

HOLIDAY SHOPPING SCAM SURVIVAL

THE DEALS ARE FAKE. HERE'S HOW TO TELL

THE 5 NOVEMBER CLASSICS:

- 01** THE 80%-OFF AD. A brand you know, a price that hurts to skip, a site you've never heard of. The product never ships, and now they have your card.

THE CHECK: search the brand name plus "official site." Buy there or nowhere.

- 01** THE DELIVERY TEXT. "Your package needs a fee / address update." You're expecting packages, so you tap. That's the whole trick.

THE CHECK: no tracking number, no package. Track only on the site you bought from.

- 01** THE GIFT CARD DRAINER. Racks of gift cards with tampered backs, codes already photographed. You load it, they drain it.

THE CHECK: take cards from the middle of the rack, confirm the scratch strip is intact, keep the receipt.

- 01** THE CHARITY THAT APPEARED YESTERDAY. Tugging names, no history.

THE CHECK: give.org or charitynavigator.org before a dollar moves.

- 01** THE "YOUR ACCOUNT IS LOCKED" RUSH. Amazon, PayPal, your bank, all suddenly locking accounts the week you're spending most.

THE CHECK: never the link. Open the app yourself.

The one rule that survives December: if you didn't start the conversation, don't finish it.

This sheet is the 5 classics. The Holiday Shopping Scam Survival Kit (\$7.99) covers the full season: marketplace scams, charity vetting, holiday card security, and the return-fraud scams that hit in January.

→ rexcalloway.com/shop

Disclaimer: Educational content only. Not financial, legal, tax, or professional cybersecurity advice. No professional-client relationship is created. Consult a qualified professional for your specific situation. Full disclaimer at rexcalloway.com/disclaimer.