As a user with access to sensitive government information at work, you are at risk at home. In order to gain access to information typically housed on protected work networks, cyber adversaries may target you while you are operating on your less secure home network.

Don't be a victim. You can help protect yourself, your family, and the Command by following these **3 easy steps** to secure your home network.

STEP 1: DOWNLOAD ANTI-VIRUS AND KEEP UPDATED

If your computer does not have an antivirus program installed and running, we highly recommend you install one today. **See the JSOC: Installing DoD Provided Home Internet Security Software.** Follow the steps below for help on how to install and update an antivirus program on your computer.

1. If you purchased the antivirus program from a retail store, insert the CD or DVD into the computer's disc drive. The installation process should start automatically, with a window opening to help guide you through the install process.

2. If you downloaded the antivirus program on the Internet, find the downloaded file on your computer. If the downloaded file is a zip file, unzip the file to extract and access the installation files. Look for a file named setup.exe, install.exe, or something similar, then double-click that file. The installation process should start, with a window opening to help guide you through the install process.

3. In the installation process window, follow the steps provided to install the antivirus program. The install process provides recommended options so the antivirus program will function properly, which in most cases can be accepted as is. The one exception is if the install process recommends that you also install any toolbars for Internet browsers or other helpful programs for your computer. If prompted to install other software along with the antivirus program, uncheck all boxes or decline the install of those extra programs. No additional programs should be needed for the antivirus program to install and run successfully on your computer.

4. When the install process is complete, close out of the install window.

5. If used, remove the CD or DVD from the computer's disc drive. The antivirus program is now installed and ready to use. While it may not be required, recommend that you restart your computer so that any modified settings in the operating system can take effect correctly.

After being installed, you may also receive a prompt to update the antivirus program. It is highly recommended that you update it, even if you do not receive a prompt to do so. Proceed to the next section below for help on how to update the antivirus program.

Update the antivirus program after installation
Out of the box, antivirus programs are not up-to-date and are missing the latest virus and spyware definitions. Without the latest definitions, the antivirus program will not know about the most recently created viruses and spyware, making your computer vulnerable to an infection.

After installing the antivirus program, we highly recommend that you update it with the latest virus and spyware definitions. The updates will allow the antivirus program to protect your computer from all viruses and spyware.
In many cases, the antivirus program will automatically ask if you want to check for and install the latest updates. If prompted to do so, select yes to update the antivirus program. If it does not prompt you to update immediately, see our page on how to update your antivirus program.

Enable automatic updates for the antivirus program By default, most antivirus programs enable the automatic update feature. It is strongly recommended that automatic updates be enabled so that your antivirus program stays up-to-date at all times.
To check if automatic updates are enabled in your antivirus program, follow the general steps below.

1. Open the antivirus program.

2. Look for a **Settings** or **Advanced Settings** button or link in the antivirus program window. If you do not see either option, look for an option like **Updates** or something similar.

3. In the Settings or Updates window, look for an option like **automatically download and apply updates**. It may also refer to virus definitions instead of updates.

4. For the automatic updates option, check the box for that option, if not already checked.

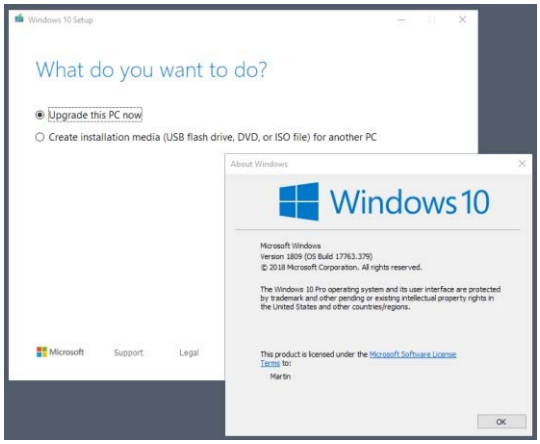
5. Click the **Save** or **Apply** button to save the settings change.

STEP 2: UPDATE IE "PATCH" YOUR OPERATING SYSTEM (WINDOWS/MAC)

To update your Windows 7, 8, 8.1, and 10 Operating System:

1. Open Windows Update by clicking the Start button in the lower left corner. In the search box, type Update, and then, in the list of results, click either Windows Update or Check for updates.

2. Click the Check for updates button and then wait while Windows looks for the latest updates for your computer.



3. If you see a message telling you that important updates are available, or telling you to review important updates, click the message to view and select the important updates to install.

4. In the list, click the important updates for more information. Select the check boxes for any updates that you want to install, and then click OK.

5. Click Install updates.

ǂ

2. If any

Note: It is important that you do not shut your computer off or allow it to run out of battery during the update process. Doing so can cause a corruption of the operating system, which can often only be fixed by reformatting the computer.

To update your Macintosh Operation System:

If you've upgraded to macOS Mojave or later, follow these steps to keep it up to date:

1. Choose System Preferences from the Apple menu, then click Software Update to check for updates.
updates are available, click the Update Now button to install them. Or click ”More info” to see details about each update and select specific

ǂ

updates to install.

3. When Software Update says that your Mac is up to date, the installed version of macOS and all of its apps are also up to date. That includes Safari, iTunes, Books, Messages, Mail, Calendar, Photos, and FaceTime.

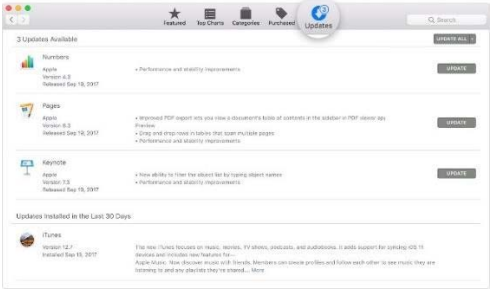
To find updates for iMovie, Garageband, Pages, Numbers, Keynote, and other apps that were downloaded separately from the App Store, open the App Store on your Mac, then click the Updates tab.

To automatically install macOS updates in the future, including apps that were downloaded separately from the App Store, select ”Automatically keep my Mac up to date.” Your Mac will notify you when updates require it to restart, so you can always choose to install those later.

If you're using an earlier macOS, follow these steps to keep it up to date:

1. Open the App Store app on your Mac.

2. Click Updates in the App Store toolbar.



3. Use the Update buttons to download and install any updates listed.

4. When the App Store shows no more updates, the installed version of macOS and all of its apps are up to date. That includes Safari, iTunes, iBooks, Messages, Mail, Calendar, Photos, and FaceTime. Later versions may be available by upgrading your macOS.

To automatically download updates in the future, choose Apple menu > System Preferences, click App Store, then select ”download newly available updates in the background.” Your Mac will notify you when updates are ready to install.

STEP 3: CREATE PASSWORDS AND LIMIT THE USE OF THE ADMINISTRATOR ACCOUNT

Although a log-in password won’t protect against a competent hacker, it can be enough to dissuade unsophisticated criminals from snooping through your personal files and accessing your online accounts.

Protecting each account (Guest, Admin, and User) with different passwords helps prevent a hacker from getting access to everything on your computer should they gain access to any one account. It is recommended you create and use a "User" account, not the "Admin" account for all daily activity. This way hackers would be limited in the damage they can do to your computer.

Windows 10 offers a number of enhanced log-in and security features.

Navigate to Start Button > Settings > Sign-in Options to setup your

‘Sign-in Options.

In your operating system, the highly-privileged administrator (or root) account has the ability to access any information and change any configuration on your system. Therefore, web or email delivered malware can more effectively compromise your system if executed while you are logged on as an administrator. Create a non-privileged “user” account for the bulk of your activities including web browsing, email access, and document creation/editing. Only use the privileged administrator account for system reconfigurations and software installations/updates.

Practical Password Tips

If you have files on your computer that you don't want anyone else to access, you can use password-protected file or folder encryption to keep them safe. However, encrypted files are only as secure as the strength of the password protecting them.

For this and the rest of your security measures to be maximally effective, make sure you follow these simple password rules:

- Use a password that’s at least 12 characters long and includes a mix of lower and upper case letters, symbols, and numbers.
- Try not to use complete words, but if necessary avoid common words that can be found in a dictionary. Not all devices, systems, or accounts allow these combinations, but do what you can within the available options.
- Avoid sharing passwords across multiple platforms, especially for sensitive accounts like a Windows logon, bank account, and email account.
- Change your passwords frequently. Every 6 months for important passwords, at a minimum.

#