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 всё 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, смену 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 всё 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 снятиях 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.

Вопрос от Светланы из Екатеринбурга:

– Я живу в Железнодорожном районе Екатеринбурга. Мне позвонили из Ростелекома и

ФСБ. Сказали, что нужно перевести все деньги на какой-то безопасный счет. Я не успела этого делать. Но мне продолжают поступать звонки от этих людей. Они звонят на городской телефон, знают мою фамилию, адрес, все данные. Я пенсионерка, мне страшно. Что делать?

– Просто не продолжать разговор. Положить трубку и всё. Это мошенники, которые пытаются по телефону выманить ваши денежные средства. Никаких безопасных счетов не существует. Ваши деньги должны находиться либо у вас, либо на вашем банковском счете. Никаких доступов, никаких паролей никому сообщать нельзя. При возникновении каких-то непонятных вопросов сразу же обращайтесь в полицию. Сотрудники полиции всегда общаются лично и обязаны показать свои служебные документы. И эту информацию вы можете проверить в полиции.

ПАВЕЛ ВОРОЖЦОВ

Вопрос «ОГ»:

– Получается, что звонят не только по мобильным телефонам, но и по обычным городским номерам?

– Да, звонят и на городские номера. В данном случае могут сообщить, что стационарный телефон зарегистрирован на другого человека и могут совершаться мошеннические действия, а также представляются сотрудниками Ростелекома и сообщают, что якобы по договору абонентского номера истекает срок действия и для его продления необходимо назвать паспортные данные. Да, еще один стоп-сигнал – когда говорят, что нельзя разглашать информацию о содержании разговора даже родным и близким. И при этом угрожают уголовной или административной ответственностью. Могут сказать, например, что вы или ваши родственники переводили на запрещенный счет денежные средства, но в полицию ни в коем случае обращаться нельзя. Просто не надо продолжать этот разговор, а сразу сообщить о нем родственникам и знакомым. Это поможет не попасть под влияние злоумышленников, которые звонят на городские номера под теми же самыми предлогами – обновления тарифа, счетчика и так далее.

– Кроме пенсионеров, кто еще находится в зоне риска?

– В последнее время телефонные мошенники усилили давление на детей. Один из последних случаев был в конце марта. Ученица девятого класса отдала мошенникам почти миллион рублей. Перевела все деньги с родительских карт и еще оформила на родителей кредит, используя их личные телефоны. Девочке позвонили якобы от оператора сотовой связи, сказали, что нужно обновить данные, для чего необходимо сообщить код, который придет на ее телефон. После этого школьнице позвонили и сказали, что из-за того, что она отправила этот код, взломали портал «Госуслуги» и скачали все данные о ее родителях. Потом на ребенка начали давить, ей поступил звонок уже в «Телеграме», якобы от сотрудников Росфинмониторинга. Они запугивали ее тем, что посадят родителей.

– Ребенку звонит посторонний и говорит «твоих родителей посадят»?

– Когда ребенку угрожают, говорят, что аккаунты родителей взломали и все деньги будут переведены на Украину, родители будут наказаны и так далее, он, конечно, пугается. Особенно если звонят люди в форме по видеосвязи. Но это только один из способов. Могут позвонить или написать и от лица преподавателя, под предлогом того, что нужно внести коррективы в электронный дневник. Точно так же запрашивают код доступа. И далее по той же схеме – методами психологического воздействия добиваются, чтобы ребенок под любым предлогом получил телефон своих родителей. И всё. Как только он завладел телефоном мамы или папы – выполняет все указанные действия на получение кредита, на перевод денежных средств. Вплоть до того, что были случаи, что дети уничтожали эти телефоны после выполнения указаний злоумышленников. Мы работаем совместно с министерством образования, активно проводим разъяснительные беседы в школах, чтобы дети понимали всю серьезность происходящего.

Вопрос от Елены Александровны из Полевского:

– Скажите, пожалуйста, могут ли телефонные мошенники переписать на себя квартиру?

– Это делается только в присутствии собственника жилья. Выселить из квартиры вас тоже никто не может. Для этого нужно судебное решение. Однако мы фиксировали, когда квартиры продавали по сильно заниженной цене. Это первый тревожный сигнал. Обо всех таких подозрительных операциях сотрудники Регистрационной палаты должны сообщать в правоохранительные органы. Точно так же продают и машины, чтобы потом передать все деньги мошенникам. Их жертв видно сразу: человек нервничает, всегда на телефоне, проясняет у кого-то какие-то моменты, настаивает на срочности сделки или банковской операции. В банке, как правило, он не может внятно объяснить, почему ему так срочно понадобились деньги. Такие сомнительные операции мы отслеживаем вместе с кредитными организациями. С человеком может быть проведена профилактическая беседа. Были случаи, когда мы вовремя останавливали операции по передаче жилья по неправомерным фактам.

Вопрос от Владимира Емельяновича из Невьянска:

– Я купил сим-карту в 2023 году. Через какое-то время она перестала работать. Я позвонил оператору сотовой связи, и мне ответили: карта зарегистрирована на юридическое лицо. Как так, она же моя? Подозреваю здесь какое-то мошенничество.

– Возможно, несколько месяцев вы просто не пользовались этой сим-картой. Если это так, то через какое-то время карта снова стала собственностью оператора мобильной связи и была передана другому абоненту, вам надо уточнить у него этот вопрос. Признаков мошеннических действий, на первый взгляд, тут нет.

Вопрос от Михаила из Екатеринбурга:

– Как обезопасить себя от использования дипфейков? Если мошенники используют голос, поддельное изображение лица?

– Мы пока таких случаев не фиксировали. Но исключать ничего нельзя. Всегда перепроверять информацию, перезванивать на реальный номер телефона, а не тот, который высветился во время звонка. Пока мошенники активно используют подменные номера либо фото в мессенджерах. Создают поддельные профили и пишут якобы от лица начальника или коллеги. Кстати, сотрудники правоохранительных органов никогда не звонят по мессенджерам. И не проводят никаких осмотров жилых помещений с использованием видеосвязи. Были случаи, когда люди начинали всё снимать на видео, соответственно, мошенники видели, что в квартире есть: сейфы, ценности и так далее.

– Говорят, что сейчас мошенники вешают на подъезды объявления с куар-кодами. Проходишь по коду, а там ссылка с вредоносной программой.

– Пока не припомню таких ситуаций. Но вот мошеннические объявления по обновлению и установке домофонов уже были. Главное, что нужно помнить, – не устанавливать на свой телефон никакие подозрительные приложения, которые вам скидывают под любым предлогом. Например, могут позвонить якобы от оператора связи и сказать, что надо обновить ПО, скидывают ссылку. Жертва проходит по этой ссылке, после чего телефон выключается. И в течение десяти минут мошенники осуществляют все возможные действия со счетами. В зоне риска в первую очередь владельцы телефонов на платформе «андроид».

Вопрос «ОГ»:

– Вообще, удается ли возвращать людям их деньги?

– Всё зависит от того, насколько быстро человек осознал факт мошенничества и обратился в полицию. Если деньги были заблокированы банком как подозрительная операция, и гражданин, находящийся под влиянием мошенников, не подтвердил данную операцию, то еще есть возможность их восстановить. Но если промедлить, и сбережения уже ушли на заграничные счета, в криптовалюту, то оттуда их достать уже невозможно. Человек может понять, что он сделал что-то не то и после того, как передал наличные кому-то на руки. Такую схему мошенники тоже используют.

– Насколько известно, злоумышленники могут даже использовать людей вслепую, чтобы они передавали им деньги?

– Да, такими курьерами поневоле могут стать, например, таксисты. Мошенники заказывают такси и просят забрать посылку. А бывает, что в роли курьера используют и самого потерпевшего, которого обманули до этого. Говорят, что у него есть шанс вернуть деньги, для этого надо сделать то-то и то-то. Часто курьеров поневоле используют втемную.

Человек идет и по указанию злоумышленников получает какую-то посылку и перевозит. Были случаи, что деньги забирала даже пенсионерка у пенсионерки. Первую уже обманули, вторая – потенциальная жертва. Был случай, когда пенсионерка просто завернула в простыню почти миллион рублей, положила в коробку и отдала. Потом мы с ней беседуем, а она говорит: «Как же так, я же знала про всё. Ко мне даже участковый приходил, у меня памятка есть про мошенников».

– В какой момент у человека выключается внутренний критик, и он начинает выполнять указания мошенников?

– Я думаю, это страх потерять деньги. Человеку создают иллюзию, что он прямо сейчас всё потеряет. Эта иллюзия возникает, когда он понимает, что его персональные данные в руках злоумышленников, он боится. Также людей пугают взаимодействием с заграничными спецслужбами. Либо говорят, что на них уже взяли кредит и там сумма какая-то заоблачная. Человек в шоке, не понимает, как он будет расплачиваться. И тут ему говорят, что необходимо взять встречный кредит, это исчерпает лимит кредитной истории, и тот, первый кредит, не выдадут. У нас был случай, когда с человека таким образом «сняли» до 15 миллионов рублей.

– Сейчас на Госуслугах можно установить самозапрет на кредиты, это решает проблему?

– Это удобная функция. При ее активации кредит дистанционно оформить на человека точно не получится. Снять самозапрет человек может только лично, в банке. При этом банки сегодня используют разные схемы противодействия мошенникам. Например, имеют право применить «период охлаждения» – приостановить выдачу кредита на несколько дней. Ну, и за оформление кредита на человека с использованием его личных данных, но без его участия, существует уголовная ответственность.

– За 2024 год свердловчане перевели аферистам 4,5 миллиарда рублей. А сколько преступлений вы предотвратили?

– Да, порядка 9,5 тысячи человек пострадали как от действий телефонных мошенников, так и от киберпреступлений, связанных с кражами с использованием вредоносного ПО. Что касается положительной статистики, то мы ведем счет уже даже не годами и не месяцами. Каждую неделю нам удается остановить от перевода денег мошенникам 10-15 человек. Информация, на которую надо реагировать срочно и принимать меры, поступает ежедневно.

Материал подготовили Алёна ПЕРФИЛЬЕВА, Михаил БАТУРИН при содействии пресс-службы Свердловского главка МВД (В.Н. Горелых)