Safe steps to download software on Linux

Negligence security risks range from information theft and virus infection, to unauthorized access to your Linux machine by other users. Therefore, this article lists safe ways to download software on Linux.

There is a common misconception that there are no viruses on Linux. In fact, they do exist. Although you can check your program files for infected files, it can take months before you realize that your Linux system has been compromised. You need to take certain steps to protect your operating system and yourself.

1. Check the hash value

A hash value (or checksum) is an alphanumeric string generated when some data is passed through a cryptographic function. It acts as a digital signature for your file.

To make sure that you don't download a corrupted file, some open source websites often provide the expected hash you will get after downloading the file. Let's take an example.

Let's say you are downloading tomcat 10, a popular web server. The hash value for Tomcat version 10.0.6 is:

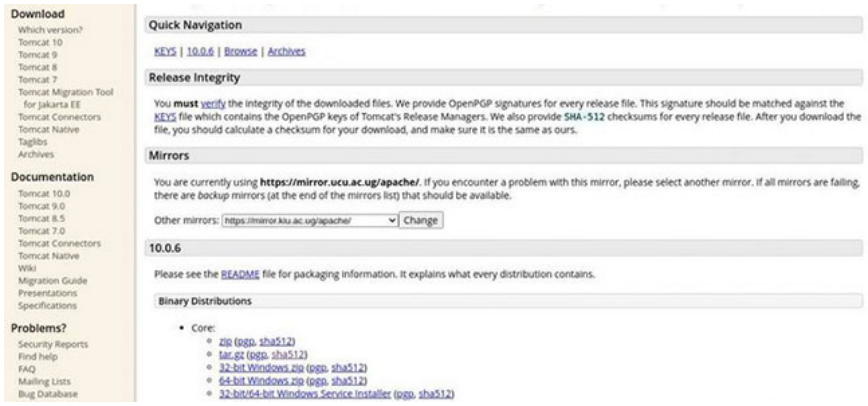
```
3d39b086b6fec86e354aa4837b1b55e6c16bfd5ec985a82a5dd71f928e3fab5370b2964a
5a1098cfe05ca63d031f198773b18b1f8c7c6cdee6c90aa0644fb2f2 *apache-tomcat-10.0.6.ta
```

The ***apache-tomcat-10.0.6.tar.gz part** is just the filename. The values ??from **3d39.2f2** include the hash value. To get this value, you need to go to the directory where you downloaded the archive and run the following command:

```
sha512sum apache-tomcat-10.0.6.tar.gz
```

You will get the hash value mentioned above. If you get a different value, it means your download has been corrupted and you need to delete it immediately.

In this particular example, the hash that the article used is **sha512.** That's because this is the function that the Apache Tomcat platform decided to use to protect the integrity of its downloads.



Other sites may use different hash functions, such as the popular **sha256** and **sha384** functions .

In case the website is using other hash functions, all you need to do is replace the name of the command with the hash function.

```
sha256sum filename-of-download sha384sum filename-of-download
```

It should also be noted that the file used is a TAR file (ie archive). But what if you downloaded a binary? The good news is that on Linux you'll get the same hash regardless of the file type.

The default mode of hash functions on Linux is text. Therefore, to switch to binary mode, use the **-b** option as follows:

```
sha256sum -b filename
```

2. Use safe websites

Downloading from secure sites greatly reduces the risk of malware infection. As a general rule, you should always use the official download site of the software you want to download. If for some reason you can't find the official website, consider using a trusted site.

Download sites like **FileHorse** and **SourceForge** are examples of trusted sites you can visit. These sites have been around for a long time and have earned the trust of users.

3. Compile your own source code

One of the biggest reasons the open source community exists is that you don't have to put your trust in the big software companies and hope that they don't do anything unauthorized on your PC.

When you download binaries, you give some rights to the compiler. But if you have access to the source code, you can take control back into your own hands.

With open source code, you can independently verify that the software does exactly what its author says. The only drawback to this is that you need to have above average programming skills. You can also decide on a strategy and check through only the important files that interest you.

For example, let's say you have some C source code cloned from a GitHub repository. Here's how you compile it yourself.

Run the command below to install the required build package. This package contains important tools needed when building software on Linux.

```
sudo apt-get install build-essential
```

Now, compile the C code using the gcc compiler.

```
gcc program-name.c -o program-name
```

After compiling, you can run the program by typing:

```
./program-name
```

4. Use the official package manager

The easiest way to install, update, and uninstall software is to use a package manager. There are some popular choices like pacman, dpkg, DNF and APT. The package manager works directly with the official software repositories and app stores.

The package manager does a lot of the heavy lifting for you. They handle standard operations such as managing the dependencies the software needs, ensuring the integrity and authenticity of downloads, and version management.

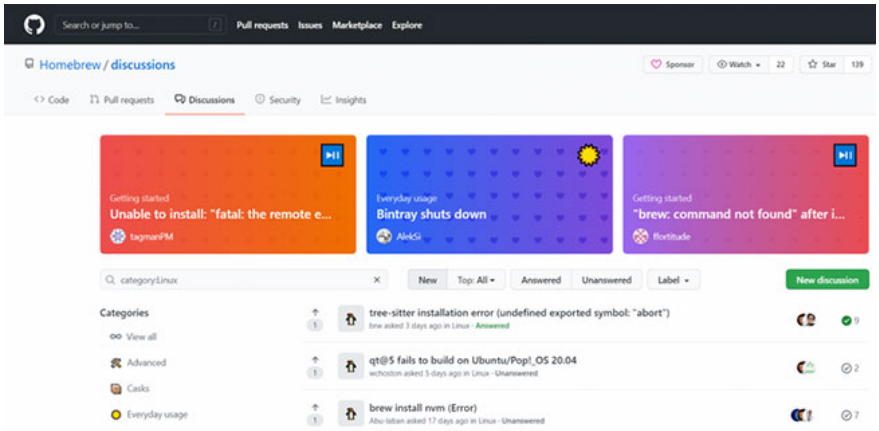
Another good thing is that distros often come pre-installed with a package manager. For example, Debian 10 comes with APT and Arch-based systems come with pacman.

5. Personal Research

The world of software is an ever-changing place, and keeping up with security trends is an important aspect of protecting yourself. There are several installation options that you can choose from in different situations. For example, install software on a virtual machine or use app containerization (a type of virtualization strategy that replaces traditional hypervisor-based virtualization).

App containerization is a particularly interesting trend because it ensures that your applications run the same way in different execution environments. It is possible to isolate the software core execution and its dependencies from the underlying infrastructure, providing unmatched security.

You should also check out software reviews and follow discussions on GitHub. Software reviews give you a good picture of what to expect after downloading, unexpected behavior users may have observed, and their recommendations.



The discussions on GitHub can also help you know what proactive measures you should take after/during software installation. You can also get a bunch of other security considerations not covered in the official documentation.

You should also pay attention to branches with multiple contributors on GitHub. There may be protocol changes going on and how your inability to keep up with these updates will affect your security.

You finished reading the article "**Safe steps to download software on Linux**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.
