Basic Guide To A Secure Linux USB Drive

While you are sitting in the comfort of your own home thinking about how to survive a crisis, do not overlook computer security. Even in a worst case scenario that includes an EMP attack, two small USB drives can still provide you with valuable information on everything from farming to preparing meals or hunting for food.

By the same token, taking the time now to secure private, web based communications channels can also make it easier to stay in contact with family members or other survivors that are of interest to you.

Do not be fooled into thinking that a computer will be useless in a crisis. If you have power, information, and a working device, it just makes sense to do everything possible to use them as efficiently as possible.

When you are on the run, it may not be a good idea to connect your laptop computer or smart phone to a WIFI hotspot. On the other hand, if you need to look up something important or communicate with someone via email, there are ways to limit your chances of being detected.

In particular, keeping a simple USB drive on hand with certain Linux distros (distro = a computer software distribution package) can help you stay safe and communicate with others at the same time.

While there is no such thing as 100% safety online, these tools may just be enough to help you get the information you need without taking increased and unnecessary risks.

Choosing USB Drives and Creating a Safe System

To begin, you should consider purchasing two USB drives for your secure system.

The first drive will be used only for the operating system, and you should not store any information on this drive. This is very important because hackers may still be able to gain access to encrypted drives regardless of how careful you are.

At the very least, if you need to access the internet, there will be no information available for others to find. You can use an 8 GB USB drive for this purpose, however a 16 GB unit will allow you to experiment with more distros and offer more space to work in.

The second USB drive should be used only for important information. If you are going to use either drive in your laptop computer or a desktop version, be sure to remove the hard drive. Depending on your computer, you may need to access the bios and make sure that the primary boot sequence places USB drives before hard drives.

If you do not know how to access the BIOS menu, call the manufacturer and ask them how to do so.

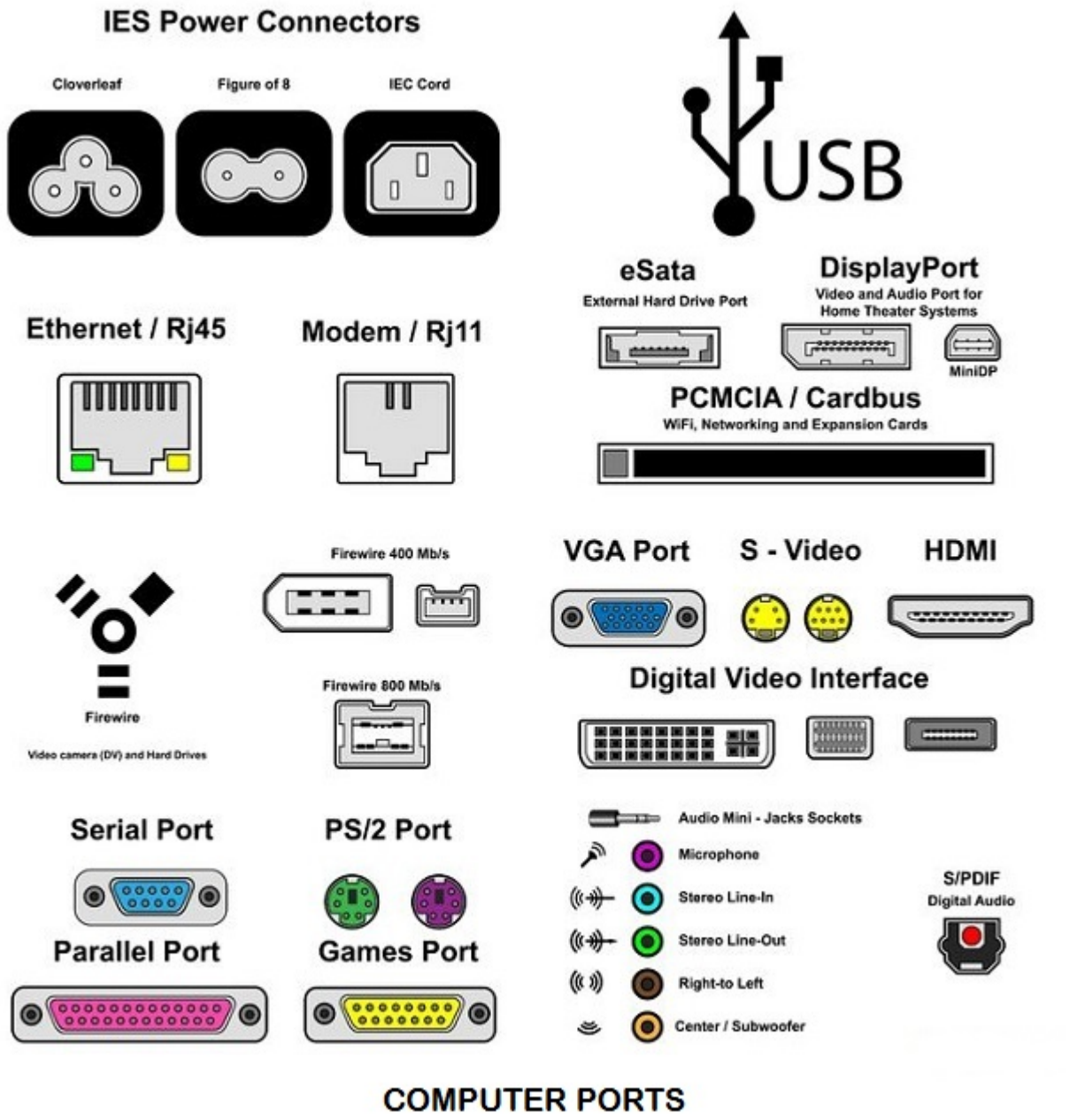
Tips for Anonymous Browsing

If you do not want to be identified while browsing online, use the Tails distro. This version only allows you to browse through a Tors connection.

Therefore, no matter where you are logging in from, your location may seem like it is in some other place. When downloading and testing out Tails, it is important to realize that this, and other security oriented Linux distros are on

the watch list for various intelligence agencies.

While these distros are not illegal to download, possess, or use, be aware that paranoid government agencies may become more determined to watch what you are doing.



Hot and Free Forensics Tools

Individuals that want to create a secure USB environment should always have tools on hand that can detect and trace possible threats and intrusions.

Caine and Kali are two Linux distros that offer a full range of network and connection testing tools. You can use these tools to test your own WIFI connections. Even if you only manage to find someone “borrowing” bandwidth it will give you good practice and help you stay safe later on.

It should also be noted that both Caine and Kali offer their own secure browsing environments.

Choosing a Distro that Meets Your Needs

There are bound to be times when you want a more secure system, but not something that is overly burdensome when it comes to saving files. For these situations, Knoppix and Puppy Linux make excellent choices.

While Knoppix takes up a bit more space than other USB based Linux distros, it comes with a robust image editing package plus plenty of other resources. In fact, if you are considering switching to Linux, Knoppix will give you plenty of options to explore without having to change your OS.

Do You Need More than One Distro?

As with many other things, the decision to use more than one Linux distro is a personal matter. You will find that some USB Linux distros vary greatly in terms of their focus and suitability for various applications.

For example, Caine is an incredibly robust distro, however when it comes to working with files, Knoppix may be more suitable for your needs. Even though Caine can be used in these capacities, you will need to do more work to make it an effective solution.

At the very least, if you are new to Linux, start out with

Knoppix or Puppy Linux so that you learn the basics before trying to adjust various settings in Caine or Kali. Unfortunately, saving files in either of these two systems can compromise the safety of your data if you don’t understand what you are doing.

Emergency Tools Distros

During the process of setting up a secure USB drive, you should always include tools that can be used to retrieve valuable information or diagnose hardware problems.

Over the years, I have found that Parted Magic offers a decent range of tools. If you cannot find a free older version, then simply install Caine 6.0. This version includes most of the tools found in Parted Magic, and is still free to download. Some of the best tools you will find for emergency care include:

- PhotoRec – this utility will let you search for, and retrieve deleted files. Even if you reformat the hard drive or it fails for non-mechanical reasons, the information may still be retrieved with this software. The interface does not use a mouse, however, with a little practice (and patience) you can still get to directories of interest and then save the files you want to the USB drive. As a word of advice, make sure that you have plenty of room on the USB drive; since that is where PhotoRec will want to place the files. Interestingly enough, PhotoRec can also be used to retrieve lost data from the Windows operating system, camera memory cards, and USB drives.
- There are also a number of tools that you can use to re-allocate space on the hard drive as well as manage other hardware issues.

Installing the Distro

You will find that installing Linux distros on a USB drive very easy. All you will need to do is download a program called Yumi.

Follow the prompts to select the operating systems you are interested in and let the program do the rest. Once you boot up with the USB drive, you will have a menu to choose the OS you want to proceed with. As simple as this menu may look, it represents one of the best and most effective disk partitioning and dual boot systems available.

Keeping Up to Date on USB Drive Linux Systems

Once you select distros of interest, it is very important to make sure that you keep an eye out for updates.

DATA STORAGE DEVICES

In some cases, hackers may have broken through critical areas on an older version.

You should also keep updated through various internet security sites to see how your Linux distros compare to others that you may not have tried yet.

Contrary to popular belief, there is a wealth of information on Linux vendor sites about the security of their distros.

You will find that the vast majority of them report problems quickly and also make adjustments as quickly as possible.

Information Is a Key to Survival

Chances are, you will never be able to remember every single skill or fact that may be required to manage a crisis in various environments. At the same time, no matter how small you print hard copies, carrying around that extra weight may eventually become more trouble than it is worth. As long as you keep a small netbook or other USB reading device onhand (and shielded from EMPs), then you can access all of your important data.

Using a Linux based distro may be very important to your privacy as well as your capacity to access your information. While you may not realize it, Microsoft can shift to web based mechanisms to shut people out of their computers because of "verification failures". If you have never installed a Windows OS onto a bare hard drive, then you have never seen the way XP and above require "online authentication" to install the system.

From there, it becomes relatively easier to control your computer from a remote location. While there is no evidence that Microsoft has taken these steps, rest assured the technology exists.

Why take that chance when you may need to access files without an internet connection to "verify your identity"?

This article has been written by ***Carmella Tyrell*** *for Survivopedia.*