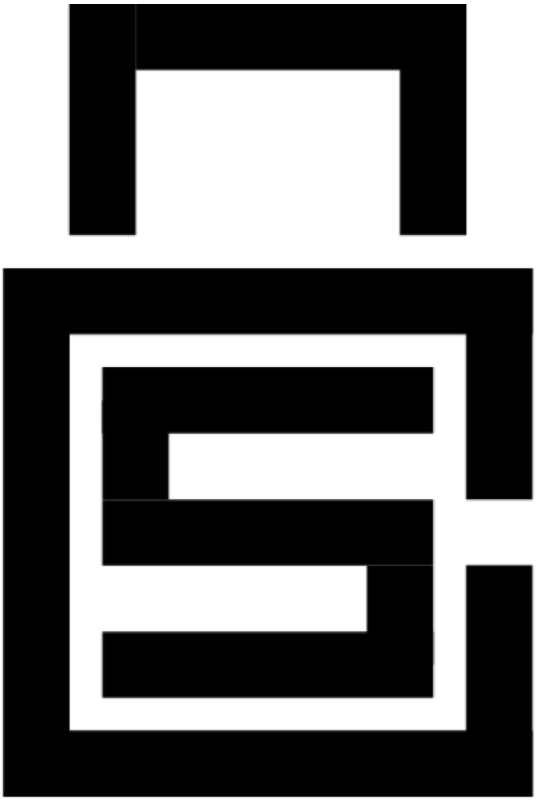


CYBER SAFE

Bilal Abu-Ghazaleh
Senior Project, Computer Science Yale University 2019
Advisor: Stephen Slade

Index

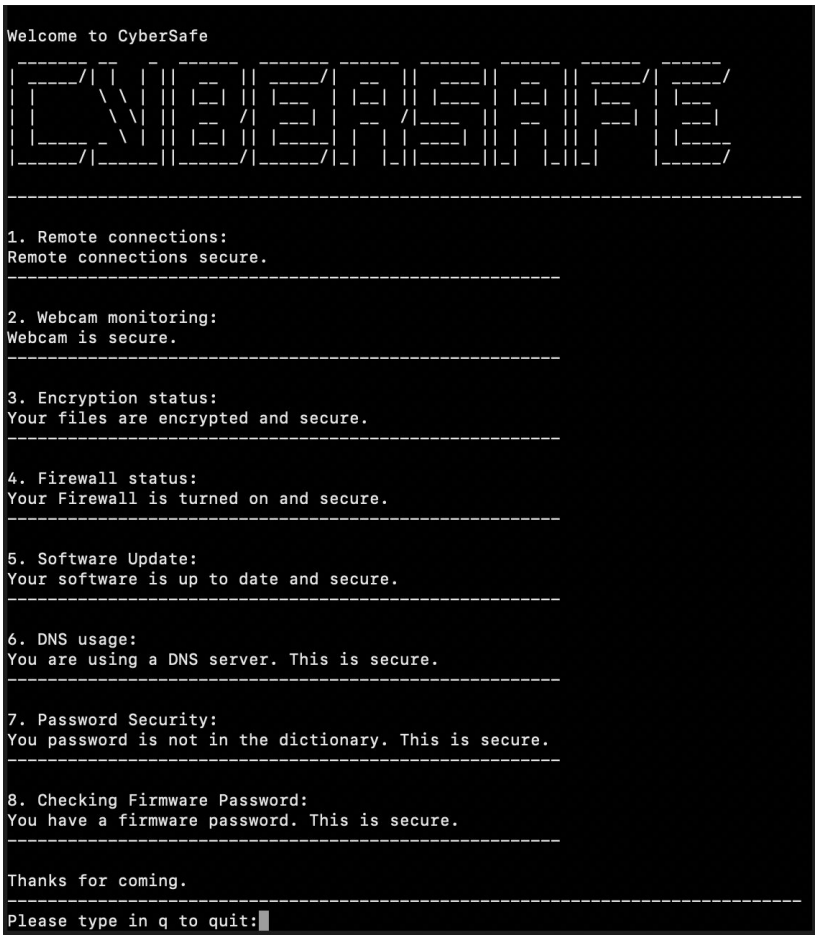
A. The need for cyber-security

Technology and computers exist all around us. We rely heavily on these machines for a variety of tasks ranging from entertainment to sensitive data storage. These devices are necessary for our academic survival in the 21st century. We spend on average about 5 hours a day connected to the internet and many more hours offline on these devices.[1]We use these devices to communicate with friends and family but also with professors and students. A student is expected to check their email at least a few times a day; it is also the norm to check texts and other forms of instant messaging at least once every few waking hours. We store our assignments, our data for our classes but also our personal, private data on the devices that have become ubiquitous.

Cybercrimes are on the rise globally. It is believed that cybercrime cost the world economy as much as $600 billion in 2017 alone.[2]In the past cybercrimes were committed only by experts in the field. Today, any person with internet access can download a set of tools that would allow him/her to gain unauthorized access to a system. Although technology is everywhere, people seem to remain unaware of the dangers and vulnerabilities that it entails. They refuse to update their software to patch a security flaw, passwords are overwhelmingly weak simply because it is a nuisance to take the necessary precautions.

B. What is CyberSafe?

CyberSafe is a computer program design to **evaluate**, **eliminate** and **alert** the user of existing security flaws in their computer. CyberSafe is designed and tailored specifically for Apple OS X computers. This is because it is aimed at educating college students of the vulnerabilities that exist in the system and teach them best cyber-security practices. The program performs a security audit of the computer and returns to the user a human readable, simple set of messages and instructions.



Ideal CyberSafe output with all tests passed.

C. User Guide

1. Got to https://github.com/bilal-abu-ghazaleh/CyberSafe/

2. Click on the green “Clone or Download” button on the top right, then click “Download Zip”.

3. After the file has downloaded, open the folder in finder and double click the file named “CyberSafe”.

4. The program will run.

5. If there are any security flaws, you will be notified and given instructions on how to proceed.

6. Security check number 7 will ask you to type in your password. Please type in the password and verify it is correct, then press enter.

8. A final result will be printed to screen, informing you on the results of the checks and any precautions you should take.

9. After the program has terminated, please follow the instruction on screen (if any) to ensure that your computer remains secure. Remember that unless you meet all eight security conditions, you are not secure.

10. Type in “q” and enter to exit the program.

In case you fail a test:

Below is a list of steps to follow in case you failed any of the above tests:

1. There is a remote connection detected.

If there is a remote connection detected (explained below) you will be prompted to terminate the connection by typing in “yes”. If you do not know what this is, please read the explanation below and type in “yes”. You will be given the IP address of the remote connection.

2. If your webcam is being monitored by an unapproved program, you will be notified and prompted to terminate the program. If you do not recognize the program or do not think it should be able to monitor your webcam, please type in “yes” to terminate.

3. Your files are unencrypted. To encrypt your files do the following:

1. Choose Apple menu () > System Preferences, then click Security & Privacy.
2. Click the FileVault tab.
3. Click Turn On FileVault.

   More details can be found at: https://support.apple.com/en-us/HT204837

4. Your Firewall is turned off. Use these steps to enable the application firewall:

1. Choose System Preferences from the Apple menu.
2. Click Security or Security & Privacy.
3. Click the Firewall tab.
4. Unlock the pane by clicking the lock in the lower- corner and enter the administrator username and password.
5. Click "Turn On Firewall" or "Start" to enable firewall.
6. Click Advanced to customize the firewall configuration.

   More details can be found at: https://support.apple.com/en-us/HT201642

5. Your software is not up to date.

1. Choose System Preferences from the Apple () menu, then click Software Update to check for updates.
2. If any updates are available, click the Update Now button to install them. Or click "More info"to see details about each update and select specific updates to install.
3. When Software Update says that your Mac is up to date, macOS and all of its apps are also up to date. That includes Safari, iTunes, Books, Messages, Mail, Calendar, Photos, and FaceTime.

   More information can be found at: https://support.apple.com/en-us/HT201541

6. You are not using a DNS.

1. Choose System Preferences from the Apple () menu, then click the Network icon.
2. Click the Advanced button near the bottom right corner.And click the DNS tab.
3. Click the + symbol at the bottom to add new ones. Add 8.8.8.8 and then 8.8.4.4. These are the Google servers.
4. Click ok then click apply.

   DNS servers such as google's are important because "they offer phishing protection and stronger security against things like DNS poisoning, spoofing and DDoS attacks." More information can be found at:

   https://www.howtogeek.com/howto/38793/how-to-switch-mac-os-x-to-use-opendns-or-google-dns/ and

   https://lifehacker.com/how-to-make-your-mac-as-secure-as-possible-1829531978

7. Your password is insecure. You should change your password immediately.

You should use a phrase composed of a combination of letters (uppercase and lowercase), numbers and special characters. Common do's and don'ts can be found at https://krebsonsecurity.com/password-dos-and-donts/

8. You do not have a firmware password. This is insecure please do the follwing

1. Start up from macOS Recovery: Press and hold Command (⌘)-R immediately after turning on your Mac, and release the keys when you see the Apple logo or a spinning globe.
2. When the utilities window appears, click Utilities in the menu bar, then choose Firmware Password Utility or Startup Security Utility. This utility is available only on Mac models that support use of a firmware password.
3. Click Turn On Firmware Password.
4. Enter a firmware password in the fields provided, then click Set Password. *Remember this password*.
5. Quit the utility, then choose Apple () menu > Restart.

   More information can be found at: https://support.apple.com/en-us/HT204455

If you fail either test 1 or test 2, it is highly recommended that you talk with your system administrator or consult a security expert. These are serious security concern.

D. CyberSafe checks

1. It checks for remote connections:

That is, the program checks whether any person or software is connected to the user's computer remotely (either using SSH, remote sharing or any other remote connection). The remote connection could potentially allow a malicious user to perform any action the computer owner could. Remote connections such as these would allow a malicious user to access data, passwords (both online and offline) as well as create, delete or modify any existing files and much more. The user has the option of terminating the connection by typing "y".

Technical details: This is first done by identifying the current user's UID. It then runs the bash command "who" to check any active connection, remote or local. It then cross lists the connections with the UID and verifies that they are all legal, local connections. If a remote connection (of any type) is detected, the user is alerted of the IP address origin and given the option to terminate the connection. The connection is terminated using the "kill" command and the PID of the connection.

2. It checks camera monitoring:

This checks all programs currently accessing the computer's camera. It then cross references these programs with a list of allowed programs. If a program is found to be accessing the camera and is not on the list of approved programs, the user is immediately alerted (with the name of the program) and given the option to terminate it. If a malicious program is monitoring

and/or recording a user's camera, this is a serious breach of security and privacy. This check is therefore essential.

Technical details: the bash command ""lsof | grep -e \"VDC\" -e \"AppleCamera\" -e \"iSight\"" is run. Lsof list all processes currently running on the computer. Grep then searches for VDC, AppleCamera and iSight, thereby making the check compatible with all operating systems created in the last 10 years. It then cross lists all the programs currently accessing the camera with the legal programs. It then terminates the unauthorized processes using the "kill" command and PID of all illegal programs, after alerting the user.

3. Encryption check:

The program checks whether encrypting is enabled on the user's computer and alerts them of the result. If the computer is not encrypted, the user is presented with a set of detailed instructions and a link on how to enable FileVault- Apple's built in encryption software.

Technical details: the program uses the bash command "fdesetup status" to check the status of the encryption. If it is on, the user is praised. If it is turned off, a user gets a set of instructions that they are recommended to follow.

4. Firewall check:

The program checks whether firewall is enabled on the user's computer and alerts them of the result. If the Firewall is not turned on, the user is presented with a set of detailed instructions and a link on how to enable Apple's built in Firewall software.

Technical details: in a similar manner to encryption, the program uses the bash command defaults read "/Library/Preferences/com.apple.alf globalstate" to check the status of the Firewall. If it is on, the user is praised. If it is turned off, a user gets a set of instructions that they are recommended to follow.

5. Software update check:

The program check whether the computer software is up to date. New security flaws are discovered on a daily basis and patches for these flaws appear in the security updates. It is therefore good practice to update the software whenever a new version is available. If the software is up to date, the user is praised. If it is not, the user is presented with a set of instructions and a link explaining how to update the software.

Technical details: the bash command "softwareupdate -l" is run and the program checks if an update is needed by using the command "grep -Eo 'Software Update found the following new or updated" on the output of the previous command.

6. DNS check:

The program check whether a DNS server is in use. DNS servers such as google's are important because they offer phishing protection and stronger security against things like DNS poisoning, spoofing and DDoS attacks. It is therefore good practice to use a DNS server. If a DNS server is in use, the user is praised. If it is not, the user is presented with a set of instructions and a link explaining how to set one up.

Technical details: the bash command “networksetup -getdnsservers Wi-Fi” is run and the program checks if a DNS is in use.

7. Password security:

The program will prompt the user for their password, it will then cross check that password with a dictionary of about 45,000 words and check whether the password is in the dictionary. A dictionary attack (testing the password by using every word in the dictionary) is one of the most commons attacks. If the password is not, the user is praised, otherwise, it is recommended that the user change their password.

Technical details: the program opens the dictionary file and compares the lower case of the password to the lower case of each word in the dictionary, if no result is found then password is secure.

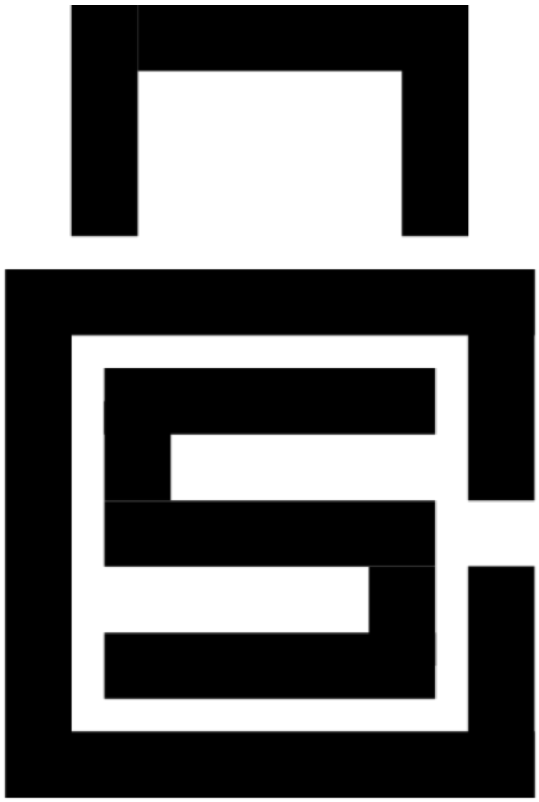
8. Firmware password:

The program will check whether firmware password on the computer is enabled. Firmware password is important as it would prevent an unwanted attacker from accessing the single user mode and gaining root access. It also prevents a malicious actor from using the recovery mode, thereby disabling the threat.

Technical details: the bash command “sudo -S firmwarepasswd -check” is used to check whether a firmware password is enabled. The “sudo” command, giving root privilege is necessary in this case otherwise the command will not run. The password presented by the user in test 7, is piped into the command so as not to have to ask the user for the password again.

E. Acknowledgments

I would like to thank Professor Stephen Slade for his guidance and all his help with this project. I would also like to thank Dan Gorodezky for his assistance in the design of the CyberSafe logo. I would like to extend my gratitude for the people who agreed to run my program and shared their results with me. Finally, I would like to thank my friends and family for their support throughout the process.



CYBER SAFE