1. Always place orders from a secure connection

If your computer isn't protected from potentially malicious software, your financial information and passwords are at risk from being stolen (and everything else you store on your computer or do online). This concept is so basic, yet only a fraction of the population adequately protects their computers. Use a secure connection – make sure your computer's firewall is on.

2. Know the merchant and their reputation

If you already know the store, shopping in their online store is very safe. You can always walk into the local store for help if there's a problem, and if you know others who have had consistently positive experiences with the online store, you can be reassured of the site's quality. If you don't know the store, it may still be the best bet; you just need to take a few more precautions. Conduct your own background check by looking at sites dedicated to reviewing online stores. If the store isn't reviewed or does not have favorable reviews, don't order from their website.

3. Avoid offers that seem "too good to be true"

Any online store that promises too much at too low a price is suspicious. If the price is too low, consider whether the merchant came by the items legally, if you will ever receive the items you paid for, whether the items are actually the brand shown or a cheap substitute, if the item will work, if you will be able to return damaged goods – or if the merchant is earning extra income by selling your financial information. Disreputable online stores may run an absurdly low-price offer and then claim the item is out of stock, to try to sell you something else in a classic "bait and switch" scam.

4. Don't fall for email scams

You might get emails or texts offering amazing bargains or claiming there's been a problem with a package delivery. Delete suspicious messages from unfamiliar senders. And don't open attachments or click links in messages because they could infect your computer or phone with viruses and other malware.

5. Don't use an online store that requires more information than necessary to make the sale.

Expect to provide some method of payment, shipping address, telephone number, and email address, but if the merchant requests other information, STOP! You never want to give them your bank account information. Some companies ask questions about your interests, but these should always be optional and you should be cautious about providing the information. Does the merchant resell, rent, or share your information? Check the site's privacy policy to understand how exposed your information may become. Many stores clearly state that they do not share, sell or rent consumer's information – others say they own your info and can use it (or abuse it) however they choose. Stick to the companies that respect your privacy.

6. Need to create a password for the site? – make it unique.

You will often be asked to create an account with a password when you make a purchase. Usually, you can choose not to do this, and unless you will use the e-store frequently, don't create an account. If you do want an account, make sure to use a unique and strong password.

7. Is the site secure?

Before entering any personal or credit card info onto a shopping site Look for a lock icon in the browser bar of a site to verify that they use SSL (secure sockets layer) encryption. look to see if the web address on the page begins with "https:", not "http:" That little 's' tells you the website is secure and encrypted to protect your information. Secure websites are configured to mask the data you share, such as passwords or financial info. Shopping only on secure sites reduces the risk that your private information will be compromised while you shop.

8. Use a Credit Card for online transactions

Do not use a debit card or check as these do not have the same security protections in place for you should a problem arise. Consider designating one credit card that is only for online shopping and transactions. This way, if the card gets compromised, you can quickly shut it down without impacting any other type of transactions.

9. Keep an eye out for fraud

Check your bank and credit card statements for fraudulent charges at least once a week. Or set up account alerts to notify you of any new activity on your card. When you receive a text or email notification, you can check your account to make sure you recognize the charge.