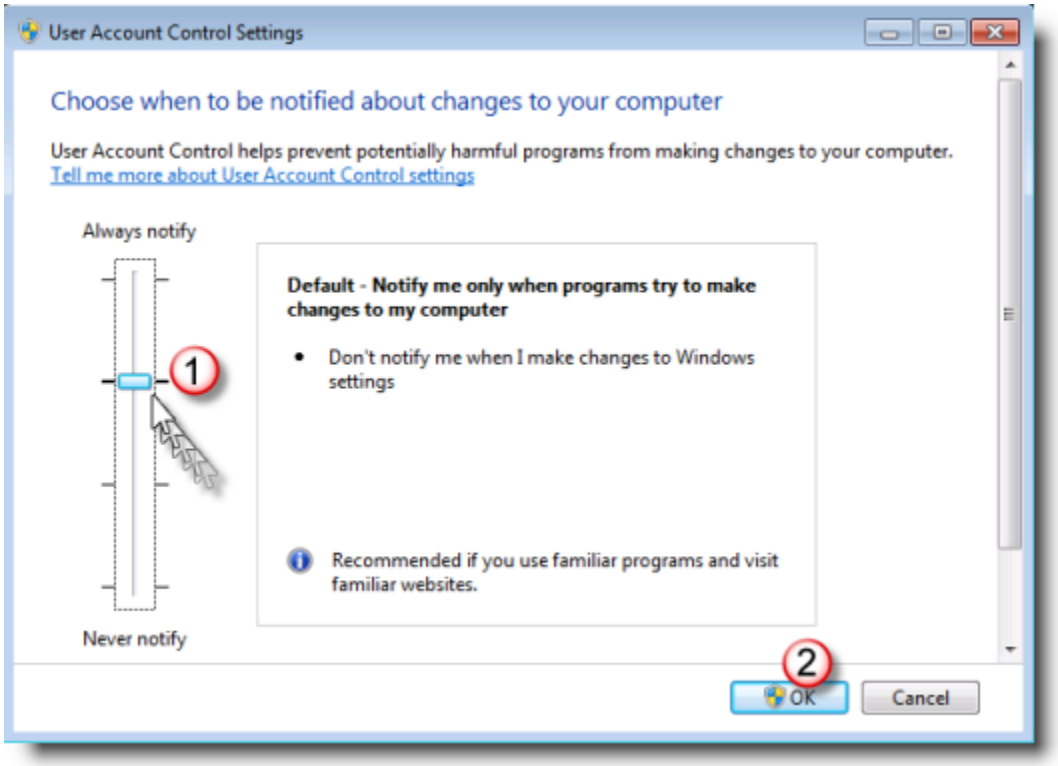
Steps to Improve Cybersecurity for Common Devices

Windows Laptops/Desktops

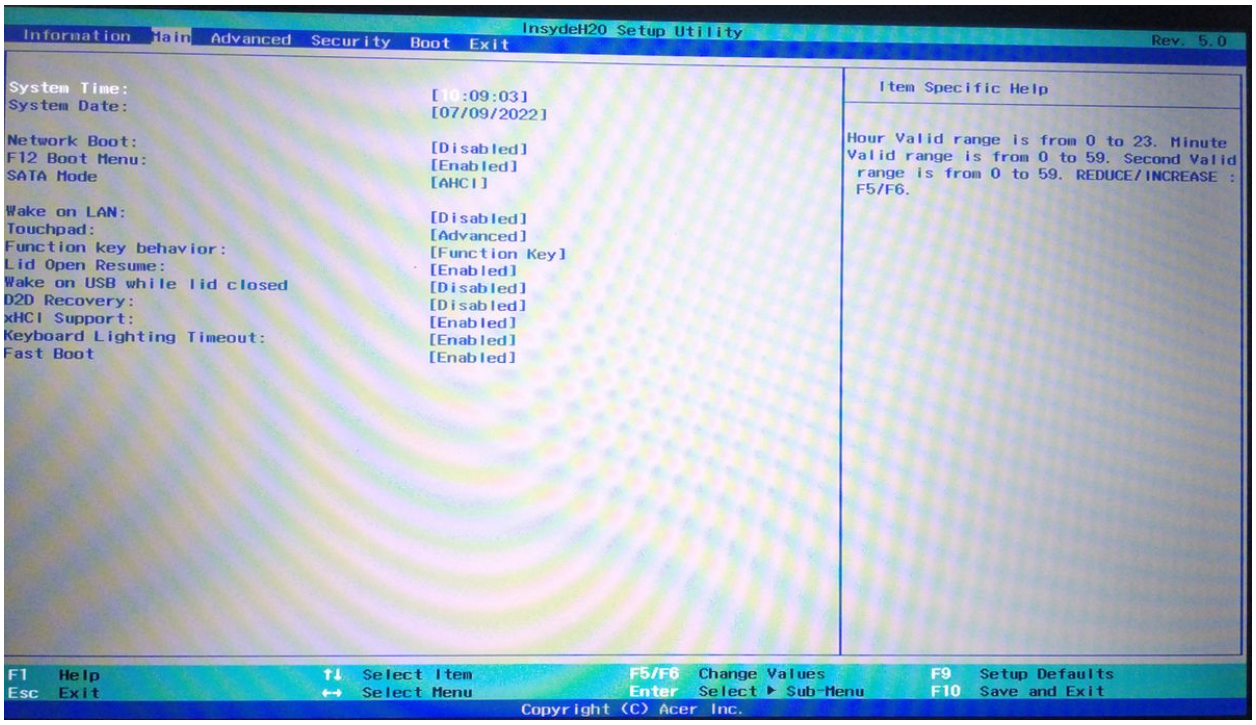
1. Configure UAC (User Account Controls) this will make all programs downloading, installing, and updating ask for normal user, or administrator permissions. Here is how to raise UAC if it is not preconfigured or set to default values.

To start, hit the Windows Key + R to open the run box. Then type into the box, Control Panel, and hit OK. Select “User Accounts” and then select “User Accounts (Classic View)” Select “Change User Account Settings” If you are prompted, select yes to continue.



Move the Slider all the way up to always notify. Then just hit OK to save and exit.

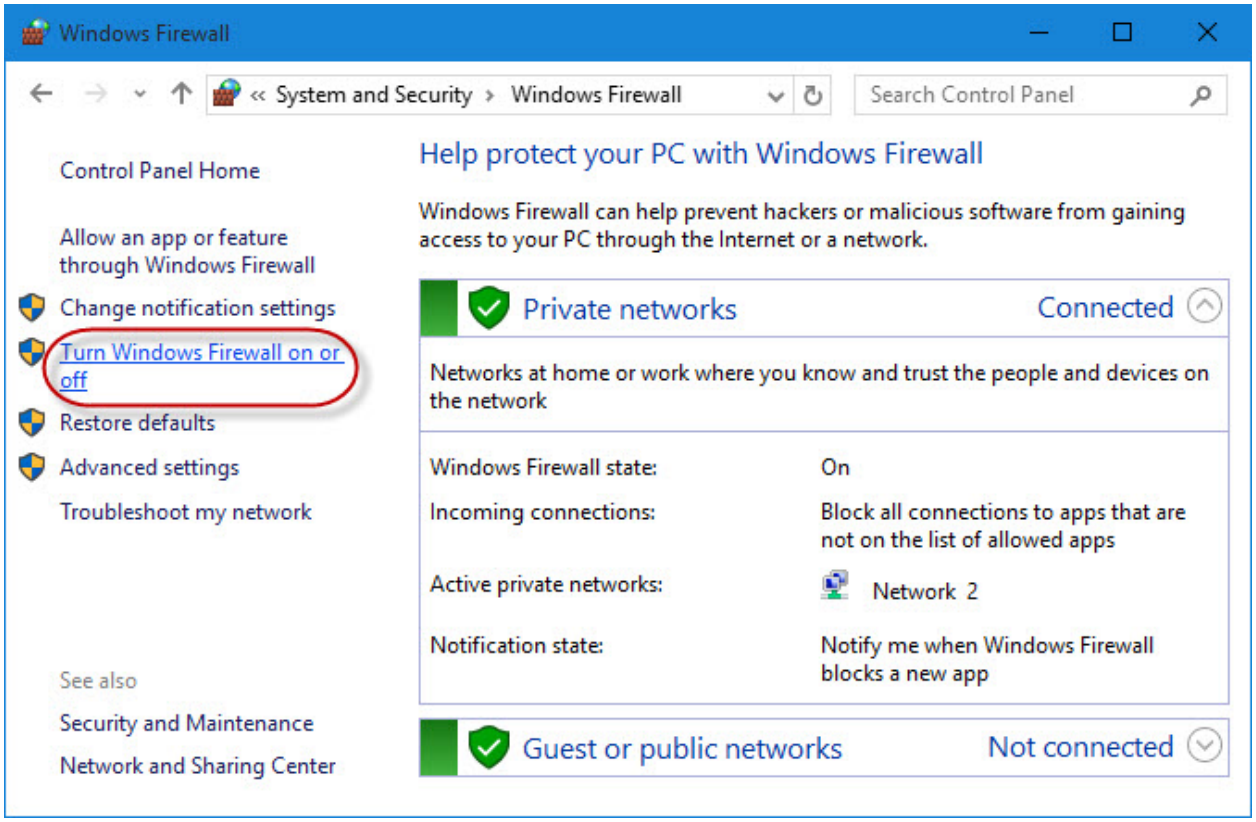
2. Set BIOS ADMIN Password. To start, shutdown your computer. On boot hit F2 + Delete or just F1 repeatedly to enter the BIOS menu. You should see the following screen or something similar.



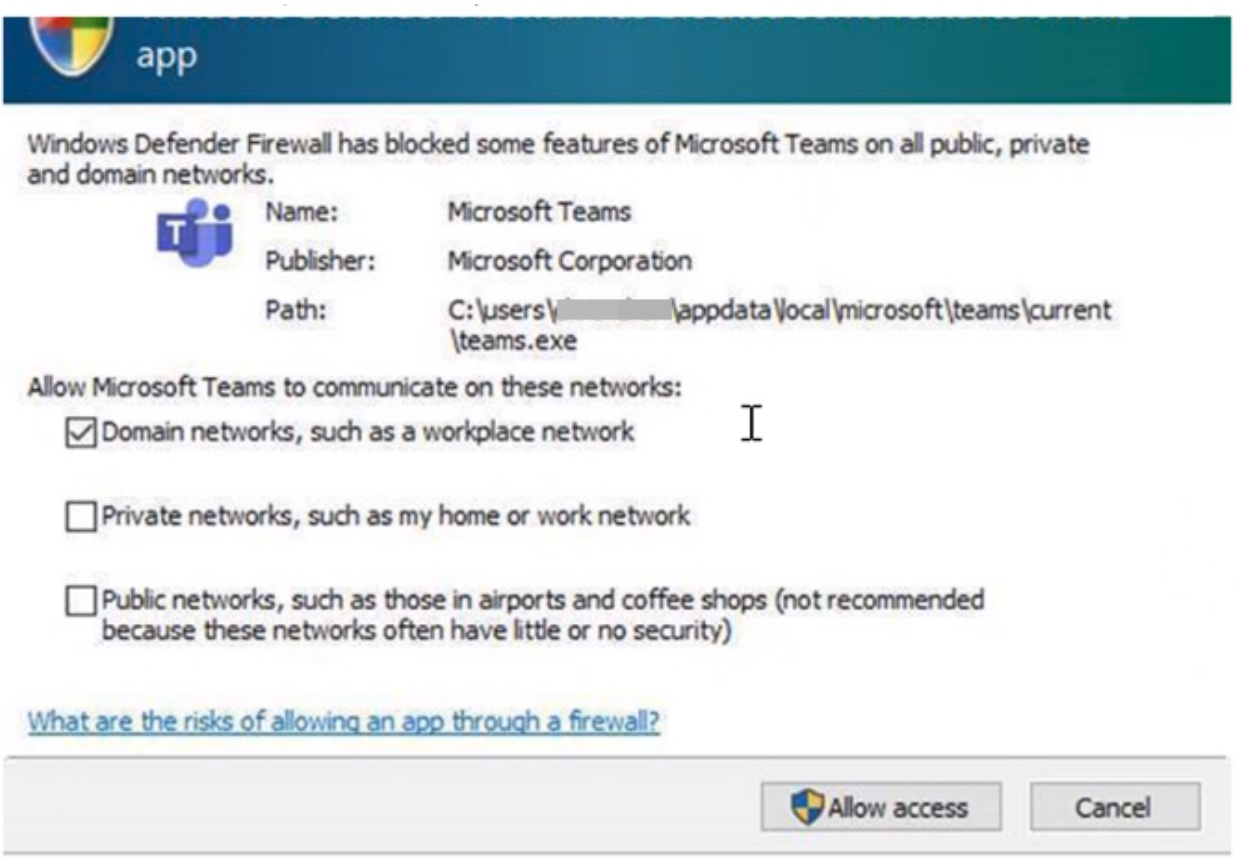
You should then find an option that says “Set Administrator Password” (Navigate through the menu with the right and left arrow keys, and up and down keys) and hit enter. Then enter and confirm the password.

3. Change Secure Boot. If you are still the BIOS go to the Boot or Advanced tab. You should see something like “BIOS mode” if it is on legacy, change it to UFEI. Also look for an area called boot order disable USB booting and network booting. You should then go to the exit tab, and hit save and exit.

4. Configure and Optimize Windows Firewall. Go to your control panel and select “System and Security” navigate to “Windows Defender” and click on “Firewall.” Choose turn Windows Firewall on or off, and turn it on for domain private and public network settings.



When you install or run an application for the first time, you should now see something like this,



Only allow programs with sensitive information to run on “Domain” and “Private” Networks. If you want more information about Windows Firewall, here are some sites that will further elaborate.

[Microsoft - Windows Defender Firewall]
[How to Optimize Windows Firewall Security]

5. Disable Built in Admin Account: To disable built in admin account open powershell as normal user (admin if the following command does not work) and paste:

```
Unset
net user administrator /active:no
```

The account should then be disabled. For more info, visit the page below.

[Microsoft- Disable Admin Account]

6. Change Default SSH Password. This is very important so someone cannot just SSH onto your laptop and run malicious software without your permission. To change the ssh

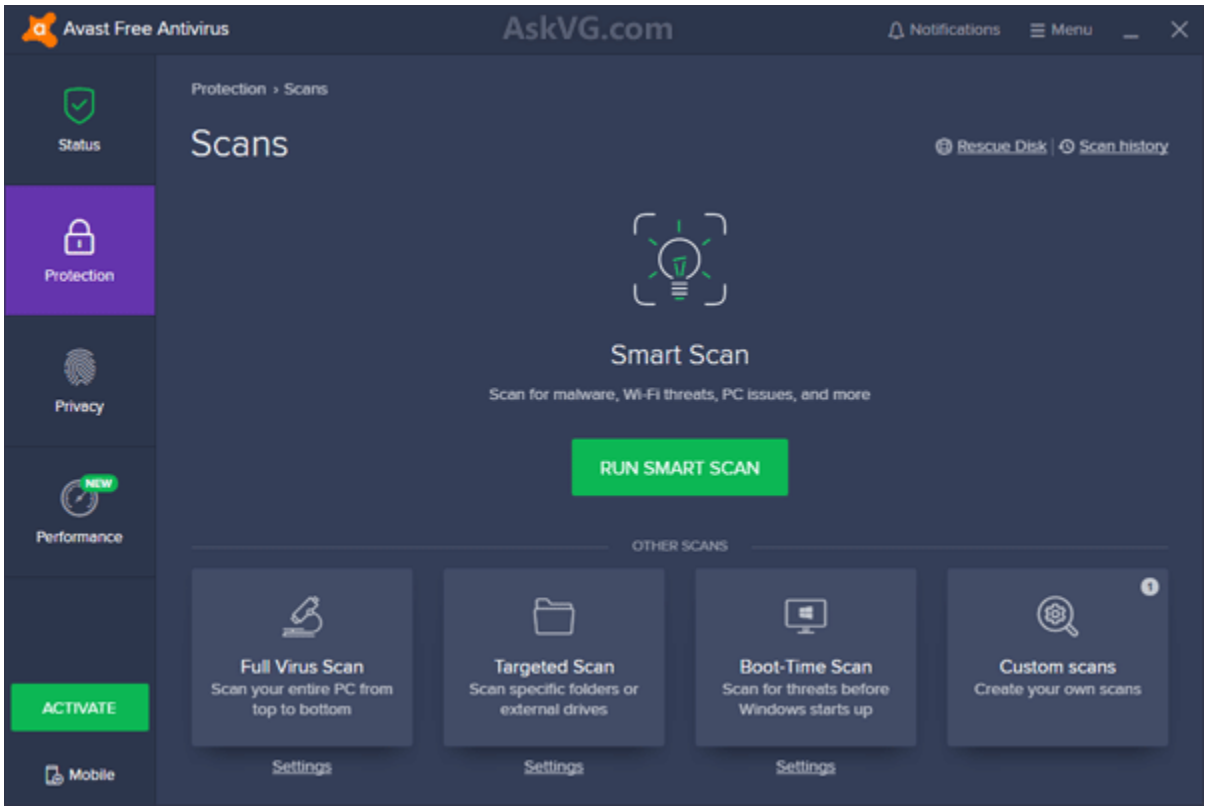
password do the following. Login as powershell for both your user account and input the following command.

```
Unset
net user [username or Administrator] [new password]
```

If you want to learn more about SSH and how to use it, please see this website

[Microsoft -Configure SSH]

7. Install or 3rd Party Antivirus. Windows Defender is good for basic tasks, however a 3rd party antivirus, like Avast Free is a better option for detection and securing your system. To install avast, goto https://www.avast.com/index#pc and download the setup.exe file. Run the setup files and go through the steps.



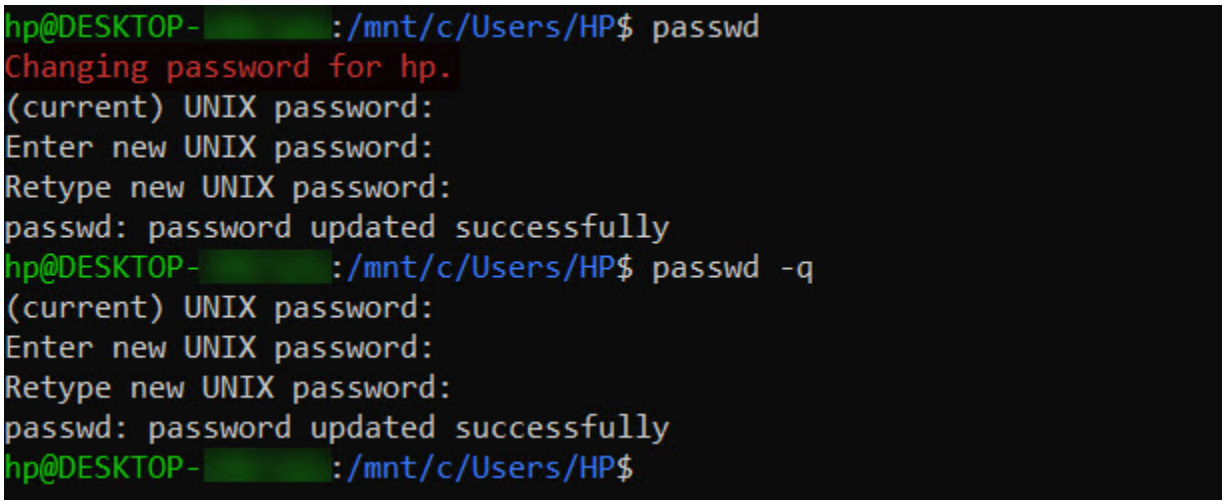
When it is done, you should see a screen somewhat like this. After installing, you should run a full scan and clean your PC.

ChromeOS and Linux Machines

1. Change Root and Normal User Password. Open the terminal as the normal user, and type

```
Unset
passwd
```

You should see something like this



Enter your old or system default password (look for your distros default) and change it. When you are done with your user account, type the following.

```
Unset
sudo -i
```

And enter your password. You are now in the Root (superuser) account. Go through the same steps to change your password as before, and exit.

2. Installing and configuring UFW (Uncomplicated Firewall.)

*Note setting up this firewall might break some applications, and you may have to write custom rules for each program. If you do not want to do this, just skip this part of the tutorial.

To start, you should login as root through the `SU` or `Sudo -i` just as before. Now we are going to update your system. To do so, enter the following:

```
Unset
Sudo apt-get update -y
```

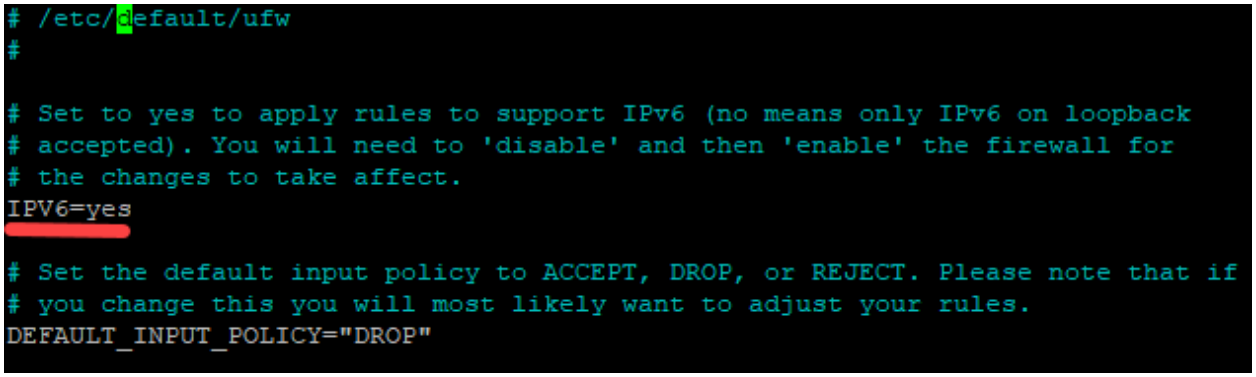
Through the update process, it might prompt you to do something. Always say yes or just input the default values. Next we are going to install UFW. Type the following.

```
Unset
sudo apt install ufw -y
```

After the install you can use nano or vim to edit the config file. Type

```
Unset
sudo nano /etc/default/ufw/
```

To enter the config file. You should then see something like this



Now I know that it looks overwhelming, but stay with me. Arrow down to the IPV6 and change the Value to yes. Then hit ctrl + x the system will prompt you if you want to save. Hit the y key and then the enter key to save and exit nano. Then type:

```
Unset
sudo ufw disable && sudo ufw enable
```

Then type

```
Unset
sudo ufw default deny incoming
```

And

```
Unset
sudo ufw default deny outgoing
```

Your system is now blocking all incoming and outgoing connections. To enable browsing and internet use type

```
Unset
sudo ufw allow out to any port 80
sudo ufw allow out to any port 443
sudo ufw allow out to any port 53
sudo ufw reload
sudo ufw status verbose
```

If this does not work consult your programs and distro for more help and information.

3. Uninstall out of date file sharing and networking tools.

*Note some users may have programs that rely on or need to use these tools. If so you can skip this part of the tutorial

A Lot of tools like FTP, Telnet, and SH are now obsolete and vulnerable to man in the middle attacks and packet sniffing. Especially on linux systems, it is important to remove these programs if they are installed. Todo so, input the following in your terminal.

```
Unset
sudo apt-get --purge remove xinetd nis yp-tools tftpd
atftpd tftpd-hpa telnetd rsh-server rsh-redone-server
```

4. Setting up Fail2bAN. Fail2Ban is a tool designed to stop tools like xhydra brute forcing ssh passwords. Fail2Ban if a password is wrong too many times, blocks the IP. To install and setup type the following in your terminal.

```
Unset
sudo apt-get install fail2ban
*then you need to edit the config file
```

```
sudo vim /etc/fail2ban/jail.conf/
sudo systemctl restart fail2ban.service
```

Fail2ban is now installed and configured.

5. Install Lynis. Lynis is a system hardening tool and vulnerability scanner. It will check your system for updates, vulnerable packages, and additional ways to secure your system. To install Lynis open the terminal and type the following.

```
Unset
git clone https://github.com/CISOfy/lynis
cd lynis && ./lynis audit system
```

After this Lynis will install and run on your system. If you want to further secure your system, or want extra tools. Go to the site below.

[40 ways to secure your linux system]

|Thank you for using this guide to secure windows and |
|Linux. If you want our mac tutorial please wait until |
|Next week! |
| |
|-CKjones |
