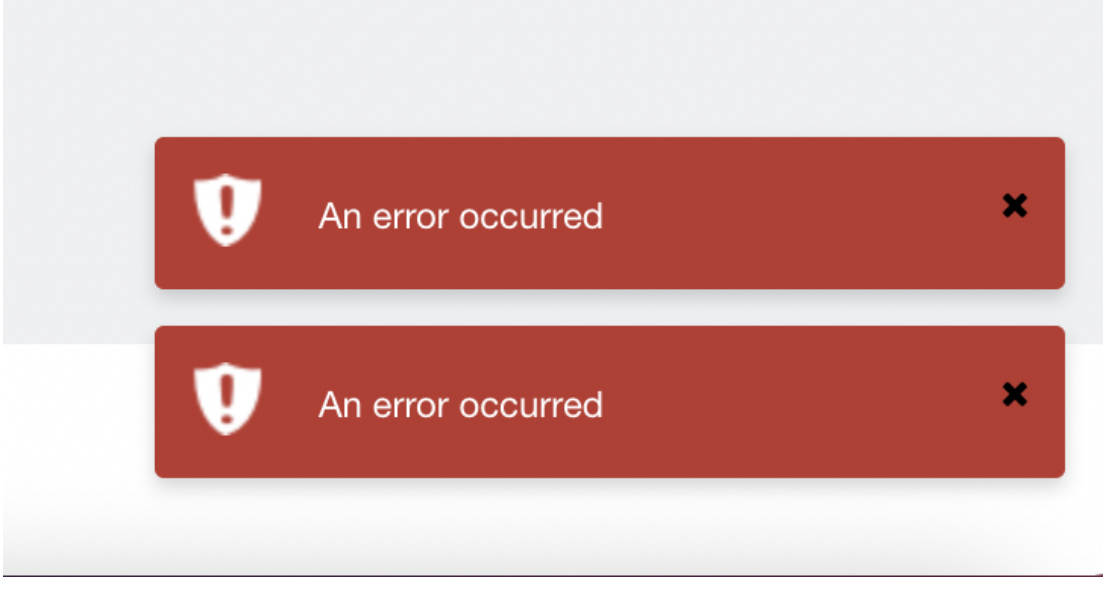
Redesign of Sophos Antivirus Software

Motivation

We investigated Sophos Home (free trial version), the antivirus software that UCSD provides students. We were motivated by how different antivirus softwares lack certain features that prevent users from getting the most effective security on their devices. Additionally, we wanted to show users of the possible ways that an antivirus software could be lacking via redesigning Sophos and showing how it could be improved to provide better security in order to help users make better decisions when choosing an antivirus software.

Things to Redesign in the Sophos Antivirus Software's Homepage:

1. Alert Messages
    - **Problem 1:** Currently, alert messages are unspecific. Therefore, the user has no way of knowing what went wrong.
    - **Solution:** Add some specific details to the alert message that inform the user as to what went wrong. If possible, offer a help link or a suggestion for a quick fix in the alert message.
    - **Problem 2:** Alerts came up too frequently and came up even if there was nothing seemingly wrong. The user may become too frustrated by the alerts and may even choose to ignore them, which leaves them more vulnerable to malware.
    - **Solution:** Only issue one alert per error that occurs and make sure that the alert is only issued if there is truly something that went wrong.
    - **Problem 3:** The alerts went away too quickly. It is possible that the user may not even have time to see the alert before it goes away. This puts the user at increased risk of not noticing potential attacks and/or vulnerabilities.
    - **Solution:** Make sure the alerts persist for a decent amount of time. If possible, wait for the user to acknowledge the alert prior to dismissing it.



2. **Scheduled Scans**

    - **Problem:** Sophos does not provide quick scans. With only a full scan available, users may have to wait up to 1 hour and 30 minutes for the scan to finish and reveal any security flaws.
    - **Solution:** Although full scans are able to detect more malware and security flaws than quick scans, Sophos should provide a quick scan option so users can be informed of at least some security flaws on their device.
    - **Problem:** Users have to set up automatic scans through the website (not set up initially). Furthermore, the automatic scans can only be set in increments of 30 minutes and can only be set for once a day. Additionally, there is no explicit confirmation that the scheduled scan is set up properly.
    - **Solution:** Since some users may not take the time to set up automatic scans and they may also forget to run scans daily, the antivirus software should be initially set up to do automatic scans at least daily in order to make sure the user is using the best security practices. Furthermore, an option to set up multiple automatic scans a day should be allowed in order to ensure greater security of the user's device. Also, an explicit confirmation of the scheduled scan being set up properly would be beneficial so that the user can know for sure that they set up the automatic scans properly and can go about their day without having to manually click scan from the Sophos icon in the toolbar.
    - **Problem**: Even after having enabled automatic scans, the automatic scan option was later found to be disabled when checked on a different day. This is problematic since a user could think that Sophos is automatically scanning their computer, when in reality there is no scanning occurring, which leaves the user vulnerable to malware.
    - **Solution**: Make sure that the automatic scan is configured correctly so that it doesn't turn off. At the very least, notify the user if the automatic scan is being turned off.

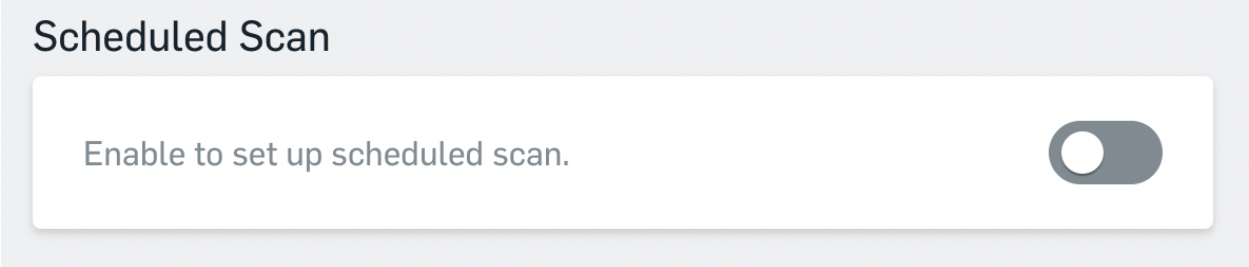
2. **Scheduled Scans**

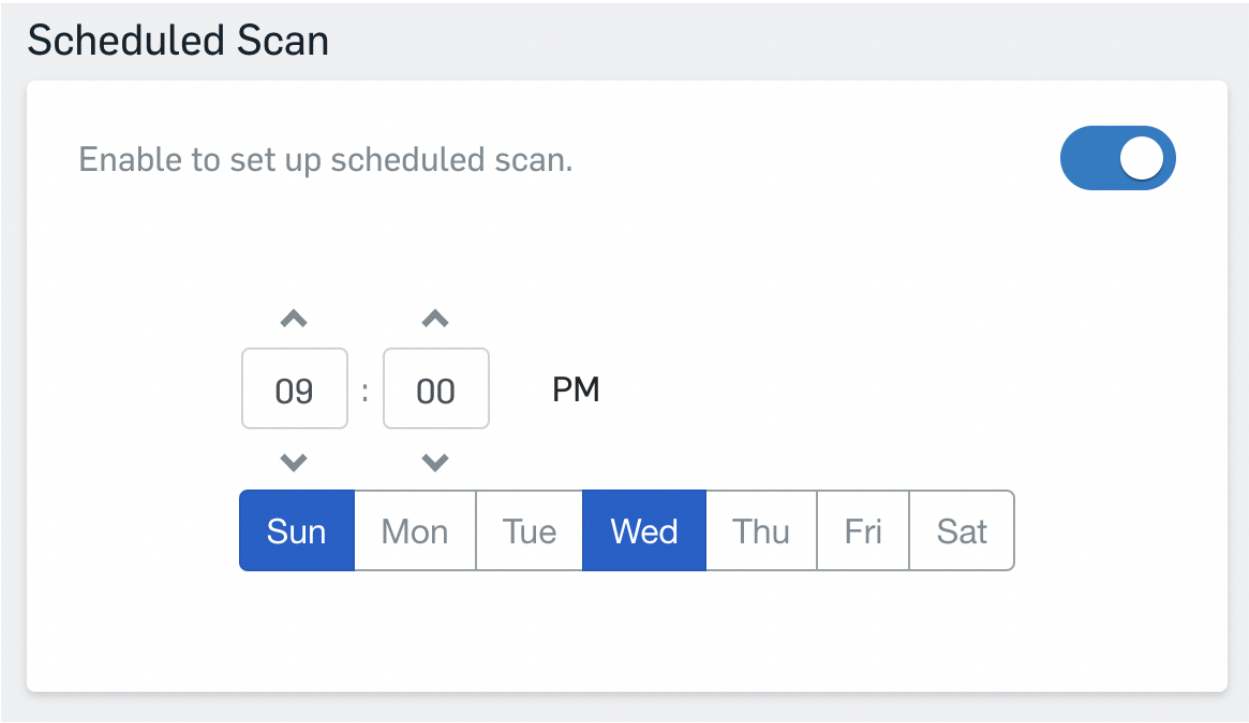
2. **Scheduled Scans**

    - **Problem:** Users have to set up automatic scans through the website (not set up initially). Furthermore, the automatic scans can only be set in increments of 30 minutes and can only be set for once a day. Additionally, there is no explicit confirmation that the scheduled scan is set up properly.
    - **Solution:** Since some users may not take the time to set up automatic scans and they may also forget to run scans daily, the antivirus software should be initially set up to do automatic scans at least daily in order to make sure the user is using the best security practices. Furthermore, an option to set up multiple automatic scans a day should be allowed in order to ensure greater security of the user's device. Also, an explicit confirmation of the scheduled scan being set up properly would be beneficial so that the user can know for sure that they set up the automatic scans properly and

can go about their day without having to manually click scan from the Sophos icon in the toolbar.

- **Problem**: Even after having enabled automatic scans, the automatic scan option was later found to be disabled when checked on a different day. This is problematic since a user could think that Sophos is automatically scanning their computer, when in reality there is no scanning occurring, which leaves the user vulnerable to malware.
- **Solution**: Make sure that the automatic scan is configured correctly so that it doesn't turn off. At the very least, notify the user if the automatic scan is being turned off.

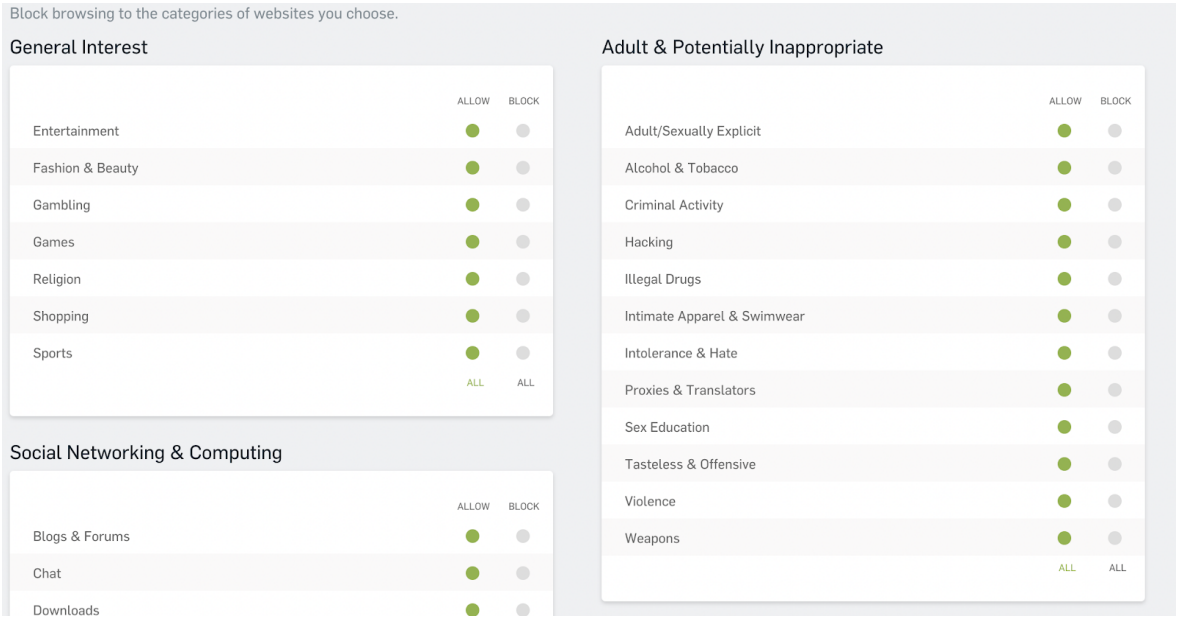




3. **Web Filtering**

- **Problem:** Every website is allowed by default. There are some website categories that may be inappropriate to not block straight from the beginning, such as the "Intimate Apparel & Swimwear" and "Tasteless and Offensive" categories. The categories are also unclear as to what websites they are blocking. For example, if a user wanted to block the category named "Illegal Drugs", it's unclear whether Sophos blocks websites that mention the words "illegal drugs" or if Sophos blocks websites that sell illegal drugs.

- **Solution**: Sophos should block adult and inappropriate categories as the default option to prevent users from accidentally going to these websites. Sophos should also provide a brief description for each category explaining which specific websites are blocked, so that users can understand exactly what they are blocking.



4. **Deleting Files**

- **Problem:** Sophos detects potentially malicious files and deletes them automatically without giving the user the choice to keep them or delete them from the device. This can be bad if Sophos incorrectly detects a user's own file as being dangerous.
- **Solution:** Provide a warning or message allowing the user to either keep the files or delete them

Resources Used

- https://bestantiviruspro.org/review/sophos-antivirus-review/#pros-and-cons
- Sophos Web Interface