Expendable Operating Systems

Welcome back to the course! Today's topic is super fun: expendable operating systems...operating systems designed to be easily removable, replaceable, and destroyable. Let's get right into it!

You know what's not expendable and meant to stay? You know where this is going...

Promotional Spot

If you watched the recent lesson going through different operating systems to use, you may recall *Qubes OS, an OS that runs every program as its own virtual program to protect the system's files.* Well, virtual machines accomplish a similar goal, but on an operating system level, opening up many possibilities. To start with security, VMs run guest operating systems completely sandboxed and separate from your host operating system. *So if you buy a Mac, your host operating system is MacOS. You can set up a Windows, Linux, or another MacOS operating system inside a virtual machine, this would be your guest OS. The host is your "real" one so to speak, and the guest is your expendable virtual machine, running on top of your host.*

This is great for security because it's isolated from your actual system, as long as you don't *share folders between the two systems, NEVER do this. Now, there have been cases, although very few, of exploits that would allow the host OS to be infected from a guest operating system.* But, this doesn't mean virtual machines don't add a HUGE layer of security. *You can even run something like Qubes OS, which keeps its programs in mini virtual machines, on a guest OS. It's like a virtual machine inside a virtual machine. This demonstrates having multiple stages of security, and not relying on a single point of protection, something you should always try to implement in your OPSEC.*

When it comes to privacy, virtual machines are an excellent tool to create pseudonyms, or ghost identities. They are expendable, can be deleted in a couple mouse clicks, are separate from your host OS (so nothing is mixed between identities) and you have full control of how you want the OS configured. As an example, let's say I used my **** show personal laptop **** personal Windows computer for work, but wanted to separate my personal life from my work life. *I can create a Debian VM to store my personal information, and have no work data whatsoever inside of it. I can set up another VM running Qubes to handle sensitive data, like banking and online purchases.* These use-cases demonstrate the potential you have as a security and privacy-minded individual to separate your life across

different virtual devices. We will cover pseudonyms much more in-depth later in the course

So how do you set one up? The two main virtual machine programs are *Virtualbox, and VMWare. Virtualbox is FOSS so I'm going to lean you in that direction.* Every OS has a slightly different setup, *so dig online to find out how to configure the guest OS of your choice, it's typically pretty straight-forward.*

Random interruption! *Whonix is an OS that runs as a virtual machine and routes everything through the Tor network, similar to Tails OS, a LiveOS we'll discuss shortly.* It isn't necessarily better or worse than Tails, they both have pros and cons. Whonix is a cool project to try for those of you wanting to properly access the Tor network in a virtual machine. Tor will be discussed in our very next lesson.

The second major type of expendable operating systems is *Live Operating Systems, which as the name implies, run live,* and don't retain any information or changes you make to the OS. Most of these run off a **** show flash drive **** flash drive, allowing you to quickly boot into the OS on any device, at any point in time. When you shut off the computer, all things you downloaded, changed, or configured in the live OS are deleted and restored back to factory settings. *Probably the most well-known strictly live operating system is Tails. It is built on the Linux distro Debian, and tunnels all of your traffic through the Tor network, similar to Whonix.* Tails attempts to offer an all-in-one anonymization tool, but keep in mind you still have to use it in an anonymous fashion, and not rely on it being your only tool to protect you. This will all be covered later in the course. *Most Linux distributions allow you to create a liveOS variant on a flash drive, so you can do this with almost all Linux distributions.*

Similar to virtual machine separation, live operating systems give us similar functionality, that you can bring with you anywhere, and delete all your data when you shut it off--truly expendable. *Maybe you have a live version of Qubes to do secure banking, Tails OS for anonymizing your casual web traffic, or a Debian flash drive used for personal accounts like email.* Being able to separate your life is essential, as we'll discuss in section 6, and having an expendable arsenal is something very important to have.

Queue Outro Promos

That's going to wrap up expendable operating systems, the next lesson will talk *about Tor which I'm sure* is a topic many of you are looking forward to viewing. I'll see you then, and thank you for watching.