Shopping Tips

- Check the online retailer's rules about refunds and returns, along with what happens if there's a problem with the purchased item.
- Pay with a safe payment method. For example, credit cards, or secure online payment systems, offer additional protections.
- If a seller requires payment via wire transfer, gift card or cryptocurrency, stop and find another seller. Scammers often prefer these payment methods because they are difficult to track.
- When shopping on secondhand sites, don't buy from a seller that requests payment from a source different from the site's system. If a consumer does this, the marketplace's protections from fraud are lost and the customer probably won't receive the item and won't be eligible for a refund.
- When selling items online, never accept more than the agreed purchase price.
- If shopping with a new retailer, check with the Better Business Bureau to determine whether other customers have filed complaints.

Florida Attorney General's Office
Scams at a Glance:

E-Commerce Cons

Visit MyFloridaLegal.com to find consumer tips or to file a complaint. By remaining vigilant and informed, savvy consumers can help us build a Stronger, Safer Florida.

Report fraud by calling
1-866-9-NO-SCAM
(1-866-966-7226)

View other Scams at a Glance resources at:
MyFloridaLegal.com/ScamsAtAGlance

Attorney General Ashley Moody
Office of the Attorney General
PL-01 The Capitol
Tallahassee, Florida 32399
MyFloridaLegal.com

Scams at a Glance:
E-Commerce Cons

OFFICE OF
ATTORNEY GENERAL
ASHLEY MOODY
Stronger, Safer Florida

Online shopping is a convenient way to get great deals without leaving the comfort of your home. But as you browse the web, beware of scammers looking to take advantage of you, obtain your personal information and leave you vulnerable to financial losses. As technology is advancing, knowing about these schemes will help you stay safe from E-Commerce Cons.

Non-Delivery Scams ???

There are two types of non-delivery scams involving online purchases: when a seller takes payment but has little to no contact with the purchaser and never delivers the product and when a scammer casts a wide net of shipping-error emails to try and trick consumers usually after the consumer has paid.

In the first case, a scammer may provide a fake tracking number and ignore contact attempts by the consumer—stealing the money.

In the second case, a scammer will send a shipping error email claiming that information needs to be updated for the product to be correctly delivered—all to steal personal and financial information and money.

To avoid a delivery scam, research the seller's reputation and read reviews from other customers. Use established, reputable online-marketplace services and consider using escrow services or payment options that hold funds until you receive the product.

Phishing Emails

Scammers often use emails to trick targets into giving personal information or installing malware on a device. What may look like a legitimate email from a well-known retailer asking to verify personal information to resolve an account issue, could actually be a phishing email from a fraudster.

Be cautious when someone sends an email requesting personal information or urges you to take immediate action. Check the sender's address for suspicious variations or misspellings of the company name or web address. Instead of clicking on links in emails, manually type the retailer's website address in the browser.

Identity Theft

Identity theft occurs when someone uses, or attempts to use, personal information of another person to commit fraud. When shopping online, providing your information to an imposter website or scammer posing as a customer service representative can lead to identity theft. Criminals use victims' information to open accounts and make fraudulent purchases.

When shopping online, only share personal information on secure websites. A secure website will have "https" or a padlock symbol in the URL address bar. Be skeptical of unsolicited requests for personal information via email. Regularly monitor financial statements and credit reports for suspicious activity. Request a free credit report through the government-authorized website AnnualCreditReport.com.

Fake Online Stores

If an online store offers heavily discounted prices on popular items like electronics or designer items, the retailer may be fake. If purchasing from a fake website, the customer may receive counterfeit or substandard goods—or worse, no product at all. If a deal appears too good to be true, it almost always is.

Research the company and check for reviews, ratings and complaints on the Better Business Bureau's website, www.BBB.org. Verify the store's contact information, including the physical address and phone number. If deciding to make a purchase, use a credit card since it may offer better consumer protection.

Overpayment Scams

An overpayment scam targets sellers through online ads or auctions. A scammer purchases the item but sends a payment for more than the agreed-upon asking price, then requests a refund for the overpayment. The seller returns the funds, but the original payment method turns out to be fraudulent. In some cases, the seller loses both the item and the funds.

When selling online, independently verify the information of your buyer. Never agree to accept a payment, especially a check, for more than the selling price and always verify the authenticity of payments before issuing any refunds. Use secure payment platforms that offer sellers protection for online transactions.