



KATOOSH SCAN DETECTOR™

Consumer Safety Quick Guide

Essential checks to make before buying, subscribing, sending money, or sharing personal information online

Before You Click, Scan the Offer

Online scams are becoming more convincing.

A questionable website may look professional, display a padlock symbol, advertise on a major platform, offer a money-back guarantee, and feature dozens of positive reviews.

None of those things proves that the offer is safe.

A product can also be real without being a good deal. It may be dramatically overpriced, tied to a hidden subscription, difficult to return, or promoted using exaggerated claims.

This guide will help you slow down, recognize common warning signs, and ask better questions before you:

- Buy from an unfamiliar website
- Sign up for a free trial
- Enter your payment information
- Send money to a seller

- Respond to an email or text message
- Apply for an online job
- Trust an investment opportunity
- Share personal or financial information

A few minutes of checking could save you money, frustration, and hours of trying to reverse a bad transaction.

If you would like to **Purchase Katoosh Scan Detector™**: [Buy Now](#)

1. The 30-Second Safety Pause

Before taking action, stop and ask these five questions:

1. Who is really behind the offer?

Can you identify the seller, company, address, and customer-service contact information?

2. Can the important claims be verified?

Are the product benefits, endorsements, awards, certifications, discounts, or guarantees supported by credible independent evidence?

3. What happens after I pay?

Will you receive a one-time purchase, or will the seller continue charging you?

4. Can I recover my money?

Does the payment method offer buyer protection or chargeback rights?

5. Is the same product available elsewhere?

The advertised “exclusive” product may be a generic item sold by other retailers for much less.

Do not allow a countdown timer, limited-stock warning, threatening message, or pushy salesperson to make these decisions for you.

2. Common Online Scam Warning Signs

One warning sign does not automatically prove that an offer is fraudulent. However, several warning signs appearing together should make you cautious.

Pressure to Act Immediately

Be suspicious when an offer tells you:

- The sale ends in minutes
- Only one or two items remain
- Your account will be closed today
- You must pay before asking questions
- You cannot tell anyone about the opportunity
- You will lose a prize or refund unless you act now

Urgency is often used to prevent careful research.

A Price That Seems Too Good to Be True

An unusually low price may be used to attract buyers to:

- A fake store
- A counterfeit product
- A bait-and-switch offer
- A subscription trap
- A non-delivery scheme
- A seller collecting payment information

Compare the price with established retailers before purchasing.

Unclear Company Information

Watch for:

- No company name
- No physical address
- No customer-service telephone number
- Only a generic email address
- Contact details that appear on unrelated websites

- An address that belongs to a mailbox, residence, or unrelated business
- A website claiming decades of experience despite having little independent history

A legitimate company should make it reasonably easy to determine who is responsible for the offer.

Suspicious Website Address

Look carefully at the full website address.

Warning signs may include:

- Misspelled brand names
- Extra words or characters
- An unrelated domain name
- A link shortened to conceal its destination
- A checkout hosted on a different, unfamiliar website
- A web address that imitates a bank, retailer, delivery company, or government agency

The presence of HTTPS or a padlock means the connection is encrypted. It does not prove that the seller is trustworthy.

Poor or Inconsistent Content

Look for:

- Incorrect company names
- Unusual grammar
- Prices shown in different currencies
- Policies referring to another store
- Broken links
- Copied product descriptions
- Low-quality or inconsistent logos
- Customer reviews describing a different product

These problems may indicate a hastily assembled or copied storefront.

Unverifiable Reviews

Be careful when reviews:

- Appear only on the seller's website
- Use repetitive wording
- Lack meaningful details

- Were all posted within a short period
- Describe unrelated products
- Use generic customer photographs
- Claim nearly perfect satisfaction without independent support

Seller-controlled testimonials are advertising, not independent proof.

Celebrity or Expert Endorsements

Scammers and misleading advertisers may use photographs or videos of:

- Celebrities
- Doctors
- News presenters
- Government officials
- Business leaders
- Social-media influencers

Do not assume an endorsement is genuine because a familiar face appears in an advertisement.

Search for confirmation through the person's official website, verified social account, or credible news reporting.

Unusual Payment Methods

Use extra caution when an unfamiliar seller requests:

- Gift cards
- Cryptocurrency
- Wire transfers
- Zelle or another direct transfer
- Cash
- Friends-and-family payments
- Payment outside an established marketplace
- Remote access to your computer
- Banking passwords or verification codes

These payment methods may provide little or no buyer protection.

3. Suspicious Website Checklist

Use this checklist before buying from an unfamiliar website.

Mark each item **Yes**, **No**, or **Could Not Verify**.

Seller Identity

- ☐ The website clearly identifies the legal company or seller.
- ☐ The company name can be verified independently.
- ☐ A meaningful physical address is provided.
- ☐ A working customer-service email address is provided.
- ☐ A working customer-service telephone number is provided.
- ☐ The same company name appears consistently throughout the website.

Website Quality and Transparency

- ☐ The website address matches the company or store name.
- ☐ Important pages open correctly.
- ☐ Product descriptions appear original and consistent.
- ☐ The privacy policy identifies the company responsible for customer data.
- ☐ The terms and conditions identify the seller.
- ☐ The website does not redirect unexpectedly to unrelated domains.

Product Information

- ☐ The product has a clear brand or manufacturer.
- ☐ A model number or detailed specification is provided.
- ☐ Important claims can be independently verified.
- ☐ Certifications or approvals include enough information to confirm them.
- ☐ The seller explains exactly what is included.
- ☐ The photographs appear to show the actual product.

Reputation

- ☐ Independent reviews exist outside the seller's website.
- ☐ Reviews describe the correct product and company.
- ☐ No serious pattern of non-delivery complaints was found.
- ☐ No serious pattern of unauthorized-charge complaints was found.
- ☐ No major government or regulatory warning was found.

Checkout and Payment

- ☐ The total price is displayed before payment.
- ☐ Shipping charges are clearly disclosed.
- ☐ Taxes and processing fees are disclosed.
- ☐ The payment method offers buyer protection.
- ☐ The seller does not request payment outside the checkout system.
- ☐ The seller does not ask for unnecessary personal information.

Returns and Refunds

- ☐ The return period is clearly stated.
- ☐ The return address or return process is explained.
- ☐ The policy states who pays return shipping.
- ☐ Restocking or cancellation fees are disclosed.
- ☐ The policy explains which products cannot be returned.
- ☐ The refund promise matches the detailed return policy.

How to Interpret the Checklist

Several "No" or "Could Not Verify" answers do not automatically prove fraud.

They do mean that important questions remain unanswered.

The more uncertainty that involves seller identity, payment protection, recurring charges, delivery, or refunds, the greater the risk.

4. Hidden-Subscription Checklist

A low introductory price or free trial can become expensive when recurring charges are buried in the terms.

Before entering your card information, check for the following.

Look Near the Price and Order Button

- ☐ Does the offer say “trial,” “membership,” “club,” “plan,” or “continuity program”?
- ☐ Does the price apply only to the first shipment or first month?
- ☐ Is a future billing amount disclosed?
- ☐ Is the billing frequency disclosed?
- ☐ Is a checkbox already selected?
- ☐ Does clicking the order button mean you agree to recurring charges?

Read the Terms

- ☐ How long does the trial last?
- ☐ On what date will the first paid charge occur?
- ☐ How much will each future charge be?
- ☐ How often will you be charged?
- ☐ Will products be shipped automatically?
- ☐ Must you cancel before a particular date?
- ☐ Can cancellation be completed online?
- ☐ Is telephone cancellation required?

- ☐ Are there cancellation fees?
- ☐ Are previous charges refundable?
- ☐ Must unused products be returned?
- ☐ Who pays the return shipping?

Check the Final Checkout Page

Before paying, confirm that the checkout clearly shows:

- The amount charged today
- The amount charged later
- The billing frequency
- Shipping and handling
- Taxes
- Membership fees
- Trial-conversion terms
- Cancellation instructions

Take a screenshot of the offer, checkout total, and cancellation terms before submitting the order.

After Purchasing

Save:

- The advertisement
- The order confirmation
- The seller's name
- The total price
- The refund promise
- The subscription terms
- The cancellation instructions
- Customer-service messages
- Tracking information

Check your bank or card statement regularly for unfamiliar or recurring charges.

5. Safer Payment Guidance

The way you pay can affect your ability to recover money.

Credit Cards

Credit cards generally provide stronger dispute and chargeback options than many irreversible payment methods.

They may be preferable when purchasing from an unfamiliar seller.

Review your issuer's rules and deadlines because protection varies by card, transaction, and location.

PayPal Goods and Services

PayPal purchases may qualify for buyer protection when the transaction meets PayPal's requirements.

Confirm that:

- You are paying through an official PayPal page
- The seller and item description are correct
- The transaction is classified as a purchase
- You understand the dispute deadline
- You retain the receipt and seller communications

Do not use a friends-and-family payment for an ordinary commercial purchase.

Debit Cards

Debit-card payments may remove money directly from your bank account.

Dispute rights and timing can differ from credit-card protections. Contact your bank promptly if a transaction is unauthorized or the seller fails to deliver.

Established Marketplaces

A reputable marketplace may provide:

- Seller ratings
- Transaction records
- Delivery tracking
- Dispute procedures
- Purchase protection

Do not allow a seller to move the transaction outside the marketplace.

High-Risk Payment Requests

Avoid sending money to an unfamiliar seller using:

- Gift cards
- Cryptocurrency
- Wire transfer
- Cash
- Friends-and-family payment
- Direct account transfer
- Payment to an unrelated person
- A QR code from an unverified source

Never give anyone:

- Your banking password
- Your card PIN
- A one-time verification code
- Remote access to your device
- A cryptocurrency recovery phrase

A legitimate bank, government agency, retailer, or support representative should not need this information.

6. Price-Comparison Checklist

A product may be genuine but seriously overpriced.

Before buying, check:

- ☐ Is a brand name provided?
- ☐ Is a model number provided?
- ☐ Can the product photograph be found on other websites?
- ☐ Is an identical product sold by another seller?
- ☐ Is the product available through an established retailer?

- ☐ Is there a generic or white-label version?
- ☐ Does the manufacturer list a suggested retail price?
- ☐ Does the advertised discount compare with a real previous price?
- ☐ Are shipping costs included in the comparison?
- ☐ Do lower-priced alternatives offer better return protection?

Compare the Total Cost

Do not compare the product price alone.

Include:

- Shipping
- Taxes
- Processing fees
- Insurance
- Membership charges
- Required accessories
- Subscription renewals
- International return shipping

A slightly higher price from an established retailer may be safer when it includes reliable delivery, clear specifications, domestic returns, and meaningful buyer protection.

7. Emails and Text Messages

Treat an unexpected message cautiously when it claims to come from:

- Your bank
- A delivery company
- A government agency
- A retailer
- A streaming service
- A toll-road operator
- A utility company
- A relative
- A potential employer
- A customer-support department

Warning Signs

- The message creates fear or urgency
- You are told to click immediately
- The sender requests payment
- The sender asks for a password or verification code
- The link does not match the claimed organization
- You are told that you won a prize
- You are offered an unexpected refund
- You are threatened with arrest, account closure, or service interruption
- The sender asks to move the conversation to another platform
- The sender asks you to install software or provide remote access

Safer Response

Do not click the message link.

Instead:

1. Open the organization's official application.
2. Type its known website address into your browser.
3. Call the number on your card, statement, or official website.
4. Ask whether the message is genuine.

Do not use the contact details supplied in a suspicious message.

8. Job and Work-From-Home Offers

Be cautious when a job offer includes:

- An interview conducted only through text messages
- Immediate hiring without a meaningful interview
- Pay that is unusually high for simple work
- A request to purchase equipment from a designated supplier
- A check that you must deposit and partially return
- Upfront training, application, or processing fees
- Requests for banking information before employment is verified
- Requests to receive or forward packages
- Requests to transfer money
- A recruiter using a personal email address
- A company name that does not match the email domain

A legitimate employer should not require you to send part of a deposited check to another person.

Confirm the vacancy through the company's official website and contact the company using independently verified information.

9. Investment and Income Opportunities

Warning signs may include:

- Guaranteed profits
- Guaranteed returns
- Claims that no risk exists
- Pressure to invest immediately
- Secret trading systems
- Celebrity endorsements
- Screenshots of profits without verifiable records
- Requests for cryptocurrency
- Difficulty withdrawing funds
- Additional fees required to release your money
- Unlicensed or unverifiable operators
- Requests to recruit other participants

Do not invest because a promoter appears successful on social media.

Verify the person or company with the appropriate financial regulator in your country.

Never pay additional "taxes," "unlocking fees," or "withdrawal fees" to an unverified platform simply because an online account displays a profit.

10. What to Do If You Already Paid

Act promptly.

If You Used a Credit or Debit Card

Contact the card issuer using the number on the back of the card.

Explain:

- What you purchased
- When you paid
- The amount
- Why you believe the transaction is deceptive or unauthorized
- Whether the product was delivered
- Whether recurring charges are expected

Ask about blocking future charges and starting a dispute.

If You Used PayPal or a Marketplace

Open a dispute through the official transaction page.

Keep all communication inside the platform whenever possible.

If You Shared a Password

Change the password immediately.

Do not reuse the new password on other accounts.

Enable multifactor authentication where available.

If You Shared Banking Information

Contact your bank.

Ask whether your account, card, or online banking credentials should be changed.

If You Installed Software or Allowed Remote Access

Disconnect the device from the internet.

Contact a qualified computer-security professional.

Change important passwords using a different, trusted device.

Save Evidence

Keep copies of:

- Advertisements
- Website pages
- Emails
- Text messages
- Receipts
- Transaction records
- Seller communications
- Tracking information
- Screenshots
- Telephone numbers
- Usernames and account profiles

Report the seller or advertisement to the platform where you found it.

11. Introducing Katoosh Scan Detector™

Checking an unfamiliar offer can take time.

You may need to research:

- The seller
- The company
- The website
- Product claims
- Independent complaints
- Return policies
- Hidden subscriptions
- Payment risks
- Competing prices
- Safer alternatives

Katoosh Scan Detector™ helps organize this research inside ChatGPT.

It is a specialized custom GPT designed to investigate online offers and explain the available evidence in plain language.

What You Can Submit

Enter:

- A website URL

- A product page
- An advertisement
- A suspicious email
- A text message
- A seller or company name
- A subscription offer
- A job opportunity
- An investment promotion
- A screenshot
- A description of the situation

What You May Receive

Depending on the information available, Katoosh Scan Detector™ may produce a report containing:

- An overall verdict
 - A risk level
 - A confidence level
 - A summary of the offer
 - Evidence supporting legitimacy
 - Important warning signs
 - Company and website findings
 - Reputation and complaint findings
 - Product-price comparisons
 - Hidden costs or unfavorable terms
 - Safer alternatives
 - Recommended next steps
 - Sources supporting important findings
-

12. Katoosh Scan Detector™ Verdicts

Likely Legitimate

Strong available evidence supports the company and offer, with no serious unresolved warning signs.

Legitimate, but Use Caution

The offer may be genuine, but concerns remain involving claims, reviews, customer service, policies, pricing, or subscriptions.

Probably Overpriced

The product may be real, but the same or a substantially similar product appears to be available elsewhere for considerably less.

High Risk

Several significant warning signs are present. Do not proceed without additional verification and strong payment protection.

Likely Scam

Strong available evidence indicates fraud, impersonation, fabricated claims, non-delivery, unauthorized charges, or another deceptive practice.

Insufficient Evidence

Not enough reliable information was available to reach a responsible conclusion.

“Insufficient Evidence” does not mean the offer is safe. It means more verification is required.

13. How Katoosh Scan Detector™ Works

Step 1: Open Katoosh Scan Detector™

Use the access link supplied after your purchase.

Sign in to your ChatGPT account.

Step 2: Paste the URL or Describe the Offer

You can begin with a simple request:

Investigate this website and produce a complete Katoosh Scan Detector™ report:
[PASTE URL]

Step 3: Add Relevant Details

Include:

- The price
- Where you found the offer
- What the seller promised
- Why you are concerned
- Whether you have already paid
- Your country when shipping, pricing, or reporting options matter

Step 4: Review the Report

Read the verdict, strongest warning signs, price comparison, hidden terms, and recommended action.

Open and review the supporting sources before making an important decision.

Step 5: Ask Follow-Up Questions

Examples:

- What are the three strongest warning signs?
- Is this product available for less?
- Explain the refund policy in plain language.
- Is the company address genuine?
- Could this be a hidden subscription?
- What payment method offers better protection?
- What should I verify before purchasing?
- Summarize the findings for a family member.

14. Example Requests

Website Investigation

Investigate this website. Identify the seller, check its company information, search for complaints, examine its policies, and tell me whether it appears safe to buy from: [PASTE URL]

Product and Price Investigation

Investigate this product. Verify the important claims and find out whether the same or a similar product is available from another seller for less: [PASTE URL]

Subscription Investigation

Review this offer for automatic renewals, trial conversions, recurring charges, cancellation restrictions, and refund problems: [PASTE OFFER]

Suspicious Message Investigation

Examine this message for phishing, impersonation, payment fraud, or identity-theft warning signs. Tell me what I should do next: [PASTE MESSAGE]

Complete Investigation

Produce a complete Katoosh Scan Detector™ Scam Investigation Report. Include the verdict, risk level, confidence level, legitimacy evidence, warning signs, company findings, complaint research, price comparison, hidden terms, safer alternatives, recommended actions, and sources.

15. Ready to Investigate an Offer?

The safest time to research an offer is before you pay.

Katoosh Scan Detector™ allows you to enter your own website URLs, advertisements, products, messages, sellers, subscriptions, and suspicious claims inside ChatGPT.

Get Access to Katoosh Scan Detector™

[INSERT YOUR PAYPAL PURCHASE LINK HERE]

After purchasing, you will receive:

- Access to the Katoosh Scan Detector™ custom GPT
- Quick-start instructions
- Ready-to-use investigation prompts
- Structured scam-investigation reports
- Company and seller research
- Complaint and reputation checks
- Price-comparison assistance
- Hidden-cost and subscription analysis
- Safer alternatives and recommended next steps

Before You Click, Ask Katoosh Scan Detector™

Paste the link.

Describe the offer.

Review the evidence.

Make a better-informed decision before you buy, subscribe, invest, respond, or send money.

Important Consumer Notice

Katoosh Scan Detector™ is an AI-assisted consumer-research and education tool.

It cannot guarantee that every scam, misleading claim, future complaint, hidden charge, security threat, counterfeit product, or deceptive practice will be identified. Information may be incomplete, unavailable, outdated, or incorrect. AI-generated responses can also contain errors.

A favorable assessment does not guarantee:

- Delivery
- Product quality
- Safety
- Customer service
- Investment performance
- Refund eligibility
- Future business conduct
- Protection from unauthorized charges

Users should review cited sources and independently verify important financial, legal, medical, cybersecurity, and other high-impact decisions.

Katoosh Scan Detector™ does not replace assistance from a bank, card issuer, attorney, financial adviser, medical professional, cybersecurity professional, regulator, consumer-protection agency, or law-enforcement authority.

Katoosh Scan Detector™ is an independent custom GPT designed to operate inside ChatGPT. It is not endorsed by or affiliated with OpenAI.

ChatGPT is a trademark of OpenAI.

A signed-in ChatGPT account is required to use a GPT. Availability, plans, features, and usage limits are controlled by OpenAI and may change. Access to Katoosh Scan Detector™ does not include a paid ChatGPT subscription.

Contact and Copyright

Customer support: support@katoosh.com

Website: <https://ht-tp.com/katoosh-scam-detector/>

Purchase Katoosh Scan Detector™: [Buy Now](#)

© 2026 Katoosh Scan Detector™. All rights reserved.

Before You Click, Scan the Offer.