SAFE ONLINE SHOPPING CHECKLIST

THE CYBER Mamushka

Online shopping is convenient, but it comes with risks such as scams, phishing, and identity theft. This checklist helps you shop safely by following essential practices to protect your devices, personal information, and financial transactions. Use this guide before, during, and after your online shopping to reduce risks, stay informed, and shop confidently.

Before Shopping:

- Secure Your Devices

□ Ensure your device's operating system, browser, and apps are up-to-date with the latest security patches.

□ Use a reputable antivirus program and enable real-time protection.

- Use a Secure Internet Connection

□ Avoid shopping on public Wi-Fi unless you use a trusted Virtual Private Network (VPN).

□ Shop using a secure, private network with a strong, unique password for your Wi-Fi.

- Choose Trusted Retailers

□ Stick to well-known retailers with a reputation for secure online shopping.

□ Verify the retailer's website URL for typos or extra characters, which can indicate phishing sites.

- Check for SSL Encryption

□ Look for "https://" in the URL and a padlock icon in the browser's address bar.

□ Avoid sites without secure connections (HTTP only).

While Shopping:

- Research Before Buying

□ Check reviews of the product and retailer on multiple platforms.
□ Be wary of deals that seem too good to be true—they often are.

- Beware of Scams

□ Avoid clicking on shopping deals from unsolicited emails, ads, or pop-ups.
□ Verify promotions by visiting the retailer’s official website directly.

- Inspect the Website

□ Ensure the website’s design, grammar, and spelling are professional and consistent.
□ Check the retailer's contact details and return policy for transparency.

- Create Strong and Unique Passwords

□ Use strong passwords for your shopping accounts, combining letters, numbers, and symbols.
□ Avoid reusing passwords across multiple sites.

- Use Guest Checkout (When Possible)

□ Avoid creating accounts on every shopping site to reduce your digital footprint.
□ Opt for guest checkout if it doesn’t compromise convenience.

- Enable Two-Factor Authentication (2FA)

□ Activate 2FA on accounts for added security against unauthorized access.

- Monitor Payment Methods

□ Use credit cards or prepaid cards or secure payment services (e.g., PayPal, Apple Pay, Google Pay) instead of debit cards.
□ Avoid wire transfers, gift cards, or cryptocurrency for online payments unless you trust the seller.

- Be Cautious of Online Marketplaces

□ Verify the seller’s reputation and reviews if shopping on platforms like eBay, Amazon Marketplace, or Etsy.

□ Use the platform’s official payment system and avoid direct payments to sellers.

- Limit Personal Information

□ Provide only the necessary information during checkout.
□ Be wary if the site asks for excessive details or unrelated personal data.

After Shopping:

- Track Your Orders

□ Use the tracking details provided by the retailer to monitor your package.
□ Be cautious of fake shipping notifications or phishing emails.

- Check Your Bank Statements

□ Review your bank and card statements for unauthorized charges after shopping.
□ Report suspicious transactions immediately to your financial institution.

- Keep Records

□ Save order confirmations, receipts, and correspondence with the seller.
□ Ensure these documents contain details like order numbers and purchase amounts.

Avoiding Advanced Scams:

- Watch Out for Fake Apps

□ Download shopping apps only from official app stores like Google Play or the Apple App Store.
□ Check app reviews and permissions before installation.

- Be Skeptical of Social Media Ads

□ Verify the legitimacy of deals and retailers promoted on social media.
□ Avoid clicking on unknown links in ads or comments.

- Beware of Fake Customer Support

□ Verify customer support contact details directly from the retailer’s website.
□ Be cautious of unsolicited support calls or emails.

- Avoid Holiday-Related Scams

□ Be extra vigilant during holiday sales seasons, as scams are more prevalent.
□ Double-check last-minute deals or time-sensitive offers for legitimacy.

Additional Safety Practices:

- Use Virtual Credit Cards (If Available)

□ Generate a virtual credit card number for a specific transaction to limit exposure.

- Activate Purchase Alerts

□ Set up notifications for transactions on your cards to detect unauthorized activity quickly.

- Enable Browser Privacy Features

□ Block third-party cookies and trackers using your browser's privacy settings.

- Clear Cache and Cookies

□ Regularly clear your browser's cache and cookies to avoid storing sensitive data.

- Know Your Consumer Rights

□ Familiarize yourself with refund and chargeback policies.
□ Be aware of your rights under local e-commerce laws.

Pro-Tip: Bookmark Trusted Retailers

Instead of searching for stores via search engines, which could lead to scam sites, bookmark legitimate retailers you frequently use. This ensures you always visit the correct website.

By following this checklist, you can significantly reduce your risk of falling victim to online shopping scams while ensuring a secure and enjoyable shopping experience.

thecybermamushka

https://www.thecybermamushka.com/