Hands-On Lab: Web Browser Security

To accompany Whitman and Mattord, Principles of Information Security, 7th Ed., 2022, ISBN 9780357506431; Web Browser Security

Table of Contents

[Introduction 2](#_Toc76734801)

[Objective 2](#_Toc76734802)

[Estimated Completion Time 2](#_Toc76734803)

[Materials Required 2](#_Toc76734804)

[Minimum System Configuration 2](#_Toc76734805)

[Web Browser Security for Google Chrome 2](#_Toc76734806)

[Autofill 3](#_Toc76734807)

[Safety Check 7](#_Toc76734808)

[Privacy and Security 9](#_Toc76734809)

[Incognito Browsing 13](#_Toc76734810)

[Web Browser Security for Mozilla Firefox 14](#_Toc76734811)

[Protections Dashboard 15](#_Toc76734812)

[Privacy and Security 17](#_Toc76734813)

[Private Window Browsing 22](#_Toc76734814)

[Web Browser Security for Microsoft Edge 23](#_Toc76734815)

[Profiles 25](#_Toc76734816)

[Privacy, Search and Services 27](#_Toc76734817)

[Family Safety 30](#_Toc76734818)

[InPrivate Window Browsing 31](#_Toc76734819)

[Web Browser Security for Apple Safari 32](#_Toc76734820)

[Self-Reflection and Response 34](#_Toc76734821)

[Instructor’s Response 34](#_Toc76734822)

# Introduction

This module describes how to configure the security and privacy features of several popular web browsers to minimize the probability of unwanted disclosures or exploits.

Modern web browsers are some of the most used tools to access remote information. Organizations develop complex web sites to share information with their customers and suppliers, and internal site to share information with employees. While the examination of all the features of the various available web browsers is beyond the scope of this lab exercise, we will look at some of the more common security features and settings of the more common browsers.

Note: if you are performing these labs on organizational equipment, like computers in a university lab or at a business, some of these options may not be available. All may be performed on your personal computer or laptop.

## Objective

Upon completion of this activity, the student will be able to:

* Review and configure the security and privacy settings in the most popular web browsers.

## Estimated Completion Time

If you are prepared, you should be able to complete:

* The Web Browser Security and Privacy labs in 1 to 1.5 hours.

## Materials Required

Access to the named web browsers.

## Minimum System Configuration

Completion of this lab requires that the user have the appropriate rights and privileges to modify software on the local system.

# Web Browser Security for Google Chrome

The first web browser discussed is Google Chrome (<https://www.google.com/chrome/>), shown in Figure L02-4.

A screenshot of a computer

Description automatically generated

**Figure L02- 1** Google Chrome Website

1. Download the Google Chrome browser by going to <https://google.com/chrome> above and clicking the **Download Chrome** button. Follow the on-screen prompts, until the software has installed.
2. Access the Google Chrome settings by clicking the *Customize and Control Google Chrome button* (looks like a vertical ellipse) beneath the close window button in the upper right corner, or type **chrome://settings/** in the URL field. On this screen are several settings important to security, including AutoFill, Passwords, Payment Methods, Safety Checks and Privacy & Security.

## Autofill

The first set of options to investigation are in the Autofill section, as shown in Figure L02-5. Here the user can configure the browser’s ability to remember Passwords, Payment Methods, and Addresses for the user.

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

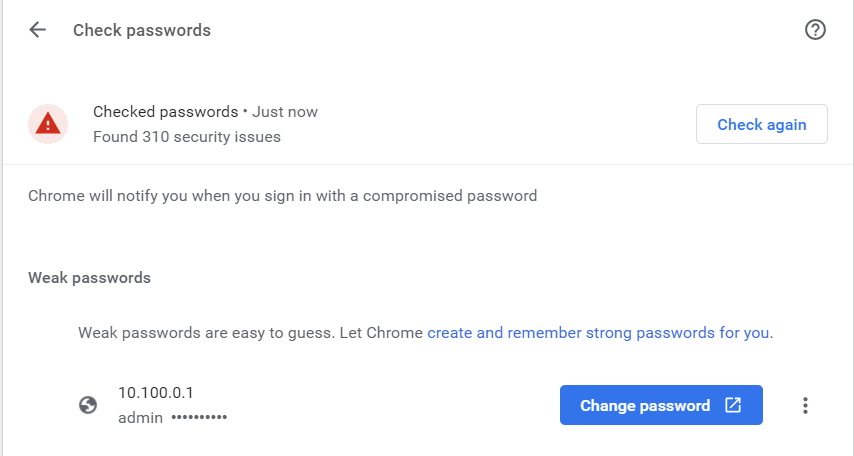
**Figure L02-2** Google Chrome Settings

1. Click the **Passwords** menu option shown in Figure L02-2. You should see the options shown in Figure L02-3. If you are sharing a computer with anyone else, even a family member, you should disable both the *Offer to save passwords* and *AutoSign-in* options, by clicking on the slider to the right of the option to the left.   
   Similarly, if you are using a computer owned by an organization, and not by you, you should disable these options.  
   On your personal systems, you can log into Google Chrome and it will sync your settings across multiple computers. This is fine if you remember to log out of Google Chrome before logging out of the computer system. Use caution with this feature as someone else using the computer could have access to your credentials. A screenshot of a computer

   Description automatically generated

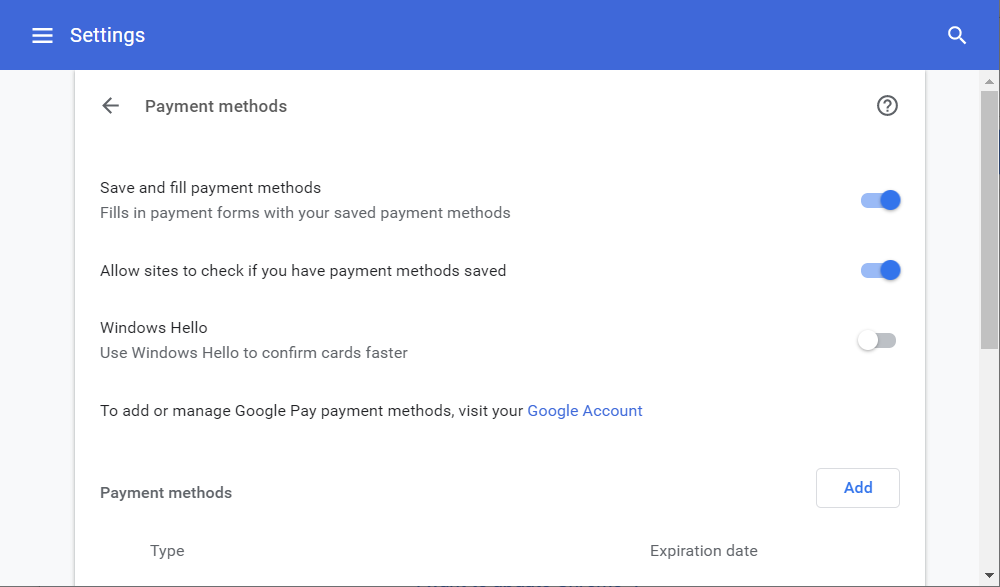
**Figure L02-3** Google Chrome Passwords Settings

1. If you have been using Google Chrome for some time, and storing system credentials in the browser, you may want to periodically check your credentials (usernames and passwords). Hackers work to compromise systems and steal credentials. They then sell or share this information on “the dark web”. Google scans the dark web and allows you to see if one of your system credentials have been found there. Click the **Check passwords** button to review your credentials.
2. As shown in Figure L02-4, Google Chrome will let you know when there is a problem with your stored credentials, including those with passwords that Chrome views as “weak”. You will have the option to chance any password Chrome has flagged for your review by clicking on the **Change password** button beside the account credentials shown. If there were any compromised passwords, they would be listed above the *Weak passwords* section.



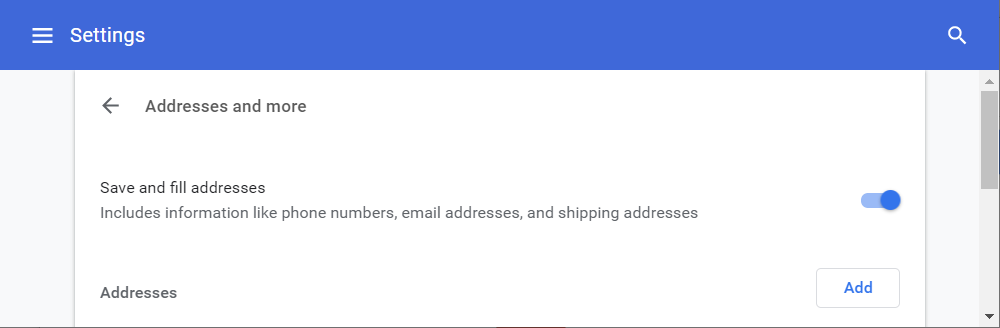
**Figure L02-4** Google Chrome Check Passwords Results

1. Return to the *Settings* menu by selecting the left arrow next to the Settings menu title, or the back arrow next to the URL field.
2. Select **Payment methods** in the Autofill field. As shown in Figure L02-5, Google Chrome can remember your commonly used payment methods. You should use extreme caution when allowing Chrome to do this, as this would allow anyone else using the system to use your payment methods. Chrome does require you to validate the use of a payment card by entering the security code on the reverse, however if someone saw you using a card, they may have remembered that information, and thus could shop with your credit.



**Figure L02-5** Google Chrome Payment Methods Settings

1. For systems you share with others, or which belong to an organization, it is recommended that you disable the *Save and fill payment methods* and *Allow sites to check if you have payment methods saved* options by sliding the button to the right of the options to the left. Any payment methods saved will be listed at the bottom of this menu and can be accessed there.
2. Return to the *Settings* menu by selecting the left arrow next to the Settings menu title, or the back arrow next to the URL field.
3. Click on the **Addresses and more** option under Autofill. As shown in Figure LM01-9, here you can allow Google Chrome to remember key addresses, much the same as passwords and payment methods. Again, disable this option on shared systems, or systems owned by an organization.

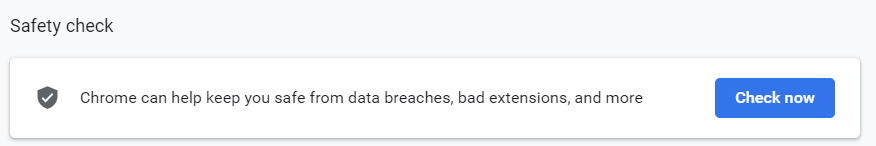


**Figure L02-6** Google Chrome Addresses and more Settings

1. Return to the *Settings* menu by selecting the left arrow next to the Settings menu title, or the back arrow next to the URL field.

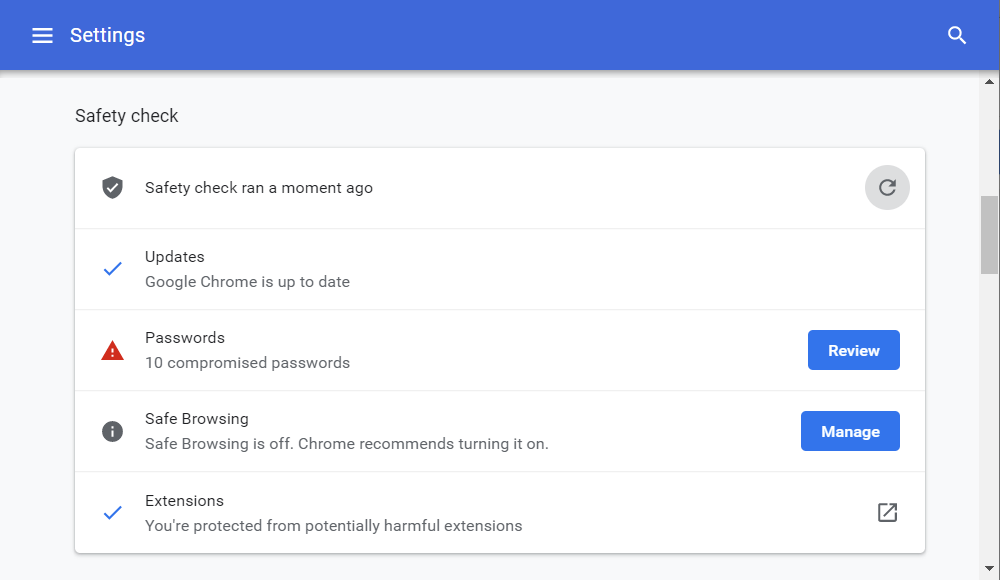
## Safety Check

The next area to examine is the Safety Check menu, shown in Figure L02-7. Just like the Password check in the previous section, this function will determine if there are any issues with your Google Chrome.



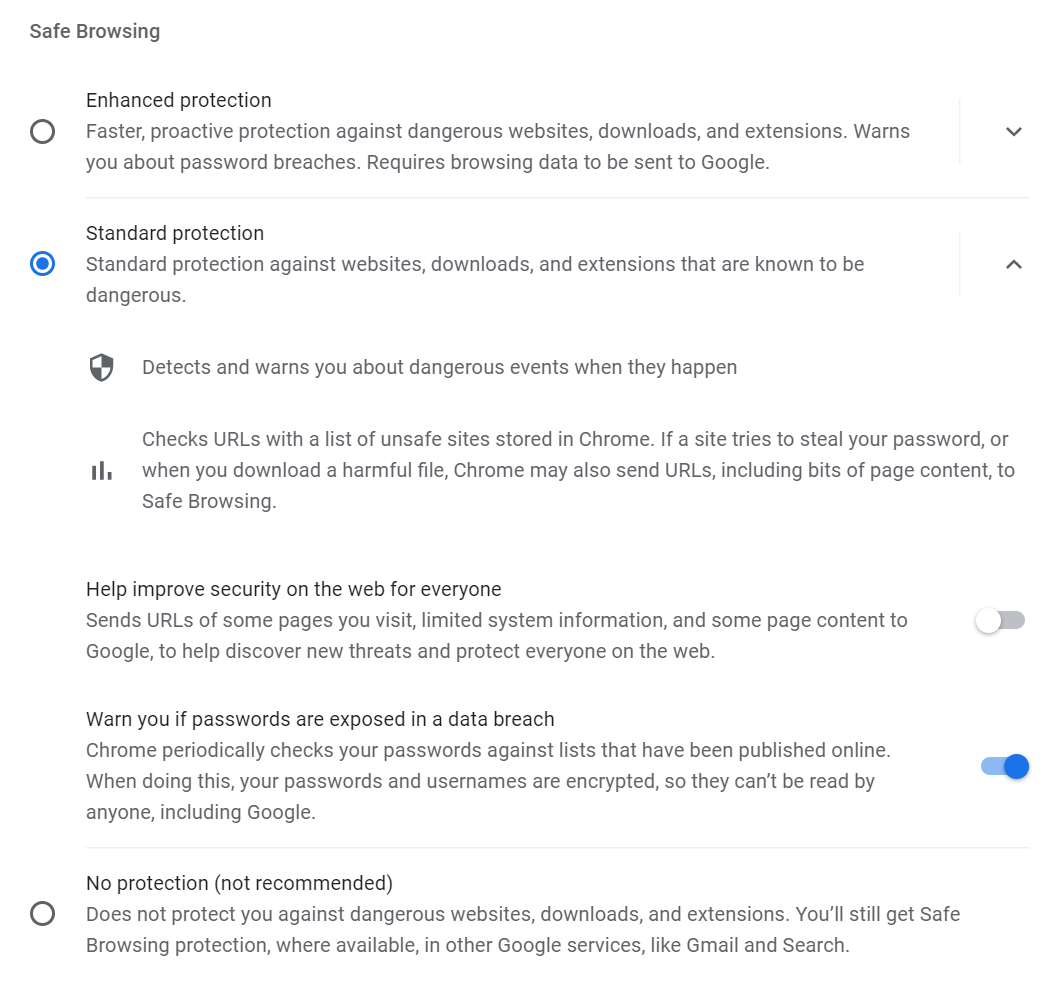
**Figure L02- 7 Google Chrome Safety Check**

1. Click on the **Check now** button to run the Safety check. Figure L02-8 shows a sample results screen.



**Figure L02- 8** Google Chrome Safety Check Results

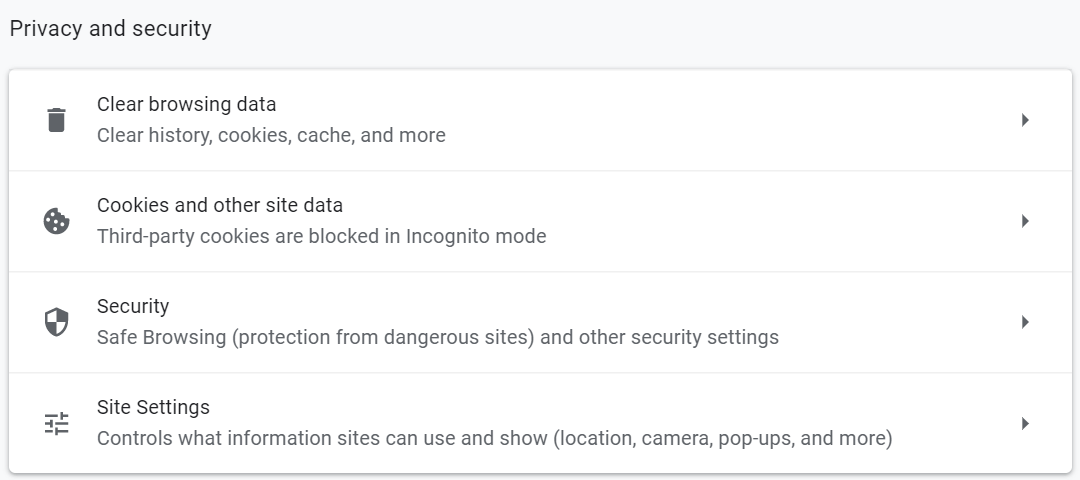
1. Review and resolve any issues identified by clicking the corresponding button to the right of the menu option. If you did not resolve all issues with Google Chrome managed passwords, you will have the option to fix those here as well, by clicking the **Review** button.
2. If your system is not currently using Safe browsing, select the **Manage** button and select the options that best suits your preferences. At a minimum you should select *Standard protection* under *Safe Browsing*. *Enhanced protection* is the best option, however it does send browsing data to Google, as illustrated in Figure L02-9.
3. There are additional options under *Advanced* you may specify. If available select **Use secure DNS**. There are also options to manage your certificates and implement the Google Advanced Protection Program here. The GAPP program allows you to implement multi-factor authentication for your Google browser, requiring the use of specifical software on your phone or a hardware token to authenticate your Google login. Visit <https://landing.google.com/advancedprotection/> if you want to learn more about the GAPP program.
4. Also available under Safety check is Extensions management. Extensions are add-ons for Google Chrome to provide additional functionality. Some however may introduce new vulnerabilities. If you have any issues with extensions in your version of Chrome, the option to resolve those will appear here (See Figure L02-8 above).
5. Return to the Settings page by using the back option again.



**Figure L02-9** Google Chrome Safe Browsing Settings

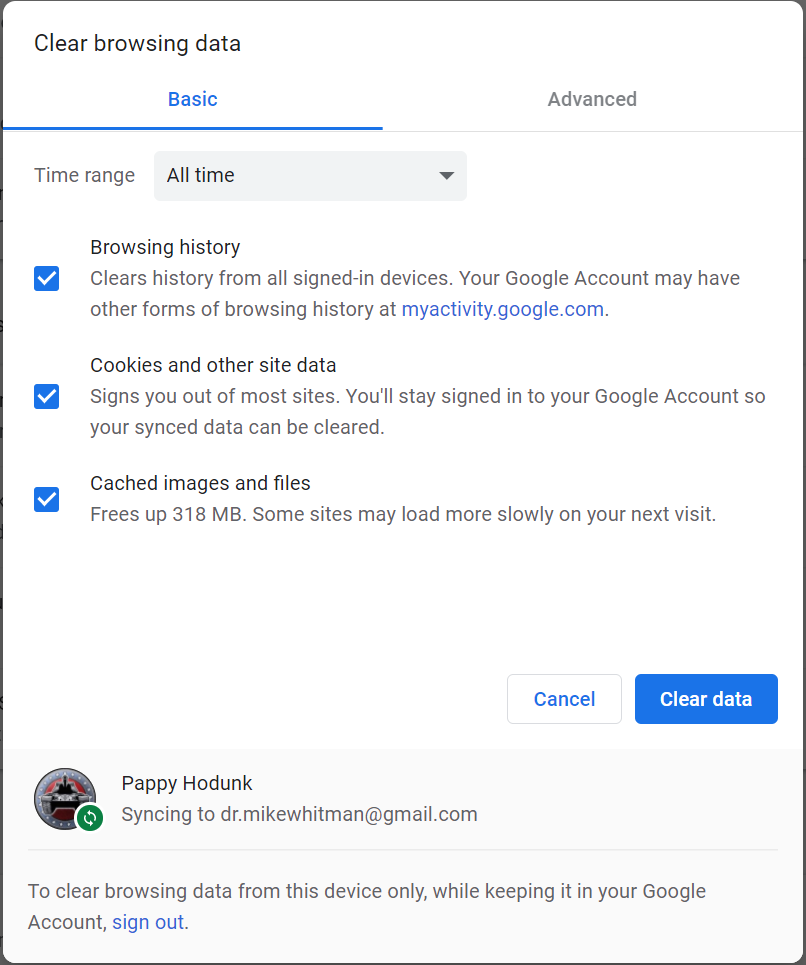
## Privacy and Security

Back at the Settings screen, the next section is *Privacy and Security*. As shown in Figure L02-10, here you can clear your browsing data, cookies and adjust other security features.



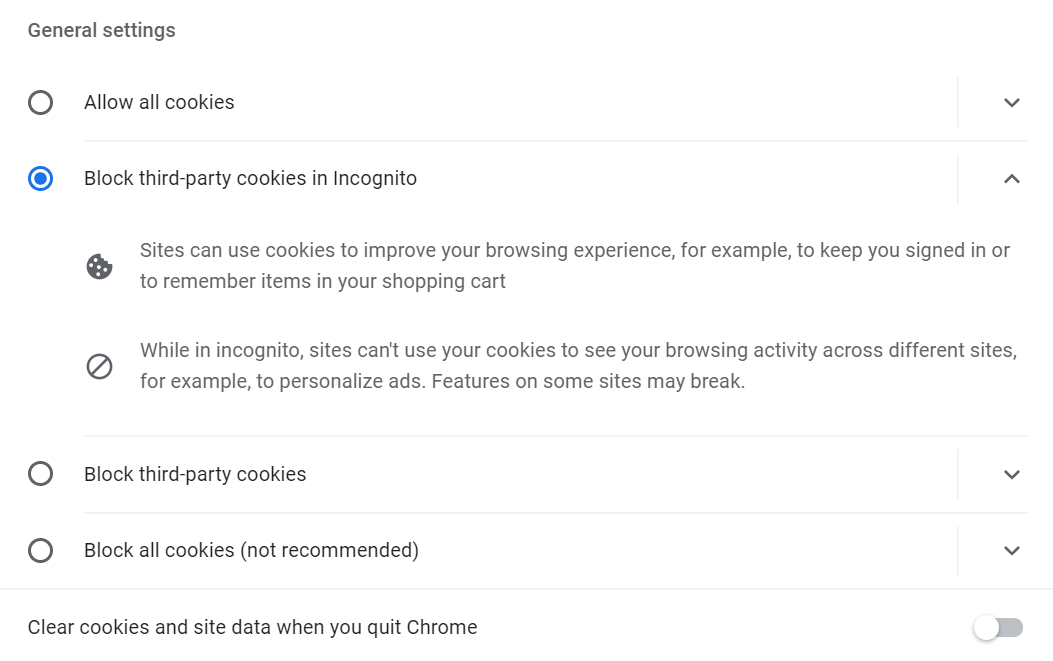
**Figure L02-10** Google Chrome Privacy and Security Settings

1. Click on **Clear browsing data**. Here you can specify whether you want to clear your browsing history, cookies and cached images and files from your browser. Periodically you may experience issues using a piece of software that caches files on your system. Clearing your browsing data by checking the options shown in Figure L02-11 and clicking the **Clear data** button will give you a fresh start and force your browser to download all new web content. If you are not logged in to Google, this action will only clear the cached information on the local machine. If you are logged in, it will clear this information for all systems you are logged into, as the data is stored and synced by Chrome.
2. You can specify how much data to clear by using the pull-down box next to *Time range.* Use this option to select All time, if not already selected and click **Clear Data**.



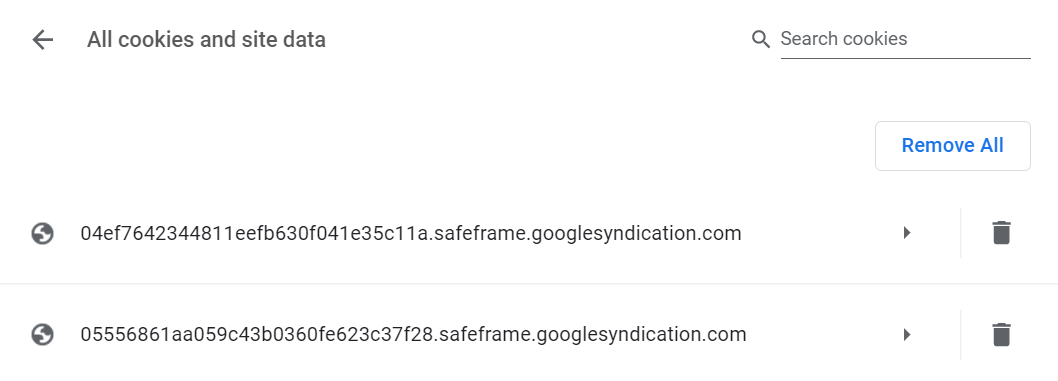
**Figure L02-11** Google Chrome Clear Browsing Data Settings

1. Click the **Cookies and other site data** option. As shown in Figure L02-12, here you can specify which Cookies to allow to be stored on your system. While you can block all cookies, you would quickly find issues trying to access some web sites. At a minimum, it is recommended you select the option **Block third-party cookies in Incognito**, as shown in the Figure, although you may decide to select **Block third-party cookies** to provide more privacy. To change your options, simply click on the radio button (circle) to the left of the desired option.



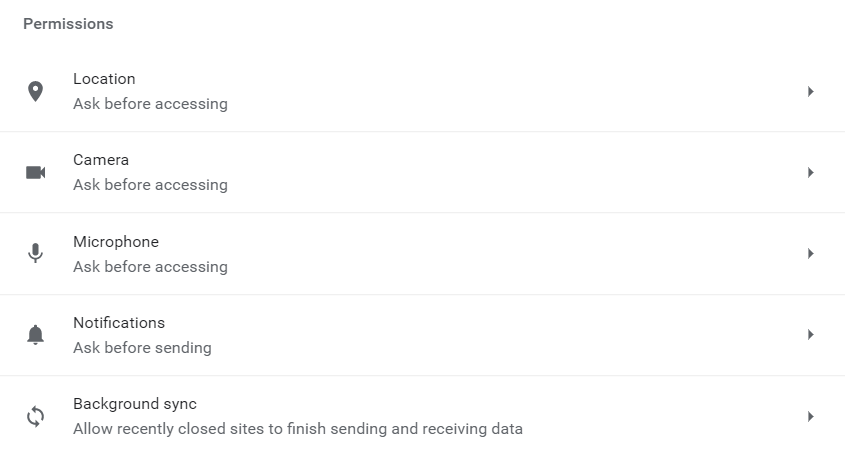
**Figure L02-12** Google Chrome Cookies and Other Site Data Settings

1. Further down this screen you can view all cookies currently stored on your system by selecting the See all cookies and site data option. This allows you to selectively delete the cookies from one vendor by clicking on the trash can icon shown in Figure L02-13.



**Figure L02-13** Google Chrome View Cookies

1. You can also add specific sites to whitelist (allow) or blacklist (deny) their access to your cookies use, if you choose to allow all or block all in the previous step. You can also specify certain sites to dump their cookies (and no others).
2. Return to the settings page using the back arrows.
3. The *Security* menu option takes you back to the Safe Browsing options.
4. Click the **Site Settings** menu option. As shown in Figure L02-14, here you can specify the permission associated with the use of your system for specific sites. This is commonly used to allow or deny the use of location information (for pizza delivery!), your camera, and your microphone (for web conferencing). It also allows you to specify permissions for notifications (popup reminders). Review the options available and adjust to your preferences.

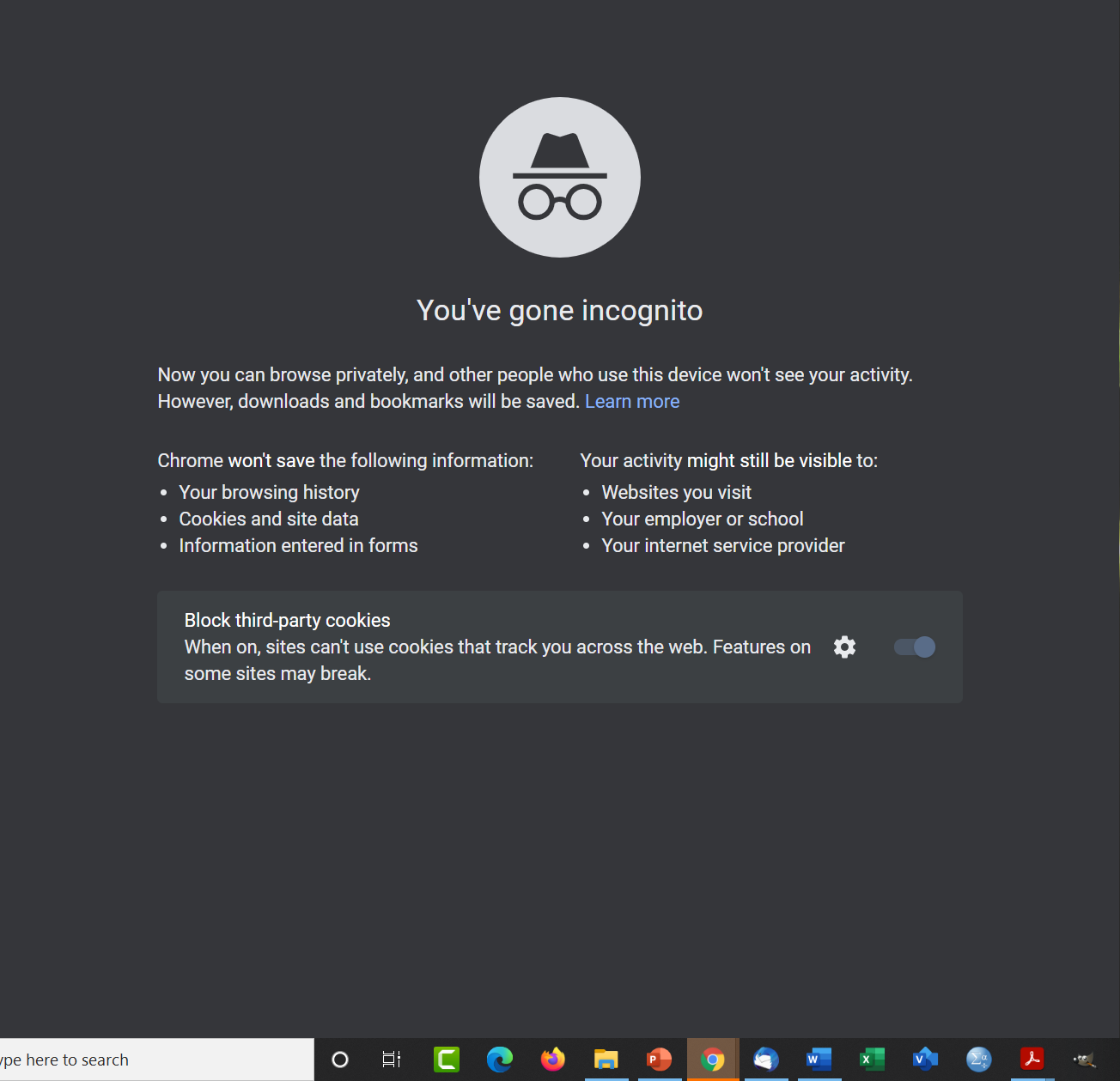


**Figure L02-14** Google Chrome Permissions Settings

1. The *Additional content settings* menu allows you to specify things like the preferred software to play sounds and open images and PDFs. It also allows you to blacklist certain sites with misleading or offensive ads.

## Incognito Browsing

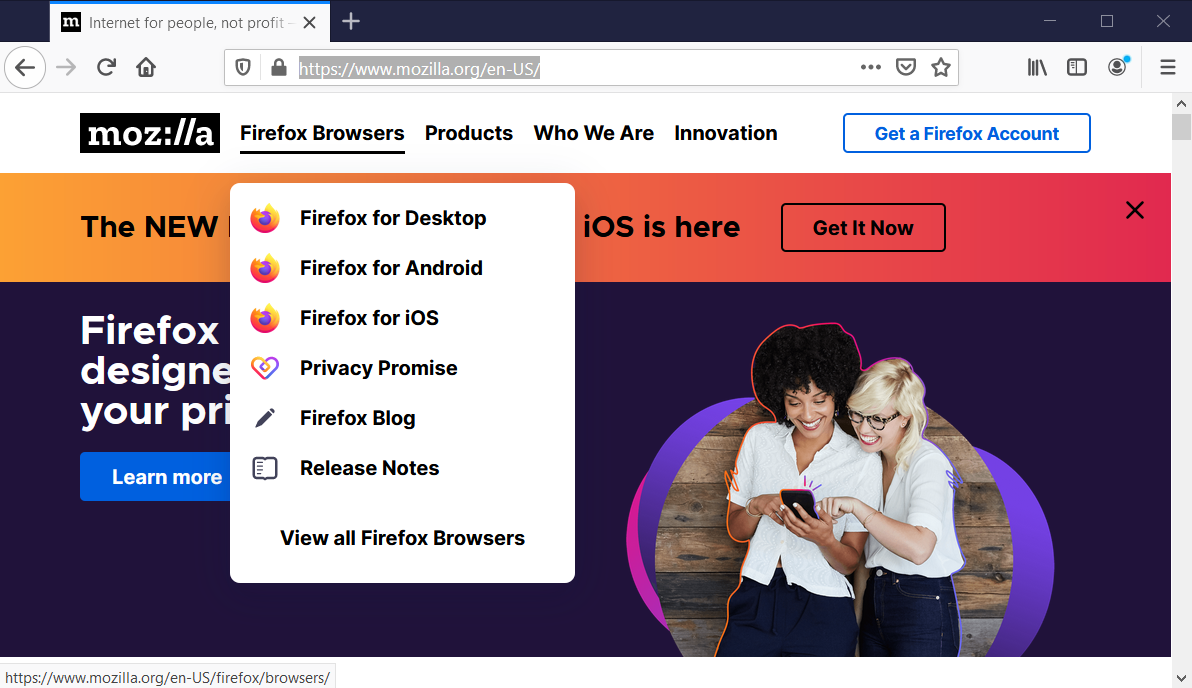
1. While there are other settings and options in Google Chrome, these are the dominant settings related to privacy and security. There is one other feature of interest, especially if you’re using a shared computer. Incognito browsing involves the use of a specifical instance of the browser to prevent the retention of history and cookies (if selected). The easiest way to start an incognito browser session is to right click on the Chrome icon or menu option and select **New incognito window**. Do so now.
2. As shown in Figure L02-15, this gives you an increased level of privacy over the standard browser. Keep in mind that this simply protects you from retained data on the local system, it does not screen you from systems that monitor network use, such as the organization or university’s IT department, or the internet service provider.



**Figure L02-15** Google Chrome Incognito Browsing

# Web Browser Security for Mozilla Firefox

Mozilla’s Firefox browser has many of the same features as other browsers. Firefox can be downloaded from <https://www.mozilla.org/en-US/>, selecting the Firefox browsers option in the top menu, as shown in Figure L02-16.

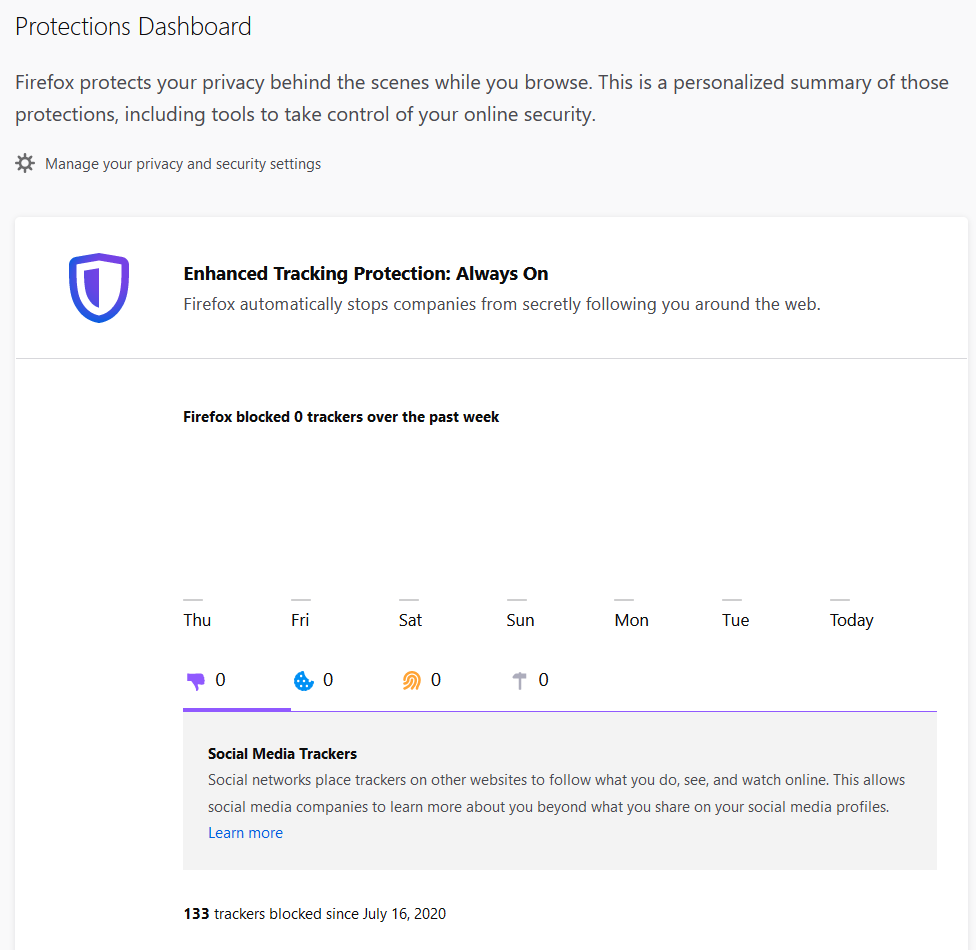


**Figure L02-16** Mozilla Firefox

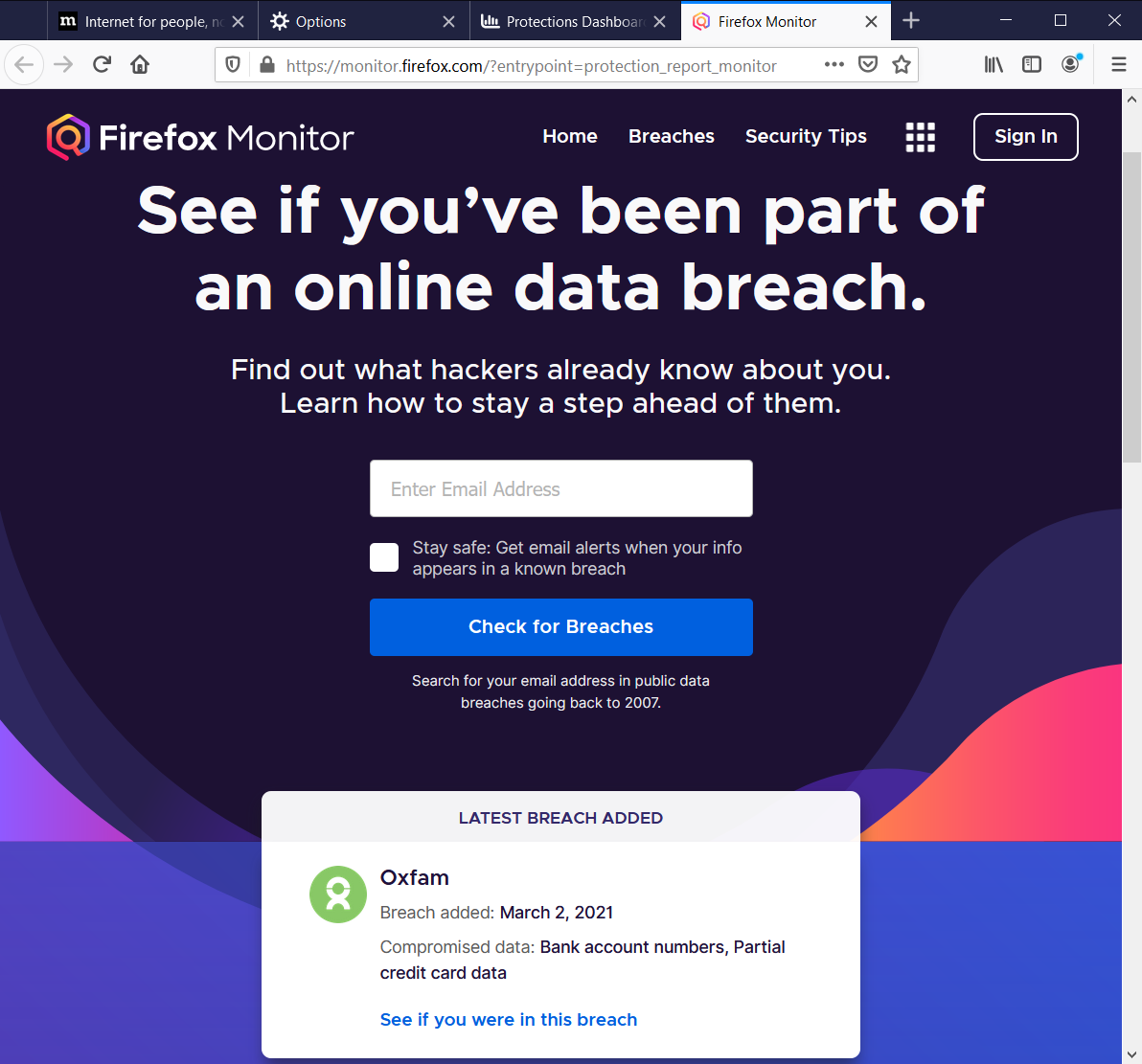
1. If you do not have Mozilla Firefox installed, go to the URL listed above and follow the instructions to download and install. Then start Firefox.
2. To access the security and privacy options in Firefox, first click on the menu button (three parallel lines in upper left corner under the Close button).

## Protections Dashboard

1. The first security option we’ll look at is the Protections Dashboard. To access the **Protections Dashboard** on the shield icon in the address bar when visiting a web page or you can accessed it by entering the text "about:protections" into the address bar.   
     
   As shown in Figure L02-17, you can see the first security feature is the Enhanced Tracking Protection. This is always on, so it’s just a report of how Firefox is working to protect you from online tracking software. Also on this menu is the offer to sign up for Breach alerts with Firefox Monitor. This is currently free but requires a Firefox account (also free). Like Google Chrome, signing into your Firefox browser allows you to sync your settings across multiple systems. Firefox monitor (Shown in Figure L02-18) will alert you if it finds your credentials (based on your e-mail address) in a compromised system.



**Figure L02-17** Mozilla Firefox Protections Dashboard



**Figure L02-18** Mozilla Firefox Monitor

1. At the bottom of this screen is the Password Management feature, shown in Figure L02-19, which allows you to manage stored passwords in Firefox. Click the **Manage Passwords** button.

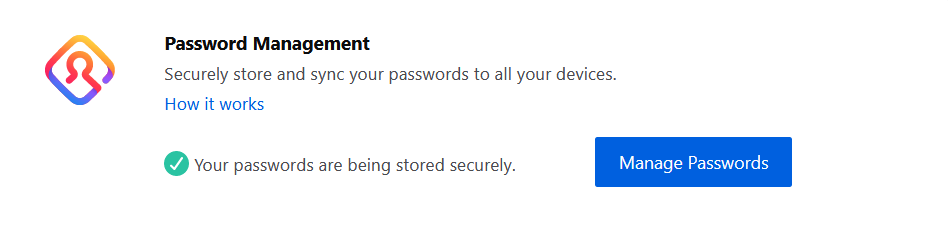
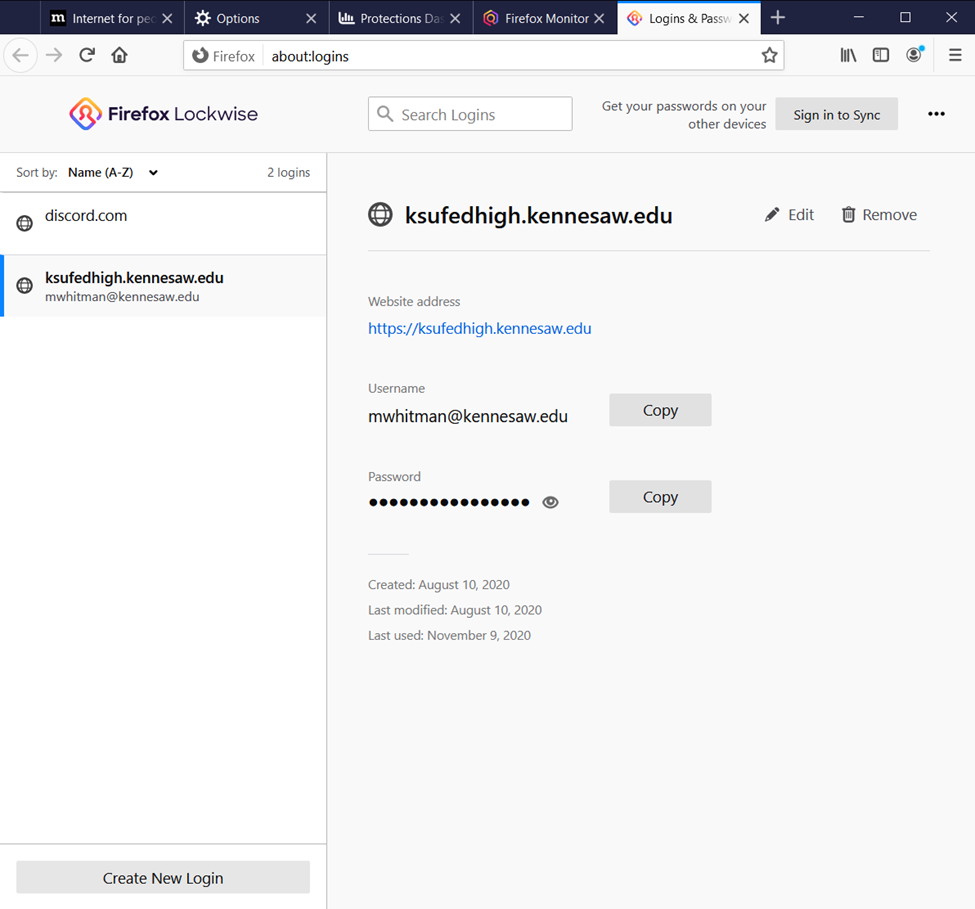


Figure L02- 19 Mozilla Firefox Password Management

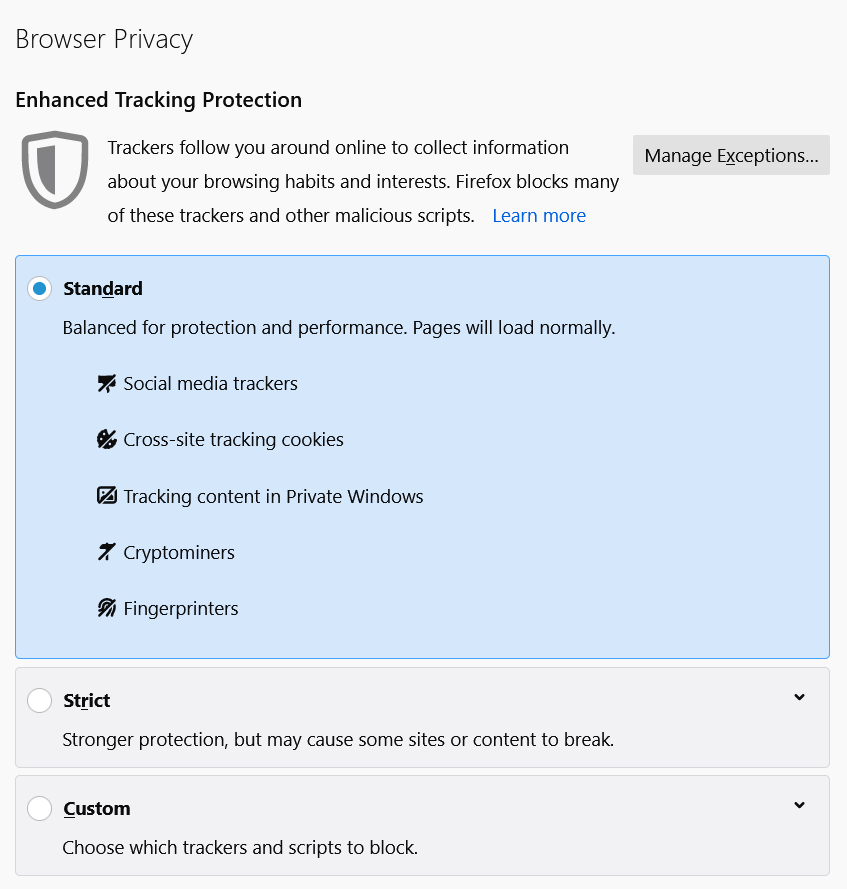
1. This opens the Firefox Lockwise feature, used to manage your passwords on various web sites, as shown in Figure L02-20. Here you can edit and remove any stored passwords for your Firefox account, if logged in, or on the local system only, if not. Lockwise can also be directly accessed through the menu by selecting **Logins and Passwords.**



**Figure L02-20** Mozilla Firefox Lockwise

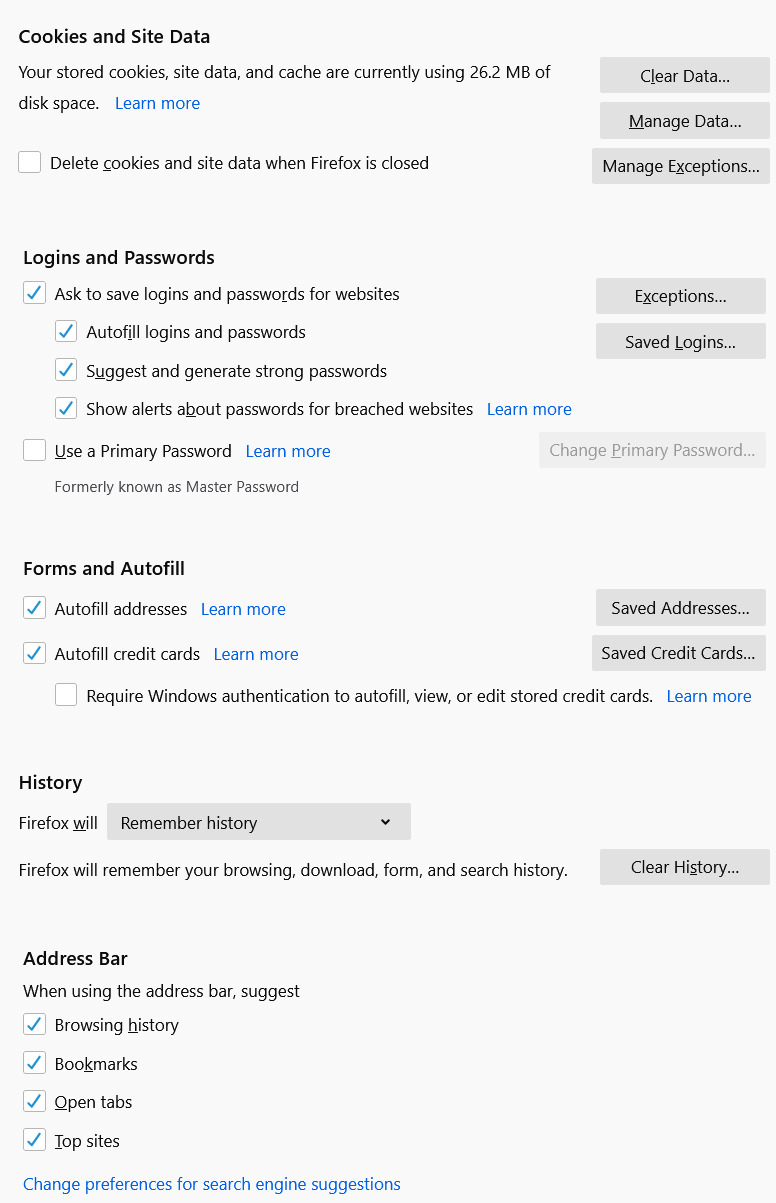
## Privacy and Security

1. Open the menu and select Options. Here you can specify general Firefox settings. In the left menu, select **Privacy & Security**. As shown in Figure L02-21, here you can specify the level of tracking allowed. At a minimum, you should ensure your system is set to *Standard*. While there is no lower setting available, someone may have created a custom configuration which allows fewer security features and protections. If you desire, you can set your system(s) to *Strict*, providing increased protection.



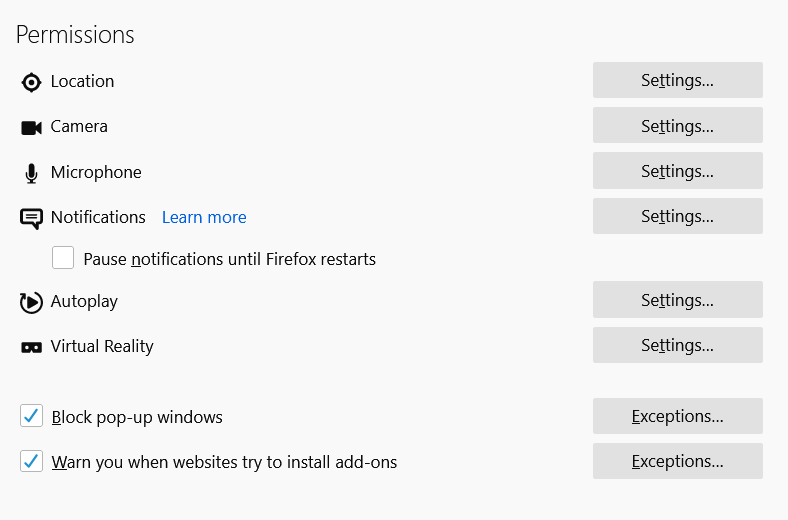
**Figure L02-21** Mozilla Firefox Browser Privacy Settings

1. Further down this page, you have the options to clear and manage Cookies, Logins and Passwords, Forms and Autofills, History, and the Address Bar as shown in Figure L02-22.



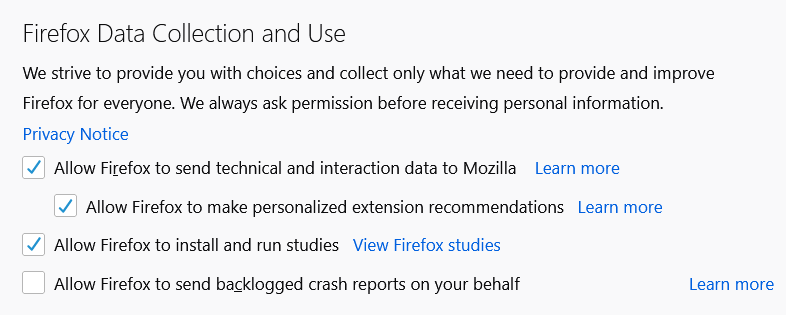
**Figure L02-22** Mozilla Firefox Cookies and Site Data Settings

1. Click **Clear Data** under Cookies and Site Data. When prompted, select both *Cookies and Site Data* and *Cached Web Content*, and click the **Clear** button.
2. Next, click **Clear History** under History. Select **Everything** in the *Time range to clear* pull down menu, and check all boxes under *History* and *Data*. Then click **OK**.
3. While most of these are self-explanatory, one feature deserves additional attention. The Primary Password is a feature that allows additional protection for systems used by multiple users, allowing the secure use of saved credentials. If this feature is enabled by checking the box to the left of the option, each session (new web browser) will prompt you for a “Primary Password” to use the saved password functions. This will prevent someone from using a shared system and then taking advantage of saved credentials. The Primary password is typically your Firefox account password. You are also prompted for this password if you try to add, remove, or edit stored passwords.
4. Review each of these options and enter the settings that you desire.
5. Further down on this screen are the Permissions settings for specific applications, as shown in Figure L02-23. Here you can specify which applications can use which features such as your location, the web camera, and microphone.



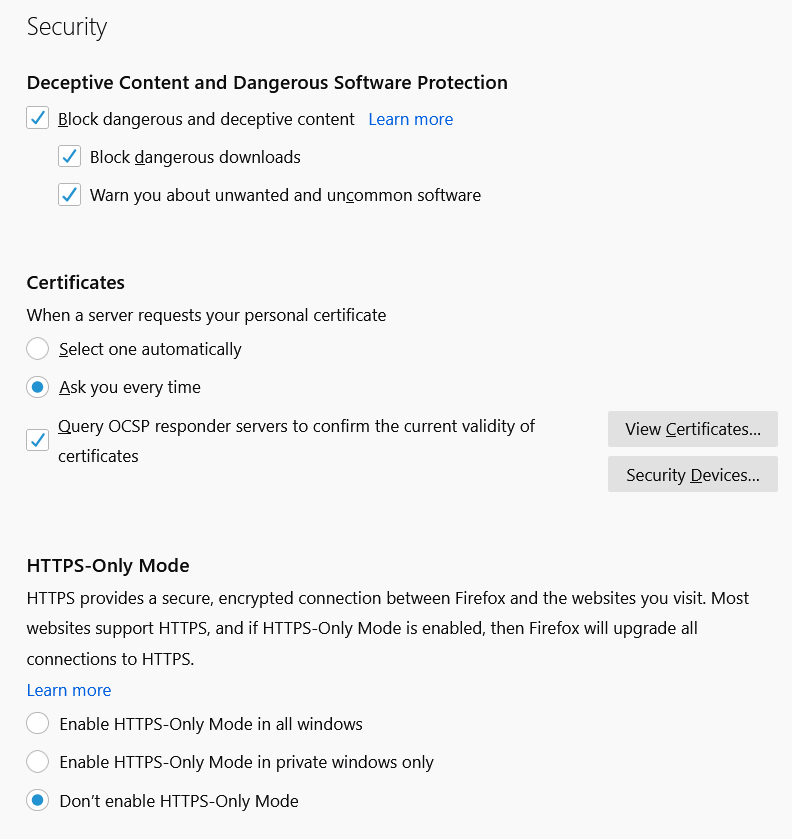
**Figure L02-23** Mozilla Firefox Permissions Settings

1. Also located in the options menu is the specification for Firefox Data Collection and Use, shown in Figure L02-24, which provides specific criteria which you can select to craft what data, if any, you allow Mozilla to collect and use.



**Figure L02-24** Mozilla Firefox Data Collection and Use Settings

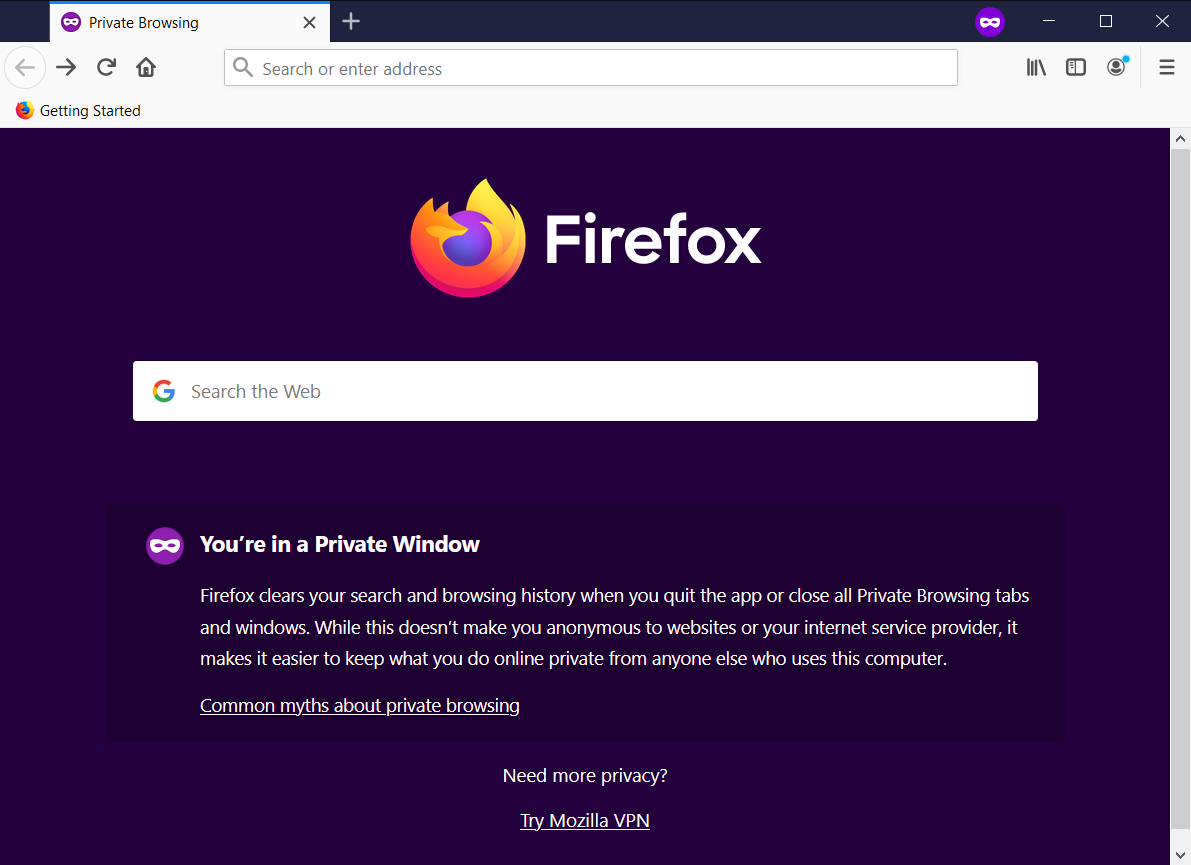
1. The last set of options in this menu are the Security features not covered elsewhere. Here you can Block dangerous and deceptive content, review your certificates, and specify the use of HTTPS (HTTP Secure) protocol. Ensure the minimum levels of security by reviewing your settings and making sure they are at least as secure as the ones shown in Figure L02-25.



**Figure L02-25** Mozilla Firefox Security Settings

## Private Window Browsing

1. Users can create anonymous browsing windows by right clicking the Mozilla Firefox icon and selecting **New Private Window**. This window, shown in Figure L02-26, allows the user to avoid saving passwords, cookies, and browsing history while in a private window. It allows the user to access any stored materials from normal browsing but will not save any new materials. Again, private windows do not block your information from an organization’s IT department or the Internet Service Provider.



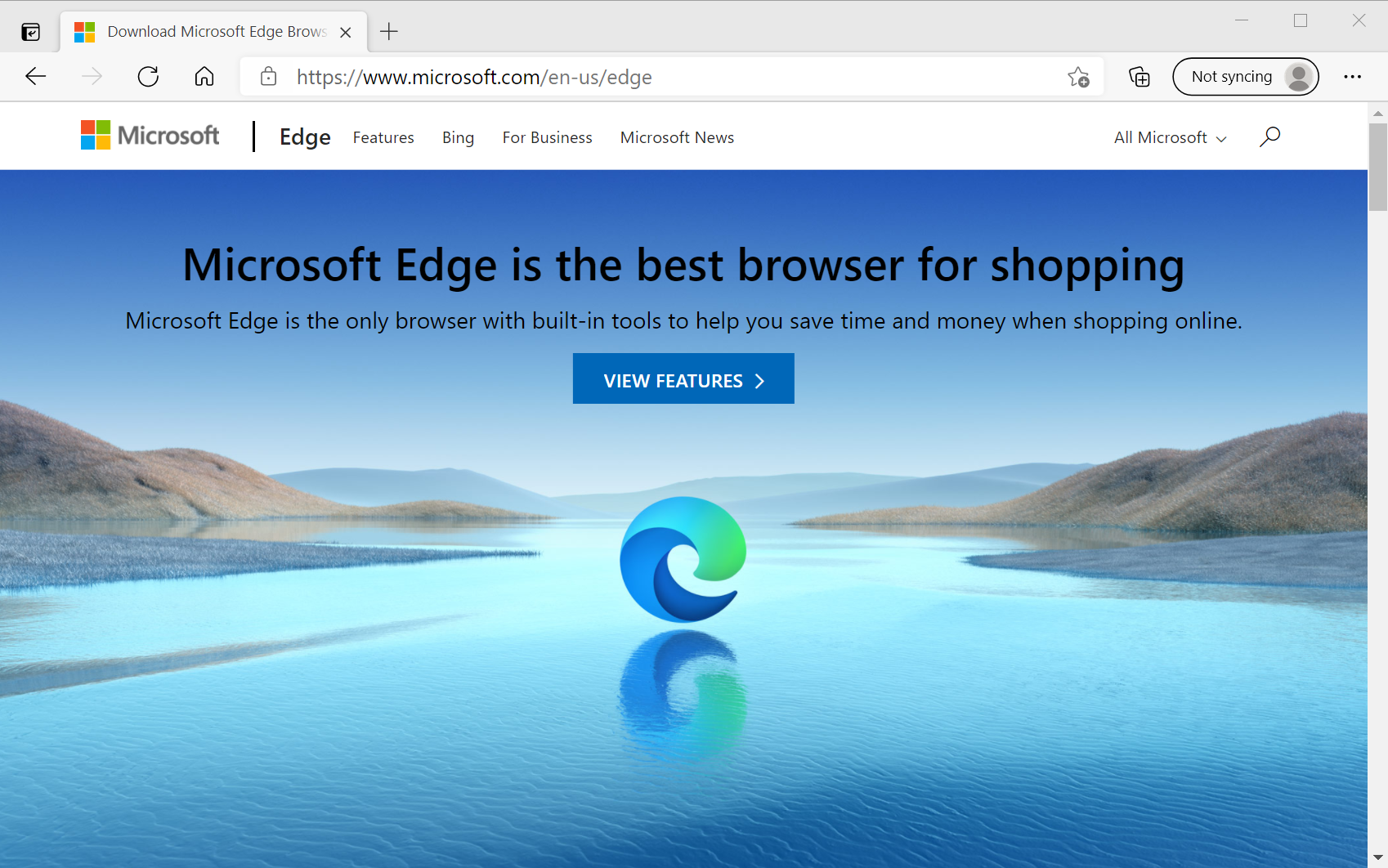
**Figure L02-26** Mozilla Firefox Private Window Browsing

While there are many other options you can configure for Mozilla Firefox, these are the primary security and privacy features.

# Web Browser Security for Microsoft Edge

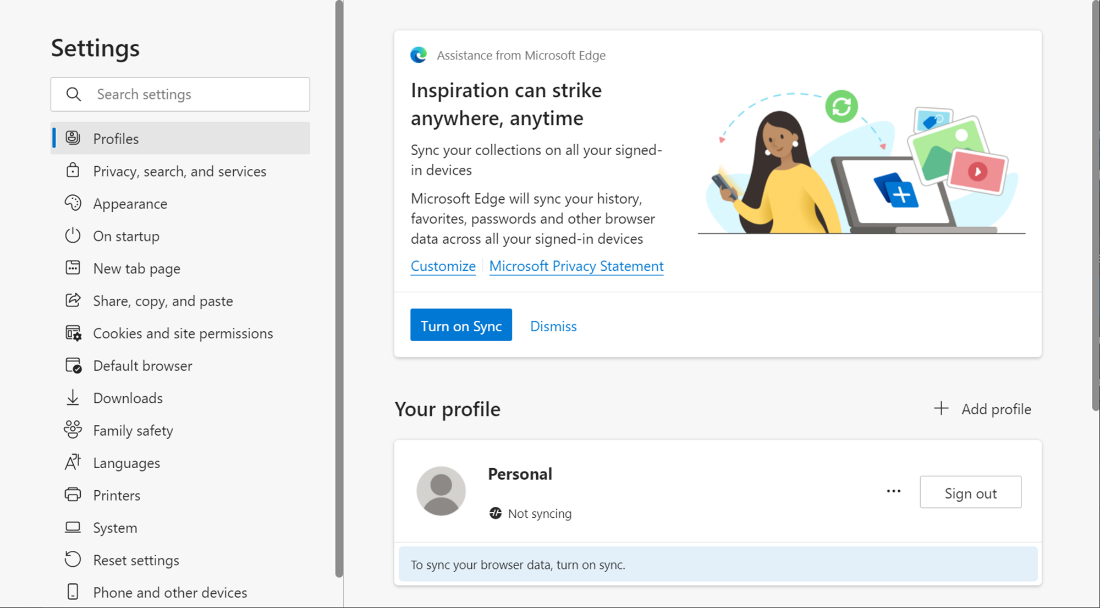
Microsoft Edge is the newest browser from Microsoft, provided with its Windows operating systems. Edge replaces the venerable (and vulnerable) Microsoft Internet Explorer. Like other browsers, Edge can sync settings between systems if the user creates an account with Microsoft and logs in.

1. Microsoft Edge can be downloaded from <https://www.microsoft.com/en-us/edge>, as shown in Figure L02-27, although it most likely is already installed if you are using a Windows operating system like Windows 10.



**Figure L02-27** Microsoft Edge

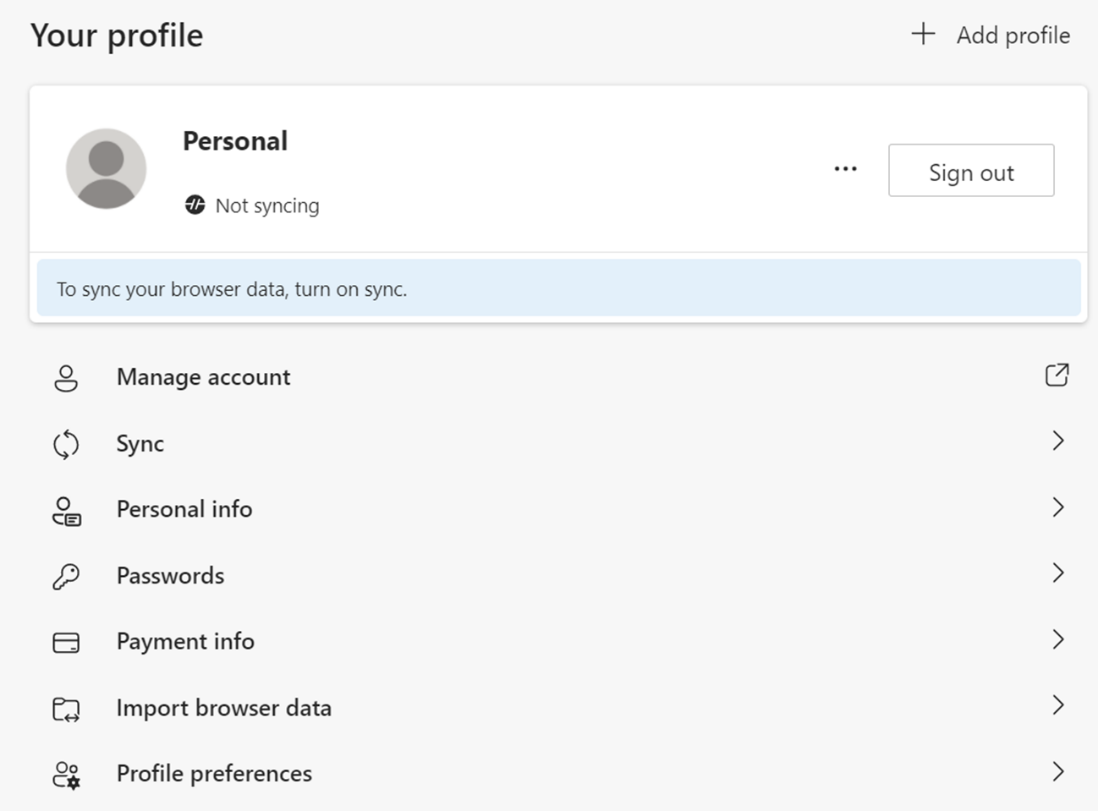
1. The first set of security and privacy features are accessed by selecting the menu (the ellipsis in the upper left corner under the close button), then selecting **Settings**. As Figure L02-28 shows, options are listed on the left, with configuration on the right.



**Figure L02-28** Microsoft Edge Settings

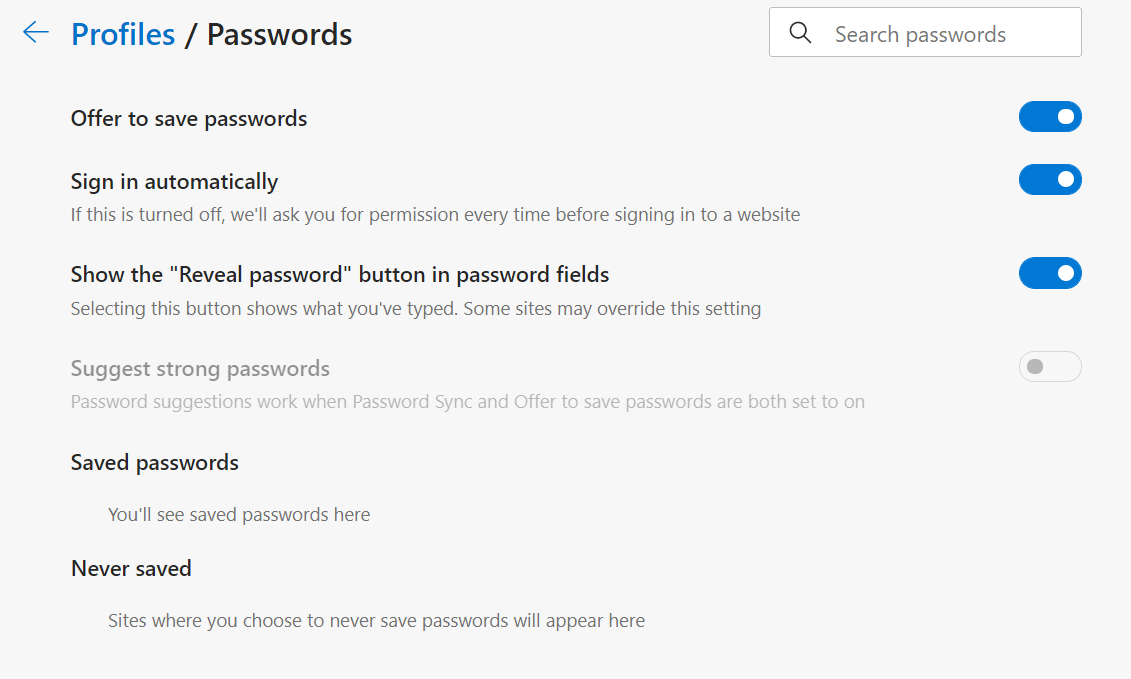
## Profiles

1. Select **Profiles** (if not already selected). The profiles section, shown in Figure L02-29, allows quick access to sync functions, password management, and retained payment preferences.



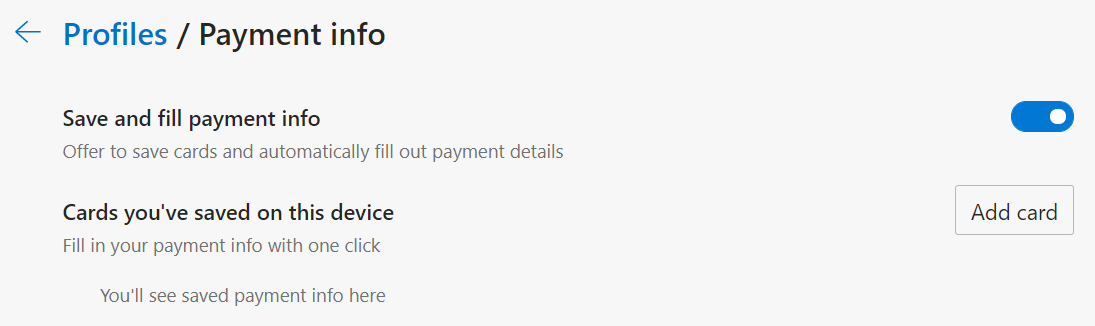
**Figure L02-29** Microsoft Edge Your Profile Settings

1. Click **Passwords**. As shown in Figure L02-30, here you can specify whether to allow Edge to save passwords for you, sign in automatically and provide a “reveal passwords” button so you can determine if you entered a password correctly. If you are using a shared computer, ensure these options are turned off.



**Figure L02-30** Microsoft Edge Profiles/Passwords Settings

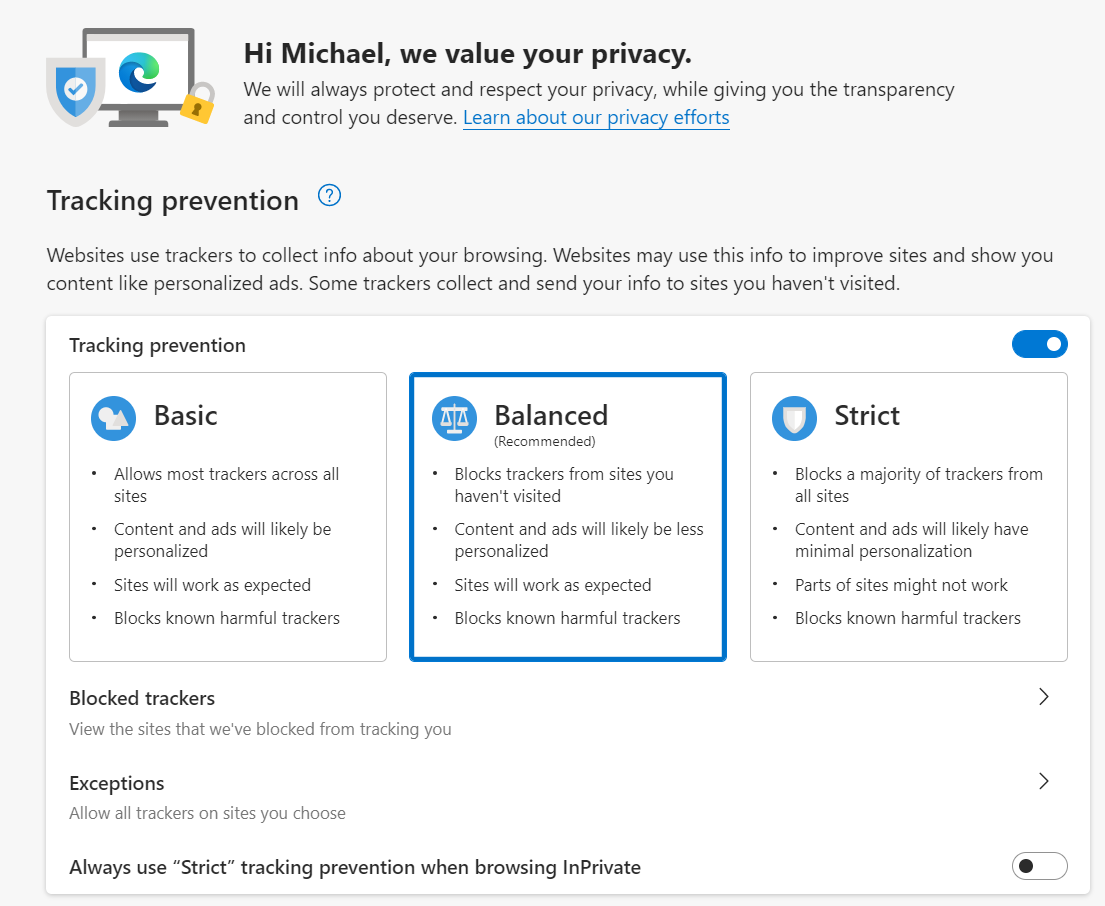
1. Click the back arrow next to *Profiles / Passwords* in the right side of the window, to return to the *Your profile* page. Next, click the **Payment info** option. As shown in Figure L02-31, here you can allow the saving and use of payment information and manage saved payment information like credit and debit cards, or online payment account. If you have already added a payment card, you can edit its attributes. On shared systems, ensure this option is disabled by clicking the blue oval with a white dot in it, located to the right of the option. Once it is off, the oval will turn white, with a black dot on the left side.



**Figure L02-31** Microsoft Edge Profiles/Payment Info Settings

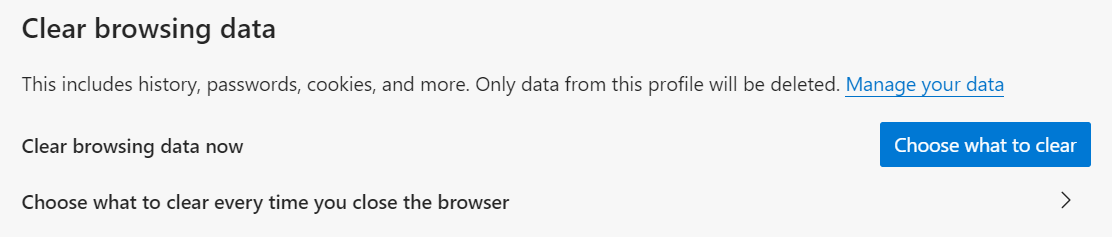
## Privacy, Search and Services

1. Click the **Privacy, search and services** option on the left side of the Settings menu. As shown in Figure L02-32, here you can specify one of three options for your Tracking prevention settings. At a minimum, you should select the **Balanced** option. You can also review blocked trackers by clicking that option beneath the three boxes and specify exceptions for trackers. Review these options now.

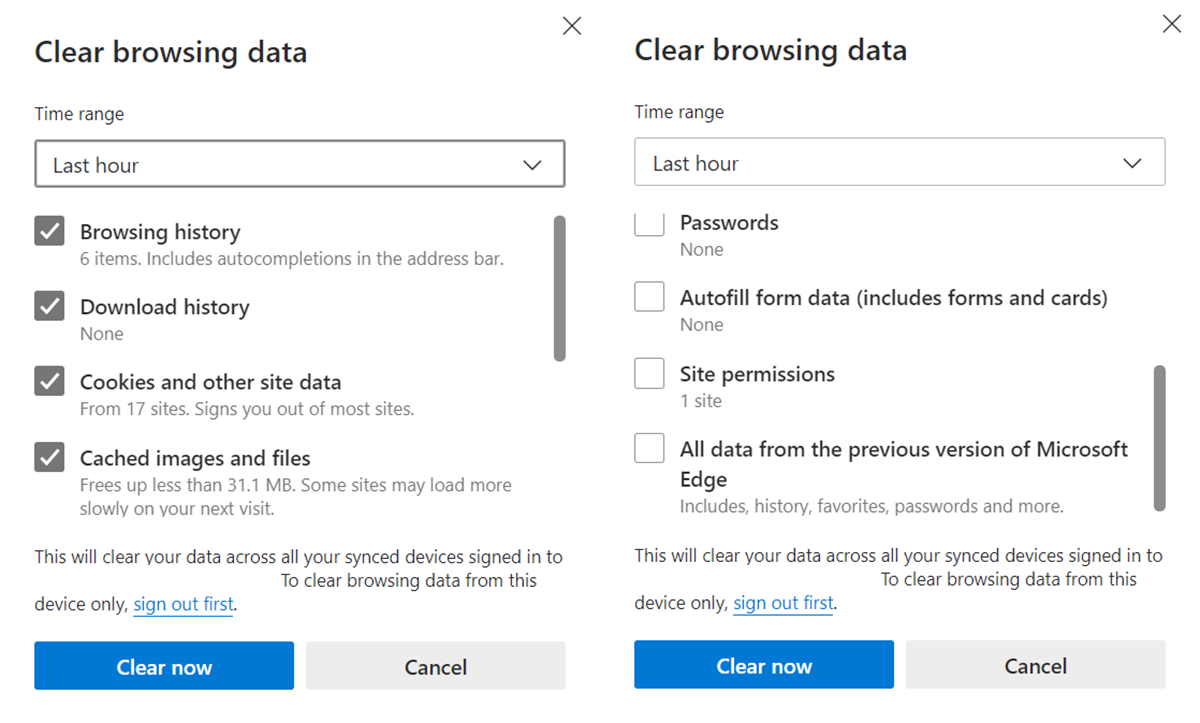


**Figure L02-32** Microsoft Edge Tracking Prevention Settings

1. Scroll down the Privacy, search, and settings menu on the right. The next section allows you to Clear your browsing data, and to specify what is cleared. Click the **Choose what to clear** button. Figure L02-33 shows the Clear browsing data area of the menu, while Figure L02-34 shows the option available once you click the Choose what to clear (there are two versions of this window as the second shows the additional options when scrolling down).

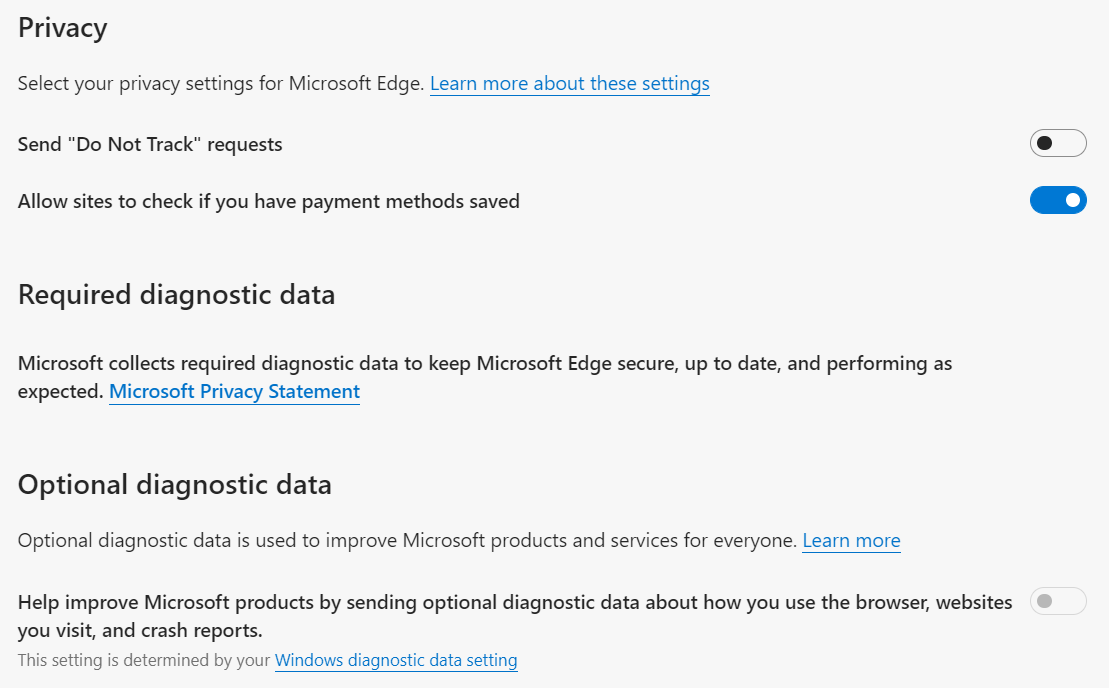


**Figure L02-33** Microsoft Edge Clear Browsing Data Selection



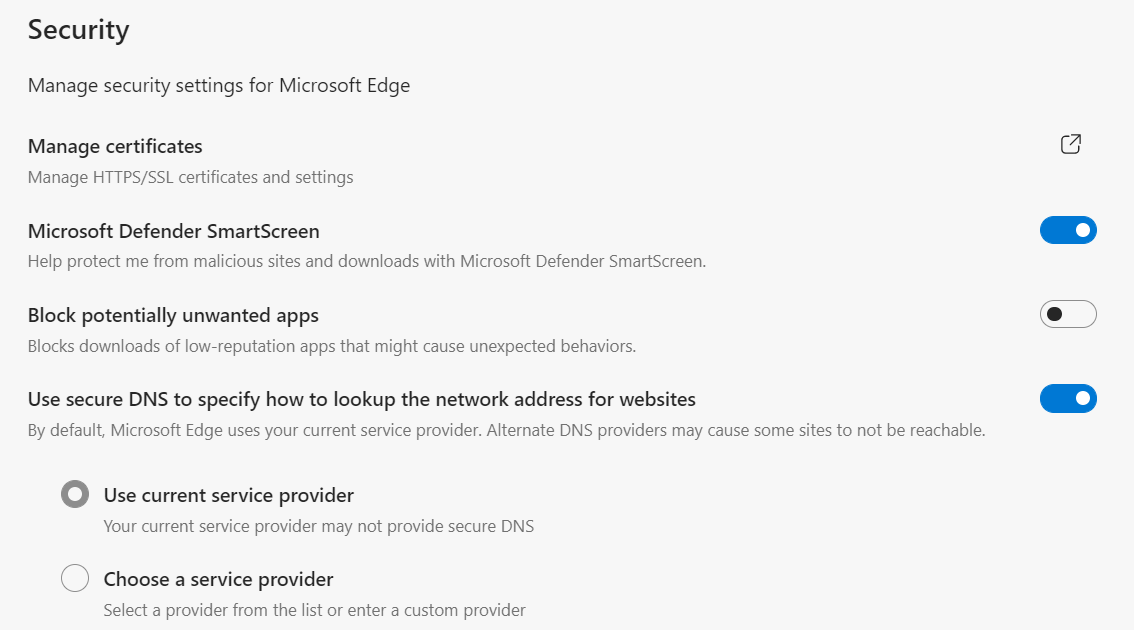
**Figure L02-34** Microsoft Edge Clear Browsing Data Settings

1. Select **All time** in the *Time range* pull down window, then check all of the option boxes and click **Clear now** to completely clear Microsoft Edge’s browsing data. You can also select *Choose what to clear every time you close the browser* to configure Edge to clear its cached data each time you close the browser.
2. The next areas of interest are *Privacy*, *Required diagnostic data,* and *Optional diagnostic data,* located in the next sections after Clear browser data. The *Privacy* options allow you to specify whether your system allows sites to check if you have payment methods stored in Edge, as shown in Figure L02-35. Shared systems should enable *Send “Do Not Track” requests* and disable the *payment methods* option.



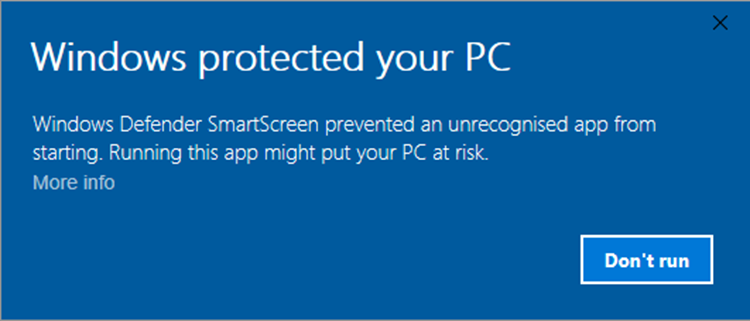
**Figure L02- 35** Microsoft Edge Privacy and Diagnostic Data Settings

1. To see what data Edge is collecting and reporting to Microsoft, you must click the **Windows diagnostic data setting** hyperlink shown at the bottom of Figure L02-38. If this is the first time you are doing this you will have to allow this action in the pop-up window that follows. You will find yourself at the Diagnostics & feedback setting. Review these options carefully to ensure you are comfortable with their current settings. Make changes as needed. You can also select **Delete** under *Delete diagnostic data* to purge data already collected and sent to Microsoft. This also deletes the data from their systems.
2. Figure L02-36 shows the *Security* menu options, including the ability to manage certificates.



**Figure L02-36** Microsoft Edge Security Settings

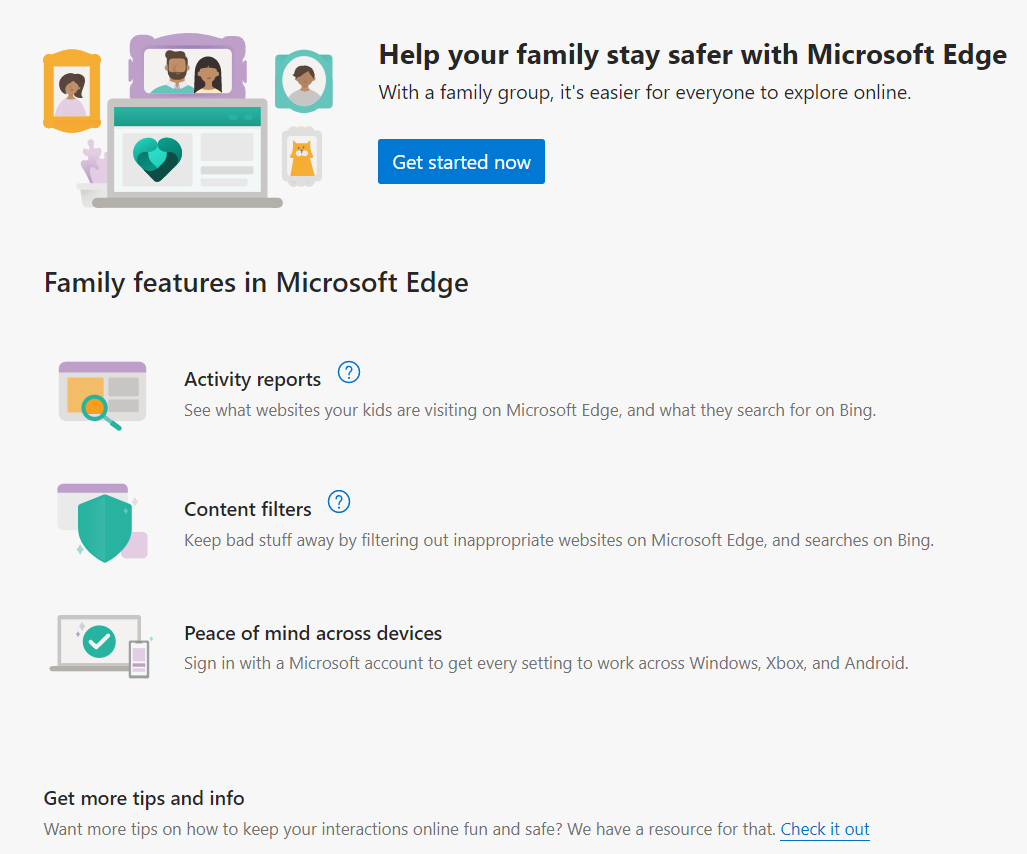
1. It also includes the Microsoft Defender SmartScreen, which can block malicious content and web sites, in conjunction with the Microsoft Defender antimalware application. This sometimes-annoying popup, shown in Figure L02-37, will stop suspicious programs. It may give you the option to “run anyway” in which case you should be sure the application is safe before running. Clicking on the **More info** option when encountering the pop-up can help you decide whether to do so or not.



**Figure L02-37** Microsoft Defender SmartScreen

## Family Safety

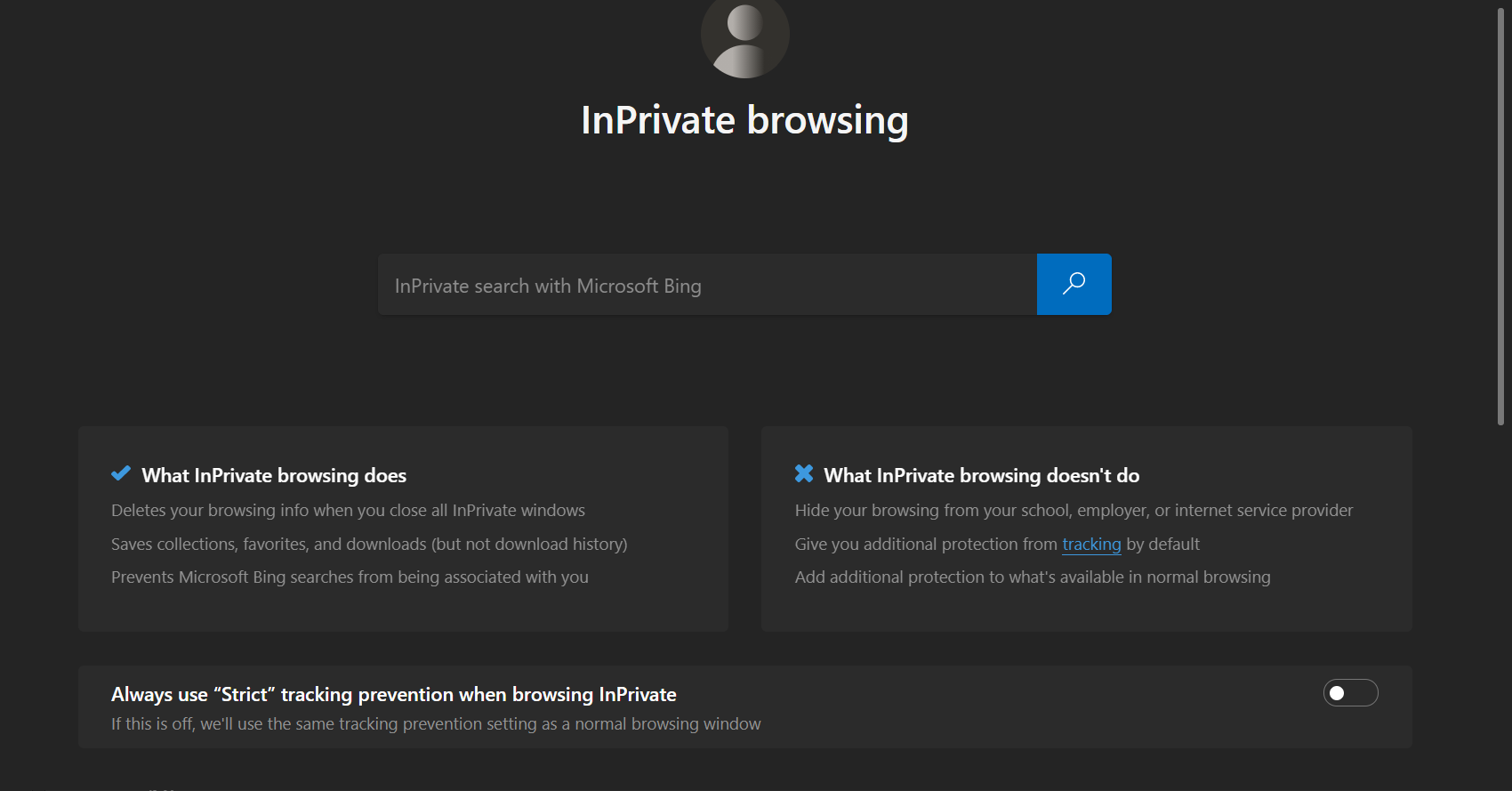
1. A feature that is relatively unique to Microsoft browsers is the Family safety options. Select **Family safety** in the left side menu of the Settings window. As shown in Figure L02-38, you can enable this to create accounts for underage children to restrict their online access, report their browsing habits, and filter inappropriate web sites.



**Figure L02-38** Microsoft Edge Family Safety

## InPrivate Window Browsing

1. Users can create anonymous browsing windows by right clicking the Microsoft Edge icon and selecting **New InPrivate Window**. This window, shown in Figure L02-39, allows the user to avoid saving passwords, cookies, and browsing history while in a private window. It allows the user to access any stored materials from normal browsing but will not save any new materials. Again, private windows do not block your information from an organization’s IT department or the Internet Service Provider.

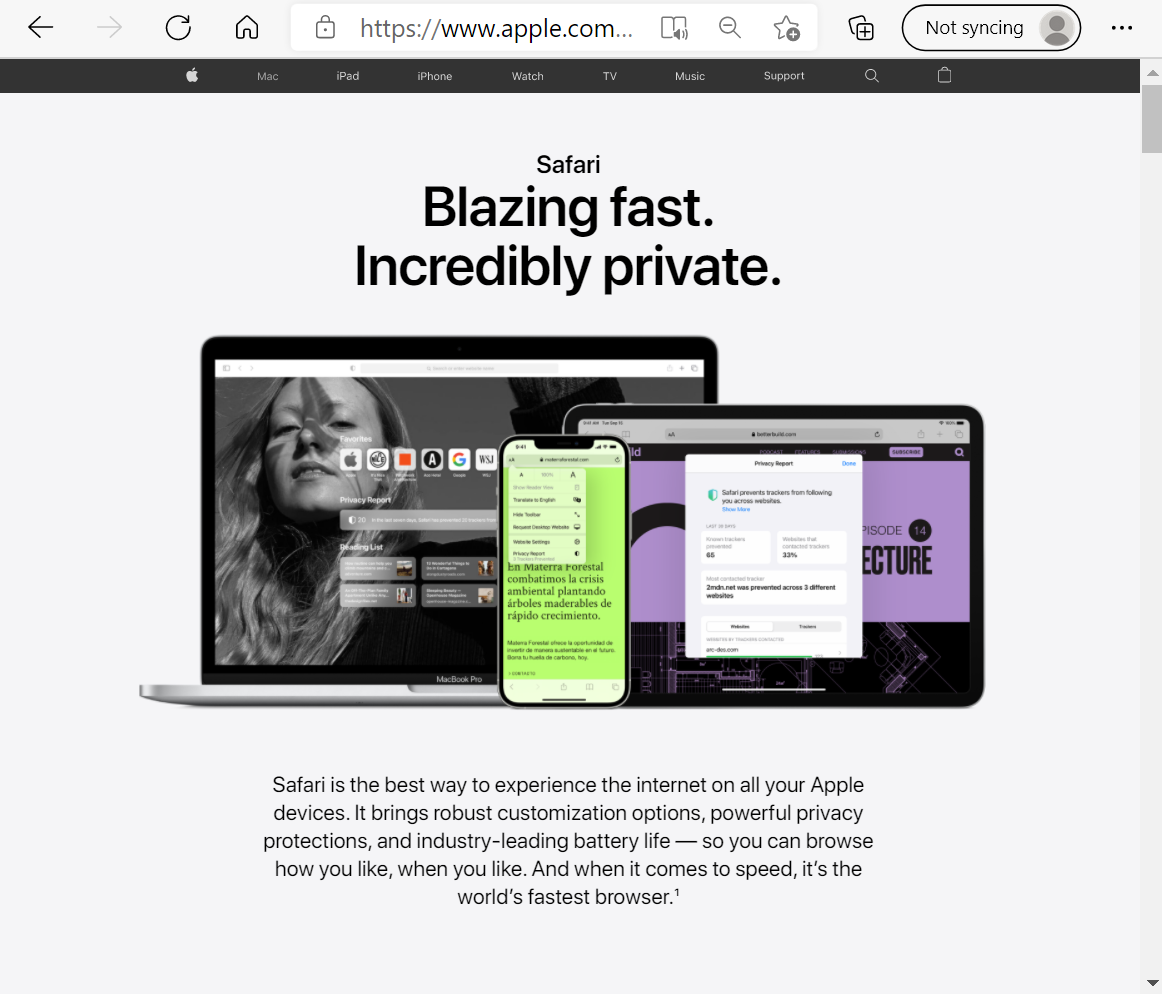


**Figure L02-39** Microsoft Edge InPrivate Browsing

While there are many other options you can configure for Microsoft Edge, these are the primary security and privacy features.

# Web Browser Security for Apple Safari

While we won’t go into detail about the security features of Apple’s Safari browser, it is available from <https://www.apple.com/safari/>, and contains many of the same features demonstrated in the other browsers noted. Apple Safari only runs on Apple Mac and other iOS devices like the iPad and iPhone. On mobile devices, much of the browser configuration is managed through the Device configuration rather than an options menu within Safari. Safari also has a Private browsing mode like other browsers.



**Figure L02-40** Apple Safari

Which browser(s) did you improve the security and privacy for? (Check all that you performed.)

* Google Chrome
* Mozilla Firefox
* Microsoft Edge
* Apple Safari

Were you able to access all the security and privacy features of the browsers you used?

* Yes

# Self-Reflection and Response

Which browser(s) did you improve the security and privacy for? (Check all that you performed.)

* Google Chrome
* Mozilla Firefox
* Microsoft Edge
* Apple Safari

Were you able to access all the security and privacy features of the browsers you used?

* Yes

Do you feel more equipped to make your browser experience more secure?

* Yes
* No

Please explain: After putting into practice all the privacy and security options provided, I believe Microsoft Edge to be safer than other browsers. Furthermore, the elements that gave me a sense of security were its performance enhancement and its many approaches to establishing tracking prevention.

## Instructor’s Response

|  |
| --- |
|  |