KaiPerm CREDIT UNION

December 1, 2020

Beware of Scams!

Top 10 Cybersecurity Tips for Holiday Shopping

1) Keep your smartphone, computer, and other devices updated. This helps ensure that your device has the latest security patches.
2) Only use trusted Wi-Fi connections and be suspicious of any network that does not require a password to connect.
3) Take the time to change any outdated or simple passwords. Use strong, unique passwords on all of your accounts.
4) Be careful not to overshare on social media. Consider anything you post to be public information
5) Keep an eye on the activity in your banking and credit card accounts. Also, be sure to monitor your credit report on a regular basis.
6) Be suspicious of emails you receive about online purchases. Check the status of your order directly on the website that you purchased from.
7) If you receive a holiday greeting card in your inbox, verify the sender before clicking the link to view the card.
8) If you're traveling for the holidays, be sure to keep your devices stored safely at all times
9) Pay close attention to the websites that you order from. Only shop on websites that you know and trust.
10) Watch out for giveaways and contests. Remember that if something seems too good to be true, it probably is.

Gift Card Scams – these can be either by email or phone calls. Someone generally posing as someone you know asking you to buy gift cards and provide them with the gift card numbers or to scan pictures of the gift cards to them and they will reimburse you the funds. You will receive a check for the funds, but the check will come back unauthorized and the funds on the gift cards will be spent by the fraudster.

Loan Scam – not all online loan companies are what they say. The newest loan scam will offer to match you with the best loan company for your needs. They will email you paperwork to fill out and ask for a debit card number for the loan processing fee if you are approved. They will then ask for your routing number and account number too electronically deposit the loan funds into.

Phone Scam – you will receive a call from someone stating they work for a specific company and that you owe them money, but to cancel the transaction they will need to access your computer. By giving them access they will have access to everything on your computer including passwords.

Smishing Scams – you may receive a short or vague email or text message with a link to look up more information. With the holidays approaching they could say regarding your order or regarding your package. By clicking on the link it will give the scammer full access to your device. Please always go to the specific website you ordered from to get any additional information or tracking.

Let us help you get ahead financially!

NCUA insured up to $250,000

Main - 7505 NE Ambassador Place, Suite A Portland OR 97220 – 971.266.4900
KPB - 500 NE Multnomah Ste 140 Portland OR 97232 - 503.813.3211 (temporarily closed)
Westside - 2875 NW Stucki Ave (Lower Level) Hillsboro OR 97124 - 971.310.3010 (temporarily closed)