The Empowering Internet Safety Guide for Women

Table of contents

Have you ever been harassed in the street? Received a crass message on a dating app? Had a coworker make a comment about your appearance that just didn't sit right?

You're not alone.

With the #MeToo movement, it's easy to log onto Twitter or Facebook and see just how many women are victims of sexual harassment. Whether in person or online, women everywhere have experienced it in one way or another. And with all the new ways the internet has opened avenues of communication, **online harassment is more prevalent than ever**.

According to a study (http://www.pewinternet.org/2017/07/11/online-harassment-2017/) by the Pew Research Center, **most online abuse takes place on social media**. Although men are also subject to online harassment – which includes name calling, derision, and physical threats – the study found that online, **women are more than twice as likely as men to experience sexual harassment**.

In addition, **more than half of women ages 18-29 report having been sent sexually explicit images without their consent**.

This number is only growing, and while 70% of women believe online harassment to be a major problem, not many know how to prevent it.

Women are often targeted simply because they are women. Attacks are often sexualized or misogynistic, and rhetoric tends to focus on their bodies and sexual violence. This is both physically and emotionally damaging, and **women are often intimidated into silence, preferring to disengage rather than put themselves at risk**.

However, there are ways we can protect ourselves.

This guide was written with the intention of empowering women to navigate the internet without fear. We discuss common occurrences in which women are subject to harassment in their daily lives – on social media, at work, while dating, and more – and give tips and advice on how women can take control.

It is important for us to note that **some of the advice given here encourages anonymity**, rather than risking being targeted. While this may seem to run counter to the idea of encouraging self-expression, we believe that every woman should be empowered to make that choice for herself.

Our job is to give you the tools you need to do that.

We hope this guide encourages women everywhere to **defend and protect themselves, and to stand up to sexual harassment, both on and off the web**.

Harassment on Social Media

The majority of online harassment takes place on social media, which makes sense given how much time most of us spend on these platforms. Broad social networks, often combined with anonymity, leads to a reality in which anything you post, tweet, or share opens you up to potential abuse.

Below, we delve into the most popular social media platforms, and show you how to protect yourself from creeps, trolls, and stalkers.

Twitter

Due to its public nature, **Twitter is one of the most notorious social media platforms when it comes to online harassment**. And it's not just celebrities and public figures who get abuse heaped on them. There are endless stories of regular people who have been attacked, often for simply speaking out about political or feminist issues.

In fact, Amnesty International released a report (https://www.amnesty.org/en/latest/research/2018/03/online-violence-against-women-chapter-1/) chastising Twitter for not appropriately addressing harassment of women. In the study, dozens of women are quoted about the abuse they experienced on Twitter, many citing unsatisfactory responses from the social media site after having reported the incidents.

Often, **the result is a silencing effect, in which women simply choose not to engage for fear of being harassed**; many women end up censoring themselves or leaving the platform altogether. And for some – particularly journalists and activists – this can be **detrimental to their careers**.

Things came to a head in October 2017 when **a series of high profile sexual assault allegations spawned the viral hashtag #MeToo**. The hashtag – used by women to identify themselves as having experienced sexual harassment or assault – took over Twitter in a matter of hours, and made crystal clear just how prevalent these incidents are.

Soon thereafter, actress Rose McGowen's Twitter account was temporarily suspended after she tweeted a series of allegations against sexual predator Harvey Weinstein and several Hollywood bigwigs she claimed enabled him. The violation cited was that one of her tweets included a private phone number.

But with so many abusive tweets against women not resulting in suspended accounts, many women had had enough. The resulting anger spawned the **hashtag #WomenBoycottTwitter, which called on women to boycott the platform for a day in solidarity**.

Twitter claims to have improved their system of addressing reports of harassment, but it's still an issue, and there are still steps individual women can take to mitigate the chance of being targeted.

5 Ways to Protect Yourself on Twitter

1. Use Multiple Profiles

Women whose careers depend on keeping up a public profile may find it helpful to use multiple accounts.

Unlike some other social media platforms, according to Twitter's terms of service, it's perfectly acceptable to do this. In fact, businesses often do in order to target different audiences.

You'll want to create a personal profile and a public one.

Your personal profile should have the strongest privacy settings. Since Twitter's default setting is public, you'll have to opt in to this.

Ordinarily, when your tweets are public, anyone can see them – even people who don't have Twitter can potentially find them. But **when your tweets are "protected," only your approved followers can see them, and no one will be able to retweet them**. Make sure that the only people you let follow you are people that you know and trust.

> **How to Change Your Privacy Settings on Twitter:**
>
> Click on your profile and go into Settings and privacy>Privacy and safety>Protect your Tweets.

Making this change retroactively protects your older tweets too. That said, it's important to note that since Twitter has no control over outside search engines, **older tweets may still be visible on the wider internet**. So if you want true anonymity, you should open a new personal profile and protect your tweets from the get-go.

It's also important to note that your replies to other tweets and mentions will also be protected, and will therefore only be seen by your approved followers. This obviously makes it a lot **harder to engage in the type of public discussions for which Twitter is famous**, so you'll have to decide if having a private profile is worth it to you.

> To create an additional account, click on your profile icon. Then click on the upside down caret next to your name. There you should be given the option to create a new account.

This second profile will be your public one. If you use Twitter for your job, **this is going to be the one that represents you professionally**, so make sure not to Tweet about anything too personal.

Another option is to simply keep this profile anonymous. That means **not using your real name or photos of you, or tweeting anything that could be used to figure out where you live or work**.

Note that **you can't keep both accounts open on the same browser at the same time**. If you want to have them both open, either use different browsers, or use the Twitter-supported app, TweetDeck.

2. Report and Block Abusers

If you do receive an abusive tweet, you can block the person who sent it.

> **How to Block Someone on Twitter:**
>
> Click on the upside down carrot on the upper right hand corner of the tweet, and choose to block the user.

One of the problems with blocking is that it's really easy for users to create new accounts – often termed "sock puppets" – that haven't yet been flagged.

One way to deal with this is with the app Block Together. Block Together will automatically block any account that tries to follow you that's been active for under 7 days, that has under 15 followers, or that your followers have blocked. It's most helpful when you're being attacked by an army of trolls.

In addition to blocking users, you can also report abusive incidents to Twitter.

> **How to Report Someone on Twitter:**
>
> Just click the upside down caret in the upper right corner of the tweet or account, select report, and follow the instructions.

Unfortunately, even though harassment is against Twitter's user agreement, Twitter is infamous for not doing as much as it could to curb ugly behavior.

In fact, according to an analysis (http://womenactionmedia.org/cms/assets/uploads/2015/05/wam-twitter-abuse-report.pdf) from the nonprofit, Women Action and the Media (WAM!), **67% of women who reported abuse claimed to have notified Twitter at least once before**.

Still, it's definitely worth reporting abusive tweets and accounts, since doing so is really easy.

Twitter does not currently provide a way of checking the status of reports of abuse. That said, as of January 2018, Twitter notifies you of their assessment once the report has been processed.

3. Don't Geotag

Geotagging is when **your post includes the location from which it was sent**. To keep yourself safe from doxing and stalking, it's best not to use this function. Fortunately, geotagging requires you to opt in, so by default your location won't be shown.

When you compose a tweet, you'll see a location button at the bottom. (It looks like a dropped pin.) If you tap it, you'll have the option of adding your location to your tweet.

Don’t do it.

Also, be aware that **you could give away your location even without geotagging, simply by mentioning where you are**. We know it’s fun to let people know in the moment that you’re enjoying a new gallery opening or a night on the town, but sometimes it’s better to wait and post about it later, when you’re not there anymore and can tweet about how much fun you HAD (past tense).

4. Prevent Doxing

The most extreme form of online harassment is doxing. Doxing is when someone’s personal information, such as their address, phone number, place of employment, banking details, and even information on their family members, is published online as **a call for others to harass them**.

You may have heard the term for the first time with reports of #gamergate back in 2014. Gamergate was a movement spawned by the angry ex of video game developer Zoe Quinn, who wrote a blog post accusing her of having slept with a journalist in exchange for a good review.

Despite the fact that no such review was ever written, **the post was taken as a battle cry by an unruly mob of mostly white, male gamers, who saw not only their favorite pastime, but free speech and their very masculinity, as under attack** by so-called social justice warriors.

The result?

Not only Quinn, but women who defended her, including game developer Brianna Wu and journalist Anita Sarkeesian, came under relentless attack by internet trolls who inundated them with **a daily barrage of murder and rape threats**, mainly via Twitter.

They were also doxed.

The effects throughout the gaming industry were chilling, and **women continue to take extra precautions for fear that they will become targets**.

For instance, Tessa,* a competitive intelligence analyst whose work requires her to interact with gamers, **knows several women in the industry who have been stalked and harassed**, and often faces flirtatious and disrespectful behavior herself. Because a lot of interactions take place on Skype, there’s no hiding the fact that she’s a woman. Still, **she takes pains to conceal that she works directly for a gaming company**, and doesn’t reveal any personal information about herself like her real name or location.

Of course, those in the gaming industry aren’t the only ones at risk for doxing. Today’s incendiary political climate has resulted in many **losing their jobs and having to leave their homes after having been doxed for attending alt-right or antifa rallies**.

But you don’t have to engage in controversial political activities to be doxed. **Some have been doxed “accidentally.”**

For instance, following the Boston Marathon bombing, a Brown University student was doxed when he was wrongly identified as the perpetrator, and following the Charlottesville Unite the Right rally, an Arkansas University engineer was doxed when he was mistakenly identified as a participant.

4 Ways to Keep from Getting Doxed

1. **Google yourself.** A simple search will show you what kind of information about you is already online. If that includes data that can be used to identify you, see if you can have it taken down. Social media profiles have privacy settings that can easily be reset, and many websites, such as the White Pages, give you the option of opting out. Unfortunately, it may not be possible to scrub all your information from the internet, but at least searching will let you know what's out there for others to find.

2. **Subscribe to a service that will delete you from data broker sites:** If you find your information on a website like White Pages, chances are it also appears in other online directories, many of which won't be easy to find. So if you have reason to believe you may targeted for doxing, consider paying for a service such as PrivacyDuck or DeleteMe.

3. **Check that your email account hasn't been involved in a data breach:** You can use the tool https://haveibeenpwned.com/ (https://haveibeenpwned.com/) to see if your email address and password may have been exposed in one of the many large-scale data breaches that have occurred in the past few years. If they have, reset your password, and consider adding two-step verification to your account. This will provide an extra layer of security by requiring additional information (besides your password) in order to log in.

4. **Use a VPN:** By using a virtual private network, you can encrypt all your online activity in order to protect yourself from hackers. VPNs work by tunneling your internet data through a third party server, keeping your IP address (and real location) from being exposed. Here are some VPNs we recommend (https://www.vpnmentor.com/bestvpns/overall/).

5. Prevent Hackers from Taking Over Your Twitter Account

From former President Obama to Britney Spears, over the years plenty of celebrities have had their Twitter accounts hacked by people who want to harm their reputations and cause chaos. That said, regular people also have their accounts hacked with alarming frequency.

4 Ways to Keep Your Twitter Account from Being Hacked

1. **Create a strong password:** This sounds obvious, but you'd be surprised how many people use weak, easily discoverable passwords. (Or maybe you won't be.) To make a strong password, make sure it's long, has capital and lowercase letters, and includes numbers and symbols.

2. **Enable login verification:** This provides an extra layer of security when you're logging in. Instead of just having to enter your password, you'll also have to enter a code that Twitter sends to your mobile device. To enable this, click on your profile icon>Account>Security>Login verification. On the same tab you can also choose to require personal information when changing your password.

3. **Be wary of any third party app that requires access to your account:** If you have any doubt as to whether an app is legit or not, don't install it. In order to see which apps do have access to your Twitter account, click on your profile icon and go to Apps. To remove an app, click Revoke access.

4. **Watch out for shortened URLs:** Given Twitter's 280 character limit, it makes sense that lots of people use shortened URLs to link off the platform. The problem is, these make it hard to know where links are taking you, or if it's to a malicious site. So if you want to be really cautious, don't click on links you see posted on other people's tweets.

A good indication that someone has been tampering with your account is if you notice unfamiliar activity, like following someone new or sending out tweets you don't remember. If you do see this, the first thing you're going to want to do is change your password. You should also report it to Twitter. You can do this by going to their help center and submitting a ticket.

You also want to submit a ticket if someone hasn't actually hacked into your account, but has **created a brand new one under your name**. To help Twitter know that you're really you, you'll have the option of uploading an image of a government issued ID or other form of identification.

(https://www.vpnmentor.com/wp-content/uploads/2018/07/WG_1.jpg)

Facebook

Rachel didn't think much of it when during a routine Facebook scroll she clicked that she was interested in attending a concert by one of her favorite bands. But she was excited when one of the members of the band friend requested her and **started sending her private messages**.

The conversation started out casual, but soon he began alluding to her profile picture, telling her that he liked that she didn't care that her nipple was showing.

Wait, what?

Her nipple was definitely not showing. Or was it? Rachel had been **using that profile picture for two years already**, and no one had ever said anything. She enlarged the photo and carefully examined it. Maybe what he saw was the shadow from her top?

She told him he was mistaken, and tried to explain the shadow, giving him the benefit of a doubt that he was just confused. But he was insistent, and **was soon asking for more nude pics**.

In retrospect, Rachel knew she should have stopped the conversation there and blocked him, but at the time it seemed like just a weird misunderstanding. It was *kind of* a provocative photo, wasn't it? **Maybe she should have expected this kind of a reaction**.

She tried to steer the conversation back toward his music and the upcoming concert, but he was like a dog with a bone, and wouldn't let up on his requests for more photos. Finally she just stopped answering, but she felt pretty icky for a few days after, **wondering how others had been viewing her all this time**.

Rachel's story isn't so shocking. It's not violent. No one got raped. It actually sounds like a pretty run-of-the-mill social media encounter. But in fact, it's the banality of it that makes it so depressing. **Every day women get solicited by strangers and end up wondering what they did to cause it,** and have to walk around knowing that while they're just trying to live their lives, others are objectifying them.

Research shows (http://www.pewinternet.org/2017/07/11/online-harassment-2017/) that **the emotional toll these type of interactions take is especially severe for women, who are twice as likely as men to describe their most recent experience of online harassment as very or extremely upsetting**.

And soliciting sexy photos is just one of the myriad forms Facebook harassment can take. Women are regularly sent **abusive messages and unwanted dick pics**, and instances of being tagged in **degrading pictures** or even having **fake profiles** created using their names and photos are far from uncommon.

5 Ways to Protect Yourself on Facebook

1. Control Exactly Who Sees What

In past years Facebook has done a lot to update the platform to allow you to customize these options, even going as far as **letting you hide your info from specific people**.

How to Control What People See on Your Facebook Profile:

On your computer, click the upside down caret on the upper right corner of the page and select settings. On the panel on the left click Privacy. From here you'll be able to manage exactly who can see your posts and how people can contact you.

Next, go to Timeline and Tagging. This lets you control who gets to post on your wall and who gets to see posts you're tagged in. Here you can also change your settings so you get to **review and approve any tags before they get implemented**.

Another cool tool you can use is the one that **lets you see exactly what others see when they look at your profile**. That way you can be sure that certain people won't see sensitive information if you don't want them to.

2. Don't Let Potential Stalkers Know Where You Are

As has been discussed above, tagging your location on posts and photos can be a way for stalkers to find out where you are. On Facebook, when you write a post, you have the option to select Check in, which will add your geolocation for any of your friends to see. It's best not to use this function.

But **Geotagging isn't the only way people can figure out where you are**.

Ever notice how after going to a particular store you suddenly start seeing ads for it on Facebook? Or you meet someone at a party and the next day Facebook suggests them as a friend?

The way Facebook knows to do that is because if you have their mobile app, and you carry your phone around with you (as most of us do) **they know your location wherever you go**.

If you want, you can actually see exactly where Facebook has been tracking you. This information is not public, so you don't have to worry about your average Facebook friend using it to locate you.

How to See Where Facebook Has Tracked Your Location:

Go to Settings. Click Location on the panel on the left, and then click View location history. A map will appear along with with a **log showing your location for as long as you've had location settings enabled. For some, that's going back *years***.

How to Delete Your Location History:

Click on the three bars on the upper right corner of the screen (or lower right if you have an iPhone). Select Account settings> Location. Tap to turn off Location Services, and below, slide left to turn off Location History.

> To delete all your past history, click View your location history and select the three dots in the upper right corner. There you'll have the option to delete your entire history. You'll need to re-enter your password to do this. (Resetting your password is actually another great way to prevent others from accessing your location or your Facebook account in general.)

3. Block Harassers and Put Creeps on Your Restricted List

Another helpful option on this page is to **place particular people on a restricted list**. By putting them here, they'll be listed as one of your friends, but will only be able to see information that you share publicly. This is especially useful if you want to avoid confrontation with someone you fear will try to intimidate or take advantage of you.

Although it's easy to say you should be straightforward and be able to tell someone to their face that you don't want them seeing the personal stuff you post, **we all know how quickly a situation can escalate when a certain type of man feels rejected**.

So next time you meet a guy at a bar who *insists* on friending you *and* watching you accept his request, just slip into the ladies' room for minute and stick him on your restricted list.

4. Report Imposter Accounts

Even though it goes against their terms of service, Facebook estimates that there are currently **66 million fake accounts on the platform**. One reason people create fake accounts is to impersonate other users. By using your real name and photos, **an imposter is able to friend people in your real life social network, and then post harmful and untruthful content about you**.

If you find a fake account using your photos and personal information, you can report it to Facebook and they should take it down.

> **How to Report a Fake Profile on Facebook:**
>
> Go to the fake profile, click on the three dots at the upper right corner of the page, and select Report>Report this profile>They're pretending to be me or someone I know.

That said, **a smart imposter is going to block you so you can't see the fake account**. If they do that, enlist a friend to report the profile for you.

Facebook has also been trying to be proactive in identifying imposter accounts, and has recently announced an initiative that uses its **facial recognition software to flag new profile pictures featuring existing users**.

It should be noted, however, that only new accounts will be scanned, so **if there's already a fake profile of you up, unless you or someone you know finds and flags it, there's no way to catch it**. Moreover, the only photos that will be scanned for your face are those within your friend, or friends of friends network – rather than all the users on the platform.

This calls into question how effective the tactic really is, especially considering how **often profiles are faked not in order to carry out personal vendettas, but instead to scam people out of money or promote products or political agendas**. Specifically, recent probes into the 2016 American presidential election have revealed an entire industry of Facebook activity artificially generated to sway public opinion.

In these cases, one simple way to protect yourself is to **make most of your photos private**. If the person making the sham account doesn't have access to your photos, you'll be a less attractive target for impersonation.

5. Prevent Revenge Porn

In recent years, sexting has left the realm of kink and become a standard mode of flirtation. In fact, according to one study (http://www.apa.org/news/press/releases/2015/08/reframing-sexting.pdf), 88% of the adults surveyed said they had sent sexually explicit messages or images at least once. This isn't necessarily a bad thing; the same study showed a **correlation between sexting and sexual satisfaction**, and found that women often find it particularly empowering.

That said, sending revealing photos can be risky if they get into the wrong hands. Far too many women have found themselves the object of humiliation campaigns, in which **vindictive former partners make their lives hell by sending intimate images to their friends, family members, and even employers**.

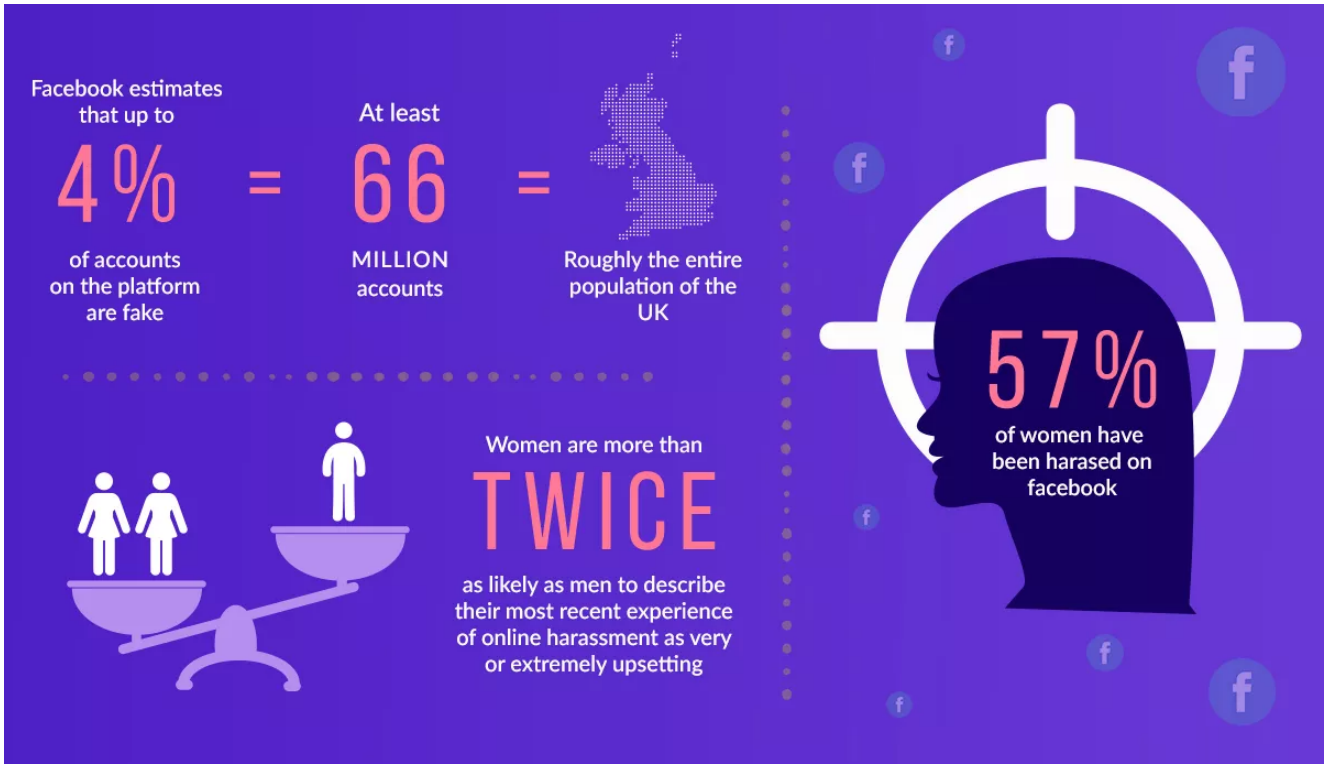
Fortunately, Facebook already has an **algorithm that identifies and removes nude images**. However, in November 2017 they also announced a new, somewhat novel approach to addressing the ugly epidemic of revenge porn. But the idea, which is first being tested in Australia, is bound to raise some eyebrows.

Basically, if you suspect a particular image may be uploaded to Facebook without your consent, **you fill out a form explaining your concern, and then send the image to yourself using the Facebook Messenger app**. After assessing the report and the photo, Facebook will then delete it.

Because Facebook owns Instagram, this will prevent the image from being disseminated there as well.

There are a few issues with this approach. First, you have to know the images are out there in the first place. (Sometimes photos and videos are taken without the victim's knowledge or consent.) Second, you have to have the images in your possession – which may not be the case if they were taken using someone else's camera. And finally, **you have to trust Facebook, and accept that a real person on their end is going to see pictures you explicitly don't want out there for public consumption**.

For many, knowing some anonymous techie has access to their intimate photos, even for a short time, will add to the trauma and anxiety they're already experiencing.



(https://www.vpnmentor.com/wp-content/uploads/2018/07/WG_2.jpg)

Instagram and SnapChat

Photos were not the only thing that changed when Instagram started in 2010 and SnapChat in 2012. Online harassment did too.

By making your photos public, **anyone can comment on your pictures**. Although it's hard to understand why someone would dedicate their time to being a troll, there are those who have a field day searching for photos to insult. Public body shaming comments and DMs (Instagram's version of a private message) with explicit and vulgar language plague millions of accounts every day.

Besides trolling, **many women are susceptible to revenge porn, dick pics, and other non-consensual nude photography**.

With different techniques, you can fight back and even prevent some of these scenarios from happening in the first place. Yes, trolls and jerks will find a way to you if you're persistent enough, but by taking the following steps, you can make it that much more difficult for them.

3 Ways to Protect Yourself on Instagram and SnapChat

(https://www.vpnmentor.com/wp-content/uploads/2018/07/WG_3.jpg)

1. Check Your Pictures for Identifying Data

There are some simple things you can do to make your photos and account a bit safer.

Let's say you're at a restaurant and want to Insta a picture of your dish. It's nice to tag the restaurant because it gives them PR. But, **by tagging this restaurant, you place yourself in that location**.

Any stalker now knows exactly where you are.

Similarly, if you enable geolocation settings, you're even more at risk. If you snap a picture of your caramel latte from Starbucks, you can be at any of the 27,339 Starbucks around the world. But **if your geolocation is on, whoever sees your picture will know exactly where you are**.

Snapchat unveiled a new feature in June 2017 called SnapMap, which shows the locations of all of your friends on a map. While this might seem innocent, it actually let's others keep constant track of your whereabouts. **Turn off the SnapMap feature, and you'll save yourself from a lot of potentially ugly situations**.

2. Don't Use Your Real Information

When you sign up for SnapChat, you are required to provide your birthday, phone number, and email address – pretty standard for social media apps. But **anyone with the slightest bit of tech savvy can then find that information through your SnapChat account**. This makes it extremely easy for someone to take their harassment off SnapChat and onto email, WhatsApp, and plenty of other apps.

The best way to protect your information is to hide it. **Create a new email address to sign up**. Also, use a fake phone number (you know, the one you might give to a creepy guy at the bar who you don't want to call you), and make up a new birth date.

Another simple trick that makes it much harder for trolls to access you is to **change your account from public to private**. This goes for both Instagram and Snapchat. Changing your account to private will limit the people who see your posts to friends, family, or anyone else you choose to approve.

> **How to Make Your Account Private on SnapChat:**
>
> Go to Settings>View My Story>My Friends/Custom. While you're in Settings you can change who can contact you and who can see your location.

> **How to Make Your Account Private on Instagram:**
>
> Go to Settings>Private Account (slide right to enable).

If you need to use these apps to promote a product, your company, or yourself, then create a separate account. This way, your personal photos won't get mixed up with your public photos.

That said, even if you do all that, rude comments could slip through the cracks. In that case, you'll need to know how to…

3. Block Creeps Both Instagram and Snapchat have blocking options. Using this technique, you can block a user and then delete their comments

> **How to Block People on Instagram:**
>
> Select the person you want to block, tap the three dots in the upper right corner, and then click block.

> **How to Block People on SnapChat:**
>
> Select the person you want to block, tap the three lines on the upper left corner, and then click block.

Harassment at Work

Unfortunately, abuse is also prevalent in work environments. According to one study (https://www.cosmopolitan.com/career/news/a36453/cosmopolitan-sexual-harassment-survey/?dom=fb_hp&src=social&mag=cos), **one in three women ages 18-34 has been sexually harassed at work**. 25% of those women were harassed online via texts or emails, yet 71% of these women did not report it.

We can only speculate the reasons for this, but one could be because sexual harassment is not clearly defined.

However, some examples of sexual harassment include:

1. Sharing sexually innaproporiate images or videos.

2. Sending letters, texts, or emails with suggestive content.

3. Telling lewd jokes or sexual anecdotes.

But even these are ambiguous! If someone sends a dick pick, that is clearly sexual harassment, but an off-hand comment could be misconstrued.

So, how do you know it's sexual harassment?

For those moments where you're not sure, think about how you feel. **Did that comment make you uncomfortable?** Is there something off-putting about it? If yes, chances are there's an underlying tone that should be considered sexual harassment.

Sexual Harassment at Work

Sexual harassment comes in different forms, and when it's online it's often even less obvious. Yet, it still happens. If you're in a professional situation where you feel uncomfortable, you should immediately start recording it. **Often larger cases are built on a pattern of small incidents, which, if not documented properly, won't be useful as evidence**.

Even if you're not sure if an encounter counts as harassment, it's better to treat it as such just in case the situation gets worse and you decide to eventually take action.

How to Report Harassment at Work

1. Document Every Encounter

Any comment, inappropriate email, or other correspondence that can possibly qualify as harassment should be recorded and stored somewhere where only you have access to it (not on the company's Google Drive, for instance). It could be that one comment was unintentional, but if it happens again, you'll be able to build a case.

If an encounter involves something said verbally or inappropriate touching, as soon as possible, write yourself an email (from your personal account) describing the incident in as much detail as you can. Include the time, date, and location of the incident.

2. Monitor the Situation

Take screenshots, record times and dates, save emails, and keep a file of everything that makes you uncomfortable.

3. Report It

Once you have evidence, it's time to file a report. While it is sometimes uncomfortable, reporting harassment in the office is one of the most productive ways you can stop it.

Send your evidence to the HR department, which hopefully already has a policy in place as to how to proceed. If there is no HR at your company, then you should construct a well-informed email and send it to office management or to your manager (as long as they are not the one harassing you).

> **How to Write an Email to Report Sexual Harassment:**
>
> It can seem daunting to construct that first email. For this reason, we included a template for you to use.
> Subject line: Official complaint of sexual harassment
>
> Dear [HR] and [boss],
>
> I am writing this email to notify you that [name of harasser] has been sexually harassing me for the past [x amount of time].
>
> The following incidents have occured during that time:
>
> > [Example 1: Describe what happened and when. Try to include as many facts as possible.]
> >
> > [Example 2: Describe the second incident that made you feel uncomfortable. Remember to include if you told anyone else at work about it.]
> >
> > [Example 3: Attach any documents or evidence that will support your case.]
>
> [If applicable, include what actions you believe the company should take. For instance, you can write, "I would like to be transferred to a different department" or "I would like this matter to be looked into, and I would like a formal apology from [name of harasser]."]
>
> Thank you for looking into this matter. Should you need any more information, I am happy to provide it.
>
> Sincerely,
>
> [Your name]

Your office should have a policy on how to assess the situation and take action.

If you don't feel as though your complaint was adequately addressed, remember that **you can always seek outside legal counsel**. A professional well-versed in the laws in your area should be able to guide you in your next steps.

We should also note that for many, **reporting the incident internally is not an option, as many women freelance or are self-employed**. In this scenario, you need to take the situation into your own hands.

Sexual Harassment if You're Self-Employed

If you're self-employed and experience an inappropriate encounter, since there's no one to report to, **you need to take care of the situation yourself**.

This is exactly what happened to Ariel*, a musician who received sexually charged messages from another professional in her industry. After commenting on the way she shakes while playing music, Ariel responded "don't be an ass" to which the harasser responded "Oh, I love the way you talk."

While Ariel decided not to publicly shame him, she did respond that his comments were suggestive and aggressive. The harasser disagreed and left it at that.

Ariel found it empowering to confront the harasser head on. Others may find that the best method of self-preservation is to ignore the harassers. **There's no right or wrong way to address harassment in this scenario**. It is your decision.

Sexual Harassment on LinkedIn

LinkedIn, an online platform for career-networking and business, has unfortunately also become an outlet for sexual harassment. **While LinkedIn's policy prohibits any form of harassment, there's no way for LinkedIn to totally prevent it**, and – unfortunately – sexual harassment still happens there every day.

Because it's a networking site, **some treat it like a dating site**. Among other complaints, women have reported men sending them inappropriate messages, and making lewd comments on their appearance based on their profile pictures.

Another potential pitfall: your resume.

Many people upload their resumes without considering that **their email address and phone number appear in the header**. Unless you want the entire internet to have access to that information, delete it from the version you post.

Unwanted phone calls asking to go out may not seem like sexual harassment to some men, but for women receiving phone calls from strangers, it could definitely feel like it.

But, that's the problem. Because most harassment is not so blatant, it's harder for women to validate and report it. While you can't prevent creepy guys from messaging you on LinkedIn, there are ways you can protect yourself.

4 Ways to Protect Yourself on LinkedIn

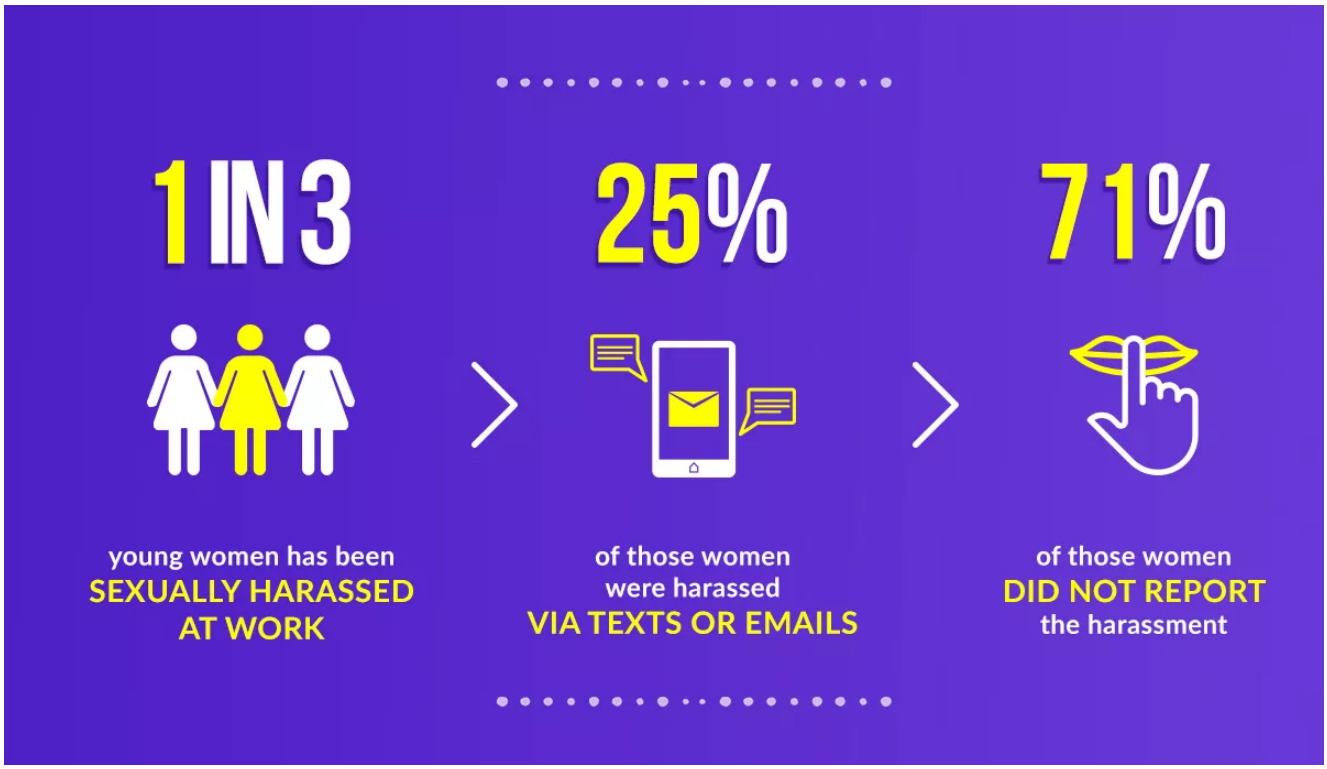
1. Before accepting a LinkedIn connection, check the degrees of separation. Do you have connections in common? Do they work in your industry? If not, don't accept.

2. If you receive an unsolicited message, you can decide to block them. Just click on the three dots at the top right and then click Report this conversation.

3. You can also block that person from viewing your profile or contacting you. Go to the person's profile, click More>Report/Block and follow the instructions.

4. If you upload your resume, check to make sure your phone number, home address, and other contact information are not listed. If someone wants to contact you for your work, they can do it through LinkedIn.

There is no guarantee that these suggestions will protect you 100%. However, they do provide you with more control regarding who can contact you.



(https://www.vpnmentor.com/wp-content/uploads/2018/07/WG_4.jpg)

Online Dating and Sexual Harassment

Kylie* had been chatting with Marco* for about a month after having connected on OKCupid, but they hadn't yet met in person. One night, after over an hour of increasingly flirty texts, Marco suggested that they switch to a more visual forum – he wanted to Skype sex.

The next day, Kylie was horrified when one of her friends called to tell her that she received a recording of the encounter. An hour later, **Kylie got a message from Marco: pay up, or the recording would be sent to even more people in her social network**.

Online dating is where women are most vulnerable to cyber-sexual harassment.

That's because unlike most social networks, **dating sites are where you go with the express purpose of meeting, and potentially getting intimate with strangers**. Whereas on other sites strict privacy settings could serve as a shield, on dating sites those tactics for staying safe would just result in another solitary Saturday night.

While dating apps are supposed to be fun, they've also been known to lead to some pretty unpleasant encounters.

For instance, Esme* met Raphael on the app Happn. After chatting on the app, the conversation moved to WhatsApp, but when Esme checked his profile picture, she noticed Raphael **looked different and his profile did not match the one on the dating app**. Not wanting a confrontation, she told Raphael that she had some personal issues to work out before she was ready to date. Instead of accepting her explanation, he started bombarding her with aggressive questions about where she was and who she was with.

Finally, Esme blocked him and reported him to Happn. Knowing he would seek her out on social media she also blocked him on Facebook, WhatsApp, and Instagram. And when he tried to call her, she blocked his number too. Whether Raphael finally got the hint (unlikely) or simply found it too hard to maintain contact, Esme was able to stop the abuse – but not all women are this lucky.

What happened to Esme is known as **catfishing – or when someone misrepresents themselves online, often using fake photos and profiles**. While Esme was able to clearly see that the person on the Happn profile was different from the person in the WhatsApp profile, most catfishers are smart enough to better hide their tracks.

Similarly, it's pretty easy to **unknowingly become the accomplice of a catfisher**. Take Cori*, for instance. One day she got a call from a friend that **her Facebook profile picture was being used on someone else's dating profile**. Cori reported the fake profile and it was deleted, but who knows how many people saw her face and information before then?

Unfortunately, there's no way to both meet people online and ensure you'll never be a victim. However, there are ways to protect yourself.

3 Ways to Protect Yourself on Dating Sites

1. Do a Background Check

When you first connect with someone online, search them on Google, Facebook, and other dating apps if you're on them. Look for inconsistencies in their pictures and profile descriptions. If you find any, report the profile to your app.

2. Get to Know Them on the App

Chat on the app before moving the conversation to a different platform. This gives you a sense of who they are before exposing further details about your personal life. Once you do feel comfortable enough to move the conversation to another platform, be aware of what they can see there. For instance, both WhatsApp and Telegram allow profile photos, WhatsApp allows status updates, and Telegram lets you write a little bio about yourself. Both apps also have a "last seen" feature that shows your contacts when you were last on the app. If you don't want someone to see any of this information, change your privacy settings. And if you do end up getting together in person, **make sure to meet in a public place, and let a friend know where you'll be.**

3. Keep Your Social Media Accounts and Pictures Private.

This minimizes the chance of someone stealing your pictures and using them on dating sites.

Safe Sexting

Most adults are familiar with safe sex. But what they may not have given much thought to is safe sexting.

This is especially important, since sexting is on the rise. In fact, according to one study (https://www.scientificamerican.com/article/sext-much-if-so-youre-not-alone/), **nearly half of the adults surveyed said that they sext**.

However, the fact that a lot of people do it doesn't mean it's not without its risks. Stories of revenge porn and hacks that have exposed people's intimate photos are commonplace. And it's not hard to imagine how having your nudes fall into the wrong hands could devastate your professional and personal life.

The easy answer would be to tell you to stop sexting, but we're not going to do that. **Sexting can be a fun and fulfilling part of your relationship or dating life**, and we're not here to deny you a good time.

What we are going to do is give you some easy tips on how sext safely. Some of these may seem like common sense, but **we're also going to get into some high tech hacks so you can relax while your smartphone gets steamy**.

7 Ways to Protect Yourself While Sexting

1. Don't Include Your Face or Other Identifiable Features

Your first line of defense if your photos go public is plausible deniability. That means making sure your pics don't include your face, unusual birthmarks, or tattoos.

2. Don't Drunk Sext

You may be feeling frisky after a couple of margaritas, but that doesn't mean it's the best time to unbutton your top and bust out your camera.

Fortunately, there are several apps available that can prevent morning after regrets. For instance, **Drunk Locker is a really comprehensive app for when you know you're going to be partying**. Besides finding you a designated driver, it can also **block certain contacts** so you can't get in touch via calls, texts, and social media.

3. Make Your Photos Self-destruct

The app **Disckreet is specifically designed for sexting**, and requires that both the sender and the receiver input a passcode in order to see a sent image. The main benefit Disckreet offers is that it **allows you to delete you images from the phone of the person you sent it to**. That said, there's nothing stopping the person receiving your photos from taking a screenshot and saving them.

An app that somewhat gets around the screenshot issue is the popular **SnapChat, which automatically deletes photos a few seconds after they're opened**. Although SnapChat allows screenshots, it'll send you a notification when one is taken. That said, it's not a perfect solution, because a little Googling provides several ways to bypass the notification – so it's still possible for someone to save your photo without you knowing.

Confide, a well-encrypted app that automatically deletes messages and photos, **doesn't allow receivers to take screenshots**. But again, if someone is really committed to saving your nudes, they'll find a way.

4. Password Protect Your Phones and Photos

To ensure that no one accidentally gets an eyeful when scrolling through your or your partner's phone, both of you should protect your phones with passcodes.

You can also download an app that will **keep your sexy photos in a seperate, password protected folder**. Some options are KeepSafe and Gallery Lock. One of the cool things about Gallery Lock is that you can choose to keep the icon hidden, so others won't realize it's on your phone. Plus, if someone repeatedly tries to login and fails, the app will take their picture.

Be aware, however, that **not all these apps provide encryption**, meaning you could be at risk of having your photos hacked.

5. Securely Save Your Photos

If you happen to snap a pic that makes your butt look like the work of art you know it to be, you may opt to save it rather than have it self-destruct. In that case, it's better to **store it on a desktop**, rather than a mobile device, which is more likely to get lost or stolen.

Bear in mind though, even on a desktop it's possible to get hacked. Therefore, you should **save your sensitive photos in an encrypted file**. VeraCrypt is a free open source program that allows you to encrypt individual files on either your Mac or your PC.

Bear in mind though, that once your photos are in an encrypted folder, **you still need to permanently erase them from your computer**. It's not enough to put them in the trash and then take out the trash.

Until that data is overwritten by new data, it still exists and can be found by an enterprising hacker. Fortunately, there's software out there to permanently delete files. For Windows, one of the most popular free options is Eraser, and for a Mac you can use Permanent Eraser.

6. Don't Sync Your Photos

If you have an Android, it's likely that your photos get automatically saved to to Google Photos, and if you have an iPhone, they get saved to the iCloud.

You may recall the infamous iCloud hack of 2014, in which the **private photos of several (mostly female) celebrities, including Jennifer Lawrence and Kirsten Dunst, were leaked** following a phishing attack. Since you don't want that happening to you, you're best bet is to **keep your sensitive photos off the cloud**.

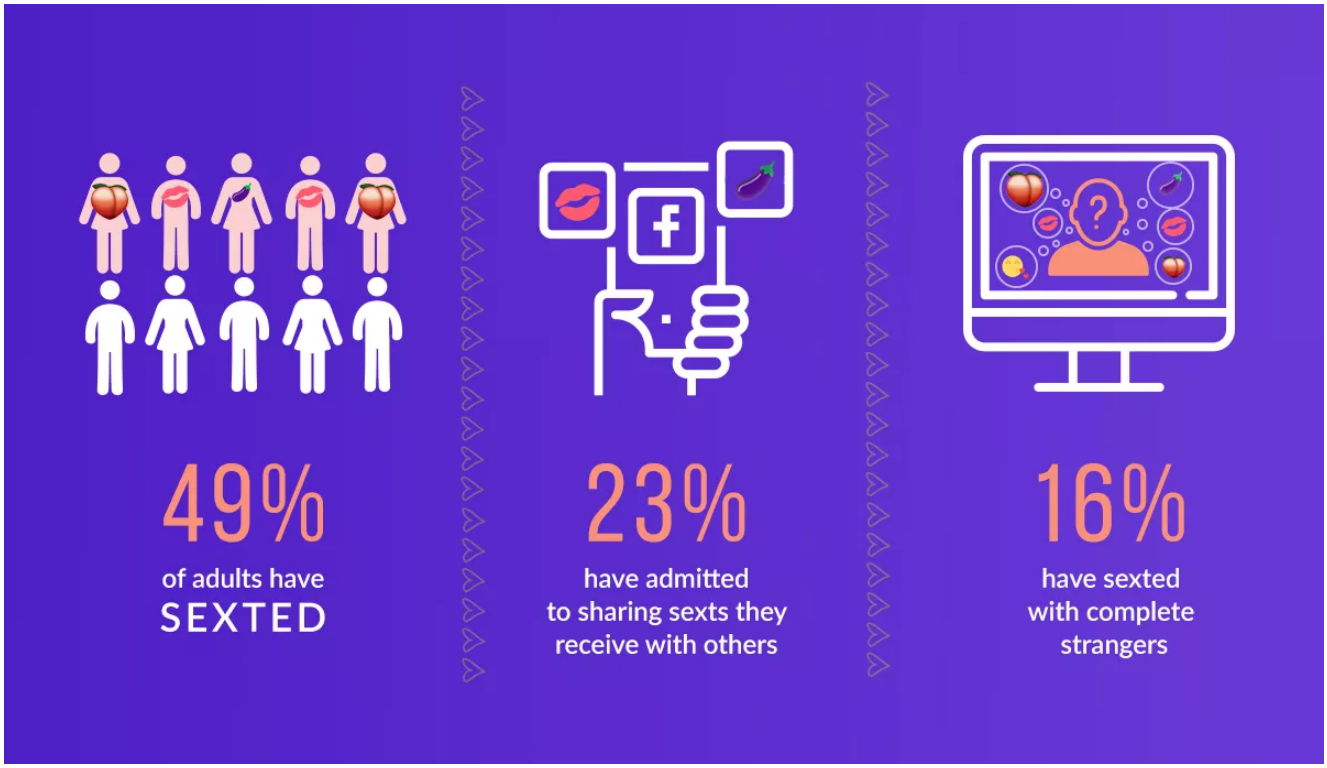
That said, we don't recommend disabling automatic syncing, since that can lead to your losing your info in the event that your phone gets lost or stolen. Instead, you should log into Google Photos or iCloud and **delete them individually**. Be aware though, that **if you have**

automatic syncing on, this could result in the photo also being deleted from your phone the next time it syncs. So if you want to save the photo, back it up somewhere else – preferably in an encrypted folder (see above).

7. Don't Send Pictures to People You Don't Trust

We know, this seems really obvious, but with **16% of people reporting having sent sexts to complete strangers** (https://www.scientificamerican.com/article/sext-much-if-so-youre-not-alone/), it's worth emphasizing.

Not sending potentially compromising photos to someone you're not sure about is especially important, since as you may have noticed from this list, **there's no condom for sexting, so there's no way to stay totally safe**. So take the precautions you can, and choose your sexting partners wisely.



(https://www.vpnmentor.com/wp-content/uploads/2018/07/WG_5.jpg)

IRL (In Real Life) Attacks

Obviously, attacks on women don't just happen online. Often attacks spill over to the real world, with perpetrators using technology to help them stalk and abuse their victims. In fact, a survey (https://static1.squarespace.com/static/51dc541ce4b03ebab8c5c88c/t/54e3d1b6e4b08500fcb455+2014.pdf) of victim aid providers revealed that 79% dealt with victims who had been surveilled using social media.

Sometimes perpetrators are people we know, like **a controlling partner**. Other times, **attacks are crimes of opportunity**, like stealing a cell phone, or taking advantage of someone who's simply in the wrong place at the wrong time.

In any case, from giving a friend the heads up as to where you'll be, to encrypting the data on your mobile devices, to keeping your passwords secure, there are precautions you can take to keep yourself safe.

How to Safely Use a Ridesharing App

Back in 2014, a woman in New Delhi was raped by her Uber driver. After it was revealed that the driver had a decade-long criminal record that included sexual assault, some were calling for the ridesharing app to be banned altogether.

After a slew of bad press, Uber now has a new CEO at the reigns. And **it looks like the company is finally ready to take passenger safety seriously** by rolling out some new initiatives.

The main one that has already been implemented allows you to share your ride with up to five trusted contacts. This means **your friends can follow along during your trip and see that you arrived at your destination**. If you want, you can also set the trusted contacts feature so that it's only enabled for nighttime rides.

Trusted contacts is similar to Lyft's Send ETA feature, which allows you to send your route and estimated time of arrival to a friend. **For both Uber and Lyft, these messages include the car's make and model, the license plate number, and a photo of the driver**.

Uber also has a **911 feature** in the works that will allow you to call emergency services with a click of a button, and which **automatically provides them with your location in real time**. Other initiatives that Uber is planning include driver background checks and scans of new DUI and criminal offenses that can be checked against their list of drivers.

In the meantime, here are a few steps you can take yourself in order to stay safe.

5 Ways to Protect Yourself While Using a Ridesharing App

(https://www.vpnmentor.com/wp-content/uploads/2018/07/WG_6.jpg)

1. Make Sure You're Getting into the Right Car

Before hitting the road, check the car's license plate, make and model, and the driver's name and photo to make sure everything matches up.

2. Don't Let Your Driver Know if Your Pick-up Point or Destination is Your Home or Place of Work

In fact, if it is, you might want to make a little small talk so you can slip in a white lie to make him think otherwise. For instance, if he asks how you're doing, you can say "great, excited to be going out to meet friends." Another option is to give a nearby location as your destination, rather than your exact address, and walk an extra block.

3. Check the Driver's Reviews

One nice feature of ridesharing apps is they allow riders to rate their drivers. If yours has bad reviews, cancel the ride and call another one. To keep from having to wait too long, have a couple of apps already installed on your phone so you can use the one that'll most quickly get you a reputable driver.

4. Track Your Route

If you're familiar with the area you're traveling in, you'll notice if the driver is going the wrong way. But if you don't, open the map app on your phone and track your route to make sure you're headed toward the destination you requested. If the route looks strange, speak up.

5. If Something Doesn't Feel Right, Get Out

Yes, you may be late for your appointment, and you may be out a few dollars, but if you feel unsafe, ask the driver to pull over and get out of the car. **Too often women put themselves in unsafe situations because they think following their gut will lead to awkwardness**.

Screw that.

What to Do If Your Phone Gets Lost or Stolen

(https://www.vpnmentor.com/wp-content/uploads/2018/07/WG_7.jpg)

For many of us, it's as if our whole lives are on our phones. Our phones contain our contacts, our photos, and the apps we use to navigate, keep up with the news, organize our work and personal schedules, and stay connected with friends and family; it's **a lot of personal information we don't want in the hands of some stranger**.

Fortunately, there are a few simple steps you can take to protect yourself if your phone gets lost or stolen.

4 Ways to Protect the Contents of Your Phone

1. Password Protect Your Phone

In order to keep someone from immediately gaining access to the contents of your phone once it's in their possession, it's best to already have a password set.

> The exact way to set a password will vary depending on your device, but for an Android, you'll probably have to go to Settings>Security>Screen lock type. Here you can choose to unlock your phone by using a pattern, pin, or password.

A password is the most secure option, but it's also the most annoying to have to input every time you want to glance at your Facebook notifications. You might also have the option to set your phone so it will only open with your fingerprint.

Another cool feature is the smart lock. If you use this, your lock function won't kick in while your phone is on you, if you're at certain locations (e.g. your home), or if you're near other trusted devices. Some phones will even give you voice and facial recognition options.

2. Locate Your Phone

One of the great things about having a GPS on your phone is that if it goes missing, you can track where it is. However, **in order for this feature to work, you need to set it up in advance**.

> If you have an Android, you have a couple of options. Some devices, like Samsung, have this feature built in – although in order to access it you have to create a Samsung account. By enabling the feature, you'll be able to locate your phone by going to https://findmymobile.samsung.com/ (https://findmymobile.samsung.com/) from a different device and logging in. Another option is to download the **Find My Device app from the Google Play Store**. This app works the same way as Samsung's and only requires you to have a Google account. Plus, if you've just misplaced your phone somewhere around the house, it has the ability to make it ring, even if your phone is set to silent. Just go to https://myaccount.google.com/intro/find-your-phone (https://myaccount.google.com/intro/find-your-phone), sign in, and you'll be able to see your phone's location on a map. From there you'll also be able to reset your phone's password.
>
> Bear in mind, however, that if you have an Android, **you'll only be able to locate your device if your location services are enabled and you're connected to the internet**. A smart thief will know to disable those functions so you can't track where he – and your phone – are.
>
> **If you have an iPhone, you'll need to download the Find My iPhone app**. Once it's installed, you'll be able to locate your device on a map by going to https://www.icloud.com/#find (https://www.icloud.com/#find) and signing into the iCloud.
>
> There you can also put your phone into Lost Mode, which will lock it. Lost Model also lets you set a message to the locked screen, so if your phone is simply lost, you can write something like, "Lost phone. Please call 212-555-1234 to return." Or, if you know your phone has been stolen, you can write something like, "You suck."

3. Erase Your Data

This is the nuclear option. If you're sure you're not getting your phone back, you can **use the Find My Device/Find My iPhone apps to remotely erase all the data on your phone**, so even if the thief manages to break through your password protections, they won't be able to access your personal information.

Bear in mind that when you do this, since all your personal accounts will be deleted, **you lose your ability to track your phone remotely**.

That said, your phone could still be getting service from your wireless carrier, meaning whoever has it could be making calls from your number and using your data plan. To cut them off, **call your service provider and let them know your phone has been stolen**.

Knowing you might have to one day erase your phone data is another great reason to **backup your phone's contents** (which you should really be doing anyway). If you have an Android, the easiest way to backup your data is to use the Google cloud. If you have an

iPhone, use the iCloud.

But what if you didn't have the foresight to install the Find My Device/Find My iPhone apps, and now you can't change your passwords, lock your phone, or erase your data remotely? In that case you should…

4. Change the Passwords for All Your Apps

Make a list of all the apps you have on your phone that require passwords, get onto another device, and start changing your passwords. This will likely include your email, social media accounts, bank accounts, and app stores.

Staying Safe on Meetup.com

One of the amazing things about the internet is that it can bring together total strangers who have something in common, but would never have found each other otherwise.

A great way to do this is through the website Meetup.com, which lets users **create and join events and activities based on themes that interest them**. Popular categories for meetups include film, health and wellness, LGBTQ, and pets. It's a fantastic way to make new friends and cultivate your interests.

But didn't your mom always tell you not to talk to strangers? Was she really onto something, or just being paranoid?

A little of both. You should absolutely get yourself out there and take a big bite out of life… but also, take some precautions.

3 Ways to Protect Yourself on Meetup.com

1. Don't Include Too Much Personal Information in Your Profile

Be aware that your profile page is completely accessible to anyone with internet, so only include information you're comfortable being totally public.

If you have a passion for food, and can't wait to find culinary meetups in your town, definitely mention the new taco truck you're totally obsessed with. But don't say it's located right outside your building on 333 Main Street, where you live in apartment 4D – which by the way doesn't have a deadbolt.

Or if you're looking for family meetups, go ahead and write that you have a ten year old and six year old, but don't include that their names are Timmy and Sue, and that they go to Lincoln Elementary, from which they usually walk home alone at 2:30 pm.

2. Get to Know People IRL Before Communicating One-on-one

Meetup has an email forwarding system, so you can get messages from members sent to your email without them having your actual email address.

But even so, if you're just not interested in people contacting you before meeting and hitting it off in real life, **you can choose to block messages from users** and only receive messages from event organizers. Just go to your account and click Settings>Privacy.

From there **you can choose whether you want your groups or interests listed on your profile**. You can also select who can contact you on Meetup – whether that just be organizers, members of your meetups, or anyone on the website.

3. Let a Friend Know Where You're Going

For any situation in which you're going out to meet strangers, it's good practice to tell a friend where you're going, and set a time to check in with them so they know you got home safe. Also, **if the meetup involves drinks, never leave yours unattended**.

Preventing Intimate Partner Violence

Intimate partner violence (IPV) affects nearly one third of American women. Although technology can provide tools for victims (e.g. for collecting evidence against an abuser), it can also unfortunately be used by perpetrators. That's because control is an integral element on IPV, and **the misuse of technology can give abusers a means of exerting control over their victims**.

According to a recent study (https://www.ipvtechresearch.org/pubs/spyware.pdf), while many perpetrators use technology specifically designed for surveillance, it is far more common to repurpose other types of apps in order to achieve the same goals. Some of those used include **find my phone apps, and family tracking and child monitoring apps**.

The problem with this is that advocates against IPV can't go after the companies that manufacture these apps, and app stores can't block them, as most of the time, they're used for perfectly legitimate purposes.

Many of these apps allow abusers to **track their victim's location, read their messages** by having them forwarded to a different device, and even **watch and listen to them remotely** by activating the phone's camera and microphone.

As mentioned above, there are also **apps explicitly marketed for nonconsensual surveillance**. While it's rare to find these in a legitimate app store, there are plenty that can be found in other corners of the internet. And even though most phones come with a default setting that blocks off-store apps, guides for overriding it can easily be found online.

One of the most nefarious elements of these type of apps is that they can usually be configured so the app icon is hidden, thus making it **nearly impossible for the victim to detect it on their phone**.

You might think the solution would then be to scan the phone for spyware, but unfortunately, even some of the biggest names in the industry, such as Symantec, Kaspersky, and Avast, have proven largely ineffective at detecting these apps.

So what can you do to protect yourself?

3 Ways to Keep an Abusive Partner from Surveilling You

1. Keep Your Phone on You at All Times

Almost all the apps studied require that the abuser physically have access to the victim's phone at least once.

2. Be Cautious Using Any Phone You Didn't Obtain Yourself

Abusers with a lot of control over their victims often control their money too – and so end up being the ones to purchase their phone. In these cases not only can they pre-install dual purpose apps, but with a little tech savvy, they can can even root the device, giving them the ability to install the most nefarious off-store apps. There are even companies that will sell phones that are already rooted, or that have surveillance software pre-installed.

3. Password Protect Your Phone, and Don't Share Your Password with Anyone

As mentioned above, having a password to keep your phone locked is the first line of defense in keeping its contents secure. If you suspect your partner is accessing your device, immediately change your password. Make it long and complex, and make sure not to use elements they might be able to guess, like your birthday or pet's name.

That said, we're not naive, and can't ignore the reality that **many victims of IPV are coerced into revealing their passwords** or "allowing" these dangerous apps to be installed on their phones.

Whether or not you're in the position to safeguard your device, **if you are the victim of IPV, there are resources that can help you get out**. These are just a few of the organizations that have made helping victims their mission:

National Network to End Domestic Violence: https://nnedv.org/ (https://nnedv.org/)

The National Domestic Violence Hotline: 1-800-799-7233, http://www.thehotline.org/resources/ (http://www.thehotline.org/resources/)

Family and Youth Services Bureau: https://www.acf.hhs.gov/fysb/resource/help-fv (https://www.acf.hhs.gov/fysb/resource/help-fv)

SOS Apps

In general, it's a good idea to have an emergency app on your phone, just in case. These let you **notify friends or family when you're feeling unsafe**, and/or **contact emergency services**.

Some types of phones have these features built in, so it's worth checking to see if yours does. If not, check out these apps, all of which are available for both Android and iOS.

1. ICE (https://play.google.com/store/apps/details?id=com.lagache.sylvain.ice_android&hl=en), which stands for In Case of Emergency, allows you to **send a message and your GPS location to selected contacts** when you want your friends or family to keep tabs on your whereabouts. **You can also set the message to be delayed**, so say, if you don't come back from your hike by nightfall, that's when they'll get the message.

2. React Mobile (https://itunes.apple.com/us/app/react-mobile-safety-app/id522851588?mt=8) does the same thing as ICE, but also has an SOS Help Me button that notifies your pre-chosen contacts via email and text, and if you choose, **posts a message to Facebook and Twitter**. At the same time, the app **automatically contacts local emergency services**.

1. Siren GPS (https://www.sirengps.com/) won't contact your friends and family, but with a push of a button, will alert emergency services and provide them with your location. You can also **set up a personal profile with relevant information that is then passed on to the authorities in case of emergency**. This can include medical conditions and emergency contact info. The app also gives you the option of calling the fire department, an ambulance, or the police.

You can also **show certain information on your lock screen** to be used in case of a situation in which you're unable to give information about yourself to emergency services. For instance, you can write something like, "In case of emergency, call [name of your partner]" and then write their phone number. Or, if you have a specific medical issue – like a severe allergy or epilepsy – you can include pertinent information there.

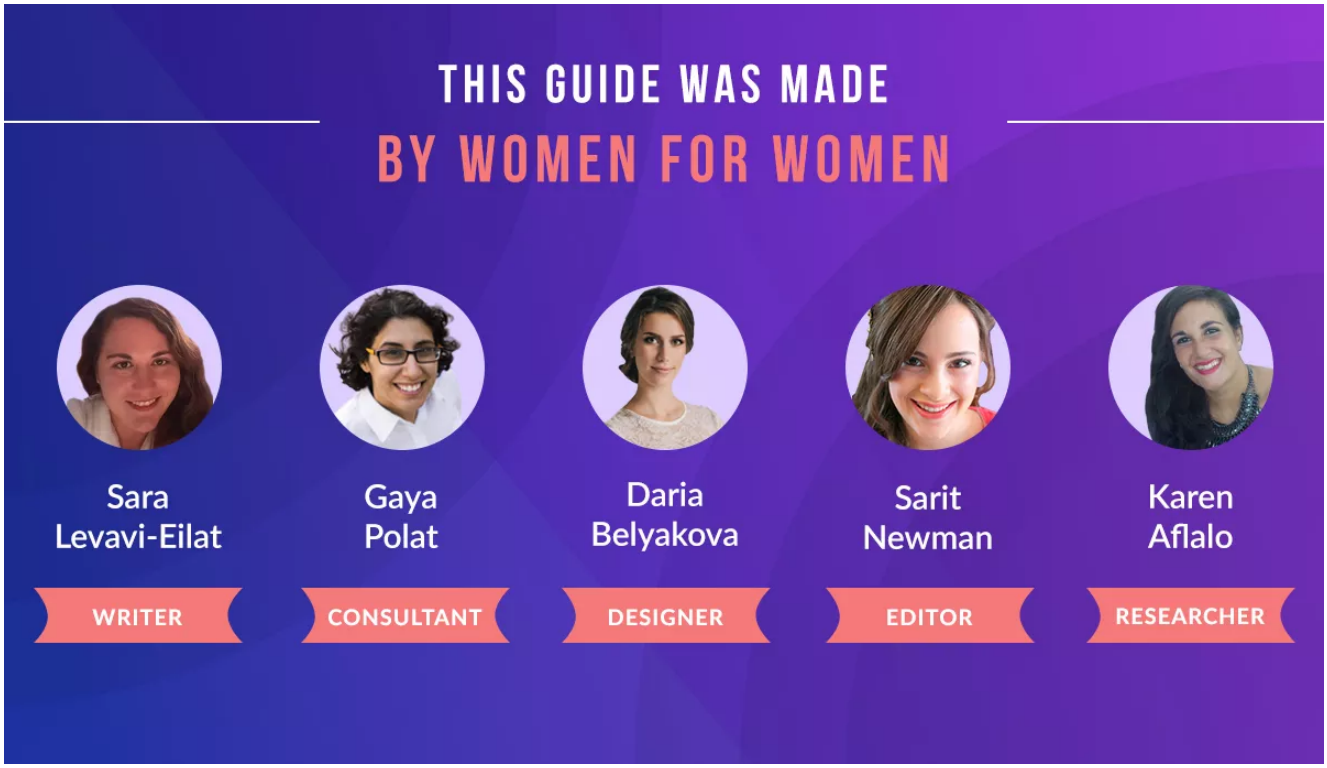
How to set a lock screen message will vary depending on what model phone you have.

Conclusion

Technology and the internet play a big part in our lives both in good ways and in bad. As women, we are targeted online for many different reasons, but that does not mean we should disengage or disconnect.

Our hope is that this guide empowers you to protect and defend yourself online and in person and that the tools we provide will help you to do so.

If you found this guide helpful in any way, please share it with others (https://www.facebook.com/sharer/sharer.php?u=https%3A//www.vpnmentor.com/blog/the-empowering-internet-safety-guide-for-women/) so more women can learn how to stay safe, both on and off the web.



(https://www.vpnmentor.com/wp-content/uploads/2018/07/WG_made_by_10.jpg)

* Some names and identifying details have been changed to protect the privacy of individuals.

Feel free to share (https://www.facebook.com/sharer/sharer.php?u=https%3A//www.vpnmentor.com/blog/the-empowering-internet-safety-guide-for-women/) and copy this post or parts of it to your site, blog, or social networks. All we ask is that you attribute it to vpnMentor.com.

Was this helpful? Share it!

Share on Facebook

0

Tweet this

14