Identifying phishing and how to defend yourself for phishing attack

Help us combat fraud. If you see anything that looks out of the ordinary (including suspicious looking emails and websites), tell us and we'll investigate.

What is Phishing?

'Phishing' is a form of web forgery designed to steal your identity, usually for financial gain.

It works by using false pretences to get you to disclose sensitive personal information, like credit and debit card numbers, account passwords, or bank account details.

One of the most common phishing scams involves sending a fraudulent email that appears to be from a trusted company or brand. This email then directs you to a fake version of a well-known website and records any information you enter, such as your password, financial details and more.

PayPal is committed to helping shut down these sites and ensure that you're able to spot phishing immediately. We make it our job to keep your identity as safe as possible, online.

Suspicious emails

"Phishing" is an illegal attempt to "fish" for your private, sensitive data. One of the most common phishing scams involves sending an email that fraudulently claims to be from a well-known company (like PayPal).

Hints about identifying scam email

1. Emails from PayPal will always address you by your first and last names or by your business name. We never say things like "Dear user" or "Hello PayPal member".
2. Don't ever open an attachment unless you're sure it's legitimate and safe. Be particularly cautious of invoices from companies and contractors you're not familiar with. Some attachments contain viruses that install themselves when opened.
3. Many fraudsters send spoofed emails warning that an account is about to be suspended, and that the account holder must enter their password in a (spoofed) webpage. PayPal will never ask you to enter your password unless you're on the login page.

If you believe you've received a phishing email, follow these steps right away:

1. Forward the entire email to **spoof@paypal.com**.
2. Do not alter the subject line or forward the message as an attachment.
3. Delete the suspicious email from your inbox.

We'll look into it and email you a response to let you know if it is indeed fraudulent. In the meantime, don't click any links or

Suspicious websites

Phishing emails often lead you to fake or "spoof" websites in an attempt to steal your private, sensitive data. These could look very unusual and not fit with what you expect from the company, or could appear very genuine – but end up having a suspicious URL in the web address bar. If you believe you're on a spoof website, don't enter any information.

Instead, all you have to do is copy the site's web address and paste it into an email message; send it to **spoof@paypal.com**. Our security experts will examine the site and if it's bogus, we'll get it shut down. With this simple action, you'll be helping us keep our entire community safe.

Suspicious SMS

SMS SPAM can be more than just annoying – it may contain suspicious content. Many carriers will let you report SPAM by simply forwarding the message to '7726' (which is the keys for 'SPAM' on most phones). Check with your service provider to find if this service is supported.

download any attachments within the suspicious email.

Learn more about phishing

Back to Purchase Protection

Back to Seller Protection