CENTRAL BANK
COMMITMENT TO COMMUNITY

Tips for Online Banking Security

1. Never give out your Online Banking ID or password to anyone (this includes verbally in person or on the phone, email, text message)
2. Never click a link in an email or a text message that you do not know from where it came.
3. Be suspicious of every text message and email that asks or demands personal information.
4. Remember, just because someone identifies themselves on the phone does not mean they are telling the truth.
5. No reputable institution will call, text or email you and ask for personal information, such as Social Security number, online banking log in information, debit card information, etc. DO NOT GIVE IT OUT.
6. Phone numbers and email addresses can be spoofed (faked). If you have questions, call the person or business or institution from reliable contact information, never from a link in an email or text or information given in a phone call that you did not initiate.
7. Do not give someone who randomly contacts you by a phone call access to your computer. IT repair people do not make cold calls looking for a computer to fix. If you suspect someone has gained access to your computer, turn it off. Disconnect the Internet before you turn it on to clean with your virus software. You can also take it to a computer repair shop.
8. If you accidently or on purpose give anyone your online banking information, account numbers or any personal banking information, contact the bank immediately.
9. You cannot get something for nothing. If it seems too good to be true, it probably is.