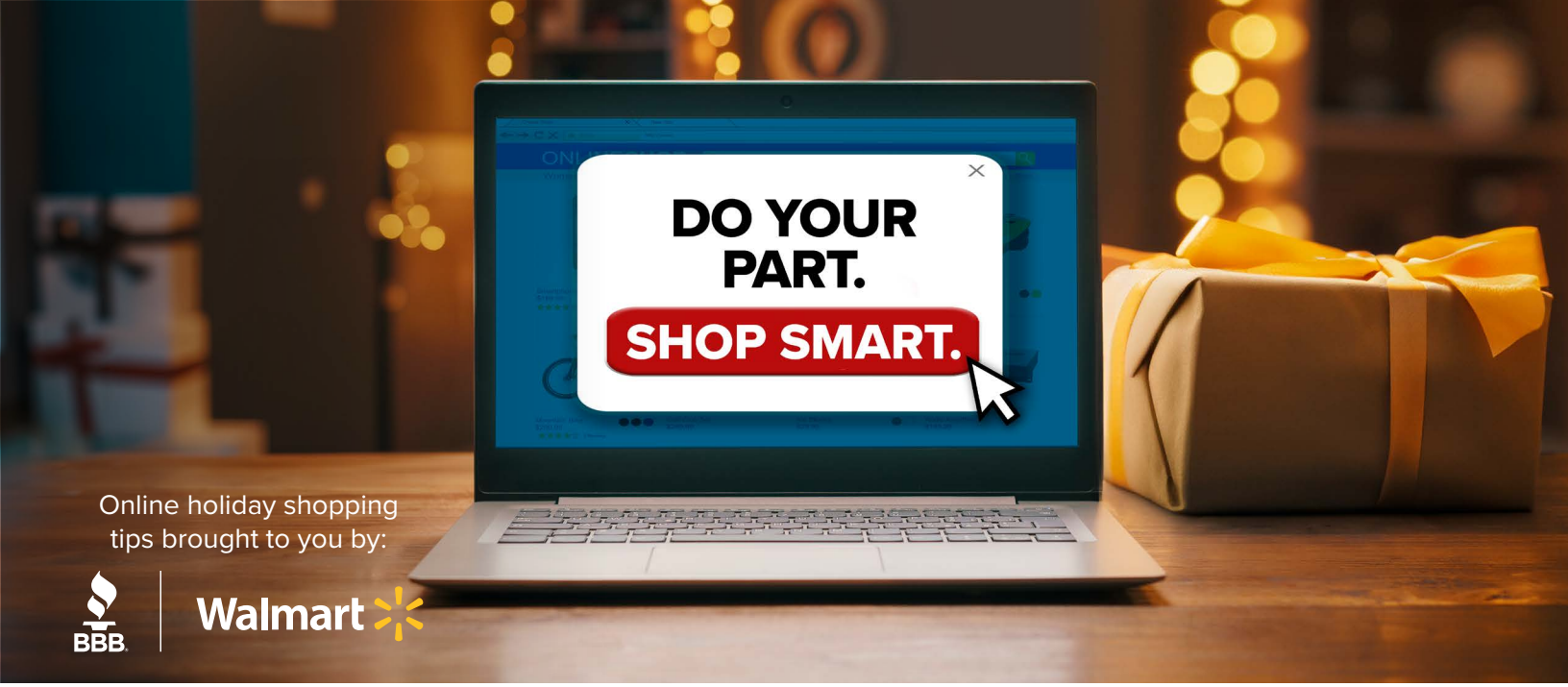

Shopping Online? Stay Safe with These Scam-prevention Tips

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 logos, 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.
  - **Find the creation date:** Scammers create attractive sites quickly to attract targets before the sites are taken down. Online tools can help you find out how long the website 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.

More than 82% reported losing money when they engaged with a scammer via social media.

- **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.

Spot and avoid impersonated shipping notices.

- **Go directly to the source:** Instead of clicking, open a new browser window and manually go to the shipping company's official website (e.g., USPS.gov, UPS.com, FedEx.com).
- **Track using the real website:** Use the tracking number from your original purchase confirmation to check for legitimate shipping issues on the official site.
- **Be suspicious of requests for payment:** Legitimate shipping companies typically don't demand immediate payment for delivery issues via unsolicited text messages.
- **Verify with the sender:** If you're concerned, contact the original retailer directly to verify any shipping notification.

If You Suspect a Scam: What to Do Next

- **Stay calm.** Don't rush decisions, even if the message sounds urgent or threatening.
- **Don't respond directly.** Ignore unsolicited calls, texts, or emails—verify using trusted contact info.
- **Go to the source.** Contact the company using verified info or call your local BBB® for advice.
- **Protect personal info.** Never share sensitive details over the phone, especially from unexpected calls.
- **Don't pay over the phone.** Verify all details through official channels before making any payment.
- **Avoid remote access.** Never allow unknown tech support to access your computer—contact a trusted provider.
- **Use BBB Scam Tracker℠.** Search it to see if others have reported similar scams.
- **Check URLs/emails.** Look closely for small errors that could indicate a fake site or email.
- **Report scams.** Help others by reporting to BBB Scam Tracker.