December 1, 2022

Dear Placentia Library District Patrons,

I hope you had a wonderful Thanksgiving with your family! Despite missing dinner with my mother due to a sick son, my family enjoyed a special meal earlier that week and I'm so thankful for them. I suspect most everyone's shopping began the early hours last Friday.

As you grab those special deals, do be wary of online shopping. While retailers and cybersecurity officials are vigilant in protecting consumers, it is a continuous game with thieves and scammers. With 76% of adults shopping online, there are endless opportunities for lawbreakers to hack into your information and create headaches for you and your family. America has experienced a dramatic increase in cyber attacks and malicious cyber activity. In the last five years, the FBI saw a 280% increase in complaints with 490% in losses to businesses and consumers – the pandemic did not help. How do you protect yourself?

Below are tips from the Orange County Intelligence Assessment Center:

1. If you are being solicited by a company or business you didn't expect to hear from, especially via email, be careful. Usually, it is best just to delete those emails.
2. Phishing and its related scams remain far and away the most common schemes, with criminals posing as legitimate companies sending out mass fake emails and text messages, sometimes hundreds of thousands at a time. Many now come via social media. During the holidays such schemes may have enough of a whiff of truth to lure in victims.
3. In general, don't open attachments or enter unknown sites. Hackers often place malware in email attachments. Legitimate retailers and shipping companies won't send offers, promo codes, and tracking numbers in attachments.
4. Check for a physical address, a customer service phone number, and a professional-looking site. Be sure tracking numbers are offered.
5. Only buy from secure sites with SSL encryption. These are URLs starting with https (rather than http) and contain a lock icon in the upper left corner of the toolbar. Even these can be spoofed, so remain careful.
6. If a site from a purported trusted retailer seems "off," step back. Warning signs of sketchy sites include poor spelling, odd design, and slow loading. Scammers often hastily post bogus sites, and international scammers may have poor English-language skills.
7. If a seller requests funds be wired directly to them via a money transfer company, prepaid card, or bank-to-bank wire transfer, it's a big red flag. Money sent these ways is virtually impossible to recover.
8. A credit card is still the safest way to pay for an online purchase because most have built-in protections. Alternatively, use a reputable third-party vendor such as Paypal or Venmo. Do this independently rather than using a vendor's link. Never give a seller direct access to your savings or banking accounts.
9. Parents who buy electronic devices for their children should consider purchasing a parental control product for android and iOS devices. With these, parents can more easily monitor a child's online activity through web filtering, location tracking, and app management and blocking.
10. Invest in a respected antivirus and malware detection system. Many are commercially available and easy to download. They can alert you if you are going into an unknown or suspicious site. They can also scan your computer to check for malware, an umbrella term for various malicious forms of software such as viruses, trojans, worms, and spyware, which can not only affect computer performance, but extract data, such as passwords, user IDs and more.

11. Use two-factor authentication (2FA) or multi-factor IDs. These add a layer of protection beyond your username and password. Usually, they involve a one-time security code sent to your device that you must enter to continue. Unless a hacker or scammer has physical possession of your device, they cannot gain access to the code.
12. Have different and strong passwords on every account you own, and especially on personal email. According to a report by Last Pass, although 91 percent of users know the risk of reusing passwords across sites, 66 percent do it anyway. A number of companies provide "vaults," where passwords can easily be stored and retrieved.
13. When your device alerts you to an update, by all means install the update.

Feel free to contact us at support@placentialibrary.org if you need assistance with implementation of these safety measurements or have questions. The assistance provided is for general information purposes only and does not constitute advice.

Always maintain a healthy dose of skepticism and common sense. Ask yourself – does it look right? If that spider sense is going off, listen to it! Additionally, if you have been scammed, report the suspected crime immediately to the FBI at www.ic3.gov. When shopping on Amazon, please consider selecting Placentia Library Friends Foundation as your charity.

What's the safest practice for gift shopping? Visit your local library and give the gift of family bonding and literacy. Check out a book, LOTs item, audiobook, e-books, movies, and much more. If you're busy with shopping and forget to return the items – no worries, there is no charge for overdue items. Your wallet will thank you! Oh! Don't forget to participate in our Yule Log cooking activity and the Winter Reading Program which ends January 13th!

I hope you'll enjoy some baking with your family today to celebrate National Cookie Cutter Day! If you have a cutout cookie recipe you'd like to share with me, I'd love to hear from you. Please email me at jcontreras@placentialibrary.org. Blessings to you all!

Respectfully,

Jeanette Contreras
Library Director