# ВНИМАНИЕ – МОШЕННИКИ!

## Как обманывают мошенники

Узнайте о распространённых приёмах злоумышленников и не дайте им себя обмануть

## Ситуация 1. Звонок из службы безопасности банка

### Вам звонит незнакомец

Номер входящего звонка очень похож на номер банка, а звонящий представляется «сотрудником службы безопасности банка».

### У вас просят конфиденциальные данные

Мошенник сообщает, что «банк выявил подозрительную операцию» или «в системе произошел сбой». Он просит у вас **полные данные карты, CVV- или CVC-код, код из СМС**. Это нужно якобы «для сохранности ваших денег».

**Злоумышленники могут поменять одну цифру в номере, которую вы не заметите и подумаете, что это банковский номер.**

### Как защитить себя

- Запишите номер банка в адресную книгу своего телефона.
- Не совершайте никаких операций по инструкциям звонящего. Все операции для защиты карты сотрудник банка делает сам.
- Сразу заканчивайте разговор. Работник банка никогда не попросит у вас коды безопасности с обратной стороны карты (CVV/CVC), коды из СМС, номер банковской карты.
- Проверьте, не было ли сомнительных операций за время разговора. Если успели что-то сообщить мошенникам, сразу позвоните в банк и сообщите о случившемся.

## Ситуация 2. Брокерские или дилерские услуги

### Выгодные инвестиции

Вам звонит незнакомец, который называет себя представителем брокерской или дилерской компании, предлагает инвестировать деньги и обещает высокий доход. Вы соглашаетесь открыть счёт и самостоятельно переводите деньги на карту третьего лица. Мошенники пропадают, вернуть деньги невозможно.

### Бинарные опционы

Вы регистрируетесь на сайте бинарных опционов. После пополнения баланса вы получаете уведомление о получении «бонусных доходов». Чтобы вывести эти деньги, вам нужно повысить «торговый статус». Для этого вы вносите на счёт дополнительную сумму. Мошенники пропадают, вернуть деньги невозможно.

### Как защитить себя

- Проверьте лицензию. Прежде чем переводить деньги брокерской компании, убедитесь, что у неё есть лицензия. Список компаний с лицензиями на брокерскую и дилерскую деятельность есть на сайте Центробанка.
- Проверьте реквизиты. Настоящие брокерские или дилерские компании никогда не попросят перевести деньги на карту обычного человека — это должен быть именно счёт компании.
- Если баланс не изменился, проигнорируйте СМС и сообщите нам номер телефона мошенника. Мы примем меры.

## Ситуация 3. Автоматизированные кол-центры

Вам звонит робот — будто бы от банка. Он сообщает, что ваша карта «заблокирована в связи с подозрительной операцией», просит вас перезвонить для выяснения подробностей и диктует номер. По этому номеру отвечает мошенник под видом сотрудника службы безопасности — пугает вас потерей денег и настойчиво предлагает их «спасти», переведя на «безопасный счёт», либо старается выманить секретные данные (например, код из СМС).

**Важно: иногда вам может позвонить настоящий голосовой помощник от банка — в том случае, когда банк подозревает мошенничество. Но это делается лишь для подтверждения, что операцию проводили вы сами. Ни сотрудник банка, ни голосовой помощник никогда не просят называть цифры и коды или звонить на номер, который отличается от официального.**

### Как защитить себя

- Запишите номер банка в адресную книгу своего телефона.
- Не совершайте никаких операций по инструкциям звонящего. Все операции для защиты карты сотрудник банка делает сам.
- Сразу заканчивайте разговор. Работник банка никогда не попросит у вас коды безопасности с обратной стороны карты (CVV/CVC), коды из СМС, номер банковской карты
- Проверьте, не было ли сомнительных операций за время разговора. Если успели что-то сообщить мошенникам, сразу позвоните в банк и сообщите о случившемся.

## Ситуация 4. Звонок из прокуратуры

Мошенник звонит и сообщает, что некий сотрудник банка с доступом к вашему счёту находится под подозрением и в его отношении ведутся следственные действия. На следующий день мошенник звонит вам под видом «представителя прокуратуры». Он сообщает, что вам необходимо выполнить гражданский долг — помочь следствию, а также убеждает вас перевести свои деньги на «специальный счёт» для гарантии их сохранности.

### Как защитить себя

- Запишите номер банка в адресную книгу своего телефона.
- Не совершайте никаких операций по инструкциям звонящего. Все операции для защиты карты сотрудник банка делает сам.
- Сразу заканчивайте разговор. Работник банка никогда не попросит у вас коды безопасности с обратной стороны карты (CVV/CVC), коды из СМС, номер банковской карты.
- Проверьте, не было ли сомнительных операций за время разговора. Если успели что-то сообщить мошенникам, сразу позвоните в банк и сообщите о случившемся.

## Ситуация 5. Приложение-кошелёк с «защищенной» картой

Злоумышленник звонит от имени банка и говорит, что для вас выпущена новая, особо защищённая карта. Такую карту якобы нужно добавить в мобильное приложение-кошелёк и перевести на неё деньги с других карт «для сохранности». Если вы под диктовку

мошенника привяжете к приложению-кошельку свою карту и пополните её, деньги уйдут мошеннику.

Дело в том, что в такое приложение можно добавить любую, даже чужую карту, а имя поставить какое угодно — мошенники этим пользуются.

## Как защитить себя

- Запишите номер банка в адресную книгу своего телефона.
- Не выполняйте инструкции звонящего и положите трубку.
- Позвоните в банк и сообщите о случившемся.