

Privacy & Safety

on Facebook

NNEDV

A GUIDE FOR SURVIVORS OF ABUSE

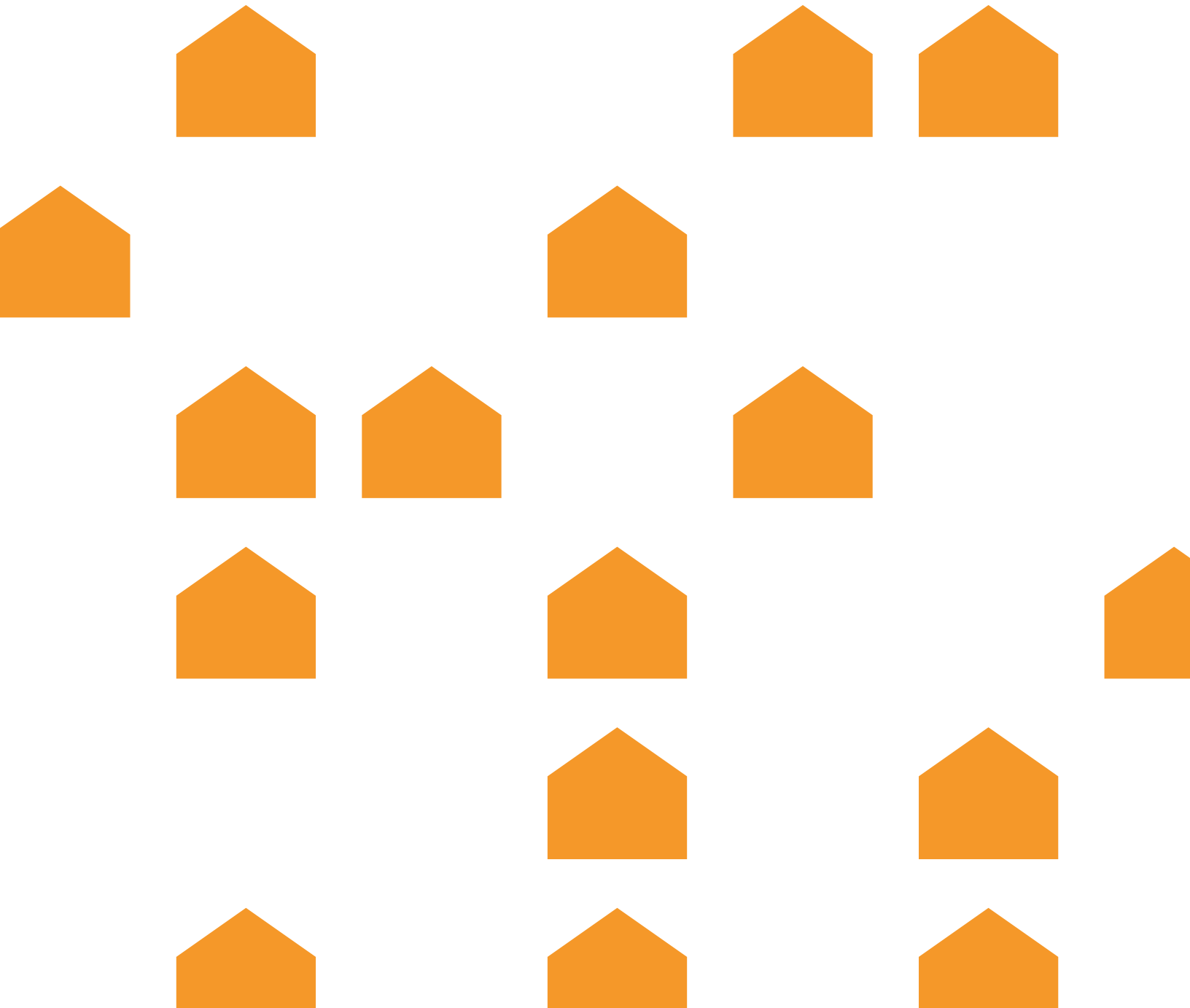


table of

C O N T E N T S

Intro

1

The First Line of Defense: Manage Who Sees Your Content

2

Take Back Control: Review Your Privacy Settings

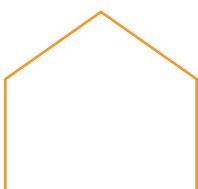
3

The Second Line of Defense: Security Settings & Notifications

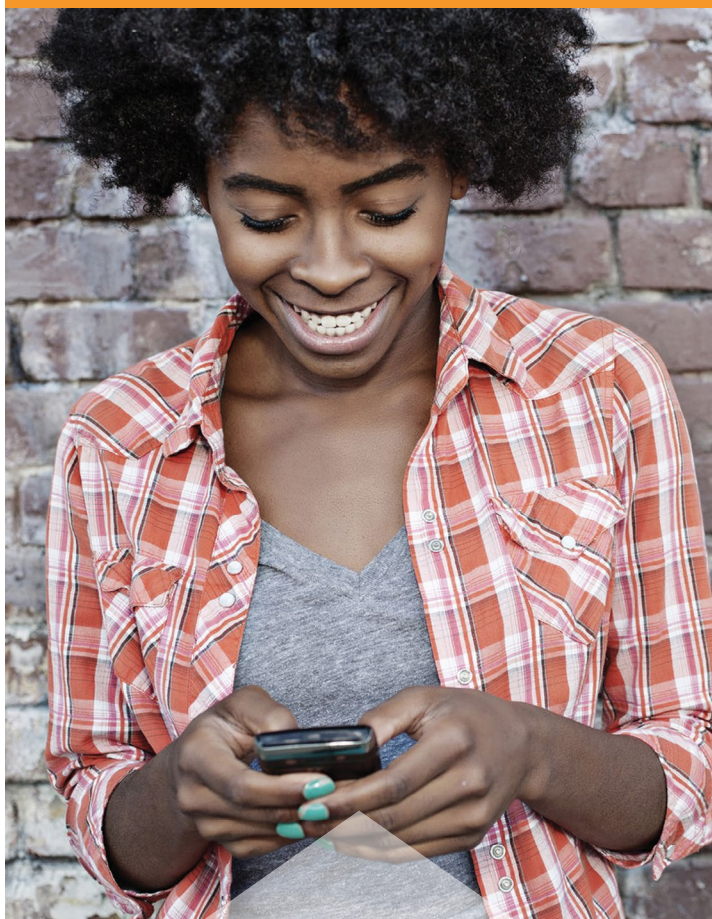
4

The Third Line of Defense: Be Safe

5-6



►►► Social media is creating a world that **is more open and connected**, enabling people to share the most important parts of their lives with families, friends and communities.



The National Network to End Domestic Violence (NNEDV) and Facebook have teamed up to offer tips for survivors of abuse so that you can still use Facebook but maintain safety and control over your information. This guide is aimed at helping survivors of domestic violence, sexual assault, and stalking with how to use Facebook in a way that ensures that they stay connected with friends and family, but control their safety and privacy to help prevent misuse by abusers, stalkers, and perpetrators to stalk and harass.

REMEMBER:

If you are dealing with a stalker or abusive individual contact the police or call the Domestic Violence Hotline at **1-800-799-SAFE(7233)**.

► **NNEDV** is the leading voice for domestic violence victims and their advocates by offering a range of programs and initiatives to address the complex causes and far-reaching consequences of domestic violence. For more information please visit **nnedv.org**.

the first line of defense: MANAGE WHO SEES YOUR CONTENT



In general, every friend you add may be able to see what you post, and depending on your privacy settings, your friends' friends may be able to see what you post as well. For some survivors, refusing to be friends with their abuser or even blocking them may not be possible and could escalate dangerous and controlling behavior by the abuser. The following are ways to manage what you share and with whom.

DID YOU KNOW?

You can choose who sees your Facebook activity either by setting a default setting or by choosing your audience on individual posts.

Select your audience

When you share information on Facebook, you can select the audience that sees that content. You have the option of sharing it with the Public, Friends, Only Me, or Custom—which gives you the most control over how you want to share a post. By creating lists of certain friends you can quickly limit the audience for any post or photo. These audience selector options can be found as part of individual posts, photo albums, and also on your basic information under the About section, however keep in mind that there are a few things that will always be public (learn more on what will always be public on the next page). You can use the “View As” feature to see what is visible to the public and friends by clicking the privacy shortcuts icon on the right hand side of your Facebook profile.

Be cautious when accepting new friends

Facebook is based on real names and authentic identities, where people represent who they are in the real world. Unfortunately, some abusive individuals use clever tactics to gain access to a victim's information. If you receive a friend request from someone you thought you were already friends with, ask them if they created a new profile. In some instances, abusive individuals maliciously create accounts impersonating a friend of the person they want to connect with.

Teach your kids

Some teens may believe that having many “friends” is a status and popularity symbol. Talk about privacy and safety with your children and why they should be hesitant to accept friend requests from people they don't know.

Discuss privacy

Maintaining your privacy isn't always just up to you since friends may post content about you or tag you. Although you can manage whether those things show up on your Timeline (as seen on the next page), friends' posts or photos will show up on their Timeline, regardless of your own settings. Since survivors of abuse may have friends who are Facebook friends with the abuser, this can be concerning.

- **Uncheck** the box that allows friends of those tagged to see content. You can find this in the custom privacy option under the audience selector.
- **Use** the tag review tool to know when you are being tagged and by whom (learn more about this feature on pg. 4).
- **Discuss** your privacy preferences with friends and family.
- **Find** out if your workplace, places you volunteer, or agencies within the community that you participate in post information about staff, volunteers, or events and ask for your information to be kept private.

For more information about how to create friend lists on Facebook, click here:

<https://www.facebook.com/help/listsbasics>



take back control: REVIEW YOUR PRIVACY SETTINGS

Who can see what you share?

You can choose who sees your Facebook activity either by setting a default setting under “Privacy Settings”/ “Who can see my stuff,” or by selecting your audience when you make an individual post. Anytime you select an audience in either place, it is remembered and set as your default for the next post you make. In other words, if you set something “Public” or to “Friends,” that will be the audience for your next post unless you change it. You can block an individual friend from seeing a particular post or limit your post to only be viewable by selected friends through the use of lists, as explained on the previous page. You can also limit the audiences for past posts if you weren’t using privacy settings previously. Take note that you control the privacy of your own information, but if you post something on someone else’s Timeline, who can see what you posted will be dictated by their privacy settings.

Who can find you?

If you are following Facebook’s Terms of Service and using your real name on your profile, then anyone can look you up and find your profile by name. How much of your information they can see will depend on what privacy settings you are using. You can also control who, if anyone, can search for your profile by your email or phone number. You can manage those options under your Privacy Settings page or the About page (hover over content to see and edit setting). The About section also allows you to limit who can see your other personal information. You can also choose to allow or not allow search engines to directly link to your Timeline. If this selection is “off” when someone searches your name in a search engine, such as Google or Bing, or on people-finder sites, your Facebook profile will not come up. This option is important for survivors who want to minimize the amount of information that comes up when someone does an online search for them. It is important to note, however, that if you post content as “Public”, that content could still show up in a search engine. In addition to turning this setting to “off,” you can limit who can view past and future posts through the audience selector. Depending on what you share and your privacy settings, you could be found in real life. For survivors, location privacy can be critical to maintaining safety. If you send Facebook messages through your cell phone make sure to turn off the location sharing feature, otherwise the person receiving the message can see your actual, physical location, complete with a map.



How to control being tagged?

Tagging is another function within Facebook that may allow others to find your Timeline. Using your privacy settings, you can choose to approve all tags before they appear on your Timeline, limit the audience of posts that you are tagged in, and turn off the “tag suggestions” feature. You can also remove tags of yourself, although removing a tag or not approving a tag does not remove the post or photo from Facebook. Those options only allow you to control what shows up on your own Timeline. If you are concerned about your privacy, you can use Facebook’s social reporting tool to ask the individuals to remove the photos or posts. If something posted is harmful to you and violates Facebook’s community standards, you can report it to Facebook. You can also discuss harmful and harassing content with law enforcement.

What are others saying about you?

Although you can’t control what others say about you on their own Timeline and elsewhere on Facebook, you can control what they say about you on your own Timeline. Under Timeline and Tagging, you can control who can post on your Timeline and who can see your Timeline.

By default: what will always be public

Although Facebook gives you many options to expand your privacy, some information will always be available if someone comes across your Timeline. This information includes your name, current profile photo, current cover photo, networks you belong to, gender, username and user ID. Survivors may want to strategize about what information to share, use a generic profile or cover photo, or determine whether they want to be a part of any network in order to maintain their privacy.

Liking or commenting on public posts: Note that posts or photos that are on other people’s profiles or organization’s pages take on the privacy settings they set for that item. In other words, if someone else’s photo is set to public (anyone can see it) and if you like it or make a comment, your comment and the fact that you liked it will also be public.

Privacy Basics Tool

The Privacy Basics Tool is designed to give people complete control over their information and experience within Facebook. Use this to easily control your privacy.

facebook.org/basics



the second line of defense: SECURITY SETTINGS & NOTIFICATIONS



Security settings control who has access to your account. This can be very important for survivors. Some abusers will try to access the survivor's account by guessing the password. Using the security settings, you can ensure that someone else cannot log into your account. Some settings that are important for survivors are the following:



SECURITY CHECKUP TOOL

Use this tool to quickly review options and add more security to your account.
facebook.com/securitycheckup

Security questions

Most of the security questions are standard personal questions that the abusive person may know the answer to or be able to guess. It's not necessary to answer these questions honestly. You can be strategic with your answers, using a word or phrase that only you will remember, so that the abuser can't reset your password by guessing the answer.

Login notifications

You can be notified, either by email or text message, if someone tries to access your account from a computer or device that you haven't used before.

Login approvals

If you are logging into your account from a different web browser or device, you must have a security code to access your account.

Recognized devices

You can manage the devices that are allowed to have access to your account and be notified if an unknown device tries to access your account. This is particularly helpful for a survivor who may have wanted to access their account from their partner's device, but now no longer wants that device to have access.

Active sessions

This is important to note because it shows sessions that are currently active or logged on. You may have active sessions if you've accessed your account or are using an app and forgot to log off. This also will show if someone else might have accessed your account. In that case, you can choose to 'End Activity,' which will block that device from continuing to access your account.

Notifications

Facebook allows you to be notified of a variety of activities, including when someone asks to be your friend, tags you, or comments on something you posted. Go through each of these notifications and determine when you want to be notified. You can select to be notified by email, on Facebook, or text messaging.

Download Your Information (DYI) tool

This tool allows you to download content and correspondence with others from your account, such as posts and photos, including some activity that is not accessible by logging in, such as ads that you have clicked on. This tool is one of the best ways for a survivor to preserve evidence of abuse, harassment, and unwanted contact. Using this tool will capture posts that have been made on your Timeline, friend requests, friends you have deleted, all messages sent and received (as long as you haven't deleted them), history of IP addresses that have accessed the account, and much more. Note that the full history of IP addresses accessing the account might not be available since Facebook does not retain the full history. To download this information go to your General Account Settings and click 'download a copy of your Facebook data.' This download will contain a lot of your personal information, so it is important to consider if anyone else could access the email that it's sent to and take caution over where you save it. Survivors are also encouraged to capture harassing or unwanted contact by taking photographs or screen shots on the computer. Some content, such as likes on a post, will not be included in the DYI and other content could be deleted by the abuser before the download finishes. Photos secure this information just in case. For more information about the DYI Tool visit:

<https://www.facebook.com/help/download>.



the third line of defense: BE SAFE

Abusers, stalkers and perpetrators misuse a variety of online spaces to harass victims. Misuse of Facebook includes: threatening or harassing someone through posts or private messages; posting information or pictures without the person's consent in order to cause harm or distress; obtaining a victim's password and accessing the account without permission; or impersonating the victim.

Although these tactics of abuse are not acceptable, they may not violate Facebook's Terms of Service and, individually, may or may not be illegal. Because of that, it is important for survivors to know what their options are and what recourses are available when someone is harassing them through Facebook.



Tools Within Facebook:

Unfriending or Blocking a person are two options within Facebook for addressing someone who is bothering you.

- **Unfriending:** When you unfriend someone, it means that activities (pictures, updates, posts) that you set to the "Friends" audience will no longer be seen by that person. Additionally, their activities will not show up on your News Feed. However, they will still be able to see whatever is public on your profile, including any activities you post with a "Public" audience, posts made by mutual friends to your Timeline, and any comments that you post on a mutual friend's Timeline. They can also re-request you as a friend.
- **Blocking:** When you block a person, they will not be able to view your Timeline activity, message or tag you, or send you another friend request (blocking automatically unfriends the person). You will also not be able to see their activity. They will still be able to see your public information and activity within apps or groups.

Use your judgment and instincts when considering the timing of these options. Since stalkers and abusers use monitoring and threats to maintain power and control over victims, when a survivor limits access, abusers sometimes find other methods of control or escalate dangerous behavior, including increased threats and even assault. Ending a relationship or contact with an abusive person can be dangerous for many survivors so it is important to plan for safety and talk to a trained victim advocate. If you are concerned about what the person might do if you were to cut off contact, call your local domestic violence program or police for more information and help.

To learn more about domestic violence programs and to find an advocate near you, contact the National Domestic Violence hotline at 1-800-799-SAFE(7233).

Reporting a person, post or picture to Facebook is a step that you can take if you feel that what is being posted or how the person is using the site is harmful. This can be done from your Timeline, from a message someone sent you, or on your News Feed.

You can report posts on your Timeline, posts that you were tagged in, or private messages. You can also report a photo, with or without a tag of you. For quick instructions on how to report certain types of content, visit: www.facebook.com/report.

For more general information about how to report something to Facebook, visit: <https://www.facebook.com/help/reportviolation>.

When using the reporting option, you also have the choice of communicating with the person who posted the content to ask them to remove or edit the content and to inform another trusted person of the content you are concerned about.

If the content violates Facebook's Terms of Service, it may be removed. Facebook also has Community Standards and will remove content if it contains violence or threats, bullying or harassment, hate speech, sexual violence and exploitation, or impersonation. Visit this link: <https://www.facebook.com/communitystandards> for a full list of Facebook's Community Standards and more information on how they define harassment and threats.

IT'S IMPORTANT TO NOTE that if a survivor is interested in preserving evidence of any harassment, threats, or other behaviors on Facebook, they should take a screenshot of the activity or use the DYI tool to save it before submitting a report requesting for it to be taken down. Once removed, the content will not be accessible again.

For more information about addressing abuse on Facebook, see the following links on Facebook's Help Center:

Tools for Addressing Abuse: <https://www.facebook.com/help/addressingabuse>

Tools for Parents & Educators: <https://www.facebook.com/help/parents&educators>

Outside of Facebook:



Some comments or posts may not violate Facebook's Terms of Service and therefore cannot be removed, even if they are meant to be and are perceived by you as threatening or harassing.

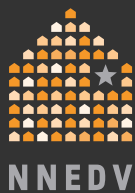
Legal Options

If someone is harassing you, threatening you, or making you feel unsafe, you can talk to a local domestic violence victim advocate or law enforcement about your options. They should be able to discuss how to preserve and document the online harassment, what legal options are available, and strategies to ensure your safety in case the harassment and threats escalate. Even if the abuser's actions on Facebook, by themselves, don't violate Facebook's Terms of Service or break any laws, taken together (a series of vague harassing messages, for example) can constitute stalking or harassment.

If you have or are seeking an order of protection or restraining order against the person, request that the order include language that restricts the person from contacting you through any means including online or posting information or photos of you online. Many states already include this in the template protection order forms. Existing orders can be amended to include this language.

Facebook has guidelines for how law enforcement can contact them for information needed in an investigation. You can share the following link with officers that you are working with: <https://www.facebook.com/safety/groups/law/guidelines/>.





facebook

BE SAFE

For More Information:

Visit the following links to learn more about your privacy & security options on Facebook:

Facebook's Privacy Page:

www.facebook.com/privacy

Family Safety Center:

www.facebook.com/safety

Basic Privacy Settings & Tools:

www.facebook.com/help/privacybasics

Security Tips & Tools:

www.facebook.com/help/securitytips

NNEDV's Safety Net Project:

www.nnedv.org/safetynet

Safety Net Resources on Online Safety:

www.techsafety.org/resources

Safety Net's Technology Safety Materials:

www.nnedv.org/safetynetdocs