TIP #2:

ONLY SHOP THROUGH TRUSTED SOURCES

Think about how you're searching online. How are you finding the deals? Are you clicking on links in emails or going to trusted vendors? Are you clicking on ads on webpages? You wouldn't go into a store with boarded up windows and without signage – the same rules apply online. If it looks suspicious, something's probably not right.
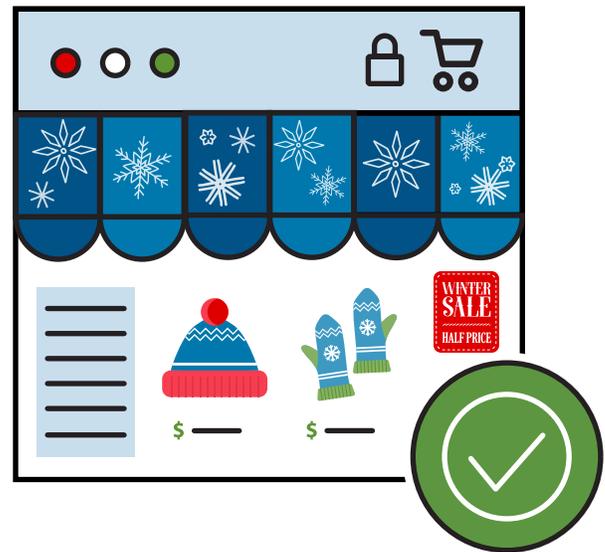
Before providing any personal or financial information, **make sure that you are interacting with a reputable, established vendor**.

Some attackers may try to trick you by creating malicious websites that appear to be legitimate. **Always verify the legitimacy before supplying any information**. If you've never heard of it before, check twice before handing over your information.

Most of us receive emails from retailers about special offers during the holidays. **Cyber criminals will often send phishing emails**—designed to look like they're from retailers—that have malicious links or that ask for you to input your personal or financial information.

Don't click links or download attachments unless you're confident of where they came from. **If you're unsure if an email is legitimate, type the URL of the retailer or other company into your web browser** as opposed to clicking the link.

Never provide your **password, or personal or financial information in response to an unsolicited email**. Legitimate businesses will not email you asking for this information.

Make sure your information is being encrypted. All reputable merchants use encryption to transmit information from your browser to their servers. Look in your browser's location bar to **make sure the website address begins with "https:"** instead of "http:". Also look at the padlock icon. If the padlock is locked, your information is encrypted.

Learn more at cisa.gov/shop-safely

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA