

Avoiding spam and phishing

From email to instant messaging to social media, the Internet is an essential communication tool. Unfortunately, it's also popular among scammers and cybercriminals. To protect yourself from email scams, malicious software, and identity theft, you'll need to understand how to identify and avoid potentially dangerous content in your inbox, including spam and phishing attempts.

Watch the video to learn more about spam and phishing.

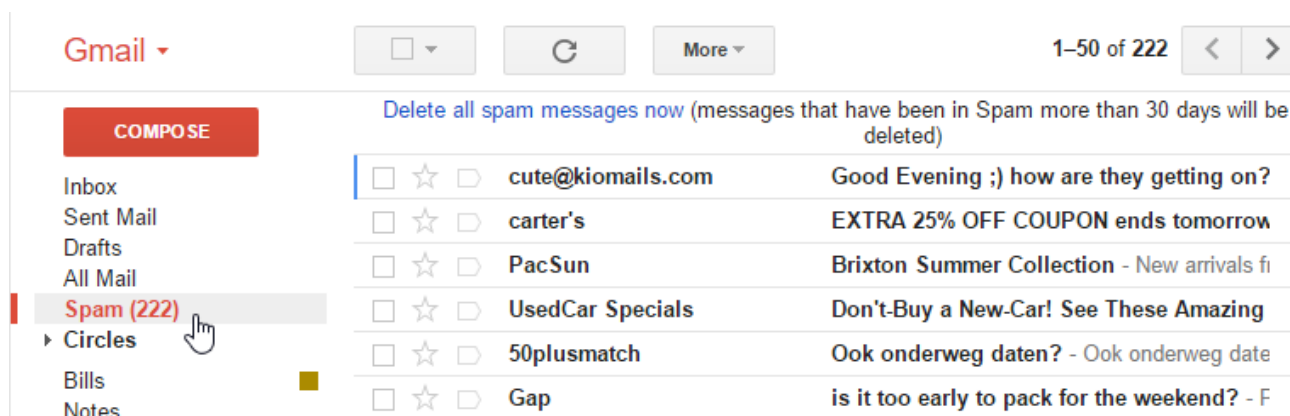
Dealing with spam

If you've ever received unwanted email advertisements, you may already be familiar with spam, also known as junk email. Spam messages can clutter your inbox and make it more difficult to find the emails you actually want to read. Even worse, spam often includes phishing scams and malware, which can pose a serious risk to your computer. Fortunately, most email services now include several features to help you protect your inbox from spam.

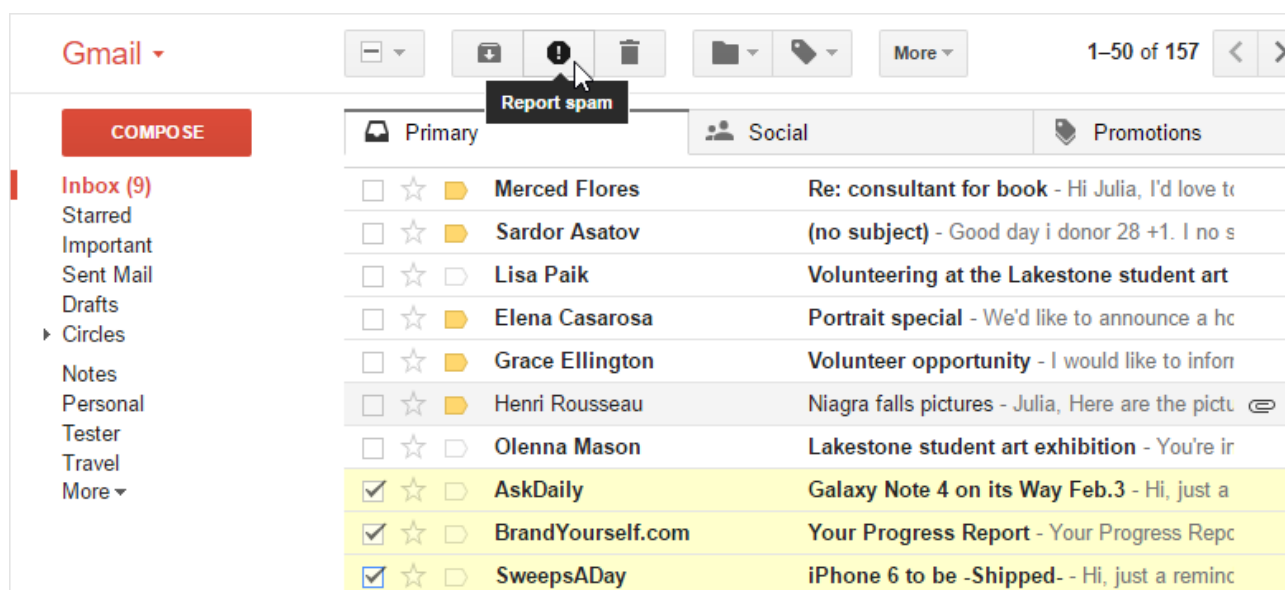
Spam filters

Whenever you receive an email, most email providers will check to see if it's a real message or spam. Any likely spam messages will be placed in the spam folder so you don't accidentally open them when checking your email.

Spam-blocking systems aren't perfect, though, and there may be times when legitimate emails end up in your spam folder. We recommend checking your spam folder regularly to make sure you aren't missing any important emails.



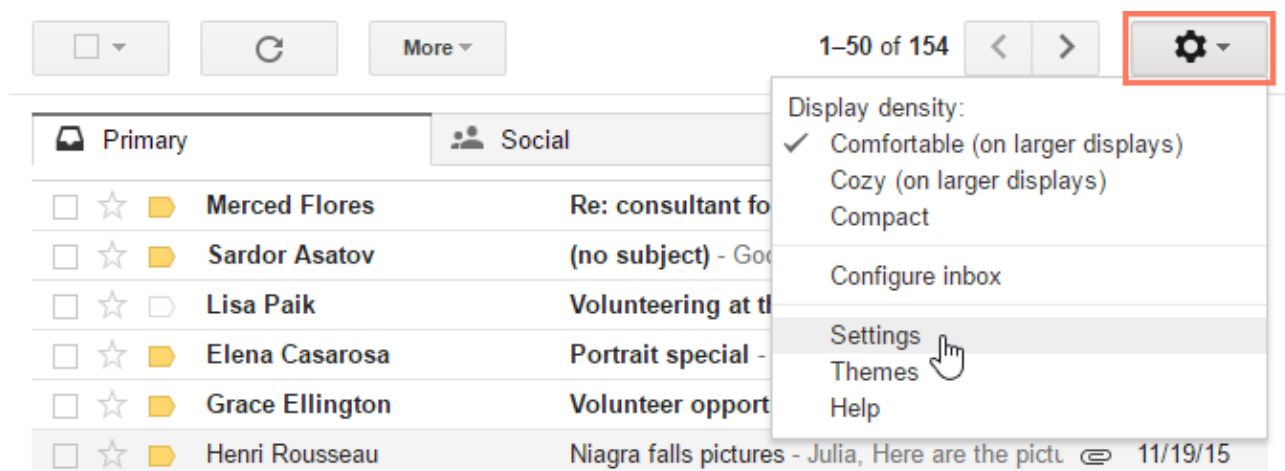
Many email services also have a feature you can use to mark emails as spam. In Gmail, for example, you can select the message and click the Mark as Spam button. This helps your email provider filter out these types of messages in the future.



Turning off email images

Spam messages often contain images that the sender can track. When you open the email, the images will load and the spammer will be able to tell if your email works, which could result in even more spam. You can avoid this by turning off email images. Let's look at how to do this in Gmail, but remember that the process will vary depending on your email service.

1. Click the gear icon, then select Settings from the drop-down menu.



2. Select Ask before displaying external images, then click Save at the bottom.

Settings



General Labels Inbox Accounts and Import Filters and Blocked Addresses
Forwarding and POP/IMAP Chat Labs Offline Themes

Language: Gmail display language: English (US)
[Change language settings for other Google products](#)
[Show all language options](#)

Phone numbers: Default country code: United States

Maximum page size: Show 50 conversations per page
 Show 250 contacts per page

Images:
☐ Always display external images - [Learn more](#)
☒ Ask before displaying external images

Default reply behavior:
☒ Reply
☐ Reply all
[Learn more](#)

3. Whenever you open a message with images, Gmail will prevent them from loading by default.

Gmail



Delete forever

Not spam



More

1 of 14

COMPOSE

Inbox (6)

Starred

Important

Sent Mail

Drafts

Circles

Notes

Personal

Tester

Travel

Less

Chats

All Mail

Spam (13)

Trash

Your Online Reputation Matters - Here's How to Fix It



Spam x



Sabrina Clark <sclark@brandyourself

May 5 (5 days ago)



to me



Why is this message in Spam? It's similar to messages that were detected by our spam filters. [Learn more](#)



Images are not displayed. [Display images below](#)

Brand Yourself Online
Reputation
Management

Email not displaying correctly? [View it in your browser.](#)



4. images prevented from loading in gmail

Phishing

Phishing scams are messages that try to trick you into providing sensitive information. These often appear to come from a bank or another trusted source, and they'll usually want you to re-enter a password, verify a birth date, or confirm a credit card number. Phishing messages may look real enough at first glance, but it's surprisingly easy for scammers to create convincing details.

Click the buttons in the interactive below to learn more about identifying a phishing email.

From: "Bank of America" customerservice@bankofamerica.com
To: "Jane Smith" jane-smith12@gmail.com
Date: Wed, May 26, 2010
Subject: Fraud Alert – Action Required



Dear Customer,


At Bank of America, your satisfaction is our number one priority. We have recently added an Advanced Online Security option for our customers with online accounts. It is urgent that you go to our website and add Advanced Online Security to your account. Click on the following and update your information www.bankofamerica.com.

If you do not take these steps, in order to protect you, we will put a hold on your account, and you will be required to visit your local branch to verify your identity.

Thank you for helping us to make Bank of America the safest bank on the internet.

If you are receiving this message and you are not enrolled in online banking, [sign up now](#). New online members will automatically be enrolled in the Advanced Online Security program.

Sincerely,

Bank of America Online Security Department 

Other common email scams

Spam and phishing are common problems, but there are many other types of email scams you may encounter. Some will promise to give you a lot of money if you advance a small amount upfront. Others may pretend to be from people you know in real life, and they'll often ask you to send money or download an attached file.

As with spam and phishing scams, remember to trust your best judgement. You should never send someone money just because you've received an email request. You should also never download email attachments you weren't expecting because they might contain malware that could damage your computer and steal your personal information.

Spam, scams, and phishing schemes will continue to evolve and change. But now that you know what to look for—and what to avoid—you can keep your inbox and computer that much safer.