# Fraud Protection

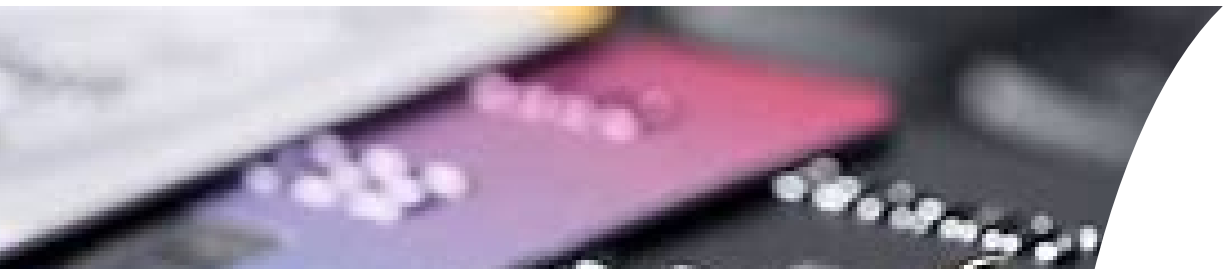
1. We will never call you to request information you received via text (SMS) or pressure you to reset your online banking password.
2. A text alert from us warning of suspicious activity on your account or card will never include a link to be clicked. A text alert from us will always be from a 5-digit number and NOT a 10-digit number.
3. We will never call and ask you for your Debit Card PIN or 3-digit security code on the back of your card. Don't give this out to an unsolicited caller, no matter what they say. Hang up and call us directly.
4. Don't provide your online banking log in credentials, password, debit card number/code, account number or personal information by email, text or on an unsolicited call. Contact your local Bank of Commerce branch directly or call us at **620-431-1400.**
5. Use caution when making online purchases. If it sounds too good to be true, it has a high probability of fraud.
6. When being solicited for charitable donations over the phone, don't give your card information directly to the solicitor. Use the charitable organization's website instead.
7. Don't trust caller ID: Caller ID may be modified to show your financial institution's name.
8. Don't give an unsolicited caller remote access to your computer.

# Tips to keep your information safe

1. Choose unique passwords
2. Use two-factor authentication when available
3. Avoid public Wi-Fi and computers
4. Sign up for alerts
5. Never give out personal information
6. Avoid clicking links in suspicious emails, text messages, or landing pages
7. Use security software to protect your devices from attack
8. Here are some more tips from the American Bankers' Association: https://www.banksneveraskthat.com/

# Monitor your online account

To help detect fraud quickly, we recommend checking your online banking account regularly, and enrolling for alerts to receive notifications of account activity. If anything looks amiss, call us directly for assistance.



Bank of Commerce