

# How to talk to patrons about: *Shopping Safely Online*

- Never enter personal information unless you see **https**, which means your information will be encrypted while transmitted.
- Some online retailers allow you to pay with a one-time code from PayPal, Google Pay, or Apple Pay. This is more secure than entering your credit card information and is a great option to protect yourself.
- When in doubt, Google a company to see if they are legitimate and if there are complaints filed against them. You can also look up the company at the Better Business Bureau website.

*“Be careful using websites or sellers that aren’t well-known. Online marketplaces may have great offers, but those offers might be too good to be true.”*



## Shopping Safely Online

Online shopping is popular, but it also creates opportunities for people to get scammed. If you're going to buy anything online, here are some tips to keep your money and personal information safe. 

-  Is the site well-known? Big companies like Amazon, Walmart, and Target are generally trustworthy.
-  **https://** Check the URL. Does it start with https? Is there a lock icon? This tells you your data is encrypted when it's transmitted to the site.
-  Look out for online offers that seem too good to be true. They probably are. Don't click links in emails or text messages that come from strangers and be cautious buying things in online marketplaces.
-  Avoid submitting sensitive information like your credit card number while on public WiFi networks.
-  Don't save your payment information on the site or on the computer, especially when using a public or shared computer.

For more information, visit <https://safedata.umd.edu>