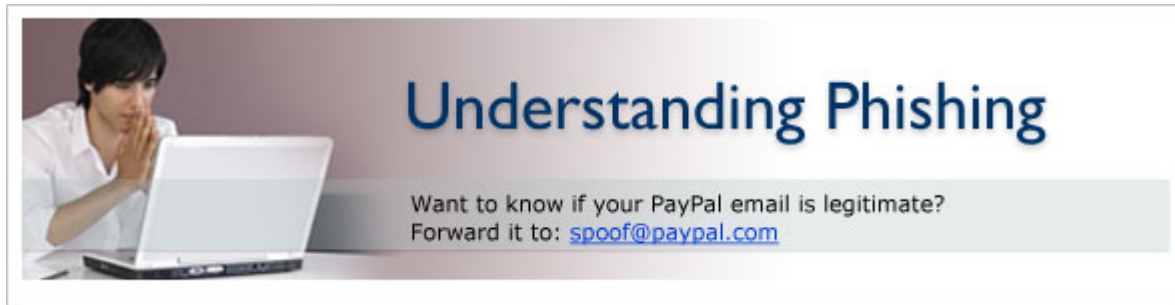


Phishing Guide Part 1



What is Phishing?

Phishing is a form of fraud designed to steal your identity. It works by using false pretenses to get you to disclose sensitive personal information, such as credit and debit card numbers, account passwords, or Social Security numbers.

One of the most common phishing scams involves sending a fraudulent email that claims to be from a well-known company. Phishing can also be carried out in person, over the phone, through fraudulent pop-up windows, and websites.

DEFINITIONS

Phishing (pronounced "fishing"): Fraudulent emails that request or initiate a scam to get sensitive personal information.

Spoof Site: Fraudulent sites – usually linked from a phishing email – that look like well-known websites.

How phishing through email works.



A fraudster will start out sending thousands, even millions, of emails to different mail accounts disguised as messages from a well-known company. The typical phishing email will contain a concocted story designed to lure you into taking an action such as clicking a link or button in the email or calling a phone number. Learn how to spot a fraudulent email with [Recognizing Phishing](#).

In the email, there will be links or buttons that take you to a fraudulent website.

The fraudulent website will also mimic the appearance of a popular website or company. The scam site will ask for personal information, such as your credit card number, Social Security number, or account password.

You think you're giving information to a trusted company when, in fact, you're supplying it to a criminal.

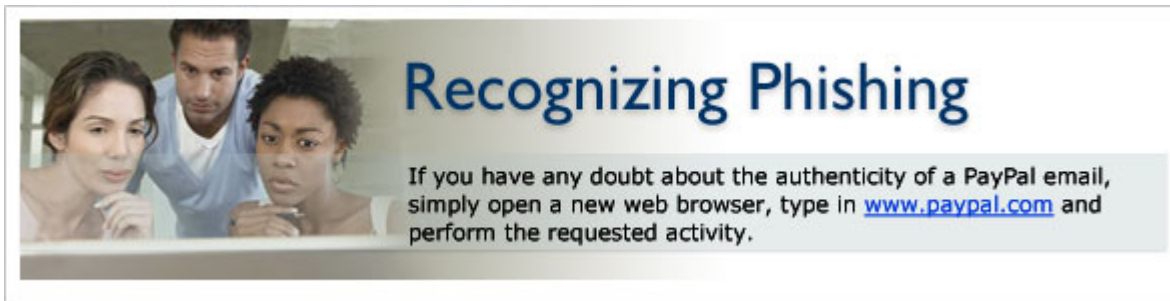
Learn how to spot a fraudulent website with [Recognizing Phishing](#).

Questions PayPal will never ask you in an email.

To help you better identify fake emails, we follow strict rules. We will never ask for the following personal information in email:

- Credit and debit card numbers
- Bank account numbers
- Driver's license numbers
- Email addresses
- Passwords
- Your full name

Phishing Guide Part 2

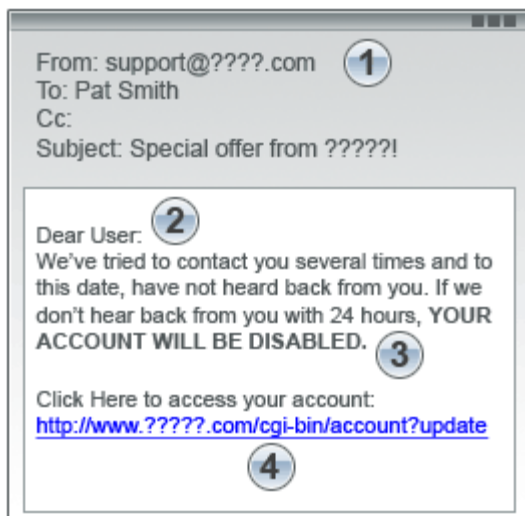


Things to look for in scam email and websites.

Fraudulent email and websites are designed to deceive you and can be difficult to distinguish from the real thing.

Whenever you get an email about your PayPal account, the safest and easiest course of action is to open a new browser, type <https://www.paypal.com>, and log in to your PayPal account directly. Do not click on any link in an email that requests personal information.

How to spot a phishing email.



There are many telltale signs of a fraudulent email.

Sender's Email Address. To give you a false sense of security, the "From" line may include an official-looking email address that may actually be copied from a genuine one. The email address can easily be altered – it's not an indication of the validity of any email communication.

Generic Email Greeting. A typical phishing email will have a generic greeting, such as "Dear User." Note: All PayPal emails will greet you by your first and last name.

False Sense of Urgency. Most phishing emails try to deceive you with the threat that your account will be in jeopardy if it's not updated right away. An email that urgently requests you to supply sensitive personal information is typically fraudulent.

Fake Links. Many phishing emails have a link that looks valid, but sends you to a fraudulent site that may or may not have an URL different from the link. Always check where a link is going before you click. Move your mouse over the URL in the email and look at the URL in the browser. As always, if it looks suspicious, don't click it. Open a new browser window, and type <https://www.paypal.com>.

Attachments. Similar to fake links, attachments can be used in phishing 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.

How to spot a spoof (fraudulent) website.



A phishing email will usually try to direct you to a fraudulent website that mimics the appearance of a popular website or company. The spoof website will request your personal information, such as credit card number, Social Security number, or account password.

You think you are giving information to a trusted company when, in fact, you are supplying it to an online criminal.

Deceptive URLs.

Be cautious. Some fraudsters will insert a fake browser address bar over the real one, making it appear that you're on a legitimate website. Follow these precautions: Even if an URL contains the word "PayPal," it may not be a PayPal site.

Examples of fake PayPal addresses:

`http://signin.paypal.com@10.19.32.4/`

`http://83.16.123.18/pp/update.htm?=https://`

`www.paypal.com/=cmd_login_access`

`www.secure-paypal.com`

Always log in to PayPal by opening a new browser and typing in the following:

<https://www.paypal.com>.

The term "https" should precede any web address (or URL) 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.

Out-of-place lock icon.

Make sure there is a secure lock icon in the status bar at the bottom of the browser window. Many fake sites will put this icon inside the window to deceive you.

[Part 3: Fighting Phishing](#)

Phishing Guide Part 3



Ways to combat scam email and websites.

Remember, when it comes to phishing, you are in control. To protect your personal financial information, ignore the requests in the email.

- Never provide any information.
- Never click on any link that seems suspicious.

How to report a phishing email.

We take online fraud seriously by investigating phishing emails reported to us. Follow these steps:

- Forward the entire email to spoof@paypal.com.
- Do not alter the subject line or forward the message as an attachment.
- Delete the suspicious email from your email account.

We'll let you know quickly if the email is legitimate. Your vigilance helps protect other PayPal users.

A genuine PayPal email will never ask for:

- Credit and debit card numbers
- Bank account numbers
- Driver's license numbers
- Email addresses
- Passwords
- Your full name

A genuine PayPal email will never include:

- Attachments
- Software

Use tools to fight phishing.

We have assembled helpful resources to protect you from identity theft and to single out potential fraud sites:

Virtual Debit Card. A digital credit card from MasterCard that is designed to increase your security when shopping online. The Virtual Debit Card will alert you when you are on a known fraudulent website. Sign up for [Virtual Debit Card](#).

Equifax Credit Alerts for PayPal Users. PayPal users can get this free service from Equifax that will alert you to fraudulent activity. Find out more with our [Equifax Credit Alert Overview](#).

eBay Toolbar with Account Guard. Helps verify that you are on the PayPal or eBay site. [Download our eBay Account Guard toolbar](#)

More steps to protect you from phishing.

Monitor your PayPal account. Check your account periodically for suspicious activity. If you notice unauthorized use, report it to us. PayPal protects you 100% against unauthorized payments sent from your account.

Keep security software current. Update your firewalls and security patches frequently.

Be smart about your password. Change passwords often and use unique passwords that include letters, numbers, and symbols.