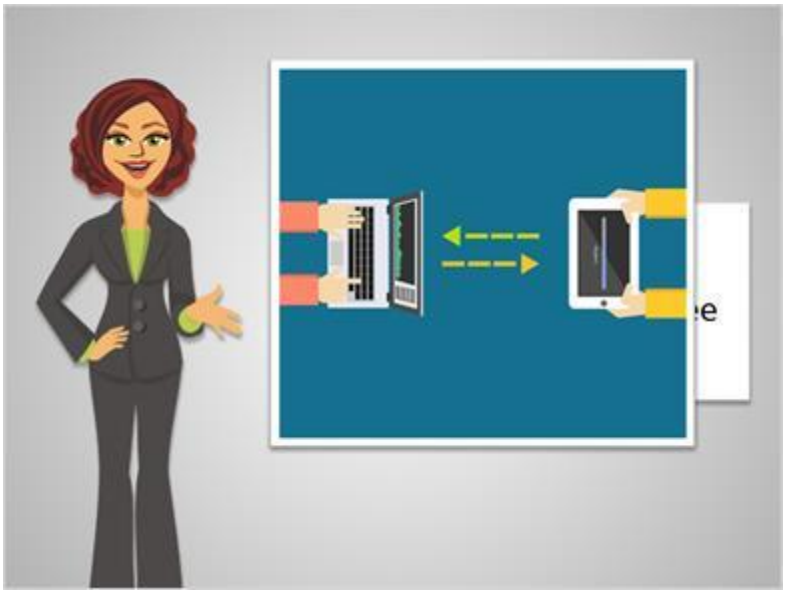
Internet Privacy

Hi, I'm Kate. We're here to learn about Internet privacy. We'll look at different internet privacy risks, and practical things you can do to help keep your personal information private and safe.

We'll follow along with Michelle as she browses the web. Today she'd like to buy a pair of shoes online and share a photo on Facebook. While she does this, we'll help her stay in control of privacy.

Ready to get started? Click the green button to continue.

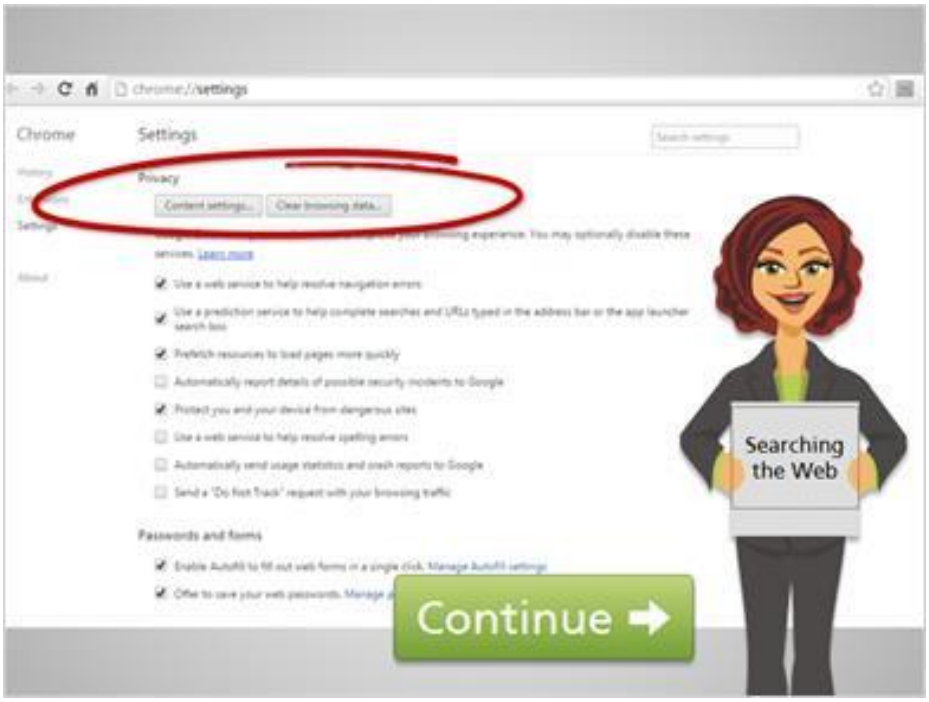


While browsing the Internet, we are constantly sending and receiving information from various websites and individuals.

When we send and receive information, we can take control of who is able to see that information, and how much information they can see. Internet privacy refers to the level of personal, private information we share.

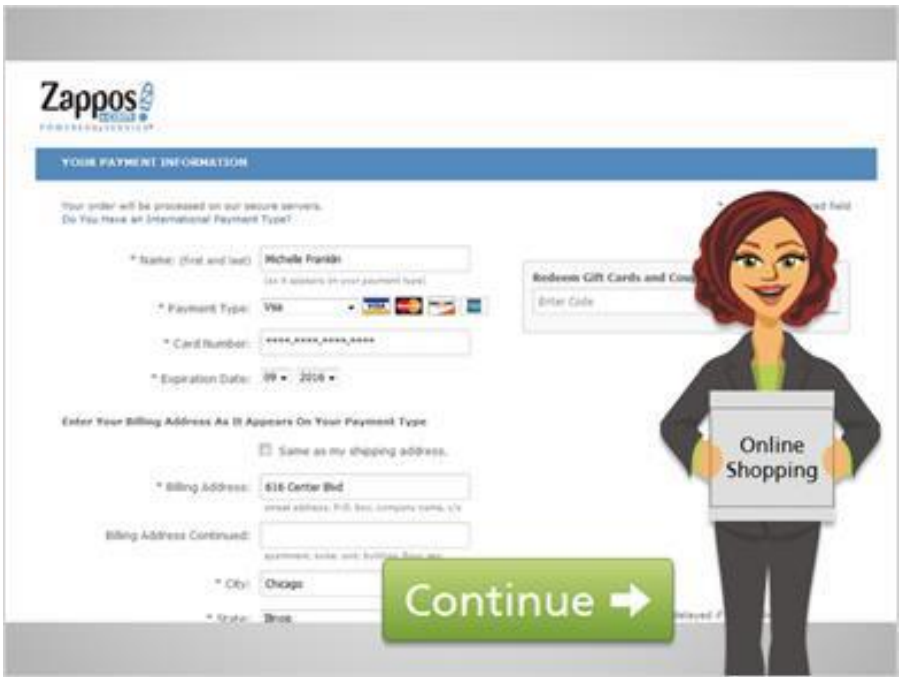
Here are four common tasks on the Internet that involve sharing information. Some information should be completely private, like credit card numbers and passwords. Other times, we may want to share something with others, but limit who can see it. In this course, we'll share tips for protecting privacy as we complete these tasks on Internet.

Click on each topic for more about privacy concerns.

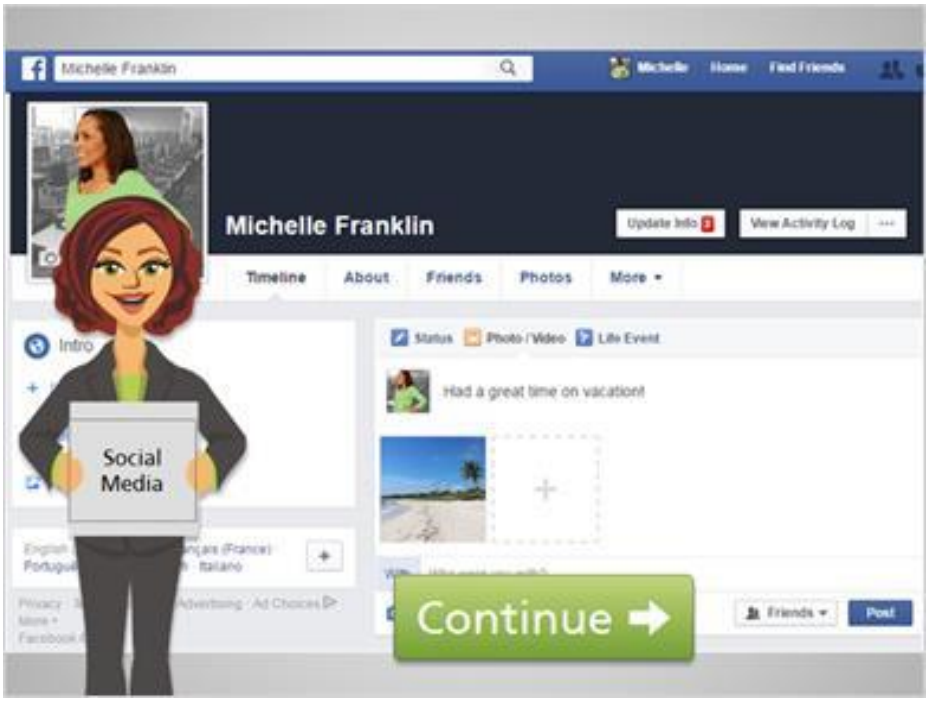


When searching the web, your searches are often saved on the computer you're using. The search engine company can also see information about what you're searching for. Web browsers have settings you can apply to control the information that is tracked and saved.

Any time you visit a website, the owner of the website can see general information about the type of computer you are using and what you are doing on the site.



Online shopping requires sending information like your passwords and credit card numbers to a website. You'll want to make sure the website is trustworthy and this information will be kept private.

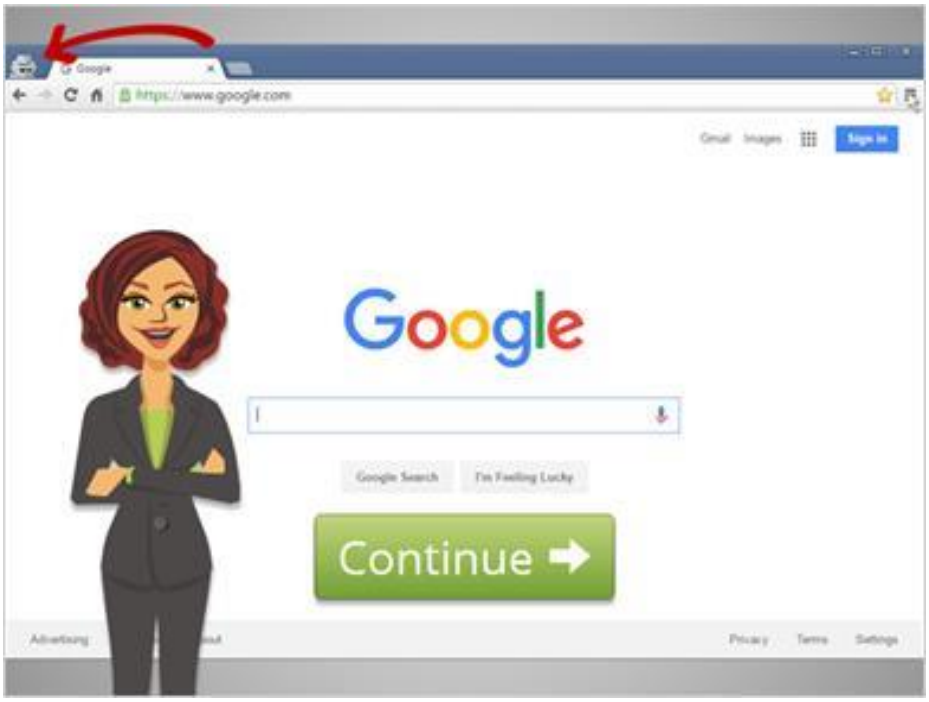


Social media sites like Facebook, Twitter, and Instagram are all about sharing. You can share things publicly, with groups of people, or with individuals. Companies like Facebook also have access to some information about what you share.

Good job. In this course, we'll see how to stay in control of your privacy as you use the Internet. Click the green button to move to the next lesson.

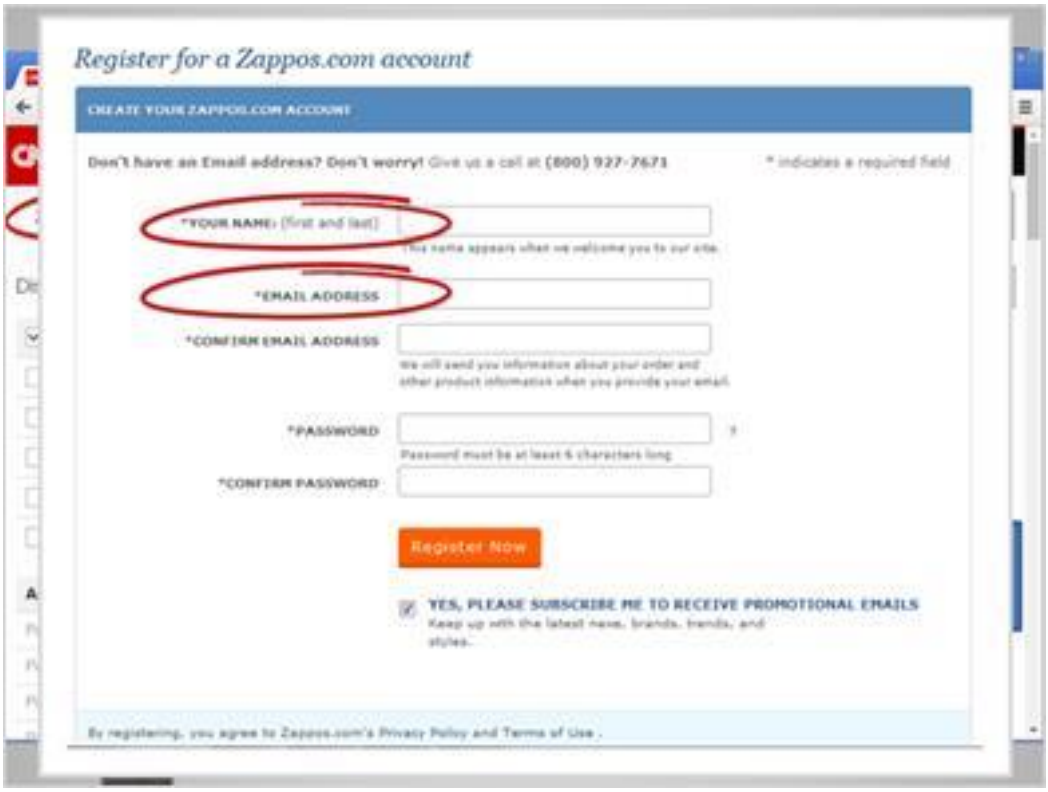
Searching and Visiting Sites

Michelle wants to buy a pair of shoes online. What privacy issues should she think about when searching the web and visiting a website?



When we use a search engine to search online, information is tracked on our keywords. Web browsers include privacy settings that allow us to control what is stored and tracked.

To be as private as possible, Michelle will open a private browser window. This will keep search engines from tracking her as she searches, and will keep the browser from saving her search history.

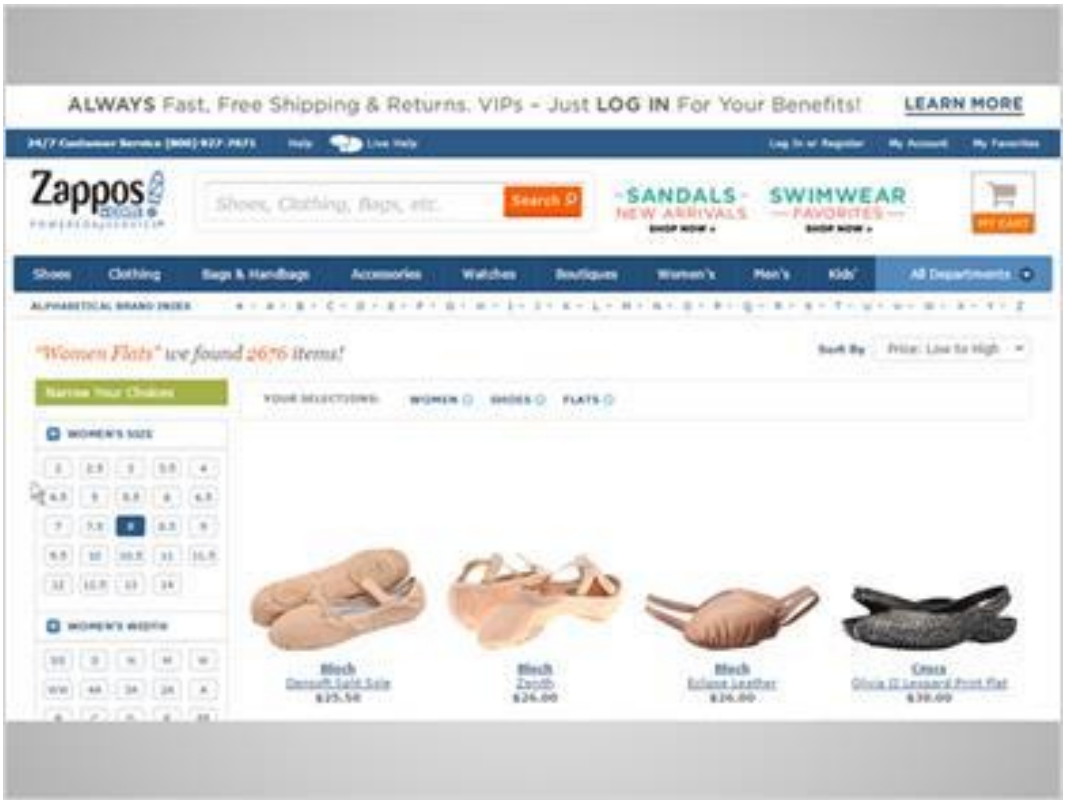


Any time you visit a website, information is collected, including your geographic location, the links you click on, and other information about your web browser, computer, or other device you're using.

This information generally doesn't identify you as an individual, but gives the website owner helpful information about demographics and technologies their visitors use.

Some websites collect more specialized information. They may scan for keywords you use, and use those words to show advertisements.

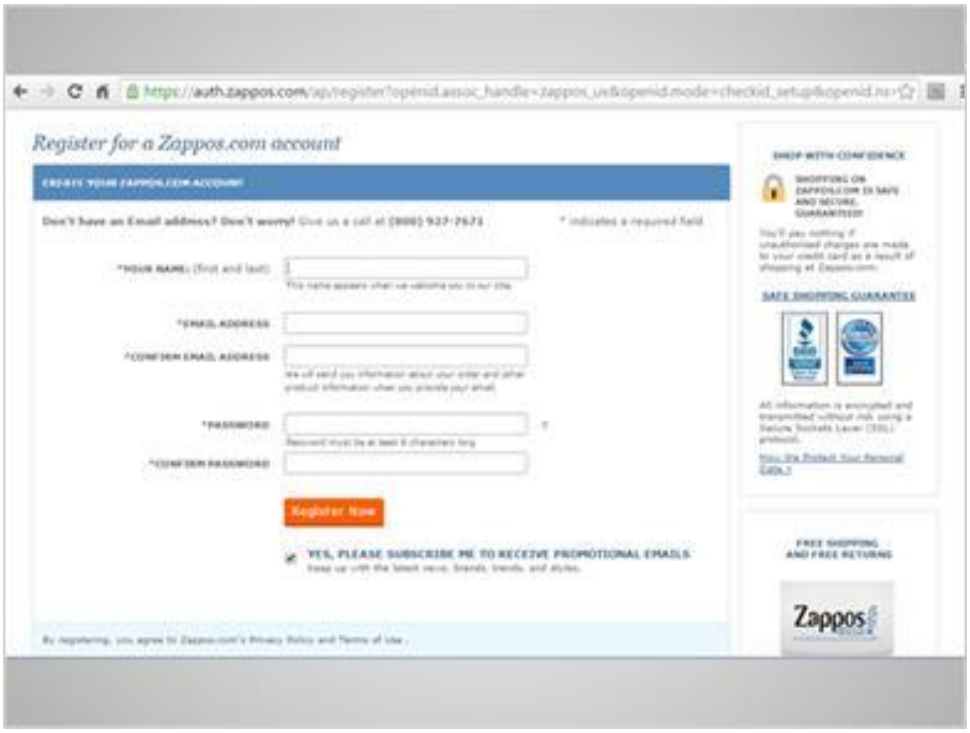
If you create an account on a website, the site owner will also have access to information like your name, email address, or even your physical address and phone number. They could use this information to send you marketing emails or letters.



Michelle has located a popular online shoe store through her search. She clicks on the style she likes, and searches for her shoe size.

The website will keep track of what she browses and searches for, but it doesn't know who she is or have a way to contact her, because she hasn't created an account with them or submitted any personal information yet.

She'll need to do that to make the purchase, but before that, she'll do some research.



First, she'll check the About Us page to make sure this is a legitimate company.

Then, she'll check for a privacy policy. This policy should explain how the company will use her information, and whether they will share it with partners or sell it to other businesses.

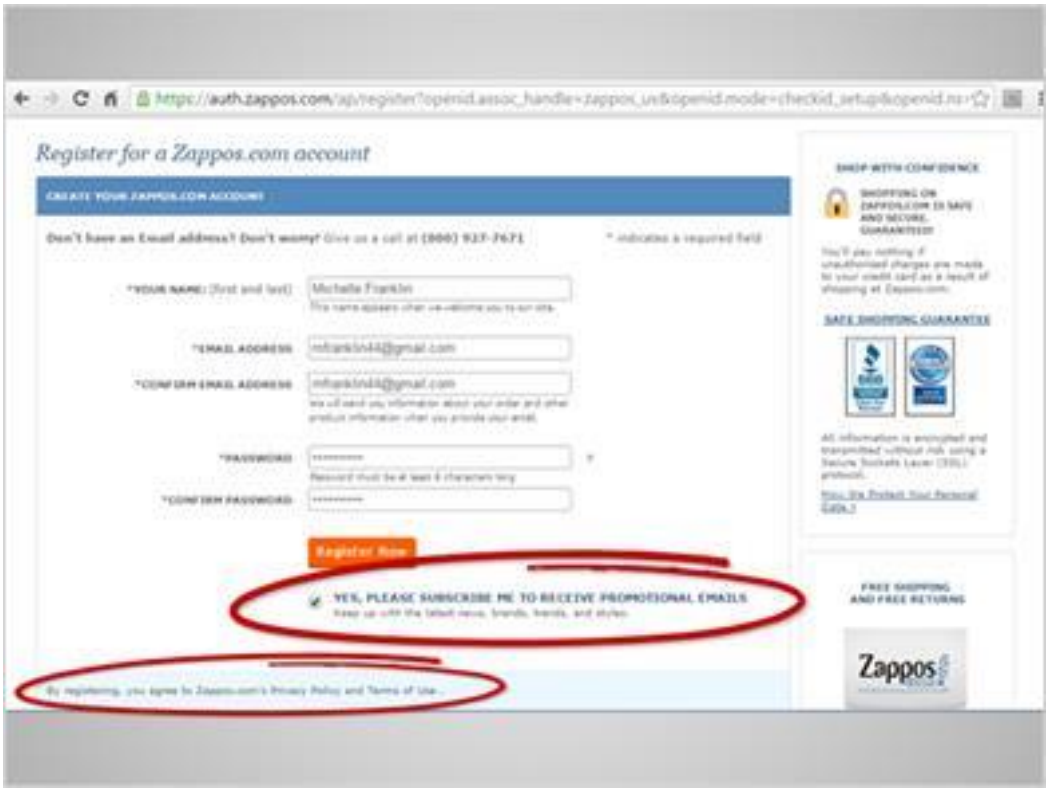
This website looks okay so far, so she gets ready to create an account.

Before entering any personal information, she should check to see if the website has a secure connection.

Michelle can see if the site is secure by looking at the web address. The web address starts with https, instead of just “http”. That “S” stands for Secure. You can also see a padlock icon here.

This means that anything Michelle enters here will be “encrypted” or put into a code before it’s sent to the website. No one else can see this data until it arrives safely on the other end.

If a website does not start with “https,” don’t enter any information that you want to keep private.



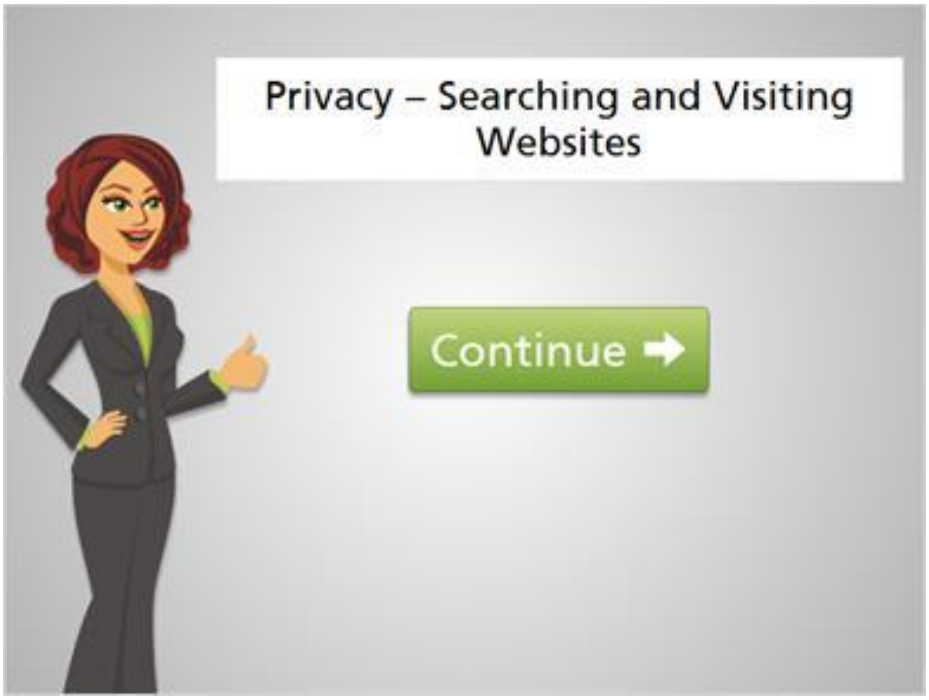
Michelle has decided to use this website, but she still has some choices to make.

This website asks her if she will give them permission to send her marketing emails. She can uncheck this box before submitting the form.

She also has to agree to their privacy policy. It's a good idea to read through any policies like this one before agreeing to them. If you see anything you aren't comfortable with, try using a different website.

	Before setting up an account on a website, it's important to control your level of privacy by:
	Checking that the connection to the website is secure
	Visiting the About Us page to ensure the company is legitimate
	Agreeing with the website privacy policy
	All of the above

The correct answer is All of the Above.

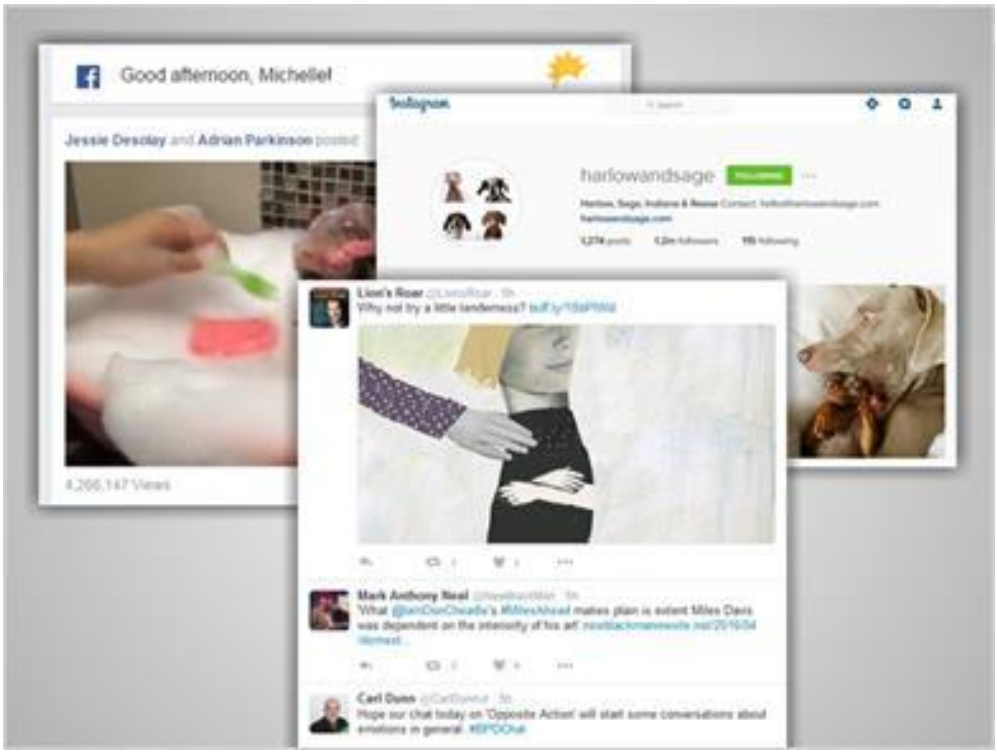


Good job. Now click on the green button to proceed to the next lesson.

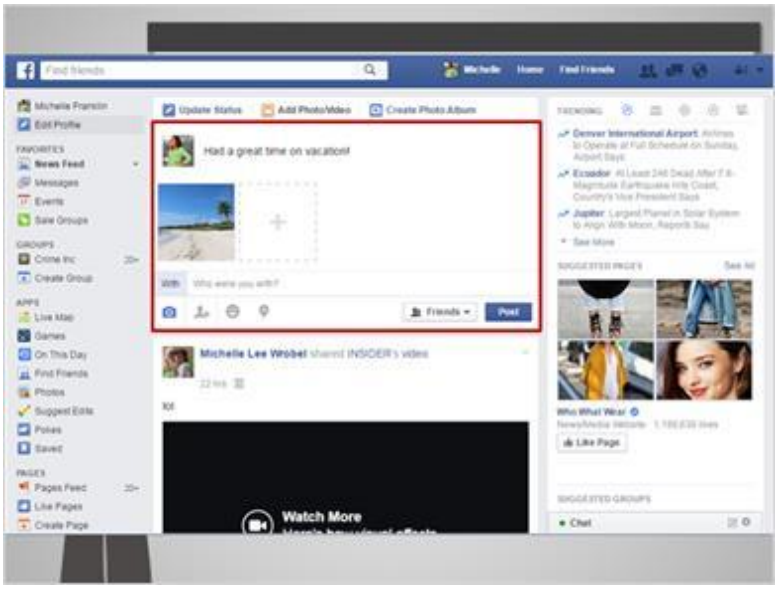
Privacy on Social Media

Michelle wants to share some photos online with her family.

Before she puts them online, it's a good idea to think about who she wants to see them.



Social media sites like Facebook, Instagram and Twitter are used to share photos and updates about the things you're doing. They are also used to share opinions, support causes, and share personal details like where you work and where you're from.



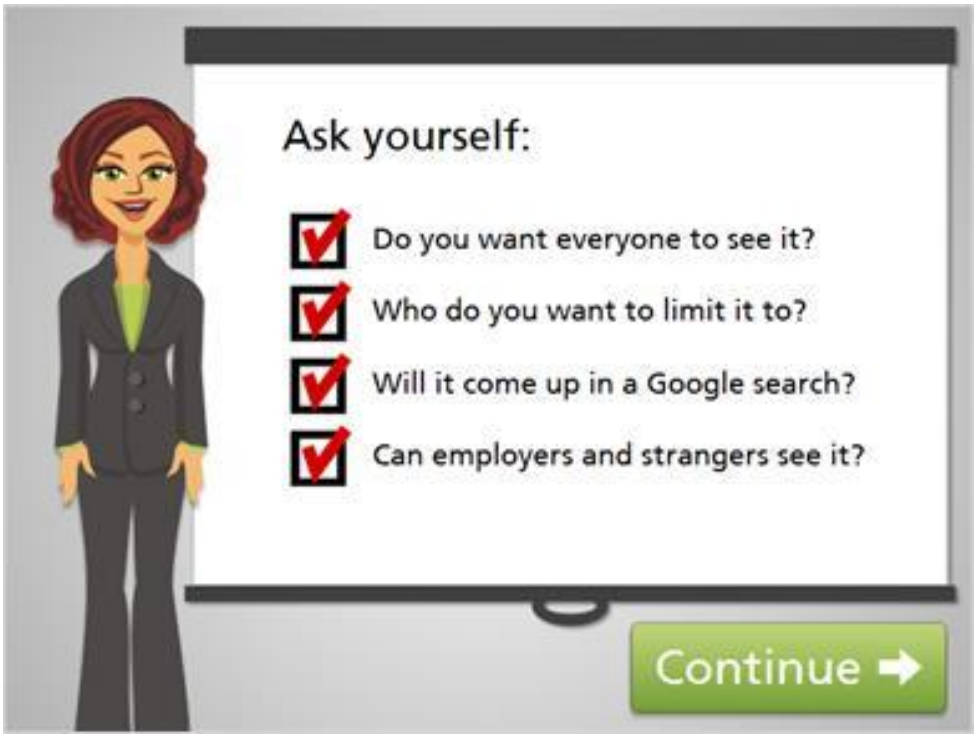
While it's fun and engaging to share online with family and friends, there are many reasons you may NOT want to share something publicly.

Once something is shared online, it can be difficult to completely erase if you change your mind later.

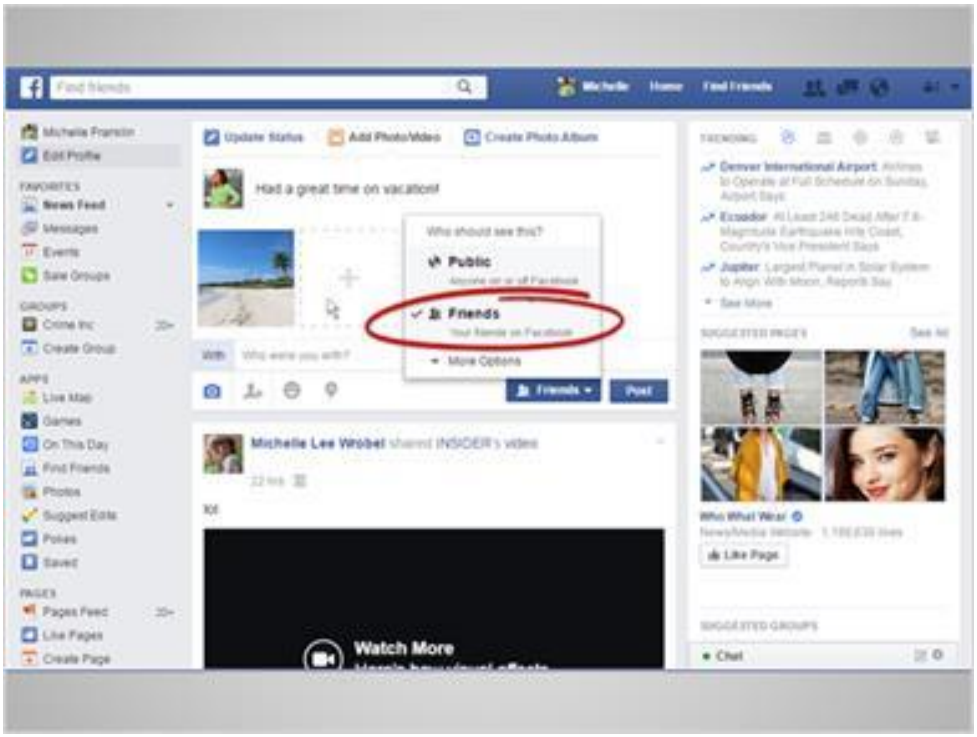
It's also hard to know exactly who will see your information. Even if you restrict a posting to a certain group of people, those people might repost the information without your permission. Also, a social network can change its privacy policies at any time, which can alter the privacy of the things you've shared.

You may feel like no one would care about your personal posts, but you never know who will be searching for information about you. For example, employers often look at the social media profiles of job applicants when they are making hiring decisions.

In Michelle's case, she's sharing a photo that she took on vacation. She wants her close friends and family to see it, but she doesn't want to advertise to everyone that she is out of town.



Before sharing information online, ask yourself these questions:
Do you want everyone to be able to see this?
If not, who do you want to limit it to?
Will it come up if you search for your name on Google?
Will employers or strangers be able to find it?

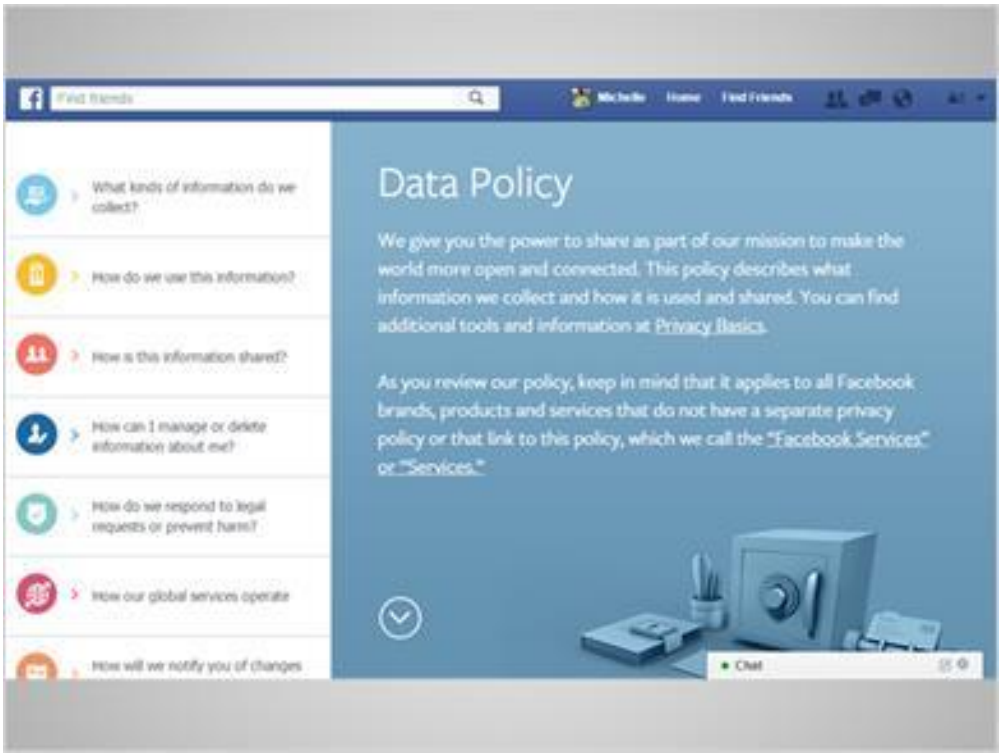


Many websites allow you to send private messages to individuals, or limit posts to particular groups.

In Facebook, you can control your general privacy settings here.

You can also control the privacy for each individual post.

Michelle will limit this message to “Friends.”



Finally, keep in mind that social networking companies have access to the information you post. Look for a privacy policy on each site to see how your information is being used.

How can we protect privacy on social media?
Learn about the site's privacy policies
Adjust general privacy settings on each site
Adjust privacy settings on each post
Avoid making posts public
All of the above

The correct answer is All of the Above.

Every social networking website offers different settings related to privacy. Be sure to review the privacy settings on any social media networks you use.

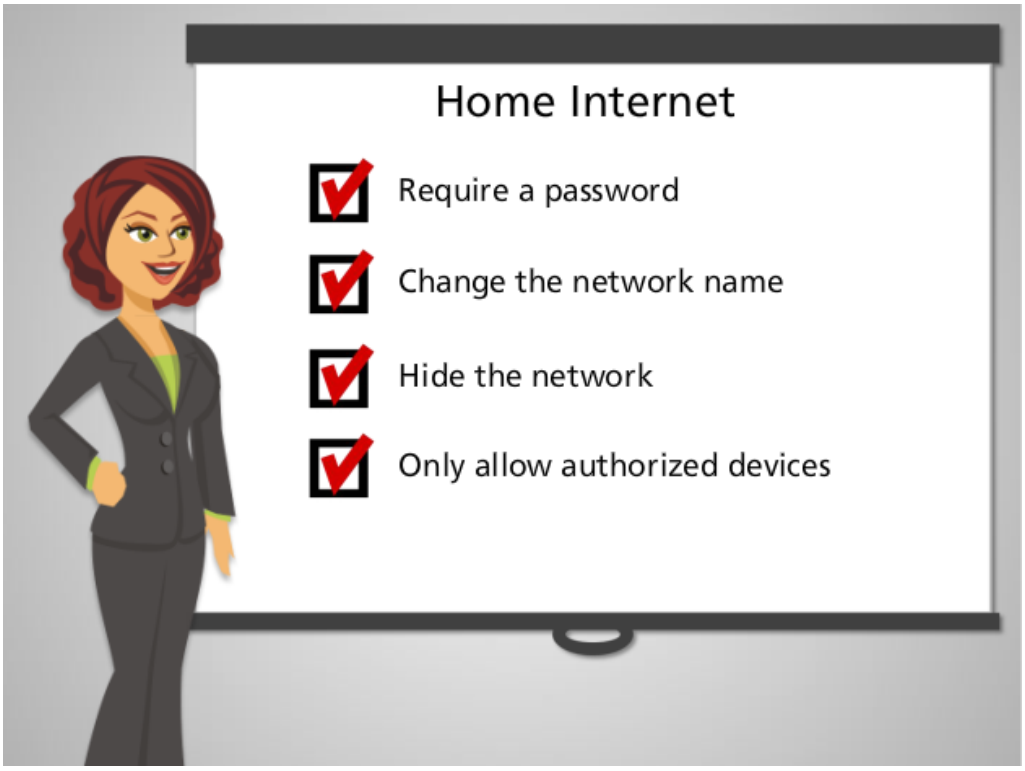
Internet Connections

The way you connect to the internet also affects your level of privacy.

Some internet connections are secured and private, others are public connections that anyone can access.

Michelle usually accesses the internet from home. At times, she uses the free Wifi at her local coffee shop. She also uses the public computers at her local library.

Click on each type of internet connection to learn how to reduce your privacy risks.

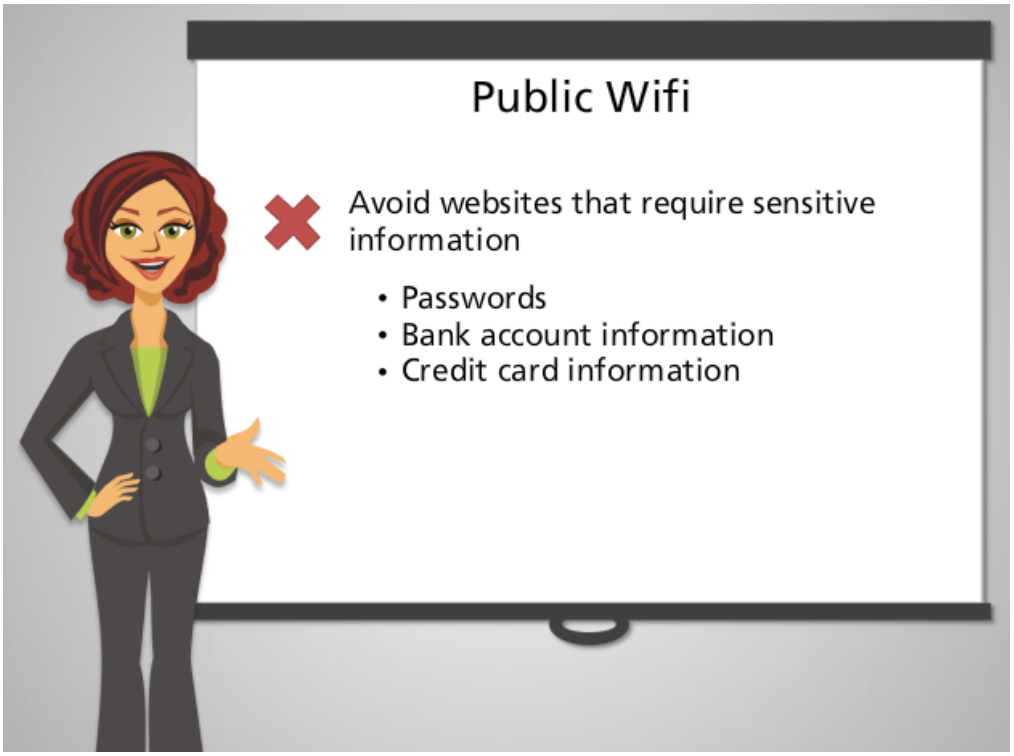


A home internet connection can be set up securely, or it can be open for anyone to connect to.

If your internet is not secured, someone might try to intercept information, such as our banking credentials, account passwords, and other valuable information. Neighbors would also be able to use your connection, making it slow.

To protect against this, you can secure your home internet connection by requiring a password to get on, changing the network name, hiding the network from view, or only allowing authorized devices to connect.

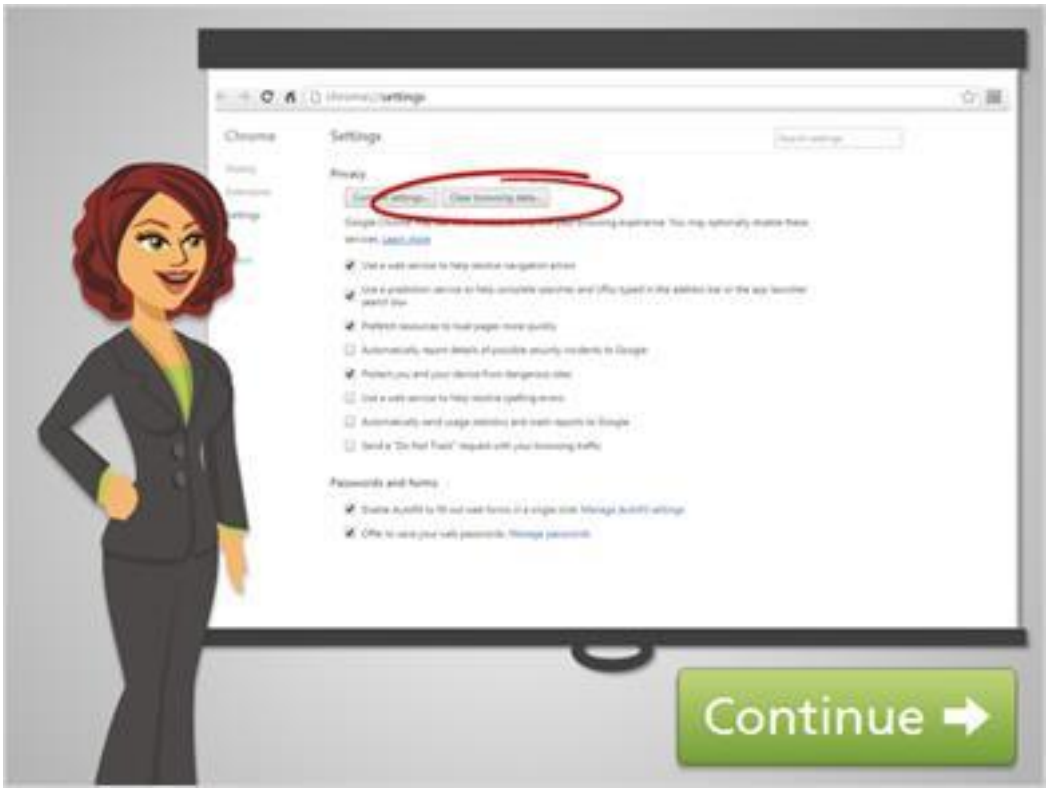
To learn how to configure your home network, visit onguardonline.gov. The steps are different depending on what equipment you use.



Free wifi is often available in coffee shops, airports, shopping malls, and other locations. While this is convenient, it can be unsafe if you aren't cautious. Those who are looking to intercept and steal private data will often use public wifi.

You can take several steps to be safe on public wifi. First, make sure your computer has a personal security system, known as a firewall, enabled. For more on firewalls, visit NEED SOURCE. Next, check with the location owner that the free wifi connection is legitimate. Then, make sure that any site you use has a secure connection before entering any personal information. To see if a website is secure, check for the HTTPS in the address bar.

It's a good idea to avoid accessing websites that require you to enter sensitive information, like passwords, bank account information, or credit card information over public wifi. Remember, anyone can access a public wifi connection.



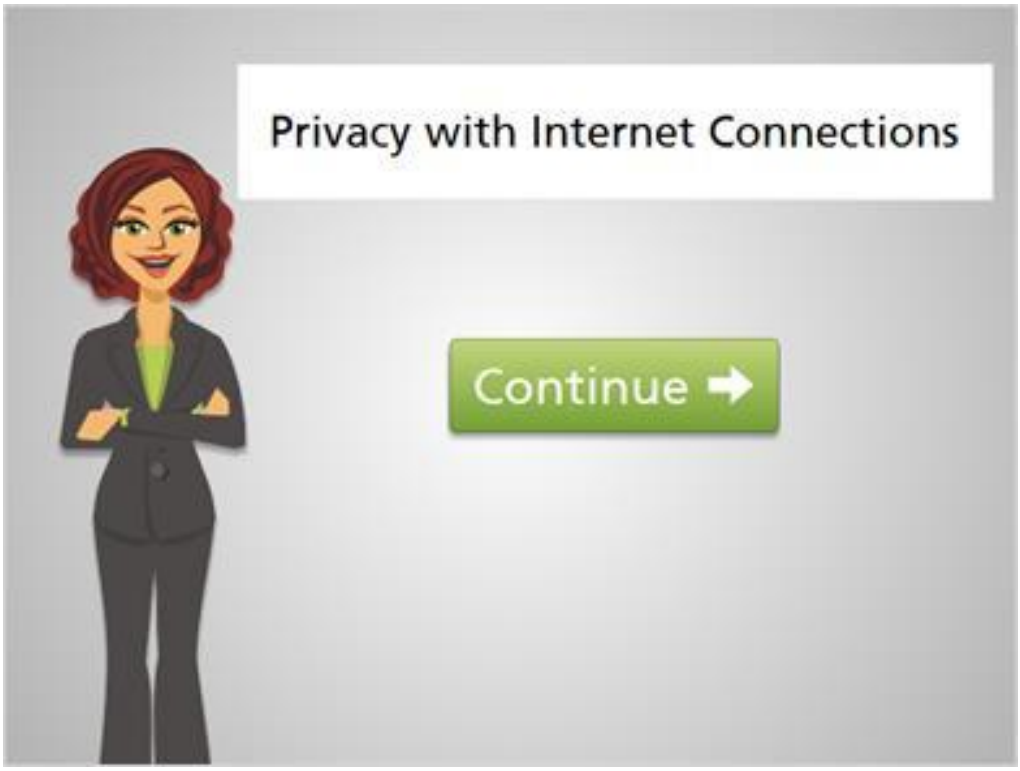
In general, public computers at libraries and community computer centers have secure networks. A primary security concern involves other people using the same computer after you've finished using it.

When using public computers, make sure that private information is not saved on the computer when you're done. Log out of any accounts you've logged into before closing the browser window. You can also clear the history in the web browser, which will delete the list of websites you have visited. Delete any files that you might have saved on the computer.

Note that most library computers have software that automatically remove any personal browsing history and files saved to the computer, but it's a good practice to ask the library staff to be sure before relying on it.

	The best way to ensure your safety when using public wifi at a coffee shop is to avoid accessing websites that ask for personal information.
	True
	False

The correct answer is True.



No matter where you're accessing the internet, it's important to keep privacy in mind. Follow the tips in this course to stay in control of who can see what you're doing online.