How to Survive the Internet:
Strategies for Staying Safer Online

Image by JD Hancock licensed under Creative Commons 2.0.

Created by Yael Grauer. Original download available here.
Contents

Introduction 2
A. Your physical safety 4
B. Your location 6
C. Your online information 9
   1. Passwords and password managers
   2. Recovery email address 10
   3. Security questions
   4. Third-party permissions
   5. Two-factor authentication 11
   6. Account recovery
   7. Account activity 12
   8. Links and attachments
   9. Privacy settings
  10. Secure URLs
  11. Patches and updates
  12. Flash and Java 13
  13. Switching services
D. Your stuff (and all the information on it) 14
E. Harassment on social media and via email 15
F. Your offline information 18
Introduction

Being subjected to threats, unwanted contact, compromised accounts, hacked websites, or having sensitive information shared online is an awful experience. In the midst of this, it can be confusing to know how to react and which steps to take to protect yourself. You’re likely to get conflicting advice on whether to take incidents seriously or ignore them, and trying to get up to speed on online security strategies with limited technical knowledge can make an already stressful situation more overwhelming. It’s not always obvious who’s responsible for ongoing harassment or how many people are involved, and trying to address a threat with limited information can be difficult. Please remember that you are not alone. If you were, this guide wouldn’t be here. You will get through this.

While there are no cut-and-dried, right-or-wrong ways to react to these types of situations, this e-book outlines some steps you can take to improve your security, for you to choose from based on your unique situation, temperament, and politics. (Special thanks to Michael Carbone, Stefan Edwards, and several people who want to remain anonymous, for reviewing early copies of this e-book, and to Maartje Gorte for editing it.)

Before getting started, there are a few disclaimers I’d like to emphasize.

First of all, although there is a lot you can do to minimize your risk of harm, there are never any guarantees. As long as you’re aware of this limitation, however, taking a proactive approach can be empowering.

Second, although I will be delving into a lot of tools, the best tool you have is between your ears. Adopting a security mindset, which can include but is not limited to finding the right tools, is key.

Third, be aware that some of the steps you can take to protect yourself online may slow down your workflow a bit. For example, password managers (which we’ll discuss below) offer a measure of security and peace of mind, but also require you to take an extra step before logging into anything. Two-factor authentication (also discussed
below) helps protect important accounts, but requires you to use verification codes sent to you by text message to log into those accounts. Sometimes, getting everything to work together will involve a few extra steps as well. For example, setting up two-step verification on Gmail on each of your devices takes some time, so you may not be able to check your email on your mobile phone or tablet right away.

Finally, I want to emphasize that you don’t have to do everything listed here. By determining what you’re most concerned about, you can prioritize the steps that are most important to you, and not spend too much time on issues that don’t matter to you as much. This can help you decide which time and workflow constraints are worthwhile. As your circumstances change, the decisions you make may change as well.

Again, please remember that you don’t have to try to do everything on this list all at once! Pick the section(s) that you think will be most beneficial to you, and start there.

This guide is a work in progress and obviously can’t cover every situation, but will hopefully provide a bit of clarity on the options and help you decide which steps you want to take. Remember that a lot of these steps can be taken ahead of time, before anything happens. That’s less stressful and more effective.
A. Your physical safety

If your fundamental concern is your physical well-being—because you’ve received credible threats or your home address has been compromised—here are some options.

1. Consider staying with a friend until things blow over. This can provide peace of mind if you feel unsafe in your home.

2. If you do need to stay in your home, consider installing a security camera with a motion detector—the kind that only records if movement is detected.

3. Make sure you have good locks, ideally deadbolts, on all of your doors. Remember to lock them at all times, even when you’re just leaving for a short time. When you’re at home, it can be a good idea to lock the door or close blinds and windows.

4. Consider varying your route to work and home, and either avoiding locations you normally frequent or making sure you are going with friends.

5. Consider contacting the authorities. Even if you don’t decide to contact them right now, start documenting what is happening so that there is a paper trail in case things escalate. (You can take screenshots or use archive.today to do this.) You’ll want timestamps and URLs for screenshots you take of comments on social media, and full headers for emails, which include the email addresses of the sender and the recipient, timestamps, etc.

If you do contact the authorities, you may want to have someone else there with you as an advocate, and to explain anything about the situation that you may not think to emphasize. Be aware that police response can be quite underwhelming.

6. If the threats that make you worry about your physical safety come from an online source, try to share information about the perpetrators with other people, because they may have additional information. Setting up a shared file is a good way to gather information that can help you narrow down the location of the people contacting you, and sometimes even determine who they are. Try to find out
information such as screen names, phone numbers, and IP addresses (if available—they can be found in email headers, site logs, chat logs, etc.).

Back up your records in case you’ll need them later.
B. Your location

If you are trying to make sure your home address isn’t released, there are a few steps you can take to make it more difficult for someone to track you down, especially if you don’t own a house and are just renting.

1. Consider paying $10 for privacy protection for any websites registered under your name. It makes sure your mailing address doesn’t show up on WhoIs, where people can run a query on your site and see which address it is associated with. (Unfortunately, it can take some time for old information to disappear.)

2. If you have to publish a mailing address online somewhere, or even on your own email list due to the CAN-SPAM Act, think about using a PO box. Using your work address is another option, depending on your work situation. If there are security cameras and plenty of coworkers around, for example, listing a work address can be preferable to listing a home address. Unfortunately, there are many databases online that record people’s addresses, and homeowners’ addresses are public record. It’s impossible to hide your location from everyone, but these measures make it more difficult for someone to track you down.

3. Remove your mailing address from people search sites. These sites includes Acxiom, Addresses, Archives, BeenVerified, CheckPeople, DOBSearch, InstantCheckMate, Intelius, MyLife, PeekYou, PeopleFinders, PeopleLookup, PeopleSmart, Pipl, PrivateEye, PublicRecords360, PublicRecordsNow, Radaris, Spoke, Spokeo, USA-People-Search, US Search, Whitepages, Zaba Search, ZoomInfo, and many others. You may be able to find your information on multiple sites by using an aggregator like DirtSearch, and also by putting your name and address, name and phone number, and various combinations of these in a search engine to see what information comes up about you.

Many of these people search sites allow you to opt out online, though some require you to provide information such as your current phone number and city and state, or even a copy of a driver’s license. Others require you to jump through hoops by
faxing or mailing in information. Unfortunately, it can take a while for your information to be removed, and it sometimes requires an ongoing effort. Read more about opting out on this Reddit thread (outdated, but still useful), and on a newer Computerworld post. Some comprehensive resources include the Privacy Rights Clearinghouse and the World Privacy Forum, particularly their data brokers opt out list.

4. If you live or have lived in the U.S. and can afford it, another option is to try a service like Abine’s DeleteMe ($129/year) to remove your information from multiple data sites either on an ongoing basis, or every three months, depending on the site.

5. Going forward, think about installing browser extensions like Privacy Badger or Ghostery to help minimize your online footprint. These tools primarily protect you from companies tracking you across multiple sites, but because they minimize the personal information websites can find out about you, they also help prevent it from being compiled and winding up online.

6. Consider using the Tor browser: it prevents websites from tracing your IP address, which makes it difficult to narrow down your location. Tor basically bounces your web traffic to different computers all over the world before it hits the internet. Browsing using Tor can be a little slow, but is a very useful tool.

Be aware that using Tor makes it look like you are logging into accounts from unusual locations. As this is usually a warning sign that an account has been hacked, you may get a warning message to that effect from a few of your regular websites. Many sites—including Twitter and Gmail—enforce separate rules for Tor users. These rules vary from requiring additional information up to being unable to access the sites from the Tor browser.

7. Pay close attention when you are posting your location, checking into places on social media, or even registering publicly for events. Eventbrite, Meetup, and other
such places may publish their guest lists publicly or make that information available to other members.

8. Make sure that image loading is turned off when you check your email on your laptop and phone. There are services that will notify the sender of an email when you open a message, and sometimes even from where. These services work by sending an invisible pixel that loads just like an image would. You may want to test some of these services (such as ToutApp or Yesware) to see what information they make available about people, or even temporarily disable location services from the apps on your phone when you are checking email.
C. Your online information

It’s hard to do anything online these days without leaving a broad trail of information and juggling a pile of passwords. However, there are some things you can do to improve security that don’t involve you giving up using the internet.

1. Passwords and password managers

The best way to keep your email address and online accounts secure is with a really strong password. Most people, however, use just one password that’s either a series of sequential numbers, their birth year, the word ‘password,’ or a pet’s name, and they use that same password for every account. It can be hard to remember a million complex passwords with symbols and numbers and letters. Luckily, there are programs such as 1Password, LastPass, and KeePass that will not only store all of your passwords, but also create complex new passwords that won’t be easily cracked. Phone apps are available for all of these password managers.

Make sure you use a unique password for each account. Since most of us start out using the same few passwords everywhere, setting this up is an incredibly time-consuming task. Load up some podcasts and grab a snack while you’re resetting everything. Generate new, secure passwords for your banks, credit cards, social media accounts, email, domain registrar, hosting provider, cell phone company, etc., and add them all to your password manager. Also make sure to generate new passwords—and save them to the password vault—for other places that are linked to your bank account, such as Amazon, any food delivery services, etc. It’s no fun when people buy stuff off of your account and send it to you or buy stuff off of your account and stick you with the bill.

Be aware that using a password manager will add an extra step to your workflow—you won’t be able to access many sites without first logging into the password manager with your security phrase. (If you can’t login to a site, either because you’ve forgotten your password or because someone reset your password maliciously, fill out the password reset request or take any other step listed on the site.)
2. **Recovery email address**

In addition to changing your password for each site you use, you may want to change your recovery email address for them all as well. Consider creating a separate email account for password recovery requests, so that if you are somehow hacked, you can see all of the password reset requests in this email account and have a checklist for what needs to be reset. Keep this account secret. (Remember that keeping the password for your recovery email account secure is paramount, since all other accounts use password reset emails as a verification mechanism.)

3. **Security questions**

Security questions are created to allow people to bypass password requests. Therefore, consider changing your security questions to require information that isn’t easy to find online. For example, it’s not difficult for a stranger to figure out your birthdate or even your mother’s maiden name. One option is to use a made up answer for commonly asked questions (example: list a secret name that you’ve made up whenever asked for your mother’s maiden name) so that even someone who has access to a lot of your personal information will be unable to compromise your account.

4. **Third-party permissions**

A third-party application is a product that’s not part of the main service that you’re using, but does have access to your main account or its credentials. For example, Hootsuite is a third-party application that works with Twitter.

Some third-party applications don’t have security standards as high as the ones the ‘mother’ service uses. Consider revoking third-party application permissions from Twitter, Facebook, and your phone for apps that you aren’t using regularly.

Twitter [has a good explanation](#) of which apps you may want to give your username and password, and which ones you shouldn’t trust with that information. It also explains how to revoke them. Facebook [has some information as well](#).

Be aware that revoking third-party app permissions may mean you’ll need to manually log into certain apps if you want to use them on your phone.
5. **Two-factor authentication**

Two-factor authentication, also known as two-step verification, adds an extra step to checking your identity when you’re logging into a website. One way this might work is that each time you want to access your account, the website sends you a text message with a password that expires within 15 minutes, and asks for this password and your regular account password. Every type of two-factor authentication adds an additional step to your workflow.

Google explains two-step verification and its common problems, and Electronic Frontier Foundation, a digital rights advocate group, has some information on how to set it up. There’s also a handy list of services that provide two-factor authentication.

If you use Gmail, be aware that you’ll need to spend some time setting up your devices afterwards so that you’ll be able to access email on them.

6. **Account recovery**

If you can’t log into an account, either because you have forgotten your password or because your account has been compromised, try to reset your password. If your password has been changed without your knowledge or consent, usually you can contact support or take other steps.

Here are the support links for a few popular sites:

- Twitter: [https://support.twitter.com/articles/185703-my-account-has-been-hacked](https://support.twitter.com/articles/185703-my-account-has-been-hacked)
- Tumblr: [https://www.tumblr.com/docs/en/account_security](https://www.tumblr.com/docs/en/account_security) (With Tumblr, make sure to remove the third-party email-to-post setting, because if someone gets into your Tumblr account, they can write posts to Tumblr that will also be posted to your Twitter account, making it look like they were posted by you.)
- Facebook: [https://www.facebook.com/help/131719720300233/](https://www.facebook.com/help/131719720300233/)
- Dropbox: [https://www.dropbox.com/support/s/92/8281995/c/2](https://www.dropbox.com/support/s/92/8281995/c/2)
• Skype: https://support.skype.com/en/faq/FA10656/what-is-live-chat-support

7. Account activity

If you use Gmail, reviewing “Last account activity” details is a powerful tool. It allows you to remotely disable access to your account if someone is accessing it from an unexpected location. Facebook has an option similar to this. (Be aware that using Tor may make it look like you are accessing your account from various locations—so make sure to keep logs of when you were browsing these sites and look at times and dates.)

8. Links and attachments

Be careful clicking on links or opening attachments, because bad links and bad attachments can be harmful to your computer or other devices. Consider using Google Drive to open attachments. Antivirus software like Virus Total can scan links and attachments and make sure they’re safe. If you want to know what you’re clicking on, use LongURL to expand shortened URLs.

9. Privacy settings

Review the privacy settings for your browser and your operating system, and pick the settings you feel most comfortable with. The specific settings are different for each operating system, but there is usually a “security and privacy” option.

10. Secure URLs

Check whether any site you enter information into has a URL that starts with https:// rather than http://. The https:// connection is encrypted, making it harder for a third party to read what you’re sending. HTTPS Everywhere is a browser extension that makes websites use https:// by default, if possible.

11. Patches and updates

Make sure to keep your software updated. That way, vulnerabilities will be patched up—ideally before anyone exploits them. Also, if you’re on Windows, using EMET adds another layer of protection against exploits.
12. Flash and Java

Speaking of easily exploitable vulnerabilities, Flash and Java put your computer at risk. Disable or uninstall Java in your browser, and use an extension block like FlashBlock. Flash and Java sometimes want to install themselves, so make sure your computer prompts you before installing software. Pay attention to any security warnings: click “Cancel” if you’re unsure about a program, so that you avoid accidentally installing something bad.

13. Switching services

Depending on the level of harassment you’re receiving and how secure you want to be, you may want to consider moving to a service that’s more secure or simply not under attack. For example, if someone is constantly trying to maliciously reset your Dropbox password, you can switch to a more secure cloud storage service like SpiderOak. It has a zero-knowledge policy, meaning the company doesn’t have access to your files or your password. Be aware, if you lose your password, zero-knowledge companies can’t reset it for you! To keep from forgetting your password, you can choose to include a hint. SpiderOak is not as user-friendly as Dropbox, unfortunately, but may be worth it if you must keep sensitive documents in the cloud.

Skype is another service that is often hacked into during prolonged harassment campaigns. This is especially bad because it can be used for impersonation. Consider switching from Skype to Jitsi if this is happening to you. If you do so, you’ll want to disable Java from your browsers (which you should be doing anyway), as discussed above.
D. Your stuff (and all the information on it)

The steps mentioned above help protect you from people hacking into your information and accounts from the internet. This section provides some steps to help you prevent people from gaining access through your own devices.

1. Make sure to keep your laptop and phone on you, and don’t leave them unattended.

2. Do not plug USB devices into your computers, unless they’ve never been plugged into any computer that isn’t yours. They might contain malware that can damage your system or expose your personal information.

3. Make sure your computers have full disk encryption (FileVault on Mac—turn it on in the “Security and Privacy” section of your system preferences—and Bitlocker on Windows). That way, if someone gets a hold of your laptop and copies the files, they’ll just see a jumbled mess.

4. Back up the data on your computers to an external hard drive that is kept in a separate, secure location. This way, you’ll always have an extra copy of your data available. Set a calendar reminder to back up your data at regular intervals, and make sure the backup is actually working.
E. Harassment on social media and via email

Social media is designed to help people get in touch with each other. Unfortunately, there are very few easy ways to restrict unwanted contact. Some workarounds are below.

1. To reduce the strain of dealing with unwanted email, take advantage of the filtering rules most email programs allow you to apply to incoming mail. You can set up a rule that files everything containing certain keywords into a separate folder automatically. That way, you can go about your day without having to constantly deal with unwanted mail, but still keep a record of it.

2. If you’re dealing with unwanted posts on social media, consider setting your accounts to private (temporarily or permanently). You can make your Twitter accessible to followers only (people who aren’t following you won’t see your posts), or make your Facebook private and limit old posts (under settings, privacy, limit past posts). Be aware that setting your Twitter account to private means that people who do not follow you will be unable to see your @replies.

Consider preemptively disallowing comments on YouTube, posts on your Facebook wall, etc. You may want to prescreen blog post comments as well.

3. If you get a lot of harassing messages, or find them highly disturbing, you may want to find an acquaintance to review your messages for you. They can check the messages sent to you on Twitter or Facebook or even by email, document the abusive ones and let you know which ones to respond to. Resetting your Twitter notifications from “all” to “people I follow” means you’ll only see @replies from accounts you follow.

4. If you have a WordPress site and are getting unwanted comments coming from Tor users, it’s possible to use WordPress extensions to make your site read-only for people viewing it on Tor browsers, or to block Tor from displaying it altogether. You may decide to do this, for example, if you are getting flooded with comments or if people coming from Tor browsers continuously filling out the comment
forms on your site. You can either block comments coming from Tor services or make them subject to review. This can be done temporarily or permanently. (When deciding which steps make sense, be aware that not all people using Tor browsers have bad intentions or are part of the group of people harassing you. Tor is used for very legitimate purposes, such as people in countries bypassing political censorship.)

If you want to block only some actions coming from Tor, Tor Blocker is the most flexible choice. You can specify for each of the following actions whether Tor users are allowed to do them or not: read public content, read private content, register, subscribe, post comments, access the admin panel, or send post requests. Tor Blocker is a good option if you believe many of your site users use Tor for legitimate purposes, and don’t want to ban them completely.

If you would like to ban Tor users completely, either permanently or temporarily, several plugins exist for that as well. WP-Maltor blocks anybody using Tor from visiting your site. Deny TOR Auth redirects anyone visiting your website using Tor to a different site. (This can make it more difficult for hackers to guess your password through what’s called a brute-force attack.) Anti-Tor allows you to restrict Tor activity on your site. You can always turn off these plug-ins once things have settled down.

5. If you are getting anonymous hate mail through contact forms on your site, such as the Cform plugin, consider replacing the contact form with an email address, which will log the IP address of the sender, and allow you to send an abuse message to their internet service provider. (Of course, there are ways around this limitation, but it may be a deterrent.)

6. If you are worried about a DDoS attack or are experiencing a DDoS attack, Cloudflare is one of several services that can help you. See https://support.cloudflare.com/hc/en-us/articles/200170196-I-am-under-DDoS-attack-what-do-I-do-. 
7. If you are often approached by unknown people online, it may be worthwhile to do some research. Investigate people reaching out to you online using WayBack Machine and check with third parties before responding to them.

8. On Twitter, several programs are available to allow you to block people who’ve been blocked by others on Twitter, or who have brand new accounts mentioning you, such as @blocktogether.
F. Your offline information

Hacked accounts or stolen devices are not the only ways your information can end up in the wrong hands. Here are some tips to help you safeguard your data even when offline.

1. Start thinking with a security mindset. Verify the identity of people communicating with you before giving out personal information, even if that means calling them back.

2. Consider changing your cell phone number if you are getting unwanted calls. To make it harder for someone to log into your voicemail, make sure you have a PIN enabled for your account.

3. If you are a victim of a prolonged harassment campaign, let your friends, past and current employers, and family members know that people may be contacting them to try to dig up information about you. Tell them that you recommend them to just hang up. Also let them know that there may be fake accounts trying to impersonate you.

4. Tell companies you’ve done business with, such as your phone company, doctors, vets, etc., not to give out your information by phone. Check to see if you can set up a special password with them or set a PIN for your account.

5. If your social security number was posted publicly either as part of a harassment campaign or through sloppy security on the part of companies that had access to it, consider signing up for credit reporting, fraud monitoring, or identity theft services.