SECURITYSTUDIO®

#MissionBeforeMoney – https://securitystudio.com

2020 Online Holiday Shopping Safety Checklist

Instructions:

1. Print a copy of this checklist for yourself and post it next to (or on) your computer.
2. Follow the checklist.
3. Share this checklist with others.

This checklist is organized into sections (**MANDATORY** and **OPTIONAL**) and subsections (**BEFORE** shopping, **WHILE** shopping, and **AFTER** shopping). If you need help with any of this, tell us! Contact SecurityStudio at info@securitystudio.com.

MANDATORY

The following checklist items are mandatory, MUST follow requirements.

BEFORE providing any information on a shopping website:

☐ **STOP** for a second and ask yourself if there's anything that seems unusual.

☐ **ALWAYS** double-check the URL (web address) in your browser.

Make sure there's nothing sneaky or unusual like a typo or funky name. Pay special attention to uppercase "I" (the 9th letter in the alphabet) used in place of a lowercase "l" (the 12th letter in the alphabet) and the like.

☐ **DO NOT** buy anything from an unfamiliar retailer without confirming legitimacy.

If you can't confirm legitimacy, go somewhere else. Ways to confirm legitimacy are through online reviews, a few Google searches, and/or scanning through their website. Telltale signs for illegitimacy are no/missing physical address, no/missing contact phone number, and/or shoddy (or missing) policies (privacy, return, etc.).

☐ **DO NOT** rush, especially when jumping at the lowest price.

Take your time and think a little. Maybe step away from the computer for a second or two and grab a cup of coffee. MMMMM coffee!

☐ **NEVER** make purchases on public Wi-Fi.

Of course, a virtual private network (VPN) can help, but shopping from your own network is always a better idea.

WHILE shopping online:

☐ **DO NOT** shop from third-party apps.

If you're shopping from a mobile device, use the official retailer app (preferred) or the built-in web browser.

☐ **DO NOT** save your credit card information in your online shopping accounts.

It might be convenient, but how hard is it to reach into your back pocket (or purse) to pull out your credit card? If you've already saved credit card information in an online shopping account, go delete it now.

☐ **ALWAYS** ship to a secure location.

Unattended packages left sitting on a doorstep are prime targets for theft.

☐ **ALWAYS** use strong passwords for online shopping accounts **and** use a password manager.

Crappy passwords are certain to get your information compromised, and life without a password manager is more miserable than it should be. If multi-factor authentication is available from the retailer, even better. Use it.

☐ **NEVER** give retailers anything more than they need.

Retailers only need information to 1) process your transaction, 2) get your product to you, and 3) get in touch with you. This means payment information, addresses (shipping/billing) and contact information only. Retailers don't ask for Social Security Numbers (or God help us, they shouldn't)!

☐ **ALWAYS** read the information on retailer webpages, paying special attention for any checkboxes.

You could be opting in for something you didn't want to opt in to.

☐ **ALWAYS** buy with credit cards, NOT debit cards.

There's better protection for credit cards in case something goes wonky.

AFTER shopping online:

☐ **ALWAYS** check your financial accounts on a regular and periodic basis, like **ALL** of them.

You should be doing this all the time, not just during the holiday shopping season. Early detection can significantly limit your losses and frustration.

OPTIONAL

These are things you should consider for additional protection.

☐ **USE** Apple Pay or Google Pay.

These payment transactions are more secure than traditional payment card transactions. Your card data is never shared with retailers, only tokenized data.

☐ **USE** a virtual private network (VPN).

All the time or whenever you do anything sensitive online (like accessing your bank account, accessing medical information, buying stuff, etc.).

☐ **CHECK** security policies on retailer web sites.

Look for and read the privacy policy, return policy, etc. If the retailer doesn't have any policies posted and easily accessible, maybe you should think twice before buying.

☐ **USE** prepaid debit cards.

If the card is compromised, your loss is limited by the limit on the card, not your entire bank account.

☐ **USE** SecurityStudio's **FREE** **S²Me** to learn how to secure yourself (and your family) better.

Good information security stems from good habits, and habits are formed over time. SecurityStudio is here to help, with no strings attached. Visit: https://s2me.io today.

About SecurityStudio: https://securitystudio.com