Click with Confidence:
Safe Online Shopping Tips

Online shopping is now a key part of retail and is likely to stay a significant way for people to buy goods. By the end of 2025, U.S. consumers are expected to spend approximately $1.3 trillion online, driven by major sales events such as Cyber Monday and Prime Day. Easy checkout, a wide range of product choices, personalized offers, and quick delivery make online shopping a convenient, on-demand option for many buyers.

****Online shopping**** is buying goods or services on a store's website or app using a computer or smartphone. You pick items, pay online, and they're delivered to your address or held for pickup.

****Cyber Monday**** is the Monday after Thanksgiving, when many online stores run big one-day sales that you can shop from home. Retailers offer lower prices, special bundles, and often include free shipping as incentives.

****Prime Day**** is a two-day sales event run by Amazon that offers discounts exclusively to Amazon Prime members. It features temporary price reductions across various product categories—electronics, home goods, clothing, and more—allowing members to purchase items at lower prices during the event.

Although online shopping provides great convenience, during busy sale periods or hurried transactions, people can easily face issues like undelivered orders, unexpected fees, and unauthorized account access due to neglecting safety measures. The solution isn't to stop shopping online but to develop smarter, more careful habits that maintain convenience while lowering risks, such as verifying sellers, using secure payment methods, enabling two-factor authentication and reading return and buyer-protection policies.

How to Identify a Legitimate Online Seller

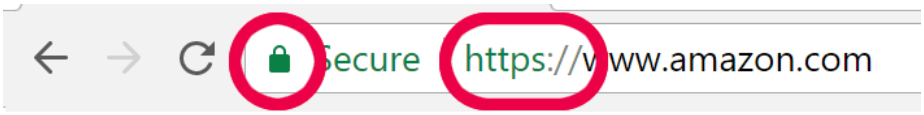
Using multiple verification methods helps you better assess the seller from whom you're buying. If one method raises suspicion, others can identify potential problems, reducing the risk of scams and irreversible transactions.

✔ Check Contact and Business Details:

Reputable online sellers usually provide comprehensive contact details, including a business address, customer service phone number, and a professional email address that matches their domain (for example, support@brandname.com). If a seller uses a free email address (such as Gmail or Yahoo) and does not list their contact details, or if you have difficulty finding them, consider this a warning sign.

✔ Look for Indicators of a Secure Website:

Look for "https://" and a padlock icon in your browser's address bar — these mean the website keeps your information safe. If you see only "http://" or no padlock, don't enter payment or card details.



HTTPS hides your personal info (e.g., your name, card number, or password) as it moves from your device to the website, making it harder for others to see. However, it doesn't prove the seller is honest or that the product is real.

✔ Research the Seller's Name:

Try doing a quick online search of the business name + "scam" or "reviews" to reveal warnings from other buyers.

✔ Read Customer Reviews and Ratings:

Check reviews outside the seller's website—on Google, Trustpilot (a site where customers rate businesses), the Better Business Bureau or BBB (an American organization that records complaints and rates companies), or the marketplace's review section. Honest feedback typically combines praise with specific issues like slow delivery or poor quality. Be cautious of numerous identical glowing reviews (likely fake) and multiple similar complaints about the same issue (likely genuine).

✔ Compare Prices:

If a price is much lower than usual, be cautious—it may indicate a scam, a counterfeit, or a poor-quality item. Check the same product on well-known retailers (Amazon, Best Buy, Walmart) and the manufacturer's official website—the maker's own site that shows the genuine product, standard price, exact features, and warranty (e.g., Apple for iPhones, Nike for shoes). If the offer is far below those verified prices, avoid it or ask questions first.

✔ Inspect Product Listings:

Choose sellers who offer clear, detailed descriptions —including brand, model, size, condition, and any defects —and multiple high-quality photos from different angles. Authentic listings attempt to showcase the item in a real-life setting, either held in the hand, next to a coin or ruler, or in its original packaging, and include readable labels or serial numbers. Vague or missing details, poor grammar, repetitive or identical images across sellers, filenames like "product123.jpg," large watermarks, or the absence of close-up pictures of flaws may signal stock photos, scams, or lower-quality items.

How to Pick the Best Payment Method

Choosing a secure and traceable payment method protects your money and makes refunds or disputes easier if something goes wrong.

➲ **Using a credit card is one of the safest choices.** If something goes wrong—such as the item not arriving or the store turning out to be a scam—generally speaking, your card issuer will investigate fraud, allow you to dispute and reverse unauthorized or incorrect charges (a chargeback), and usually limit your potential loss if someone steals your card. They also keep your bank account number private and make refunds easier, as returned funds are sent directly back to the card.

💡 Best for larger purchases or when you're unsure about the store's trustworthiness.

➲ **Debit cards offer less protection than credit cards.** With a debit card, fraudulent charges are deducted from your bank account immediately, and recovering them can take longer. Banks may investigate, but disputes and refunds are generally slower and sometimes more challenging to win. Liability limits exist, but are often smaller and depend on how quickly you report the fraud. Debit cards also expose your actual bank account (not just a card line), increasing potential disruption to other funds.

💡 Best for smaller purchases from stores you already know and trust.

➲ **Services like PayPal, Apple Pay, and Google Pay act as middlemen between you and the seller.** Instead of giving the seller your actual card or bank details, they send a temporary code that hides your real information. They also monitor for fraud and offer formal dispute processes, which can make resolving issues easier than with a direct bank transfer. They're more private and convenient than using your card directly, but not foolproof: still avoid phishing, check sellers, use a strong password, and enable two-factor authentication. Consider each provider's policies before trusting them.

💡 Best for everyday shopping or when buying from smaller sellers.

****PayPal**** works like an online account you load with cards or bank info to send and receive money on websites.

****Apple Pay** and **Google Pay**** are digital wallets on your phone that store your card and authorize payments using your device's security (fingerprint, face, or passcode).

➲ **Buy Now, Pay Later (BNPL) splits an online purchase into smaller payments, often interest-free for a short period.** BNPL is convenient for planned purchases and quick checkouts. However, it can lead to overspending; missed payments may incur fees, interest, and harm your credit score. BNPL can complicate returns and usually offers weaker protections than credit cards. Use it only for purchases you can pay off within the interest-free period.

💡 Best as a short-term convenience, not free credit; always read the fine print for fees and protections.

Steps to Reduce Payment Fraud

🔺 **Activate fraud alerts in your online banking:** A fraud alert is a quick warning (text, email, or app notification) that your bank sends when it detects unusual activity and asks you to confirm it. If you say it's not you, the bank can block the charge, freeze the card, or contact you to prevent further theft—helping to recover funds and protect against criminals using your details elsewhere.

For example, you receive a bank alert about a $200 TV purchase you don't recognize. You press the alert's *"This wasn't me"* option or call the bank using a familiar phone number; the bank then cancels the charge and freezes the card so that no further purchases can be made.

🔺 **Review your statements regularly:** Look over transactions weekly to spot small "test" charges or unfamiliar fees. Catching these early lets you report them right away so the bank can block the card, refund unauthorized charges, and issue a replacement before theft grows.

For example, while paying bills on Sunday, you notice a $5 "trial" charge you didn't authorize. You report it to the bank, they refund the small amount and issue a new card before larger charges occur.

🔺 **Use single-use virtual card numbers when available:** A virtual card creates a one-time number for each purchase, so merchants never see your real card. The number expires or can be canceled, preventing later or recurring charges and making it easy to isolate and stop problematic merchants.

For example, when ordering medication online, you use a one-time virtual card number. If that pharmacy's records are later compromised, only the expired virtual number is exposed — your real bank card remains protected.

Why 2FA Matters for Online Shopping

Two-factor authentication, or 2FA, is an extra security measure that helps protect your online accounts. Instead of relying solely on a password, 2FA requires a second method of verification to confirm your identity—usually something you have (like your smartphone) or something you are (such as a fingerprint).

Why should you consider it?

🔑 Passwords alone aren't enough. Hackers can steal or guess them through phishing, data breaches, or by exploiting weak password reuse across multiple sites.

🔐 Even if scammers obtain your password, they won't be able to access your account without the second factor enabled.

Common 2FA Methods

- **SMS codes:** A short number is texted to your phone. Easy to use, but risky if someone hijacks your phone number.
- **Authenticator apps (Google Authenticator, Authy).** A rotating code is generated by the app, which you then enter elsewhere for verification. It's more secure than texts because it doesn't depend on your phone number network.
- **Email codes:** A code is sent to your email. Simple, but if someone gains access to your email, they can view the code.
- **Biometrics:** Your fingerprint or face is used to verify your identity. It's fast, generally secure, and available on most modern phones.

How to Set Up 2FA - General Steps

1. Sign in to the shopping site (Amazon, eBay, Walmart, etc.).

2. Go to either **"Account Settings"** or **"Security"** and choose **"Two-Step Verification" / "Two-Factor Authentication."**

3. Pick the method of your choice: SMS (text), an authenticator app, or biometrics (fingerprint/face).

4. Follow the on-screen prompts:

- If using SMS, enter your phone number, wait for the verification text, then type the one-time code sent by the site.
- If using an authenticator app (e.g., Authy, Google Authenticator), install the app, scan the site's QR code with it, then enter the short code displayed by the app.
- If using biometrics, register your fingerprint or face by placing your finger on the sensor or positioning your face in the frame until the device captures the sample. Afterwards, you'll approve sign-ins by touching the sensor or looking at the screen.

5. Many sites give you one-time backup codes in case you lose your phone. Store them securely (not in your email inbox).

6. Test it: log out and sign back in to confirm the 2FA method works and that you can use your backup codes or recovery option if needed.

🔎 **Quick tip:** Keep an alternate recovery method, such as a second phone number or email, up to date so you can regain access if you lose your primary device.

Return Policies

They vary by retailer, but here are the common elements you might encounter with online stores and retailers that you should pay close attention to:

✔ Return Window

Most stores accept returns within 14–30 days of delivery; some extend this around holidays.

✔ Condition Required

Does it ask to keep the item unused, with tags and original packaging? For electronics, do you need to include chargers and accessories from the item packaging to avoid refusal? Please note that final sale items cannot be returned.

✔ Refund vs. Store Credit

If you return an item, will the refund be credited back to your card or as store credit? Buyer protection typically covers the following: items not received, items not as described, and counterfeit goods.

✔ Return Shipping

The cost and steps for returning an item after purchase.

Knowing and following return rules helps to prevent fraud by making it harder for criminals to exploit you. Reading policies reveals how returns are handled and who pays shipping, so you can spot suspicious sellers or unusually lenient terms that may be scams. Checking deliveries immediately (with photos, receipt, and date) creates evidence if someone tries to claim you returned an item you didn't, or if a thief tests your card with minor charges.

Smart Returns—What To Know

❎ Check the fees and refund type before purchasing: see if the seller charges restocking or inspection fees. Some retailers deduct a percentage from your refund if you return opened items.

❎ Confirm any prepaid return label: if the seller provides a return label, verify its expiry date, which carrier it is for, and the drop-off location.

❎ Expect varying refund times: big retailers tend to refund quicker than small sellers — keep that in mind for costly purchases.

❎ When the package arrives, take a photo of the item and its packaging, and keep the order receipt — this provides proof of the condition and delivery date in case of a dispute.

❎ Note the delivery date: the return clock usually begins on the day the carrier delivers, so record that date if possible.

❎ Check the item immediately: test electronics and ensure chargers or accessories are included while the return period remains open. Is the warranty valid internationally or only in the seller's country of origin?

❎ Keep the original box and tags: many sellers require them for a full refund, so don't throw the packing away.

❎ Keep proof of postage: if you pay to return an item, save the receipt and tracking number so you can claim reimbursement.

Device, Account & Delivery Safety

Why are they relevant? Each protects a different stage of the online shopping process.

Device safety — protects what you do online: Keep your phone, tablet, and computer updated, and delete apps you don't trust. Software updates fix security issues and close vulnerabilities that hackers could exploit to steal card details or passwords. Use your home Wi-Fi (set with a password) or mobile data for payments. Avoid public Wi-Fi unless you're using a trusted Virtual Private Network (VPN), as public networks can let others see what you're typing.

Account safety — protects who can use your accounts: Use a unique, strong password for each shopping account and either save them in a password manager or write them down and keep them locked away. Regularly review account activity; if you notice unfamiliar logins, change your password immediately and sign out of other devices.

Delivery safety — protects the items you buy: Select tracked shipping and request a signature for high-value items to prevent packages from being left unattended. Consider sending deliveries to pickup lockers or to a trusted neighbour when you're not home.


Connecting Generations
Cyber-Seniors™


be well
ILLINOIS


aetna®


BEYOND
FORCE


trail
TOTAL RETIREE ADVANTAGE ILLINOIS

DEFINITIONS

***Amazon Prime** is a paid membership from Amazon that bundles faster shipping (often free two-day or same-day delivery), access to streaming movies and TV shows, ad-free music, and special shopping benefits like Prime Day deals.

- **Amazon** is a large online retailer and technology company where you can buy products, stream media, and subscribe to services. Its website and app let customers search for items sold by Amazon or third-party sellers.

***Authy** is an app that shows a short, changing code you use as the second step when signing in to online accounts (like your email, bank, or shopping sites). Unlike some apps, Authy can securely back up those codes to the cloud (protected by a password) so you can recover them if you lose or replace your phone.

- **Cloud** storage refers to a secure online service where your Authy codes are stored on remote servers, not on your physical phone.

***Backup code** is a one-time-use number or word you keep safe and use to sign in if you can't access your usual two-step verification method (like your phone or authenticator app).

- **Authenticator app** generates short, changing codes used for two-step verification. When you sign in, you enter the current code from the app (instead of or in addition to a text message). This makes accounts much more challenging for thieves to access.

***Biometrics** are physical features—like your fingerprint, face, or sometimes your voice—used to confirm your identity. On phones and computers, the device scans that feature and checks it against a stored record; if it matches, you're signed in or a payment is approved.

***Browser address bar** is the long box at the top of your internet browser (like Chrome, Safari, or Edge) where you type a website address or search. It shows the exact web address (so you know which site you're on) and can display a padlock icon to indicate a secure site.

***Data breach** is when someone breaks into a company's systems and steals customers' private information — like names, email addresses, passwords, or card numbers — so that information can be exposed.

***Digital wallet** is an app or service on your phone or computer that stores your payment cards and lets you pay without handing over your real card details.

***eBay** is an online marketplace where people and businesses buy and sell new and used items through listings or auctions.

***Email inbox** is the place in your email app or website where new messages arrive. It's like a digital mailbox: you open it to read, reply to, delete, or keep messages you want to save.

***Gmail** is Google's free email service that lets you send, receive, and organize messages from a web browser or phone app.

***Google Authenticator** is a free app that generates short, changing security codes for use as a second verification step when signing into accounts. Instead of receiving a text message, you open the app to read a six-digit code and enter it into the website.

***Hijacking** means someone tricks or fools a phone company or service into giving them control of your phone number or account, so messages or codes intended for you are sent to them instead.

***HTTPS** stands for HyperText Transfer Protocol Secure. Without the "S", HTTP—HyperText Transfer Protocol indicates web data in plain text; anything you type (passwords, credit card numbers) can be intercepted more easily.

***Marketplace's review section** is where buyers leave star ratings and comments about a seller's product and service. It shows others' experiences with quality, delivery, and support—use recent, specific reviews to judge a seller's reliability.

***One-time card** is a temporary, single-use virtual payment number linked to your real card or account. It works like a regular card for one transaction (or a short time), then expires—so merchants can't charge you again, and your real card details stay hidden.

***Passcode** is a short secret number or word you enter to unlock a device or confirm your identity. It's a backup to biometrics (fingerprint/face) and a recovery option if those don't work.

***Password reuse** is using the same password for more than one account. If one site is hacked and the password is stolen, attackers can attempt to use it on your other accounts and gain access.

***Phishing** is a scam where someone pretends to be a trusted person or company (via email, text, or fake websites) to trick you into giving passwords, credit-card details, or other personal information.

***QR code or quick response code** is a black-and-white square image that stores a link or small data. Scan it with your phone camera to open a website or set up an app.

***Stock photos or images** are ready-made photos one can buy to use on websites, ads, or printed materials instead of hiring a photographer. Some are free, while others require a fee. For example, a café owner can download a photo of a latte and purchase a license to use it on the menu and website, rather than paying a photographer to take the picture.

***Two-factor authentication (2FA)** is an extra security step that helps protect your online accounts. Instead of logging in with just a password, 2FA requires a second form of verification that you are who you claim to be — typically something you have (such as your phone) or something you are (like a fingerprint).

➢ **Online account** is a record you create with a website or app (such as email or banking service) that uses a username and password, allowing you to sign in and access your personal information or services.

***VPN (Virtual Private Network)** is a service that makes your internet connection private and secure. It creates an encrypted "tunnel" between your device and the internet so other people on the same network (like in a café) can't see what you do.

***Yahoo Mail** is Yahoo's free email service for sending, receiving, and organizing messages via a web browser or phone app.