Avoiding malicious software updates

Government software maintenance teams and users should also be informed to be aware of fake update messages. These messages are another way threat actors try to access computers and mobile devices.
Malicious messages can appear to users in the following ways:

- **Pop-ups.** They may look real but clicking on a pop-up may lead to a hack. Users should be advised to avoid malicious pop-ups. Updates should only be obtained from verifiable sources such as directly from the vendor website. Updates should also appear on the software's website, app store or within the program.
- **Emails.** The email may state that an update is long overdue. It may even have the company logo with all the correct spelling in the text. Don't click on links or respond to these types of emails. For information about updates, it's best to contact the software's support desk or check the vendor website.

One of the best ways to avoid malware downloads is to let the software automatically update where available. Many external vendor software solutions have an option to automatically run updates when available.
Mobile devices are increasingly being used for work purposes. Users should therefore also be reminded to keep their mobile devices updated. They should check for software update notices in the settings of their mobile devices.

Revision #2
Created 8 October 2025 10:01:22 by RISA
Updated 8 October 2025 10:02:37 by RISA