Simple Ways to Protect Yourself Online

Beginner

For people who haven’t thought much about Internet safety and would like to start.

Intermediate

For people who have an idea about what Internet safety looks like, but want to learn more.

Expert

For people who are already employing Internet safety measures and want to take it to the next level (Safety Ninjas).

Table of Contents

Passwords 2

Phishing and Suspicious Links 3

Viruses 4

Browsers 5

Cookies and Trackers 7

Privacy Settings 10

Encryption 13

Data Detox 14

Passwords

Beginner

Creating a strong password does not have to be hard. If you are sort of person using “Password123” or “123456” as your passwords, then the first step is to realize that these passwords are so overused that they will be the first guesses of anyone hacking your account. You might think that you’re being original using a simple password, but the fact is that a lot of people have the same idea.

Another issue with using a simple password is that they are easier for others to guess - especially if your password includes some form of personal information, such as a family name, a pet’s name, a birthday, the street name of your childhood home, etc. If it could be used as a security question or in any other part of the signing up/registration process, do not use it as a password.

A suggestion for password creation would be selecting several random words and stringing them into a phrase that you could easily remember. This gets even better if you include foreign languages or gibberish as well.

Never reuse passwords! However secure your passwords may be, reusing your passwords is putting all of your eggs in one basket. If a hacker steals one password, they get access to all your accounts.

Intermediate

It is also a good idea to change your passwords every so often. It is recommended that all passwords be changed once every six months, at the least, although preferably as often as every three months. The more frequently you change your passwords, the more secure you’ll be.

One of the best ways to secure your passwords is to use two-factor authentication, which is far simpler than the name suggests. When you log in with 2-factor authentication, you type in your password and get sent a text with a code, which you also enter in. This protects your accounts because a hacker would need to have your password and your phone in order to be able to access your account.

Expert

In conjunction with other good password practices, a good way to protect your passwords is a password manager such as Lastpass. A password manager works by auto-generating secure passwords for you and saving them, so that the only password you need to remember is the password for the manager itself.

Phishing and Suspicious Links

Beginner

Auto-fill data phishing. Never save autofill data, because certain sites can hide their information fields from your view. In this case, if you allow autofill, you may not see the field for something such as your address or credit card information, but it could still be there collecting your information. To turn it off in Google Chrome (taken from Google support):

1. Open Chrome.
2. At the top right, click More Settings.
3. At the bottom, click Show advanced settings.
4. Under "Passwords and forms," uncheck "Enable Autofill to fill out web forms in a single click."

To turn off in Firefox:

1. Click on the Firefox menu icon. (Three lines at top right of screen.)
2. Click on Options.
3. Choose the Privacy icon.
4. In the History section choose Firefox will: "Use custom settings for history."
5. Uncheck "Remember search and form history."
6. Click OK.

To turn off or edit in Safari (taken from the Apple website):

1. Choose Safari > Preferences, then click AutoFill.
2. Turn AutoFill on or off: Select each type of information you want Safari to fill in, and deselect the rest.
3. Change or delete autofill information: Click Edit for the type of information you want to change or delete.

Never give out your passwords. Never save your passwords in your browser. Always logout of applications/social media, especially on shared computers.

If you are unsure of a link, do not click it. (See Copycat Websites for what these links could be/could look like)

Downloading

Do not download something unless you know exactly what it is you are downloading, and it comes from a trustworthy source. Things like viruses could get onto your computer through a suspiciously originated download.

Avoid downloading alternate toolbars for your browser. These become annoying and often have a range of useless buttons that you will never need. More often than not, they come with data collectors and a bunch of trackers following your online activities, which isn't something you would necessarily want.

Copycat Websites

These websites look like government websites and offer services from government departments, but charge a lot of money for the services without providing the customer with any additional benefit. They use website tools to put themselves high up on search results, and sometimes even appear before the official sites. The web address and the design of the site itself are made to mimic the official website.

- Leads to you paying more than necessary for services
- Take the time to search for the official website
    - Look for .gov
    - Look for contact info for the agency
    - Has the official logo
    - Cheaper prices
- If you DO use a third party site, check that payment page is secure
    - Use https:// (the secure address) before the address
    - Do not use if the site does not allow https://

Source

Viruses

Beginner

Every computer should have anti-virus software. You can get top-end antivirus for free these days, and however much you think that you can avoid viruses by being smart online, the truth is that eventually you will slip up and get malware on your computer. It is difficult to get viruses off of a computer, but it's much easier to prevent them from getting there in the first place. Anti-virus isn't even hard. Just download and install, and the software will handle the rest.

There are several good options for free antivirus software, including Panda, AVG, and Avast, but for simple, free protection, BitDefender is probably the best. It is simple and easy to download from their website (https://www.bitdefender.com/solutions/free.html) and there are versions for both Mac and PC. Simply download, install, and forget about it.

The other simple way to protect yourself from viruses is to always install updates as soon as possible. Out-of-date software is huge vulnerability, and installing updates is the best way to ensure that as many security flaws have been fixed as possible.

Browsers

Beginner

When you access the internet, you probably don't think too much about the browser you're using to do it. However, browsers are often the only things standing between you and the internet, and are an essential component to staying secure. Here's a rundown of the most common browsers, and how the measure up in terms of security and privacy.

Safari (Apple)

Safari comes preinstalled as the default browser on Apple products. It is a fairly secure browser, with Apple quickly fixing security holes when they are found. Safari also employs sandboxing, which prevents websites from accessing your computer or downloading things without your permission.

However, Safari is not open-source and is controlled directly by Apple, which is not perfect for user privacy. While there is no evidence that suggests that Apple is collect and selling data from Safari, it is something to consider.

Internet Explorer (Microsoft)

There is only one reason to use Internet Explorer, and that is to download a different browser. Seriously, do not use Internet Explorer. It is so full of security flaws that it's about as safe as a car without seatbelts. All of the other options listed here are free and easy to download, so there is really no reason not to use them. Please, please, anything but Internet Explorer.

Google Chrome

Generally considered to be the most secure browser on the market, Google Chrome regularly comes out on top of security tests. Google also fixes security holes impressively quickly, and employs sandboxing to prevent harmful websites from attacking your computer.

For privacy, Chrome is probably the worst browser to pick. While there are extensions that allow for increased privacy online, the browser itself is created by Google, a company that makes money from selling user data. While this has not been a problem yet, as far as we can tell, it could become a problem in the future. Download Google Chrome at https://www.google.com/chrome/browser/desktop/index.html (there is a link to install for non-windows devices below the install button)

Firefox

Firefox is the least secure of the options listed here, for a couple of reasons. First of all, it's made by a small team, which means security fixes are slower than for other browsers. Second of all, it is built on an old framework from 2004, which opens up unfixable security problems. Finally, Firefox is not capable of sandboxing, which prevents websites from attacking your computer directly.

That said, Firefox is the best browser for privacy. The browser is completely open-source, meaning that anyone can look at the code to ensure that nothing suspicious is happening. Firefox is also created by a Mozilla, a non-profit organization dedicated to not sharing user data, a bonus to privacy. Download Firefox at https://www.mozilla.org/en-US/firefox/products/

Intermediate

There are also less well-known browsers out there which are better for privacy. While none beat the mainstream browsers in terms of security, there are browsers that are better for privacy, such as Dragon and Epic. These browsers take privacy one step further by never recording your search history, automatically disabling trackers and cookies, using HTTPS whenever possible, and other useful privacy steps. Epic will even route all of your traffic through its own proxy server for free, hiding your identity from anyone on the web.

To increase safety on mainstream browsers, consider installing HTTPS Everywhere, which encrypts your data whenever possible, making it unreadable for anyone snooping. This can be installed on Google Chrome here, for Firefox here. Currently, HTTPS Everywhere isn't available for Edge or Safari.

Expert

Often seen as the best browser for privacy the Tor Browser. The Tor browser sends all your data through a random network of computers, so no one can trace which computer actually requested the data or where it went. However, logging into websites will still reveal your identity to anyone looking, so in practice there is a limit to how much you can hide with Tor. Furthermore, Tor is significantly slower than normal browsing due to all of the different computers that your data gets sent through.

Tor, therefore, only has a limited usefulness for average users. The Tor browser is best reserved for time when anonymity is truly important, not just for looking at cat gifs.

Cookies and Trackers

Beginner

It’s a smart idea to go through and clear your browser history every so often. The easiest way to do this is by opening your browser and simultaneously hitting CTRL + Shift + Delete on your keyboard. This brings up the window from which you may choose to clear various items, including (on Google Chrome): browsing history, download history, cookies and other site and plugin data (see intermediate for more info on cookies), cached images and files, passwords, autofill form data (see the topic on phishing), hosted app data, and media licenses. Other browsers have similar, if not the same, items to clear. You may also choose how far back you would like to clear the data selected, typically between one hour and to “the beginning of time,” which is a more exciting way of saying “all of it.”

Using incognito mode is a great way to keep your browser from collecting certain data, but it is in no way a perfect system. It prevents collection of local data, such as browsing history and certain cache data, but does not necessarily prevent all data from being collected.

Intermediate

Browser cookies are bits of data used to collect information based on what a user has entered while they are browsing, such as web addresses, usernames, and even passwords. They can record a user’s browsing, and there is even a kind of tracking cookie that collect a more-long term record of a user’s browsing activities. In order to delete these, follow the same steps from beginner, by hitting CTRL, Shift, and Delete after opening your web browser, then selecting to delete your browser’s cookies.

Installing and using Ghostery
Ghostery is a neat little browser plugin that allows users to see what internet trackers are collecting information on your internet activities, as well as what information it is they are gathering. It also allows you to block these trackers from collecting this information. It is a simple way to help gain some control of what information is being taken from your online experience.

Installing Ghostery to your web browser:
(I used Google Chrome. Instructions may vary slightly if using a different browser, such as Firefox or Safari.)

1. Begin by going to the home page, at www.ghostery.com
2. In the navigation bar, go to: “Our Solutions.”
3. Select: “For Consumers/Ghostery Browser Extension.”

4. Select: “add to browser.”
5. Select your web browser to download the correct version.
    a. On Chrome, this will guide you to Chrome add-ons, where you get more information about the extension and may select “Add to Chrome.”
6. A pop-up will appear, double checking that you wish to add the extension to your browser.
7. After adding the extension, a new tab will open, and a box appears asking if you would like to share certain kinds of data with Ghostery to better improve their products. *All data sharing is optional and up to you.*
8. Finally, it asks if you would like to create an account. This is also *optional and not required*.

To use Ghostery:

1. In the top right corner of your browser (when using Chrome), there will be an icon of a little blue ghost paired with a square containing a number. Click on this icon.
2. A box will appear, containing a list of whatever trackers are present on the site you are currently visiting.
3. You will be given the option to block these trackers, map the trackers, and trust or restrict the site.
4. By selecting one of the trackers listed, you may also find out more information about that tracker, and even view the tracker’s full profile.

Installing and using TrackMeNot

TrackMeNot is a background application that, rather than hide your internet activities, creates more “noise” to distract and confuse trackers and data collectors.

Installing TrackMeNot to your web browser:

(I used Google Chrome. Instructions may vary slightly if using a different browser, such as Firefox.)

1. Begin by visiting https://cs.nyu.edu/trackmenot/.
2. At the top of the page, you will find two links. One is for installing on Firefox, the other on Chrome (I will be using the Chrome installation for this guide). Select the appropriate link.
3. For Chrome, you will be redirected to the Chrome app store page for TrackMeNot. Click on the “Add to Chrome” button.
4. A pop-up will appear, double checking that you wish to add the extension to your browser.
5. TrackMeNot is now installed in your browser.

How to use TrackMeNot:

1. In the top right corner of your browser (when using Chrome), the icon for TrackMeNot will be listed.
2. TrackMeNot runs automatically. By clicking on the icon, you may:

   a. Disable the app.
   b. View options for how the app runs.
   c. View help and frequently asked questions about the app.

Installing and using Privacy Badger
Privacy Badger, another fun little browser add-on, blocks ads and trackers that may be collecting your data to better cater to your preferences based on past browsing patterns.

Installing Privacy Badger to your web browser:
(I used Google Chrome. Instructions may vary slightly if using a different browser, such as Firefox or Safari.)

1. Begin by going to the home page, at www.eff.org/privacybadger.
2. Scroll down until you see the "Install Privacy Badger" button, located in the center of the page. Click on the "Install Privacy Badger" button.
3. On Chrome, you will be redirected to the Google Chrome app store page for Privacy Badger. Select "add to Chrome."
4. A pop-up will appear, double checking that you are sure you wish to add this extension to your browser.
5. A new tab thanking you for installing the extension will pop-up. It will ask if you want to share that you have installed Privacy Badger through your social media apps. *This is completely optional* (though I would advise against it).

To use Privacy Badger:

1. In the top right corner (when using Google Chrome) there will be an icon of a badger, as well as a number within a box. Click on this icon.
2. From here, you can learn how Privacy Badger works, as well as view which potential trackers are currently being blocked by the extension.
3. The extension allows you to adjust what access the potential trackers have to your activities on your current web page, such as no access, blocking cookies, or full access. It automatically adjusts based on predictions of what each tracker is, though you may adjust each slider based on your own preferences as well.
4. There is an option to turn of Privacy Badger for a specific web page, by visiting that page in your browser and opening the extension, then selecting "Disable Privacy Badger for This Site." You also have the option to turn it back on.

Expert

At the end of the day, your browsing activity can only be partially hidden by using incognito mode and disabling trackers. When you access the internet, your computer is given a unique identity called an IP address. Every time your computer sends out a request for a website, that request contains your IP address, so that the server on the other end knows where to send the data too. The problem with this is that your IP address can be tracked and traced back to you. Even if you have cookies disabled and trackers blocked, websites can record what IP addresses were used to access their websites, and track what you access that way.

Virtual Private Networks (VPNs) are one way around this. When you access a site through a VPN, your computer actually sends the request to the VPN's server which makes the request to the website on your behalf and returns the results to you. Essentially, the VPN acts as a middle man, so the website can't see who is actually requesting the data.

VPNs are not a perfect solution, of course. While there are free VPNs out there, it's a much better idea to go with a paid option, which are often $5-10 per month. Furthermore, some VPNs can slow down your internet access because all of the data has to travel through your servers before it makes it to your computer. VPNs are also run by private enterprises who often record your IP address and requests, which can be retrieved by the government through search warrants.

An alternative to VPNs is the Tor Browser. The Tor Browser acts like a VPN, but it sends all of your data though a randomized network of computers instead. That way no one knows where the data came from or where it is going. This raises the privacy of the browser, but it can also slow down internet access significantly, as the data takes a long path to your computer. Tor is best reserved for when anonymity is truly important.

Privacy Settings

Beginner

It's important to know how to access your privacy settings to control how much information you're allowing others to access about you.

iOS: Settings

- Recommendations
    - Privacy
        - Turn location services off until you need to use them
        - Check what apps have access to your contacts, calendars, photos, Bluetooth sharing, and Health/Fitness data, as well as what apps have access to your social media account
            - Limit access as much as possible

        - At the bottom of the privacy settings, choose Advertising and turn on "Limit Ad Tracking"
    - Siri
        - Disable Siri: it records everything you dictate and sends it to Apple, including your relationship to your contacts (if you tell Siri), names of HomeKit-enabled devices in your home, your name, the names of your photo albums, the names of Apps installed on your device
    - Touch ID & Passcode
        - Don't allow Touch ID: it's easier to force you to unlock your phone with your finger than with a passcode
        - Review what you want to allow access to when locked
    - iCloud
        - Turn iCloud off as much as possible
    - Wallet & Apple Pay
        - Do not add any cards, remove any that are already on
    - Other
        - Review specific permissions for your apps, especially social media apps, and disable as much access as possible

Mac: System Preferences > Security & Privacy > Privacy

- Recommendations
    - Turn location services off until you need to use them
    - Minimize how many applications have access to your contacts, calendars, and reminders
    - Under "Accessibility," disallow all apps from controlling your computer
        - TextExpander is a built-in app that expands abbreviations into their long forms when you type (Ex. "tyvm" becomes "thank you very much.")
    - Under "Diagnostics and Usage," uncheck "Send diagnostic and usage data to Apple."
    - Click "Advanced" at the bottom of the window and check "Require and administrator password to access system-wide preferences"
    - When you're done making changes, click the lock at the bottom left corner of the window to prevent further changes without your password.

Android:

- Recommendations
    - Go to Settings and find "Location." Turn off location services so apps can't track you everywhere you go
    - Go to Settings and find "Apps." Click on each app and turn off permissions for everything you don't want that app to know about, especially if you don't know why it needs access. For example, does a flashlight app need access to your

contacts? Probably not. If in doubt, remove permissions; you can always add them back later.

- Go to Settings and find “Security.” At the bottom, find “Apps with Usage Access.” Open and turn off for all apps listed. This is not an essential setting for any app, so it will not break anything on your phone.
- Go to Settings and find “Google”
  - Find “Personal info and privacy.”
    - Find “Shared endorsements” and disable
    - Find “Search settings.” Clear “Recent Locations” and set to “Do not save.” Set “Private results” to “Do not use private results.”
    - Find “Activity controls.” Pause everything inside.
    - Find “Ad Settings.” Turn off ad personalization.
  - Find “Ads.” Turn on “Opt out of Ads Personalization”
  - Find “Connected apps.” Review what apps you actually want connected to your google account.
- Search through other settings, as devices from different manufacturers may have more settings.

Windows:

- Recommendations
  - Open up Settings, find “Privacy”
    - Under “General,” turn off all settings except for SmartScreen filter. Click the link “Manage my Microsoft advertising…” and disable all options.
    - Under “Location,” disable all available settings.
    - Under “Camera,” disable permissions for all apps except what you need. If you don’t need any, disable camera altogether.
    - Under “Microphone,” disable permissions for all apps except what you need. If you don’t need any, disable microphone altogether.
    - Under “Account Info,” turn off all settings.
    - Under “Contacts,” turn off all settings.
    - Under “Calender,” turn off all settings.
    - Under “Call History,” turn off all settings.
    - Under “Email,” turn off all settings.
    - Under “Messaging,” turn off all settings.
    - Under “Other Devices,” turn off “Sync with devices.”
    - Under “Feedback & diagnostics,” find “Diagnostics and usage data” and set to “Basic”
    - Under “Background apps,” disable everything you’re not certain you want running all the time, especially the camera.

Removing Yourself from MSU People Search

1. Go to stuinfo.msu.edu
2. Click on the “Other” tab and select “Directory Restrictions”

3. Scroll to the bottom of the page and select “Update Restrictions”
4. We recommend restricting everything except Academic Status and MSU email address

Intermediate

Fake information: Use fake information for unimportant accounts in order to avoid having your data being collected and tied back to you easily. This sort of practice is best reserved for accounts that you don’t want tied back to you in real life. For important accounts, like ones for your bank, your school, your government, or other important and official sources, always use your real information.

Burner email accounts: Use 10 Minute Mail to get a temporary email address for any accounts you set up that are temporary or unimportant (a website you’re only accessing once or twice), or not connected to your real identity (game accounts). These accounts are also good for websites that require an email address or an account to access, or for signing online petitions.
If you want a more permanent burner account, create an email account using fake information and immediately check the privacy settings of the account.

Expert

If you really want to go the extra mile, look through every application, browser, and website you use for their privacy settings and adjust as necessary. Advice on how to do this for everything would take up too much space, but google should help you find anything you need to find.

Encryption

Intermediate

There are several apps and services you can use to better secure your communications online and over SMS.

Signal and **Whatsapp** allow you to text and call securely through their apps using end-to-end encrpytion. While nothing is ever totally secure, even the parent companies that provide these services can’t decrypt your data in these services, making them about as secure as you can get.
The TOR Browser provides the most anonymous online experience possible, although even TOR has its limits. If you want to know more, take a look at the entry for TOR in the “Browsers” section.
DuckDuckGo is an alternative to Google for searching the web, and has the primary advantage of not recording your searches.

ProtonMail is a free, secure email provider which encrypts all of your communications to ensure that no one can read your emails. As always, though, communication is only as secure as the person on the other end.
Periscope is a live video streaming tool often used by activists concerned that the authorities will delete any videos they take of a situation. However, keep in mind that Periscope publishes metadata like the location of the video by default, so turn those off if you are concerned about those things.

It is also highly recommended that you don't use your fingerprint scanner; it's possible for someone to force you to put your finger on a scanner against your will, but not possible for someone to force you to input your password against your will. Legally speaking, law enforcement can force you to use your finger to open your phone, but your passwords might be protected by your constitutional right against self-incrimination.

Expert

Encrypting the information on your phone or hard drive is the best way to secure it against other people, but it isn't without risks. Encrypting your phone or hard drive means that the information is coded and gibberish unless unlocked with the password. It is generally extremely secure, but if you forget the password, no one can access it, not even you. If you are going to encrypt your hard drive or phone, then, be aware of the risk.

Encrypting phones smartphones is easy. If you navigate the settings of your smartphone, you should find an option to encyrpt your device. Numerous guides exist online to help you do this. Note that you will probably have to have your phone plugged in for this to work, and your device will not be usable while it's encrypting.

Encrypting a hard drive is more complicated, and has the potential to go very wrong. If you encrypt a hard drive and forget the password, there is nothing you can do to save it. This does not mean that you should not encrypt your hard drive, but it does mean that you should think carefully before you decide to go ahead. If you decide that encrypting your hard drive is something you want to do, visit this site for Windows, or this site for Mac.

Data Detox

Intermediate

You may think that it doesn't matter if someone has information about what you like, whether you work out, or where you shop, but put together, this information creates a startlingly accurate picture of you as a person. It's as though someone is watching everything you do and recording it. This is an 8-day plan for data detox, a way to take some of your information offline and make that picture a little less clear for the corporations who want to track you. The *8-Day Data Detox Kit* by The Glass Room by Mozilla + Tactical Tech is available for download here: https://theglassroomnyc.org/data-detox/

Expert

If you have already taken basic detoxing steps, it's a good idea to take a look at *A DIY Guide to Feminist Cybersecurity*, a detox guide designed for activists. This guide focuses much more on safety and keeping your personal information offline and secure, in order to avoid doxxing. *A DIY Guide to Feminist Cyber Security* is available here: https://hackblossom.org/cybersecurity/