

ПАМЯТКА «Телефонные мошенники»

Вариант 1: неизвестный представляется сотрудником полиции, следователем, сотрудником ФСБ и т.д. (номер телефона может соответствовать реальному отделу госучреждения, так как мошенники используют программу подмены номера) и сообщает, что проводится спецоперация по поимке мошенников, которые незаконно пытаются оформить кредит от Вашего имени. Для предотвращения якобы мошеннических действий предлагают срочно взять «зеркальный» кредит (исчерпать свой кредитный потенциал, чтобы мошенники не смогли оформить кредит) и полученные денежные средства требуют перевести на «безопасный счет». На самом деле данный счет находится под контролем злоумышленников. При этом злоумышленник требует не звонить в банк, так как сотрудники банка, якобы, подозреваются в совершении мошеннических действий. Известны случаи, что перед звонком «службы безопасности» жертве мошенничества приходили сообщения в мессенджерах от руководства организации или предприятия, где сообщалось о том, что якобы на предприятии произошла утечка персональных данных и мошенники пытаются оформить кредиты, от имени руководителя сотрудников просят действовать по указанию «службы безопасности», в том числе по указанию сотрудников ФСБ.

Вариант 2: Вы нашли объявление в сети интернет о заработке на инвестиционных площадках. С Вами связываются якобы консультанты и предлагают инвестировать Ваши денежные средства в различные акции. Злоумышленники отправляют ссылку на якобы официальные торговые площадки (на самом деле страницы поддельные), после перевода Вами денежных средств на данных сайтах вы будете видеть ложную информацию о прибыли. «Консультанты» будут просить Вас внести все большую и большую сумму денежных средств для получения максимальной прибыли. Как только Вы попытаетесь вывести свои денежные средства, злоумышленники перестанут Вам отвечать. Данный способ мошенничества длительный от нескольких дней до нескольких месяцев. Как правило жертва мошенничества на протяжении длительного времени лишается всех своих сбережений и оформляет на свое имя несколько кредитов и денежных займов на сумму в несколько миллионов рублей!

Вариант 3: Мошенники под различным предлогом (якобы была попытка взлома личного кабинета или получения какой-либо услуги, в том числе начисления пенсии либо продления договора на обслуживание номера сотового телефона, получения заказного письма или посылки) пытаются узнать пароль от личного кабинета «Госуслуг», просят назвать код приходящий в СМС сообщении, после чего получают доступ к персональной информации и смогут оформить онлайн кредиты. Ни в коем случае никому не сообщайте четырехзначный пароль от «Госуслуг» и не передавайте данные приходящие в СМС сообщениях. Известны случаи что после «взлома» личного кабинета «госуслуг» начинают поступать звонки от якобы «сотрудников службы безопасности, росфинмониторинга, правоохранительных органов, ФСБ», которые сообщают, что взломан личный кабинет «Госуслуг», убеждают граждан оформить займы и перевести денежные средства на «безопасные счета».

Вариант 4: неизвестный сообщает, что Ваш родственник, либо близкий человек попал в беду (попал в дорожно-транспортное происшествие, сбил человека на автомобиле или обвиняется в преступлении) при этом задержан сотрудниками правоохранительных органов, и для освобождения необходимо перевести на счет либо передать курьеру денежные средства для примирения с пострадавшим либо в качестве взятки сотрудникам полиции. Возможны варианты, при которых в разговоре могут принять участие, якобы, сотрудники полиции, медицинские работники, которые будут подтверждать сказанное.

Вариант 5: неизвестный представляется сотрудником службы безопасности банка и предлагает для корректной работы онлайн приложения банка установить дополнительное приложение на телефон для защиты от несанкционированного доступа и от мошенников. На самом деле злоумышленники, с помощью лица, введенного в заблуждение, которое действует по указаниям мошенников, устанавливают приложения, которые предоставляют мошенникам удаленный доступ к вашему телефону, после чего мошенники получают доступ ко всем приложениям Вашего телефона, похищают денежные средства и оформляют онлайн займы.

Вариант 6: вы нашли в интернете или на различных мессенджерах информацию о продаже товара по привлекательной цене. Связываетесь с продавцом и продавец просит Вас перевести деньги,

обещая отправить товар почтой, указывает номер карты. После перевода денежных средств, продавец перестает отвечать на сообщения (самый простой и нехитрый способ). По этой-же схеме продавец может скинуть ссылку на якобы официальный сайт магазина или торговой площадки, где попросит Вас оплатить товар (указать данные вашей карты, в том числе трехзначный код на обратной стороне карты). После введения данных карты злоумышленники получают доступ к Вашему счету и похитят все денежные средства, находящиеся на счету.

Вариант 7: Вы нашли объявление о заработке, либо с Вами связываются «консультанты» с помощью мессенджера и предлагают не хитрые задания (просмотр страниц, оставление отзывов и т.д.), за которые в начале даже переводят Вам денежные средства, чтобы усыпить бдительность, а в дальнейшем «консультанты» уже просят вас внести денежные средства на покупку товаров, бронирование отелей, покупка криптовалюты и т.д., чтобы, якобы, получить большую прибыль, просят оформлять кредиты. При попытке вывести денежные средства с Вами перестают общаться.

Вариант 8: Мошенники взламывают аккаунты пользователей страниц в социальных сетях и различных мессенджерах, где от имени ваших друзей и родственников просят занять крупные суммы денежных средств под различными предложениями (на лечение детей, оплаты штрафов и т.д.). Не переводите деньги не убедившись в том, что с вами действительно общается Ваш знакомый или родственник. Для предотвращения попыток взлома Ваших аккаунтов не переходите по «сомнительным» ссылкам для голосования, приходящим даже от Ваших знакомых и родственников.

Вариант 9: Мошенники начали использовать несовершеннолетних, так детям, играющим в онлайн-игры в чате игры поступает сообщение от другого игрока о возможности получить игровую валюту, но для этого необходимо отправить через онлайн-банк денежные средства, после чего на счет аккаунта будет зачислена игровая валюта и осуществлен возврат переведенных ранее денежных средств. После чего в силу возраста малолетние, не осознавая происходящее, под различными предложениями берут сотовые телефоны родителей и под руководством игрока, использующего системы мгновенных сообщений, такие как «Discord», «Telegram», с банковских счетов своих родителей в приложениях онлайн-банков переводят денежные средства, в том числе кредитные, на счета, подконтрольные мошенникам.

Вариант 10: Осуществление звонков из поликлиник или коммунальных служб. В ходе звонка преступники сообщают, что давно не пройдена диспансеризация, для записи необходимо скачать мобильное приложение "Емиас" на сотовый телефон, после чего по "WhatsApp" отправляют загрузочный файл (либо отправляют посредством СМС ссылку на скачивание с фишинг-сайта), который необходимо установить на свой мобильный телефон. После установки данного приложения преступники получают удаленный доступ к мобильному устройству и банковским приложениям.. Аналогично вышеуказанному способу, в ходе звонка преступники сообщают, что необходимо произвести замену счетчиков, отправляют загрузочный файл приложения «Энергосбыт» («Энерго плюс» либо иное название). После установки данного приложения преступники получают удаленный доступ к мобильному устройству и банковским приложениям.

Вариант 11: Злоумышленники представляются сотрудниками банковских организаций и предлагают установить новое приложение ЦБ РФ на операционную систему «Android», для предотвращения каких-либо противоправных действий. Под видом скаченного приложения замаскирована вредоносная программа, которая позволяет перехватывать данные телефона. Далее злоумышленники предлагают отсканировать и верифицировать свою банковскую карту, поднеся ее к NFC-модулю мобильного телефона. Получив виртуальный образ банковской карты, злоумышленники осуществляют снятие всех денежных средств с карты потерпевшего.

Вариант 12: Злоумышленники, представляясь сотрудниками учебного заведения, под различными предложениями, в том числе корректировки данных в электронном дневнике, узнают у несовершеннолетнего код от портала Госуслуг. Используя полученный код, убеждают несовершеннолетнего, что его аккаунт и аккаунт его родителей взломаны и используются для переводом в недружественные страны. Далее вынуждают несовершеннолетнего осуществить переводы денежных средств с банковских карт родителей на «безопасные счета» подконтрольные злоумышленникам.