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.

Не станьте жертвой мошенников

1. **Злоумышленник** после несанкционированного доступа к страницам пользователей в социальных сетях рассылает пользователям, находящимся в разделе «Друзья», сообщения с просьбой об оказании помощи в переводе денежных средств под различными предлогами: «Привет, не мог ли ты одолжить мне денег, отдам через пару дней», «Привет, положи, пожалуйста, 10 рублей на телефон, я отдам›), «Привет, можно я переведу тебе на карту свои деньги, а то у меня закончился срок действия карты (или не получается перевести на свою)». Далее входит в доверие к неравнодушным пользователям и, якобы для перевода им денежных средств, просит сообщить реквизиты БПК и коды из смс-сообщений. Пользователь, введенный в заблуждение относительно лица, осуществившего указанную рассылку, и не догадываясь о преступности намерений, сообщает ему указанные сведения, ввиду чего злоумышленник получает доступ к денежным средствам пользователя и совершает их хищение.

   Проведя несанкционированную операцию по переводу денежных средств, злоумышленник часто сообщает пользователю, что по техническим причинам не может осуществить операцию и просит повторить указанные действия с какой-либо другой картой (родственников или знакомых).

2. На торговых площадках «Куфар», «Барахолка» и других **злоумышленник** находит объявление, размещенное пользователем о продаже какого-либо имущества, после чего в различных мессенджерах пишет данному пользователю о том, что хотел бы приобрести его имущество, указанное в объявлении, однако по различным причинам не имеет возможности за ним приехать. Он предлагает произвести оплату путем перевода денежных средств на БПК пользователя и, после того как пользователь соглашается, высылает в его адрес ссылку с фишинговой страницей сайта какого-либо банковского учреждения (страница может быть визуально схожа со страницей интернет-банкинга и отличаться только символом в адресной строке доменного имени сайта). Переходя по указанной ссылке, пользователь не замечает, что находится не на действующей странице интернет-банкинга определенного банка.

   В открывшемся окне на указанном сайте пользователю, как правило, предлагается ввести свой логин и пароль от интернет-банкинга либо паспортные данные, а также коды из смс-сообщений. Введя указанную информацию пользователю, как правило, сообщается об ошибке либо отсутствии платежа. В это время всю введенную информацию видит злоумышленник и вводит на действительном сайте банка, получая тем самым доступ к денежным средствам пользователя и совершая их хищение. Проведя несанкционированную операцию по переводу денежных средств, правонарушитель нередко сообщает пользователю, что по техническим причинам не может осуществить операцию, и просит повторить указанные действия с какой-либо другой картой (родственников или знакомых).

3. На торговых площадках «Куфар», «Барахолка» и других злоумышленник размещает объявление о продаже какого-либо имущества, пользующегося спросом, и выставляет цену, как правило, ниже рыночной. Пользователи, увидевшие указанное объявление, пишут лицу, его разместившему, и в ходе переписки злоумышленник сообщает, что не имеет возможности встретиться для передачи указанного в объявлении имущества и предлагает воспользоваться услугами «Доставка Куфар», «Белпочта (ЕМС)», «курьерская служба (СДЭК)» и т. д. При согласии покупателя **злоумышленник** высылает в адрес пользователя ссылку с фишинговой страницей сайта какого-либо вида доставки, где предлагается ввести реквизиты банковской карты для оплаты товара, услуг курьера, паспортные данные, номер мобильного телефона, а также коды из смс-сообщений. После ввода указанной информацию пользователю обычно сообщается об ошибке либо сайт перестает загружаться (зависает). В это время всю введенную информацию видит злоумышленник и вводит ее на действительном сайте банка, получал доступ к денежным средствам пользователя и совершая их хищение. Проведя несанкционированную операцию по переводу денежных средств, злоумышленник сообщает пользователю, что по техническим причинам не может

осуществить операцию и просит повторить указанные действия с какой-либо другой картой (родственников или знакомых).

4. На мобильный телефон физического лица поступает входящий звонок от злоумышленника. Как правило, данным способом злоумышленник пользуется сервисом по подмену номера телефона и указывает абонентский номер, принадлежащий какому-либо банку или схожий с ним. Далее он представляется сотрудником банка (может назвать пользователя по имени и отчеству, а также назвать часть номера банковской карты либо информацию о недавно совершенных оплатах). **Злоумышленник** сообщает о подозрительных операциях по переводу денежных средств в крупных суммах на карт-счета иностранных банков. Когда пользователь сообщает, что никаких операций он не производил, злоумышленник сообщает, что указанные операции необходимо заблокировать, в связи с чем просит пользователя сообщить отдельные реквизиты БПК либо паспортные данные, и сообщает, что в адрес пользователя высылает смс-сообщения с кодами, которые необходимо назвать после звукового сигнала. В это время всю полученную информацию злоумышленник вводит на действительном сайте банка и получает доступ к денежным средствам пользователя и совершает их хищение.

5. На мобильный телефон физического лица поступает входящий звонок от злоумышленника. Как правило, данным способом злоумышленник пользуется сервисом по подмену номера телефона и указывает абонентский номер, принадлежащий какому-либо банку или схожий с ним. Далее он представляется сотрудником правоохранительных органов (милиционером, следователем) (может назвать пользователя по имени и отчеству, а также назвать часть номера банковской карты либо информацию о недавно совершенных оплатах). **Злоумышленник** сообщает о том, что на имя потерпевшего от неустановленного сотрудника банка взят кредит, и с целью установления данного сотрудника банка, в настоящее время проводится спецоперация и потерпевшему необходимо принять в ней участие, а именно — взять кредит на своё имя (в одном или нескольких банках). После получения кредита, просит предоставить сведения о карте, либо самостоятельно перечислить денежные средства на указанным им счёт, с целью аннулирования кредита. В последующем предлагает направиться в другой банк, либо просто прекращает общение с потерпевшим. В дальнейшем потерпевший узнаёт, что на его имя оформлен кредит (либо кредиты), а денежные средства похищены неустановленным лицом.

6. На мобильный телефон физического лица (как правило пожилым родственникам) поступает входящий звонок от злоумышленника. Как правило, данным способом **злоумышленник** пользуется сервисом по подмену номера телефона. Далее он представляется сотрудником правоохранительных органов (милиционером, следователем) и сообщает, что родственник потерпевшего попал в ДТП и находится без сознания (либо иногда дают пообщаться по телефону якобы с дочерью, сыном, мужем и т.п., которые в ходе разговора просят помочь) и родственник виноват в данном ДТП и для «решения» вопроса просят передать через курьера конверт с денежными средствами. После чего приезжает курьер и забирает данные денежные средства.