

за: нужно срочно на безопасный счет вывести ваши деньги. Но на самом деле такие понятия, как «специальный счет», «безопасный счет», это как раз те маркеры, которые говорят о мошеннической схеме.

Потерпевший под таким давлением начинает действовать по инструкции преступников. Приходит в банк, снимает все свои вклады, сбережения. Казалось бы: уж куда безопаснее – деньги в твоих руках. Но нет! Человек с наличными идет к банкомату и переводит деньги на подконтрольные мошенникам счета. А нередко его еще и уговаривают взять так называемый зеркальный кредит и опять-таки все деньги положить на «специальный безопасный счет».

? Что такое «зеркальный кредит»?

Это когда злоумышленник говорит потерпевшему: вашими данными завладели мошенники, и, чтобы они не смогли взять от вашего имени кредит в банке, вы должны взять его первым. Так сказать, чтобы упредить. А далее – по схеме: деньги переводятся на «безопасный счет».

Конечно, сейчас ведется колоссальная работа по взаимодействию МВД, Центрального банка, финансовых учреждений, операторов связи с целью противодействовать таким схемам. Ведется глобальная пропагандистская работа со стороны Главного управления и территориальных подразделений МВД. Мы доводим до граждан новые способы мошенничества, предупреждаем, разъясняем, как им действовать в случаях столкновения с ними.

Работаем с банками по упреждению, а также блокированию денежных средств, поступивших на подконтрольные мошенникам счета. Так, с 25 июля 2024 года вступили в законную силу Федеральные законы, которые позволяют МВД, Центробанку и банковским учреждениям обмениваться информацией о фактах правонарушений, операций, осуществляемых без согласия клиентов, и упреждать вывод средств с дропперских счетов. Препеденты уже есть. Счета блокируются, средства возвращаются потерпевшим.

Вопрос от читателя «ОГ»
Елены Витальевны
из Екатеринбурга:

? У меня на днях мошенники похитили мои «Госуслуги». Я обратилась в МФЦ, в полицию, в налоговую инспекцию. Везде очень быстро и оперативно приняли меры. Когда я стала проверять по инструкции из МФЦ, выяснилось, что на «Госуслугах» отображен IP-адрес тех, кто туда зашел. Вопрос: если я предоставлю этот адрес в полицию, это поможет как-то обезвредить мошенников?

– Да, конечно, эта информация нам поможет. Действительно, на «Госуслугах» фиксируется верификация, последние заходы в личный кабинет. Я так полагаю, что под каким-то предлогом вы передали информацию из СМС, и мошенники вошли в ваши «Госуслуги». Вы восстановили и уви-



МАКСИМ СМАГИН



ПАВЕЛ ВОРОЖИЛОВ

дели, с каких адресов в ваш личный кабинет заходили. Заявление вами подано в территориальное подразделение полиции. Состав преступления у этих злоумышленников уже есть: это неправомерный доступ к компьютерной информации. Вам необходимо предоставить данные по IP-адресам, и эту информацию мы, конечно же, проверим. Постараемся определить их принадлежность.

Вопрос «ОГ»:

? К вам обращаются, когда уже «ой». А есть смысл звонить в полицию и сообщать, что мне звонили мошенники, но у них ничего не вышло?

– К сожалению, эффект от таких обращений минимальный. В основном злоумышленники звонят с мессенджеров: через «Ватсап» или «Телеграм». Вычислить их по этим номерам практически невозможно, они виртуальные.

Стати, важно помнить: ни одна государственная структура обращаться к вам через мессенджер не будет.

Вопрос от читателя «ОГ»
Валентины Александровны
из Верхней Синячихи, 85 лет:

? Живу одна в частном доме. От соцпомощи по договору мне помогала семья из трех человек (называет фамилию. – Прим. «ОГ»). Я им доверяла. Услуги оплачивала. Мне родственники подарили девять лотерейных билетов «Мечталион». Я дала билеты проверить этой семье. После чего они пропали: и билеты, и люди. Обратилась к участковому, мне отказали в связи с недостатком улик.

– Валентина Александровна, я записал информацию. Давайте мы свяжемся с сотрудниками

полиции Верхней Синячихи. И уточним информацию по этому факту: есть там состав правонарушений, причинен ли ущерб. Разберемся.

Вопрос «ОГ»:

? Есть ли примеры удачного разрешения дела, когда человеку возвращали похищенные средства?

– Конечно. Мы же не только занимаемся профилактикой. Прежде всего мы – оперативное подразделение, которое занимается выявлением и раскрытием преступлений.

Есть реализации, когда мы задерживаем злоумышленников, содействовавших совершению преступлений. Большинство мошеннических действий идет с сопредельных государств – Украины, Польши, Грузии и других. Но есть лица, которые помогают им на террито-

рии нашей страны. Их задержания проходят регулярно.

В этом году была успешная большая реализация: взяли кол-центр, который действовал на территории Российской Федерации. Злоумышленники задержаны и содержатся в СИЗО, идет следствие.

? В Москве уже были случаи, когда мошенники пользовались технологией дипфейка: на видео подменялось лицо человека и голос. А как у нас?

– В Свердловской области зафиксированы случаи, когда поддельвался голос звонившего. Как правило, звонки идут через «Телеграм», звонят от имени бывшего руководителя или от вышестоящего действующего руководителя. Речь идет не о взломе аккаунта, а о подложном аккаунте, созданном от имени человека, с использованием его фотографии.

Но вы правы, технологии развиваются: пока у нас подделывали только голос, но ко всему надо быть готовым. Самым лучшим способом здесь будет положить трубку и перезвонить на обычный номер человека, а не на мессенджер. Это вас обезопасит.

Мошеннических схем много, и появляются все новые. Злоумышленники тоже не стоят на месте, следят за информационной повесткой. Сейчас, к примеру, в преддверии новогодних праздников, когда все покупают подарки, наступает время активности граждан при совершении покупок, мошенники также активизируются – создают фейковые аккаунты в соцсетях, маркетплейсах, фейковые сайты. Мошенники размещают объявления о продаже товаров с большими скидками, а на самом деле пытаются украсть ваши деньги или данные.

? Как противостоять этому?

– Прежде всего быть внимательными. Любой звонок или СМС с незнакомого номера изначально должны вызывать недоверие. Это первый маркер, чтобы задуматься. Второй маркер: любая беседа с мошенником рано или поздно упрется в деньги. Третий – огромные суммы: лжеброкеры предлагают под 1 000% доходности. Такого не бывает, бесплатный сыр – только в мышеловке.

Четвертый – у вас настойчиво пытаются выведать данные карты или персональные данные.

Последний и, пожалуй, главный маркер. Мошенники свою жертву постоянно подгоняют, эмоционально и психологически раздвигают: все нужно делать быстро, решения принимать немедленно. Не давая вам спокойно проанализировать услышанное.

В таких случаях нужно просто положить трубку и подумать, а что же, собственно, происходит?

Материал подготовлен при содействии пресс-службы ГУ МВД РФ по Свердловской области (В. Н. ГОРЕЛЫХ)