PAYPAL SECURITY TIPS AND HELPFUL INFORMATION:

PayPal Security Center:
https://www.paypal.com/us/cgi-bin/webscr?cmd=_security-center

PayPal Secure Login (always login from PP homepage):
https://www.paypal.com/

FTC Security Tips:
http://www.ftc.gov/infosecurity

Protect Yourself from Fraudulent Emails:

At PayPal, protecting your account's security is our top priority. Recently, PayPal members have reported suspicious-looking emails and fake websites. These emails are not from PayPal and responding to them may put your account at risk. Please protect your PayPal account by paying close attention to the emails you receive and the websites you visit.

PLEASE USE THE FOLLOWING TIPS TO STAY SAFE WITH PAYPAL:

Safe Log In: To log in to your PayPal account or access the PayPal website, open a new web browser (e.g., Internet Explorer or Netscape) and type in the following: https://www.paypal.com

Greetings: Emails from PayPal will address you by your first and last name or the business name associated with your PayPal account. Fraudulent emails often include the salutation "Dear PayPal User" or "Dear PayPal Member".

Email Attachments: PayPal emails will never ask you to download an attachment or a software program. Attachments contained in fraudulent emails often contain viruses that may harm your computer or compromise your PayPal account.

Request for Personal Information: If we require information from you, we will notify you in an email and request that you enter the information only after you have safely and securely logged in to your PayPal account.

Often, fraudulent emails will request details such as your full name, account password, credit card number, bank account, PIN number, Social Security Number, or mother's maiden name.
If you think that you have received a fraudulent email (or fake website), please forward the email (or URL address) to spoof@paypal.com and then delete the email from your mailbox. Never click any links or attachments in a suspicious email.

SECURITY TIPS AND FRAUD PREVENTION...

At PayPal, maintaining your account's security is our top priority. To augment the security measures that we take on your behalf, there are steps that you can take to help protect your account from fraud and scams.

Website Security:

Type in the PayPal URL: To safely and securely access the PayPal website or your PayPal account, open a new web browser (e.g., Internet Explorer or Netscape) and type in the following: https://www.paypal.com/

Password Safety:

Never share your PayPal password: PayPal representatives will never ask you for your password. If you believe someone has learned your password, please change it immediately and contact us. Create a secure password: Choose a password that uses a combination of letters, numbers, and symbols. For example, $coo!place2l!ve or 2Barry5Bonds#1. Avoid choosing obvious words or dates such as a nickname or your birth date.

Keep your PayPal password unique: Don't use the same password for PayPal and other online services such as AOL, eBay, MSN, or Yahoo. Using the same password for multiple websites increases the likelihood that someone could learn your password and gain access to your account.

EMAIL SECURITY:

Look for a PayPal Greeting: PayPal will never send an email with the greeting "Dear PayPal User" or "Dear PayPal Member." Real PayPal emails will address you by your first and last name or the business name associated with your PayPal account. If you believe you have received a fraudulent email, please forward the entire email—including the header information—to spoof@paypal.com. We investigate every spoof reported. Please note that the automatic response you get from us may not address you by name.

Don't share personal information via email: We will never ask you to enter your password or financial information in an email or send such information in an email. You should only share information about your account once you have logged in to https://www.paypal.com/.

Don't download attachments: PayPal will never send you an attachment or software update to install on your computer.

Use Your Account Wisely:

Don't share your account: Don't use your PayPal account to collect or transfer money for someone else. These types of activity are often conducted as forms of money laundering or mail fraud and may result in significant criminal penalties. If someone contacts you and asks you to transfer money on their behalf, you should deny the request and contact us immediately.

Increase your security: Become a Verified PayPal member.

Look for legitimate sites: Examine all privacy and security seals before doing business with a particular website and make sure they are legitimate. PayPal is a licensee of the TRUSTe Privacy Program.

PAYPAL CUSTOMER SERVICE CENTER:

PayPal Customer Service Agents are available to help you during the following times:

4:00 AM PDT to 10:00 PM PDT Monday through Friday
6:00 AM PDT to 8:00 PM PDT on Saturday and Sunday

Call us at: 402-935-2050 (a U.S. telephone number)
Call us toll-free at: 1-888-221-1161

We may only discuss an account with the account-holder. Please have the following information available when you call:
Your telephone number
Your email address
The last 4 digits of your credit card or bank account registered with PayPal
For security reasons, we must verify the above details before discussing any account-specific information.

Try Our Self-Service Phone Options:
PayPal's Speech-Enabled phone system allows you to speak, or use your telephone keypad, to let us know exactly what you would like to do when contacting us. For example,
Listen to recent transactions - say "Transaction History"
Check the status of claims and disputes - say "Case Status"
Request a password reset email - say "Password"
Hear other account-specific information

TIPS FOR SAFER ONLINE SHOPPING

Knowing how to shop safely is essential when you're buying online. Check out these quick tips for safer spending:

Know Your Seller:
Don't Sacrifice Caution for an Impulse Buy
Use Extra Caution with High-Demand Items
Be Wary of Items with Delayed Delivery Dates
If It Sounds Too Good to Be True...
Warning Signs
Know Your Seller

Check the Seller's Feedback: Most auction sites and many online malls have a forum where buyers can comment on their experiences with sellers. Be cautious of sellers with little or no feedback, and take negative comments very seriously.

Compare Listings: Search for similar items to see if your item's price is fair-trade. Be suspicious of hard to find items offered at a very low price. If a seller is offering many of the same items, ask to speak with the seller's supplier. Verify that the supplier is a legitimate business with the correct address and phone number through a telephone directory.

Choose PayPal Verified Sellers: See if the seller is a Verified member of PayPal and has been a PayPal member for at least a couple of months. To check PayPal membership status, go to the "Send Money" tab and initiate a payment to the seller. On the "Check the details of your payment" page, before the payment is sent, you'll see the seller's reputation link (e.g. Verified Premier Member) next to his email address. Click the link to see more information about the membership status.

Don't Sacrifice Caution for an Impulse Buy: Always shop with a level head. Take the time to research the item and get to know your seller before agreeing to buy. Don't buy if there isn't enough time to check for warning signs.

Use Extra Caution with High-Demand Items: Particularly around the holidays, certain high-demand items are associated with higher purchasing risks. Do additional checking, especially with computers, jewelry, electronics, and items that are sold out in stores.

Be Wary of Items with Delayed Shipment: Pay attention to the advised delivery date. Delivery dates further than 20 days after your payment involve more risk. Be aware that PayPal sellers are not allowed to sell goods with delivery dates delayed more than 20 days from the date of payment.

If It Sounds Too Good to Be True: If it sounds too good to be true, it probably is. Ask yourself if the information in the item description sounds believable.

WARNING SIGNS:

Seller Has Large Quantity of Hard to Find Items If a seller claims to suddenly have a large quantity on an item that's impossible to find, question the validity of the claim. Ask to speak with the seller's supplier, and use a phone directory to verify that the supplier is a legitimate business with the correct address and phone number.

Seller Buys Low Dollar Items and Lists High Ticket Items On many sites, it is possible to improve your feedback rating by buying *and* selling items, so read the feedback comments carefully. If the seller has only made purchases (rather than sales), his feedback is not necessarily an indication of his selling reputation.

Seller Has Little, No, or Negative Feedback While a low feedback rating may simply indicate that the seller is new, transactions with low feedback sellers tend to involve more risk.

Seller Lists Multiple Items with the Same Picture Be wary of multiple listings with the same picture, particularly if the picture is from the manufacturer's website. If the photo looks like it was taken at a home or office, chances are better that the seller does have that item.

Following the above tips will help you have a safer shopping experience.