ПАМЯТКА
по обеспечению безопасности при работе
в системе дистанционного банковского обслуживания «Банк Заречье»
для физических лиц

Для обеспечения достаточного уровня защиты информации при работе с системой дистанционного банковского обслуживания «Банк Заречье» (далее по тексту – система, ДБО) с использованием web-браузера или мобильного приложения, «Банк Заречье» (АО) настоятельно рекомендует соблюдать следующие меры информационной безопасности:

1. В обязательном порядке **УСТАНОВИТЬ** на SIM-карту телефона, с которого планируется пользоваться мобильным приложением, PIN-код и **ВКЛЮЧИТЬ** в телефоне запрос PIN-кода SIM-карты при включении телефона;
2. Самостоятельно устанавливать мобильное приложение на свое мобильное устройство только с интернет-сайтов и из магазинов приложений, перечень которых указан на информационных стендах в операционных залах полевых учреждений и на официальном сайте Банка;
3. **НЕ ХРАНИТЬ** код и пароль для входа в мобильное приложение непосредственно на мобильном телефоне, планшете или компьютере, на котором оно установлено;
4. Использовать **СЛОЖНЫЙ ПАРОЛЬ**: не менее восьми символов, заглавные и прописные буквы латинского алфавита, цифры. Не рекомендуется использовать последовательность одинаковых символов, персональную информацию (например, имя, дату рождения клиента, членов его семьи, номера телефонов);
5. При утрате логина/пароля или подозрении об их компрометации необходимо **СРОЧНО ИЗМЕНИТЬ** его или **СООБЩИТЬ** в Банк о необходимости блокировки доступа к Системе ДБО:

   - по телефонам: (843) 557-59-74, (843) 557-59-88 с 8 часов 00 минут до 17 часов 00 минут (в рабочие дни)
   - передать сообщение по электронной почте на адрес dbo@zarech.ru

6. При утрате мобильного устройства необходимо **СРОЧНО ОБРАТИТЬСЯ** в Банк для временной блокировки карты и доступа в Систему ДБО. При восстановлении доступа на новом мобильном устройстве **ПРОВЕРИТЬ** все действия и операции в Системе ДБО за период его отсутствия;
7. **МЕНЯТЬ** код для входа в мобильное приложение не реже одного раза в три месяца;
8. **ИЗБЕГАТЬ** присутствия третьих лиц при вводе логина и пароля или регистрации в мобильном приложении, включая момент формирования логина и пароля.
9. **ОБЕСПЕЧИТЬ** хранение мобильного устройства способом, исключающим доступ к нему третьих лиц;
10. **НЕ ВЫПОЛНЯТЬ** операции по повышению привилегий или взлому операционной системы мобильного устройства (получение root-прав для Android, установка jailbreak для iOS), на котором установлено или планируется установка мобильного приложения. Не устанавливать мобильное приложение на устройство, которое уже получило такие привилегии;
11. **ИСПОЛЬЗОВАТЬ** современное антивирусное программное обеспечение предпочтительно российского производства и следить за его регулярным обновлением для своевременного обнаружения вредоносных программ;
12. По рекомендации компании-производителя мобильного устройства **СВОЕВРЕМЕННО ОБНОВЛЯТЬ** его операционную систему;
13. При прекращении использования мобильного устройства **УДАЛИТЬ** установленное мобильное приложение, личные данные и финансовую информацию.