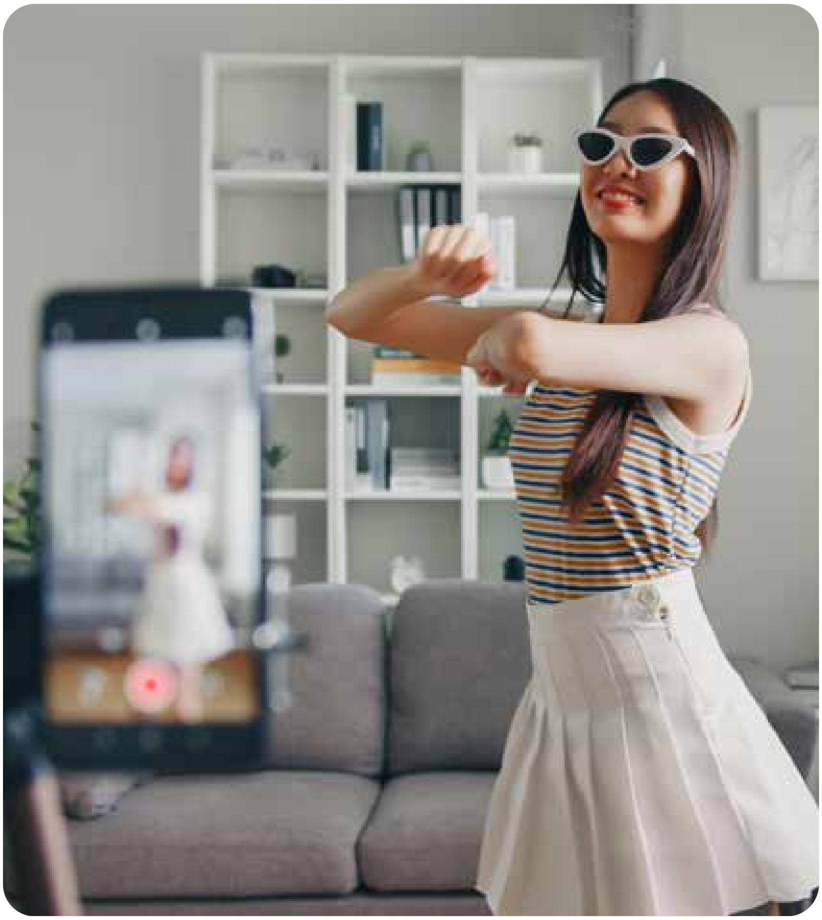
SECURITY GUIDE

The McAfee Safety Series

Staying Safer on Social Media



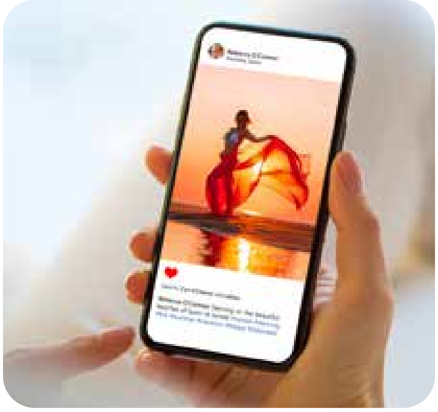
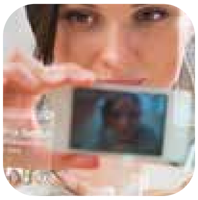
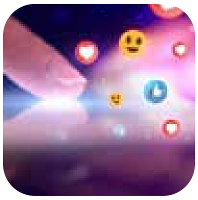


Table of Contents





Social media—A digital expression of ourselves

It began simply enough.

In the late 90's and early 2000's, a handful of websites launched with an intriguing proposition. By creating a personal account, you could build a network of dozens, hundreds, or even thousands of people. Once there, you could look up old friends, make new ones, or maybe rekindle an old flame. Share photos. Post status updates. Message your crush. Build a following. You could do all of it, and all through a personal page that worked like your own mini website.

These newly coined "social media" sites caught on. Then they absolutely transformed the internet.

Up until that time, the internet was largely a place where people passively consumed web content. Relatively few people created content of their own. The advent of social media turned the internet into an active space for the everyday user—a place where practically anyone could create and share their content with a global audience. No special software or technical expertise required. Just a browser.

Now click ahead to where we are today. Nearly 50% of the global population use social media to some degree. And it does more than connect with others. We get our news on it, spin reel after reel of video on it, and even get customer service on a company's social media page. Further, we can use our social media accounts to log into other sites and apps or use it to make payments.

No question about it, social media has evolved into something else entirely from its simple beginnings.

People worldwide now spend an average of 145 minutes a day on social media. In some nations, that number pushes four hours a day. With all that time spent on social media, all that content we view and post, and all that data social media companies harvest from our activity, our social media profiles have become a digital expression of ourselves. And like anything that's uniquely your own, it needs to be protected.

With this guide, we'll show you some ways you can do exactly that. We'll touch on four broader topics and drill down into each with tips, tricks, and advice that can help you enjoy social media safely on your own terms:

- Basic Social Media Security
- Steering Clear of Social Media Scams
- Social Media and Your Privacy
- Dealing with Harassment and Bullying

Let's start with the basics of protecting your social media profile online.

Basic social media security

Light user or heavy user, single account or multiple apps, everyone who hops on social media benefits from basic security. A social media account is indeed a digital expression of yourself, which calls for protecting it just like any other aspect of your personal identity.

So whether you're using Facebook, Instagram, TikTok, or whatnot, here are several things you can do that can help keep you stay safe and secure out there:

1. Set strong, unique passwords. Passwords mark square one in your protection, where strong and unique passwords across all your accounts form a primary line of defense. Yet with all the accounts we have floating around, juggling dozens of strong and unique passwords can feel like a task—thus the temptation to use (and re-use) simpler passwords. Hackers love this because one password can be the key to several accounts. Instead, try a password manager that can create those passwords for you and safely store them as well. Comprehensive online protection software will include one. You can also look into free options as well, like our own True Key.

2. Go private. Social media platforms like Facebook, Instagram, and others give you the option of making your profile and posts visible to friends only. Choosing this setting keeps the broader internet from seeing what you're doing, saying, and posting, which can help protect your privacy and your identity as well.

3. Say "no" to strangers bearing friend requests. Be critical of the invitations you receive. Total strangers could be more than just a stranger, they could be a fake account designed to gather information on users for cybercriminals, spread false information, or open a channel of communication for a scammer looking to bilk you out of money. There are plenty of bogus accounts. In fact, in Q3 of 2021 alone, Facebook took action on 1.8 billion fake accounts. Reject these requests.

4. Think twice before checking in. Nothing says "there's nobody at home right now" like posting that picture of you on vacation or sharing your location while you're out on the town. In effect, such posts announce your whereabouts to a broad audience of followers (even a global audience, if you're not posting privately, as called out above). Consider sharing photos and stories of your adventures once you've returned.

5. Remember that the internet is forever. It's a famous saying for a reason. Whether your profile is set to private or if you are using an app with "disappearing" messages and posts (like Snapchat), what you post can indeed be saved and shared again. It's as simple as taking a screenshot. If you don't want it out there for potentially all to see, simply don't post it.

6. Protect yourself and your devices. Online protection software can help steer you clear of threats on social media, like clicking on malicious links and other headaches like viruses, ransomware, and phishing attacks. It can look out for you as well, by protecting your privacy and monitoring your email, bank accounts, credit cards, and other personal information.

7. Check your Protection Score and see how safe you are. Now you can point to a number that shows you just how safe you are with our Protection Score. It's an industry first that's included with our online protection software, and it works by taking stock of your overall security and grading it on a scale of 0 to 1,000. From there, it calls out any weak spots and walks you through the steps to shore it up with personalized guidance. This way, you're always in the know about your security, privacy, and personal identity on social media and practically wherever else your travels take you online.

0–399	Low
400–599	Fair
600–699	Good
700–849	Very good
850–1000	Excellent

Figure 1. Protection Score Ranges

Steering clear of social media scams

There're millions of dollars to be made in social media. For scammers.

Take the U.S. as an example. Recent data from the U.S. Federal Trade Commission (FTC) suggests that Americans lost nearly three-quarters of a billion dollars to social media fraud in 2021, signaling that social media may be the most profitable method of scamming victims—marking an 18-fold increase over 2017.

And that's just cases of reported fraud.

Of the roughly 95,000 cases tallied in 2021, the actual number of reports and losses are arguably much higher because fraud victims infrequently report these crimes to the FTC or other agencies. Likewise, few take advantage of the FTC's resources for recovering from fraud. Instead, they'll share the sad news with family or friends if they even share it with anyone at all.

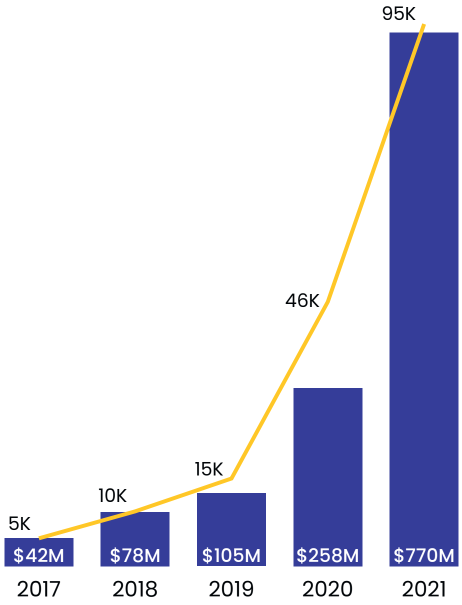


Figure 2. Reports and Losses Associated with Social Media Fraud – FTC

Of course, social media scams aren't limited to the U.S. alone. The International Criminal Police Organization (INTERPOL) conducts annual multi-nation clampdowns on fraudsters, which includes social media scammers—raking in hundreds of arrests and recovering millions of illicit dollars, once again representing just a fraction of the overall crimes committed internationally. In the UK, figures point to more than 1 billion pounds lost in 2021, no thanks to online scams.

Despite the rise of these online crimes, there are several things you can do to increase your awareness of social media fraud—what it looks like and how it's pulled off—along with other ways you can prevent scammers from targeting you and the ones you care about.

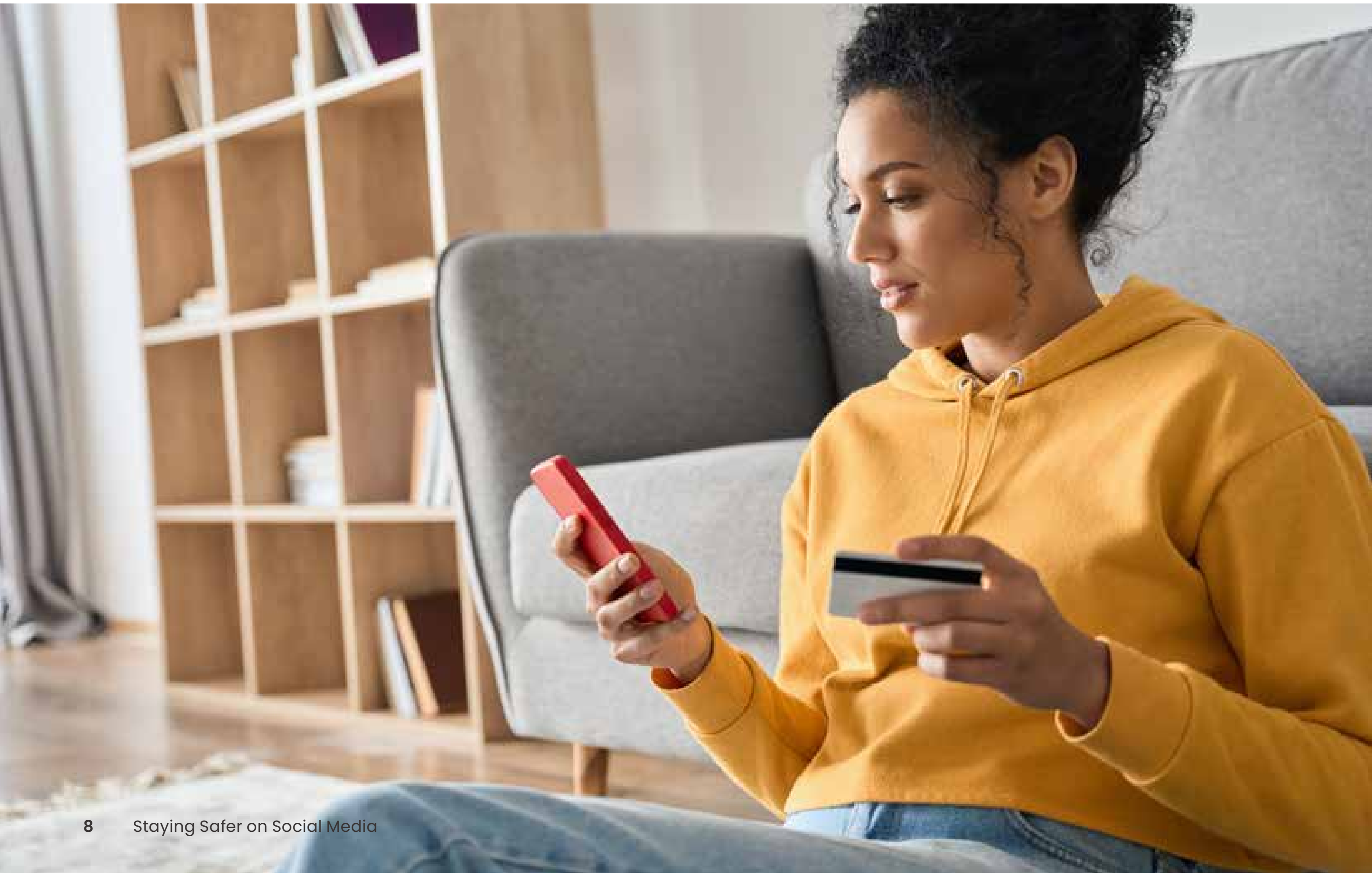
What does social media fraud look like?

Several types of social media fraud abound, yet the FTC reports that three types of scams prevail:

Investment scams: These often involve bogus sites that promote opportunities to mine or invest in cryptocurrencies. Rather than use these sites to trade in legitimate cryptocurrencies, scammers use these as a front to collect funds. The funds are never invested and never returned. Thanks to social media, scammers have a quick and easy way to drive victims to such bogus sites.

Romance scams: By starting up a chat through an unexpected friend request or a message that comes out of the blue, a scammer develops a budding romantic relationship with a victim—and eventually starts asking for money. Public social media profiles are particularly attractive to scammers because they're loaded with information that scammers can use to win a victim's confidence, or heart.

Online shopping scams: Using social media ads, scammers drive victims to phony online stores that will take people's money but that don't deliver the goods. They're simply a way for scammers to reap cash from unsuspecting shoppers. These sites may impersonate reputable brands and stores, or they may sell bogus products altogether. Either way, victims pay and receive nothing in return.



What makes social media such a happy hunting ground for scammers?

For one, reach. Earlier we mentioned that nearly half of the global population uses social media today, which translates into billions of people who can be made into potential victims. Secondly, social media provides the tools to reach those people. In the case of investment and shopping scammers, social media ad platforms are of particular use. For romance scammers, direct messaging and profile pages are potential avenues for fraud.

How scammers use social media ads to swindle victims

Scammers make cagey use the highly targeted ad platforms that social media companies use to generate revenue. With millions of detailed user profiles in their data stores, social media companies then allow businesses to create ads designed to reach people based upon age groups, hobbies and interests, past purchases, and so on. Just as easily, a scammer can use the same tools to cook up bogus ads for their bogus products, services, and sites at relatively low cost—all targeted at a specific audience. A straightforward example of this is an ad for a scam site aimed at single women over 40 who live in North America and who have shown an interest in cryptocurrencies. And it can get far more targeted than that.

The FTC reports that the median loss for an online shopping scam in 2021 was $118, while online investment scams on social media racked up a median loss of $1,800 per victim. These stats make a strong case for sticking to reputable and established retailers and accredited financial services.

Friend requests

In the case of romance scammers on social media, the posts and personal profiles that form the heart of social media offer a treasure trove of targets for a would-be con artist. With a potential victim's life a relatively open book, full of birthdays, events, interests, and activities for all to see, scammers have the hooks they need to form a phony romantic relationship online—or least make the attempt at one.

For example, a scammer reaches out to a potential victim with a friend request. With the profile and posts this romance scammer has at hand, they can spin all manner of intriguing, yet utterly false tales designed to gain the victim's trust. With that trust established, they can follow up with a similarly intriguing story about needing "a little help" to cover some "unexpected expenses," often in the form of a gift card or reloadable debit card—sometimes stringing out a series of requests over time. According to the FTC, the median loss for this type of romance scam in 2021 was around $2,000 per victim.

Preventing social media scams

Watch out for phishing attempts.

We're increasingly accustomed to the dangers of phishing emails, yet phishing attacks happen on social media as well. The same rules for staying safe apply. Don't follow any links you get from strangers by way of instant or direct messengers. And keep your personal information close. Don't pass out your email, address, or other info as well.

Skip the quizzes.

Those so-called "quiz" posts and websites can be ruses designed to steal bits and pieces of personal info that can be used as the basis of an attack. There's a reason they're asking for things like your birth month, the make of your first car, and so on—these are often security words that institutions like banks and credit card companies use to verify who you are.

Do a background check—on businesses and people.

When you're shopping online, do some quick research on the company. How long have they been around? Have any complaints been recorded by your attorney general or local consumer protection agency? When you meet someone new, do a reverse image search on their profile pic to see where else it appears. Look up their name in search as well. If the results you find don't match up with the person's story, it may be a sign of a scam.

Report any social media scams.

Strongly consider filing a report if you believe you've been a victim of a social media scam. While some of the scammers behind these crimes are small-time operators, there are larger, almost business-like operations that conduct these crimes on a broader and sometimes international scale. So whether filing a report will help you recover some or all your losses, it can provide information to businesses and agencies that can help keep it from happening to others.

Social media and your privacy

What do social media companies really know about you? It's a fair question. And the quick answer is this: the more you use social media, the more those companies likely know.

Taken together, all of those likes, taps, clicks, links, and time spent reading or watching videos can add up and paint a detailed picture of who you are.

Why are they collecting all this information? Largely, it's for two reasons:

1. To make improvements to their platform, by better understanding your behavior and ways you like to use their service.
2. To create an exacting user profile so that advertisers can target ads that they think will interest you.

That's the exchange in play here. You use the company's social media service for free, and in return they gain rights to gather specific information about you, which you consent to by agreeing to their terms of service.

Let's get into the details of what social media companies may collect and know about you—along with ways you can limit the data and information they gather.

(Some of) the things social media companies may know about you

Different social media platforms have different user agreements that cover what types of information they collect and use. So for starters, we'll speak broadly about social media companies in general, and then we'll weave in a few specific examples along the way. Generally, they may know:

- **Basic information about you and the devices you use:** This includes personal information that people include in their profiles, such as names, birthdates, locations, relationships, and gender. This can extend to other identifiers like IP addresses, unique device ID numbers, connection type, connection speed, your network, other devices on your network. Also, device behavior can get tracked as well. That may include whether a window is open in the foreground or background and what mouse clicks and finger taps you make while using the service. Note that this type of information gathering isn't unique to social media—many sites and experiences online track this information as well.
- **What interests you:** People, pages, accounts, and hashtags that are associated with you and that you interact with in some way can get tracked. Likewise, how those people, pages, and accounts associate themselves with you in return get tracked as well. All of it builds up a profile with increasing levels of detail the more you engage with others and as they engage with you.
- **What makes you stick around:** Social media companies may measure the frequency and duration of your interactions. The more you interact, the more likely you are to have a strong connection to certain topics and opinions—and subsequently social media companies may suggest similar content that they believe you will engage with just as strongly. For example, Facebook puts it this way on their privacy page (as of October 2021): *We collect information about how you use our Products, such as the types of content you view or engage with; the features you use; the actions you take; the people or accounts you interact with; and the time, frequency and duration of your activities.*

- **Who you're chatting with:** Depending on the platform and its terms of use, information about direct messages you send using the platform may be collected as well. For example, Twitter does the following (as of October 2021): *When you communicate with others by sending or receiving Direct Messages, we will store and process your communications and information related to them. This includes link scanning for malicious content, link shortening to http://t.co URLs, detection of spam, abuse and prohibited images, and use of reported issues. We also use information about whom you have communicated with and when (but not the content of those communications) to better understand the use of our services, to protect the safety and integrity of our platform, and to show more relevant content.*
- **Things you purchase on the platform:** In some cases, social media companies will track information about transactions you make on their platform. For example, Instagram includes the following language in its terms of use (as of October 2021): *If you use our Products for purchases or other financial transactions (such as when you make a purchase in a game or make a donation), we collect information about the purchase or transaction. This includes payment information, such as your credit or debit card number and other card information; other account and authentication information; and billing, shipping and contact details.*
- **Where you are and where you go:** Simply disabling location sharing or GPS functionality on your device does not rule out other ways that social media companies can determine your whereabouts. They can infer your location to some extent when you log in by looking at your IP address and public Wi-Fi networks, along with nearby cellular towers if you're on mobile.

By the way, none of this is secret. What's listed here can be found by simply reading the terms of use posted by various social media companies. Note that these terms of use can and do change. Checking up on them regularly will help you understand what is being collected and how it may be used.

Your content says a lot about you too

This nearly goes without saying, yet another layer of data and information collection comes by way of the pictures and updates you post. Per Instagram (as of October 2021), *We collect the content, communications and other information you provide when you use our Products, including when you sign up for an account, create or share content, and message or communicate with others. This can include information in or about the content you provide (like metadata), such as the location of a photo or the date a file was created.*

Another consideration is how the content you interact with on other sites may be shared with social media companies in return. Some social media companies partner with other third parties to gather this data, which is used to round out your user profile in yet more detail. That information can include purchases you made, how often you visited that third party's site, and so on.

In the case of Facebook, they refer to this as "Off-Facebook Activity." In their words, *Off-Facebook activity includes information that businesses and organizations share with us about your interactions with them. Interactions are things like visiting their website or logging into their app with Facebook. Off-Facebook activity does not include customer lists that businesses use to show a unique group of customers relevant ads.* The good news here is that you can take control of the Off-Facebook Activity setting with a few clicks.

So no doubt about it, the content you create and interact with, both on the social media sites and sometimes off them as well, can generate information about you that's collected by social media companies.

Limiting what social media companies know about you

Short of deleting your accounts altogether, there are several things you can do to take control and limit the amount of information you share.

1. You can access, update, correct, move, and erase your data, depending on the platform. For example, you can visit your Facebook Settings, Instagram Settings, and Twitter Settings, which each give you options for managing your information—or download it and even delete it from their platform outright if you wish. (Note that this will likely only delete data associated with your account. Content you posted or shared with other people on their accounts will remain.)

2. Disable location sharing. As noted above, this isn't an absolute fix because social media companies can infer your location other ways. Yet taking this step gives them one less piece of precise information about you.

3. Review your privacy and account settings. Each platform will have its own settings and options, so give them a look. Here you can determine which information is used to serve ads to you, set rules for facial recognition, enable or disable location history, and much more. If possible, do this from your browser. Often, the account controls that you can access from a browser are far more comprehensive than the ones in a mobile app.

4. Consider using other messaging platforms. Using direct messaging on social media platforms may tell social media companies even more about you and who you interact with. When possible, think about using text messaging instead or other means of communication that aren't tied to a social media company.

5. Decouple your social media account from other apps and sites. Some apps and sites will allow you to use your social media login instead of creating a new one. While convenient, this can provide the social media company with more information about you. Additionally, if your social media account is compromised, it could potentially compromise the other accounts that are tied to it as well. Check your settings and look for "Apps and Websites" to see what's connected to your social media account, what's being shared, and how you can disable it.

Dealing with harassment on social media

Trolls, cyberbullies, and griefers. Unfortunately, they're online too. And whoever they are, and whatever their motivation, they can make you feel anywhere from angry and uncomfortable to frightened and unsafe.

For starters, if you ever feel you are in imminent danger from any kind of harassment online, contact your local emergency number. If it's happening to someone else you know, warn them, and advise them to do the same if they feel they're in danger.

Of course, not all harassment goes that far. Yet that doesn't mean it still isn't dangerous or harmful. According to StopBullying.gov, it can lead to depression, anxiety, and other health complaints, along with decreased performance at school or work.

This behavior separates itself from the throwaway and offhanded remarks that we may occasionally come across online, which can certainly sting, yet don't form a pattern. In fact, a telltale sign of serious harassment is that it persists over time and the victim feels consistently targeted. Another sign is that the harassment is permanent, meaning that it's posted online for others to see, time and time again.

Turning to figures in the U.S. as an example once again, findings from the Pew Research Center indicate that 4 in 10 of Americans say they have been subjected to some form of harassment online over the course of 2020. All forms saw a rise, including less severe forms like name-calling and purposeful embarrassment, along with more severe forms like physical threats, stalking, and sexual harassment.

With figures such as these, there's a good chance you or someone you know will get harassed online—if it hasn't happened already.

Steps you can take

Whatever form it takes, the best way to deal with harassment is to deal with it immediately.

Don't respond to it. While you might want to strike back with a message or post of your own, don't. This may only escalate the situation or, worse yet, make you look like the instigator. In all, responding will only do more harm than good.

Document everything. Grab screenshots of the messages, posts, texts, photos, or whatever was involved in the harassment. Include the screenname of the person behind it, along with a time and date. This will help you document a timeline of the harassment.

Report it. Depending on the context and situation, you have options here. For example, this may be a matter that you want to report to your child's school. Likewise, harassment will nearly always violate the terms of service on websites, services, and apps. You may be able to flag a negative post to get it removed and other sites, services, and apps may have other avenues to report harassment. Use them. And get that content taken down if it is posted publicly.

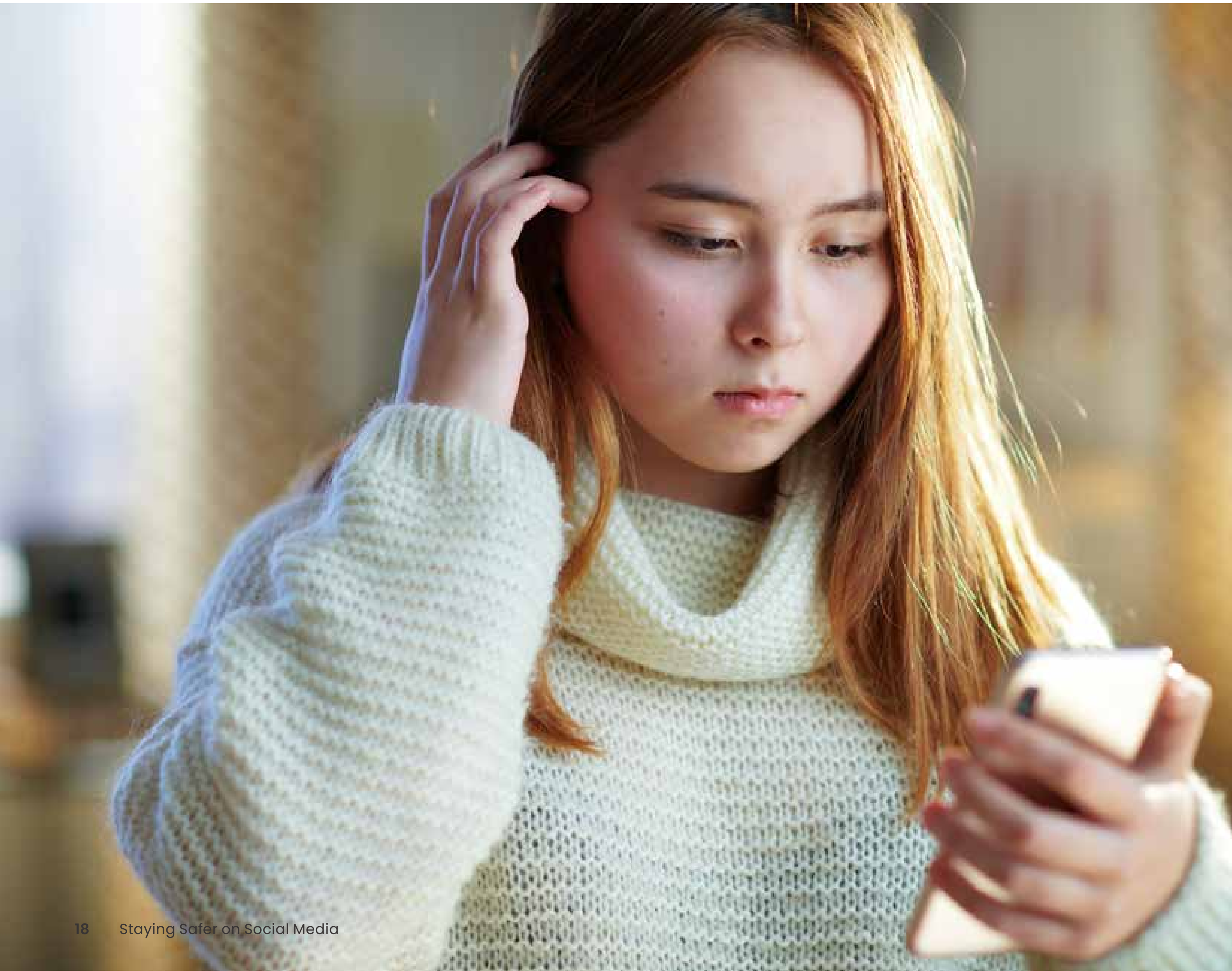
Determine if it breaks the law where you live. Of course, laws will vary based on your nation, state, or province, yet anti-harassment laws are on the books—not to mention defamation, slander, and libel laws. A search for governmental resources on cyberbullying and online harassment give you a good sense if a law was broken, and you can consult with licensed counsel in your area for a more definitive answer.

Monitor. As said, harassment is often persistent. Keep an eye out for more of it and follow the same steps here as needed.

Contact your local emergency number if you're in immediate danger. Simply repeating what we said above. If you believe that a threat made online can turn into a threat against you, your family, or your property, follow through just as you would if that threat were made anywhere else.

While another important consideration falls outside the realm of online protection, it bears mentioning. Harassment and threats in their more extreme expressions can leave emotional scars. Victims may need support in the wake of them, possibly from a professional. You and your judgment will know what's best here, yet given the harm harassment can potentially cause, keep an eye for signs of lasting effects such as the ones mentioned above, in addition to others like low self-esteem, insomnia, or eating disorders.

Where can you start if you have concerns? Several national and local governments support websites for mental health resources, along with others dedicated to cyberbullying and harassment. In the U.S., the Department of Health & Human Services has a list of resources available for victims and their families. Likewise, the Canadian government website hosts a list of similar mental health resources, and in the UK the NHS hosts a list of resources as well.



Safer, more private social media

With the way social media commands so much of our attention, it makes sense to carve out some time to make sure it's as safe and private as can be.

We've covered some rather comprehensive measures here, and we encourage you to take them even if your use of social media is relatively light. And don't feel any pressure to address them all at once. Simply setting aside a few minutes over a few days to chip away at them will make you safer and safer as you go.

For more on protecting yourself on social media, our blog offers you and your family a terrific resource across a wide range of topics from online banking, gaming, and shopping to tough yet important topics like cyberbullying and which apps are safe for kids.

Our aim is to help you think about what's best for your family and the steps you can take to see it through so that you can make everyone's time online safer and more enjoyable.

Visit us any time!

https://www.mcafee.com/blogs

About McAfee

McAfee is a worldwide leader in online protection. We're focused on protecting people, not devices. Our solutions adapt to our customers' needs and empower them to confidently experience life online through integrated, easy-to-use solutions.

www.mcafee.com

For more information about online protection, visit us at mcafee.com/blogs

McAfee™

6220 America Center Drive
San Jose, CA 95002
888.847.8766
www.mcafee.com