

Paypal phone number: 1-888-2211161

A message from Paypal : Please read that letter carefully. Thank you

At PayPal we continually strive to exceed our customers' expectations to provide a safe, secure method to send and receive money online. PayPal has agents that work 24/7 monitoring accounts and transactions, enabling you to buy and pay safely.

PayPal periodically contacts our customers by phone to verify activity on the PayPal account is authorized. During these phone calls, we will never ask you for your full credit card, or bank account information. By speaking to our customers, we ensure you are in control of your account and this further secures our system.

The terms "spoofing" and "phishing" are industry phrases used to describe the act of collecting personal information by using a fake email, website, or phone calls to entice victims into entering personal information such as your birthday, credit card numbers, bank accounts, passwords, etc. This sensitive information allows perpetrators to commit identity theft, credit card, and Internet fraud. These emails and sites appear identical to real ones, however, they are not. Unfortunately, some people fall prey to such scams and unknowingly surrender their password, credit card number, and a wide array of other personal information.

At PayPal, we care about the security of your account and financial information, therefore, we offer Security Tips that allow us to work together to protect against fraud.

Please remember these steps to help protect your PayPal account from Unauthorized Account Access.

Emails - Make sure they are sent from PayPal

1. If you receive an email and are unsure whether it is from PayPal,

open a new web browser (e.g., Internet Explorer or Netscape) and type in the following: <https://www.paypal.com/> Do not click on any link in an email which seems suspicious to you.

2. Some spoof websites will send emails that pretend to come from PayPal to entice you to log in at the spoof URL. Be extremely cautious of emails that direct you to a website that asks for sensitive information.

3. Stay safe; don't respond to emails asking for any of the following:

7 Your password and email address combination

7 Credit card numbers

7 Bank account numbers

7 Social security number

7 Drivers license number

7 First and Last Names

If you have surrendered financial or password information to a suspicious email or website, promptly report this to the issuing institution as well as change your password and security answers on your PayPal account. This can be completed in the Profile section of your account.

Email Greeting -

7 PayPal will never send you an email with the greeting "Dear PayPal User" or "Dear PayPal Member." Emails initiated by PayPal will address you by your first and last name, or the business name associated with your PayPal account.

7 Please note that the automatic response you get from us may not address you by name.

Always log into the PayPal site

7 PayPal will only ask for information after you have securely logged in

7 For your security, PayPal will never ask you to re-enter your full bank account, credit, or debit card number without providing you at least the last two digits of the number. These digits let you know that we already know the full number and are asking you for the rest of it. Beware of any website or email asking for these numbers for "verification" that does not prove that it knows the number by providing at least the last two digits

7 Use Account Guard on the eBay toolbar. If you use Internet Explorer, download the eBay toolbar. Account Guard helps ensure you are on PayPal or eBay

Website pages - make sure that they are hosted by PayPal

1. When using the PayPal service, always ensure that the URL address listed at the top of the browser is

<https://www.paypal.com/>. This ensures that the website is secure. Even if the URL contains the word 'PayPal', it may not be a PayPal webpage.

2. Look for the "lock" symbol that appears in the lower right hand corner of the browser. This symbol indicates that it is a secure site.

Do not download attachments, software updates, or any application to your computer via a link you received in an email. PayPal will never send you an attachment or software update to install on your computer.

Passwords - keep it on PayPal

1. Use a unique password for the PayPal account and change it every 30-60 days.

2. The password should be one that is not used on any other site, service, or login.

If you think you have received a fraudulent email, forward the entire email, including the header information to spoofer@paypal.com and then delete

the email from your mailbox. Never click any links or attachments in a suspicious email.

Click the "Security Center" link located at the top right hand corner of any PayPal website page to learn additional tips for staying safe online and to find tools that you can use to increase your security.

If you have any further questions, please feel free to contact us again.

Sincerely,

Israel

PayPal Community Support

PayPal, an eBay Company