

How to Protect Yourself Online When Your Personally Identifiable Information Is Leaked

While no one wants to think about having their personally identifiable information exposed, it's important to know what to do if this situation ever arises.

While no one wants to think about having their personally identifiable information exposed, it is important to know what to do if this happens to them. Acting as quickly as possible is the best way to protect yourself and possibly even prevent it from happening to someone else.

Record everything

The first step is to document any evidence that your personally identifiable information has been exposed. You will need evidence to provide to law enforcement. The more information you have, the better. Document any personal information that has been publicly posted about you and where. Then, compile any threats and harassment associated with that information.

Revealing personally identifiable information is not illegal everywhere. However, using someone else's personal information for blackmail is illegal. Additionally, harassment, malicious threats, identity theft, and other crimes involving the disclosure of someone else's information are illegal. So don't just take it personally. Document the evidence and then report it.

Report any breach of personally identifiable information immediately.

Almost every website prohibits the disclosure of personally identifiable information in their terms of service. You'll find that many sites even have a section that explains what to do if your personally identifiable information is disclosed, including how to report the incident to them, including the social media platform.

Once reported, the sites are supposed to immediately delete any personally identifiable information, such as your address, phone number, social security number, etc. They are also supposed to ban users who reveal other people's personally identifiable information. Sure, determined individuals can get around this, but at least the sites are trying to protect you as much as possible.

Don't stop at reporting the disclosure of personally identifiable information to the site where it occurred. Report it to local law enforcement. This is especially true if you receive any threats. If you are in immediate danger, report it to the police immediately.

Notify friends and family

If you've been targeted, your friends and family may be next. It's not uncommon for identity thieves to target people close to you. This is another way to threaten and harass you.

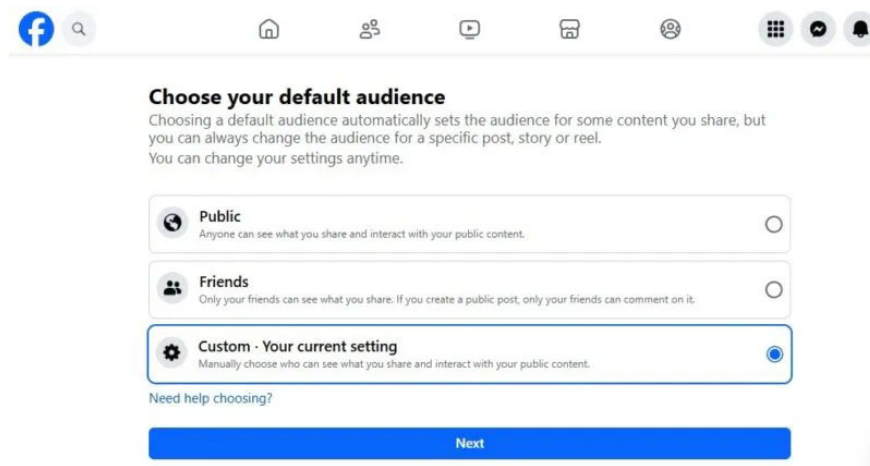
Giving them advance notice helps them better protect themselves. This includes going through the same processes as you.

Social Network Lock

Social media has made it more common for personally identifiable information to be exposed. This is because we share so much of our personal information without thinking about how it could be used against us. On top of that, hackers who gain access to your account also have access to information that you haven't made public, such as your phone number and home address.

Always make sure you never share certain types of information on social media. You can even keep yourself fairly private on WhatsApp .

Immediately make all social media profiles private and change your passwords. As mentioned earlier, report the exposure of personally identifiable information to the platform so they can remove the information and ban the user responsible.



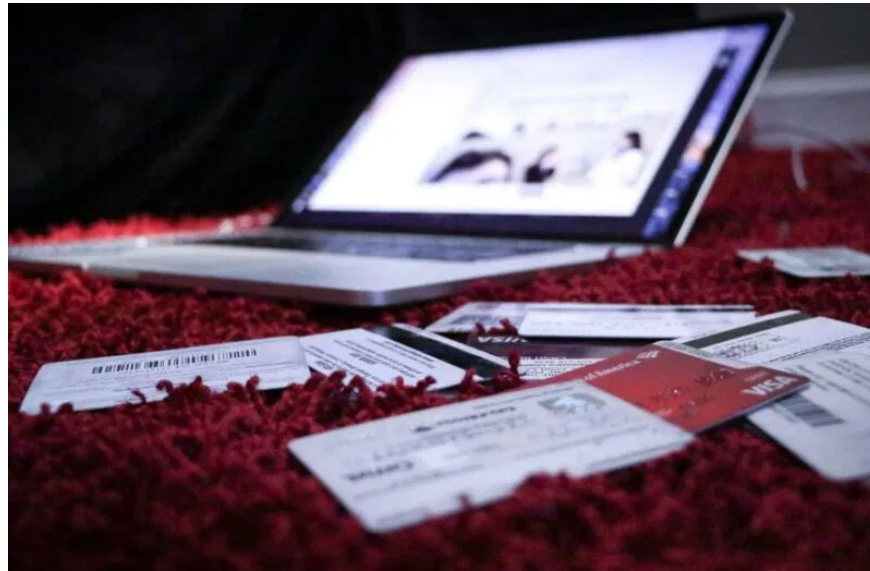
If the platform doesn't ban the user, block them. Post information about the leaker so all of your followers and connections can block them too.

If the problem persists or the hacker gets back into your account, delete everything, including your personal photos. While most platforms, like Facebook , won't delete your account for at least 30 days after you request it, immediate deletion is often granted in cases where personally identifiable information has been exposed.

Change all passwords

If someone collects personal information about you that isn't easily accessible online, assume they also have details about any websites you have accounts on, including financial and shopping sites. While it's annoying to have to change passwords for multiple sites when you're already racking your brain about what to do if your personally identifiable information is exposed, locking it down will help keep you safer.

If any financial information has been exposed, including credit card information, contact your financial institution. They will help you cancel your credit card and get a new one with a new number. You should also freeze your credit report through Experian, Equifax, and TransUnion to help reduce the risk of identity theft. It's free and you can unfreeze it at any time. Experian provides detailed information on how to do this on all three websites.



You should also monitor your credit report for any unusual activity. Many places offer free credit monitoring services.

Request Google to remove content

Since Google is the first place most people think of to search, search for yourself on Google. Keep track of where your personal information appears. But if it's not public information, you can send a takedown request to Google to have it removed.

Google provides a variety of categories and procedures for removing specific types of information. Record the information you want removed and why. The more detailed your request, the more likely Google is to take action. Depending on the site, Google may even remove the site itself from search results.

Report a problem

* Required field

Request personal content removal from Google Search

Google's [personal content and product policies](#) apply wherever you are in the world, but we also have processes in place to remove or restrict access to content based on local laws. To remove content based on a specific legal reason—including, but not limited to copyright infringement, trademark violations, or a court order—create a request through the [Legal Help Center](#).

You may report the same content through both legal and content/product policy reporting paths, but you must file each report separately. Reporting content through a content/product policy path does not substitute for reporting it through a legal path and does not serve as legal notice.

Why are you requesting personal content removal from Google Search? *

- Content contains nudity or sexual material
- Content contains your personal information
- Content is on a site with exploitative removal practices
- Content shows a person under 18

Your country of residence *

United States

Remember, this only removes the information from search results, not from the site itself. Reputable sites will remove the information, but unreliable sites will not.

Consider a Content Removal Attorney

If the exposure of personally identifiable information begins to damage your reputation or tracking down content becomes impossible, consider contacting a content removal attorney who not only specializes in tracking and removing harmful content online, but also advises you on your legal rights.

Whether you are a business or an individual, these attorneys can help minimize damage to your online reputation while protecting your identity. They can also ensure you have all the evidence you need to pursue legal action.

While it is difficult to completely prevent the exposure of personally identifiable information, at least you know what to do if your personally identifiable information is exposed so you can take immediate action. Prevent the exposure of personally identifiable information by sharing as little information about yourself online as possible. Also, block webcams in your home, as they can provide a leaker with more information about you. This includes protecting your speakers and personal assistant screens.

You finished reading the article "**How to Protect Yourself Online When Your Personally Identifiable Information Is Leaked**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.