The following instructions are vital to stay safe when handling malware. Please read them and use the videos in this section whenever you don't know how to proceed. Feel free to skip videos if some of these seem trivial for you.

Complete the quiz at the end of this section to make sure that you know how to stay safe.

Always follow the safety instructions, even if they are inconvenient. Otherwise you put your own systems at risk. I am not reponsible for any damage caused by infecting your system.

Virtual Machine

Use a virtual machine with snapshot capabilities for your analysis lab. We need those snapshots to revert the system back to a clean state.

In this course we use VirtualBox. But if you have a license for VMWare, you can use this too.

Not okay: Sandboxie

Ideal case - you have a spare computer

Ideally you have spare machine:

- this machine is dedicated to malware analysis. That means no personal accounts (banking, gaming, email) on that machine unless they are for malware analysis
- if anything goes wrong on this dedicated machine, malware will not be able to steal things like banking credentials or encrypt your only copy of the bachelor's thesis one day before submission

On this spare machine, you ideally use another operating system than Windows, e.g., Remnux would be a good choice. We will be analysing Windows malware, and most of these will only run on Windows.

Please follow these rules:

- keep network access turned off for the guest system, turn it only on to download tools and samples
- do not auto-mount shared folders that are writeable for the guest system
- deny execution for shared folders
- store samples in password protected archives
- do not download malware unless it is already archived (password protected)
- keep your host system up-to-date
- keep VirtualBox up-to-date
- use adblockers for your browsers
- do not attach external drives to the guest system while executing samples
- use different wallpapers for host and guest to prevent mix-ups

If you want to keep using Windows because you don't know your way around Linux/Unix and don't use a Mac, read the section below.

The not-so ideal case - you have only one computer

I am aware that many people cannot afford a second system, and will use their main system for analysis training. I am also aware that running a different operating system than Windows may be too much to ask.

Please take the following steps to secure your system. Do not forgoe any of this if you want to keep your system safe.

- keep network access turned off for the guest system, turn it only on to download tools and samples
- keep clipboard sharing between guest and host turned off
- never auto-mount shared folders that are writeable for the guest system
- deny execution for shared folders, on a Windows host: apply ACLs that deny execution for 'Everyone' for shared folders and sample folders
- on a Windows host: use a Standard User Account
- store samples in password protected archives
- do not download malware unless it is already archived (password protected)
- keep your host system up-to-date
- keep VirtualBox up-to-date
- on Windows host: use an antivirus program on the host system and keep it up-to-date
- do not analyse malware on the host
- use adblockers for your browsers
- do not attach external drives to the guest system while executing samples
- use different wallpapers for host and guest to prevent mix-ups

Handling samples

If you have a dedicated analysis machine, you can analyse samples statically on the host system.

For dynamic analysis, that means, running or debugging the samples, you should use a virtual machine that allows to use snapshots. We use VirtualBox for this course.

The default state for any (potential) malware sample should be:

- without executable file extension; during the course we use .vir as extension
- stored in password protected archives in folders without execution rights while on the host system or while being used for transfer

The industry standard for password protected archives is to use the password 'infected' without the quotes. That password makes sure that anyone who extracts samples from the archive is aware that they are handling malware.

Please do the same whenever you provide samples for others too, even if they are analysts. Never transfer malware samples without placing them in such an archive.

If you deal with potential phishing emails, do not directly forward them to anyone. Export the email instead and treat the exported file like any malware sample by putting it into a password protected archive.

Handling URLs

Defang all malware URLs or potential malware URLs. Even if you are using an application where nothing becomes clickable, it might change. For example someone tweeted malware URLs that were not clickable on Twitter but third party applications and forum plugins showed the same tweets with clickable URL.

This is how defang works:

1. replace 'http' with 'hxxp'
2. replace '.' with '(dot)'

This is how it looks like for https://example.com: hxxps://example(dot)com

Do **not** navigate to malware URLs with your browser!

Transferring files between host and guest

Option 1 Download sample repository in guest system

The biggest drawback is that you will need to turn Internet on before transfer and turn it off whenever want to run the sample. If you forget or forgoe this because it is inconvenient, you will infect your network.

For the course you only do this once at the beginning and I will instruct you to turn your Internet off before executing a sample. So during the course it should not be a problem.

Once you are on your own, there will be no one to tell you to turn off the Internet for the guest. Using a shared folder might be the better option if you cannot make this a habit.

Option 2 Shared folder

Use 2 types of shared folders

1. A share that is meant for transfer of analysis results or logs from guest to host. This share is writeable for the guest and not automatically mounted. You only mount it when you need it.
2. A share that is for transferring samples and tools from host to guest. This share is read-only for the guest and can be auto-mounted

Be aware that shares which are writable by the guest will become infected by worms or viruses or become encrypted by ransomware. That is why they must not be auto-mounted.

Do not use writeable shares for permanent storage, only for transfer.

Option 3 USB flash drive

This will infect the USB drive at some point. Make sure you use specifically marked USB flash drives, e.g., put a label on them or use red ones for malware analysis. Make sure that no one in your proximity will plug in these flash drives if you have them lying around.

Any Windows machines that are involved in the transfer must make sure to have viewing unknown file extensions and hidden files view enabled. Most USB infecting malware replaces files on the drive with shortcuts and hides the original files. On non-Windows systems this will be visible either way.

Automatic execution via autorun.inf is not a thing anymore since Windows 7. It can only happen if you use older Windows operating systems in which case keeping it free from malware is impossible.

Optional steps - VPN

We keep the network off when executing malicious samples, so this step should not be strictly necessary. However, in the event that you forget to do that, a VPN will prevent that your Internet provider will cut off your connection. So if you can use a VPN, it is certainly a good idea to do that.