10 ПРАВИЛ
безопасного использования карты

1. ХРАНИТЕ ПИН-КОД ОТДЕЛЬНО ОТ КАРТЫ
2. НИКОГДА И НИКОМУ НЕ СООБЩАЙТЕ СВОЙ ПИН-КОД ИЛИ CVV
3. В СЛУЧАЕ ПОТЕРИ КАРТЫ ИЛИ ПИН-КОДА НЕМЕДЛЕННО ОБРАТИТЕСЬ В БАНК ДЛЯ БЛОКИРОВКИ КАРТЫ
4. ПОДКЛЮЧИТЕ СМС-УВЕДОМЛЕНИЯ ОБ ОПЕРАЦИЯХ ПО КАРТЕ
5. НИКОГДА И НИКОМУ НЕ СООБЩАЙТЕ ПАРОЛЬ ДЛЯ ДОСТУПА В МОБИЛЬНЫЙ ИЛИ ИНТЕРНЕТ-БАНК
6. ХРАНИТЕ ПОД РУКОЙ КОНТАКТНЫЙ НОМЕР СЛУЖБЫ ПОДДЕРЖКИ ВАШЕГО БАНКА
7. РЕГУЛЯРНО ОБНОВЛЯЙТЕ АНТИВИРУСНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ
8. НЕ ОСТАВЛЯЙТЕ КАРТУ БЕЗ ПРИСМОТРА. ПРИКРЫВАЙТЕ РУКОЙ КЛАВИАТУРУ ПРИ ВВОДЕ ПИН-КОДА КАК В БАНКОМАТЕ, ТАК И ПРИ ОПЛАТЕ КАРТОЙ В МАГАЗИНЕ
9. УСТАНОВИТЕ ДОСТУПНЫЙ ЛИМИТ СПИСАНИЙ ПО КАРТЕ В ДЕНЬ
10. ОБРАЩАЙТЕ ВНИМАНИЕ НА ВНЕШНИЙ ВИД БАНКОМАТА. ЕСЛИ У ВАС ВОЗНИКЛИ СОМНЕНИЯ, СООБЩИТЕ ОБ ЭТОМ СОТРУДНИКАМ БАНКА И ВОСПОЛЬЗУЙТЕСЬ ДРУГИМ БАНКОМАТОМ. ЗВОНИТЕ В БАНК ТОЛЬКО ПО ОФИЦИАЛЬНОМУ НОМЕРУ БАНКА, УКАЗАННОМУ НА ОБОРОТНОЙ СТОРОНЕ КАРТЫ

Какие схемы используют мошенники?

1. При продаже товара мошенники – потенциальные покупатели или продавцы – ***просят не только номер карты, но и секретные данные.***
2. Ваши знакомые в социальных сетях ***просят одолжить деньги или отправляют Вам странную ссылку***.
3. На электронную почту ***приходит письмо с информацией о выигрыше или с предложением работы***, которую Вы не искали.
4. На сайтах гос. органов, например, ГИБДД или ФНС, присутствуют некие изменения – лишняя буква в строке браузера, измененный номер телефона для связи с той или иной службой.

Помните о том, что нельзя сообщать посторонним лицам CVV или CVC-коды, ПИН-код банковской карты, срок действия, пароли из банковских уведомлений!

ТЕЛЕФОННОЕ МОШЕННИЧЕСТВО

Звонят из банка. Говорят об угрозе вашим деньгам на счете и ипросят перевести деньги на другой счет. Спрашивают данные карты.

- что делать?

СРАЗУ ПОЛОЖИТЕ ТРУБКУ – ЭТО МОШЕННИКИ!

Позвоните по телефону, который указан на вашей банковской карте, сотрудник банка прояснит ситуацию.

Звонят и сообщают о выигрышах, выплатах, конпенсацичх и т.д.

- что делать?

НЕ ПЕРЕДАВАЙТЕ ДАННЫЕ КАРТЫ!

если во время разговора вас просят совершить платеж - это мошенники. Положите трубку и, чтобы не сомневаться, уточните информацию на официальном сайте организации, от имени которой звонят.

Звонят и сообщают, что близкий человек попал в беду, просят перевести деньги.

- что делать?

ПРОЯСНИТЕ СИТУАЦИЮ!

Спросите фамилию звонящего и название организации, которую он представляет.Прекратите разговор и позвоните близкому человеку. Если дозвониться не удалось, сами найдите телефон организации, от имени которой был звонок, и выясните, что случилось.

ИНТЕРНЕТ

Предлагают вложить деньги на очень выгодных условиях.

- что делать?

ОТКРОЙТЕ САЙТ WWW.CBR.RU/FINORG

Обо всех финансовых организациях, у которых есть лицензия Банка России, можно узнать на его официальном сайте.

На сайтах с объявлениями (”Авито”, “Юла” и т.д.) предлагаюттовары и услуги по заниженным цунам.

- что делать?

НЕ ВНОСИТЕ ПРЕДОПЛАТУ!

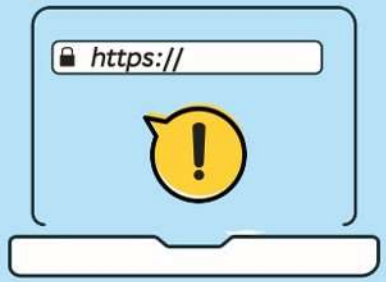
Во время общения с продавцом не сообщайте данные банковской катры, не переходитепо ссылкам. Пользуйтесь услугой “Безопасная сделка”, которая доступна на сайте с объявлениями.

Нужно перевести или купить билеты. На одном из сайтов условия намного выгоднее, чем на знакомых ресурсах.

- что делать?

ПОЛЬЗУЙТЕСЬ ТОЛЬКО ПРОВЕРЕННЫМИ САЙТАМИ!

Безопасный сайт должен иметь надписьhttps:// и “замочек” в адресной строке браузера.



5 примет, по которым можно вычислить мошенников

1 Незнакомец неожиданно связывается с вами сам

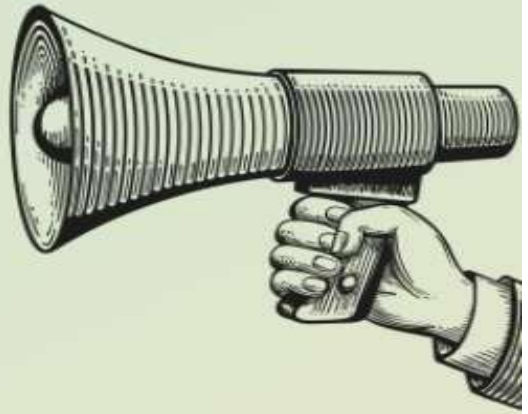
Например, от имени банка, полиции, магазина. Способы могут быть разные — звонок, СМС или ссылка в мессенджере.

Общее у них одно — кто-то сам вышел на связь с вами. Значит, ему что-то от вас нужно.

2 С вами говорят о деньгах

Основная задача мошенников — получить доступ к чужим деньгам.

Вам могут предложить:



- перевести все деньги на «безопасный счет»
- оплатить «страховку для получения кредита»
- «очень выгодно» инвестировать свои сбережения.

И многое другое. Главное:

речь всегда будет идти о деньгах.

3 Вас просят сообщить данные

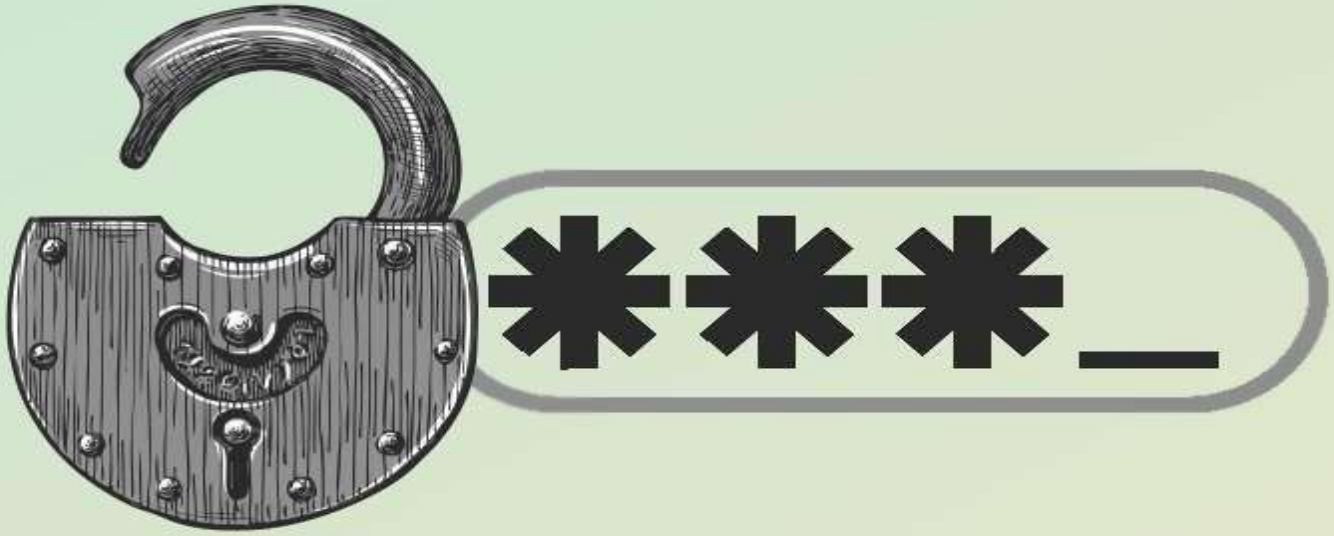
Обычным ворам нужен ключ от квартиры, мошенникам — «ключ» от вашего счета:

срок действия карты и CVC-код

логины и пароли к приложению банка или личному кабинету на сайте

коды из банковских уведомлений.

Настоящий сотрудник банка
никогда не спросит секретные
реквизиты карты,
ПИН-коды и пароли.



Если о них спрашивают — будьте
уверены, звонят не из банка
и вас точно пытаются обмануть.

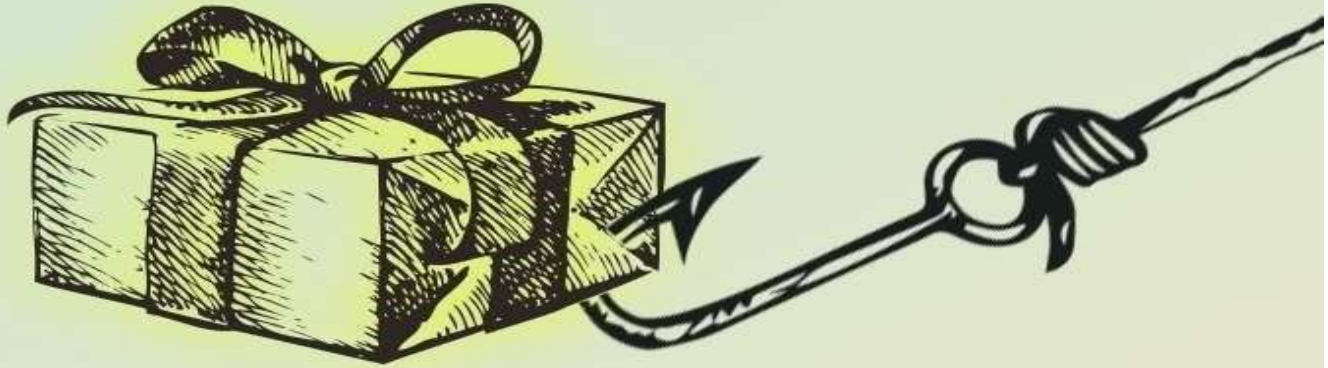
4 Вас выводят из равновесия

Мошенники стремятся
вызвать у вас сильные
эмоции — напугать или обрадовать.
Например, сообщают:

чтобы вы растерялись
и выдали любую информацию,
лишь бы спасти деньги.

Еще вас могут обрадовать внезапным «выигрышем в лотерею». Взамен нужно лишь оплатить комиссию на сайте.

С которого, конечно, мошенники уведут данные вашей карты.



Не торопитесь следовать чужим инструкциям, как бы ни были взволнованы.

5 На вас давят:

торопят

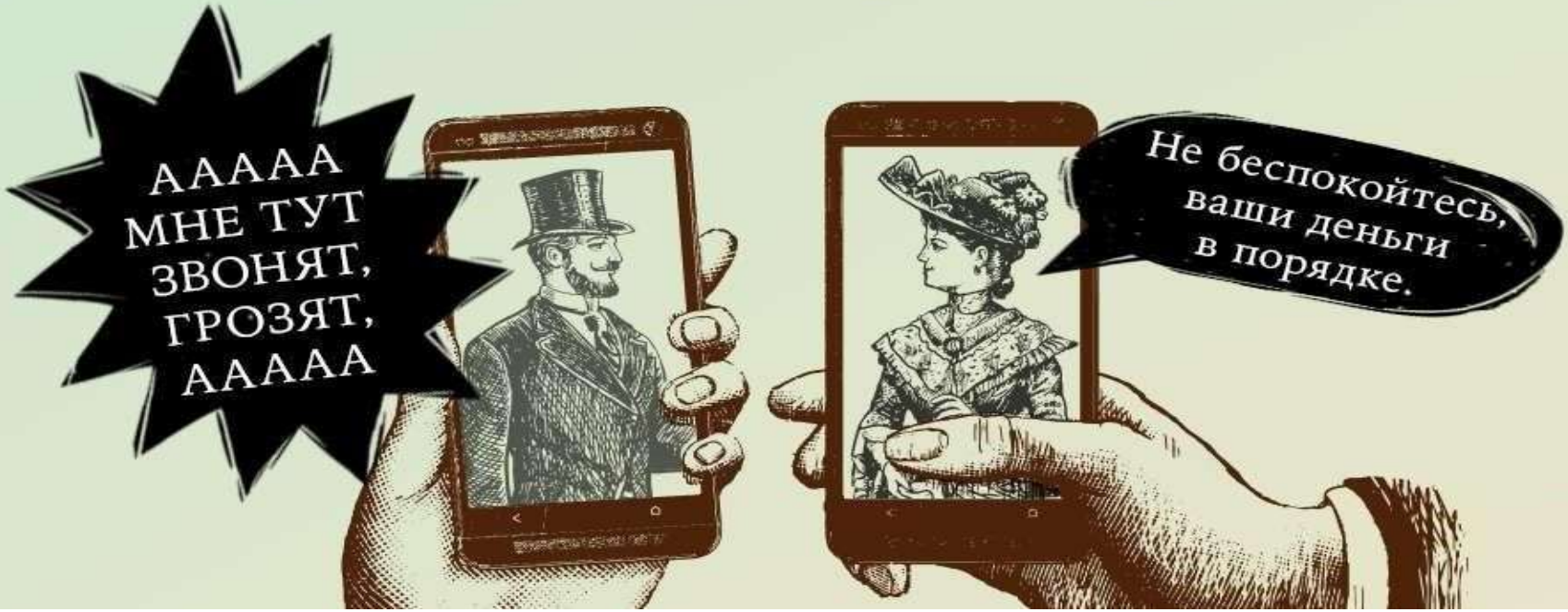
принуждают к чему-то

ставят условия:
«сейчас или будет поздно».

Такие ситуации подозрительны.
Поэтому общение лучше
прекратить сразу.

Никогда не принимайте поспешных решений, особенно если они касаются ваших денег.

Звонят из банка с тревожными новостями? Положите трубку и наберите номер горячей линии банка сами, чтобы прояснить реальное положение дел.



Будьте бдительны, не поддавайтесь на уловки мошенников!

Банк направил вам уведомление о совершенной операции в порядке и в сроки, установленные договором

нет

Банк обязан возместить вам сумму похищенных средств, о которой вы не были проинформированы банком

да

Вы предоставили в банк уведомление о несогласии с совершенной операцией и/или об утрате банковской карты незамедлительно после обнаружения факта утраты карты и (или) ее использования без вашего согласия, но не позднее дня, следующего за днем получения уведомления о совершенной операции

да

нет

Банк не обязан возмещать вам денежные средства

Банк обязан возместить вам денежные средства, если не сможет доказать, что причиной возникновения неправомерной операции, совершенной до момента предоставления вами в банк уведомления о несогласии или утрате, стало нарушение вами порядка использования банковских карт

Что делать, если вы пострадали от действий мошенников

Срочно позвонить в свой банк

Например, в Сбербанке действует бесплатная круглосуточная «горячая» линия. Набирайте 900 с мобильного телефона (звонок на территории России бесплатный).
Номер 8 800 555-55-50 - для бесплатных звонков с любых телефонов на территории России и +7 495 500-55-50 - для звонков из любой точки мира (стоимость звонка по тарифам оператора связи).

Приготовьтесь сообщить информацию, по которой вас смогут идентифицировать.

Вам потребуется назвать фамилию, имя и отчество, паспортные данные и иную информацию по запросу оператора

Попросите зарегистрировать заявление на незаконные действия с вашей картой.

После вашего сообщения о несанкционированных действиях с картой оператор должен немедленно ее заблокировать, даже если были похищены все средства, хранящиеся на ней.

Обратитесь в полицию

Подайте в любое подразделение полиции заявление о совершенном мошенничестве.