Suspicious Emails

Look for these scam clues

Scam emails, also known as phishing emails, often feature legitimate company logos, return addresses, and even 1-800 phone numbers. They often use scare tactics to get people to provide their information.

Here are some things to check in any suspicious email. They follow the initials of a handy little acronym, SCAMD!

S — Spelling and grammar. This is usually the first and best tip-off that something's bogus. If you're looking at an email with multiple spelling or grammar errors, it's probably a scam.

C — Certified Mail. Certified AOL Mail is a feature designed to help you easily identify email that has been sent by AOL. In your inbox, you'll see an AOL icon or green ribbon next to any AOL Certified Mail. Also, above the email details (above the From:, To:, and Subject box), you'll see a banner that says AOL Certified Mail.

A — Asking for personal information. No legitimate company will email you requesting personal information such as your password or your social security number. If you have any suspicions about the email, don't click any links. Instead, go to the website of the company and use the “Contact Us” link to find a company's phone number and call them. Don't use the phone number provided in a suspicious email as it might be a fake number to collect your personal info.

M — Mass Mailings. If you got an email claiming you've been selected to win a prize, and there are a ton of other recipients listed in the “to” or “cc” fields, chances are it's a scam.

D — Details. You can often find out the true return email address of a sender by clicking on the “Details”, “Show Details”, or “Full Headers” link under the “To:”
section, in the header of your email. If the sender is using a fake “from” address, you'll see the real one in the details view, usually under “Reply to.”

- DOES THE EMAIL SCREAM AT YOU IN ALL CAPS or have lots of !!!!!! at the end?

Beware of emails that try to get your attention by using all capital letters, especially in the subject line, or that try to scare you with lots of exclamation marks. The authors of scam emails tend to write over-the-top and very emotional content. Also, keep an eye out for dire warnings, such as "Urgent!" or "Danger!"

One final word of advice: Don’t respond to a spam email. By doing so, you confirm that your email account is active, and you'll likely be flooded with more spam and scam attempts.

If you are unsure of an email's authenticity, forward the email to aol_phish@abuse.aol.com. If you prefer, you can also provide additional information before sending the email.