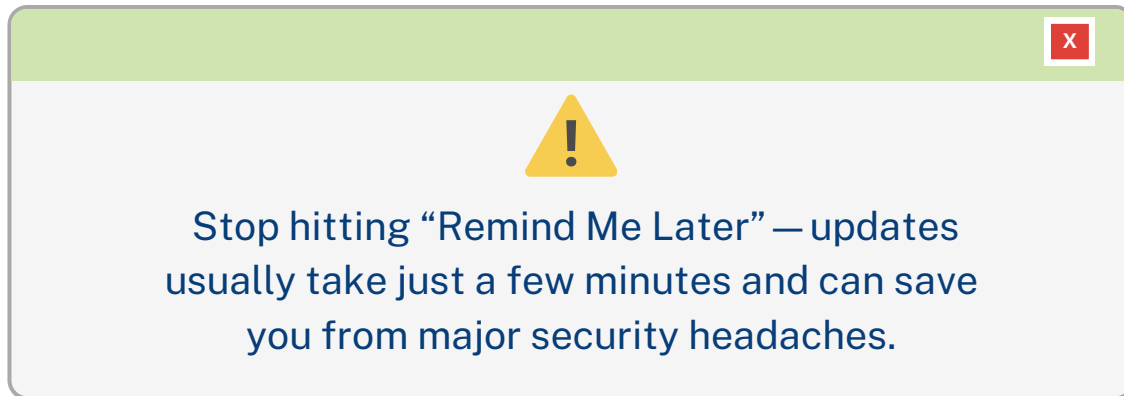


# KEEP YOUR SOFTWARE UPDATED



Source: National Cybersecurity Alliance

## WHY IT MATTERS



Software updates fix security flaws that hackers can exploit.



They also improve performance and add new features.

## BEST PRACTICES



**Turn on automatic updates** in your device settings.



**Install updates ASAP** - don't delay when notified.



**Watch for update alerts** - especially for browsers and antivirus software.



**Avoid fake update scams** - never click pop-ups or suspicious emails.



**Only download updates from trusted sources** - official websites or app stores.



**If your device is no longer supported**, consider replacing it or using it offline for non-sensitive tasks.

# SOFTWARE UPDATES: A COMPREHENSIVE GUIDE

## OVERVIEW

Keeping software up to date is one of the simplest and most effective ways to protect your devices and personal data.

## BEST PRACTICES

### Enable Automatic Updates

- Check settings under “Software” or “Security.”
- Search for “Automatic Updates” in your device settings.

### Respond to Notifications Promptly

- Not all updates are automatic.
- Install updates for browsers, antivirus, and operating systems ASAP.

### Watch for Fake Update Scams

- Close suspicious pop-ups.
- Don’t click on urgent-looking update messages from unknown sources.

### Verify Update Sources

- Only update via official app stores or developer websites.
- Never trust pop-ups, emails, or third-party sites.

### Make Updates a Habit

- Check settings monthly to ensure updates are working.
- Restart devices when needed to complete updates.

### Know When It’s Time to Upgrade

- Unsupported devices are vulnerable.
- Replace or disconnect outdated tech from the internet.
- Avoid using unsupported devices for sensitive tasks like banking.

## UPDATES CAN:



Fix  
malware



Improve  
performance



Install latest  
features