Памятка по профилактике мошенничества в отношении граждан посредством телефонных звонков и интернета

Уважаемые граждане!

Министерство внутренних дел Республики Беларусь предупреждает, что за последние два года участились случаи мошенничества путём телефонных звонков. В милицию поступают заявления от жертв *вишинга* (не путать с фишингом) — людей, которые купились на увещевания мошенников, с разной степенью успешности атакующих клиентов банков. Предлагаем вам рекомендации, как их избежать, и комментарии специалистов.

В последнее время случился натуральный набег мошенников — откуда они действуют, можно только предполагать. Вероятность того, что они орудуют с территории Беларуси, минимальна: хватает зарубежных «специалистов».

Для примера приводим историю «развода», которая произошла совсем недавно. К сожалению, она не получила хеппи-энда: пострадавшей стала женщина 50-ти лет, потерявшая заметную сумму денег. Ирина (имя изменено) честно признается: «Я прекрасно понимаю, что виновата сама, но была на то время очень расстроена, испытывала стресс от болезни близкого человека. Мошенникам это на руку: наиболее эффективно они работают именно с уязвимыми по тем или иным причинам людьми.

Ирина: «Мне позвонили в понедельник, представились службой безопасности «Беларусбанка». Сказали, что у меня с карточки пытались снять деньги, и уточнили, подтверждаю ли я перевод денег. Естественно, я не подтвердила. Тогда мне предложили проверить информацию — тут мой мозг полностью отказал: я назвала им номер карты после звукового сигнала. Дальше разговор подвели к тому, что на телефон придет код, его нужно будет сказать. Я это сделала, на что мне ответили: теперь всё в порядке… И разговор закончился. Через пять минут я поняла, что меня ограбили». Женщина обратилась в милицию, где приняли заявление, а также в банк. «Прекрасно понимаю, что толку не будет никакого. Вряд ли кого-то найдут, и придется свыкаться с мыслью, что деньги потеряны, а для меня это очень большая сумма».

Внимание! Обычно мошенники пугают потерей большой суммы денег!

Стратегия мошенников

Как следует из рассказов пострадавших и тех, код входящего звонка отличается от белорусского совсем незаметно. Кто ж обратит внимание? Схемы разнообразные, но обычно мошенники пугают потерей большой суммы денег, которая «вот-вот произойдет, но можно все исправить».

«Здравствуйте, вас беспокоят из службы безопасности… (здесь может быть название любого белорусского банка. —. Меня зовут В…., на ваш счет завели овердрафт и пытались снять деньги, но мы заблокировали операцию как подозрительную. Необходимо проверить все ваши данные», — мошенники стараются говорить скороговоркой, чтобы наводнить внимание жертвы информацией. Испугав «овердрафтом», мошенник (звонивший с подставного номера, сходного с банковским) пытается выяснить паспортные данные, номер карты и просит продиктовать номер с оборотной стороны карты из SMS от банка — чтобы получить доступ к интернет-банкингу и завладеть деньгами.

В этом случае мошенники заранее владеют частью информации о жертвах: в частности, последними цифрами номера банковской карты и номерами телефонов. Откуда они? Точно не известно, но реквизиты могут быть указаны, например, во время проведения международных платежей на иностранном ресурсе, во время регистрации на белорусских интернет-площадках.

Комментарии банков

Представители финансовой сферы Беларуси, специалисты в области информационной безопасности сходятся во мнении: такой высокой активности мошенников они не припомнят, слабым звеном остается клиент. Чаще мошенники имеют лишь «черновик» данных о жертве, которая затем сама диктует полный номер карты, SMS-коды, строчки из паспорта и так далее. Кроме того, можно сколько угодно говорить: «со мной такого не случится», «простаки всегда найдутся», и жертвы в состоянии психологического давления ведут себя непредсказуемо для них самих. И именно чрезмерная самоуверенность играет против человека.

Что касается возврата средств, в такой ситуации это практически невозможно по ряду причин. Во-первых, обработка платежей ведется в режиме реального времени. Во-вторых, в Беларуси достаточно давно действует принцип «нулевой ответственности»: когда операции совершаются с подтверждением PIN-кодом и иной аутентификацией пользователя, они считаются подтвержденными и не могут быть оспорены. Проще говоря, если вы передали мошеннику данные, которые передавать не должны (подтверждающие SMS, логин/пароль, CVV и т. п.), и он ими воспользовался, — деньги списаны по правилам.

Управление защиты информации Национального банка (FinCERTby) рекомендует в случае поступления подобных звонков немедленно завершить разговор и обратиться в контакт-центр банка, эмитировавшего карточку, рассказать о ситуации и далее следовать рекомендациям сотрудника банка.

Как надо себя вести

- Никогда и никому не сообщайте полный номер карточки, период ее действия, фамилию, имя, отчество, одноразовый код из SMS, пароли от интернет-банкинга третьим лицам. Сотрудники банка могут попросить назвать только четыре последние цифры номера карточки и ФИО владельца.
- Ни в коем случае не передавайте CVV на обратной стороне карты (три цифры).
- Никому не передавайте сеансовые пароли, которые приходят по SMS. Если вы не запрашивали пароль сами (пытались войти в интернет-банкинг, например), а пароль пришел — также время бить тревогу.
- Не стесняйтесь проявить недоверие в случаях, когда вам звонят от имени банка и рассказывают о краже денег, незаконных операциях с вашей картой, оформлении кредитов, рассрочек и так далее — перезванивайте сами по телефонам, указанным на официальном сайте банка.
- Не публикуйте в сети данные вашей карты, если это не доверенная платежная система, которая требует ввода информации при проведении платежа. А лучше не используйте основную банковскую карту для интернет-платежей (заведите отдельную, перечисляйте деньги на нее по необходимости).
- Включите двухфакторную аутентификацию, где это возможно.
- Помните: мошенники считают вас слабым звеном. Разочаруйте их.
- В случае, если вы стали жертвой мошенников, блокируйте карты через контакт-центр, в мобильном интернет-банке или в чате поддержки. Если деньги уже вывели, остается только обращение в правоохранительные органы.

Внимание! Уважаемые граждане!

Чтобы не стать жертвой мошенников, которые работают посредством телефонных звонков и интернета, надо прочитать и запомнить эти правила поведения!

1. Никогда и никому не сообщайте полный номер карточки, период ее действия, фамилию, имя, отчество, одноразовый код из SMS, пароли от интернет-банкинга третьим лицам. Сотрудники банка могут попросить назвать только четыре последние цифры номера карточки и ФИО владельца.

2. Ни в коем случае не передавайте CVV на обратной стороне карты (три цифры).

3. Никому не передавайте сеансовые пароли, которые приходят по SMS. Если вы не запрашивали пароль сами (пытались войти в интернет-банкинг, например), а пароль пришел — также время бить тревогу.

4. Не стесняйтесь проявить недоверие в случаях, когда вам звонят от имени банка и рассказывают о краже денег, незаконных операциях с вашей картой, оформлении кредитов, рассрочек и так далее — перезванивайте сами по телефонам, указанным на официальном сайте банка.

5. Не публикуйте в сети данные вашей карты, если это не доверенная платежная система, которая требует ввода информации при проведении платежа. А лучше не используйте основную банковскую карту для интернет-платежей (заведите отдельную, перечисляйте деньги на нее по необходимости).

6. Включите двухфакторную аутентификацию, где это возможно.

7. Помните: мошенники считают вас слабым звеном. Разочаруйте их.

8. В случае, если вы стали жертвой мошенников, блокируйте карты через контакт-центр, в мобильном интернет-банке или в чате поддержки. Если деньги уже вывели, обращайтесь в правоохранительные органы.