Cleanup Steps

Note: Always assume the client computer is contaminated and infectious, do not attach personal drives etc with the client's device.

Antivirus Scans (Avast)

1. Download Avast free version from here and AirDrop it to the person. This is done in case of a hosts file redirect.

    1. If the previous step fails, do Hosts File Clean Up phase first, then

    2. Download Avast free version from https://www.avast.com/en-us/index#mac

    DO NOT USE USB DRIVES TO TRANSFER FILE

2. Run a scan with Avast and jot down the folders (full path) with any suspicious files that were quarantined

3. **SKIP to next phase if you are not confident!** Go to the outermost suspicious folders recorded in the previous step and compress the folders into zip files. For example, compress SafariHelper if the suspicious file is at `/User/student/Library/Application Support/MacHelper/sscvuaxy/suspiciousFileHere` . Check online if you aren't sure if a folder should be there, don't compress indiscriminately.

4. Delete the suspicious folders but keep the zip files as backup.

Hosts File Clean Up

1. Open terminal (spotlight search terminal)

2. type in `sudo nano /etc/hosts` and hit ENTER

3. Ask the client to enter their password. LOOK AWAY from the keyboard.

4. Delete all the host entries that don't belong. This should be every line unless the client has already customized this file in the past.

5. Press CONTROL+O , then ENTER to save the changes. (Use CONTROL, not COMMAND)

6. Press CONTROL+X to exit back to terminal.

User Crontab Cleanup

1. Use the terminal window from the previous step, or open terminal (spotlight search terminal) if you closed it.
2. Type in `crontab -e`
    1. If it asks you to choose a editor, select `nano`
3. (If it is vim) Press I to start Insert mode
4. Delete all crontabs set that the user didn't create (likely all crontabs)
5. Exit
    1. (if it is vim) Press ESC and then type `:wq` to save changes and exit
    2. (if it is nano) Press CONTROL+O , then ENTER to save the changes. Press CONTROL+X to exit back to terminal.
6. Confirm the application of changes in the popup window.

SUDO Crontab Cleanup

1. Use the terminal window from the previous step, or open terminal (spotlight search terminal) if you closed it.
2. Type in `sudo crontab -e`
    1. If it asks you to choose a editor, select `nano`
3. (If it is vim) Press I to start Insert mode
4. Delete all crontabs set that the user didn't create (likely all crontabs)
5. Exit
    1. (if it is vim) Press ESC and then type `:wq` to save changes and exit
    2. (if it is nano) Press CONTROL+O , then ENTER to save the changes. Press CONTROL+X to exit back to terminal.
6. Confirm the application of changes in the popup window.

LaunchAgent/LaunchDaemon Cleanup

1. Go to terminal again and type in `open ~/Library/LaunchAgents; open /Library/LaunchAgents; open /Library/LaunchDaemons` A series of Finder windows will

appear

2. For each open Finder window from the previous step
    1. Record all the files that have the names of apps the user does not have installed.
    2. Google the above files names and see if there are any reasons it should exist there
    3. If any files shouldn't exist, compress them into a zip file as backup and delete the original file

Browser Cleanup

IMPORTANT: Only do this step is the browser is behaving in unexpected ways, such as popup, mysterious redirects, etc.

1. Check the installed plugins and delete suspicious plugins (not from an official source and not common)

    Instructions for Chrome, Firefox, Microsoft Edge, Safari, Opera: https://www.computerhope.com/issues/ch001411.htm

2. If the previous step fails, reset the browser.

    Instructions for Chrome, Firefox, Microsoft Edge, Safari, Opera: https://www.computerhope.com/issues/ch001748.htm

3. If the previous step fails, backup bookmarks for the client and reinstall the browser.
    1. Backup bookmarks

        Instructions for Chrome, Firefox, Microsoft Edge, Safari, Opera: https://www.computerhope.com/issues/ch000524.htm

    2. Uninstall browser (**REMOVE THE APPLICATION SUPPORT FILES TOO!**)

        Some sites below will recommend you install their "cool app that does it for you." Don't listen to them and use the manual uninstall instructions.

        - Chrome: https://support.google.com/chrome/answer/95319?co=GENIE.Platform%3DDesktop&hl=en#zippy=%2Cmac
        - FireFox: http://kb.mozillazine.org/Uninstalling_Firefox
        - Microsoft Edge: https://www.thewindowsclub.com/uninstall-microsoft-edge-from-mac

    - Safari: There is NO SOLUTION for uninstalling Safari, recommend client to use a different browser in the future or escalate to other senior volunteers.

    - Opera: https://nektony.com/how-to/uninstall-opera-on-mac#delete_opera_manually

3. Re-install browser

4. Import bookmarks from before:

   Instructions for Chrome, Firefox, Microsoft Edge, Safari, Opera: https://www.computerhope.com/issues/ch000524.htm

User Training

Accounts Hygiene

1. Recommend using different passwords for each website.

2. Check password on https://haveibeenpwned.com/Passwords

3. Check email account(s) https://haveibeenpwned.com/

4. Recommend using password generator here: https://preshing.com/20110811/xkcd-password-generator/ Tell the client to write the first word in caps, connect all the words with '-', and add 2 numbers at the end. Use this as new password.

Anti-Phishing / Scams

1. Hover over links to see where they go

2. Legitimate emails from companies will include personally identifiable information, such as your username or name you gave them, in emails to you

3. Scam emails often promise a reward or threaten immediate consequences. Legitimate companies can rarely do this.

4. Common scams can be found on the reddit thread r/scams

5. Porn-related blackmail is almost certainly fake. It is too much work and too little gain for a legitimate attacker to follow through on threats anyways.

6. If they claim that they know your password, check to see if it was already leaked in the past. They might have gotten it that way instead of by "hacking you."
7. Check the URL bar when it asks you to enter the username/password. Verify that is legitimate.

   Common url tricks to mask phishing sites are:

   1. "youtube.com.scamsite.com"
   2. "scamsite.com/youtube/com"

Fileshare / Torrent

Just don't share executable files and/or use torrent for pirated content. Nothing is truly "free". Malware often lays dormant for some time before taking effect to maximize its chances to spread to other people, so a friend having a functioning computer a week after opening a pirated game is not "proof" that it is safe.

Backups

Always make backups regularly. Set up time machine following this tutorial here: https://www.imore.com/how-set-and-start-using-time-machine