



Банк России

ФИНАНСОВОЕ МОШЕННИЧЕСТВО

Защити себя и свою семью!

Финансовая грамотность
для старшего поколения





С банковскими картами



Кибермошенничество



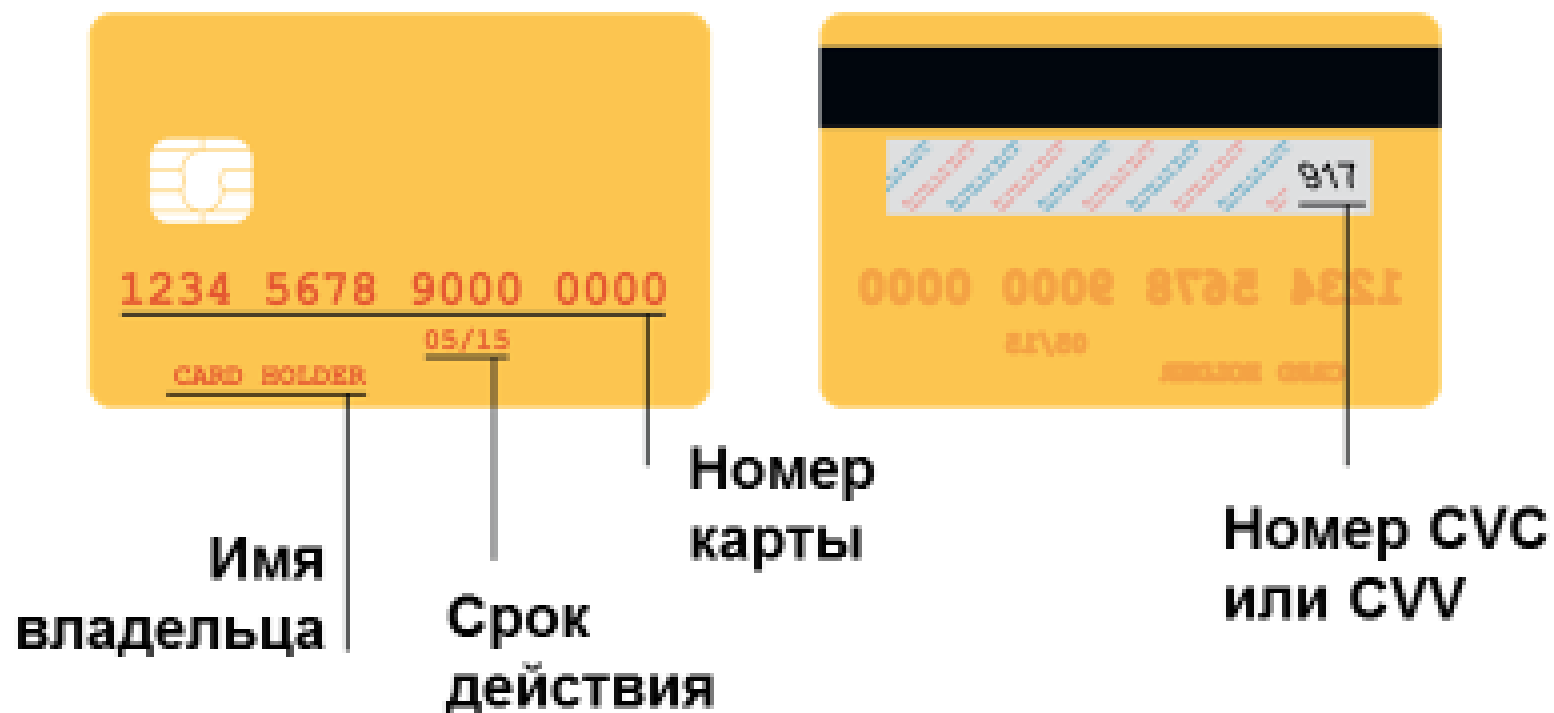
От имени государственных учреждений



Финансовые пирамиды

Врага надо знать в лицо

Информация
банковской
карты:





МОШЕННИЧЕСТВО С БАНКОВСКИМИ КАРТАМИ

- ПИН-код – четырехзначный код!
- Выдается в конверте!
- Можно поменять самостоятельно!
- Прикрывайте ПИН-код своей рукой, чтобы окружающие вас люди не видели ваших цифр!
- Никогда и никому не сообщайте свой ПИН-код!
- Не храните конверт с ПИН-кодом и карту в одном месте!



- номер вашей карты
- имя и фамилию владельца
- срок действия

Ваша персональная информация

- ПИН– код

Мошенник может снять все деньги с карты.

- код проверки подлинности карты (на оборотной стороне)

Мошенник может оплачивать вашей картой свои покупки в интернете.

- одноразовый пароль (смс-сообщение для подтверждение платежа)

Мошенник может войти в интернет-банк и получить доступ к вашим счетам.



В БАНКОМАТЕ И МАГАЗИНЕ

Проверьте, нет ли посторонних устройств.

Банкоматы внутри отделения банка безопаснее.

Прикрывайте рукой вводимый PIN-код.

Сохраняйте чек, полученный в банкомате и магазине.

Сверяйте все платежи с банковской выпиской.

Не разрешайте забирать карточку в магазине — настаивайте на том, чтобы все операции проводились при вас.



Не оставляйте карту без внимания, не передавайте посторонним лицам!

- Никому не говорите свой логин и пароль для входа в интернет-банк, а также код подтверждения оплаты!
- Платите только на защищенных страницах.
- Установите антивирусную программу против «фишинга».
- Заведите специальную карту для оплаты покупок в интернете и не держите на ней много денег!
- Не экономьте на SMS-уведомлениях о платежах и переводах с вашей карты – это малая цена за спокойствие!

Интернет тебе не враг, если знаешь что и как!





Если мошенники списали деньги с ВАШЕЙ БАНКОВСКОЙ КАРТЫ

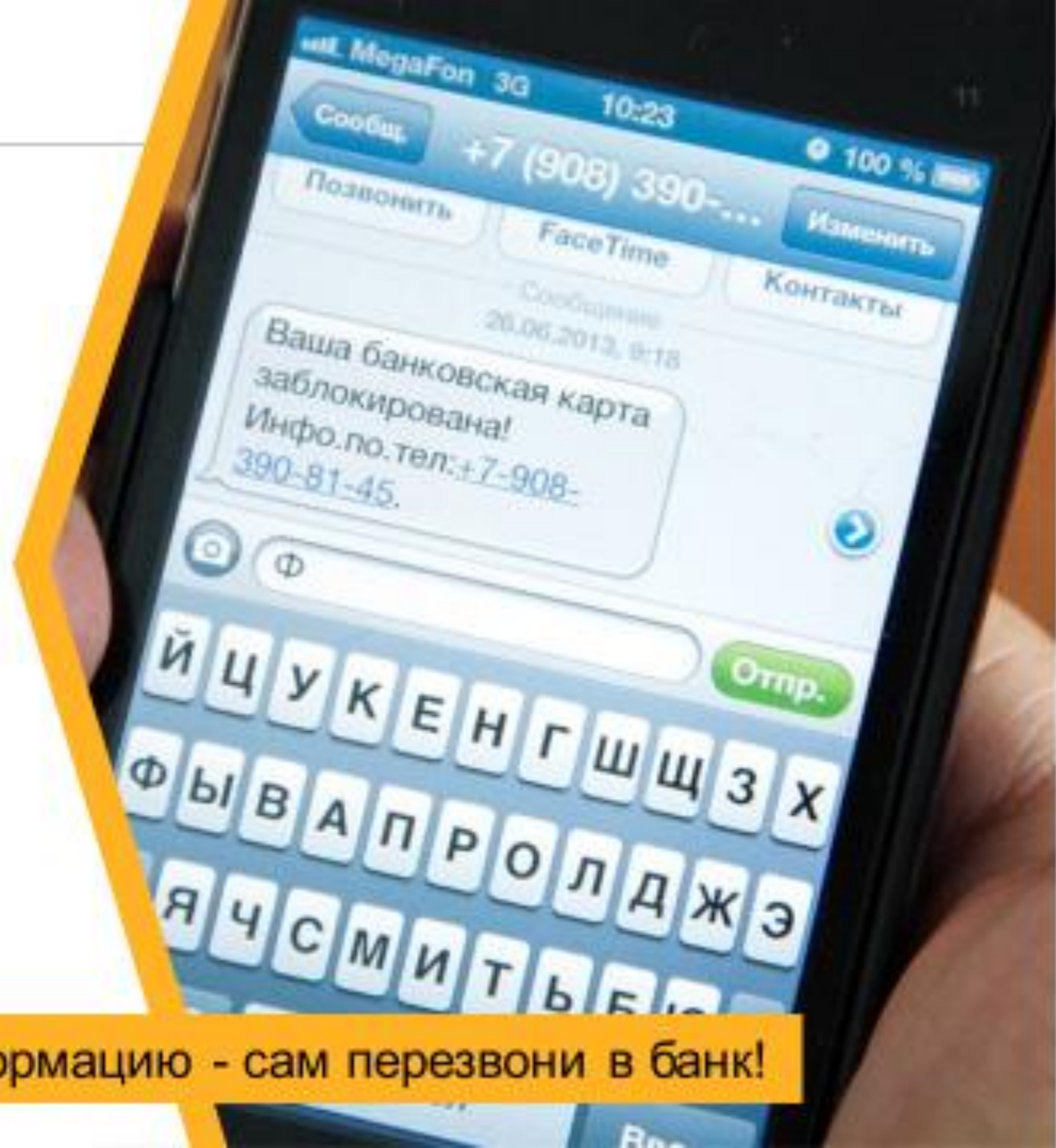
1. Позвоните в банк и заблокируйте карту.
2. Обратитесь в отделение банка и попросите выписку по счету.
3. Напишите заявление о несогласии с операцией.
4. Сохраните экземпляр заявления с отметкой банка о приеме.
5. Обратитесь полицию с заявлением о хищении.





Кибермошенничество. Каким оно еще бывает?

- СМС или письмо якобы от банка со ссылкой или просьбой перезвонить.
- Звонок якобы от имени банка: вас просят сообщить личные данные.
- СМС об ошибочном зачислении средств или с просьбой подтвердить покупку.
- СМС от имени родственников, которые просят перевести деньги на неизвестный счет.



Проверяй информацию - сам перезвони в банк!



- Не верьте безоговорочно даже «солидным организациям».
- **Не спешите** и задавайте вопросы.
- Если поверили, спросите ФИО, должность и контактный телефон для подстраховки.
- Не покупайте на дому.
- Не принимайте поспешных решений, не переводите никому деньги.



- Отсутствие лицензии Банка России.
- Обещание гарантированного сверхдохода.
- Компания-«новичок», отсутствие собственных основных средств и активов.
- Предварительные взносы.
- Размытые формулировки инвестиционной деятельности.
- В договоре четко не прописаны обязательства организации перед инвестором.
- Вас просят приводить новых клиентов, выплаты за счет средств других вкладчиков.

Обещания высокой доходности – признак финансовой пирамиды!



**В Банк России через
интернет-приемную
на сайте CBR.RU**



Правоохранительные органы



Роспотребнадзор

Финансовому
уполномоченному

Общественные организации:



«За права заемщиков»
www.zapravazaemschikov.ru



Конфедерация обществ потребителей
www.konfop.ru



Федеральный общественно-государственный
фонд по защите прав вкладчиков и акционеров
www.fedfond.ru



Задать вопрос и оперативно получить ответ с разъяснениями тех или иных законов/правил, проверить лицензию финансовой организации, найти на карте её ближайший офис, прочитать новости из мира финансов можно в мобильном приложении **«ЦБ онлайн»**.

App Store**Google Play****ЦБ онлайн**