DIGITAL BANKING BEST PRACTICES

Protect Sensitive Information

- Never share banking information or login credentials with someone by phone, text or email (even when told it is someone from your institution). This includes Username, Password, Security Question answers, and Out of Band Authentication Codes.
- Use longer, unique passwords or pass phrases.
- Contact your financial institution immediately and change all passwords and security questions if you ever feel your digital banking credentials or financial information has been compromised.

Protect Debit/Credit Cards

- Use tap and pay (contactless) and/or chip instead of swiping, when possible.
- Store debit and credit cards in a place that isn't susceptible to theft.
- Never release your personal identification number (PIN) to anyone, including your financial institution.

Monitor Accounts Closely

- Set up account alerts to verify and monitor account activity. Check with your financial institution on what options are available for you.
- Access accounts and review all communications shared by your financial institution on a regular basis.

Be on the Lookout for Common Fraud Schemes

- "Too good to be true" deals are most often just that and usually a scam.
- Beware of fraudsters who play on consumers' emotions to acquire personal and financial information.
- Never respond to an Out of Band Authentication (text/call/push notification) that you did not initiate.
- Don't assume a call from your bank's phone number is legitimate. Fraudsters can spoof caller ID to masquerade as someone from your bank. If you receive a call from your bank asking for sensitive information or asking for you to log into your digital accounts, do NOT provide answers. Hang up and call your bank directly.
- Beware of phishing emails/texts claiming to contain information about a delivery parcel or fraudulent transactions.
- Just because it looks official doesn't mean it is. Fraudsters are becoming more genuine in appearance. They can use CAPTCHA, send out of band codes or messages, and utilize virtual assistants or chat bots.

sun canyon™ BANK