

ВЕРОЯТНЫЕ СЦЕНАРИИ ДЕЙСТВИЯ МОШЕННИКОВ!

► Сперва поступает первый звонок. Сценарий может быть разный: продлить договор оказания услуг связи, замена счетчиков либо домофона и т.д. Цель одна – любым обманным способом получить Ваши персональные данные (Ф.И.О., адрес, дата рождения) либо данные Вашей банковской карты.

► Спустя время – следующий звонок, в ходе которого Вам сообщат: «Вы ранее общались с мошенниками», «Вы подозреваетесь в финансировании экстремистской деятельности» либо «На Ваше имя в банке открыт счет в банке (оформлен кредит)» и т.д.

► Далее – Вас будут ЗАПУГИВАТЬ: поступят угрозы проблем с законом, начнут угрожать проведением обыска по месту жительства. Чтобы их избежать:

- потребуют задекларировать денежные средства, для чего придется их кому-то передать
- взять кредит в банке
- забрать деньги у другого лица

При поступлении подобных предложений – положите трубку и сообщите об этом по номеру «102»! Ни в коем случае не сообщайте посторонним персональные данные! Их цель – завладеть Вашими сбережениями!

Если от Вас требуют забрать у кого-то деньги и передать третьим лицам – знайте – это втягивание Вас в преступную цепочку.

Курьеры, согласно ст. 209 УК (Мошенничество), работающие на аферистов, наравне с другими участниками преступных схем отвечают по закону и обязаны возмещать материальный вред, причиненный потерпевшим.



ВАШ УЧАСТКОВЫЙ ВСЕГДА РЯДОМ!



ВАШ УЧАСТКОВЫЙ КАЖДУЮ СРЕДУ ОСУЩЕСТВЛЯЕТ ПРИЕМ ГРАЖДАН В ОБЩЕСТВЕННОМ ПУНКТЕ ПРАВОПОРЯДКА



В ГОРОДЕ

С 17:00 ДО 20:00



В СЕЛЬСКОЙ МЕСТНОСТИ

С 10:00 ДО 13:00

Мы всегда рядом!

**ВАМ ЗВОНЯТ И СООБЩАЮТ
О ПОДОЗРИТЕЛЬНЫХ
ОПЕРАЦИЯХ С БАНКОВСКОЙ
КАРТОЧКОЙ, ПРОСЯТ
НАЗВАТЬ ПЕРСОНАЛЬНЫЕ
ДАННЫЕ?**



**СЛЕДУЮЩИЙ
ЗВОНОК БУДЕТ
С УГРОЗАМИ ОБЫСКА
ПО МЕСТУ ЖИТЕЛЬСТВА**

**ТАК ДЕЙСТВУЮТ ТОЛЬКО
МОШЕННИКИ**

**ЭЛЕМЕНТАРНЫЕ ПРАВИЛА,
КОТОРЫЕ ПОЗВОЛЯТ
СОХРАНИТЬ ВАШИ
СБЕРЕЖЕНИЯ:**

- не выполняйте указания лиц, позвонивших с незнакомого номера
- не сообщайте незнакомцам свои персональные данные, реквизиты персональной банковской карты
- не устанавливайте приложения по просьбе посторонних
- не переводите деньги незнакомым людям в качестве предоплаты
- не соглашайтесь на онлайн-предложения о покупке вещей по слишком низкой цене

**ВАМ ПРЕДЛАГАЮТ УСТАНОВИТЬ
ДОМОФОН, ЗАДЕКЛАРИРОВАТЬ
ДЕНЕЖНЫЕ СРЕДСТВА?**

ЭТО МОШЕННИКИ



**ПОЛОЖИТЕ ТРУБКУ
И ЗАБЛОКИРУЙТЕ НОМЕР**

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 обратной 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 предложениями: «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 равнодушным 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 информации 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 высылают 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.

Как не стать жертвой киберпреступлений

Достижения науки и техники, создание всемирной сети интернет позволили преступности выйти на новый уровень и захватить киберпространство.

Теперь преступнику не нужен прямой контакт с жертвой, он может стать угрозой для каждого пользователя «глобальной паутины», крупных корпораций и целых государств.

Защита пожилых людей от мошенников — это постоянный процесс. Чем больше вы будете общаться и информировать их, тем меньше шансов, что они станут жертвами обмана. Мошенники постоянно совершенствуют схемы обмана, поэтому наша задача — не просто предупредить, а научить человека моментально распознавать угрозу.

Лучшая защита — это бдительность и знание простых правил: никаких кодов из СМС, никаких «безопасных счетов», только личный визит в банк и звонки правоохранителям.

Мошенники постоянно придумывают новые способы обмана, и пожилые люди часто поддаются на их уловки. Поговорите с ними о мошенничестве. Объясняйте, какие схемы сейчас популярны и расскажите реальные истории о тех, кто попался на удочку мошенников.

Основные схемы мошенничеств:

«Оператор сотовой связи» и «Белтелеком». В ходе беседы злоумышленник сообщает человеку, что у него заканчивается срок действия договора на оказание услуг. Путем оформления заявки мошенники узнают паспортные данные и склоняют к установке сторонних приложений.

«Обновление кода домофона». Мошенник звонит жертве, представляясь сотрудником управляющей компании, службы безопасности или другой официальной организации. Злоумышленники сообщают, что новый код придет в СМС и его надо сообщить для обновления в системе. Только на самом деле СМС поступает от банка для получения кредитов, где получателями денежных средств являются злоумышленники.

«Водоканал» и «Электросети»: проверка или замена счетчиков. В ходе беседы злоумышленник предлагает человеку оставить заявку на поверку или замену счетчиков. Используя легенду о необходимости заполнения заявки, злоумышленники выманивают конфиденциальные паспортные данные. Следует отметить, что злоумышленники активно используют как мессенджеры, так и домашние телефоны для осуществления указанных схем преступлений.

«Декларирование денежных средств с целью их сохранности». Мошенник убеждает потерпевшего сообщить поступивший из СМС код. Затем поступает второй звонок, где неизвестный угрожает возбуждением

уголовного дела, проведением по месту жительства обыска, в ходе которого все денежные средства будут изъяты и предлагает во избежание этого сбережения передать «курьеру» для декларирования и сохранности. Не единичны случаи, когда в роли курьеров мошенники используют лиц, ранее обманутых аферистами и убеждают в том, что они участвуют в проводимой правоохранительными органами спецоперации.

Необходимо на постоянной основе доводить до сведения населения, особенно пожилым и престарелым, что:

Сотрудники милиции и иных правоохранительных органов никогда не звонят в мессенджерах и не требуют перевода денег для «декларирования» или «освобождения от ответственности»!

Никому нельзя сообщать свои личные данные, данные банковских карт, коды из SMS по телефону, даже если звонящий говорит, что он из банка или другой организации!

Ни при каких обстоятельствах нельзя оформлять кредиты по просьбе третьих лиц и переводить денежные средства на неизвестные банковские «безопасные» счета!

Нельзя открывать электронные письма от незнакомцев и переходить на подозрительные ссылки!

С целью повышения цифровой грамотности населения (в том числе с целью профилактики преступлений в отношении пожилых и престарелых граждан) и профилактики киберпреступлений в Брестской области, функционирует телеграм-канал «КИБЕРКРЕПОСТЬ», администрируемый управлением по противодействию киберпреступности УВД.

В связи с вышеизложенным, всем сотрудникам, в том числе и гражданскому персоналу рекомендуем подписаться на телеграм-канал «КИБЕРКРЕПОСТЬ».

С целью охвата всех слоев населения, профилактики киберпреступлений в рамках проведения бесед в трудовых коллективах организаций, предприятий и учреждений, учебных заведениях, предлагать подписаться на телеграм-канал «КИБЕРКРЕПОСТЬ» и иные Интернет-ресурсы УВД для получения актуальной и оперативной информации о совершаемых киберпреступлениях и способах противодействия таким преступлениям.



Осуществить подписку на вышеуказанный телеграм-канал можно с использованием QR-кода, а также путем введения в поисковую строку мессенджера «Telegram» «КИБЕРКРЕПОСТЬ».

УОПШ УВД Брестского облисполкома