# How the Grinch can steal your data

**Image:** Included in toolkit.

**Suggested Alt Text:** Colorful holiday shopping bags with a credit card marked by an exclamation, intended to warn shoppers to be safe.

The online shopping season is about to start. It’s a prime time for fraudsters and scammers to tap into your increased online activity, busyness, and seasonal distractions. They’re hoping to steal your personal and financial information.

It’s a great time to think about ways scammers might try to deceive you and how to be on guard against them. Can you tell which of these statements is true or false?

1. **If a website looks legit, it is.**

**FALSE.** Imposter websites are being built that closely mimic the real thing, making it difficult to tell the difference. Make sure the URL has **https**, a padlock on it, and usually ends in .gov or .com in the United States. When you select the padlock, confirm it says the connection is secure. If a site is hard to navigate or missing sections, that's a major warning sign that it's fraudulent. A missing “About Us” page or contact information is another sign. Scammers typically include fake or no contact information. If you can't find or verify in other ways the accuracy of the information about the company on their website, it could be a scam.

1. **If an email comes to my inbox and not my junk folder, it must be valid.**

**FALSE.** The junk mail feature of email providers is not foolproof. If it’s an option, be sure it’s turned on. Don’t depend on the junk mail filter. Evaluate each email you receive before opening any attachments or links.

* **If I pick up the phone and the caller asks for me by name, and inquires how I’m doing, they sound friendly enough and I should engage.**

**FALSE.** Scammers and salespeople can sound downright friendly and perhaps confide they’re Veterans and share common interests and concerns with you. It doesn’t mean it’s true. It might be their cover story or schtick. If you don’t know someone, don’t answer, nor engage. Screen calls and if the caller is legit, they’ll leave a message with details about how to contact them. Check all the information out first through other resources to see if it’s authentic. Even then, you have no obligation to return calls from cold callers. One general rule: If anybody contacts you and wants personal, financial, health, or background information about you, your family, or friends, don’t give it and hang up. Some scammers will try to record your voice and use it for nefarious purposes. The less you say, the better.

* **I’m looking for a special gift and see an ad for such a gift as I scroll through social media, so the ad must be safe.**

**FALSE.** Scammers are using social media to place fake ads that point to fake websites. If you see an ad on social media, don’t select the link. Write down separately the business information and do internet sleuthing and recognizance to see if they’re real and a sound business. Red flags also include no recent reviews, few discussions, or recent engagements.

* **If I get a text saying, “thanks for your order” and can’t remember ordering something, I should click on the link within the text for more information.**

**FALSE.** Text messages and emails like this are sent to millions of people every day looking for anyone who–perhaps in a hurry or despair–will take the bait. Instead of opening, reading, or selecting attachments and links, take a pause and logically evaluate the situation. If you didn’t order anything from that company, it doesn’t pass the sniff test. **Delete the text or email immediately** and report it as junk if your mobile device or email service gives that option.

**More tips here**

* [Holiday Online Shopping](https://www.cisa.gov/holiday-online-shopping)
* [Talking Santa, Shopping, and Scams](https://digital.va.gov/cyber-spot/talking-santa-shopping-and-scams/)
* Report issues to your banks and financial institutions if you believe there is fraud or identity theft.
* Veterans who suspect they have been the victim of VA disability benefits fraud should call VA at 1-855-578-5492, right away.
* File complaints with the [Federal Trade Commission](https://reportfraud.ftc.gov/), [with the FBI](https://www.ic3.gov/Home/ComplaintChoic), and with the [Federal Communications Commission](https://consumercomplaints.fcc.gov/hc/en-us).

**Remember to Secure Your World.**