How to Securely Leak to the Press

In times of political or social strife or upheaval, you may have information that needs to be revealed to the public. Sometimes you can't talk openly about the information you have without risking government persecution, losing your job,...

Method 1 of 4:

Using Encryption Services

1. 

Research the news organization. Different news organizations use various apps that allow citizens to send them information in a secure and anonymous way. If you already have a news organization in mind that you want to use, find out what service they use.[2]

1. You typically can find this out by checking the news organization's website. Don't use a work computer or search from your own home. Go somewhere with free public Wi-Fi and do your research there so there's no trace of you having visited that news organization's website.
2. On the website, search for "leak" or "tip" or "source." One of these words should get you to the page that you need.
3. For example, you can find information about how to leak to the Washington Post by going to https://www.washingtonpost.com/securedrop/. The landing page for leaks to the New York Times is located at https://www.nytimes.com/newsgraphics/2016/news-tips/.

2. 

Download the appropriate app. Some news organizations use a free mobile app, such as Signal, to send and receive encrypted messages and phone calls. If you need to talk to a journalist, you may be able to use one of these apps.[3]

1. You typically cannot send documents through these services, but you can talk to journalists or send and receive messages regarding document delivery, or other information.
2. If the service requires you to add the journalist to your phone's contacts before you can communicate with them over the app, add them under a fake name.

3. 

Go through SecureDrop. SecureDrop is an online document transfer service used by more than 20 news organizations. This service allows encrypted, anonymous documents to be transmitted from sources to journalists.[4]

1. You also can communicate with the journalist, and they with you, by typing a document and sending it. Once the document has been sent, you can reply from within the service.

2. SecureDrop only operates on the Tor browser, so you'll have to download that. The process is the same as downloading any other app, and the browser operates just like any other web browser.
3. Make sure your security settings are set to the highest level before you start using SecureDrop for communications.
4. 

Stick to public Wi-Fi. Even though these encrypted services ensure that the information you send can't be opened or read, there may still be a record of the contact itself. For that reason, avoid using the Wi-Fi at home or work, since that can be traced back to you.[5]

1. Find a café, library, or another public place that has open Wi-Fi available. Go somewhere on the other side of town, or that isn't located in a place near your work, school, or any other place you frequent on a regular basis.
2. If you have to communicate more than once, don't go back to the same place – find a new location for each communication.
3. If you have to spend any money to get to the location, use cash. Credit or debit cards can all be traced back to you and put you in that location. Leave all electronic devices at home, since they also can be traced.[6]
4. As far as transportation is concerned, walk if possible. Do not drive your own car. If you need to use public transportation, get off several stops before your destination and walk in the opposite direction, then circle back. You may want to take several forms of transportation. Avoid taxis, and avoid areas with modern surveillance cameras.

Method 2 of 4:

Leaking by Email

1. 

Buy a dedicated computer. If you've decided to send a regular email, you'll have to spend a little money to make sure the information cannot be traced back to you. Your first purchase should be a computer or tablet that you will only use to communicate with the journalist to whom you're leaking information.[7]

1. It doesn't have to be a fancy computer – a cheap machine running Windows is sufficient. Buy a new machine, not a used one, because you don't know what's on a used one. This machine shouldn't set you back more than a few hundred dollars.
2. Get the information or data you need onto the computer, but do not email yourself anything from your own work or personal email address, and don't log onto any of your personal accounts on this computer. If you do, the computer can potentially be traced back to you.
3. Do not access your home or work Wi-Fi network using this computer.

2. 

Enable full disk encryption. Almost all newer personal computers provide you the ability to encrypt all information on the hard drive with a few clicks. Once enabled, no one will be able to access any

information stored on your hard drive without your username and password.[8]

1. On a Windows machine, enter "encryption" from the start menu and select "change device encryption settings." Choose the "Manage BitLocker" option, turn on BitLocker, and follow the instructions from there to set it up.[9]
2. On a Mac, click on "Security & Privacy" from your system preferences. Choose the FireVault tab and unlock it with your username and password so you can update your preferences. Then turn on FireVault and follow the instructions.[10]
3. If the dedicated computer you bought does not have an option for full disk encryption, you also can download software that will do this for you. Download a free program such as TrueCrypt or DiskCryptor.

3. 

Find a location with open Wi-Fi. To securely leak to the press using email, go to a café or other place that has open Wi-Fi available to the public. Look for a location that isn't in an area you normally frequent, and don't go to the same location more than once.[11]

1. Once there, turn the Wi-Fi on the computer and connect to the network. Don't bring any personal devices with you, because they can be traced and you don't want them to show that they've accessed the same network.
2. Both on the way to the location and once you get there, use cash to pay for any purchases you have to make – do not use your own credit or debit cards, even a prepaid card, because they can be traced back to you.

4. 

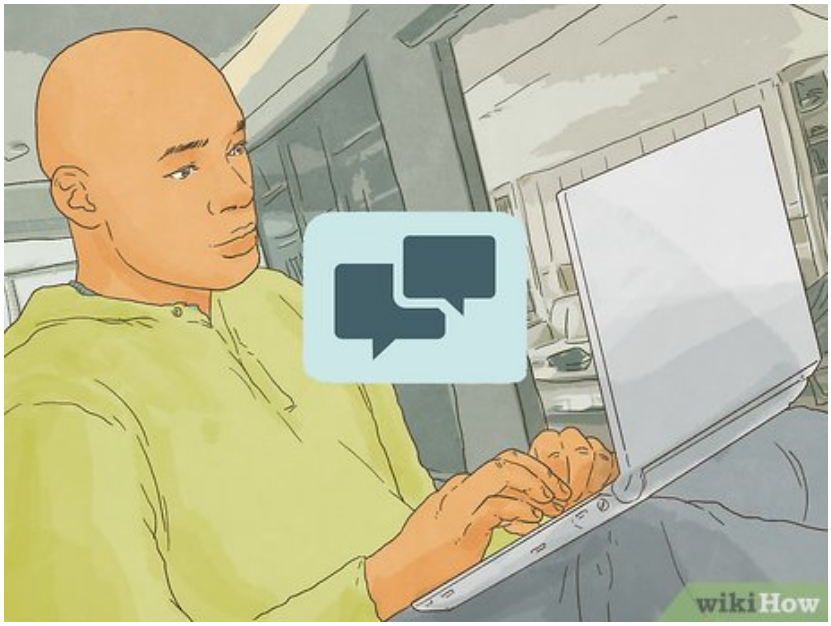
Set up email encryption. Encryption can be set up on any computer and protects your information and data from being read or understood by even the most sophisticated government surveillance technology. [12]

1. You can install encryption software within your email service, as well as on the computer as a whole. Once encrypted, the information is scrambled and cannot be read unless the person has the right key to decrypt it.
2. "Pretty Good Privacy" (PGP) is a free encryption service for emails. Go to the PGP website at http://www.pgpi.org/ and download the latest version of the software for your computer. Save the file to your computer, then unzip and install it.
3. Follow the prompts on the installation screen to finish setting up PGP. You will then be prompted to restart your computer to complete the installation. Once PGP is running, no one can read emails you send without the proper key to decrypt them.

5. 

Create a new email account. You don't want to email the journalist from a personal or work email account. A free account from a service such as Gmail will work just fine. Avoid using any name that can be connected to you.[13]

1. The best email address for purposes of anonymity is a series of random letters and numbers.
2. Do not use a personal email address or any email address that can be traced back to you, as a "recovery" email address.

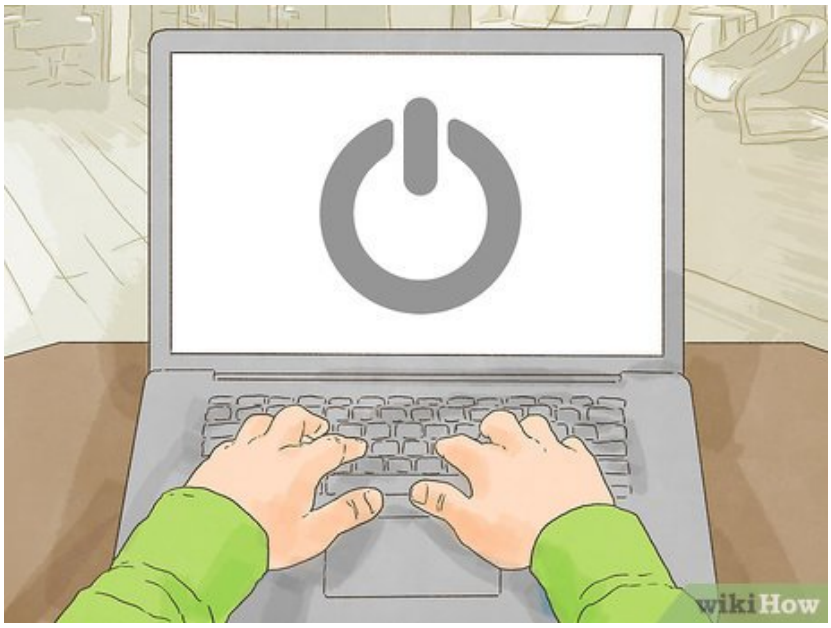
6. 

Activate two-factor authentication (2FA). Two-factor authentication will keep your new email account more secure because it adds an additional step to the log-in process. Most of them send a text message to your mobile phone. Even if someone obtains or hacks your password, they still won't be able to get into your email account.[14]

1. If the email service you're using sends a text message as the second factor, make sure you don't enter the phone number associated with a personal or work phone. You might use the phone number associated with your burner phone.
2. You can find a list of all websites and email services that support 2FA at https://twofactorauth.org/.

7. 

Email your contact. Once you've got your email address set up, use it to email the journalist the information you want to leak. If you're writing a personal account, avoid giving any personal information that could lead to the discovery of your identity, or your role in the organization from which you're leaking information.[15]

8. 

Shut everything off. After you've finished typing your email and sent it, turn off the Wi-Fi on the computer and close all apps. Fully delete the cache and cookies from the web browser, then shut down the computer.[16]

1. After you've shut down the computer, remove the battery. If at all possible, carry the battery separately from the computer. For example, you might put the battery in your pocket and carry the computer in a backpack.

9. 

Destroy the device when you're done. If you no longer need to communicate with the journalist, or if you fear you're about to get caught, you must thoroughly destroy the computer so that no information can be pulled off of it.[17]

1. Wipe the device back to its factory settings, using the most secure erase option that is available. Then turn the device off and smash it with a hammer.
2. Place the pieces in another piece of trash, such as a fast-food snack. Then go out for a walk and throw it away in a public trash can or dumpster well away from anywhere you live, work, or frequent.

Method 3 of 4:

Making a Phone Call

1. 

Buy a burner phone. If you want to call in a truly anonymous tip to the press, you can't do it from your personal phone, or from work. In fact, you should leave all electronic devices at home when you go to purchase the burner phone.[18]

1. The best place to buy a burner phone is a convenience store or bodega in a low-income part of town. Look for a place that doesn't seem to have surveillance cameras, or has older cameras with footage that gets erased and taped over frequently.
2. Buy a cheap prepaid phone that has enough minutes to last as long as you need it. Expect to make at least a few phone calls. Pay for the phone with cash.
3. If you're exceedingly concerned about your security or believe you are being followed, you might want to enlist a trusted friend to buy the phone for you. Don't tell them why you need it.

2. 

Go to a random location. To make your phone call, you need to go somewhere that you don't normally frequent. Mobile phone signals can be traced, and the phone keeps records of the wireless networks and

locations where it has accessed them.[19]

1. Choose a place where you're not likely to be overheard, and don't turn the phone on until you reach your destination. Again, only use cash for any purchases you have to make along the way.
2. Do not take any of your personal electronic devices along with you, as the records of them can be used to put you in that location.
3. Avoid storing the phone number on the phone. Once you call the number and have your conversation, delete the phone's call history.

3. 

Turn the phone off. After you've finished your phone call, wipe all information from the phone, power it completely off, and remove the battery. Return home by a different route than the route you took to get to the location.[20]

1. If you have to make more calls in the future, do not go to the same location more than once. Try to keep your locations as random as possible, so a pattern cannot be discerned.

4. 

Destroy the phone when you're done. Either when you're done communicating to the journalist, or when the phone runs out of minutes, you have to get rid of it. You'll want to go through the same process if you fear that you're about to get caught.[21]

1. If you believe authorities know what you're doing and are on your trail, you may want to destroy the phone after every call.
2. To destroy the phone, restore it to its factory settings, wiping all data. Then smash the phone with a hammer, including all chips in the phone.
3. Disguise the pieces by wrapping them in something else, and throw them away in a public trashcan or dumpster not located near your work or home.

Method 4 of 4:

Mailing Documents

1. 

Gather written copies of the information you want to leak. Make copies of any documents with care. Make sure that any printing, scanning, or downloading you have to do cannot be traced back to you.[22]

1. If you have an extensive number of documents, you might want to consider downloading them to a thumb drive and mailing that instead. You can buy a thumb drive at most any discount or electronics store.
2. Make sure there is nothing on the thumb drive that can be traced back either to you or to a personal or work computer.

2. 

Buy mailing supplies in advance. You need thick manilla envelopes and stamps for mailing. You also may want to invest in a postal scale, so you can accurately determine how much postage will be necessary.[23]

1. Don't go to your usual post office to buy your supplies, and don't order them online. Instead, go to a post office across town to get what you need. Pay for your mailing supplies with cash, and don't give any identifying information to the postal clerk.
2. Don't get rare or collectible stamps, just get basic, standard stamps. Another option may be to get a pre-paid, flat-rate mailing envelope.

3. 

Do not include a return address. When you address the envelope, use nondescript, block letters if you're hand-lettering the envelope. Another option is to type up a label on the computer and use that.[24]

4. 

Use an unfamiliar sidewalk mailbox. The envelope will be post-marked, and authorities can use that information to narrow down where you might live or work. For that reason, it's important to use a sidewalk mailbox in some other part of town where you don't normally go.[25]

1. As with any other trips you've made in connection with the leaking of documents or information to the press, do not use any credit or debit cards, or anything else (such as a public transportation pass) that can be traced back to you. Use only cash.
2. Try to find a mailbox that isn't near or within range of any surveillance cameras. For example, you don't want to use a mailbox that's sitting in front of an ATM, because the mailbox likely can be seen from the ATM's surveillance camera.

You finished reading the article "**How to Securely Leak to the Press**" 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.

© 2019 TipsMake.com