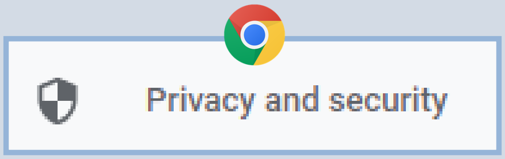
Internet Beyond Basics

Tips for online security and privacy

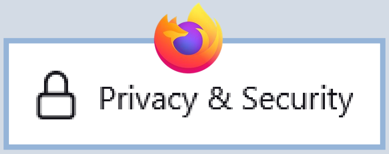
Online Safety and Privacy

Staying secure online can feel like a challenge with the variety of threats and hard-to-spot scams used by hackers. On top of that, marketing schemes often trail you around the web tracking your activity. The good news is there are things you can do to protect yourself online. As web users demand more security and privacy, web companies are creating new options for online protection. Learning to use the tools available can dramatically improve online safety and privacy. This course will give you tips and tricks for protecting yourself online and maintaining your anonymity.

TIP Many web browsers offer privacy and security options in Settings. To access your web browser's settings, look along the browser toolbar for the menu icon. (Many browsers have either three lines or three dots to indicate the menu.) Once the menu is open, click on Settings. In Settings, look for a section called Privacy and Security to get started.



Privacy and security



Privacy & Security

POUDRE RIVER PUBLIC LIBRARY DISTRICT | CONNECT TO CURIOSITY

www.poudrelibraries.org

Maintaining Strong Passwords

An important way to increase your online account security is to practice strong password measures. Follow these tips for password safety:

- Use a mix of upper and lowercase letters, numbers, and symbols in your password. Complex passwords are harder to guess.
- Create a long password (8 or more characters). This increases your password's complexity.
- Use a different password for every online account. Although this can be a challenge, it is essential for online security. Otherwise, if someone finds out one password they could access several accounts.

TIP Password generators are a handy tool for creating complex passwords. Password generators let you set your preferred length and complexity and then create a strong password for you. Try Norton's Password Generator:

https://my.norton.com/extspa/passwordmanager?path=pwd-gen

Norton™

Remembering Passwords

Most people struggle with remembering passwords. Having a plan for keeping track of passwords makes it easier to use multiple passwords and saves the hassle of frequently resetting passwords. If you would like to keep a written record of your passwords, I recommend getting a notebook dedicated to only your passwords. Keep it in a secure place. Another option for keeping passwords is using an online password keeper like Bitwarden or Myki. An online password keeper stores the logins for all of your accounts. Often, it will also autofill passwords on website login pages.

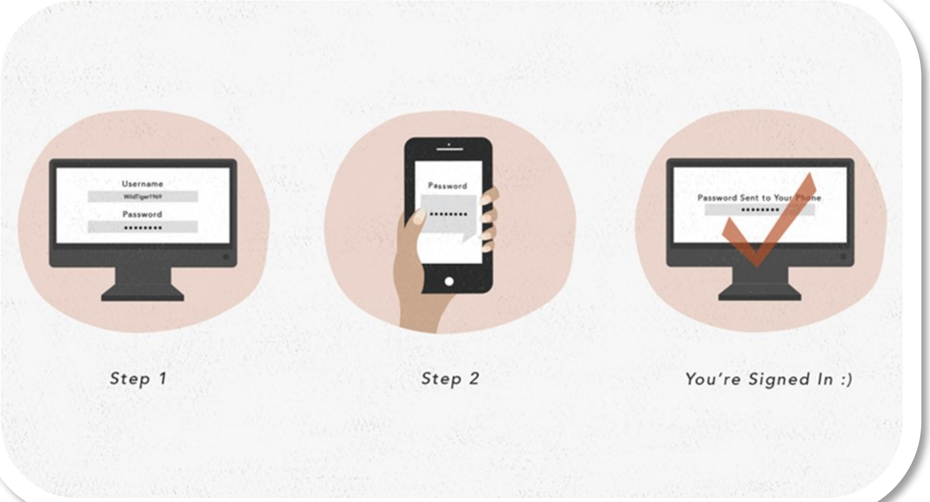
bitwarden

MYKI

Two Factor Authentication

Some accounts feature an additional layer of security called "two factor authentication." This security feature requires two types of verification to login to your account. It will ask for two of three types of verification. **Something you know,** such as, a PIN or password. **Something you have,** like your phone or ATM card. Or, **something you are,** like your fingerprint or voice response. By requiring two things rather than just a password, two factor authentication strengthens account security. Even if someone gains access to the password, they will not be able to complete the additional verification step. Some accounts automatically have two factor authentication. Others allow you to set up two factor authentication as a security option.

Definition and Illustration from GCF Learn Free. Learn more here: https://edu.gcfglobal.org/en/thenow/what-is-twofactor-authentication/1/



Avoiding Phishing Scams

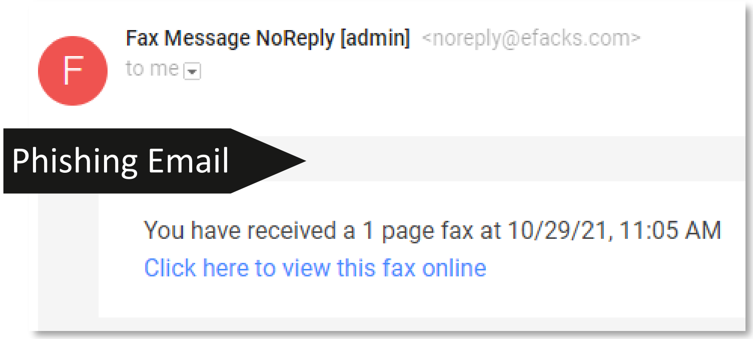
Phishing scams are attempts to retrieve your personal information by posing as a trusted service or offering a reward. Phishing scams often come in the form of emails that mimic legitimate messages.

Here are some tips for avoiding phishing scams:

- **Check the sender's email address for errors.** Phishing scams often come from email addresses that look legitimate at first glance but contain typos or incorrect spelling when you take a closer look.
- **Review the content.** Phishing scams ask for sensitive information, such as, account logins, birthdates, or SSN. If an email is asking for sensitive information, do not click on the link in the email. Instead, go to the website for that company directly and

check your account to see if your information needs to be updated.

- **Don't open files or links you were not expecting to receive.** If you were not expecting a shipping notice, fax or other email you receive, chances are it is a phishing scam.
- **If unsure, ask.** When in doubt, call and ask the sender directly if the email is legitimate.
- **Hover over links to see full URL.** If you move your cursor over a link, the location for that link will appear in the bottom left corner of the browser. Check this URL carefully to see the link's destination.



Fax Message NoReply [admin] <noreply@efacks.com>
to me

You have received a 1 page fax at 10/29/21, 11:05 AM
Click here to view this fax online

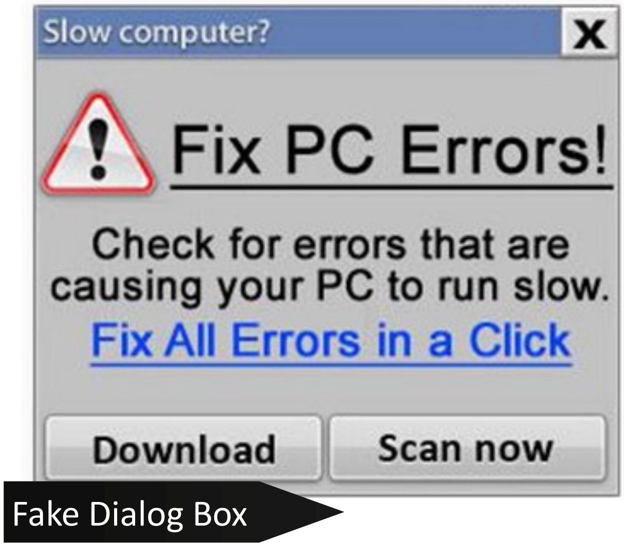
Phishing Email

Take this quiz to test your ability to identify phishing scams: https://phishingquiz.withgoogle.com/

Malware

Malware can prevent your computer from working, cause frequent crashing, or even corrupt data. For most malware to get onto your device, you must click on or download a malware file. Often, malware attempts mimic legitimate computer windows or services. Types of malware include computer viruses, ransomware, and adware. Follow these safety tips:

- Be cautious about downloading from websites or emails
- Verify a link's destination before clicking
- Be suspicious of urgent statements
- Keep your operating system up-to-date
- Install anti-virus/anti-malware software on your computer
- Keep your browser up-to-date



Slow computer?

Fix PC Errors!

Check for errors that are causing your PC to run slow.

Fix All Errors in a Click

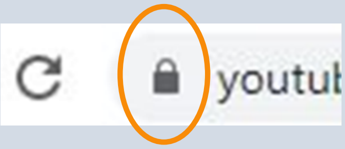
Fake Dialog Box

Identifying Secure Sites

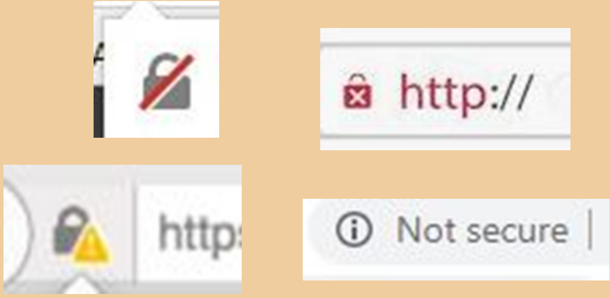
While browsing on the internet, it is important to keep an eye out for insecure websites. Secure sites begin with https while insecure sites begin with http. Your web browser will indicate whether a site is secure or insecure. Look at some of the symbols here to familiarize yourself with this feature.

TIP Try Google's Safe Browsing tool to see if a website has been flagged: https://transparencyreport.google.com/safe-browsing/search

Secure Site



Insecure Site



Browser Data & Privacy

With many hidden trackers across websites, it can be difficult to know how to keep your activity online private. Understanding browser data and how to change browser privacy settings can make a difference in your online privacy experience. There are three types of browser data:

History – A list of webpages visited in the browser beginning with most recently visited webpages.

Cache – Information on webpages, such as, logos or images, saved in your browser's memory for quicker loading times.

Cookies – Small files that record activity on a website, such as, logging into an account. Some cookies are required for a website's features to work. Other cookies are used to track user behavior.

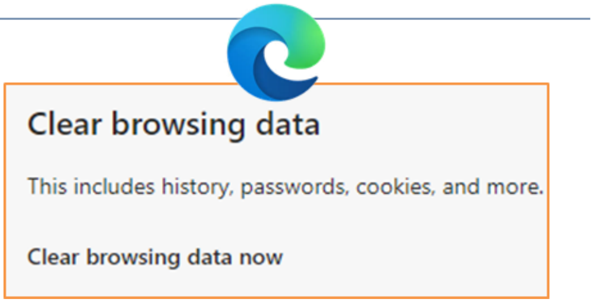
Clearing Browser Data

It is a good idea to periodically clear your browsing data both for privacy and to keep your browser running optimally. To clear browser data, follow these steps:

1) Go to the settings page

2) Choose Privacy/Security

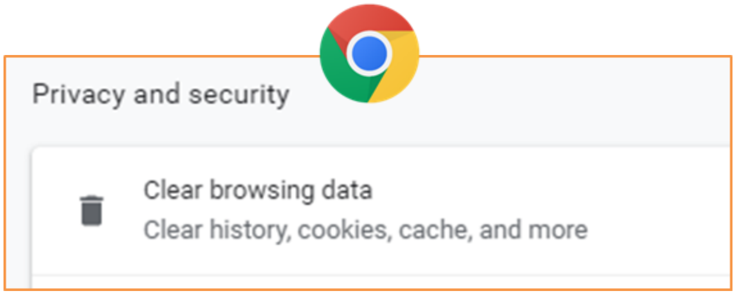
3) Select the option to clear data.



Clear browsing data

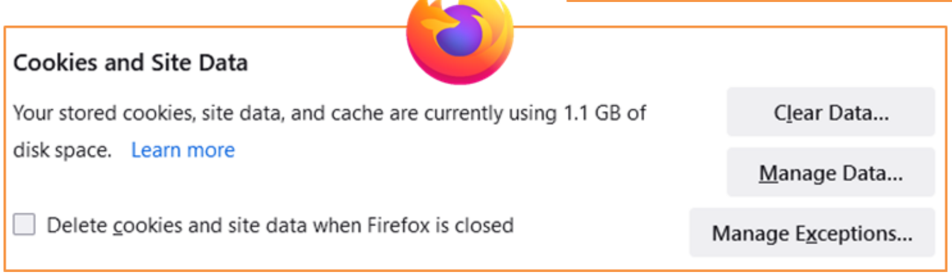
This includes history, passwords, cookies, and more.

Clear browsing data now



Privacy and security

Clear browsing data
Clear history, cookies, cache, and more



Cookies and Site Data

Your stored cookies, site data, and cache are currently using 1.1 GB of disk space. Learn more

Clear Data...

Manage Data...

□ Delete cookies and site data when Firefox is closed

Manage Exceptions...

Tips for Private Browsing

If online privacy is a priority for you, here are some tips for staying private online.

- **Use Incognito/Private mode** – Browsers now offer an incognito or private session. When set to incognito/private mode, the browser does not keep your browsing history. To access this mode, open settings in your browser and look for the option for opening a new window in Incognito or Private mode. This is most important on a shared computer.

- **Use a browser with strong privacy settings** – Try the Firefox or Brave browsers which offer strict privacy settings. Visit the settings page to view all the privacy options.

- **Replace Google as your search engine** - Google search tracks user location and browsing habits and sells this data to advertisers. Try DuckDuckGo instead of Google. DuckDuckGo does not track your location or searches.

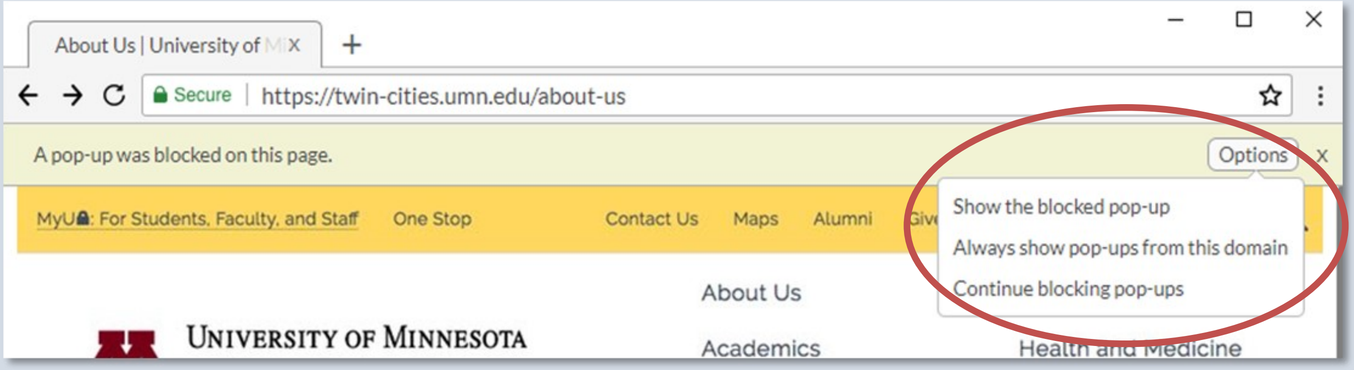
- **Configure Privacy/Security Options** – Whatever browser or online account you use, review the Privacy/Security section to make adjustments that fit your privacy preferences. These options can be found under settings.

- **Install Privacy Extensions** – Try a web browser extension to help block trackers. Some suggestions: Privacy Badger or DuckDuckGo Privacy Essentials
- **Review Privacy Policies** — Reviewing privacy policies for online accounts is a good way to protect your information. Different companies require different information to use their websites. The company's privacy policy explains what data it collects and why. Some things to look for include what information is required to use the website and whether the website shares your information with third parties. For more information on what to look for in privacy policies, checkout TechBoomers' course on privacy policies including 10 questions to ask: https://techboomers.com/t/privacy-policies.

TIP

Opening Pop-up Windows

Browser security features block pop-up windows from opening in your browser. This is a good thing as many pop-ups are advertisements, malware, or phishing attempts. Sometimes, however, a pop-up window is required to complete a task. If you need to see a pop-up window that your browser has blocked, choose options from the notice that appears and select "Show the blocked pop-up."


A pop-up was blocked on this page.
About Us | University of M X
+
Secure
https://twin-cities.umn.edu/about-us
Options
x
Show the blocked pop-up
Always show pop-ups from this domain
Continue blocking pop-ups
MyU: For Students, Faculty, and Staff
One Stop
Contact Us
Maps
Alumni
Give
About Us
University of Minnesota
Academics
Health and Medicine

Resources for Further Learning

Continue developing computer skills with the following resources:

Poudre River Public Library — We are committed to supporting you as you Connect to Curiosity in technology tools. Take advantage of our free assistance at a class or by stopping by a help desk.

Recommends: Hands on Tech: Google Docs and Tech Tips video collection. Visit our resources at https://read.poudrelibraries.org/research/z264.html

GCF Learn Free — Quality collection of technology tutorials free of advertisements and free to use.

Recommends: Using the Web to Get Stuff Done, Tech Savvy Tips and Tricks. Check out all they have to offer at https://edu.gcfglobal.org/en/subjects/tech/

TechBoomers — This website's collection of insights and tutorials are valuable for anyone working on strengthening their tech skills. They house a great collection of tutorials on specific websites and apps.

Recommends: Internet 101: Privacy and Internet 101: Security. Access the course directory at https://techboomers.com/courses

Learn My Way — Step-by-step courses for building computer skills in bite-size pieces. Includes built-in read-aloud software for audio accessibility.

Recommends: Online Safety and Video Calling. View their courses at https://www.learnmyway.com/subjects

LinkedIn Learning — Access to this database of computer and business classes is offered with a library card.

Recommends: Working and Collaborating Online. Find it on the Library's Research page: https://read.poudrelibraries.org/research/eresources.cfm?flter=alll

Digital Learn — Free tech tutorials from the Public Library Association.

Recommends: Being Safe Online and Intro to Email 2: Beyond Basics.

Access these courses at: https://www.digitallearn.org/