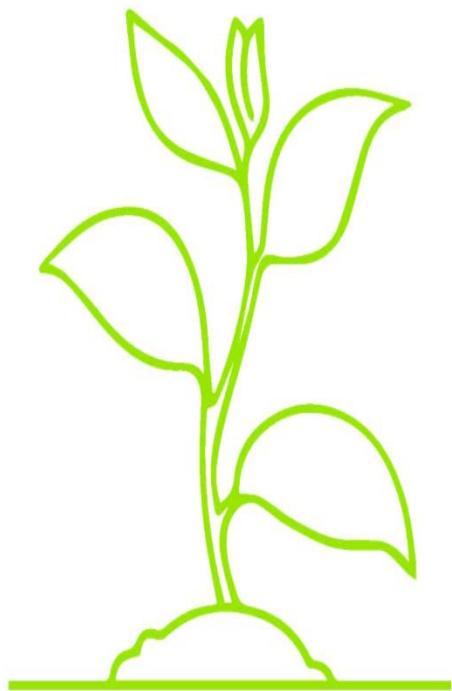





Банк России



«Правила безопасности»


Финансовая грамотность

A decorative background of fresh green leaves and branches, some of which are partially obscured by a central text box.

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

A photograph of a branch with several bright green leaves, positioned horizontally across the top and bottom of the page. The leaves are slightly out of focus, creating a soft background for the text.

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



**Заведите карточки или блокноты
для записи PIN-кода к карте,
логина и пароля от ваших личных
кабинетов.**

Держите в отдельном месте!

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. Банкомат

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

Безопасное использование банковских карт. Магазин/кафе

- ✓ Следите, чтобы никто не смотрел, как вы вводите PIN-код.
- ✓ При оплате в ресторане не выпускайте банковскую карточку из рук, при необходимости оплачивайте счет в кассе ресторана самостоятельно

A photograph of a branch with several bright green leaves, positioned horizontally across the top and bottom of the slide. The leaves are slightly out of focus, creating a soft background for the text.

Банк обязан по вашему требованию незамедлительно заблокировать утраченную карту!

Чтобы украсть деньги, мошенникам надо узнать

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

- ✓ PIN – код

- ✓ код проверки подлинности карты


- ✓ одноразовый пароль (sms-сообщение для подтверждения 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

A photograph of a branch with several bright green leaves, positioned horizontally across the top and bottom of the slide. The leaves are slightly out of focus, creating a soft background for the text.

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

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

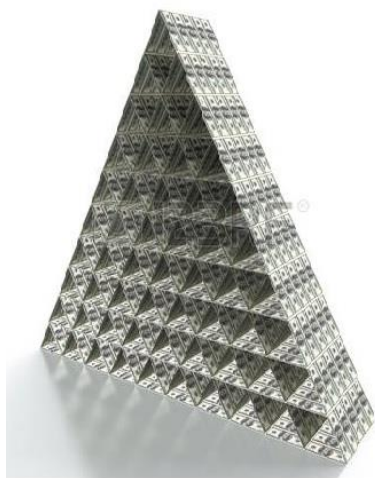
Мошенничество

Самые распространенные способы мошенничества:

- ✓ Финансовые пирамиды;
- ✓ Кибермошенничество - 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

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

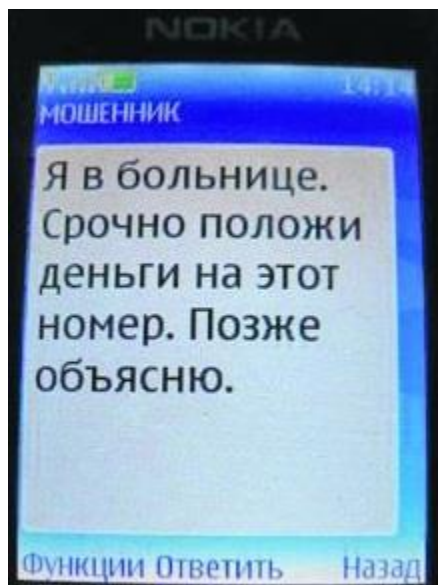
Куда еще обратиться с жалобой?

В Банк России
через интернет приемную **на сайте sbr.ru**

и в общественные организации:

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

Вы получили тревожное SMS-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!**



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

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**

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 branch, containing the text.

Кто предупрежден – тот вооружен!