Online Shopping Security Checklist

Chapter 8.2: Online Shopping

This checklist provides a comprehensive guide to safe online shopping. Use it before, during, and after making online purchases to protect your personal and financial information. Check off each item as you complete it to ensure you're following all recommended security practices.

Before You Buy

- [ ] **Research the retailer's reputation**
  Search for reviews of the company (not just the product). Look for patterns in customer experiences and complaints.

- [ ] **Verify how long the website has been operating**
  Use tools like "WHOIS" lookup or search "[company name] how long in business" to check if it's a new, potentially untrustworthy site.

- [ ] **Confirm the company has a physical address and phone number**
  Look for an "About Us" or "Contact" page with verifiable information. Be wary if only an email address is provided.

- [ ] **Check that the website URL begins with "https" (not just "http")**
  The "s" stands for secure and indicates that your connection to the site is encrypted.

- [ ] **Verify the padlock icon appears in your browser's address bar**
  This indicates the site has a security certificate and your information will be encrypted.

- [ ] **Use a secure internet connection**

Avoid shopping on public Wi-Fi networks. If necessary, use a VPN (Virtual Private Network) for added security.

- [ ] **Use strong, unique passwords for shopping accounts**
  Create different passwords for different shopping sites. Consider using a password manager.

- [ ] **Be skeptical of deals that seem too good to be true**
  Compare with standard retail prices. Extreme discounts (like 80-90% off) are often signs of counterfeit products or scams.

- [ ] **Read the return policy before purchasing**
  Understand the timeframe for returns, who pays return shipping, and any restocking fees.

- [ ] **Check for customer service options**
  Verify multiple ways to contact the company (email, phone, chat) in case issues arise.

During Purchase

- [ ] **Use secure payment methods**
  Credit cards generally offer better fraud protection than debit cards. Consider using digital wallets (PayPal, Apple Pay, Google Pay) for added security.

- [ ] **Never use wire transfers or cash-equivalent methods**
  Avoid payment methods like Western Union, MoneyGram, cryptocurrency, or gift cards when purchasing from unfamiliar retailers.

- [ ] **Only provide necessary information**
  Be suspicious if a site asks for excessive personal details. Your Social Security number is never needed for standard purchases.

- [ ] **Check for security indicators during checkout**
  Look for trusted payment processor logos, security badges, and encryption symbols.

- [ ] **Verify the total cost including shipping, taxes, and fees**
  Make sure there are no unexpected charges added at checkout.

- [ ] **Review your order details before final submission**

Check shipping address, product details, quantity, and total cost on the order review page.

- [ ] **Save or screenshot the order confirmation page**

  Keep a record of your order number, purchase details, and confirmation.

- [ ] **Save confirmation emails and receipts**

  Keep all transaction records in a dedicated folder in your email or computer.

After Purchase

- [ ] **Track your packages**

  Use provided tracking numbers to monitor delivery status. Take screenshots of tracking updates if possible.

- [ ] **Report any suspicious delivery updates immediately**

  Contact both the retailer and shipping company if tracking shows unexpected changes.

- [ ] **Check your credit card and bank statements regularly**

  Review for unauthorized charges or duplicate charges from your purchase.

- [ ] **Report suspicious activity immediately**

  Contact your credit card company or bank at the first sign of unauthorized charges.

- [ ] **Inspect delivered items promptly**

  Check that products match description and are in good condition. Document any issues with photos.

- [ ] **Initiate returns promptly if needed**

  Follow the retailer's return process within the specified timeframe. Keep all return shipping receipts and confirmation numbers.

- [ ] **Document all communication with the retailer**

  Keep records of all emails, chat logs, or phone calls regarding your purchase, especially for issues or returns.

- [ ] **Leave honest feedback about your experience**

  Help other shoppers by reviewing both the product and the retailer.

Red Flags to Watch For

- [ ] **Website has numerous spelling and grammar errors**

  Professional retailers maintain professional websites. Poor grammar may indicate a fraudulent site.

- [ ] **No privacy policy or terms of service**

  Legitimate retailers will always have these legal documents available on their site.

- [ ] **Limited or suspicious contact information**

  Be wary if the only contact method is a generic email address (like gmail.com or hotmail.com).

- [ ] **Prices that are dramatically lower than all other retailers**

  If a deal seems too good to be true, it probably is—especially for luxury or high-demand items.

- [ ] **Requests for payment via wire transfer, gift cards, or cryptocurrency**

  These payment methods offer little to no consumer protection and are rarely used by legitimate retailers.

- [ ] **Website URL that's slightly different from a popular brand**

  Check carefully for misspellings or added words (like "amazon-deals.com" instead of "amazon.com").

- [ ] **Pressure tactics urging immediate purchase**

  Be wary of countdown timers, "only 1 left!" messages, or excessive urgency to complete purchases.

- [ ] **No return policy or unreasonable return conditions**

  Legitimate retailers have clear, reasonable return policies.