## TIP #1:

# CHECK YOUR DEVICES

**Before making any online purchases, make sure the device you're using to shop online is up-to-date. Next, take a look at your accounts and ask, do they each have strong passwords? And even better, if multifactor authentication is available, are you using it?**

**Protect your devices** by keeping the **software up-to-date**. These include items like mobile phones, computers, and tablets, **but also appliances, electronics, and children's toys.**

Once you've purchased an internet connected device, **change the default password** and **use different strong passwords** for each one. Consider using a password manager to help.

**Check the devices' privacy** and **security settings to make sure you understand how your information will be used and stored**. Also make sure you're not sharing more information than you want or need to provide.

**Enable automatic software updates** where applicable, as running the latest version of software helps ensure the manufacturers are still supporting it and providing the latest patches for vulnerabilities.

CISA
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

**Learn more at cisa.gov/shop-safely**

# 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.
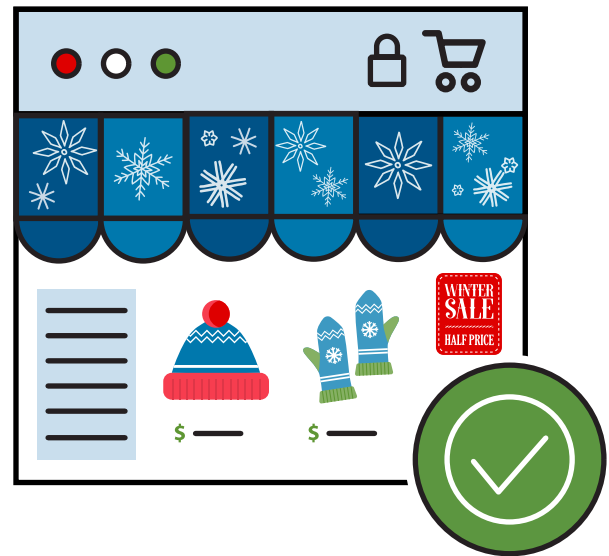
Before providing any personal or financial information, **make sure that you are interacting with a reputable, established vendor**.

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**

# TIP #3:

# USE **SAFE** METHODS FOR PURCHASING

If you're going to make that purchase, what information are you handing over? Before providing personal or financial information, check the website's privacy policy. Make sure you understand how your information will be stored and used.



If you can, **use a credit card as opposed to a debit card**. There are laws to limit your liability for fraudulent credit card charges, but you may not have the same level of protection for your debit cards. Additionally, because a debit card draws money directly from your bank account, unauthorized charges could leave you with insufficient funds to pay other bills. Also use a credit card when using a payment gateway such as PayPal, Google Wallet, or Apple Pay.

You'll likely make more purchases over the holiday season, **be sure to check your credit card and bank statements for any fraudulent charges frequently**. Immediately notify your bank or financial institution.

**Be wary of emails requesting personal information.** Attackers may attempt to gather information by sending emails requesting that you confirm purchase or account information. Legitimate businesses will not solicit this type of information through email. Do not provide sensitive information through email.

If you receive a suspicious email that you think may be a phishing scam, **you can report it at:** *cisa.gov/uscert/report-phishing*