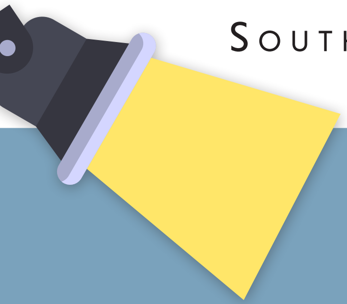
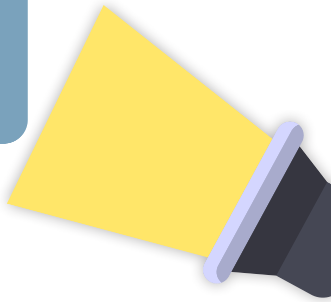
South Carolina Department of Consumer Affairs

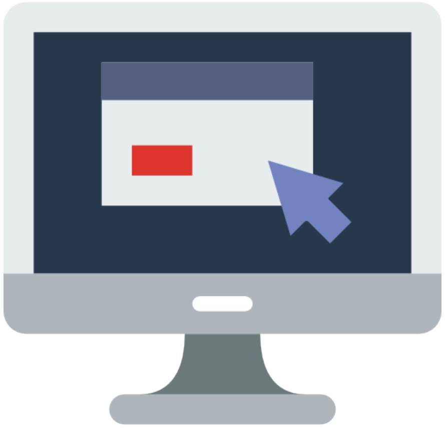


SPOTLIGHT: SHOPPING SCAMS



DON'T BE FOOLED BY A GOOD-LOOKING WEBSITE

Here are a few tips to keep in mind to avoid scams as you shop online:



WEBSITES ARE EASY TO CREATE

Just because a website looks good doesn't mean it's real. Scammers often use a name similar to a real business. Do your homework before you hand over your financial information. Check SCDCA's complaint portal, the Better Business Bureau's complaints and search for reviews of the company too.

IF IT SEEMS TOO GOOD TO BE TRUE, IT PROBABLY IS.

If you see a product advertised online with a rock-bottom price compared to its suggested retail price, it's a huge red flag of a scam. You can find good deals by comparison shopping, but be wary of deeply discounted prices.

KNOW THE SIGNS OF A FAKE

Be suspicious of website URLs registered within the last six months. You can search any sites domain registration through the Whois Public Internet Directory. If a website has pictures and information that are copy-and-pasted from other websites, or the sites are advertised on social media, this could be a sign it's fake.

PAY WITH A CREDIT CARD IF POSSIBLE.

▪A Credit card offers more consumer fraud protections than a debit card. There are laws to limit your liability for fraudulent credit card charges, but you may not have the same level of protection for your debit cards. Keep a record of your purchases and copies of confirmation pages, and compare them to your bank statements. If there is a discrepancy, report it immediately.

▪Debit cards are linked to bank accounts. A thief using your debit card number can drain your bank account before you even notice it. With a hijacked credit card number, while your available credit may be affected, your pocketbook is unchanged.

TIPS TO STAY SAFE WHILE SHOPPING ONLINE

USE REPUTABLE, ESTABLISHED WEBSITES

Before providing any personal or financial information, make sure that you are interacting with a reputable, established business. Some attackers may try to trick you by creating malicious websites that appear to be legitimate, so pick online stores that you already trust or have previously visited before providing any personal or financial information.

MAKE SURE YOUR INFORMATION IS BEING ENCRYPTED

Look for a closed padlock icon and Uniform Resource Locator (URL) that begins with "https:" instead of "http:". Use unique, strong passwords for each of your accounts and multi-factor authentication where possible to verify your identity. Keep your software up to date.

BEWARE OF PHISHING ATTEMPTS

Some cyber thieves may pose as retailers in emails or text messages. Don't click on links or download attachments unless you are sure where the message came from.

CHECK THE PRIVACY POLICY

Before providing personal or financial information, check the website's privacy policy. Make sure you understand how your information will be stored and used.

KNOW THE RETURN POLICY

Review return and exchange policies before you check out, especially if you are purchasing items that often have a restocking fee, like computers.

VICTIM OF AN ONLINE SHOPPING SCAM?

- File a scam report with SCDCA by visiting consumer.sc.gov or call (800) 922-1594.
- Report the fraudulent or suspicious activity to the service you bought the product on, the online payment service and your bank. If possible, direct your bank to stop or reverse any transactions.
- If the fraudster posed as a legitimate business, contact them to make the real company aware of the scam.

For more information on protecting yourself from identity theft, visit consumer.sc.gov and click Identity Theft/Scams.

South Carolina Department of Consumer Affairs
293 Greystone Blvd., Ste. 400 • PO Box 5757 • Columbia, SC 29250
(800) 922-1594 •consumer.sc.gov