SECURE LAPTOP CHECKLIST

HUDSON INFOSEC

WWW.HUDSONINFOSEC.COM

INTRODUCTION

In today’s highly mobile world, it is inevitable that our mobile devices would become the target of thieves and competitors. Whether it be the real estate agent who has lost their laptop because someone smashed the car window, to the startup who had a laptop stolen from an agent of a competitor or a government laptop that seem to be left, well, anywhere. These laptops tend to have very sensitive information on them and need to be protected.

There’s not much you can do to defend against someone smashing your car window, there are steps that you can take to deny them the fruits of their labor. The good news is that you don’t need the help of a full-fledged IT department to help you secure your laptop. In the following pages, you’ll find a checklist with some very simple steps you can take to stop you from being the lowest hanging fruit on the tree.

ENCRYPT YOUR DRIVE

The hard drive in your laptop is where all the good stuff resides. It needs to be protected. The best way to protect it is to encrypt it. Encryption “scrambles” the contents of the drive to those who don’t have the credentials to unlock it, rendering it useless. This alone goes a long way to alleviating the stress regarding having sensitive information on a stolen or lost laptop.

ENCRYPT YOUR DRIVE (WINDOWS)

WINDOWS

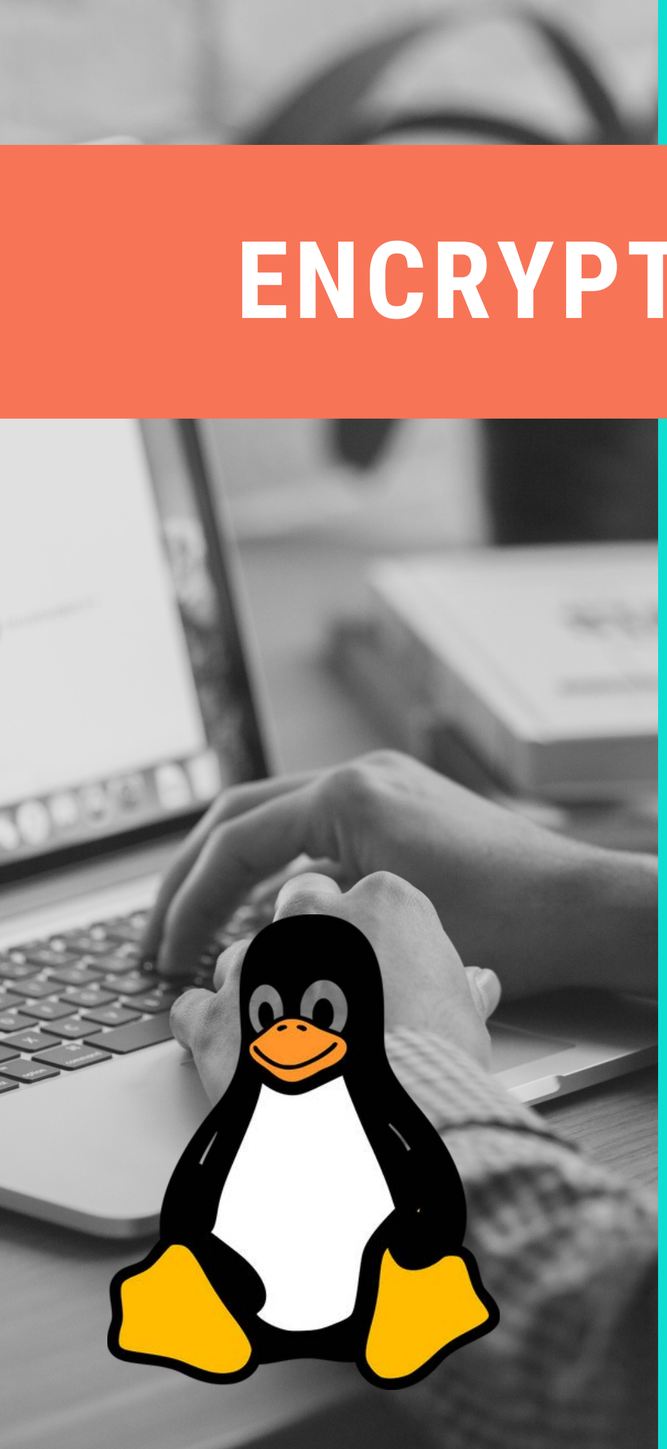
The best way to encrypt your hard drive under Windows is to use BitLocker. It provides excellent protection and doesn’t require you to reinstall Windows. In fact, the setup process works in the background while you work. Best of all, it’s free and included. There’s one caveat: you have to have Windows Pro or Enterprise for this feature to be present.

ENCRYPT YOUR DRIVE (macOS)

macOS

The best way to on macOS is to use FileVault. Like BitLocker for Windows, it too doesn’t require the reinstallation of the operating system and also will run in the background while you work. Even better for Mac owners, there is only one version of macOS so FileVault is available for everyone.

ENCRYPT YOUR DRIVE (LINUX)



Linux

Drive encryption on Linux – like Linux itself – can be achieved in more than one way. My preferred way of hard disk encryption is using Luks. Luks works on all variants of Linux, unfortunately, it requires you to reinstall the operating system. The good news is that the all the major Linux distributions – Ubuntu, Red Hat, Debian, Arch – offer you the option to encrypt the disk during operating system install.

SAFE COMPUTING AT THE COFFEE SHOP

Ok, so now that you have protected the data from physical theft, it’s time to protect yourself whilst “working” at the coffee shop. This is super simple to achieve. You just need a piece of software called a VPN (Virtual Private Network). What this does is secure ALL of your Internet communications through an encrypted “tunnel” to the VPN providers computers and from there to your requested site and back. This means that anyone snooping on the WiFi can’t see what you’re doing. There are many brands out there, but the one that I have personally used for years is PIA (Private Internet Access). They are extremely well priced, and their products work on Windows, macOS and Linux. In addition, it works on iOS and Android as well.

ANTI-MALWARE

The last simple thing you can do is to one that has been recommended for many years. That is, Anti-Virus / Anti-Malware. On Windows 10, you have anti-virus built-in, in the form of Windows Defender. Now that’s “ok” but honestly, you can do MUCH, MUCH better. It’s not enough to simply scan for viruses, you need to check for more sophisticated threats such as worms and rootkits. These nasty types of malware can be devastating. The big anti-virus / anti-malware software producers such as SOPHOS , Avast and Malwarebytes offer excellent protection for the money.

SECURITY UPDATES

Finally, APPLY SECURITY UPDATES. These security updates are critical as they fix problems that can’t be fixed by anti-virus software. When you hear about massive security breaches at large firms such as SONY and Equifax, eight times out of ten, the problem can be traced back to an unpatched system.

IN CONCLUSION...

If you follow the steps in this guide, you will be well ahead of the pack when it comes to not only protecting your clients data but yourself as well.

If you want someone to just do it for you, at Hudson Infosec, we have a very affordable Soloprenuer / Freelancer Secure Laptop service that we offer, where you bring in your laptop and we walk you through the process and do it for you. The checklist we go through is more comprehensive and utilizes more advanced tools.

You can book your appointment today at
https://www.hudsoninfosec.com/book-online