14 Tips for Safe Holiday Online Shopping

Holiday shopping online can be irresistible. This year, 83 percent of U.S. consumers plan to shop online for holiday gifts, according to a Coresight Research report. What's not to love? You make a list, check it twice, then go wild. Such joy. Until you land on a bogus retail website or your *credit card information gets swiped.* Here's the gift you can really use: tips for safer holiday online shopping. Why? Consider this: In 2017, the FBI's Internet Crime Complaint Center received nearly 300,000 online-theft complaints. Victims reported losses totaling $1.4 billion. That'll put a dent in your budget. Meanwhile, online shopping is forecast to boom during the 2018 holiday season, according to eMarketer, a research company that provides insights related to commerce and marketing in the digital world. Here's what the agency predicts for November 1 to December 31, when nearly a quarter of annual online buying happens.

- Total holiday sales: $986 billion
- Online holiday sales: $123 billion
- Online percentage of total sales: 12.5%
- Online holiday sales growth (vs. 2017): 16.2%

Don't let fake companies and identity thieves dampen your holiday spirit. Before you click the 'Buy' button this holiday season, check out these tips to help you enjoy safer online shopping.

1. Shop at websites you trust: Expect a record for online holiday spending this year. But shopping IRL — in real life — offers one advantage: you can usually be sure the business and the inventory exist. On the web, some businesses are fabricated by people who *just want your credit card information* and other personal details. To play it safe, consider doing online business only with retailers you trust and have shopped with before.

2. Check out the business: Did you find the perfect gift on an unfamiliar website? Break out your detective skills whenever you want to buy something from a new merchant. Does the company interact with a social media following? What do its customer reviews say? Does it have a history of scam reports or complaints at the Better Business Bureau? Take it one step further by contacting the business. If there's no email address, phone number, or address for a brick-and-mortar location, that could be a signal that it's a fake company.

3. Beware rock-bottom prices: Black Friday, Cyber Monday, and other big sales along the way have become a tradition of holiday shopping. But if a website offers something that looks too good to be true, then it probably is. Compare prices and pictures of the merchandise at similar websites. Rock-bottom prices could be a red flag that the business doesn't have those items in stock. The website may exist only to get your personal information. Bah humbug!

4. Avoid public Wi-Fi: You might be tempted to take your shopping spree to a coffee shop for a cup of joe. Keep in mind, Wi-Fi networks use public airwaves. With a little tech know-how and the freely available Wi-Fi password at your favorite cafe, someone can intercept the data you send and receive while on free public Wi-Fi. Shopping online usually means giving out information that an identity thief would love to grab, including your name and credit card information. Bottom line: It's never a good idea to shop online or log in to any website while you're connected to public Wi-Fi.

5. Use a VPN: Still can't resist the lure of shopping online while sipping that peppermint latte? If you must shop online on public Wi-Fi, consider installing and using a VPN — short for "virtual private network" — on all mobile devices and computers before connecting to any Wi-Fi network. A VPN creates an encrypted connection between your smartphones and computers and the VPN server. Think of it as a secure tunnel your Internet traffic travels through while you browse the web, making your data safer from interception by nearby hackers.

14 Tips for Safe Holiday Online Shopping

6. Create strong passwords: If someone has the password to your account, they can log in, change the shipping address, and order things while you get stuck with the bill. Help keep your account safe by locking it with a strong password — "Santa123" won't do. Here are some tips on how:

- Use a complex set of at least 10 lowercase and uppercase numbers, letters, and symbols.
- Don't use personal information that others can find or guess, such as birthdates, your kids' names, or your favorite color.
- Don't use the same password — however strong — on multiple accounts. A data breach at one company could give criminals access to your other, shared-password accounts.

7. Check out website security: That small lock icon in the corner of your URL bar tells you that the web page you're on has privacy protection installed. The URL will start with "https." These websites mask any data you share, typically on pages that ask for passwords or financial information. If you don't see that lock or the "s" after "http," then the webpage isn't secure. There is no privacy protection attached to these pages, so we suggest you exercise caution before providing your credit card information over these sites.

8. Watch out for email scams: Sometimes something in your email in-box can stir your holiday consumer cravings. For instance, it might be tempting to open an email that promises a "special offer." But that offer could be special in a bad way. Clicking on emails from unknown senders and unrecognizable sellers could infect your computer with viruses and malware. It's better to play it safe. Delete them, don't click on any links, and don't open any attachments from individuals or businesses you are unfamiliar with.

9. Don't give out too much information: No shopping website will ever need your Social Security number. If you're asked for very personal details, call the customer service line and ask whether you can supply some other identifying information. Or just walk away and find a better-known, accommodating website for your holiday buys.

10. Pay with a credit card: Attention, holiday shoppers: You'll usually get the best liability protection — online and offline — when you use a credit card. Here's why. If someone racks up unauthorized charges on your credit card, federal regulations say you won't have to pay while the card company investigates. Most major credit cards offer $0 liability for fraudulent purchases. Keep in mind, your liability for unauthorized charges on your debit card is capped at $50, if you report it within two business days. But if someone uses your account and you don't report the theft, after 60 days you may not be reimbursed at all.

You can also try a virtual credit card. Some banks offer this nifty tool that acts like an online version of your card. With a virtual credit card, the issuer will randomly generate a number that's linked to your account, and you can use it anywhere online and choose when the number expires. It might be best to generate a new number every time you buy something online, or when you shop with a new retailer. Anyone who tries to use that number will be out of luck.

11. Check your statements: Robust holiday shopping can add pages to your credit card statements. Check your statements for fraudulent charges at least once a week, or set up account alerts. When you receive a text or email about a charge, you can check the message and likely easily recall whether you made the charge.

12. Mind the details: The holiday season is a busy time, but it's smart to stay organized. After you make the purchase, keep the receipt, order confirmation number, and postal tracking number in a safe place. If you have a problem with the order, this information will help the merchant resolve the problem.

13. Take action if you don't get your goods: Call the merchant and provide the details noted in Tip 12. If the merchant turns out to be fake, or they're just plain unhelpful, then your credit card provider can help you sort out the problem. Often, they can remove the charge from your statement.

14. Report the company: This is no time for holiday cheer. If you suspect the business is bogus, notify your credit card company about the charge and close your account. File a complaint with the U.S. Federal Trade Commission. The FTC offers an identity theft recovery plan, should you need it.