

ПРИВИВАЕМ КУЛЬТУРУ ФИНАНСОВОЙ ГРАМОТНОСТИ



Банк России

FINCULT.INFO



УРОК 1



УРОК 2



УРОК 3



УРОК 4



Урок № 4

«Правила безопасности»



**Не экономьте на СМС-уведомлениях
о платежах и переводах с вашей
карты
– это малая цена за спокойствие!**



**Никому не сообщайте ПИН-код!
Не записывайте ваш ПИН-код на
карту!**

Безопасное использование банковских карт: банкомат

- Проверьте, нет ли посторонних устройств
- Банкоматы внутри отделения банка безопаснее
- Прикрывайте рукой вводимый ПИН-код
- Сохраняйте чек, полученный в банкомате
- Сверяйте все платежи с банковской выпиской

Основные виды мошенничеств с банковскими картами: скимминг

**ОРИГИНАЛЬНАЯ НАКЛАДКА
ДЛЯ ВВОДА КАРТЫ**



**ФАЛЬШ - НАКЛАДКА
ДЛЯ ВВОДА КАРТЫ**

**ОРИГИНАЛЬНАЯ НАКЛАДКА
ДЛЯ ВВОДА КАРТЫ**



**ФАЛЬШ - НАКЛАДКА
ДЛЯ ВВОДА КАРТЫ**

Лучше проводить операции через банкоматы, которые находятся в помещении отделения вашего банка. Это более безопасно и надежно.

Безопасное использование банковских карт: магазин или кафе

- Следите, чтобы никто не смотрел, как вы вводите ПИН-код
- Не разрешайте забирать карточку в другие комнаты — настаивайте на том, чтобы все операции проводились при вас
- Не забудьте получить чек

A photograph of a branch with several bright green leaves, positioned horizontally across the top and bottom of the slide, framing the central text box.

Банк обязан по вашему требованию незамедлительно заблокировать утраченную карту!

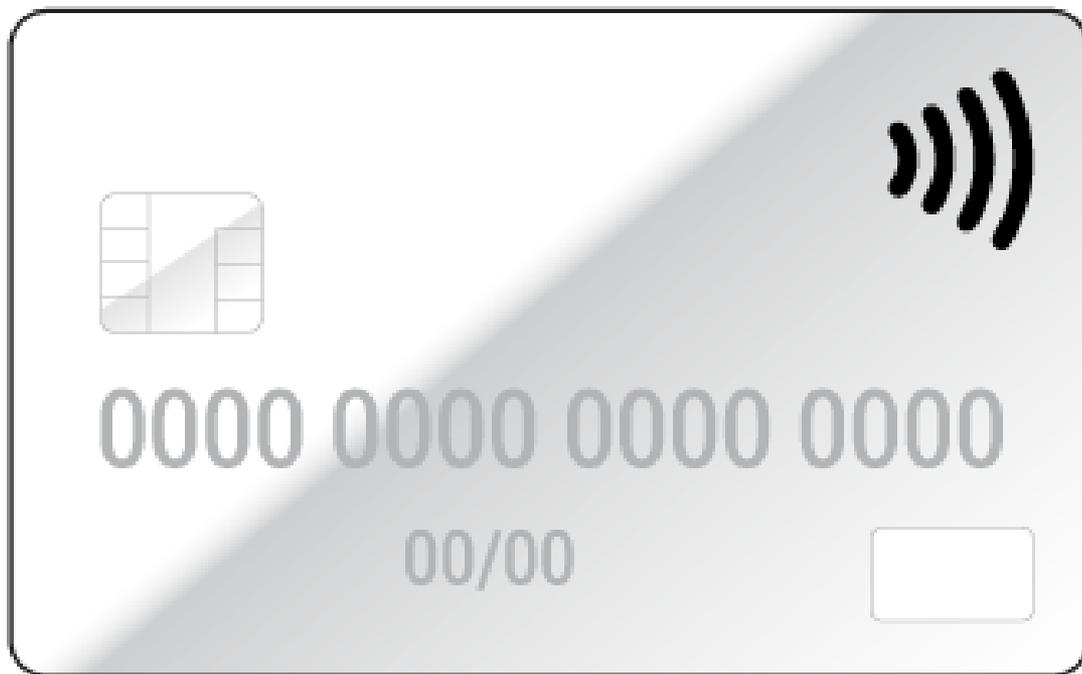
Как платит молодежь: бесконтактные платежи



- Приложите свою карту к терминалу
- Держите ее так, пока банковский терминал не подаст сигнал
- Покупка оплачена – не забудьте получить у кассира чек!

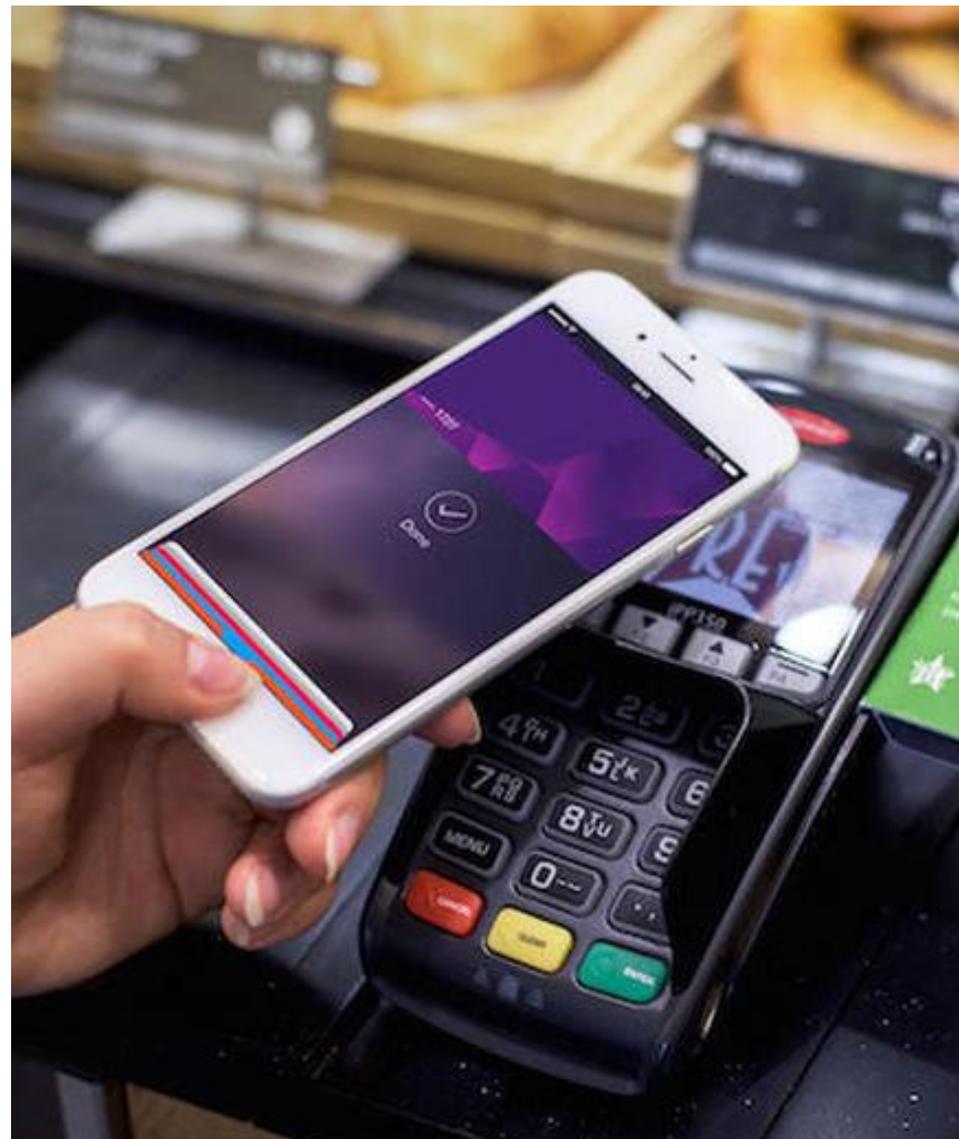
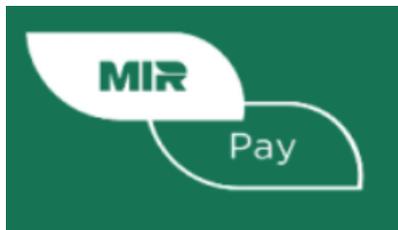
Как понять, что ваша карта поддерживает бесконтактную оплату?

Банки выпускают специальные бесконтактные карты, которые отмечаются значком в виде радиоволн



Как платит молодежь: мобильный вместо кошелька

Чтобы начать платить телефоном, вам нужно скачать специальные мобильные приложения, например Mir Pay и привязать к ним свою банковскую карту



Мошенничество с банковскими картами

Чтобы украсть ваши деньги, мошенникам нужно узнать:

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

- ПИН- код

- код проверки подлинности карты

- одноразовый пароль (смс-сообщение для подтверждение платежа)

Ваша персональная информация

Мошенник может снять все деньги с карты

Мошенник может оплачивать вашей картой свои покупки в интернете

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



**Одноразовый пароль – это
последний защитный рубеж между
вами и мошенниками!**



Вам пришло сообщение «от банка»

- Не паникуйте!
- Настоящие банки обычно присылают уведомления с одного и того же номера
- Не перезванивайте по незнакомому номеру
- Позвоните в банк и выясните, действительно ли звонок был из банка
- Либо обратитесь в ближайшее отделение к сотрудникам вашего банка

Вам звонят «из госучреждения»

- Не торопитесь!
- Не следуйте указаниям и не оплачивайте ничего
- Не давайте персональные данные
- Обратитесь в учреждение лично или по телефону, найденному в официальных источниках

Вам звонит «покупатель» по объявлению о продаже

- Не сообщайте свои персональные данные и сведения о карте по телефону никому, тем более незнакомым людям
- Не храните крупные суммы на карте, которую используете для совершения интернет-покупок или получения переводов от незнакомых людей

Вам пришло письмо или уведомление

- Не спешите связываться с контактным лицом, указанным в письме, – Банк России не пишет подобных писем
- Обратитесь в правоохранительные органы

Что делать, если мошенники списали деньги с вашей 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



**Доверять – хорошо,
слишком доверять – опасно**

Мошенничество

Самые распространенные виды мошенничества:

- финансовые пирамиды
- телефонное мошенничество
- навязывание «услуг», «уникальных» товаров, «бесплатных» процедур

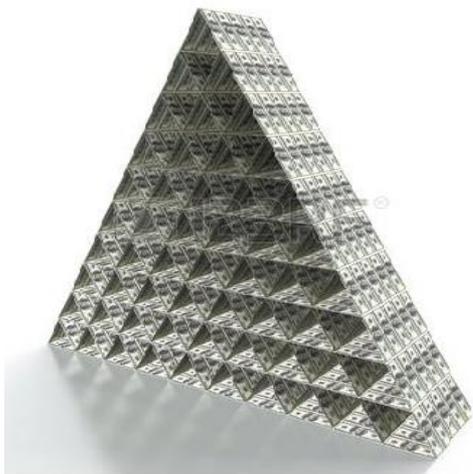
Финансовые пирамиды

Вам предлагают вложить деньги под невероятно высокие проценты!

Мошенническая схема получения дохода, известная сотни лет

Финансы поступают за счет постоянного привлечения новых участников

Организаторы скрываются с деньгами обманутых вкладчиков





**Вкладывать деньги в компанию без
лицензии нельзя – вы их потеряете**

Финансовые пирамиды



Принимая решение об инвестиции средств

- Соберите всю возможную информацию о компании. Используйте возможности интернета!
- Внимательно изучите документы
- Не торопитесь! Не поддавайтесь на провокации, если вас торопят внести деньги
- Советуйтесь с юристом, близкими людьми

Как вложиться и не попасть в пирамиду

Что такое кредитный потребительский кооператив (КПК)?

1. некоммерческая организация
2. объединяет группу единомышленников
3. привлекает денежные средства членов кооператива

Как не спутать КПК с пирамидой

- Проверьте название
- Изучите документы
- Найдите в справочнике финансовых организаций на сайте Банка России
- Не стройте пирамиды
- Опасайтесь агрессивной рекламы

Если вы стали жертвой пирамиды

**Организаторов финансовой пирамиды
можно привлечь к ответственности!**

- Уголовное наказание за организацию финансовых пирамид **по ст. 172.2 УК РФ**
- Административное наказание за привлечение денежных средств и рекламу пирамид **по ст. 14.62 КоАП.**

Если вы стали жертвой пирамиды

1. **Не молчите** - иначе жертв станет больше
2. **Составьте письменную претензию** в адрес компании и потребуйте вернуть деньги
3. **Обратитесь в полицию**, если деньги не вернут
4. **Готовьте доказательства** (договор, выписку по банковскому счету, приходный кассовый ордер)
5. **Действуйте сообща** с другими жертвами, составьте коллективный иск

Куда еще обратиться с жалобой?

В Банк России через интернет приемную на сайте cbr.ru

и в общественные организации:

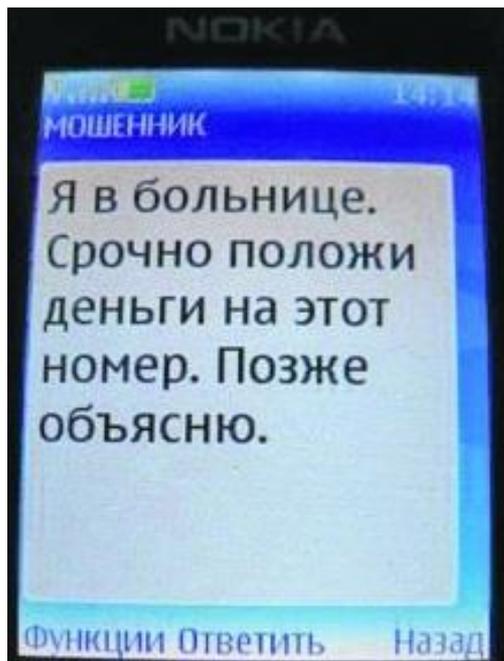
- «За права заемщиков»
- Конфедерация обществ потребителей
- Федеральный общественно-государственный фонд по защите прав вкладчиков и акционеров



**Не всегда успешно,
что поспешно!**



Вы получили тревожное СМС-сообщение от родственника



- Не спешите отдавать деньги
- Попробуйте выяснить детали
- Перезвоните близкому, от имени которого обращаются злоумышленники

Злоумышленники часто совершают звонки в крайне неудобное время - например, ночью

Вы получили звонок о «выигрыше»



Не перечисляйте деньги.
Бесплатный сыр бывает
только в мышеловке!

Вам звонит «сотрудник поликлиники»

- обследование и лечение на дому
- «чудодейственные» лекарства
- медицинские приборы

Не соглашайтесь и не оплачивайте ничего!

**Обратитесь лично к врачу поликлиники, а
лекарства и медтехнику приобретайте у
официальных продавцов**

Вам звонят «работники собес»

Начислена ежегодная выплата или компенсация и для выплаты (якобы) нужно сообщить номер банковской карты и код доступа...

Не сообщайте свои персональные данные и сведения о карте по телефону!

Навязывание услуг, не связанное с мошенничеством

Вам звонит оператор настоящего банка и делает эксклюзивное предложение...

- ✓ Запишите все условия
- ✓ Примите взвешенное решение, оценив, действительно ли это будет для вас выгодно

Манипуляции у вас дома

Мошенники обманывают пожилых людей, представляясь социальными работниками...

**Посторонние люди не должны
попадать к вам в дом!**

Как уберечься от мошенничества

1. Не верьте безоговорочно даже «солидным организациям»
2. Не спешите и задавайте вопросы
3. Если поверили, спросите ФИО, должность и контактный телефон для подстраховки
4. Не покупайте на дому
5. Не принимайте поспешных решений, не переводите никому деньги
6. Воспользуйтесь сервисом «второй руки» или возможностью установить ограничения на онлайн-операции

A photograph of a green leafy branch, likely a dogwood, with several large, serrated leaves. The branch is positioned horizontally across the upper half of the image. A semi-transparent green banner with rounded ends is overlaid on the lower half of the branch, containing the text.

Кто предупрежден – тот вооружен!