TIPS FOR A SAFE SEASON OF SPENDING

KEEP YOUR ONLINE SHOPPING SECURE FROM CHECKOUT TO DELIVERY

FAKE BILLS AND SHIPPING NOTIFICATIONS – Keep track of your orders and shipping confirmations. Be skeptical of notices you receive about orders you've made and those you don't remember placing. Scammers may send you a fake bill or shipping notification to make you believe something went wrong with your order. These email notifications will often ask you to provide additional personal or payment information. Don't automatically trust these emails. Instead, if you want to know the status of your order, go to the retailer's official website to view your order or contact them directly.

BOGUS PROMOTIONS – Exercise caution when you get an email offer that seems too good to be true from a company you don't recognize. Don't open any links or attachments from suspicious emails; they could install malware or viruses on your device.

VERIFY HYPERLINKS - Even in emails from retailers you trust, it is important to verify every link's destination. To do this, hover your cursor over the link or press and hold on your smartphone, this will show you the full web address. If it looks like a legitimate address that matches the description described in the email, it is probably safe to click through.

AVOID TRANSACTIONS OVER PUBLIC WI-FI – Shopping or banking on public Wi-Fi can be a serious risk. Many of these internet connections are not secure, which means your information isn't either.

SHOP ON SECURE HTTPS WEBSITES – When shopping online make sure the website URL starts with HTTPS, this means the webpage is encrypted and your payment information is protected.

PREVENT DOORSTEP THEFT – Nearly one-third of Americans report having packages stolen from their doorsteps. Take steps to protect yourself from parcel theft. Look into requiring a signature for your delivery or see if your order can be delivered to a carrier operated pick up location. You might consider sending packages directly to the intended gift recipient or to your workplace.

WATCH OUT FOR SCAMS THIS HOLIDAY SEASON

SURVEY SCAMS – Companies use surveys as a tool to receive valuable feedback, but scammers use them too. Many surveys incentivize your participation by offering a chance to win money or prizes. Most reputable surveys will only ask for basic personal contact information to notify you, like your name and email. Remember to never enter personal information like your Social Security Number or bank account information into an online survey, no matter the prize.

FAKE CHARITIES – During the season of giving, scammers take advantage of our generosity with fake charities. Take time to verify a charity's credibility before making a donation. Never feel pressured to give out your debit or credit card information over the phone or online. Give.org, run by the Better Business Bureau, is one resource you can use to verify charities.

GIFT CARD THEFT – Gift cards are a holiday gift staple, but before you pick up a few consider this risk. Gift cards sold on large display racks are more susceptible to tampering. Thieves open the packaging to copy the card information and use it to steal the funds once the card is activated. When you buy gift cards, it is better to buy directly from the retailer. For extra security ask a retailer's associate to purchase gift cards stored behind the counter, these are less likely to have been tampered with. Another option is to purchase Visa® Gift Cards from your local branch.

PHONY APPS – Smartphone apps can help you conveniently purchase gifts on the go and track your orders, but there are many fake apps available that mimic well-known brands. These apps can contain malware to steal your payment information or ransomware to disable your mobile device. Spot a phony app before you download by looking for red flags like a pixelated logo, bad customer reviews or misspellings and poor grammar in the description.

REMEMBER TO MANAGE AND MONITOR YOUR ACCOUNT

REVIEW YOUR BANK ACCOUNTS REGULARLY – Use one of our online banking or mobile banking services to access your balances and account history. Make sure the only transactions on your account are transactions you've made. If you find fraudulent charges, contact your local branch to shut down your debit card and file disputes immediately.

CARDVALET® – We now offer the CardValet® card management app to all Pinnacle Bank customers for free. This easy to use app gives you the ability to set up alerts for debit and/or credit card usage, deny certain types of transactions and turn your card off and on when needed. Download the app from the App Store or Google Play to help reduce your risk of fraud.

Bank of Colorado
THERE'S ONLY ONE

bankofcolorado.com