Главное – не бояться и разговор прекращать сразу

Органы МВД предотвращают действия мошенников ежедневно

В 2024 году чересчур доверчивые свердловчане отдали мошенникам в общей сложности 4,5 миллиарда рублей. За первые два месяца 2025 года – еще 600 миллионов. Злоумышленники придумывают все новые схемы для выманивания «наших кровных», используя для этого самые изощренные психологические уловки и современные технологии. Правоохранительные органы нашего региона держат вопрос на особом контроле. В Главном управлении МВД РФ по Свердловской области противодействием преступлениям в киберсфере занимается специальное подразделение – Управление по борьбе с противоправным использованием информационно-коммуникационных технологий. Заместитель начальника отдела управления подполковник полиции Алексей ШАКЛЕИН в ходе прямой линии в редакции «Областной газеты» ответил на вопросы читателей «ОГ» и рассказал, как понять, что вам звонят телефонные аферисты, на какие новые схемы интернет-мошенничества уральцы попадаются чаще всего и как защитить свои сбережения.

ПОЛИНА ЗИНОВЬЕВА

Вопрос «ОГ»:

– Алексей Валерьевич, как меняется статистика по интернет-мошенничеству в Свердловской области? Количество пострадавших идет на спад либо наоборот?

– К сожалению, граждане продолжают терять свои деньги. За 12 месяцев 2024 года мы зафиксировали 7 500 преступлений в сфере телефонного и интернет-мошенничества. Жители Свердловской области перевели аферистам 4,5 миллиарда рублей. И это больше, чем в 2023 году. На начало этого года картина такая же. Люди продолжают терять свои деньги. За январь-февраль 2025 года ущерб составил более 600 миллионов рублей, показатели прошлого года – 520 миллионов за первые два месяца.

– Появляются какие-то новые схемы телефонного мошенничества? Или люди попадаются на одно и то же?

– Я бы не сказал, что они принципиально новые. Злоумышленники могут использовать любой предлог: замена ключей от домофона, смена или продление тарифных планов, улучшение качества связи или предоставляемого Интернета на 5G, необходимость замены медицинского полиса, обновление счетчиков, могут представиться сотрудниками Энергосбыта или другой подобной организации, представляются сотрудниками службы доставки, сообщают о поступлении какой-либо посылки, для доставки которой необходимо продиктовать код из СМС-сообщения. Могут даже просто позвонить и сказать: «Вас взломали, у вас отсутствует доступ к «Госуслугам». Человек, который не проверяет информацию, уже начинает верить. И, к сожалению, таких схем очень много, они меняются. Под влияние мошенников попадают не только пенсионеры, но и молодежь. Когда люди слышат, что их деньги прямо сейчас переводят на территорию другого государства, что на них берут большие кредиты, то срабатывает эффект внезапности, испуг. В это начинают верить даже вполне здравомыслящие люди. Под влияние телефонных мошенников также попадает все больше школьников. Важно помнить: главная цель всех подобных звонков – завладеть персональными данными человека.

– Есть ли какие-то стоп-слова в телефонном разговоре, после которых человек точно должен понять, что говорит с мошенниками, и положить трубку?

– «На вас оформлен кредит», «необходимо сберечь деньги путем перевода их на безопасный счет», «необходимо задекларировать ваши денежные средства, которые у вас находятся», «произошла утечка данных». После этих фраз все должно стать понятно. А также требование каких-то персональных данных, любые коды доступа. Не надо никому диктовать цифры из СМС, которые могут выманивать под любым предлогом – смены тарифного плана, замены счетчиков и так далее. Таким образом злоумышленники отправляют жертве СМС о смене пароля на «Госуслугах». Это их первая цель – чтобы человек продиктовал эти четыре цифры. Многие из тех, кто отдал свои деньги мошенникам, оказались заложниками именно такой ситуации.

– Если мошенники уже получили доступ к личному кабинету на «Госуслугах», сменили пароль и скачали оттуда все данные, что делать?

– Не теряя времени, принять меры к восстановлению доступа. Это можно сделать несколькими способами. Если злоумышленники еще не успели сменить привязанный номер, то сделать повторную перерегистрацию. Если доступ по номеру телефона уже потерян, самый надежный вариант – как можно скорее обратиться в ближайшее отделение МФЦ и там восстановить доступ. После этого проверить, были ли оформлены кредиты – это можно сделать через бюро кредитных историй, также через «Госуслуги». Там же, в разделе «Безопасность», есть информация об осуществленных действиях: кто и что делал в вашем личном кабинете, куда обращался, какую информацию запрашивал.

Вопрос от *Риммы Сергеевны* из Асбеста:

– Могут ли мошенники снять деньги со вклада в Сбербанке, если им известна дата открытия вклада, адрес филиала, где он открыт, какая на этом вкладе сейчас лежит сумма, а также известен СНИЛС вкладчика?

– Все снятия денежных средств могут производиться только в присутствии собственника счета. Если он будет отсутствовать в банке, то без него деньги никто не выдаст. Важно, чтобы человек сам не осуществлял никаких переводов под влиянием злоумышленников, которые требуют перевести деньги на якобы безопасный счет. И здесь надо знать – никаких безопасных счетов не существует. Если человек лично переведет свои сбережения на другой счет, который ему не принадлежит, то мошенники смогут их снять. Также надо сразу же обращаться в полицию, если по телефону поступают СМС о внезапных кредитах или снятии средств с вашего счета.

– Моей соседке-пенсионерке звонили якобы из Уралтелекома и сказали, что пересматривают плановый тариф по домашнему телефону, что надо обновить договор, и попросили для этого сообщить номер СНИЛСа. Она его назвала. На следующий день ей позвонил некий «капитан ФСБ», назвал адрес, где его можно найти: Екатеринбург, ул. Вайнера, 4, второй этаж, номер кабинета. И сказал, что они поймали уроженку Украины, которая хотела совершить диверсию, и что у нее изъяли 700 тысяч рублей, которые якобы были переведены по СНИЛСу моей соседки. И что за это ей грозит статья 350-я, и ее пригласят по повестке в Екатеринбург.

– Это классическая схема. Сначала мошенники под любым предлогом получают личные данные человека. Потом представляются сотрудниками правоохранительных органов и запугивают. Цель – подвести потенциальную жертву к тому, чтобы она сама перевела свои деньги на «дополнительный или безопасный счет» или отдала наличные курьеру. Главное сейчас: вовремя сориентироваться и не совершать этих действий. Если же такие звонки будут повторяться, то сразу сообщить об этом родственникам и знакомым.

А общение с представителями власти необходимо вести только глаза в глаза, не по телефону. В нужных случаях в правоохранительные органы приглашают повесткой.

Вопрос «ОГ»:

– Допустим, мошенники получили доступ к личному кабинету на «Госуслугах», и у них есть все данные человека – паспорта, СНИЛСа, ИНН и другие. Что они могут сделать с этой информацией?

– Использовать для психологического давления. Цель, как я уже сказал выше, сводится к одному – вынудить жертву перевести свои деньги на «безопасный счет» либо отдать их в руки курьеру наличными. Для этого мошенникам нужна конфиденциальная информация с «Госуслуг». Человек пугается, когда понимает, что злоумышленники имеют доступ к его личным данным. Но сделать с ними они ничего не могут. Самое страшное, что может произойти, – на человека могут оформить кредит в микрокредитной организации, если он вовремя не спохватится. Однако сам сайт «Госуслуги» не является кредитно-финансовой организацией, поэтому непосредственно через него оформить на человека кредит невозможно. Мошенникам надо будет дистанционно обращаться в банк либо в микрокредитную организацию. Таких случаев в Свердловской области мы не фиксировали уже давно. Но чтобы исключить такую возможность, надо просто выключить панику и обратиться в ближайшее отделение МФЦ, восстановить доступ к своему личному кабинету на «Госуслугах». И, конечно, обратиться в полицию, чтобы зафиксировать факт взлома.