

How to Spot a Fake or Spoof Email

1. Generic greetings. Many spoof emails begin with a general greeting, such as: "Dear PayPal member." If you do not see your first and last name, be suspicious and do not click on any links or button.
2. A fake sender's address. A spoof email may include a forged email address in the "From" field. This field is easily altered.
3. A false sense of urgency. Many spoof emails try to deceive you with the threat that your account is in jeopardy if you don't update it ASAP. They may also state that an unauthorized transaction has recently occurred on your account, or claim PayPal is updating its accounts and needs information fast.
4. Fake links. Always check where a link is going before you click. Move your mouse over it and look at the URL in your browser or email status bar. A fraudulent link is dangerous. If you click on one, it could:
 - Direct you to a spoof website that tries to collect your personal data.
 - Install spyware on your system. Spyware is an application that can enable a hacker to monitor your actions and steal any passwords or credit card numbers you type online.
 - Cause you to download a virus that could disable your computer.
5. Emails that appear to be websites. Some emails will look like a website in order to get you to enter personal information. PayPal never asks for personal information in an email.
6. Deceptive URLs. Only enter your PayPal password on PayPal pages. These begin with <https://www.paypal.com/>
 - If you see an @ sign in the middle of a URL, there's a good chance this is a spoof. Legitimate companies use a domain name (e.g. <https://www.company.com/>).
 - Even if a URL contains the word "PayPal," it may not be a PayPal site. Examples of deceptive URLs include: www.paypalsecure.com, www.paypa1.com, www.secure-paypal.com, and www.paypalnet.com.
 - Always log in to PayPal by opening a new web browser and typing in the following: <https://www.paypal.com/>
 - Never log in to PayPal from a link in an email
7. Misspellings and bad grammar. Spoof emails often contain misspellings, incorrect grammar, missing words, and gaps in logic. Mistakes also help fraudsters avoid spam filters.
8. Unsafe sites. The term "https" should always precede any website address where you enter personal information. The "s" stands for secure. If you don't see "https," you're not in a secure web session, and you should not enter

data.

9. Pop-up boxes. PayPal will never use a pop-up box in an email as pop-ups are not secure.
10. Attachments. Like fake links, attachments are frequently used in spoof emails and are dangerous. Never click on an attachment. It could cause you to download spyware or a virus. PayPal will never email you an attachment or a software update to install on your computer.

If you receive a spoof email, forward the entire email - including the header information - to us at: spoof@paypal.com, then delete it from your mailbox. Please note that the automatic response you get from us may not address you by name.

Thanks to PayPal

<https://www.paypal.com/cgi-bin/webscr?cmd=xpt/general/SecuritySpoof-outside>