Shopping Safely Online
By LeRoy Harris
Programming & Technology Services Librarian

Black Friday, Cyber Monday, Holiday Deals, Last Minute Shopping, and many other phrases, slogans, and buzz words bombard us this time of year. It's easy to feel overwhelmed or to get shopping fever. Advertisements, websites, and email promotions promise big discounts or special pricing. Cyber criminals know this and will take advantage of the hectic holiday happenings to create hoaxes and hijinks. To further complicate things, websites and businesses will sometimes use predatory tactics like deals contingent on applying for store credit, buy now pay later schemes, automatically renewing subscriptions, and discounts in exchange for targeted advertising. Each is designed to keep you buying, pay more in the long run, or to share personal information for their profit. I've written before about the need for digital literacy, and that need remains. Here are just a few tips to help you be aware as you shop online.

Number one, never allow your web browser to "autofill" forms. This convenience feature helps you access websites faster. The browser saves information you have entered into boxes on websites. This can include usernames, passwords, addresses, and payment information. An individual website can save information like payment methods, but it gets encrypted within the website. On the other hand, what your browser saves is fair game for spyware, malware, or websites that track your browsing. Anyone who gets on your device can find them too. Convenience is nice but less secure.

Number two, never click a link for a website or promotional deal until you have verified the link's destination. Hyperlinking is a neat tool. It allows you to take a word, phrase, or image and make it an action button to go to a web address. Advertisements you see on websites are hyperlinks. They try to catch your attention with flashy visuals or word choices, so you click on them. Unfortunately, many such links include redirects that record your information like what kind of device you have and where it is located or what websites are open in your browser. Those are just the actual advertisements. Some hyperlinks are predatory or even criminal. The link will go to the website, but it will also download spyware or malware to your browser or allow a hacker to view your screen. Others will take you to look-alike sites that seem legitimate but are scams. You can investigate a link by hovering over it with your mouse. The web address it links to should show up in a grey box in the lower left of your screen. If you feel a bit more confident in your computer skills, you can also check a link by right clicking on it with your mouse and selecting "Inspect". This will bring up a window of code at the bottom of your screen with the link address and associated command highlighted.

Lastly, watch out for hidden fees and subscriptions. Many websites sell items more cheaply than at a physical store, so how do they make money? Two ways: advertising investments and extra fees. Some websites have reasonable prices but charge exorbitant shipping costs or add on processing fees per order. Another tactic used is to have optional advertising, subscription, and information sharing boxes included as part of the checkout process for your purchase. They use two ways to trick you into agreeing

to this scheme. One, the boxes will be pre-checked, so if you don't uncheck them, you just agreed to all their requests. Two, you must check a box to opt out of the scheme otherwise you automatically agree when you purchase. Keep your eyes open as you shop online and stay safe.

We hope you'll take advantage of the wonderful resources we have here at the library to help you improve your digital literacy or conduct your online business. The library is located at 17 N. Broadway and is open to the public Monday to Thursday 9:30 a.m.-8 p.m. and Friday and Saturday 9:30 a.m.-5 p.m.