Identify legitimate emails from the App Store or iTunes Store

If you’re not sure whether an email about an App Store, iTunes Store, iBooks Store, or Apple Music purchase is legitimate, these tips may help.

Scammers often try to trick you into sharing personal or financial information by sending you messages or links to websites that might look like they’re from Apple, but their actual purpose is to steal your account information. Some phishing emails will ask you to click on a link to update your account information.

Others might look like a receipt for a purchase in the App Store, iTunes Store, iBooks Store or for Apple Music, that you’re certain you didn’t make.

Never enter your account information on websites linked from these messages, and never download or open attachments included within them.

Is this email legitimate?

If you receive an email about an App Store or iTunes Store purchase, and you're not sure whether it is real, you can look for a couple of things that can help confirm that the message is from Apple.

Genuine purchase receipts—from purchases in the App Store, iTunes Store, iBooks Store, or Apple Music—include your current billing address, which scammers are unlikely to have. You can also review your App Store, iTunes Store, iBooks Store, or Apple Music purchase history.

Emails about your App Store, iTunes Store, iBooks Store, or Apple Music purchases will never ask you to provide this information over email:

Social Security Number
Mother's maiden name
Full credit card number
Credit card CCV code

Update your account info safely

If you receive an email asking you to update your account or payment information, only do so in Settings directly on your iPhone, iPad, or iPod touch; in iTunes or the App Store on your Mac; or in iTunes on a PC.

To update your password for the Apple ID that you use for purchases, do so only in Settings on your device or at appleid.apple.com.

If you received or acted on a likely phishing message:

If you received a suspicious email, please forward it to reportphishing@apple.com. If you're on a Mac, select the email and choose Forward As Attachment from the Message menu.

If you think you might have entered personal information like a password or credit card info on a scam website, immediately change your Apple ID password.