8 CHECKS BEFORE YOU ENTER YOUR CARD NUMBER.

01. CHECK THE URL. Always starts with https:// with a padlock. The URL should match the real brand exactly. amazon.com is not amazon-deals.net.

02. USE CREDIT, NOT DEBIT. Credit cards carry federal fraud protection. Debit cards drain your actual bank account. Use a credit card or a virtual card number.

03. AVOID PUBLIC WI-FI. Never enter payment info on public wifi. Use mobile data, or wait until you're home. If you must, use a VPN first.

04. LOOK UP THE SELLER. Unknown store? Search "[store name] reviews scam" before buying. Check Trustpilot, the BBB, and Reddit. Only 5-star reviews? Be suspicious.

05. CHECK THE RETURN POLICY. Legitimate stores have clear return policies. Can't find one, or it's vague? Walk away.

06. USE VIRTUAL CARD NUMBERS. Services like Privacy.com generate single-use card numbers. Even if the merchant gets hacked, your real card stays safe.

07. WATCH FOR FAKE REVIEWS. Look for verified-purchase reviews only. A sudden flood of 5-star reviews right after bad ones is a red flag.

08. MONITOR YOUR STATEMENT. Check your card statement within 48 hours of purchase. Fraudulent charges often start small, a dollar or two, before a larger hit.

Eight checks, thirty seconds each, done before you type a single digit.

→ rexcalloway.com/free-tools
