Общие рекомендации и правила безопасной работы с мобильными устройствами

Пользуясь мобильным телефоном или планшетом, не следует забывать об уязвимости устройства для мошеннических атак, если не предпринимать мер предосторожности, необходимых при работе с такими устройствами.
Соблюдая следующие рекомендации, вы обезопасите себя от угроз интернет-мошенничества:

- не передавайте и не сообщайте никому личную информацию (в т.ч. свои пароли, переменные коды, съемные носители с криптографическими ключами и другие средства доступа);
- в случае утраты каких-либо данных (паролей, переменных кодов, ПИН-кодов и т.д.) или подозрении об их утрате необходимо немедленно сообщить об этом в банк и заблокировать
- используйте только лицензионное программное обеспечение;
- установите на своё устройства антивирус и регулярно обновляйте его;
- избегайте на своём мобильном устройстве настроек типа root и jailbreak;
- не проходите по сомнительным ссылкам;
- не устанавливайте приложения из неизвестных источников, приложения необходимо устанавливать только через официальные магазины: Google Play, Apple Store;
- для входа в официальный магазин не использовать внешние ссылки с других ресурсов, вход осуществлять только через «иконку» магазина в мобильном телефоне;
- вход в мобильное приложение через ввод логина и пароля не дает гарантии сохранности средств, если клиент будет пренебрежительно относиться к правилам безопасности. Нельзя хранить конфиденциальную информацию, такой как логин, пароль, номера карт, коды CVV2 и др., в памяти мобильного телефона;
- рекомендуется изменять пароль для доступа в приложение не реже чем один раз в квартал;
- если вы обнаружили, что ваша SIM-карта заблокировалась без вашего ведома, немедленно заблокируйте доступ в Мобильный-банк, обратившись в службу поддержки по телефонам в Самаре: (846) 251-0000, в Новокуйбышевске: (84635) 57-058, в Тольятти: (8482) 55-80-93, в Калуге (4842) 22-03-03.

Политика конфиденциальности мобильного приложения.

Контакты – Позволяет просматривать список контактов из мобильного устройства и осуществлять вызовы. Необходимо для поддержания функции приложения «Перевод другому клиенту банка по номеру телефона», быстрому переходу к набору номера службы поддержки (Call-центр), а так же отправке приглашений через оператора мобильной связи.

Управление SMS (Прием / Просмотр SMS) – Позволяет следить за входящими сообщениями. Разрешение необходимо для автоматического заполнения поля пароля, пришедшего в SMS.

Сведения об устройстве – такие как модель, версия операционной системы, уникальные идентификаторы устройства, а также данные о мобильной сети и номер телефона). Идентификаторы устройств позволяют определять, какое оборудование вы используете для доступа к нашим услугам. Это позволяет нам лучше понять, что подходит для вашего устройства, и анализировать связанные с ним сбои в работе наших продуктов.

Управление камерой – Позволяет получать изображение с камеры устройства. Разрешение необходимо для автоматического предзаполения номера карты другого клиента банка для выполнения перевода.

Другое – Также для удобства использования приложения запрашивается разрешения для: управления вибросигналом, предотвращение переключения устройства в спящий режим, использования доступа Internet на мобильном устройстве.

С правилами предоставления услуг по дистанционному обслуживанию можно ознакомиться на сайте Банка