



СОЦИУМ-БАНК

**БЕЗОПАСНОСТЬ
МОБИЛЬНЫХ УСТРОЙСТВ**



Наша цель - рассказать основные правила безопасности при работе с мобильными устройствами.

Согласно отчету Центрального банка РФ, наибольший объем хищений денежных средств за 2024 год осуществлялся по операциям, связанным с использованием систем дистанционного банковского обслуживания (9 602,57 млн рублей). В общем объеме хищений основную долю составляют денежные средства, похищенные у клиентов — **физических лиц**.

Наиболее распространенным методом осуществления операций без добровольного согласия с использованием мобильного устройства является его заражение вредоносным кодом. Использование методов социальной инженерии (ссылки в СМС-сообщениях, реклама на сайтах и так далее) существенно повышает вероятность заражения мобильного устройства. При этом злоумышленник получает возможность составления распоряжений об осуществлении переводов денежных средств, а уведомления о совершении операций по переводу денежных средств могут быть недоступны владельцу мобильного устройства.

По статистике за 2024 год объем операций без добровольного согласия клиентов увеличился по сравнению с 2023 годом на 74,36% ¹



¹ https://cbr.ru/analytics/ib/operations_survey/2024/

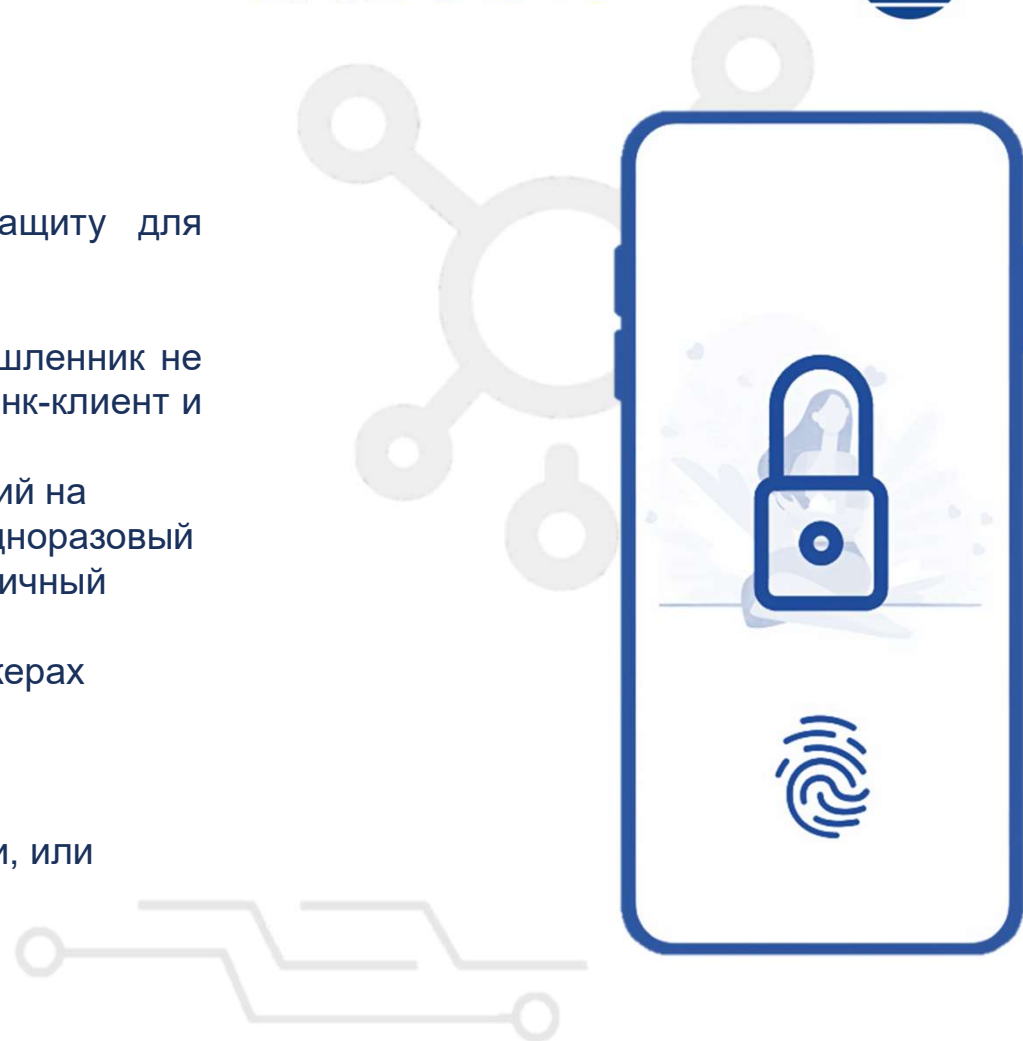
МОБИЛЬНЫЙ ТЕЛЕФОН



1. Защита смартфона на случай его утери:

- Используйте пароль или биометрическую защиту для входа в телефон;
 - Включите функцию «**Найти устройство**»;
 - Установите **PIN-код на SIM-карту**. Так злоумышленник не сможет ей воспользоваться для входа в Ваш банк-клиент и другие приложения;
 - **Отключите отображение SMS (push)** сообщений на заблокированном экране. Так никто не узнает одноразовый код, который отправляют сервисы для входа в личный кабинет;
 - Храните пароли в специализированных менеджерах паролей;
 - Создавайте резервные копии.
- Удалите чувствительные данные с карты памяти, или шифруйте их.

При утере телефона они могут быть доступны злоумышленнику.



МОБИЛЬНЫЙ ТЕЛЕФОН



2. Безопасность в сети:

- Используйте платные средства Антивирусной защиты для мобильных устройств (предпочтительно отечественные);
- Своевременно обновляйте операционную систему и приложения своего устройства;
- **Не переходите по неизвестным ссылкам** из SMS или мессенджеров;
- **Избегайте** использования **публичных Wi-Fi сетей**. Если на каком-то сайте Вам нужно ввести свой пароль, он будет доступен владельцу Wi-Fi;
- **Не отправляйте** конфиденциальную информацию **через бесплатный Wi-Fi**;
- **Не «раздавайте» свой Интернет** неизвестным личностям;
- **Отключайте Bluetooth и Wi-Fi**, если они не используются;
- Обучайтесь основам цифровой гигиены.

МОБИЛЬНЫЙ ТЕЛЕФОН



3. Осторожность при звонках:

- **Не сообщайте пароли**, коды из СМС и PUSH-уведомлений, конфиденциальную информацию по телефону, **даже работникам Банка!**
- **Будьте бдительны при звонках** от «служб безопасности» или «техподдержки». Перезванивайте по официальным номерам для проверки информации, которую Вам сообщают;
- Если при разговоре Вы слышите слово **«деньги»**, **«срочно»** или Вам кто-то угрожает, даже если это родственник или руководитель - убедитесь, что это он Вам звонит. Сверьте номер телефона или аккаунт в мессенджере с теми, что написаны в Ваших контактах. Может оказаться, что у звонящего **«начальника»** в *Telegram* аккаунт написан как @ravei, а в ваших контактах руководитель записан как @ravel;
- **Номер телефона** при входящем звонке **может быть подделан**. Опять же, если разговор идет о деньгах или угрозе для Вас, перезвоните по официальному номеру самостоятельно, а этот звонок завершите.



МОБИЛЬНЫЙ ТЕЛЕФОН



4. Приложения и QR-коды:

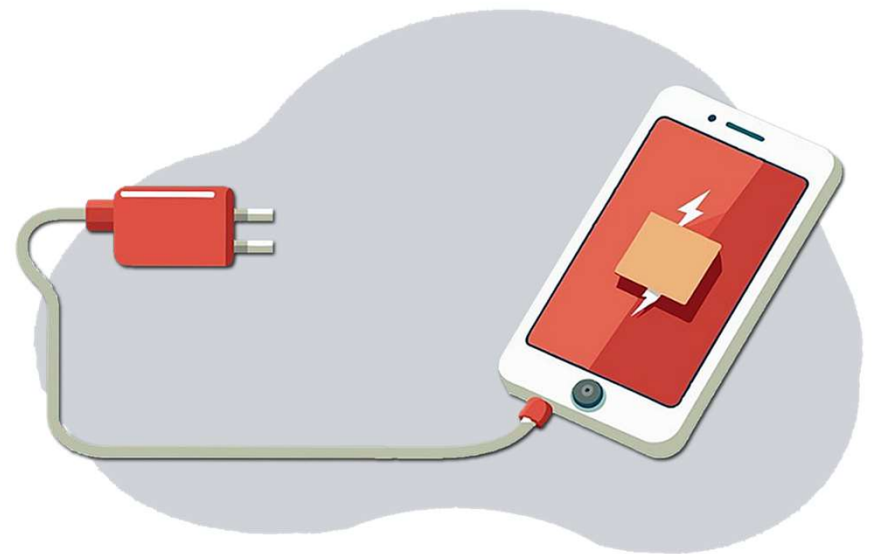
- Устанавливайте приложения **только из официальных магазинов** (App Store, Google Play, AppGallery, RUSTORE);
- **Проверяйте разрешения** приложений;
- **Проверяйте приложения** Антивирусом;
- При сканировании QR-кодов в публичных местах **проверяйте, не наклеен ли поверх него еще один QR**;
- Если Вам пришла квитанция для оплаты по QR-коду, то **внимательно изучите платёжные данные**, которые увидите после сканирования. Убедитесь, что они действительно принадлежат той организации, чьи услуги Вы собираетесь оплатить;
- **Не сканируйте всё подряд!** Одно дело QR-код в меню ресторана или в магазине, другое — в объявлении на заборе;
- Относитесь к любому QR-коду, как к любому мошенническому сайту на который Вы можете попасть. При переходе сайт для ввода данных может быть похож на официальный, тщательно проверяйте адрес.

МОБИЛЬНЫЙ ТЕЛЕФОН



5. Физическая безопасность и конфиденциальность:

- **Не оставляйте телефон без присмотра!**
- **Не давайте детям доступ** к своему устройству (игры, мультки, фото, Интернет), ведь на нем банковское приложение – это риски незапланированных покупок и переводов денежных средств;
- Будьте осторожны при использовании публичных зарядных устройств. **Используйте свой шнур** для зарядки;
- **Не подключайте телефон** к незнакомым компьютерам;
- Наклейте на устройство «**антишпионское защитное стекло**» для защиты экрана в публичных местах;
- **Не обсуждайте** конфиденциальную (рабочую) информацию в общественных местах;
- **Не копируйте рабочие документы** на личное устройство и **не отправляйте их** на личную почту.



В СЛУЧАЕ ПОТЕРИ ИЛИ КРАЖИ ТЕЛЕФОНА



Немедленно сообщите об этом в БАНК !

1. Попробуйте удаленно заблокировать устройство.
(Посмотрите в Интернете, как это сделать)
2. Позвоните своему Оператору связи и заблокируйте SIM-карту!
3. При возможности, смените пароли ко всем важным сайтам и службам.
4. В случае кражи, напишите заявление в Полицию.



1

ОБРАЩЕНИЕ В БАНК



- ✓ Позвонить на общий номер банка **+7 (499) 943-96-05**
- ✓ Прийти лично в офис банка
- ✓ Написать на электронную почту: DBO_FL@socium-bank.ru (для физических лиц)
DBO_UL@socium-bank.ru (для юридических лиц)
- ✓ Написать обращение через обратную форму связи <https://socium-bank.ru/appeal/>