FRSecure Online Holiday Shopping Safety Checklist

Holiday Shopping Scams: Some Things Never Change, But Some Do

First, what matters most. We wish you and your loved ones a safe, health, and happy holidays! Thanksgiving generally marks the start of the holiday season. It's tradition for many American families to get together with family and friends, stuff ourselves with more food than we thought possible, take a nap, then scour the newspaper (or internet) for great holiday shopping deals.

2020 is different.

This year many of us will be separated from family as COVID-19 continues to ravage what was a "normal" and traditional lifestyle. Sure, we'll still eat, nap, and shop. We'll just do it differently this year.

Sadly, shopping scams will not be different. What is supposed to be a time for joy, love, and hope should not become a time for worry, fear, or scams.

Don't let scammers steal ANY of your joy this holiday season!

Scammers are given a prime opportunity to cash in on our busy lives, poor habits, and inadvertent mistakes. It's not just consumers who fall prey either, it's the people we do business with too.

How Is Holiday Shopping Different in 2020?

This year is a perfect storm for scammers. Opportunities for the scammers have never been greater and neither has our level of distraction. The math looks a little something like this:

Opportunity + Distraction = Success

Increased opportunity or distraction means more success for scammers. Increase both at the same time, and it's the best-case scenario for them (worst case scenario for us).

More Opportunity Than Ever (for Scammers)

2019 was a record-breaking year for overall holiday spending ($730 billion), online holiday spending ($135.35 billion), and mobile retail sales ($71.3 billion). The best opportunity for scammers is online transactions because there are more potential victims in a single attack—a better return on their investment.

Online holiday shopping has increased every year since it became a reality, but this year could witness an explosion, especially with the second wave of COVID lockdowns.

eMarketer, a leading market intelligence firm is predicting a 35.8% sales increase to $190.47 billion. https://www.emarketer.com/content/us-holiday-ecommerce-sales-will-surge-35-8-190-47-billion-offsetting-brick-and-mortar-declines

Less Attention Than Ever (from Consumers)

People are distracted. There are thousands (maybe millions) of impactful things going on all around the world seemingly at the same time. From COVID-19, to election controversies, to social justice issues, to online schooling and work from home, etc. It might be safe to say people are more distracted this holiday season than in any holiday season past.

Nobody is more responsible for your protection more than you are, though. The equation for protection is a simple one.

Awareness + Habits = Protection

This holiday season we're not just into protecting our money, we're also into protecting our safety and joy.

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, contact FRSecure at info@frsecure.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" used in place of a lowercase "l" and the like.
- ☐ **DO NOT** buy anything from any unfamiliar retailer without confirming it's legitimate.
  If you can't confirm legitimacy, go somewhere else. Ways to confirm legitimacy is through online reviews, a few Google searches, and scanning through their website. Telltale signs for illegitimacy are missing physical addresses, lack of a 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, 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.

FRSECURE

While Shopping Online:

- [ ] **DO NOT** shop from third-party apps.
If you're shopping from a mobile device, either use the official retailer app (preferred) or the built-in web browser.

- [ ] **DO NOT** save your credit card information in any of your online shopping accounts.
It might seem 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 any online shopping account, go delete it.

- [ ] **ALWAYS** ship to a secure location.
Unattended packages left sitting on your doorstep are a prime target for theft.

- [ ] **ALWAYS** use strong passwords for all 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 things like Social Security Numbers!

- [ ] **ALWAYS** read the information on the web pages, paying special attention for any check-boxes.
You could be opting in for something you really 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—ALL of them.
You should be doing this all the time—not only during the holiday shopping season. Early detection can significantly limit 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.

FRSECURE

- [ ] **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.

—

It's FRSecure's mission to fix the broken information security industry, so we feel it's important to provide resources like this. For other resources about personal and business security, head to frsecure.com/resources, and don't hesitate to reach out with any questions!