How To Keep Your Data Safe In The Modern World

Even if you do not own a computer or use the internet, your personal information is more than likely in the hands of people, businesses, and government agencies that do.

As a result, there is no such thing as a person today that is completely safe from the impact of computer hacking and other noxious intrusions. That being said, there are some things you can do to thwart attacks that target your home computer or other devices.

Keep an OS that Never Goes Online

There are bound to be a number of things you do with your computer that do not require internet access. For example, you may have photos of valuable items that you need to keep for insurance purposes, prepper plans, and other things that should not be in the hands of other people.

Even though you may think you are disconnected from the internet, that doesn’t mean your computer isn’t storing the information to be transmitted at a later date. This problem may be even worse if you have a computer with Windows pre-installed. Interestingly enough, if you take a look at the hard drive partition data for these computers, you will see there is a small partition set aside for “diagnostics”.

These partitions may only be accessed by the manufacturer of the computer or a computer repair person that will use that partition to restore all your data – including things you never meant to have online. Given the increased reliance on cloud servers, it would not surprise me at all if all data winds up online one way or another via this or other programs running on the computer.

If you want to get rid of that partition, you will need to purchase the Windows operating system disks because the manufacturer's install license with Microsoft does not allow you to reinstall at will. This can cost hundreds of dollars, not to mention the fact that you have no idea where your data has been going all along.

Click here to find out how to survive when the lights go out!

When you need to use the computer, but not have information reach the web, the best thing you can do is have a USB based operating system that never accesses the web. Keep reading to find out about some operating systems that will suit your needs.

Change Your Computer's Operating System

Windows is notorious for having all kinds of security breaches. In fact, it seems like every time there is a major problem, Windows users are the most vulnerable.

By the time you factor in the cost of having to buy new hardware to accommodate a bloated, security deficient operating system, it is easy to see why so many people are turning to other operating systems. Since MAC computers and devices are still on the more expensive side, that leaves Linux. In most cases, you can run even the latest versions of

Linux distros on older systems and get improved speed and efficiency in the bargain.

If you do even a little research, however, you will find that there are hundreds of distros. Here are my recommendations for the most secure free Linux Distros:

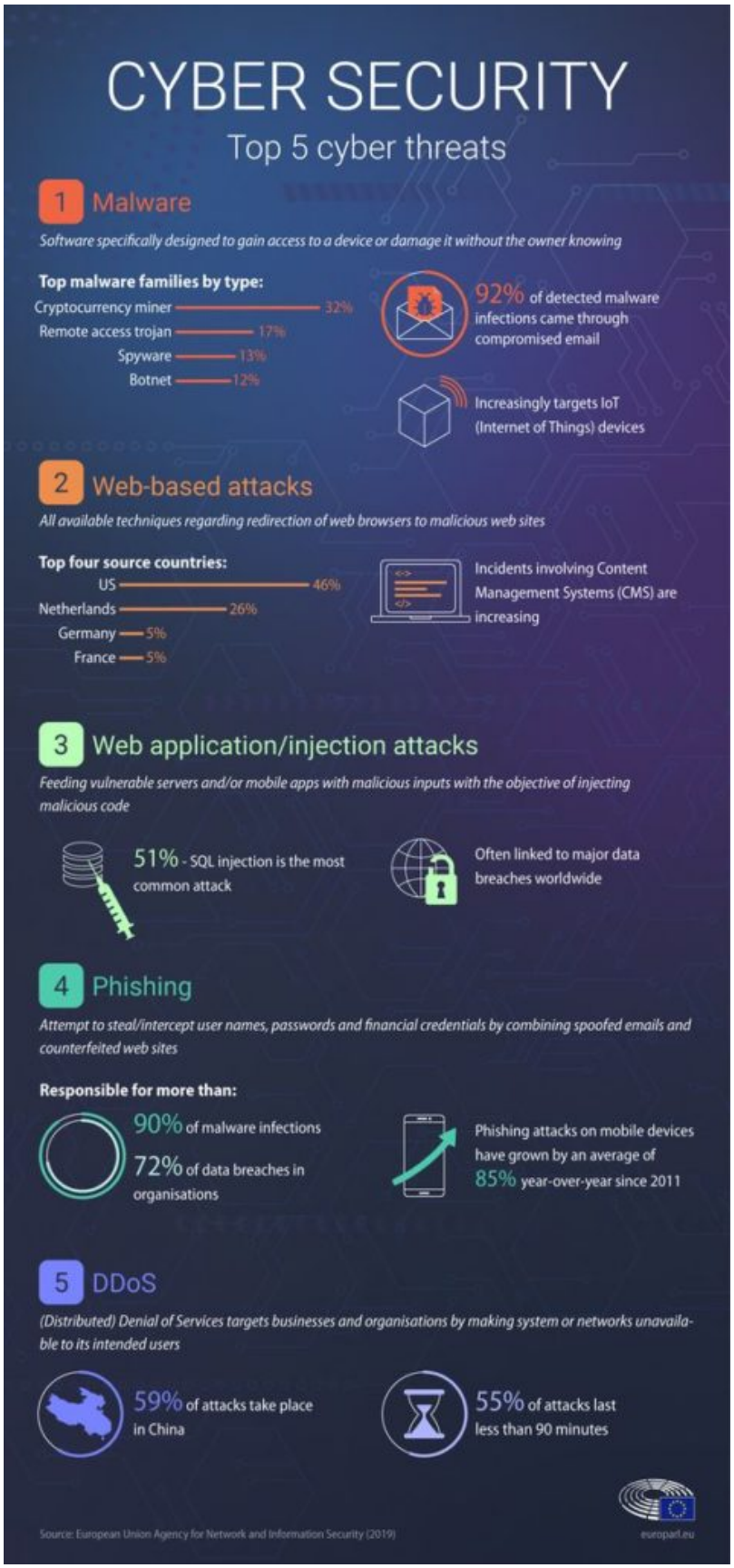
- Kali – this is one of the most secure operating systems. It is often used for hacker or "penetration" testing by professionals looking to stop computer threats. You can do a lot with this operating system to protect your data as well as figure out who is trying to get into your system.
- Caine – Caine is actually based on Ubuntu. The name itself is an acronym for Computer Aided INvestigative Environment. This operating system also has a number of tools that allow you to watch incoming network traffic. If someone does get into your system, you will also have a number of tools onhand to retrieve your data or figure out how it was damaged in the first place.

There are also a number of free tools pre-installed with this OS that are routinely used to recover data from Windows and other systems. The other nice thing about Caine is that you can run it completely from a USB drive. You can also run the whole operating system without access to the internet. From this perspective, it is one of the most hardened operating systems that you can run in complete privacy.

- Ubuntu – Ubuntu is a robust operating system that is often easier for people to migrate to after years of working with Windows. It has the distinct advantage of not being as heavily integrated with Windows crosswalks that, in my opinion, make Red Hat and many other distros less secure than they once were. While it is not designed to be a purely hardened OS, it is still far more secure than Windows.
- Mageia – Lineage wise, Mageia stems from Mandrake Linux,

which was built with security in mind from the getgo. Even though Mageia has increased its crosswalks with Windows, it is still a reliable and secure system. It can also be run completely from a USB drive and has a number of useful security utilities pre-installed.

If you are interested in trying Linux out, you have only to go to the respective developer websites for each distro. Once there, you can download free Live versions of the OS and either burn them onto a DVD or install them to a USB drive. The live versions will let you test drive the operating system without disrupting your current installation.



Get a Modem That Allows You to do Penetration Testing

Let’s say you installed Kali Linux and want to see if someone is trying to intercept data as it enters or leaves the computer. If you are on a WIFI internet connection, there are

special adapters that will work with Kali and other Linux distros to help you get that information. Sadly, many WIFI cards and adapters on the market are not designed to work with pen testing software. Getting one of these adapters will be well worth your effort.

Break Up Your Online Footprint Among Multiple Devices

If you use the internet for online banking, social interactions, finding information, or playing games, it may help to use different devices (or USB based operating systems) for different purposes. Today, many hackers target more popular websites and then use them as a springboard into your system.

When you limit the types of sites to different drives or devices, it may be easier to keep some of your other information secure. At the very least, use just one device for banking or financial transactions, and then something else for other online activities.

Politics and Your Browser

It is also important to explore more secure browser options. As with the Windows operating system, many people found out the hard way that Internet Explorer is one of the least safe browsers available.

On the other side of the equation, there is an increasing body of evidence to indicate that Google’s relationship with the government of China[1], and companies like Huawei[2] is problematic. To add insult to injury, there is even more evidence to suggest that Google may try to use search engine results to sway the 2020 elections.

While Chrome and Chromium are considered more secure than

Internet Explorer, don’t be surprised if your research results aren’t what they used to be. Given the fact that many websites, including Google products use various tracking tools, you may also find you are not browsing as privately as you thought when using these browsers.

Given increased awareness of foreign influence on the United States, it might be useful to try browsers such as Firefox, Brave, and Tor. You may also want to look into VPN services that allow you to browse with increased privacy.

Other Devices that Rob you of Privacy Online

Quite frankly, if you have smart speaker devices like Alexa, Siri, Google Home, or even nanny cams that tether to your smart phone, there isn’t much point to worrying about the security of your computer. There is potential for all of these devices to be hacked, or accessed via the companies that manufactured them.

If you have a need for security cameras or other smart home devices, you will need to find some way to keep them from accessing the internet while giving you the service you need from them. Unfortunately, many of these devices have proprietary controllers that cannot be adjusted to work offline or without some kind of cloud based storage.

You can try finding a programmer that can rewrite the driver so that it connects via a local network to a device that doesn’t access the web. You can also shift away from smart devices and use web cams that will store information on your computer instead of send it to the web. If you do need to monitor your home while away, then make sure those cameras and devices are powered off when you are home.

The more convenient computers and associated devices get, the

less privacy you have. Today, as Iran and North Korea increasingly jam GPS systems and engage in other hostile acts, it should come as no surprise that the average computer user needs to take extra security precautions. While it would take volumes to cover every threat and how to solve it, there are some simple things you can do to increase your safety while browsing online as well as when using various “smart” devices.

Resources

[1] https://www.washingtonexaminer.com/opinion/googles-anti-trump-bias-calls-attention-to-its-questionable-ties-to-china

[2] https://www.rollcall.com/news/congress/republican-senators-target-googles-relationship-chinese-tech-giant-huawei