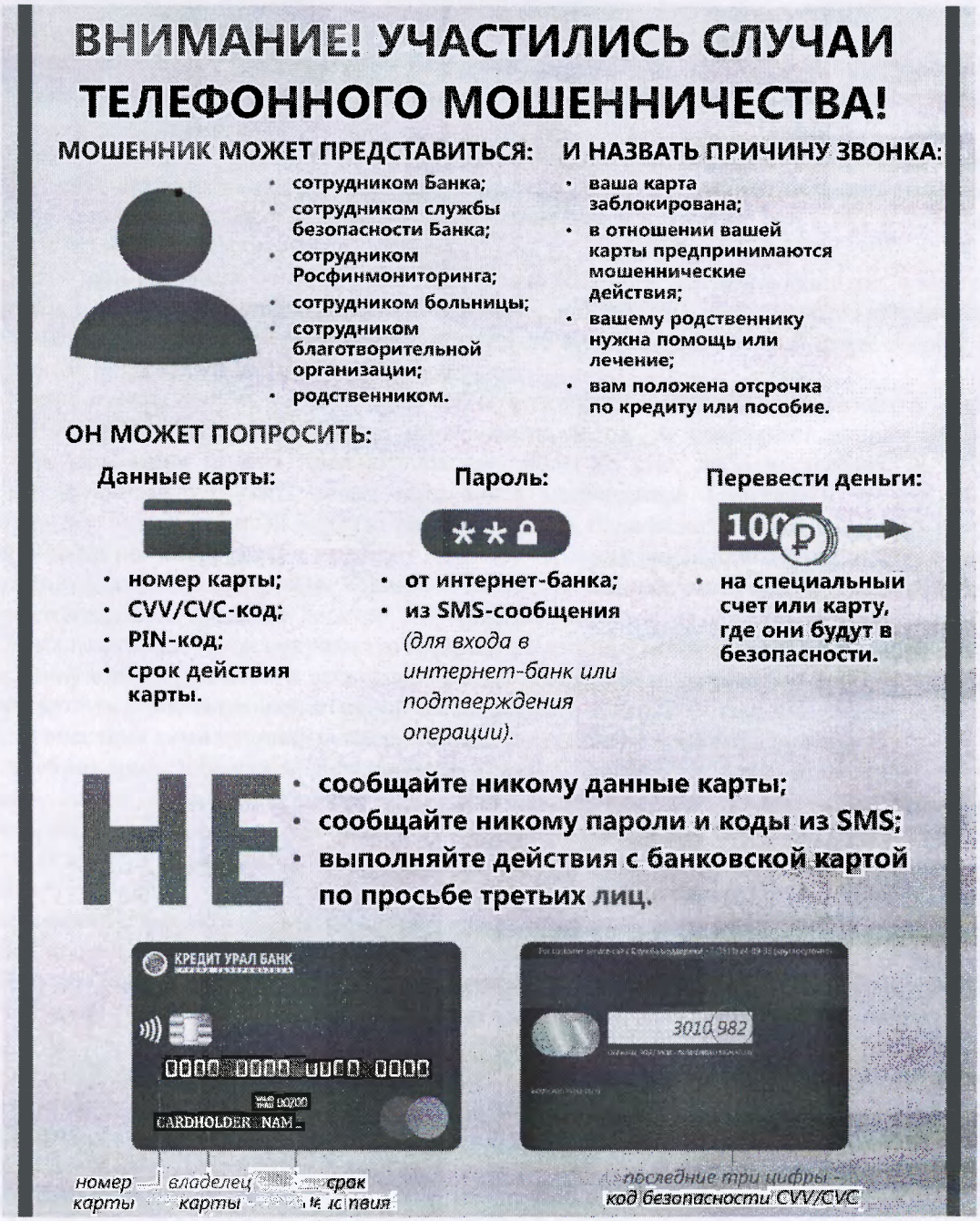
В первую очередь нужно акцентировать внимание на использовании преступниками ключевых стоп-слов и фраз: **«ФСБ», «МВД», «Центральный банк», «безопасный счет», «сообщите код из СМС / данные карты / паспорта / СНИЛС», «перейти по ссылке», «скачать программу», «передать деньги курьеру»**, услышав которые необходимо незамедлительно прекратить разговор.



Актуальные схемы телефонного мошенничества.

. **Сотрудник банка завладел вашими персональными данными, чтобы взять на вас кредит.** Злоумышленники представляются сотрудниками прокуратуры, полиции, ФСБ, Банка России, и других ведомств. «Следователь» сообщает примерно следующее: «Проводится расследование, с целью задержания злоумышленника, который хотел взять кредит по вашим данным, все что вам стало известно находится под грифом «секретно», никому нельзя разглашать полученную информацию, и строго выполнять все инструкции». Далее происходит опрос, звонящего интересует в каком банке у вас открыты счета, номера карт, срок действия, CVC-код с оборота, и код из смс, после чего мошенники получают доступ к личному кабинету, и похищают денежные средства. Однако, существует и другой вариант развития событий: «следователь» связывает вас с «сотрудником банка», который сообщает, что во избежание хищения, деньги со всех счетов на период расследования необходимо перевести на «безопасный счет», а также необходимо быстрее злоумышленников взять в банке кредит, чтобы обнулить свой кредитный потенциал, после чего жертва переводит личные сбережения, и полученные по кредиту средства, на счета злоумышленников.

Также, злоумышленники чтобы ввести вас в заблуждение, могут сообщать Вам об изменении номера телефона в личном кабинете банка, после чего связывают с «оператором банка», который также действует по вышеуказанной схеме, пытаясь завладеть данными банковских карт, либо вынудить жертву перевести денежные средства на счета мошенников.

Для доступа к кодам из смс, а также push уведомлениям жертвы, злоумышленники во время звонков через мессенджеры Telegram и WhatsApp просят активировать функцию «демонстрации экрана», которая позволит им видеть все что происходит на экране устройства жертвы, в том числе приходящие смс и push, получив коды из которых получат доступ к онлайн банку, и похитят деньги со счетов.

2. **Поможем вернуть ваши деньги.** После того, как человек уже стал жертвой злоумышленников, с ним связывается «юридическая кампания», и предлагают списать имеющиеся долги, или вернуть похищенные мошенниками деньги, рассказывая об имеющихся у них для этого возможностях, которые основываются на принципе отмены банковских операций. После получения предоплаты за свои услуги, исчезают.
3. **Спасем от звонков мошенников.** Злоумышленники сначала атакуют жертву звонками, после чего поступает звонок от «сотрудников» Центрального банка, их службы безопасности, и т.д., и предлагает подключить вас услугу «Антиспам». Для этого, мошенник просит продиктовать ему коды из смс, либо установить на свой телефон приложение, файл для установки которого может прислать в мессенджере Telegram и WhatsApp. Указанное приложение содержит в себе вирус, который похитит данные о ваших банковских счетах, входящих смс, и т.д., что позволит злоумышленниками получить доступ к вашему личному кабинету банка, и похитить деньги со счетов.
4. **Заработок на маркетплейсах «Вайлдберриз», «Озон» и иных.** Мошенник связывается с жертвой по телефону, чаще посредством мессенджеров Telegram и WhatsApp, и предлагает заработок, суть которого заключается в поднятии рейтинга продавцов, что достигается путем покупки его товаров. По легенде, чтобы помочь «продавцу», нужно купить его товар, затем заказ аннулируется, а деньги возвращаются, да еще и с благодарностью в 4-5 % от суммы заказа. Затем, вам предлагают купить с последующей отменой более дорогой товар, сообщая что только сейчас есть такой шанс заработать. После внесения вами крупной суммы, мошенник исчезает с вашими деньгами
5. **Предложения от лжеброкеров.** Обещание легких денег многих привлекает. Злоумышленники связываются с потенциальными инвесторами через социальные сети или звонят им под видом сотрудников известных инвестиционных компаний. Предложение заманчивое – нужно лишь открыть «брокерский» счет и инвестировать от 10 000 рублей. Доход – не меньше миллиона. Для открытия такого счета мошенники требуют установить приложение. Далее программа имитирует якобы рост доходов от инвестиций, в том числе в крипто валюту. Как только у «инвестора» возникает желание вывести деньги со счета – начинаются проблемы. Лжеброкеры говорят, что сделать это сложно. Нужно пополнить счет еще раз на определенную сумму, оплатить «страховку» или ежедневное размещение валюты в «европейской ячейке» либо найти поручителя и даже зарегистрировать его в Минфине России, чтобы можно было «обналичить» средства. В итоге инвестор теряет свои деньги, а заодно и надежду на будущие миллионы.

Вариант этой мошеннической схемы – участие в уникальном инвестиционном онлайн-проекте известного банка. Завлекают потенциальных жертв при помощи писем на электронную почту. Злоумышленники, оформляя сообщение, копируют визуальный стиль финансовой организации и далее для убедительности используют те же корпоративные цвета, логотип и другие элементы. Для участия в «выгодной» кампании предлагается перейти по ссылке из письма. После жертве предложат пройти опрос: указать заработок, предпочитаемый способ хранения средств и контактные данные для связи с представителем организации, а также дадут доступ к специальному приложению. А уже там понадобится ввести данные своей банковской карты – с нее аферисты потом и спишут деньги.

Не ведитесь на обещания гарантированного высокого дохода в короткие сроки

6. **Сохраним ваши сбережения.** Мошенники звонят и вводят в заблуждение информацией о том, что из-за санкций хранить деньги в российском банке небезопасно, поскольку в любой момент их якобы могут заморозить и снять их не получится. Вам предлагают дистанционно открыть счет в иностранном банке, поскольку там сбережения будут в большей безопасности. Для того, чтобы открыть счет, нужно внести первоначальную сумму. После внесения вами денежных средств, мошенник исчезает с вашими деньгами.
7. **Родственник попал в беду.** Как правило, пожилым людям поступает звонко на стационарный или мобильный телефон, от «внучки», которая плача рассказывает о том что попала в ДТП, в котором пострадали люди, и просит срочно занять крупную сумму денег, чтобы решить вопрос с пострадавшими. По другой схеме, мошенник сообщает что задержан полицией пьяным за рулем, или с наркотиками, и просит денег для решения вопроса с

правоохранителями. Когда жертва соглашается помочь, приходит курьер, который забирает деньги. При этом, звонок может поступать как от «родственника», так и от «сотрудника полиции», который предлагает выручить родственника. Аналогичным образом могут поступать СМС сообщения, с просьбой перевести определенную сумму денег на указанный номер, используя обращения «мама», «сынок», «друг» и т.д.

8. Онлайн покупки, оплата товаров и услуг. На таких сайтах, как «Авито», «Юла», в группах по продажам в соцсетях, мошенники часто просят предоплату за несуществующий товар или услугу. Перед переводом денег, убедитесь в надежности продавца, например попросите сфотографировать товар на фоне какой-либо надписи на листе бумаги. Также, рекомендуется пользоваться «Авито доставкой», в таком случае продавец получит деньги только после того, как вы получите товар и убедитесь в его качестве.

Также, при проведении онлайн аукционов в социальных сетях, вам могут поступать сообщения с поддельного профиля организатора аукциона, с предложением выкупить лот, так как предыдущий человек отказался от своей ставки.

9. Звонок от оператора сотовой связи. Злоумышленник представляется сотрудником технической поддержки оператора сотовой связи (МТС, Билайн и т.д.), и сообщает что у вас истекает срок действия сим карты, и предлагает продлить его, для чего необходимо продиктовать код из смс. В случае если указанный номер телефона привязан к банку, злоумышленник получает доступ к вашим счетам, либо аккаунту "ГосУслуг", где получит ваши персональные данные, при помощи которых сможет взять на ваше имя, к примеру онлайн микрозайм.

10. Просьба занять денег. В социальной сети, или мессенджере, жертве поступает смс с аккаунта друга или родственника, который просит срочно занять ему денег, обещая вернуть в ближайшее время. Денежные средства как правило просит перевести на банковскую карту неизвестного лица. В отдельных случаях, мошенник может прислать фотографию банковской карты, на которой будет написано имя вашего друга, родственника, однако это сделано с помощью фотошопа. Перед переводом денег, обязательно созвонитесь с другом, родственником, так как его аккаунт возможно был взломан и попал в руки злоумышленников.

11. Установка банковских приложений. В последнее время, не все банковские приложения доступны в официальных приложениях, таких как «Гугл плей». Ни в коем случае не устанавливайте банковские приложения с подозрительных сайтов. Для установки приложений используйте официальные сайты банков, либо обратитесь в отделение банка. В случае если вы авторизуетесь в приложении банка, которое установлено из ненадежного источника, мошенники получат доступ к вашим банковским счетам и похитят ваши деньги.

12. Поступление смс от имени руководителя в «Телеграмм», который просит оказать содействие правоохранительным органам в связи с утечкой персональных данных, в дальнейшем с жертвой также связываются «правоохранительные органы», «сотрудники банка» и иные лица, которые убеждают перевести свои средства на неизвестные счета, либо оформить кредит, продиктовать смс.

13. Подозрительные ссылки, и файлы. Мошенники присылают в мессенджерах вредоносный файл, с заманчивой надпись, например, «Посмотри, это ты на фото», и после того как жертва скачает указанный файл на свое устройство, мошенники удаленно через вышеуказанную вредоносную программу получают удаленный доступ к устройству жертвы, похищают деньги с карт, оформляют кредиты.

Как защититься от мошенников?

1. Не сообщайте никому номер карты, срок действия, CVC-код с оборота карты, коды из смс сообщений и PUSH уведомлений.
2. Не включайте функцию демонстрации экрана, во время звонков через мессенджеры, это позволит злоумышленникам увидеть содержимое ваших смс, в том числе коды, которые позволят им получить доступ к онлайн банку.
3. Не переводите свои деньги на «безопасный» счет по инструкции звонящего.
4. Не оставляйте свои персональные данные на сайтах, в анкетах и подозрительных формах сбора информации.
5. Устанавливайте приложения банков только из официальных источников, сайтов банка.
6. Перед тем, как занять кому-либо денежные средства, обязательно созвонитесь с получателем, также обращайте внимание на кого открыта карта, на которую вы переводите средства.
7. Если у вас требуют деньги для помощи родственнику, попавшему в беду, постарайтесь сначала дозвониться до родственника. вероятнее всего с ним всё в порядке. Если вы вдруг не дозвонились, то обратитесь в ближайший отдел полиции.
8. Не принимайте поспешных действий, связанных с вашими финансами. Если вас торопят с принятием решений, требуют незамедлительно продиктовать данные или перевести деньги на другой счет незнакомые люди, пугают последствиями отказа это сделать, пытаются вывести из эмоционального равновесия – прервите разговор. Ели есть сомнения, позвоните на горячую линию своего банка, в полицию, а также обсудите ситуацию со своими родными и близкими.
9. Проверяйте подлинность кампаний, которые оказывают услуги. У финансовых организаций – лицензию на сайте Банка России, компании по продаже ОСАГО и подлинность полиса – в базе РСА, предложение от госслужб – на официальных сайтах организаций.
10. Не стоит верить звонкам роботов-помощников. Если у вас возникли вопросы или сомнения, лучше позвоните в банк по официальному номеру.
11. Не переходите по ссылкам из писем и сообщений в мессенджерах.
12. Чтобы не попасться на удочку инвестиционных мошенников: Проверьте сайт инвестиционной компании или брокера. Обратите внимание на реквизиты и наличие лицензии Банка России. Откажитесь от услуг компании или ее представителей, если они просят перевести деньги за услуги на карту физического лица (либо через электронный кошелек). Обязательно заключите договор и запрашивайте отчет об оказании брокерских услуг.