Наиболее актуальные действия мошенников

1. Мошенники используют новую и убедительную для жертв схему с использованием Госуслуг и приложения для электронной подписи «Госключ».

Сначала аферисты получают доступ к личному кабинету жертвы на Госуслугах. Затем загружают поддельную нотариальную доверенность на распоряжение всеми счетами человека в специальный раздел «Госуслуг» для подписания документов в «Госключе». Жертве приходит уведомление о том, что нужно подписать документ. Далее звонит якобы сотрудник органов, который убеждает, что все счета скомпрометированы, поэтому надо срочно подписать доверенность, чтобы он смог спасти деньги. После подписания снова звонит сотрудник, но уже якобы настоящий, и сообщает, что человек стал жертвой мошенников. После осле подписания доверенности мошенники получили доступ ко всем счетам, поэтому средства с них нужно незамедлительно перевести на «безопасный счет».

Кроме того, получив доступ к аккаунту жертвы на Госуслугах мошенники используют личный кабинет для получения микрокредитов от имени жертвы.

2. Мошенники используют новую схему с корпоративными групповыми чатами.

Злоумышленники создают чаты и добавляют в них сотрудников организации, а также фейковые аккаунты их руководителей. После этого от лица начальника пишут, что в компании проходит проверка и предупреждают работников о звонке «от правоохранительных или контролирующих организаций». Далее мошенники могут попросить потенциальных жертв перевести средства на посторонние счета якобы для нужд организации. Также аферисты могут предложить установить какое-либо вирусное ПО или попросить список сотрудников с персональными данными.

3. Мошенники начали обманывать самозанятых и индивидуальных предпринимателей от имени сотрудников ФНС.

Они говорят, что видят неучтённые при расчёте налога доходы, и предлагают провести сверку, якобы документ уже направили. Жертва его у себя не находит, что псевдо- налоговик объясняет рассинхронизацией с Госуслугами. А чтобы восстановить работу, нужен код из SMS. Далее с этой информацией преступники получают доступ к Госуслугам и личным данным жертвы.

4. Мошенники начали обманывать россиян от несуществующей «Единой медицинской службы» или от имени районной поликлиники.

Они звонят и интересуются, когда была сделана последняя флюорография или сообщают, что жертве назначены анализы в рамках диспансеризации, а после сообщают об устаревших данных, которые нужно обновить. Для этого они просят номер СНИЛС и/или код из SMS. Далее с этой информацией преступники получают доступ к Госуслугам и личным данным жертвы.

5. Мошенники представляются сотрудникам операторов сотовой связи.

В таком случае мошенник сообщает жертве, что срок ее контракта подошел к концу и необходимо продлить его. Для этого надо сообщить код из СМС иначе телефон будет отключен. По такой же схеме сообщают о подключенных дорогостоящих услугах, для отключения которых также нужно сообщить код из СМС. Далее с этой информацией преступники получают доступ к Госуслугам и личным данным жертвы, а также к системам дистанционного банковского обслуживания.

6. Старые схемы еще используются. По-прежнему популярны у мошенников давно известные схемы со звонками от имени сотрудников «службы безопасности банка», сотрудников правоохранительных органов или Центрального Банка.

Мошенники убеждают жертву, что кто-то получил доступ к ее счетам и необходимо перевести средства на «безопасный счет».

Мошенники также могут сообщить, что кто-то, используя похищенные персональные данные жертвы пытается получить от её имени кредит. Чтобы обезопасить себя и способствовать поимке злоумышленников, жертве надо срочно взять кредит и также перевести его на «безопасный счет». В результате жертва не только теряет деньги, но и становится должником банка или микрокредитной организации.

Помощники мошенников – дропперы.

В состав преступной мошеннической группы всегда входят дропперы, которые занимаются выводом денежных средств с карточных счетов, куда мошенники переводят похищенные денежные средства со счетов потерпевших для последующего обналичивания. Обычно в дропперы завлекают молодых людей в возрасте 18-25 лет через объявления в социальных сетях Интернета, обещая легкий заработок. Молодые люди, соглашаясь на такую работу, обычно никогда не увидят своих «работодателей», но они становятся соучастниками преступления в составе организованной преступной группы лиц при осуществлении мошеннических операций их «работодателей». Также мошенники предлагают просто продать карты или сдать в аренду на время за вознаграждение. Это тоже является пособничеством мошенникам.

При выявлении дропперов и доказательстве их вины суд обычно назначает им реальные сроки наказания в виде лишения свободы от 5 лет и выше.

Остерегайтесь сами и предостерегайте своих детей о непоправимых последствиях таких видов заработка.

Рекомендации:

В телефонной беседе никому и никогда не сообщайте никакие коды из SMS-сообщений, push-уведомлений, номера карт и счетов, логины и/или пароли от интернет или мобильного банка, Госуслуг. Нельзя разглашать незнакомым лицам Ваши персональные данные.

При поступлении телефонных звонков от имени «Центрального Банка», «служб безопасности банка» или «представителей правоохранительных органов» и прочих организаций, в которых пытаются выяснить Ваши персональные данные и/или просят сообщить коды из СМС, немедленно прекращайте телефонный разговор и при необходимости перезвоните в Ваш банк сами.
Помните, что сотрудники банков НИКОГДА не просят сообщить им какие-либо коды и пароли.

Сотрудники Банка России (Центрального Банка) НИКОГДА не звонят клиентам банков с информацией о попытках списания средств со счетов граждан и не просят сообщить какие-либо коды.
Представителям государственных структур, в том числе правоохранительных органов, КАТЕГОРИЧЕСКИ ЗАПРЕЩЕНО использовать мессенджеры типа WhatsAPP, Viber, Telegramm и т.д. в служебных целях.

НЕ СУЩЕСТВУЮЕТ «БЕЗОПАСНЫХ СЧЕТОВ» В ЦЕНТРАЛЬНОМ БАНКЕ И В ЛЮБОМ ДРУГОМ БАНКЕ. Если Вам предлагают перевести средства на «безопасный», «защищенный» или какой-либо другой такого рода счет, не важно по безналичному расчету, путем передачи курьеру или через банкомат. ЭТО МОШЕННИКИ. Ни в коем случае не переводите средства на такой счет.
Пожалуйста, незамедлительно сообщите реквизиты такого счета (номера карты и других, известных Вам реквизитов мошенников) в Ваш банк, а также обратитесь в правоохранительные органы. Это поможет обезопасить Вас и других граждан от мошенников.