Маскируются даже под нотариусов

Статистика. За 5 месяцев этого года в Челябинской области ущерб от преступлений, совершённых с использованием IT-технологий, уже превысил один миллиард рублей

Главное управление МВД России по Челябинской области продолжает информировать южноуральцев как о проверенных, так и о новых способах мошенничеств. В последнее время стали набирать обороты новые схемы обмана. Вот наиболее популярные из них.



Ваш отпуск под угрозой

В разгар летнего сезона отпусков злоумышленники предлагают липовые туры, бронирование билетов и жилья якобы по выгодным ценам. Всегда внимательно проверяйте правильность написания названия сайта и пользуйтесь услугами проверенных компаний. Если незнакомцы просят внести стопроцентную предоплату за тур, аренду жилья и так далее – будьте крайне осторожны! Изучите отзывы, потребуйте выставить счёт на оплату, обязательно проверьте реквизиты. Если фирме нечего скрывать – счёт вам выставят безоговорочно.

Звонок от нотариуса

Гражданину поступает звонок, неизвестный представляется нотариусом и сообщают, что от его имени подписана доверенность, которая будет передана на портал госуслуг. Обеспокоенный человек сообщает, что никаких доверенностей он никому не выдавал. Тогда лженотариус диктует номер телефона, на который необходимо позвонить и сообщить данную информацию. Пострадавший верит и, позвонив по указанному номеру телефона, продолжает общение с аферистами, которые представляются сотрудниками правоохранительных органов и финансового мониторинга. Телефонные мошенники сообщают, что сбережения гражданина пытаются похитить, и нужно срочно перевести их на «безопасную банковскую ячейку». Введённый в заблуждение пострадавший, выполняет указания злоумышленников, вследствие чего теряет собственные и кредитные денежные средства.

На связи – начальник

Всё чаще злоумышленники звонят и пишут в мессенджерах пользователям под видом их руководителей. Для этого они создают реалистичные профили директоров и начальников. Аферисты сообщают своим «подчинённым» о каких-либо проблемах и о том, что с сотрудником свяжется представитель правоохранительных органов.

Затем в разговоре мошенники убеждают гражданина в том, что его деньги хотят украсть, перевести на счета террористических организаций или оформить на его имя кредит. Предлогов может быть много, но итог один – вывести деньги на «безопасный счёт».

Перерасчёт пенсии

В процессе телефонного разговора мошенники сообщают потенциальной жертве о неучтённом стаже, выявленном в ходе некой проверки, и предлагают оформить официальное заявление на перерасчёт пенсии в сторону её увеличения. В случае согласия с такой процедурой злоумышленники предлагают подать заявление в телефонном режиме. Для идентификации просят продиктовать поступивший код из смс.

Однако если продиктовать данный код, то мошенники получат доступ либо к порталу госуслуги, либо к мобильному банку, что приведёт к компрометации учётной записи на госуслугах, или к попытке перевода мошенниками денежных средств с банковского счёта жертвы.

На заметку.

Как защититься от мошенников

Схема действий злоумышленников всегда одинакова: обманным путём они вынуждают человека самостоятельно сообщить данные для входа в личный кабинет банковского приложения, мобильного оператора, госуслуг и других полезных ресурсов. Чтобы звучать убедительно и воздействовать на эмоциональном уровне, они затрагивают самые актуальные темы.

Мошенники могут представляться сотрудниками социальных служб, медиками, правоохранителями, обещать выигрыш в лотерею или увеличение пенсии, выплаты от государства или выгодный кредит. Такие методы получения доступа к данным называются социальной инженерией.

Как защитить себя от социальной инженерии?

– Будьте бдительны во время телефонных разговоров. Не торопитесь. Если диалог кажется вам подозрительным, прервите звонок. Лучше перезвоните в банк или организацию по номерам, указанным на официальном сайте. Помните, что представители госуслуг и служб безопасности банков никогда не звонят первыми.

– Обратите внимание на способ связи. Для звонков мошенники часто используют мессенджеры. Настоящие представители ведомств и органов власти никогда не будут звонить через WhatsApp или Telegram.

– Не сообщайте никому логины и пароли от личных кабинетов. Внимательно читайте назначение смс. Например, смс-коды госуслуг могут потребоваться только лично вам и никому больше. Не говорите никому ответ на контрольный вопрос, который вы используете для восстановления доступа.

– Внимательно следите за актуальностью номера, к которому привязан аккаунт.

– Используйте сложные пароли, периодически меняйте их. Если сервис позволяет, подключите двухфакторную аутентификацию. На госуслугах в качестве второго фактора можно выбрать смс, одноразовый ТОТР-код и вход по биометрии.



– Внимательно изучайте адрес страницы, на которой вводятся данные, чтобы не попасть на фишинговый ресурс. Единственно верный адрес госуслуг – gosuslugi.ru.

Госуслуги надёжно защищены, и злоумышленник может получить доступ к аккаунту только в том случае, если пользователь сам передаст всю необходимую для входа информацию. На портале есть все инструменты для того, чтобы обезопасить аккаунт. Но и самому нужно бережно относиться к своим данным.

Запомните

Из Соцфонда не звонят!

Пенсионерка из Озёрска лишилась денег, поверив в звонок из Социального фонда. Мошенники всё чаще стали обманывать пожилых людей, предлагая им под различными предлогами записаться на приём в Социальный фонд. Так, пенсионерке из Озёрска позвонил неизвестный, представился работником Пенсионного фонда (так раньше назывался Социальный фонд). Мужчина убедил её оформить талон через портал госуслуг, чтобы записаться на приём в организацию.

Доверчивая озерчанка предоставила незнакомцу доступ к своему телефону, а также продиктовала коды из смс. Собеседник, получив нужную информацию, похитил с её счёта 140 тысяч рублей. Следственным отделом г. Озерск возбуждено уголовное дело по статье 158 УК РФ – «Кража».

Ещё одна схема отъёма денег

Злоумышленники стали активно использовать просрочку по ипотеке как предлог для запугивания и хищения денег. Вот как действуют мошенники:

1. Представляются по телефону сотрудниками банка, заверяют о просрочке по ипотеке и предлагают срочное решение.

2. Просят сообщить данные СНИЛС и коды из смс. Так они получают доступ в ваш личный кабинет госуслуг и далее – в онлайн-банк.

Мошенники специально сбивают с толку доверчивых граждан, уточняя, что код – это альтернатива персональным данным, запрашивать которые нельзя. Однако помните, что данные из смс тоже относятся к секретным!

3. На последнем этапе с вашего счёта исчезают все деньги или на ваше имя оформляют кредит.

Обман бизнесменов и самозанятых

От имени сотрудников налоговой аферисты звонят своей потенциальной жертве и предлагают сверить налоговые платежи под предлогом якобы найденных неучтённых расчетов.

Для этого предприниматель должен ознакомиться с присланным ему документом в приложении «Мой налог» или в личном кабинете на сайте ФНС. Естественно, никаких документов бизнесмен не находит, а злоумышленники сообщают ему, что произошёл сбой в синхронизации ресурса налоговой службы и портала госуслуг. Чтобы восстановить работу, требуется только сообщить код из смс. Если налогоплательщик попался на удочку преступников и сообщил нужную им информацию, они получают доступ к личному кабинету потерпевшего с возможностью проведения различных финансовых операций от его имени.