# 3. Using Linux

## 3.2 Linux Essentials Exam Objectives

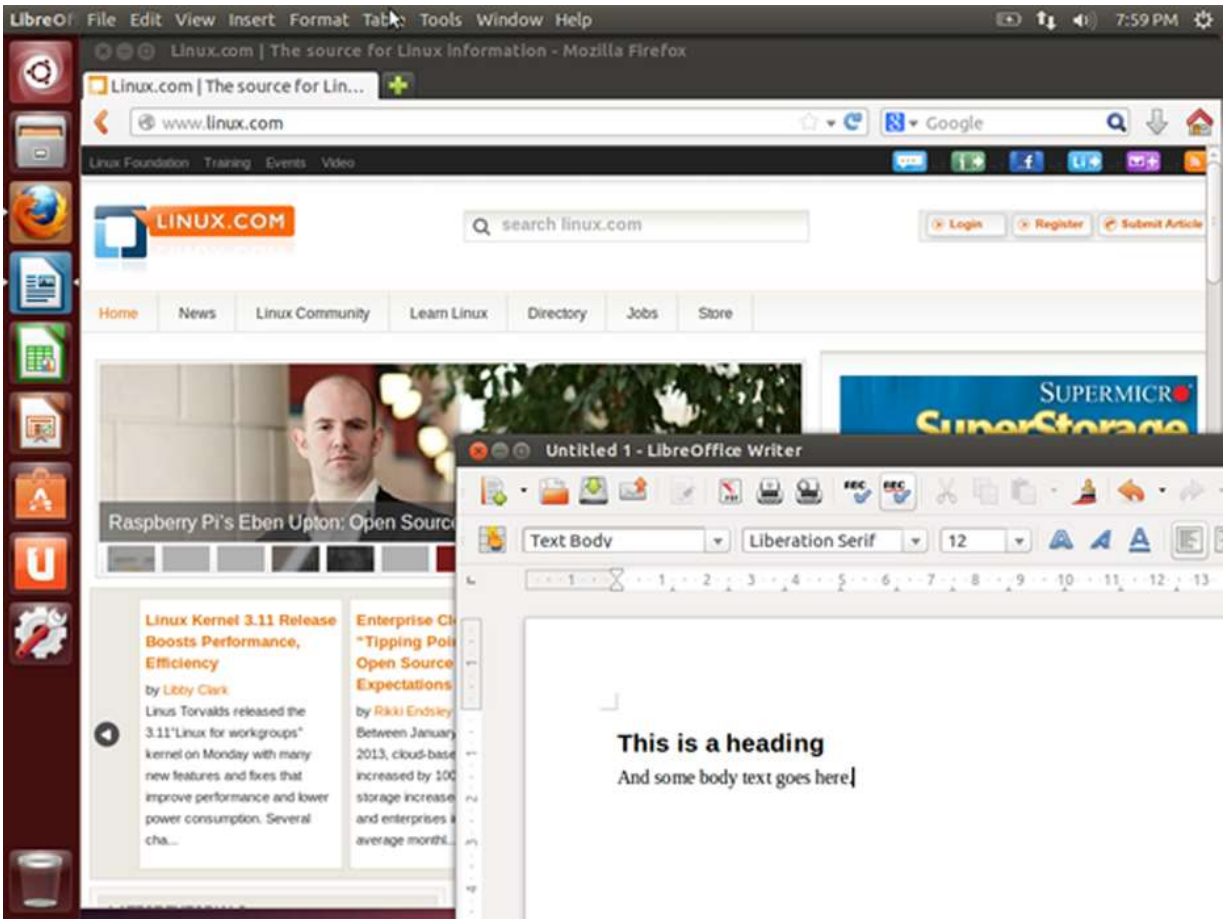
This chapter will cover the topics for the following Linux Essentials exam objectives:

Topic 1: The Linux Community and a Career in Open Source (weight: 7)

- **1.4: ICT Skills and Working in Linux**
    - Weight: 2
    - Description: Basic Information and Communication Technology (ICT) skills and working in Linux.
    - Key Knowledge Areas:
        - Desktop Skills
        - Getting to the Command Line
        - Industry uses of Linux, Cloud Computing and Virtualization
    - The following is a partial list of the used files, terms, and utilities:
        - Using a browser, privacy concerns, configuration options, searching the web and saving content
        - Terminal and Console
        - Password issues
        - Privacy issues and tools
        - Use of common open source applications in presentations and projects

## 3.3 Graphical vs. Non-Graphical Mode

Linux can be used in one of two ways: graphically and non-graphically. In graphical mode your applications live in windows that you can resize and move around. You have menus and tools to help you find what you'll use a web browser, your graphics editing tools, and your email. Here we see an example of the graphical desktop, with a menu bar of popular applications to the left and a LibreOffice document being edited with a web browser in the background.

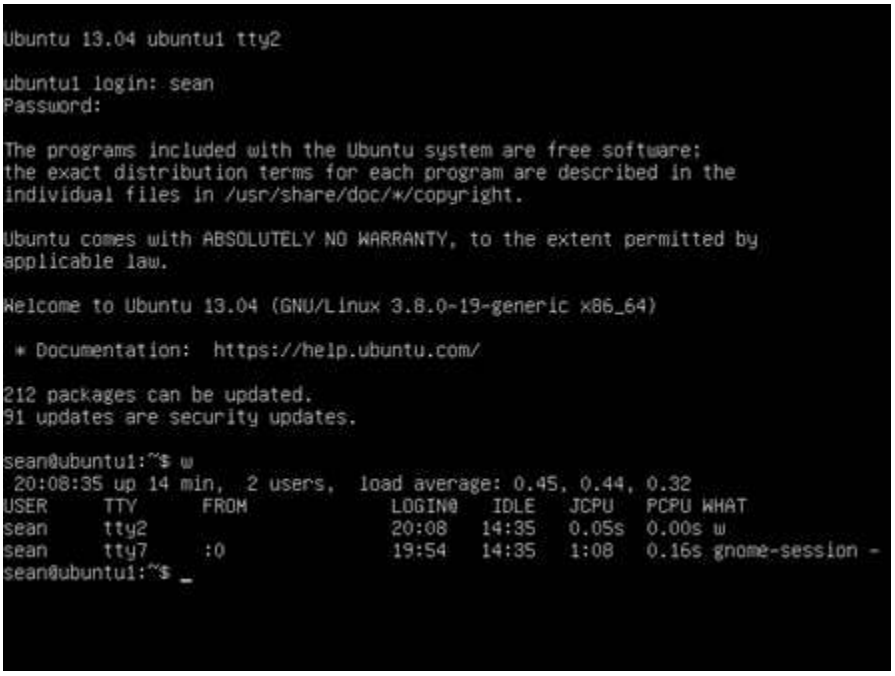



In graphical mode, you can have several shells open, which is very helpful when you are performing tasks on multiple remote computers. You even log in with your username and password through a graphical interface. An example of a graphical login is shown in the figure below.


After logging in, you are taken to the desktop where you can load applications.

Non-graphical mode starts off with a text-based login, shown below. You are simply prompted for your username and after that, your password. If the login is successful, you are taken straight to a shell.


In non-graphical mode, there are no windows to move around. Even though you have text editors, web browsers, and email clients, they're text only. This is how UNIX got its start before graphical environments were the norm. Most servers will be running in this mode too, since people don't log into them directly, which makes a graphical interface a waste of resources. Here is an example of the screen you might see after logging in.




You can see the original prompt to login at the top with the newer text added below. During login, you might see some messages, called the message of the day (MOTD), which is an opportunity for the systems administrator to pass information to the users. Following the

MOTD is the command prompt. In the example above, the user has entered the w command, which shows who is logged in. As new commands are entered and processed, the window scrolls up and older text is lost across the top. The terminal itself is responsible for keeping any history, such as to allow the user to scroll up and see previously entered commands. As far as Linux is concerned, what is on the screen is all that there is. There's nothing to move around.

### 3.4 Command Line

The *command line* is a simple text input that lets you enter anything from one word commands to complicated scripts. If you log in through text-mode, you're immediately at the console. If you log in graphically, then you'll need to launch a graphical shell which is just a text console with a window around it so that you can resize and move it around.

Each Linux desktop is different, so you will want to look around your menus for an option called either **terminal** or **x-term**. Both of those are graphical shells, differing mostly in appearances rather than functionality. If you have a search tool such as Ubuntu One, you can look for **terminal**, as shown here.


These tools let you quickly search your system for exactly what you want to run instead of hunting through menus.

## 3.5 Virtualization and Cloud Computing

Linux is a *multiuser operating system*, which means that many different users can work on the same system simultaneously and for the most part can't do things to harm other users. However, this does have limitations – users can hog disk space or take up too much memory or CPU resources and make the system slow for everyone. Sharing the system in multiuser mode also requires that everyone run as unprivileged users, so letting each user run their own web server is very difficult.

Virtualization is the process where one physical computer, called the *host* runs multiple copies of an operating system, each called a *guest*. The host runs software called the *hypervisor* that switches control between the various guests just like the Linux kernel does for individual processes.

Virtualization works because servers spend most of their time idling and don't need physical resources such as a monitor and keyboard. You can now take a powerful CPU and spread it around multiple virtual machines and maintain more equitable sharing between

the guests than is possible on a bare metal Linux system. The main limitation is usually memory and with advances in hypervisor technology and CPUs it is possible to put more virtual machines on one host than ever.

In a virtualized environment one host can run dozens of guest operating systems, and with support from the CPU itself, the guests don't even know they are running on a virtual machine. Each guest gets its own virtual CPU, RAM, and disk, and communicates with the network on its own. It is not even necessary to run the same operating system on all the guests, which further reduces the number of physical servers needed.

Virtualization offers a way for an enterprise to lower power usage and reduce datacenter space over an equivalent fleet of physical servers. Guests are now just software configurations, so it is easy to spin up a new machine for testing and destroy it when its usefulness has past.

If it is possible to run multiple instances of an operating system on one physical machine and connect to it over the network, then the location of the machine doesn't really matter. *Cloud computing* takes this approach and allows you to have a virtual machine in a remote datacenter that you don't own, and only pay for the resources you use. Cloud computing vendors can take advantage of scales of economy to offer computing resources at prices better than what it would cost to procure your own hardware, space, and cooling.

Virtual servers are only one facet of cloud computing. You can also get file storage, databases, or even software. The key in most of these products is that you pay for what you use, such as a certain amount per gigabyte of data per month, rather than buying the hardware and software then hosting it yourself.

Some situations are more suitable for the cloud than others. Security and performance concerns are usually the first items to come up, followed by cost and functionality.

Linux plays a pivotal role in cloud computing. Most virtual servers are based on some kind of Linux kernel and Linux is often used to host the applications behind cloud computing services.

## 3.6 Using Linux For Work

The basic tools used in most offices are:

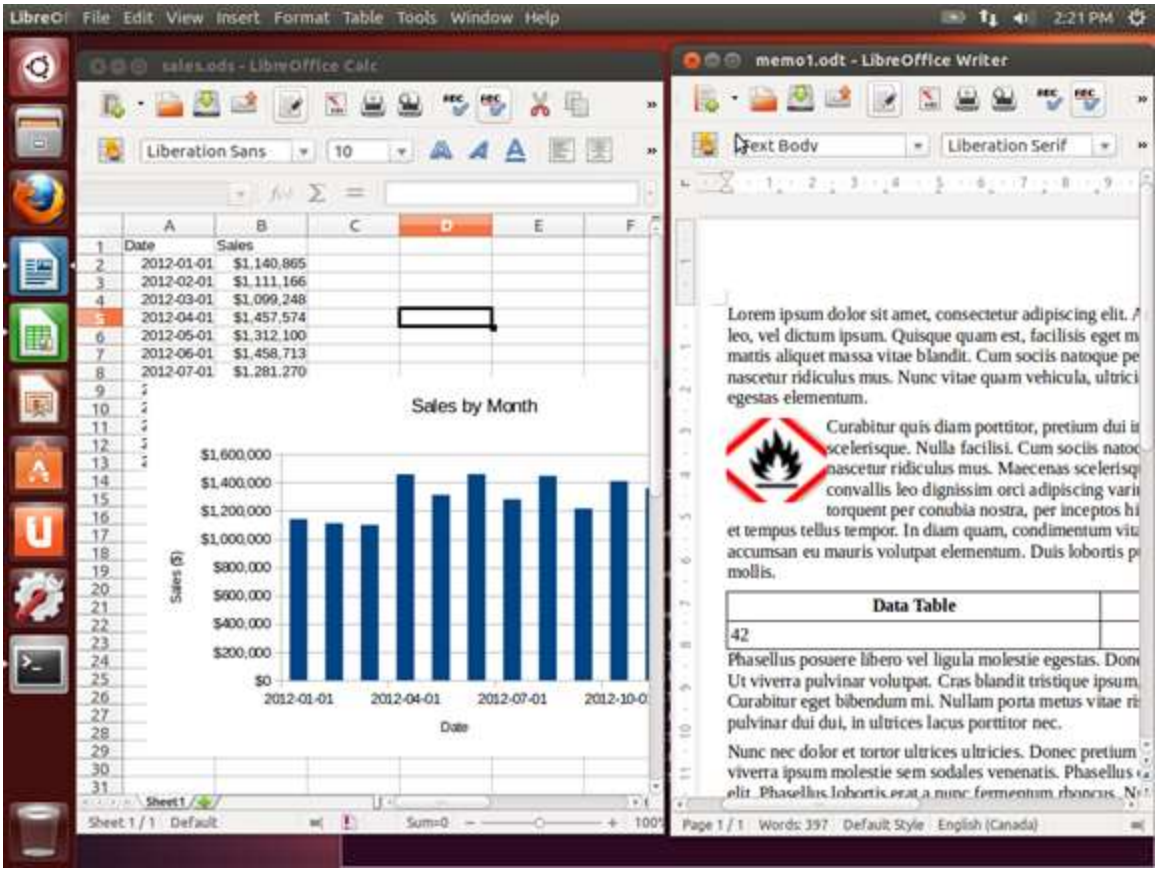
- Word processor
- Spreadsheet
- Presentation package
- Web browser

**OpenOffice**, or the more active **LibreOffice**, takes care of the first three roles. A *word processor* is used to edit documents, such as reports and memos. *Spreadsheets* are useful for working with numbers, such as to summarize sales data and making future predictions. A *presentation package* is used to create slides with features such as text, graphics and

embedded video. Slides may be printed or displayed on a screen or projector to share with an audience.

Shown below is the spreadsheet and the document editor of LibreOffice. Note how the spreadsheet, LibreOffice Calc, is not limited to rows and columns of numbers. The numbers can be the source of a graph, and formulas can be written to calculate values based on information, such as pulling together interest rates and loan amounts to help compare different borrowing options.

Using LibreOffice Writer, a document can contain text, graphics, data tables, and much more. You can link documents and spreadsheets together, for example, so that you can summarize data in written form and know that any changes to the spreadsheet will be reflected in the document.




LibreOffice can also work with other file formats, such as Microsoft Office or Adobe **Portable Document Format (PDF)** files. Additionally, through the use of extensions, LibreOffice can be made to integrate with Wiki software to give you a powerful intranet solution.

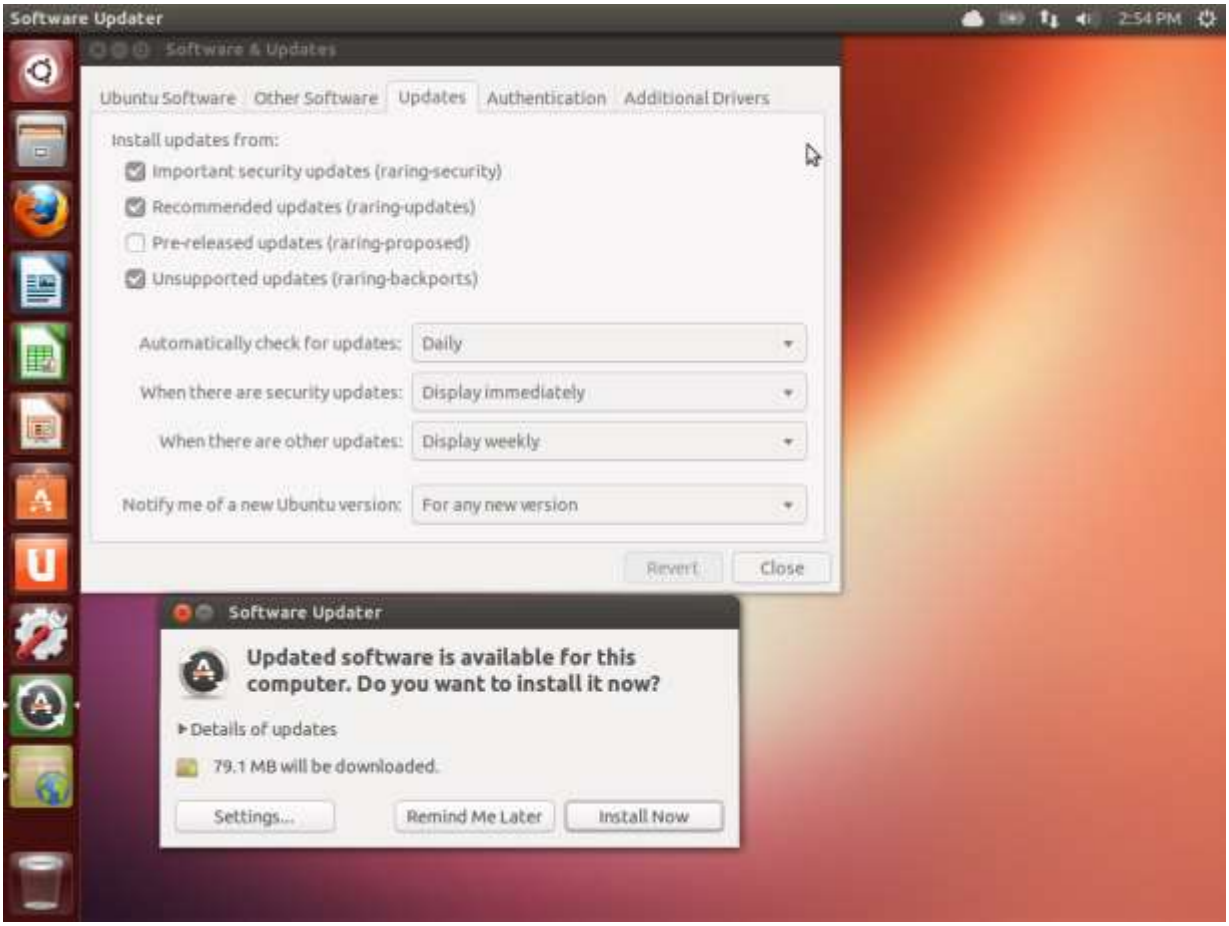
Linux is a first class citizen for the Firefox and Google Chrome browsers. As such, you can expect to have the latest software available for your platform and timely access to bug fixes and new features. Some plugins, such as Adobe Flash, may not always work correctly since those rely on another company with different priorities.

## 3.7 Keeping Your Linux Computer Safe

Linux doesn't care if you are on the keyboard of a computer or connecting over the Internet, so you'll want to take some basic precautions to make sure your data is safe and secure.

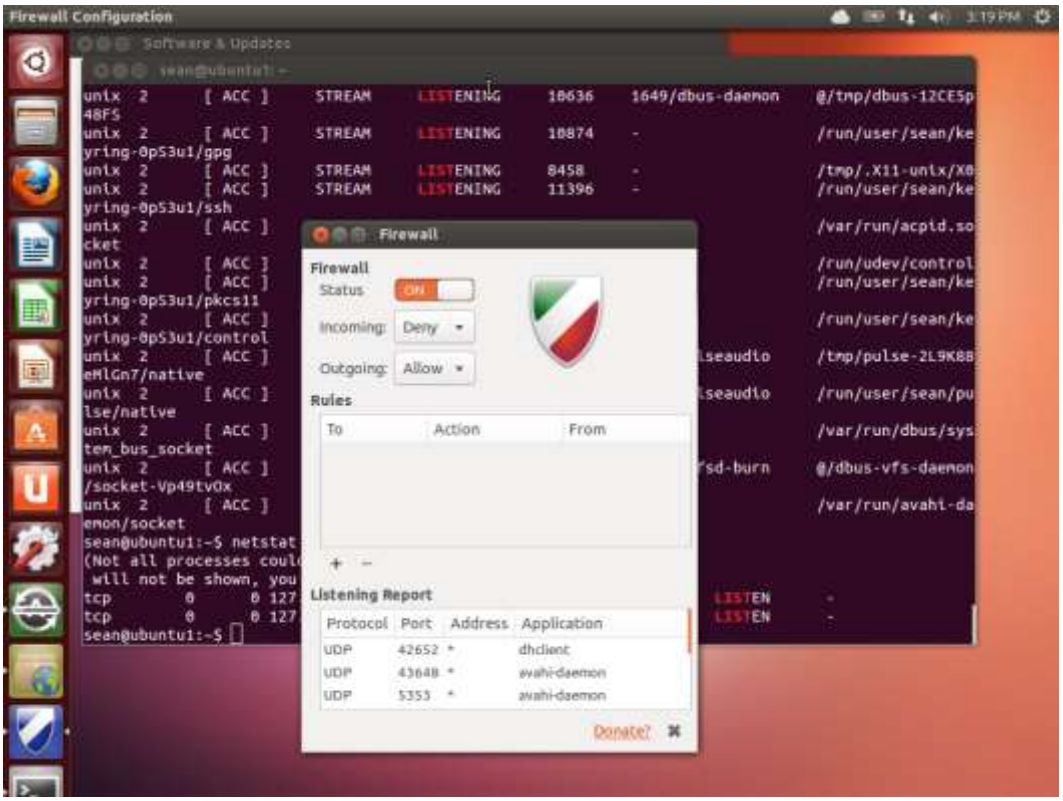
The easiest thing you can do is to use a good, unique, password everywhere you go, especially on your local machine. A good password is at least 10 characters long and contains a mixture of numbers, letters (both upper and lower case) and special symbols. Use a package like **KeePassX** (http://www.keepassx.org/) to generate passwords, and then you only need to have a login password to your machine and a password to open up your KeePassX file.

After that, make a point of checking for updates periodically. Here, we show the Ubuntu software update configuration, which is available from the **Settings** menu.




At the top, you can see that the system is configured to check for updates on a daily basis. If there are security related updates, then you will be prompted immediately to install them. Otherwise, you will get the updates batched up for running every week. At the bottom of the screen is the dialog that comes up when there are updates. All you have to do is click on **Install Now** and you will be updated!

Finally, you will want to protect your computer from accepting incoming connections. A *firewall* is a device that filters network traffic, and Linux has one built-in. If you are using Ubuntu, then the **gufw** is a graphical interface to Ubuntu's "uncomplicated firewall".




By simply changing the status to "on" you will block out all traffic coming into your computer, unless you initiated it. You can selectively allow things in, by clicking on the plus sign.

Under the hood, you are using *iptables*, which is the built in firewall system. Instead of entering complicated iptables commands you use a GUI. While this GUI lets you build an effective policy for a desktop, it barely scratches the surface of what iptables can do.

## 3.8 Protecting Yourself

As you browse the web, you leave a digital footprint. Much of this information goes ignored, some of it is gathered to collect statistics for advertising, and some can be used for malicious purposes.

As a general rule, you should not trust sites you interact with. Use separate passwords on each website so that if that website is hacked, the password can't be used to gain access to other sites. Using KeePassX, mentioned earlier, is the easiest way of doing this. Also, limit the information you give to sites to only what is needed. While giving your mother's maiden name and birthdate might help unlock your social network login if you lose your password, the same information can be used to impersonate you to your bank.

*Cookies* are the main mechanism that websites use to track you. Sometimes this tracking is good, such as to keep track of what is in your shopping cart or to keep you logged in when you return to the site.

As you browse the web, a web server can send back the cookie, which is a small piece of text, along with the web page. Your browser stores that and sends it back with every request to the same site. You do not send cookies for example.com to sites at example.org.

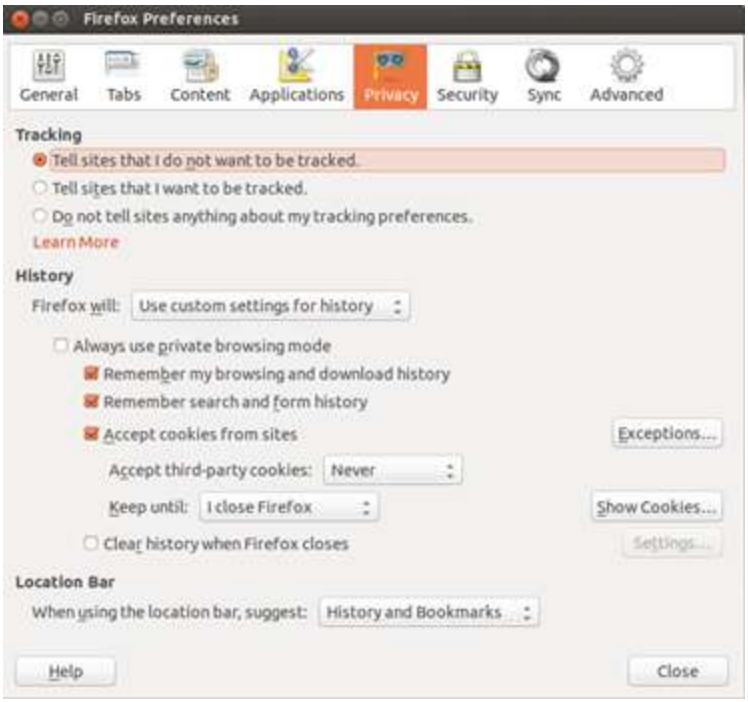
However, many sites have embedded scripts that come from third parties, such as a banner advertisement or analytics pixel. If both example.com and example.org have a tracking pixel, such as one from an advertiser, then that same cookie will be sent when browsing both sites. The advertiser then knows that you have visited both example.com and example.org.

With a broad enough reach, such as social network "Like" buttons and such, a website can gain an understanding of which websites you frequent and figure out your interests and demographics.

There are various strategies for dealing with this. One is to ignore it. The other is to limit the tracking pixels you accept, either by blocking them entirely or clearing them out periodically.

The cookie related settings for Firefox are shown in the figure below. At the top, you will see that the user has opted to have Firefox tell the site not to track. This is a voluntary tag sent in the request that some sites will honor. Below that, the browser is told to never remember third party cookies and to remove regular cookies (such as from the site you are browsing) after Firefox is closed.

Tweaking privacy settings can make you more anonymous on the Internet, but it can also cause problems with some sites that depend on third party cookies. If this happens, you might have to explicitly permit some cookies to be saved.




Here you are also given the option to forget search history or to not track it at all. With search history removed, there will be no record on your local computer of which sites you visited.

If you are very concerned about being anonymous on the Internet, you can download and use the **Tor Browser**, (https://www.torproject.org/projects/torbrowser.html.en). Tor is short for "The Onion Router" which is a network of publically run servers that bounce your traffic around to hide the origin. The browser that comes with the package is a stripped down version that doesn't even run scripts, so some sites may not work correctly. However, it is the best way of concealing your identity if you wish to do so.