone networks, and ISPs won't see where you're logging in from. This further protects the security of their location and connection to Facebook. Access Facebook using the Tor browser at <https://facebookcorewwi.onion/>. Facebook also provides support for Tor on Android through the Orbot proxy app, which you can download from Google Play.





BLOCK HARASSMENT

When you block someone they will no longer be able to do things such as tag you or see things you post on your Timeline. If you are friends, blocking will also unfriend them.

TO BLOCK SOMEONE ON DESKTOP

1. Click at the top right of any Facebook page.
2. Click **Privacy Shortcuts**
3. Click **How do I stop someone from bothering me?**
4. Enter the name of the person you want to block and click **Block**
5. Select the specific person you want to block from the list that appears and click **Block** again

TO BLOCK SOMEONE ON MESSENGER

iPhone and iPad:

1. Open a conversation with the person you want to block
2. Tap their name at the top of the conversation
3. Scroll down and tap **Block**
4. Tap next to **Block Messages**

Android:

1. Open the conversation with the person you want to block
2. Tap, scroll down, and then tap **Block**
3. Tap **Block all messages**

People will not be notified when you block them.

If you can't find the person you want to block using this method, visit the person's profile and select **Block** from the menu on their cover photo.

9

REPORT ABUSIVE CONTENT AND IMPERSONATION

The best way to report abusive content, spam, or impersonation on Facebook is by using the “Report” link that appears near the content itself. We will review the report and take appropriate action.

Here are some examples of how you can report content to us:

- To report a comment on Facebook
 - In the top right, click the down arrow
 - Select **Report post**
- To report a message on Messenger on desktop
 - Open the message you’d like to report
 - Click the Options gear in the top right
 - Click **Report** or **Block** and follow the on-screen instructions
- To report impersonation:
 - Go to the impersonated profile
 - Click on the “...” next to “Message” on the cover photo
 - Select **Report**
- To see instructions for all types of content, go to <https://www.facebook.com/report>

Contact law enforcement if you feel threatened. To report harassment to law enforcement, take screen shots and copy URL links of any unwanted attention **before** blocking the harasser. After blocking someone, their prior engagement with you will no longer be visible.

10

KNOW WHAT TO DO IF YOU'RE HACKED

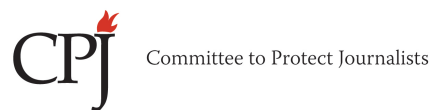
If you think your account has been hacked or taken over, you'll want to secure it as soon as possible. Having two-factor authentication enabled will help to prevent this.

If you can log into your account, we recommend changing your password. Check the contact information stored on your account to make sure it is correct and has not been altered. If you can't get into your account, we can help you secure your account by requiring you to change your password and review recent login activity. Or you can visit facebook.com/hacked.



Thanks to these partners for reviewing these safety guidelines:

COMMITTEE TO PROTECT JOURNALISTS



CONNECTSAFELY

Connect*Safely*

EUROPEAN JOURNALISM CENTRE



INTER AMERICAN PRESS ASSOCIATION (IAPA)



JAMES FOLEY FOUNDATION

JAMES W. FOLEY
LEGACY FOUNDATION

JON CAMFIELD, MEGAN DEBLOIS/INTERNEWS



facebook.com/journalists