







Online Shopping: Protect Yourself

When online shopping, please keep these tips in mind to help minimize your risk. If you suspect fraud on your accounts or cards, contact us immediately.

- > **Secure your mobile device and computer.** Be sure to keep the operating system and application software updated on all of your computers and mobile devices. Ensure your anti-virus/anti-spyware software is running and receiving automatic updates. Confirm your firewall is enabled.
- > **Use passwords.** If you need to create an account with the merchant, be sure to use a strong password. Always use more than ten characters, with numbers, special characters, and upper and lower case letters. Use a unique password for every unique site.
- > **Do not use public computers or public wireless for your online shopping.** Public computers may contain malicious software to steal your credit card information when you place your order. Additionally, criminals may be intercepting traffic on public wireless networks to steal credit card numbers and other confidential information.
- > **Pay by credit card, not debit card.** A safer way to shop on the Internet is to pay with a credit card rather than debit card. Debit cards do not have the same consumer protections as credit cards. Credit cards are protected by the Fair Credit Billing Act and may limit your liability if your information was used improperly. Check your statements regularly.
- > **Do not auto-save your personal information.** When purchasing online, you may be given the option to save your personal information online for future use. Consider if the convenience is really worth the risk. The convenience of not having to reenter the information is insignificant compared to the significant amount of time you'll spend trying to repair the loss of your stolen personal information.
- > **Know your online shopping merchants.** Limit your online shopping to merchants you know and trust. If you have questions about a merchant, check with the Better Business Bureau or the Federal Trade Commission. Confirm the online seller's physical address, where available, and phone number in case you have questions or problems. Look for "https" in the web address when making an online purchase. The "s" in "https" stands for "secure" and indicates communication with the webpage is encrypted.


https://www



http://www

- > **Do not respond to pop-ups, links or attachments on emails.** If a window pops up promising you cash or gift cards for answering a question or taking a survey, close it by pressing Control + F4 for Windows or Command + W for Macs. Be cautious about all emails you receive—even those from legitimate organizations including your favorite retailers. The emails could be spoofed and contain malware. Instead, contact the source directly.
- > **Use common sense to avoid scams.** Don't ever give your financial information or personal information via email or text.
- > **Review privacy policies.** Review the privacy policy for the website/merchant you are visiting. Know what information the merchant is collecting about you, how it will be stored, how it will be used, and if it will be shared with others.



Information provided by Wespay