

Software Security Update

The purpose of this guidelines is to train Workforce on How to Identify and Report if Their Enterprise Assets are Missing Security Updates

You may have noticed that a lot of K-12 institutions, colleges and hospitals have had news coverage that they were victimized by cyber criminals.

Besides increasing our user awareness on how to identify phishing emails, another way we can contribute to cyber safety at SDCOE is to keep our computer and applications updated to ensure they are protected against vulnerabilities.

When a software is purchased, it is not automatically and forever safe to use. Often the software has unknown vulnerabilities that are waiting for cyber criminals and researchers to discover. Once these vulnerabilities are reported or exploited the software manufacturer will develop and release an update to ensure that the vulnerability may no longer be taken advantage of.

To stay protected we must constantly update our computer's operating system, web browsers and other applications or they will just be sitting exposed waiting for someone to notice and take advantage of vulnerabilities.

SDCOE recommends that we run the various update utilities on our computer once a month. It is best to start some of the updates before we take a break for lunch or leave for the day.

Here are the four major rules regarding updates:

Update often.

Always keep your software updated when updates become available and don't delay. These updates fix general software problems and provide new security patches where criminals might get in. You can be sure the bad guys are always looking for new ways to get to your data through software, so updating your software is an easy way to stay a step ahead.

Get it from the source.

When downloading a software update, only get it from the company that created it. Never use a hacked, pirated, or unlicensed version of software (even if your friend gave it to you). These often contain malware and cause more problems than they solve.

Make it automatic.

Software from legitimate companies usually provides an option to update your software automatically. When there's an update available, it gives a reminder so you can easily start the

process. If you can't automatically update it, remind yourself to check quarterly if an update is available.

Watch for fakes!

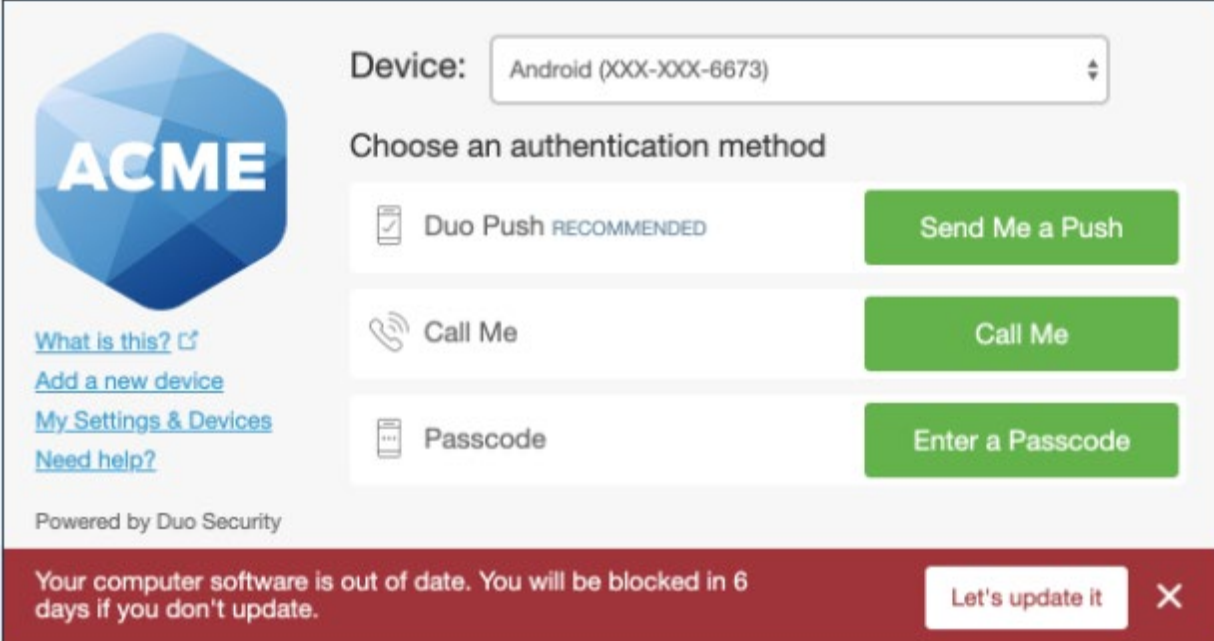
Maybe you've seen these pop-up windows when visiting a website or opening software that urgently asks you to download something or fill out a form? These are always fake and should not be followed. A browser will only warn you not to move forward or stay on a specific web address because it might not be secured, or it could contain malware

Let's go over some of the communications you may see.

Your computer may give you a notice (bottom right for Windows) (top right for Mac) unless told otherwise it is safe to perform these updates.

When you open your web browser you may see a thin banner notifying you to restart the web browser to apply newly applied updates, this is also safe.

When you log in using MFA, you may notice a message on your Duo screen recommending that you update, this is safe to click on and will lead you to a page with instructions.



ACME

Device: Android (XXX-XXX-6673)

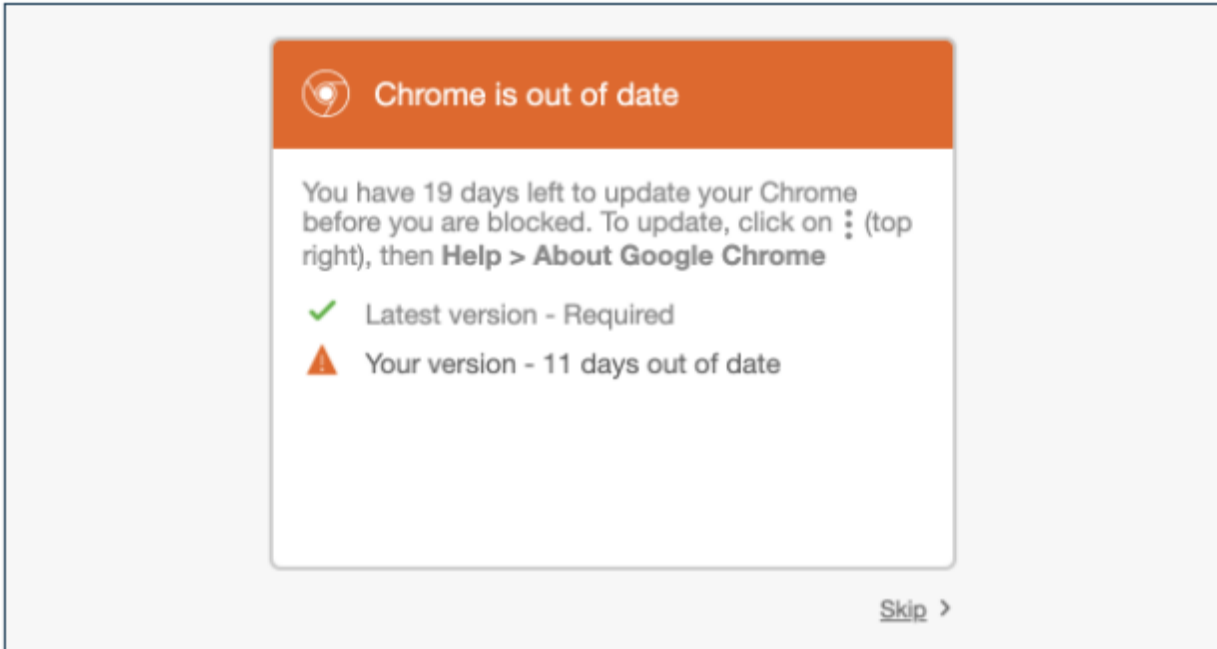
Choose an authentication method

- Duo Push RECOMMENDED [Send Me a Push](#)
- Call Me [Call Me](#)
- Passcode [Enter a Passcode](#)

[What is this?](#) [Add a new device](#) [My Settings & Devices](#) [Need help?](#)

Powered by Duo Security

Your computer software is out of date. You will be blocked in 6 days if you don't update. [Let's update it](#) ✕

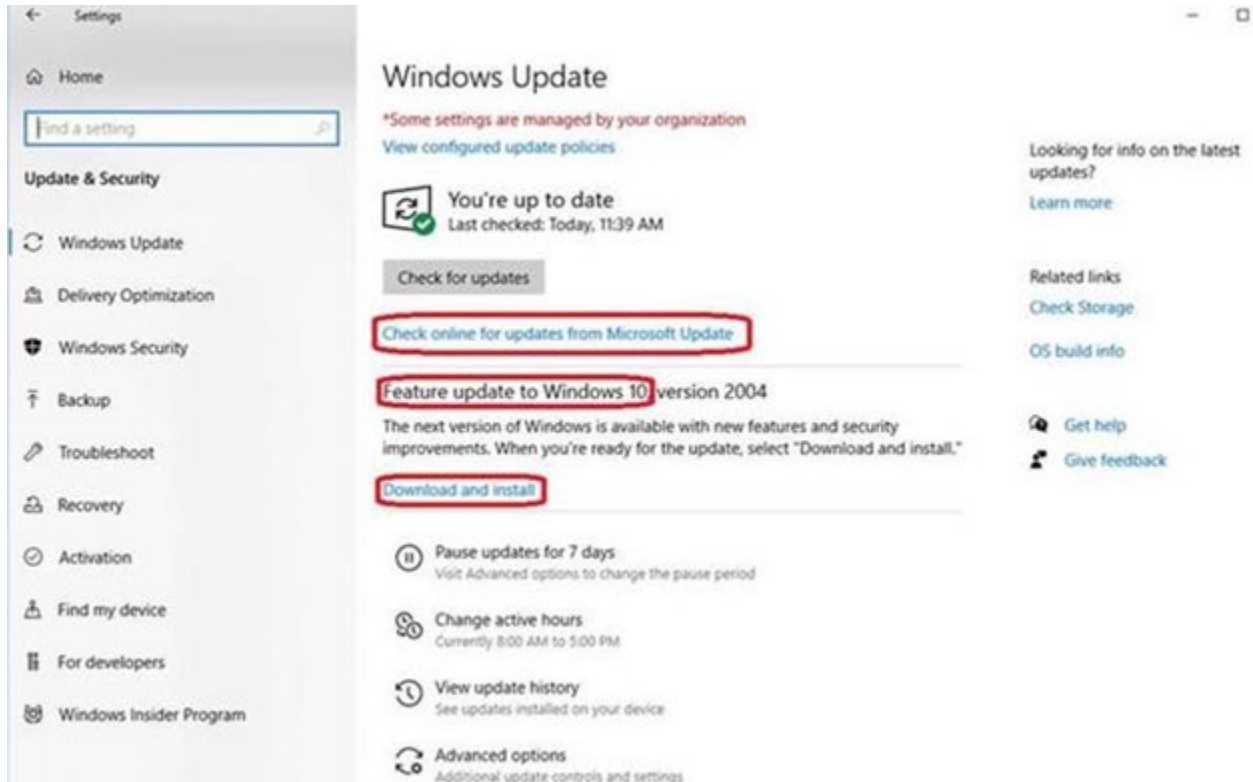


You may also receive emails from securinginfo@sdcoe.net and other ITS personnel, please attend to the email as soon as possible.

While web browsing you may see a pop-up window alerting you that your computer is infected or that you need a free update. These are bogus and are often found on sites with heavy advertising. It is best to not click on any of these buttons and to just close the window. If you hover over top right corner of Window, you should see a subdued X, click on that to close window or right click on the app's icon in toolbar and select Close Window or Close All Windows.

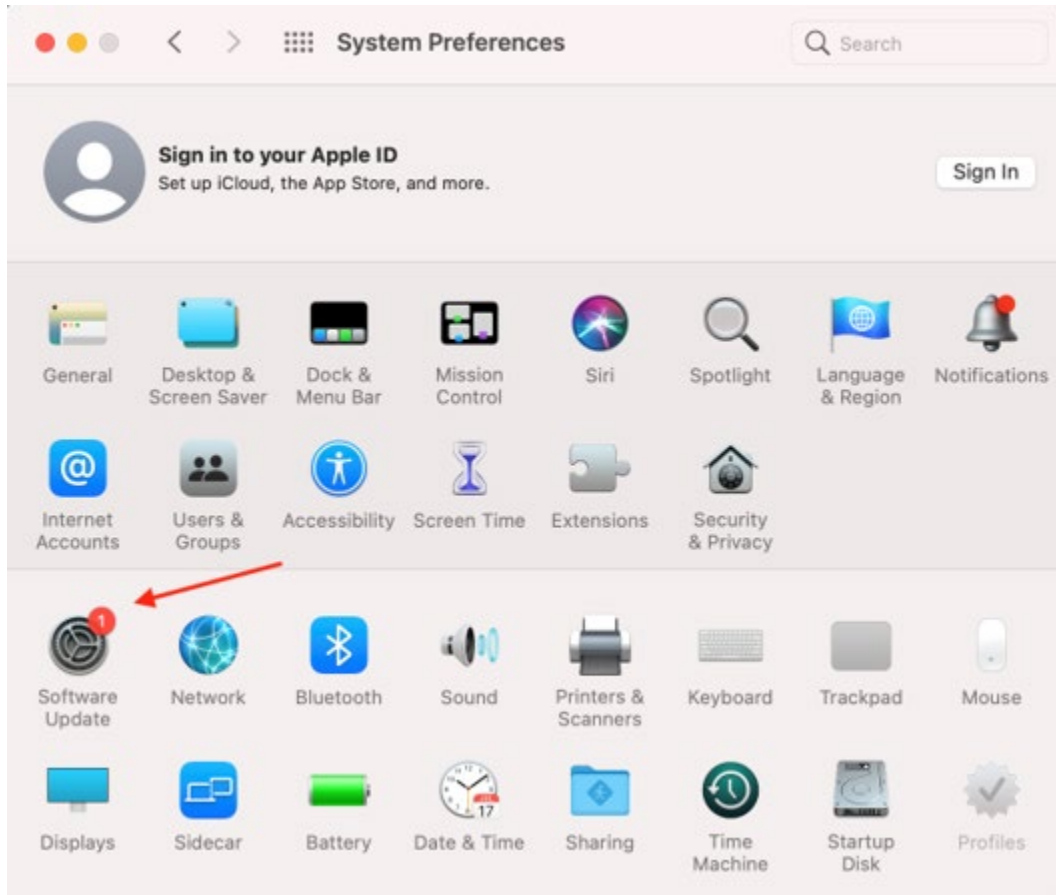
If you get an email from an unknown source asking you to click a link or download an update file these are bogus. If in doubt forward the email to securinginfo@sdcoe.net

To Update the Windows operating system, go to the Start Menu or search bar in bottom right and type in "Check for updates" Once the Windows Update page opens check to see if it is asking you to restart to apply updates, if there is no message click on Check for updates button. It may take a few minutes for it to scan for updates, download them and install them. While this is happening feel free to minimize the window and work on something else. Once it is done scanning, you may see a message asking you if you want to apply the latest Feature Update, click on "Download and install" to apply the Feature Update.

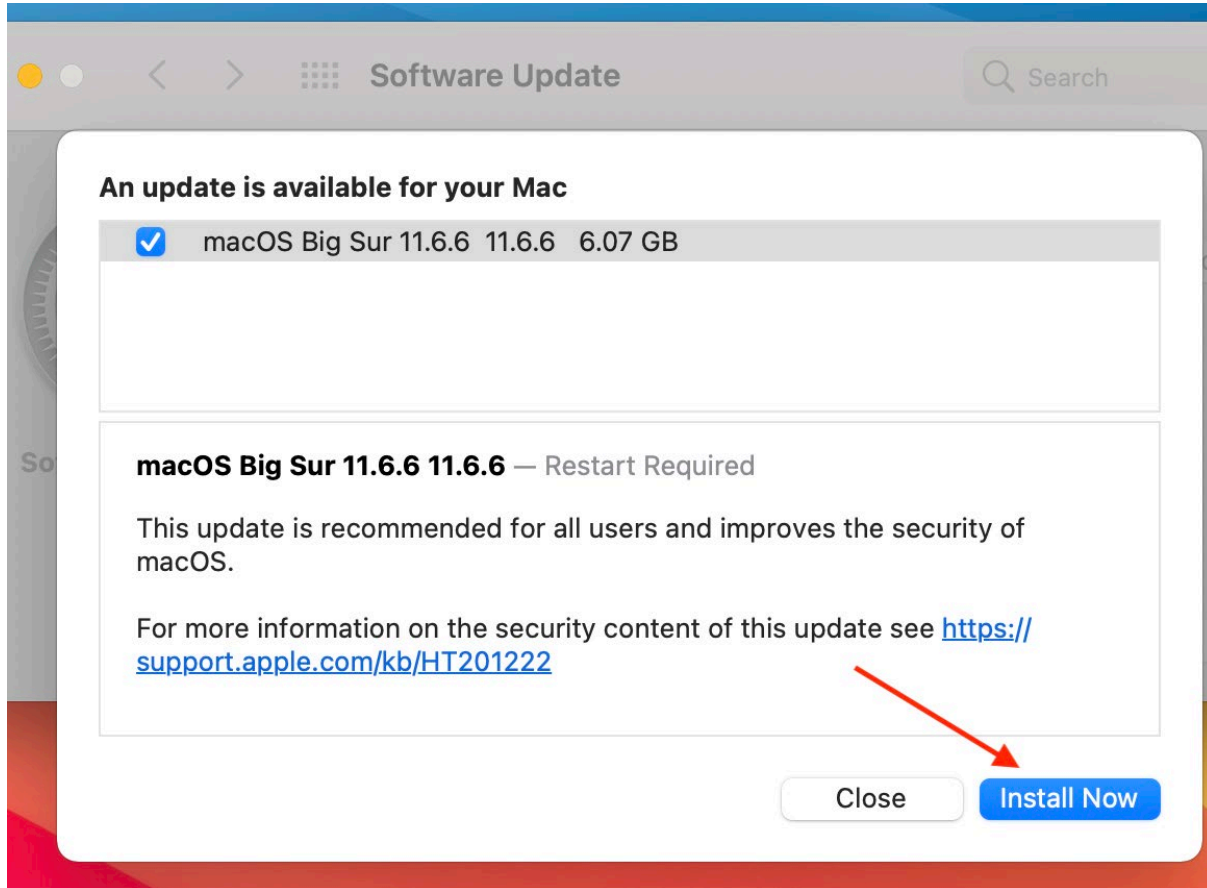


To update the Apple Macintosh operating system

1. From the **Apple Menu** in the corner of your screen, choose System Preferences
2. In the System Preferences window, click **Software Update**



3. Select appropriate update depending on the version of MacOS



The image shows a screenshot of a macOS Software Update dialog box. The window title is "Software Update" and it has a search bar. The main heading is "An update is available for your Mac". Below this, there is a list of updates with a checked box next to "macOS Big Sur 11.6.6 11.6.6 6.07 GB". The details for this update are shown below, including the version "macOS Big Sur 11.6.6 11.6.6" and the note "Restart Required". The text explains that the update is recommended for all users and improves security. A link is provided for more information: <https://support.apple.com/kb/HT201222>. At the bottom right, there are two buttons: "Close" and "Install Now". A red arrow points to the "Install Now" button.

Software Update

Search

An update is available for your Mac

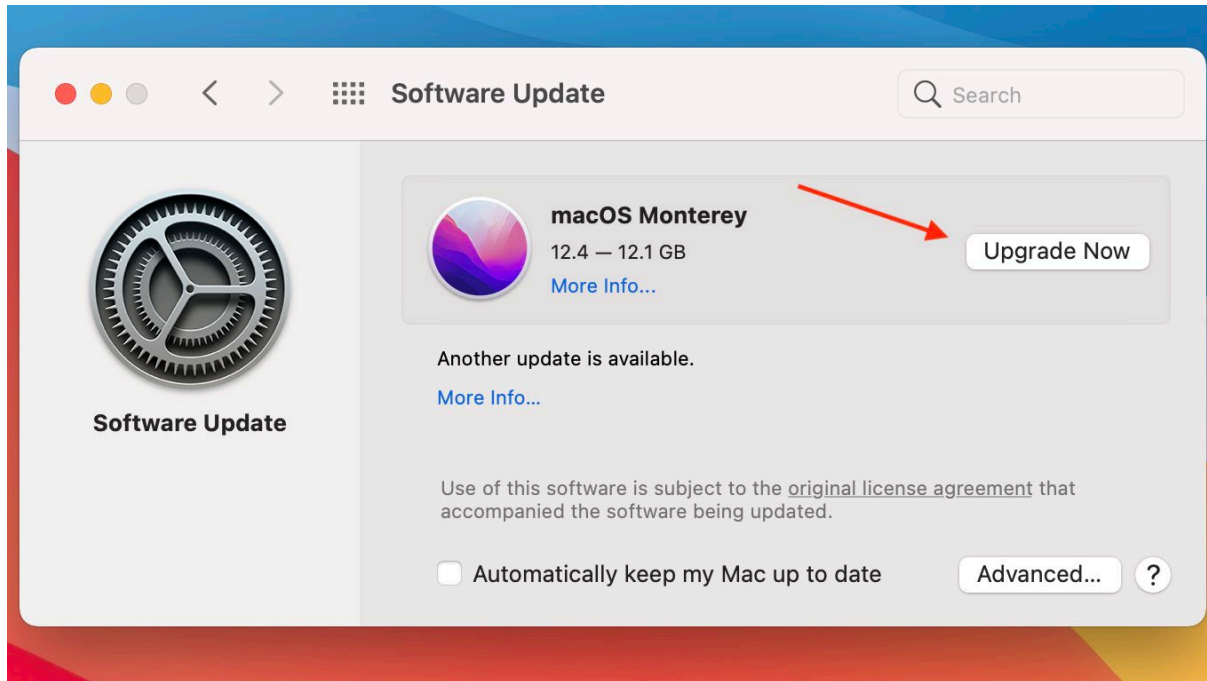
| | |
|-------------------------------------|-------------------------------------|
| <input checked="" type="checkbox"/> | macOS Big Sur 11.6.6 11.6.6 6.07 GB |
|-------------------------------------|-------------------------------------|

macOS Big Sur 11.6.6 11.6.6 — Restart Required

This update is recommended for all users and improves the security of macOS.

For more information on the security content of this update see <https://support.apple.com/kb/HT201222>

Close Install Now



4. Make sure to also apply any updates for Safari and iTunes
5. Reboot after the update is applied

To update your web browser, go to the settings icon and click on the Help menu item and then About “Web Browser” you will then get a pop-up window that will automatically scan for update and download it. You will then have to restart the web browser to apply changes. In fact, most application can be updated in a similar manner.

For the Adobe Creative Cloud application, please go to Help > Check for Updates

That covers all the major software that we all have, for anything else please go to the vendors support site and search for software update instructions.

If you encounter issues with applying these updates, please submit an incident through <https://service.sdcoe.net> or call 858-298-2205.