



Online Shopping Safety Tips for the Holiday Season

Holly jolly spending season is sneaking up fast. Shopping for gifts online makes it easy to compare prices, find the best deals, and have packages delivered right to your front door. Convenience is king, but you'll want to be sure that your purchases arrive on time, the quality is what you expect, and that there is a way to make returns or get support with any issues you may have. This can be a hectic time for some, creating the perfect opportunity for fraudsters to take advantage of busy, distracted, and overwhelmed consumers. Don't get Scrooged! Check out these tips to improve the ease, security, and safety of your online shopping experience.

Make sure the shopping site is secure. Especially before entering any personal or payment information. The easiest way to tell is by looking for "https," not just "http," at the beginning of the merchant's web address. That little 's' tells you that all communication between your browser and the website is encrypted and secure, using a security certificate. All legitimate shopping sites will begin with "https" for your protection.

Avoid deals that are "too good to be true." Be wary of those incredible deals you see while scrolling through Facebook or Instagram. While it may be enticing, don't click any link associated with these offers. Fraudsters create fake ads that appear genuine, and they're trying to trick you into "purchasing" an item. The associated webpage looks real enough, but once you submit your payment information, they've got your credit or debit card information. Instead, go directly to the merchant's legitimate site using your web browser. If the offer is real, you can make your purchase there.

Check the shipping terms and return policy. Excessive shipping fees can turn the deal of a lifetime into an expensive mistake. Shop with merchants who provide tracking information and optional shipping insurance. And, be wary if your purchase won't ship within 10 business days.

It's also best practice to review the merchant return policy before making a purchase. Look for detailed points, including:

- how to initiate a return,
- the time frame allowed for returns,
- accepted items and exclusions,
- item condition requirements,
- how you'll be reimbursed,
- an estimated timeline for reimbursement,
- applicable return fees or restock fees, and
- contact information.

Use strong passwords. Setting up an account with an online retailer may offer a rewards program, and it definitely makes future purchases fast and easy. More often than not, your address and preferred payment information is saved to your account profile. Be mindful to create a strong password that contains both upper-case and lower-case letters, numbers, and special characters. Each online account should have its own unique password as well.

Don't share more information than necessary. You'll be required to supply an address and payment information when making an online purchase. But, if providing your phone number or other information is optional, then skip those fields. Remember, the more you put out there, the more accessible you become to fraudsters. It's also wise to read the retailer's privacy policy to learn where and how your information will be shared.

Use a credit card or payment service. When shopping online, use a credit card or payment service, like PayPal. A debit card is linked to your checking account, and you're at a much higher risk if that payment information is hacked or stolen. Credit cards offer more protection and less consumer liability if the information is compromised and used for unauthorized purchases. This is one time when it's actually smart to "charge it."

Important reminder: Account fraud and identity theft cases spike during the holiday season. So as a final reminder, **we will never contact you via phone call, email, or text message requesting personal identification or account information.** This includes Social Security numbers, account numbers and passwords, and any other personal confidential information. We will ask out-of-wallet questions to identify members who initiate the contact and reach out to us, concerning their accounts.