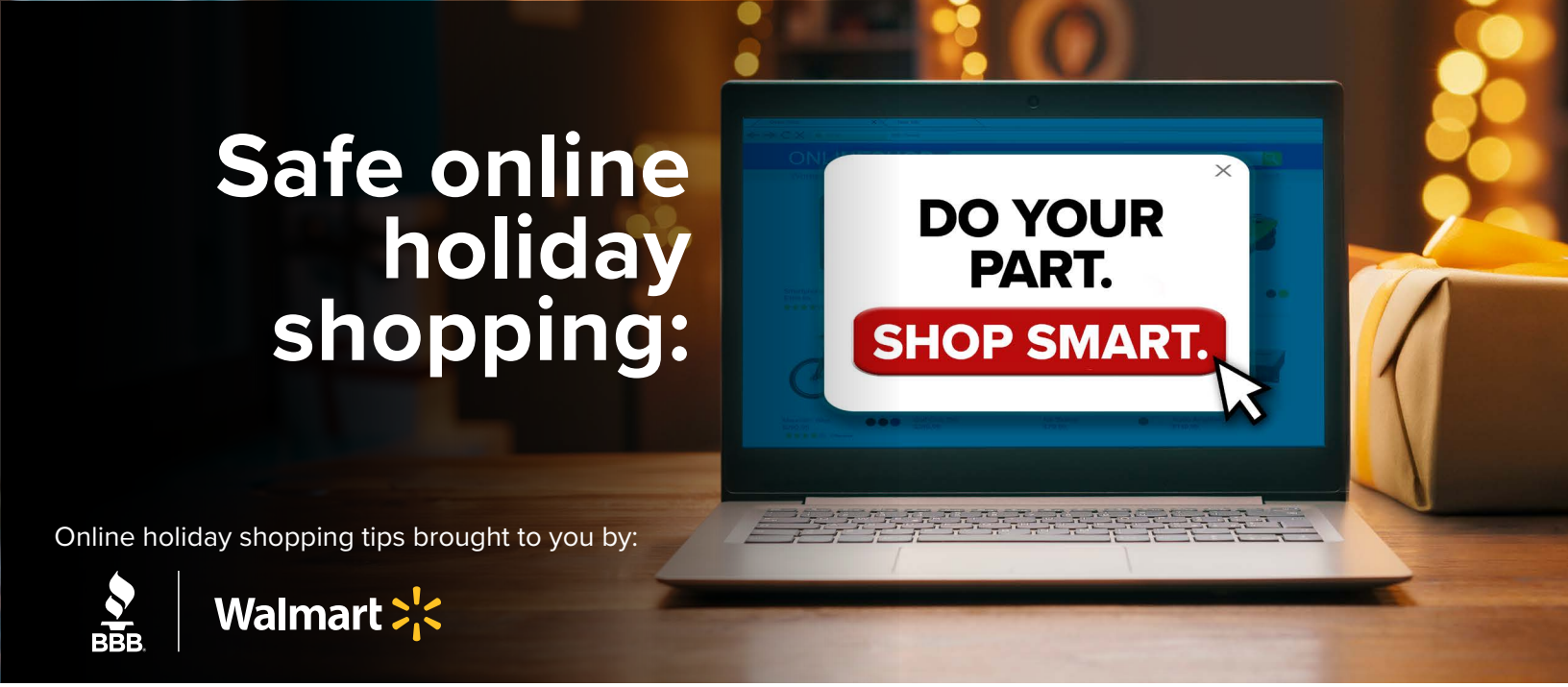
Safe online holiday shopping:



Online holiday shopping tips brought to you by:

BBB | Walmart

It's that time of year, when many of us plan to do at least some of our holiday shopping online. To keep you and your loved ones safe, here are some tips to spot and avoid scams.

Unfamiliar sellers/websites.

If you're interested in buying from a new seller or unfamiliar website, take time to do research before you buy.

- **If the deal looks too good to be true, it probably is.** Don't shop on price alone. Low prices and hard-to-find items are a red flag the website might be fake.
- **Don't believe everything you see.** Scammers are great at mimicking official seals, fonts, and other details. Just because a website looks official does not mean it is.
- **Take a few moments to research a new website:**
  - **Check the URL:** Scammers will create fake URLs that mimic well-known brand names. If you look closely, you can usually detect one character or something else that is incorrect.
  - **Watch for bad grammar:** Read the content carefully—you may detect typos and bad grammar, indicating the website was put together quickly.
  - **Research age of domain:** Scammers create attractive sites quickly to attract targets before the sites are taken down. Online tools can help you find out how long the domain has been active. If it's a newer website, proceed with caution.
  - **Search for contact information:** Is there a way to contact the business (phone, email, address, online chat)? If the only contact information you can find is an online form, that's a red flag.
  - **Make sure it's secure:** Look for the "https" in the URL (the extra s is for "secure") and a small lock icon on the address bar.

"Porch pirates."

Millions of packages are stolen every year. Take steps to protect your deliveries.

- **Don't leave unattended packages.** When possible, do not leave delivered packages unattended for long periods. If you are expecting a package, attempt to schedule delivery when you know you will be home.
- **Ship to store.** If purchasing an item from a retailer with a physical location near your home, consider shipping it there instead. Retailers will require proof of purchase or identification before releasing packages.
- **Use a security camera.** Installing a home security system with cameras or a camera-enabled doorbell is a great way to deter package theft, especially if it's highly visible. Consider including a sign that specifically states that the residence is under surveillance.
- **Require a signature**. Many delivery companies include the option to require a signature before leaving a package, letting you take physical possession of the item as soon as it is delivered.

Gift cards are for gifts, NOT unsolicited payments.

Gift cards can be the perfect holiday present for friends or loved ones, but they can also be a red flag for fraud.

- **Beware of people asking you to make an unsolicited payment with a gift card.** Scammers ask their victims to pay them with gift cards because they're a convenient way to steal money and they're difficult to trace or recover. Legitimate organizations will never ask you to pay them with a gift card.
- **Use secure and traceable transactions.** Avoid paying by wire transfer, prepaid money order, gift card, or other non-traditional payment methods.

Protect yourself on social media.

Scams perpetrated via social media rose 63% in 2023.

- **Avoid making quick purchases while browsing social media.** Be more intentional about your online purchases and avoid impulse buying.
- **Be wary of "new online friends" who direct message you with incredible opportunities.** Scammers sometimes pose as people you know, or build an online relationship before targeting you for a scam.
- **Avoid sharing too many personal details in your social media posts.** These details can be used for social engineering/phishing.
- **Do not make a buying decision solely based on comments.** Make sure you expand your research beyond customer comments before you make a buying decision. Always research the seller and only shop from their official website or app.

.

If you think you're being targeted by a scammer:

- **Stay calm.** If you are being pressured to act quickly, resist the urge to make a snap decision no matter how dramatic the story is or how threatening or intimidating the caller sounds.
- **Don't reply directly.** Don't respond to unsolicited calls, texts, or emails. Instead, call the company or person directly to verify the message or the call you received is legitimate.
- **Go to the source or get help.** Contact the company via information you already have or can find on their website. When in doubt, call your local BBB® to ask for a second opinion. If you made a purchase, always verify and track it using the company's app or website.
- **Never give personal information (SSN/SIN, account numbers/passwords, license number, etc.) over the phone, especially if the call was unexpected.** Scammers may impersonate a customer service representative from a known company, even spoofing a call (falsifying the name/organization on your caller ID). If you're unsure, end the call/chat and reach out directly to the company's customer service phone number or website.
- **Never pay over the phone, especially if the call was unsolicited.** Never make a payment until you have verified all the details with a third party or via the organization's official call center or website.
- **Never allow remote access to your computer if somebody offers tech support.** Shut down your computer immediately and seek support directly from a trusted service provider.
- **Search BBB Scam Tracker℠.** If you're suspicious about the situation, search BBB Scam Tracker to see if anyone else has reported a similar situation. BBB Scam Tracker enables you to search by email, URL, phone number, and more.
- **Check the email address or URL more closely.** Scammers use similar website addresses or emails to appear legitimate, but if you look closely, you may find one letter or number that is off.
- **Report any scam activity to BBB Scam Tracker.** Reporting scams helps protect others. BBB publishes scam reports so others can avoid the scam that targeted you.