



ВСЕРОССИЙСКАЯ ПРОГРАММА
**ДНИ ФИНАНСОВОЙ
ГРАМОТНОСТИ**
В УЧЕБНЫХ ЗАВЕДЕНИЯХ





Банк России

Отделение – Национальный банк по Республике Коми
Северо-Западного главного управления
Центрального банка Российской Федерации



ОСНОВЫ ФИНАНСОВОЙ КИБЕРБЕЗОПАСНОСТИ: правила безопасного использования банковских карт

Басенко Алексей Олегович

заведующий сектором технической защиты информации
Отделения Банка России по Республике Коми

Сыктывкар, 2018



0,96
млрд
₽

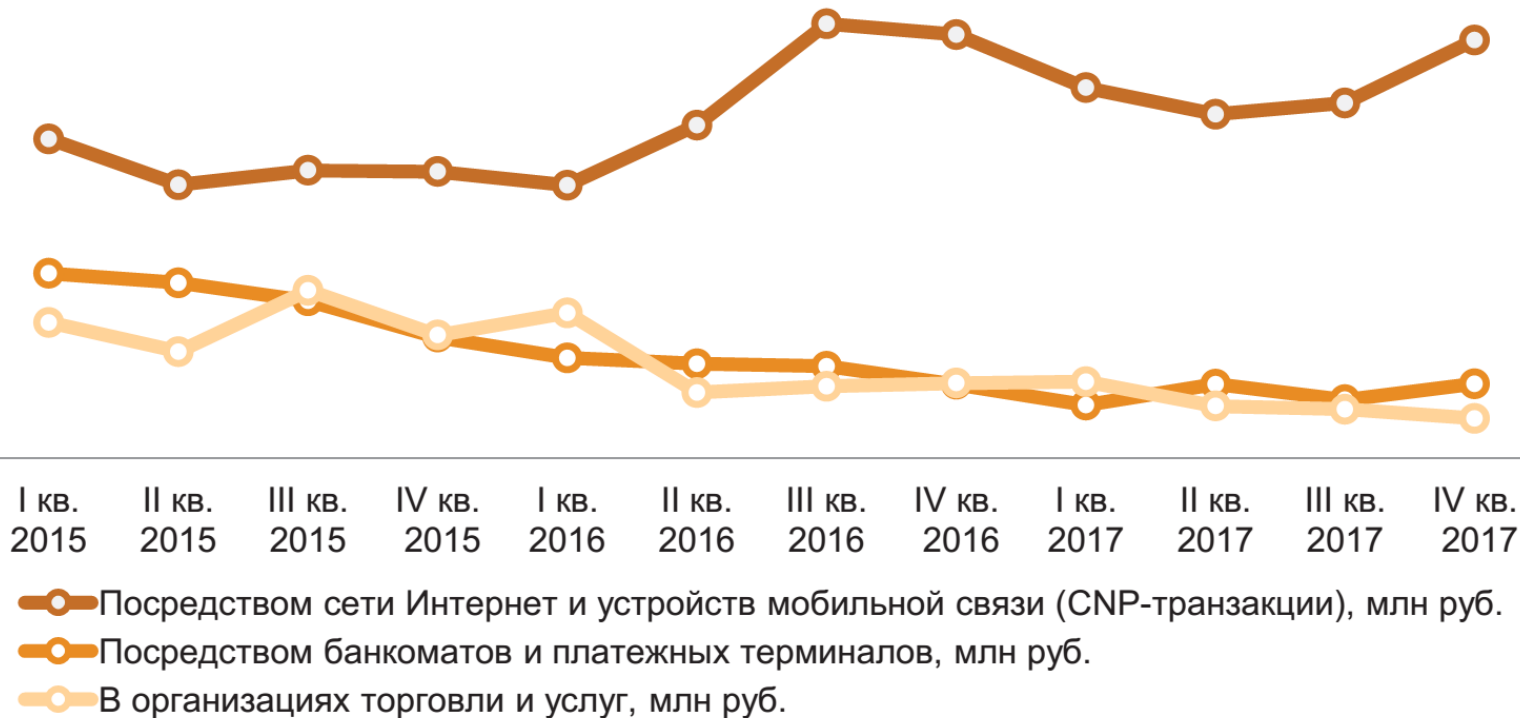




Объем несанкционированных операций, совершенных в 2017 году с использованием платежных карт, эмитированных на территории Российской Федерации



Динамика несанкционированных операций с использованием платежных карт в разрезе условий их проведения



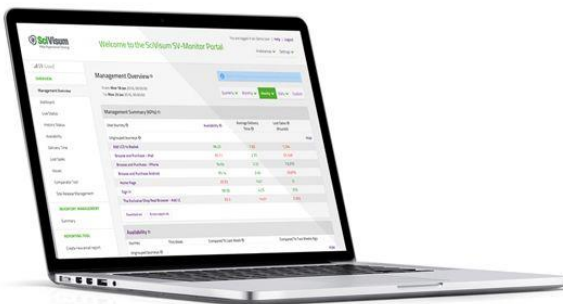


Оригинал банковской карты + ПИН-код

Реквизиты банковской карты + код из СМС

- номер карты, имя и фамилия владельца, срок действия, код проверки подлинности карты (три цифры на обратной стороне, CVV/CVC)

СМС с телефона о переводе





Банк России

Отделение – Национальный банк по Республике Коми
Северо-Западного главного управления
Центрального банка Российской Федерации



**Место действия:
магазины, кафе и другие
торговые точки**



Злоумышленником может оказаться работник сферы торговли и услуг.

Официант, кассир или продавец может сфотографировать нужные данные на карте, а после расплатиться ей в интернете.

Как предотвратить?

- рассчитываясь, постарайтесь не упускать из вида свою карту
- вводите ПИН-код так, чтобы он не был виден посторонним





В кафе официант приносит вам **POS-терминал**, вы расплачиваетесь, но тут официант говорит, что оплата не прошла, и просит повторно ввести ПИН-код.

Делая это, вы рискуете заплатить дважды.

Как предотвратить?

- подключите СМС-уведомления о платежах
- обязательно попросите чек с уведомлением о сбое или отказе от операции





Картами с системой бесконтактной оплаты можно расплачиваться без ПИН-кода, если платеж не превышает 1000 рублей.



Злоумышленники могут похитить деньги с такой карты, прислонив считыватель или POS-терминал к сумке.

Как предотвратить?

- храните карту в экранирующем отсеке кошелька, сумки или специальном чехле для банковских карт





Банк России

Отделение – Национальный банк по Республике Коми
Северо-Западного главного управления
Центрального банка Российской Федерации



**Место действия:
банкомат**



Скимминг (skimming) - незаметное копирование данных с магнитной полосы, а также получение ПИН-кода с помощью специальных устройств.

С использованием скопированных данных может быть изготовлен дубликат карты

Копия магнитной полосы:

- «скиммеры»

Получение ПИН-кода:

- микрокамеры
- накладная клавиатура
- человек, стоящий за спиной





Обычный банкомат?





Установленный скиммер
для записи данных
с магнитной полосы



Скрытая видеокамера
для записи ПИН-кода





Накладные наборные панели,
записывающие введенные
ПИН-коды





1. Проверьте банкомат: нет ли на нем посторонних устройств. Клавиатура или картоприемник не должны отличаться по фактуре, а тем более шататься
2. Когда вводите ПИН-код, всегда прикрывайте клавиатуру свободной рукой, чтобы никто не подсмотрел
3. Старайтесь пользоваться банкоматами внутри отделений банков. Их чаще проверяют и лучше охраняют
4. Не используйте устройства, которые требуют ввода ПИН-кода для доступа в помещение, где расположен банкомат





Банк России

Отделение – Национальный банк по Республике Коми
Северо-Западного главного управления
Центрального банка Российской Федерации



Место действия: сеть Интернет и мобильные устройства

- ✓ Фишинг
- ✓ Вредоносные программы (вирусы)
- ✓ Неосмотрительность в социальных сетях



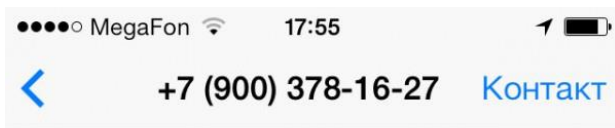
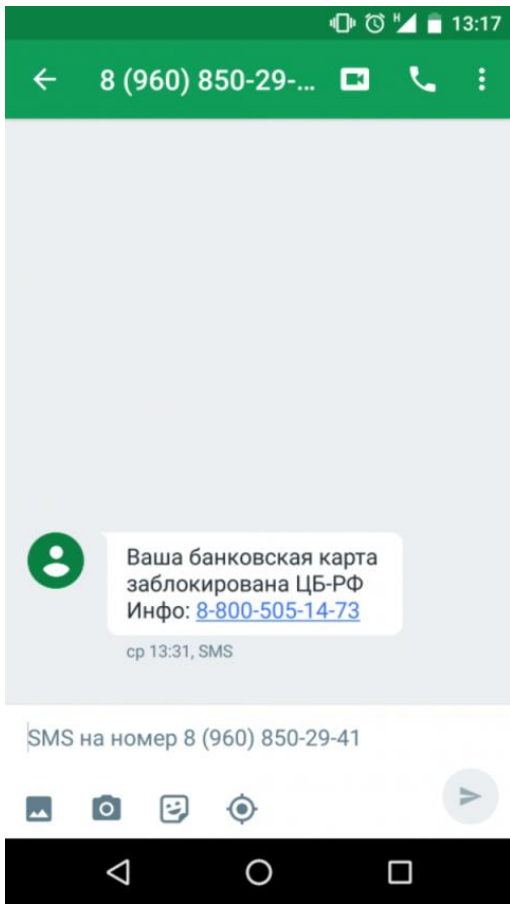
Фишинг (phishing) - измененная форма от английских слов phone (телефон) и fishing («рыбная ловля»).

Термин появился в английском для обозначения мошеннических схем, служащих для того, чтобы выманить у пользователей номера их кредитных карт, пароли доступа к банковским счетам и счетам платежных систем.

Фишинг реализуется через

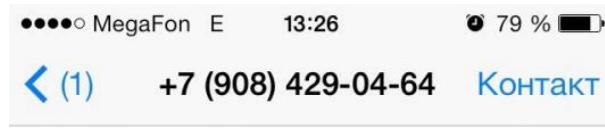
- СМС
- телефонные звонки
- электронную почту
- социальные сети
- поддельные интернет-сайты





Сообщение
Сегодня, 15:18

Ваша банковская карта
заблокирована.
Сбербанк. ИНФО
[8\(900\)379-21-30](tel:8(900)379-21-30)



Сообщение
Среда, 16:58

Ваша Банк.карта
заблокирована!срочно
звонить:
[+7\(909\)343-18-02.ЦБ/РФ](tel:+7(909)343-18-02)

Как защититься?

- обращайте внимание на номер, с которого пришло СМС
- не перезванивайте по номеру из сообщения



Только три счастливица займут это место. Заработок от 1000 USD

Спам x



Новая вакансия <business.news@todaynewscom.net>
кому: мне ▾

9 апр. (3 дн. назад) ☆



Почему это письмо попало в спам? Оно отправлено с домена todaynewscom.net, откуда часто рассылают нежелательные сообщения. [Подробнее...](#)

Картинки отключены. [Показать картинки](#)

Если ты не можешь открыть это сообщение, [кликни здесь!](#)

Как защититься?

- обращайте внимание на адрес отправителя
- смотрите на ошибки в тексте и названиях
- не переходите по ссылкам из подозрительных писем и не вводите данные своей карты
- не скачивайте вложения

Здравствуйте, друзья,
меня зовут Наталья.
Я работаю менеджером по набору удаленных сотрудников в InvestForum.
Мы заинтересованы в Вашей кандидатуре. Предлагаем Вам высокий заработок от 1000 USD, нужно выполнять простую работу на дому.
[Нажмите здесь и создайте визитную карточку](#)



Как защититься?

- если странные сообщения шлет ваш друг, позвоните и выясните, действительно ли нужна помощь
- если незнакомцы пишут от лица компании, уточните информацию на официальном сайте компании или по телефону
- компании никогда просто так не запрашивают ваши личные данные, а тем более полные данные карты

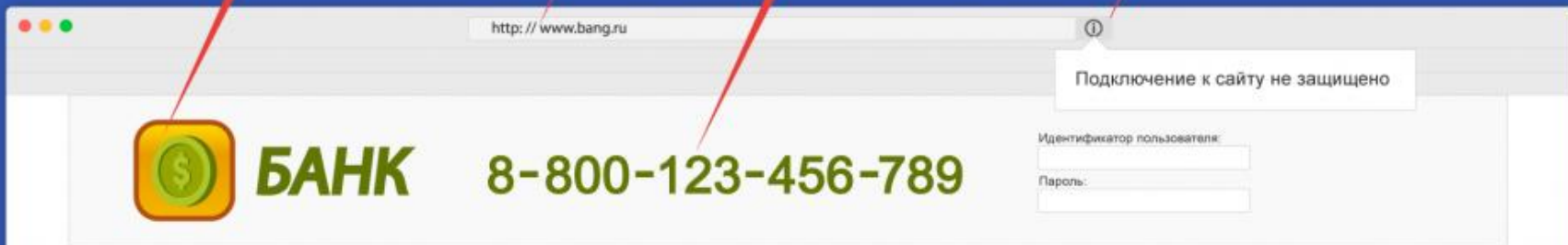


Логотип может быть похож на настоящий, но изменен

Адрес сайта похож на официальный, но отличается

Контакты на фишинговом сайте не соответствуют официальным

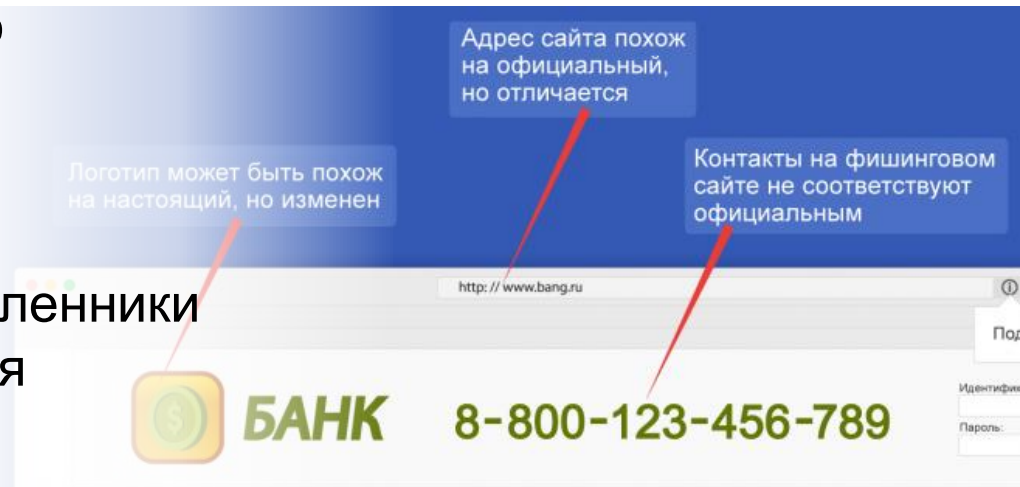
Нет значка защищенного соединения



Вводимые на таких сайтах данные
попадают к мошенникам!



1. Всегда обращайте внимание на адресную строку браузера: на сайте-клоне будет допущена ошибка
2. Добавьте в закладки сайты, которыми часто пользуетесь, чтобы не набирать адрес вручную — так вы не ошибетесь в названии и попадете на нужный сайт.
3. Оплачивайте покупки только через сайты с защищенным соединением
4. Обращайте внимание на содержание сайта — злоумышленники часто невнимательно относятся к наполнению сайта.





Банк России

Отделение – Национальный банк по Республике Коми
Северо-Западного главного управления
Центрального банка Российской Федерации



Место действия: сеть Интернет и мобильные устройства

- ✓ Фишинг
- ✓ Вредоносные программы (вирусы)
- ✓ Неосмотрительность в социальных сетях



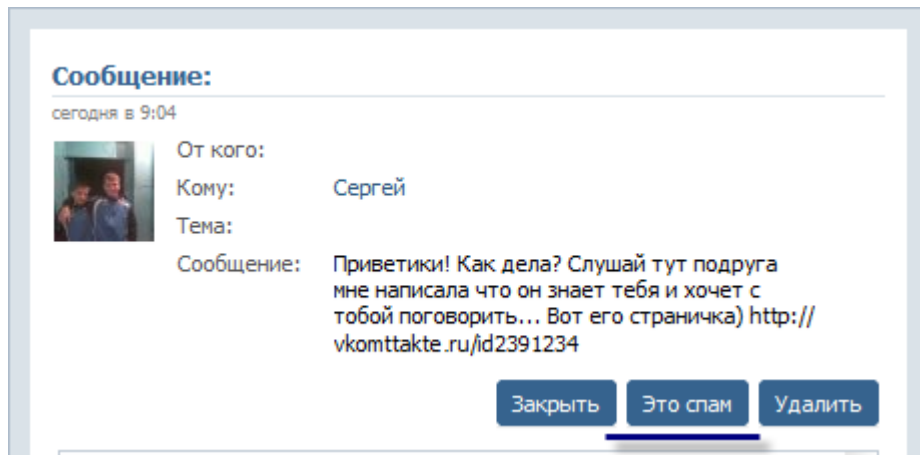
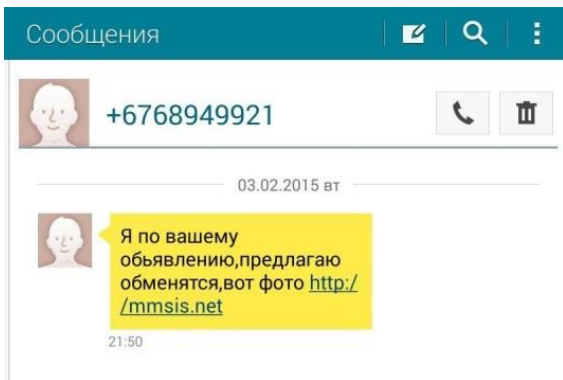
Принцип действия троянских программ для систем ДБО

- перехватывают логины и пароли для доступа к системам ДБО, данные банковской карты
- перенаправляют на фишинговые сайты (сайт-двойники)
- совершают несанкционированные операции в СМС-банкинге (на мобильных устройствах)





Вредоносные ссылки



Сомнительное ПО



1. Установите антивирус и регулярно обновляйте его базы. Хороший антивирус поможет защититься в т.ч. от фишинга.
2. Не переходите по ссылкам в письмах, сообщениях и СМС, в особенности от незнакомых адресатов
3. Скачивайте и устанавливайте приложения только из официальных источников. Обращайте внимание на разработчиков приложения
4. Устанавливайте последние обновления операционной системы и прикладных программ
5. Не скачивайте сомнительные приложения и не посещайте сомнительные ресурсы





Банк России

Отделение – Национальный банк по Республике Коми
Северо-Западного главного управления
Центрального банка Российской Федерации



Место действия: сеть Интернет и мобильные устройства

- ✓ Фишинг
- ✓ Вредоносные программы (вирусы)
- ✓ Неосмотрительность в социальных сетях



КАК ТЕБЯ БУДУТ ЗВАТЬ

НА ЯЗЫКЕ МИНЬОНОВ



ИМЯ: НОМЕР ТВОЕЙ БАНКОВСКОЙ КАРТЫ

ФАМИЛИЯ: СРОК ДЕЙСТВИЯ КАРТЫ

ОТЧЕСТВО: CV-КОД(НА ЗАДНЕЙ СТОРОНЕ КАРТЫ)

♥ Нравится 2771 💬 Комментировать 🔊 160

👁 66K

♥ Нравится 2771 💬 Комментировать 🔊 160

👁 66K

Показать все 33 комментария



Иван

6390024590

11/

191

только я не понял

24 минуты назад Ответить



Иван

а, понял

ДАТА	СУММА
Сегодня в 19:14	-3500,00 руб.
Сегодня в 19:12	-20000,00 руб.
Сегодня в 19:06	-18000,00 руб.
Сегодня в 19:01	-10500,00 руб.
Сегодня в 18:57	-7400,00 руб.



Проверила! Работает!!!

У ТВОЕЙ КРЕДИТНОЙ КАРТЫ ЕСТЬ ДАТА РОЖДЕНИЯ!

Возьми три цифры с обратной стороны карты и
выложи их в комментарии внизу, прикрепив фото
карты, вот так:



123

Через некоторое время вам на телефон придут
цифры (например: 1205 р.)

ЭТО И БУДЕТ ДАТА РОЖДЕНИЯ КАРТЫ!

Удивительно, но это правда!!! 100 процентная инфа, попробуйте!

Авторство [redacted] а он то уж не даст соврать - честнейший человек, всё проверил на своих картах!



Like



Comment



Share



Василий

Москва · 🌐

КОНКУРС: Сфотографируй свою кредитку с двух сторон, пришли на наш адрес и получи шанс выиграть iPhone 6

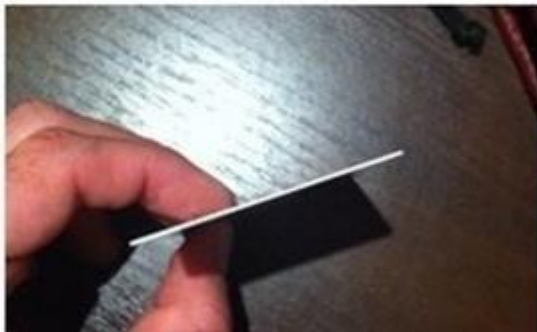
Нравится · Комментарий · Поделиться

Поделиться 🗨 7 Мне нравится ❤ 81

Показать все 5 комментариев



Где айфон получить?









Банк России

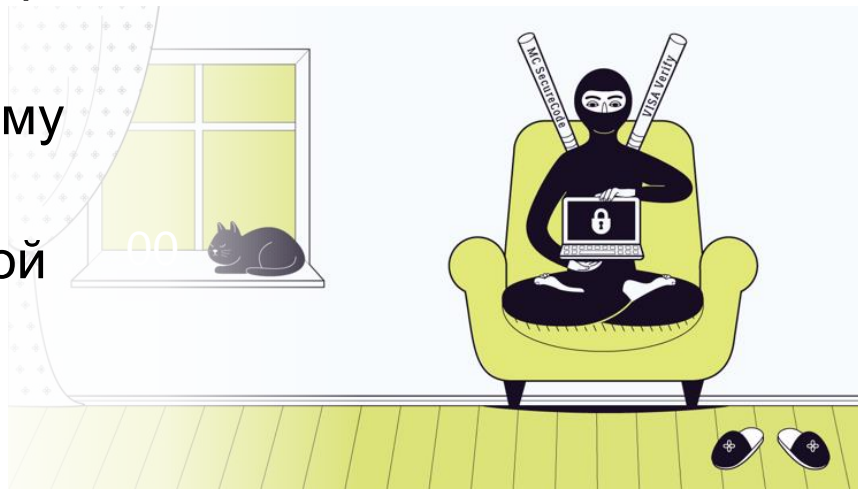
Отделение – Национальный банк по Республике Коми
Северо-Западного главного управления
Центрального банка Российской Федерации



Универсальные советы и лайфхаки



1. Подключите услугу СМС-оповещения о проведенных операциях по карте
2. Никому не сообщайте персональную информацию (ПИН-код, реквизиты карты. Даже сотрудники банка не вправе требовать от вас эти данные)
3. Имейте всегда при себе телефон горячей линии банка, выпустившего карту
4. Установите суточный лимит на сумму операций по банковской карте
5. Не рассчитывайте своей основной картой. Заведите дополнительную карту для осуществления расчетов





Банк России

Отделение – Национальный банк по Республике Коми
Северо-Западного главного управления
Центрального банка Российской Федерации



**Что делать, если деньги
все-таки украли?**

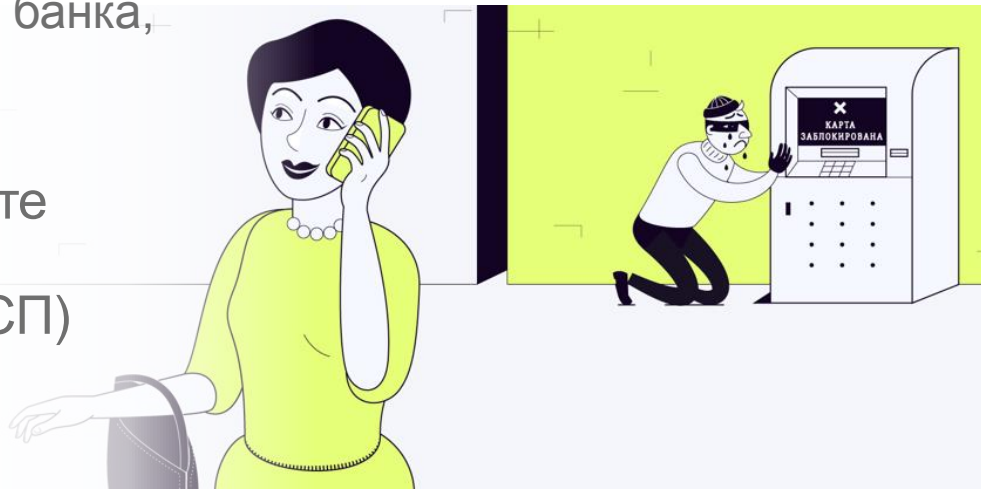


1. Немедленно **заблокируйте карту**, позвонив в банк по телефону или через интернет-банк

2. **В течение суток** после несанкционированного списания обратитесь в банк и **опротестуйте операцию**:

- ✓ запросите выписку по счету
- ✓ напишите заявление о несогласии с операцией, которую не совершали
- ✓ экземпляр заявления с отметкой банка, что оно принято, оставьте у себя

3. **Обратитесь в полицию** с заявлением о хищении. Получите номер заявления в Книге учета сообщений о преступлениях (КУСП)

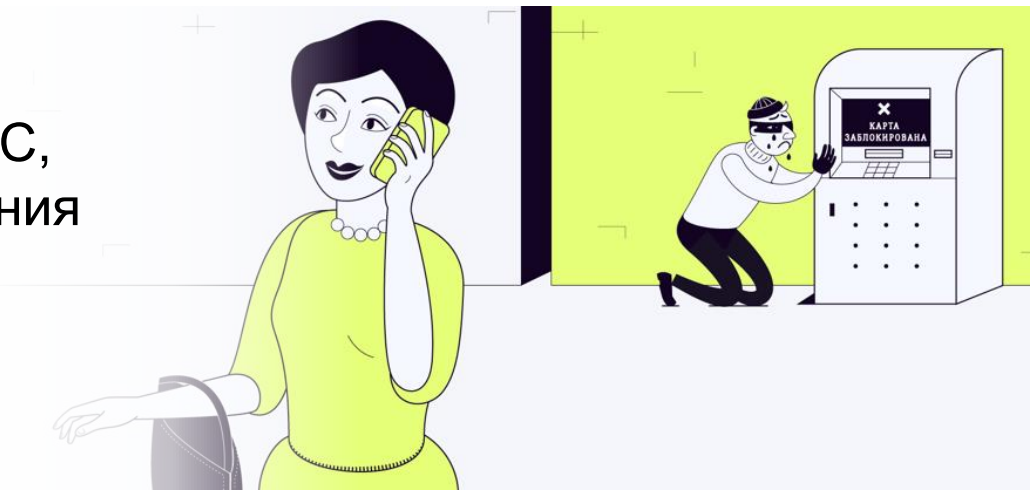




Получив заявление, банк проведет служебное расследование и решит вопрос о возмещении ущерба.

Если вы **соблюдали меры безопасности** и обратились в банк не позже, чем через сутки после списания денег, то можете рассчитывать на возмещение.

Если вы сами сообщили злоумышленникам реквизиты карты, ПИН-код или код из СМС, необходимый для подтверждения платежей и переводов, банк не вернет вам денег.





Узнай как

Защитить имущество

Взять в долг

Вычислить мошенников

Планировать финансы

Увеличить доход



fincult.info

Больше, чем финансовая
грамотность



Узнай как

Защитить имущество

Взять в долг

Вычислить мошенников

Планировать финансы

Увеличить доход



fincult.info

Больше, чем финансовая
грамотность

Это Петя.

**Петя сам заботится
о безопасности
своих финансов.**

Петя умный.

Будь как Петя.





Банк России

Отделение – Национальный банк по Республике Коми
Северо-Западного главного управления
Центрального банка Российской Федерации



Спасибо за внимание!