



**ПРАВИЛА БЕЗОПАСНОСТИ
ПРИ ИСПОЛЬЗОВАНИИ
БАНКОВСКИХ КАРТ И
БАНКОМАТОВ**



Наша цель - рассказать основные правила безопасности при работе с банковскими картами, в том числе при оплате в Интернете.

Системы банков надежно защищены от мошенничества, но существует риск раскрытия Вами личных данных и использования их злоумышленниками.

И все таки задайте себе вопрос, сталкивались ли Вы:

1. Со звонками из «Центрального Банка, ФСБ, МВД, Прокуратуры и пр. органами власти»?
2. Получением СМС от банка со «странными номерами»?
3. Просьбой перевода денег «по ошибке» от неизвестных?
4. Просьбой ребенка или родственника «попавшего в беду» перевести деньги?
5. Давлением и угрозами перевести деньги на «безопасный счет»?
6. С нелегитимными списаниями денежных средств со своего счета?

Согласно статистике Центрального Банка РФ, 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/



БАНКОВСКАЯ КАРТА



ЧТО ВАЖНО ЗНАТЬ?



Банковская карта – пластиковая карточка, которая используется для оплаты товаров и услуг, в том числе через Интернет, а также для снятия наличных денег.

CVC/CVV – три цифры на задней стороне банковской карты – код для проверки её подлинности. CVC был придуман для того, чтобы можно было подтвердить подлинность карты при оплате дистанционно, например в Интернете.

Токенизация банковской карты - это метод замены конфиденциальной информации банковской карты на уникальный обезличенный аналог (токен). Например токенизация лежит в основе технологии **Mir Pay**, которая позволяет платить телефоном вместо банковской карты.

PIN код – код, обычно состоящий из четырёх цифр и использующийся для подтверждения личности владельца карты при обналичивании денежных средств через банкомат, пополнении баланса карты через терминалы и банкоматы, совершении покупок в магазинах (не в Интернет), начиная с определённой суммы.

НИКОМУ НЕ СООБЩАЙТЕ ДАННЫЕ КОДЫ – ДАЖЕ РАБОТНИКАМ БАНКА!

ОПЛАТА В ИНТЕРНЕТЕ



РЕКОМЕНДАЦИИ

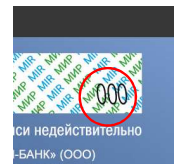
Желательно оплачивать покупки при защищенном соединении сайта, о чем будет свидетельствовать значок «щита», и адрес будет начинаться с протокола **https://**



 **Банк «Социум Банк»**
socium-bank.ru 



При использовании отечественных поисковых систем, лучше отдавать предпочтение сайтам с [галочкой подтверждения](#) организации



CVC/CVV код карты НУЖЕН при:

- Совершении покупок в Интернете
- Операциях в Интернет-банкинге — это действия держателя карты через приложение или личный кабинет через сайт банка
- Входе в отделение Банка (где карта используется как ключ)



Для оплаты покупок в Интернете выпустите виртуальную карту, и перечислите на нее необходимую сумму

РАБОТА ЧЕРЕЗ БАНКОМАТ



РЕКОМЕНДАЦИИ



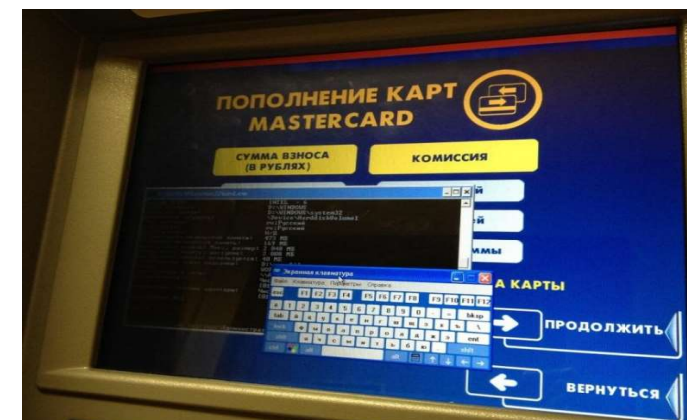
Осмотрите банкомат на предмет посторонних устройств (накладной клавиатуры, считывателя, камер направленных на поле ввода **PIN** – кода т.д.) В случае обнаружения подозрительных вещей, просьба сообщить об этом по общему телефону банка или воспользоваться формой обратной связи
<https://socium-bank.ru/appeal/>

PIN - код карты НУЖЕН при:

- Денежных операций в банкомате (когда снимаете и вносите наличные, совершаете переводы, оплачиваете ЖКХ и т.д.)
- Расчёт за «оффлайн» товары и услуги через платёжный терминал в магазине



Не пользуйтесь банкоматом, если видите подозрительные всплывающие окна, или если по Вашему мнению банкомат некорректно себя ведет. В случае обнаружения такой активности, просьба сообщить об этом по общему телефону банка или воспользоваться формой обратной связи <https://socium-bank.ru/appeal/>



МОШЕННИЧЕСТВО



КАК РАСПОЗНАТЬ МОШЕННИКА ПО ТЕЛЕФОНУ?



- ! Ваш родственник, «попавший в беду» просит перевести деньги через банкомат на неизвестные счета
- ! Сотрудник ФСБ, МВД, Прокуратуры или ЦБ, предлагающий перевести деньги на «безопасный счет»
- ! Работник банка, выманивающий данные карты и пароли из СМС под предлогом мошенничества по Вашей карте или сбоях системы
- ! Работник ЖКХ, предлагающий выполнить оплату «за долги» посредством внесения данных карты на мошеннический ресурс
- ! Внезапность и требование быстрого принятия решения от звонящего



МОШЕННИЧЕСТВО



КАК РАСПОЗНАТЬ МОШЕННИКА ЧЕРЕЗ ИНТЕРНЕТ?



Вам приходят СМС под видом Вашего банка о списаниях крупных сумм, после чего происходит звонок от мошенника



В социальные сети или на электронную почту приходит письмо с выигрышем и ссылкой, где нужно ввести данные своей карты



Вам приходит СМС об «ошибке зачисления» денежных средств



Человек в Интернете просит оплатить ему покупку за «бартер»



Оплата товаров через [Telegram-боты](#) и прочие ненадежные сервисы



РЕКОМЕНДАЦИИ



- Не передавайте карту третьим лицам
- Не сообщайте никому данные своей карты
- Измените PIN-код в банкомате на известный только Вам и запомните его
- Никому не говорите PIN-код и код безопасности (CVC/CVV) Вашей карты
- Не храните PIN-код рядом с картой
- Осмотрите банкомат перед пополнением или снятием денег
- Не выбрасывайте в урну чек, который печатает банкомат
- Если потеряли телефон или сменили номер мобильного, обратитесь в банк
- Не подключайте к СМС - информированию чужие телефоны
- Не сообщайте никому коды из СМС
- Если получили СМС о переводе, который не совершали, обратитесь в банк
- Если получили СМС о получении средств которых не ждете, обратитесь в банк
- Не переводите самостоятельно денежные средства «полученных по ошибке»
- Не совершайте какие-либо операции с картой по инструкциям звонящего
- Не оплачивайте товары на сомнительных сайтах и сервисах
- Своевременно обновляйте ПО и используйте Антивирусы на устройствах



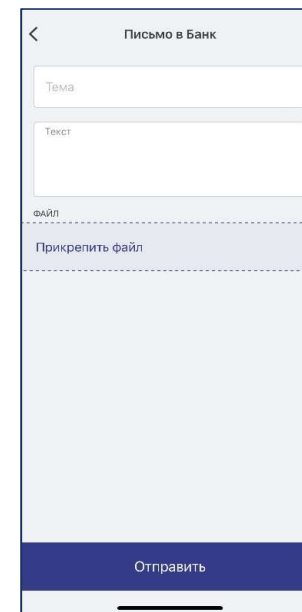
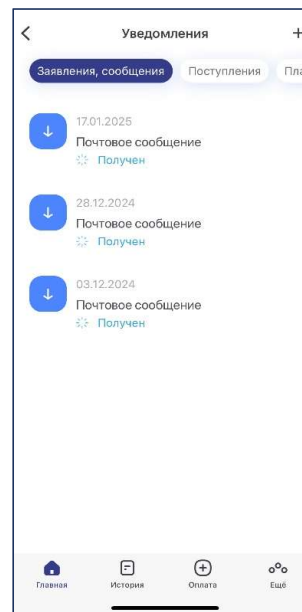
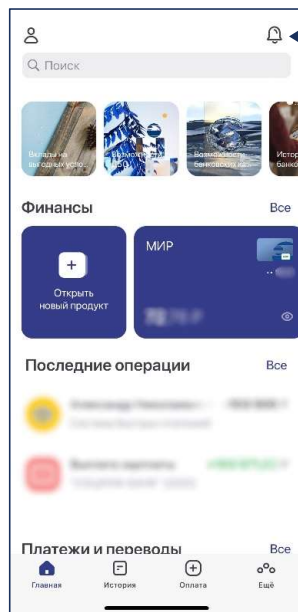
ПРИ КОМПРОМЕТАЦИИ ВАШЕЙ КАРТЫ, ОБРАТИТЕСЬ В БАНК!

ОБРАЩЕНИЕ В БАНК



- ✓ Прийти лично в офис банка
- ✓ Позвонить на общий номер **+7 (499) 943-96-05**
- ✓ Обратиться через моб. приложение «СОЦИУМ-БАНК»

ОБРАЩЕНИЕ В БАНК



ЧЕРЕЗ МОБИЛЬНОЕ ПРИЛОЖЕНИЕ

- 1 В своем личном кабинете щелкнуть на значок «колокольчика»
- 2 Далее нажать на значок «+»
- 3 В поле тема напишите кратко цель обращения, а в поле текст опишите подробно свою проблему