COMPUTER & INTERNET SECURITY FOR BEGINNERS

Hello and welcome to our free computer and internet security guide this guide is not intended to explain every option available to you nor will it go into depth on how to install and use each individual product.

The aim of this guide is to help educate the less Tech savvy amongst us for a safer online experience for everyone.

In a Youtube video we released we looked at the tails operating system what it was and how to install it for use.

After releasing that video we had lots of comments and questions regarding internet security in general things like VPN services and proxies were mentioned.

So we thought we would compose this basic guide explaining some of the options available to you and what these products/services actually do for you.

Ok so let's jump right into it, we are going to cover briefly...

Antivirus software.
Antivirus & Firewall combination software.
Virtual private network services.
Proxy servers.
Encryption containers.
Encryption (whole drive)
Tor browser for windows (onion proxy browser)

ANTIVIRUS

Ok we all know that we need to be using an antivirus solution these days we can't even load the Google home page without being at risk of infection so if you aren't using one and by some miracle your system still works go and get this sorted asap.

Free services can be found here...

www.avg.com
www.sophos.com

Or better still grab yourself an antivirus & firewall package to get protected against hackers to.

ANTIVIRUS & FIREWALL

These are much better packages over your basic antivirus package pretty much all of these are a pay for service and offer protection against viruses and hackers, some even offer encryption services for whole hard drives and containers both explained in more detail later.
We recommend ESET www.eset.com

Ok so wave got our antivirus/firewall up and running but what else can we do to protect ourselves both on and offline?.

Well this is where things get murky and the simple answer to this is that it all depends on what you want to do and or what your personal security needs are.

You may choose to use all or none of the below options available to you most are a pay for service but to better understand if you need or want any of the below were going to break them down one by one.

VIRTUAL PRIVATE NETWORKS (VPN)

Right so you may have heard about virtual private networks or VPN servers so for the beginner what is a VPN.

A VPN is a private service that encrypts your internet connection and spoofes your ip (changes you ip) to either a false one from your own country or a false one from another country making it look like your computer is actually in the spoofed location.

Such as someone surfing from the UK using a VPN that points to a server in the US would look to anyone looking in like they were sat in the US cool right☺.

Ok but that's not all a VPN does for you as I said at the beginning your whole network connection is encrypted and wrapped up inside a tunnel at one end there is you the other your target website.

But heres the cool part should anyone try to see inside your tunnel the tunnel will be instantly shut down and a new one opened up in milliseconds causing no interruption to you but making you invisible once again to your attacker.

Some examples of VPN services are...

www.cyberghostvpn.com
www.tunnelbear.com

PROXY SERVERS

Let's talk proxy ok so there are many ways of using a proxy and what these basically are is a man or multiple men in the middle and here is how it works.

Your computer routes through another computer or computers before moving on to your target site once again similar to a VPN masking your true identity and making it look like you are one of the computers that you are routeing through as opposed to your real location.

Some proxies are stronger than others some are very slow but lots can be used free of charge such as the service here...

www.ninjacloak.com

Go try it first head on over to nijacloak then use their URL bar to navigate to www.whatsmyip.org and have a look at your result.

Now repeat the procedure without the proxy and match up your results.

ENCRYPTION CONTAINERS

Let's talk encryption in this guide we are going to cover two different types of encryption the first being container based encryption.

Container based encryption utilises a piece of software such as our example below that can create a secure encrypted folder or vault if you like on a computer that you can open up with a variation of passwords or USB security keys etc.

Once open you can add or delete data etc but then once you exit out you leave only one file visible your vault.

All data within the vault will be scrambled using a special algorithm based on your passwords and the type of security method used when making your container.

Such as the beyond DOD standards triple blowfish 1344bit encryption cipher with 256bit SHA encryption protecting the password hash.

Without the correct passwords or keys the data is impossible to access.

A good example is SecureStar Drivecrypt

www.securestar.biz

ENCRYPTION (WHOLE DISC)

Not at all the same as container based encryption this method encrypts entire hard drives including the operating system.

Rather than your passwords opening a single file once your computer is already running this style of encryption requires passwords to be entered before the computer is even started up.

Failure to do so prevents access to the computer and data, should your hard drive be removed and added to another system it would be inaccessible.

A good example is SecureStar Drivecrypt Plus Pack

www.securestar.biz

TOR BROWSER

Want to surf the web anonymously hiding your IP and utilize proxies all for free?

TOR is the answer built on a variation of Firefox and utilising strong privacy measures.

TOR is a free to use open source browser that protects your privacy and lets you access the deep web/Darknet.

You can try out Tor free here.

www.torproject.org

We hope you enjoyed this short guide and have enjoyed having a play around with some new software.

This is not meant to be an in depth guide and there are way more options available to you than the examples we have stated.

Written by – Matthew John Callear – Owner @ Callear Technology

www.calleartechnology.co.uk

www.facebook.com/calleartech