Осторожно, мошенники!!!

Все новые схемы мошенничества - это немного модернизированные старые. Несмотря на то, что мобильные операторы и компании, занимающиеся информационной безопасностью, пытаются максимально осложнить жизнь кибермошенникам, те находят новые способы для получения персональных данных граждан.

Так, аферисты при звонке представляются сотрудниками: Социального фонда — с вопросом о перерасчете пенсии, Сотовых операторов — для оформления продления договора об оказании услуг сотовой связи, Жилищно-коммунальных услуг — по факту записи на замену счетчиков, пересчета электроэнергии и т.п. В случае согласия граждан на ту или иную услугу, злоумышленники предлагают подать заявление в телефонном режиме. Для идентификации просят продиктовать поступивший код из СМС-сообщения. Узнав данный код, мошенники получают доступ к аккаунту «Госуслуг», либо к банковскому приложению, что приводит к компрометации учетной записи или к попытке перевода денежных средств со счета граждан.

После чего жителям поступают звонки от лже-сотрудников правоохранительных органов, Центрального банка и кредитных организаций, которые сообщают потрепевшим о том, что доступ к порталу «Госуслуг» взломан. Далее мошенники поясняют гражданам, чтобы обезопасить свои денежные средства необходимо по их указанию перевести сбережения на «безопасный» счет.

Полиция напоминает, для того чтобы обезопасить себя от мошеннических действий, запомните ПРОСТЫЕ ПРАВИЛА:

- Никому не сообщайте коды безопасности из СМС-сообщений;

- Никому не сообщайте данные банковской карты: номер карты, имя и фамилия владельца, срок действия, CVC код, пин-код карты;

- Не переводите денежные средства на незнакомые счета и карты;

- Не устанавливайте на свой телефон приложения по просьбе незнакомых людей, даже под предлогом технической поддержки.

Прокурор района И.В. Катыхин

Самые распространенные схемы мошенников в 2024 году

Подавляющее большинство россиян сталкивались в этом году с мошенничеством —

по разным опросам от 70 до 85%. За 9 месяцев ущерб от мошенников оценивается в 150 млрд рублей, а самих фактов стало на 25% больше, чем в прошлом году. Злоумышленники постоянно модернизируют старые схемы обмана.

Для обмана людей мошенники мимикрируют под сотрудников различных государственных ведомств — ЖКХ, поликлиник и других. Легенды у злоумышленников самые разные: от необходимости восстановить доступ к ресурсам до оказания технической поддержки.

Во всех случаях они предлагают потенциальной жертве перейти в WhatsApp (принадлежит компании МЕТА, которая признана в России экстремистской) для видеозвонка. После этого мошенники сообщают о некой технической проблеме и просят включить демонстрацию экрана. После того, как собеседник соглашается выполнить это действие, ему отправляют ссылку на приложение и просят его скачать. Злоумышленники выдают приложение за официальный ресурс ведомства, но на самом деле это вредоносный вирус SpyMax.

Установка псевдо-приложения полностью лишает человека контроля над смартфоном. В это же время на телефон приходит СМС с секретным кодом от входа в банковское приложение. Злоумышленники используют его для входа в онлайн-банк, после чего переводят на свои счета все доступные на счету средства либо оформляют от имени жертвы кредиты.

Вернуть контроль над смартфоном человек самостоятельно уже не может, а потому самый верный способ не оказаться в числе обманутых — не общаться с незнакомцами, не переходить по их ссылкам и не устанавливать сторонние программы.

Заместитель прокурора В.Н. Толстая