Mobile Banking Fraud Protection

New and sophisticated ways to commit fraud are increasing at an alarming rate. The rapidly growing number of individuals using smartphones for mobile banking has created a new target for cybercriminals to exploit.

Much like online fraud, mobile banking fraud involves attempts to obtain a user's confidential login information — including passwords, personal ID numbers and token codes — to accounts and improperly transfer money or commit other fraudulent acts.

Mobile banking fraud is often difficult to detect. You may be unaware information has been stolen until the money is gone from your accounts.

Here's what you should do to protect your money:

- Protect your login information. Never give your user IDs, passwords or access codes to anyone who contacts you by telephone, email or text message. Commercial State Bank will never contact you to ask for this information.
- Be careful choosing apps. Follow safe practices to avoid unnecessary risks, such as installing apps from third-party sites or unreliable sites.
- Don't follow links in emails or text messages that claim to be from your financial institution, especially those expressing an urgent need for you to update your information, activate an account, or verify your identity by calling a phone number or submitting information on a website. It likely is a scam. Go directly to your bank's mobile banking service to do your banking. Forward all suspicious emails and text messages to csb@csbec.com or security@csbec.com.
- Monitor online accounts regularly to detect suspicious activity. Immediately contact your Commercial State Bank account representative if you notice anything out of the ordinary.
- Lock your smartphone when it's not in use, and store it in a secure location. Keypad and phone lock functions password-protect your smartphone so no one else can use it or view your information.
- Delete text messages from your financial institution frequently, especially before loaning, discarding or selling your smartphone.
- Utilize additional controls around the movement of funds. (e.g. transaction authorization controls)