**BEFORE YOU START READING THIS, DELETE YOUR PERIOD TRACKING APP FROM YOUR PHONE---EVEN IF YOU DON’T THINK YOU’LL NEED TO USE THE INFORMATION IN THIS GUIDE**

**IF YOU ARE IN A STATE THAT HAS BANNED ABORTION, OR IS AT RISK OF BANNING ABORTION, DO NOT GOOGLE ANYTHING RELATED TO ABORTION ON AN UNPROTECTED DEVICE**

**Why go through all the effort of protecting yourself**

Even before the fall of Roe, thousands of people were unable to access abortion services in person. Many people turned to online services to buy abortion pills and have them sent to their homes. Now that Roe has fallen and Republicans have stated they want there to be a federal ban on abortion, more people will turn to the internet to get this vital healthcare.

BUT.

If you do this wrong, you will be arrested if you live in a state that has banned abortion. You could be facing anywhere from 10 years in prison to the death sentence just for having an abortion---never mind other legal charges you could face. Buying abortion pills online is not as simple as buying a toothbrush from Amazon. You need to protect yourself.

I’m hoping this guide can help you.

You may find it convenient to print out this guide for reference, but you should only do so if you’re in a safe location. Another option is to put this guide on a USB drive. This guide does contain hyperlinks, and you may need to have a separate copy of this guide for reference if you choose to use your own computer to order pills.

**How much protection do I need?**

It depends. My goal for this guide is to help you protect yourself from the run-of-the-mill officer who’s taken your computer and/or phone because they suspect you’ve had an abortion. The more protection you have, the better chance you’ll have in this situation. This includes protecting your browsing history, “hiding” your device from the websites you access, and masking your location. However, there’s no such thing as foolproof. There are few protections you can use to cover your tracks if you use your own devices and a digital forensic expert gets their hands on them. Use as much protection as you reasonably can and hope for the best.

Do not tell anyone other than a spouse that you’ve had an abortion. Your spouse cannot be compelled to testify against you---**everyone else can.** Do not tell your spouse you’ve had an abortion if you believe there could be negative consequences for you.

If you do get caught, do not allow the police to search you, your home, or your devices without a warrant. Do not unlock any device for the police without a warrant. If you have a phone that unlocks via facial recognition, disable that feature. Do not speak to the police without a lawyer **representing you** present. Do not answer any questions that the police ask you without your lawyer present, no matter how innocent they seem. Comply with the police only as required by law.

**What to do after you’re done with the guide**

You should protect yourself by deleting this guide off your computer the minute you’re done with it. A simple “delete” will not work---a forensic expert will still be able to recover it. This is because when you delete a file, your operating system will (usually) just move it to a different part of your hard drive. You can’t protect yourself by emptying the recycling bin, either. What you need to do is overwrite the part of the hard drive where the delete files are stored. Deletion is not foolproof, and sometimes forensic experts are still able to recover your data.

These instructions are specifically for Windows, as it is the most common operating system and OSX has a few built-in protections such as encrypting your drive and automatically overwriting deleted files (this features may need to be turned on---consult google).

Here are some options to help you, ranked by level of technical difficulty:

1. Changing how your recycling bin operates
   1. Right click on the Recycle Bin
   2. Click on Properties and choose which drive you want to permanently delete data from
   3. Select the option “Don’t move files to the Recycle Bin. Remove files immediately when deleted.”
   4. Click “Apply”
2. Using Eraser (this option will ensure that files cannot be recovered)
   1. Install Eraser from this link: <https://eraser.heidi.ie/>
   2. Launch Windows Explorer and locate the file that contains the guide
   3. Right click on the file and hover over “Eraser”
   4. Select “Erase” from the drop-down menu
3. Using Cipher, a built-in deletion tool on Windows OS
   1. Delete the guide from your computer
   2. Launch PowerShell from the Start menu
   3. Input “cipher /w:C”
      1. This will overwrite deleted files on your C drive. Adjust which drive you want to use by typing in another drive, like D, after the “:”
      2. If you know the path, you can input it after the “:” to save some time.
      3. This will overwrite deallocated files from the given drive or path, and will not touch existing files

After you’ve gone through one of these steps, you should check to make sure that the files are permanently deleted. iMyFone AnyRecover is a professional data recovery tool that you can use to check your work.

The tool can be found here: <https://www.anyrecover.com/>

Run the program after installation. If you can’t find the guide, you should be in the clear.

You should use these steps to delete any potentially incriminating files you downloaded while trying to acquire medication for an abortion.

If you followed the steps to anonymously access the internet via your own computer, erase all files using the steps listed above and then delete the surfer account.

If you printed out the guide at any point, shred it.

If you put the guide onto a USB, use the steps above to delete it or destroy the USB.

**Choose your device**

Choosing what device you use to access the internet is probably the most important choice you’re going to make. If you’re suspected of obtaining an abortion, the police will be going through your devices to find proof that you ordered pills online. Protect yourself accordingly.

Here are the options I recommend:

1. Use your local library: The computers are free to use and can often be accessed without having to give personal information. Libraries will generally erase all the data about your session, but it’s not guaranteed. Some libraries may require that you have a card to use their computers. If that’s the case, carefully consider your options.
   1. Don’t save your login information to any website at any point while using the computer
   2. Never leave the computer unattended
   3. Use Chrome incognito
      1. This won’t prevent someone from discovering what websites you’re accessing if they’re actively monitoring the network, but it will prevent the browsing history from being stored
      2. If you’re unable to use Chrome incognito, shift the web browser into a private browsing session
         1. This can be done by searching “[browser name] private browsing”
            1. This will return keyboard shortcuts that will make your session private so that the history will not be stored
   4. Never type in sensitive information, such as addresses or payment information. A semi-safe workaround is to open a document and type out the alphabet, both upper and lowercase, as well as numbers and special characters. If you need to input information into a website, copy/paste each character you need individually. This is time consuming, but can be an effective way to avoid keyloggers.
   5. Use a VPN if possible. Not all libraries will allow you to use a VPN, but using one is **strongly** recommended. VPNs created a “tunnel” through the internet, allowing you to access websites without being tracked.
   6. Delete any files downloaded and your browsing history before you leave
      1. Ctrl+Shift+Del will delete browsing history
   7. Log out of your session and shut down the browser manually
2. Use a burner smart phone: This will not have any of your information but your location can be detected.
   1. Purchase a burner phone from Walmart, or another store, that can access the internet AND has a removeable battery
      1. If possible, pay in cash
      2. If possible, go to a store in another part of town or another city. Avoid being anywhere where you may be recognized by people you know
      3. Do not bring your own phone to the store
   2. Do not use the phone except for in public locations, such as a park or coffee shop
   3. Never connect to publicly available Wi-Fi---**only use data**
   4. If you plan to leave a public location, turn off the phone **and remove the battery**
      1. Many phones are still able to track location when off. Removing the battery prevents this.
      2. Never have the battery connected to the phone when you are not in a public location---including when you are leaving the store after purchasing the phone
   5. Do not use this phone to make calls to anyone you know or give the phone number out
   6. When you are done with the phone, make it unusable
      1. Factory reset the phone: you can find this option under settings, although the exact location will vary by brand
      2. Drill a hole through the phone
      3. Soak the phone in water
   7. Find a safe place to dispose of the phone
      1. Find a trashcan that is accessible by the public (or is used by a variety of people, such as a bin at an apartment complex) and far away from your home or anywhere you frequent
      2. Do not take your own phone with you when you go to dispose of the burner
3. **Use your own computer** (do not use your own phone under any circumstances): If you use your own computer, be prepared to take extensive measures to protect yourself and your data. **This is likely the most secure option.** The steps I list may seem like overkill, and they might be. It may be possible to order your pills safely by following only part of these instructions but remember: if you are caught ordering this medication, you could be facing a lengthy prison sentence or death. These steps may not completely protect you from forensic experts, but they will give you a fighting chance against your average police department. The goal is to make finding your computer an incredibly annoying and tedious task.

**If you are following this list, you may find it is more convenient to put this guide onto a USB so that you can follow along no matter which account you are using.**

We will be setting up multiple layers of protection so that if one layer fails for any reason, you will still have adequate protection. As you make your way through these steps, make sure that you have the previous steps operational. This process may seem intimidating. Don’t worry, it’s much easier than it appears.

The layers we will be creating are:

Surfer account -> VPN -> Virtual Machine -> Linux Distro -> Tor Browser

**Always work from left to right when you want to browse the internet anonymously. Do not skip a step. When you are done, close each application from right to left.**

The first thing you’ll want to do is create a “surfer” account. This is a non-administrative account that you will use only to acquire abortion medication. At no point should you use this account to log in to email, Facebook, Twitter, or any other account that can be used to identify you.

* 1. Update all your applications and your operating system. Patch My PC Updater is a free tool that will assist you. It can be found [here](https://www.lifewire.com/patch-my-pc-review-2625194).
  2. Make sure you have a working firewall, such as Windows Defender. To turn on Windows Defender:
     1. Click “Start”
     2. Click “Control Panel”
     3. Click “System and Security”
     4. Click “Windows Defender Firewall”
     5. Click “Turn Windows Firewall on or off”
     6. Click “Turn on Windows Firewall for domain, private, and public network settings”
  3. Enable full-disk encryption on Windows (Windows 10 and 11 should automatically have encryption enabled, but double check)
     1. Click “Start”
     2. Click “Settings”
     3. Click “Privacy and Security”
     4. Click “Device encryption”
     5. If encryption is turned off, toggle it to turn on
  4. Create a new, non-administrator Windows account
     1. Click “Start”
     2. Click “Setting”
     3. Click “Accounts”
     4. Select “Family and other users” or “other users”
     5. Select “add account”
     6. Select “I don’t have this person’s sign-in information” and then “add a user without a Microsoft account”
     7. Create a username and password
     8. Make sure you did not click “administrator” under account type

After you have your surfer account, the next step is to install a VPN. VPNs create a “tunnel” between you and the internet where all your data and traffic are encrypted. Your IP address is masked, making it harder to locate you. You should never access the internet on your surfer account without using a VPN once installed.

* 1. If you are on the surfer account, switch back to your normal account.
  2. Create an anonymous email address, like [fakeemail12345@gmail.com](mailto:fakeemail12345@gmail.com)
     1. Do not use any of your real information when signing up for this account
     2. If you need to enter a phone number, use [this site](http://receive-sms-online.info/) to receive SMS via a fake number.
        1. If that site does not work for you, try any of the sites listed [here](https://www.raymond.cc/blog/top-10-sites-receive-sms-online-without-phone/)
  3. Sign up for a VPN using the fake email address
     1. ExpressVPN is $12.95/month and is one of the fastest VPNs, as well as one of the easiest to use. If you don’t want to use ExpressVPN, search for a VPN that:
        1. Will not log any information about your browsing or computer should their server be compromised
        2. Avoids DNS leaks that would expose your IP address
           1. You can use sites like [Doileak](https://www.top10vpn.com/tools/do-i-leak/) to ensure that no leaks have occurred
        3. Has a “kill switch” that stops all network traffic if the VPN connection is interrupted or fails
     2. To purchase a subscription to a VPN, sign up at privacy.com using the fake email address to generate a fake credit card and cardholder name.
        1. This requires your bank account information. If you are uncomfortable with this, here are some other options:
           1. Abine: this is a company dedicated to online privacy. They have a feature called “Blur” that creates a burner credit card number.
           2. Prepaid card: most websites will accept prepaid cards, like a Visa gift card. You can get one from just about any store, although it’s recommended that you pay in cash.
           3. Paypal: You will need to provide Paypal with a real credit card or bank account, but the recipient will only see the name and email address you used to register the account. You should create a new account for this, free of any identifiable information. This is the least secure option.
           4. Cryptocurrency: This option allows you to be completely anonymous, although it’s a bit tricky to set up if you have no experience with it.
     3. Do not use a free VPN. Remember: if it is free, then you are the product.
  4. Log in to the surfer account and download the VPN you subscribed to.
  5. When connecting to the VPN, **pick a location outside of the United States.** Preferably, pick a location where abortion is legal.

The next step is to install a virtual machine. A virtual machine is a piece of software that emulates a physical computer and can run the same programs that a regular computer can. The benefit of using a virtual machine is that it contains its own “hardware.” You can install software onto the virtual machine without it ever touching your personal computer. The virtual machine will help protect you in case your browser is compromised. Never access your virtual machine without enabling the VPN first.

* 1. Download Virtual Box [here](https://www.virtualbox.org/wiki/Downloads)
     1. You will want to select “Windows hosts” under VirtualBox 6.1.34
     2. Follow the steps in the wizard. You will be momentarily disconnected from the internet during the installation.
     3. Open the application after installation
  2. Install your operating system
     1. It is strongly recommended that you use Linux. This guide will walk you through on how to install Linux Mint. Here are other good distro options for virtual machines if you have some technical knowledge and wish to install something different:
        1. Lubuntu
        2. Linux Lite
        3. Manjaro
        4. OpenSUSE
        5. Ubuntu
        6. Slackware
        7. Debian
        8. Note: not all Linux distros are suitable for virtual machines, and some of the distros in this list are resource intensive. If you don’t want to use Linux Mint, research if your desired distro is suitable.
     2. Make sure you are on your surfer account and your VPN is active
     3. Download and install Linux Mint ISO file [here](https://www.linuxmint.com/download.php)
        1. You should choose “Cinnamon Edition”
           1. Scroll down until you see “Download mirrors”
           2. Select one to download (Harvard School of Engineering is a good option but all are fine)
        2. You should now see something along the lines of “linuxmint-20.3-cinnamon-64bit” appear in your downloads folder
     4. Return to the VirtualBox and click “New”
     5. Name the machine “Mint”
     6. The type should automatically switch to Linux
     7. Select the drop down menu for Version and select “Ubuntu 64 bit” if it does not automatically switch
     8. Click “Next”
     9. You will now be asked to select a memory size in megabytes
        1. The recommended memory size is automatically given to you. Do not go under this.
        2. You should assign at least 2GB (2,000 MB), but more is recommended
        3. If you are unfamiliar with how much RAM you have in your machine, you should not assign more than 3GB (3,000MB) of RAM
     10. Select “Create” when prompted to create a virtual hard disk
     11. Select “VDI (VirtualBox Disk Image)” and click “Next”
     12. Select “Dynamically allocated” and click “Next”
     13. File location will automatically appear. Move the slider until you see at least 14.00 GB on the right-hand side. Do not go over 20.00 GB.
     14. You should now see the name you gave the OS highlighted in blue on the lefthand side
     15. Click “Settings” and then “Storage”
     16. Under “Controller: IDE” click on “Empty”
     17. Click on the blue disk to the right of “Optical Drive” on the right-hand sidebar and select “Choose a disk file”
     18. Go to your downloads file and select the Linux Mint ISO you downloaded in step (iii)(1) and click “open”
     19. Select “OK”
     20. Click the green “Start” button shaped like an arrow
         1. Note: if you wish to leave your virtual machine at any point, make sure you power it off after you attempt to close the window. The machine will automatically ask you if you wish to power it off.
     21. Press enter. It may take a couple of minutes for the machine to boot up
         1. If you think that the machine has stalled out, you can close the window and reopen the machine.
     22. Click the “Install Linux Mint” icon and follow the installation wizard
         1. When you are asked to erase the disk and install Linux, this will not affect the rest of your computer so long as you’re working in the virtual machine.
         2. Do not enter any of your real information during the installation process.
         3. Choose a secure password that is:
            1. At least 12 characters
            2. Contains upper- and lower-case characters
            3. Contains numbers
            4. Contains special characters
         4. Do encrypt your home folder when prompted
     23. Once installation is complete, click “Restart Now” and then press enter
         1. If you think that the machine has stalled out, you can close the window and reopen the machine.
  3. Install Tor Browser: Tor is a free browser that allows you to anonymously browse the internet via a worldwide network. It masks your computer by using other computers, called relays, as a detour before you reach whatever website you wish to access. If someone is trying to figure out who is accessing Planned Parenthood, for example, they would have to track your path through dozens of other computers before they found you---a task that most people won’t wish to undergo. Should someone try this, they will be wasting their time as they track you. By the time they reach the “beginning,” all they will hopefully find is your VPN and virtual machine.
     1. Make sure you are on your surfer account, your VPN is active, and you are on your virtual machine.
        1. The steps I will be giving you assumes that you installed Linux Mint
     2. At the bottom of your screen, you should see a black box with “$ \_”. Hovering over it should tell you that this is called your terminal
     3. Click on the terminal. A screen should appear with your fake username and the name you gave your virtual computer
     4. Let’s check to make sure your operating system is up to date
        1. Type: sudo apt update && sudo apt upgrade
        2. Press enter and then type your password
        3. Press y and then enter
        4. Get some coffee because this will take awhile
     5. Type: “sudo apt install torbrowser-launcher” and press enter
        1. Press y and then enter
     6. Confirm installation by typing: tor --version and pressing enter
        1. If installation went correctly, you should see something like: Tor version 0.4.2.7
     7. Close the terminal
     8. Access Tor by clicking the menu in the lower left-hand corner, then navigating to “Internet”
        1. Click on “Tor Browser”
     9. You can now browse the web like normal
     10. Your firewall may try to prevent Tor from installing/connecting to the internet. You can look in the settings under your firewall to make Tor/your virtual machine a trusted application if this happens.
  4. When you are done accessing the internet, close the applications in the reverse order you accessed them
     1. Tor -> Linux Distro -> Virtual Machine -> VPN -> Surfer Account

**NEVER USE A PUBLIC COMPUTER OTHER THAN ONES FOUND AT A SECURE LIBRARY**

**NEVER USE A FRIEND’S DEVICE**

**NEVER CONNECT TO PUBLICLY AVAILABLE WIFI FROM YOUR OWN DEVICES**

**Where to start your search for pills**

Make sure you are on a secure device. If you’re on your computer, double check that each of your protection layers are active (surfer account -> VPN -> virtual machine -> Linux distro -> Tor).

Where you choose to order your pills from is vital. You want to make sure that whoever you get the pills from is reputable as taking the wrong pill can seriously injure or kill you. **Do not order pills from Amazon or from any source that does not have a medical professional assisting them. Do not attempt to order pills from any source that may be a pro-life clinic posing as an abortion provider.**

The cost will depend on where and when you order pills. As of May 2022, it could cost between $40 and $1,195 to obtain a medical abortion. There are several organizations who will help cover the cost if you cannot afford it. This non-exhaustive list contains trustworthy sources as of May 2022:

* [National Network of Abortion Funds](https://abortionfunds.org/funds/)
* [National Abortion Federation](https://prochoice.org/patients/naf-hotline/)
* [Access Reproductive Justice](https://accessrj.org/) (California)
* [Chicago Abortion Fund](https://www.chicagoabortionfund.org/) (Illinois)
* [Cobalt Abortion Fund](https://cobaltadvocates.org/) (Colorado)
* [Northwest Abortion Access Fund](https://nwaafund.org/) (Washington, Oregon, Idaho, and Alaska)
* [West Fund](https://www.westfund.org/) (Will comply with all laws pertaining to abortion, including SB8)

It is likely that where you can order pills will change rapidly when Roe v. Wade is overturned. This list is accurate as of May 2022. Each of these sources have confirmed they will be discreet when shipping medication to your home and will not store your information after the transaction is complete. That does not mean that there is no risk involved, so carefully weigh your options. Here are some good places to start your search:

* [National Women’s Health Center](https://nwhn.org/safe-online-delivered-how-to-get-the-abortion-pill-by-mail/)
* [Planned Parenthood](https://www.plannedparenthood.org/planned-parenthood-keystone/services/remote-services/dtp-mab)
* [HeyJane](https://www.heyjane.co/home-v2) ($249)
* [Whole Woman’s Health](https://www.wholewomanshealth.com/abortion-care/abortion-medication-by-mail/) ($400) (Maryland, Minnesota, New Mexico, Virginia, or ability to travel to these states)
* [Abortion Finder](https://www.abortionfinder.org/?gclid=EAIaIQobChMIoJGejq7a9wIVh9rICh2l3wqvEAMYASAAEgIbrvD_BwE)
* [Aid Access](https://aidaccess.org/) ($110-$150) (Alaska, California, Colorado, Connecticut, Idaho, Illinois, Maine, Maryland, Massachusetts, Minnesota, New York, New Jersey, New Mexico, Nevada, Oregon, Rhode Island, Vermont, Virginia, Washington to have prescription filled in America within 1-3 days) (All other states will have the prescription filled in India and will take 3-4+ weeks)
* [Plan C](https://www.plancpills.org/) ($40-$300)
* [Ms.: Abortion Pill FAQs](https://msmagazine.com/2022/05/04/abortion-pills/)

**How to send this guide to someone else**

Do not send this guide to anyone you do not personally know.

Do not send this guide without encrypting it.

* Click “File”
* Click “Info”
* Click “Protect Document”
* Click “Encrypt with Password”
* Enter a reasonably secure password
* After you email or send it to someone, call them and tell them the password
  + Avoid putting anything in writing if you can help it

**Taking care of yourself after an abortion**

These recommendations come from medical professionals.

* Drink plenty of water.
* Eat healthy food.
* Get plenty of rest.
* Avoid strenuous exercise and lifting heavy objects for at least one week
* Only use pads and avoid sex for at least two weeks
* Avoid swimming for at least two weeks
* Use heating pads to ease the pain from cramps
* Do not douche for at least 2 weeks
* Do not use perfumes, bubbles, or oils in bath water

Common side effects as reported by medical professionals:

* Bleeding that lasts for 14-21 days
  + Bleeding may be spotty, dark brown, and include clots
* Cramping
* Slight dizziness
* Drowsiness
* Moderate nausea and vomiting
* Sore breasts

**When to seek medical attention**

Medical abortions are as safe as taking Tylenol. However, in rare circumstances, you may need to seek medical attention. It is unlikely that medical professionals will be able to tell the difference between having a medical abortion and experiencing a miscarriage. Despite this, they may be required to report you and there may be an investigation. If you followed the steps to protect yourself listed in this guide, they will likely be unable to prove you ordered abortion pills.

**Please seek medical attention if you need it even if seeking help might lead to an investigation. It is always better that you survive.**

This list comes from medical professionals.

Seek medical attention if you experience:

* Excessive bleeding (soaking through 2 or more pads within one hour)
* Severe back or abdominal pain that is not relieved by an over-the-counter pain medication
* Severe nausea, vomiting, or diarrhea that lasts more than 24 hours
* Blood clots the size of a lemon or larger
* Fever that lasts more than 24 hours
* Chills and severe shivering
* Strong-smelling discharge that is itchy or painful/pus-like
* Loss of consciousness