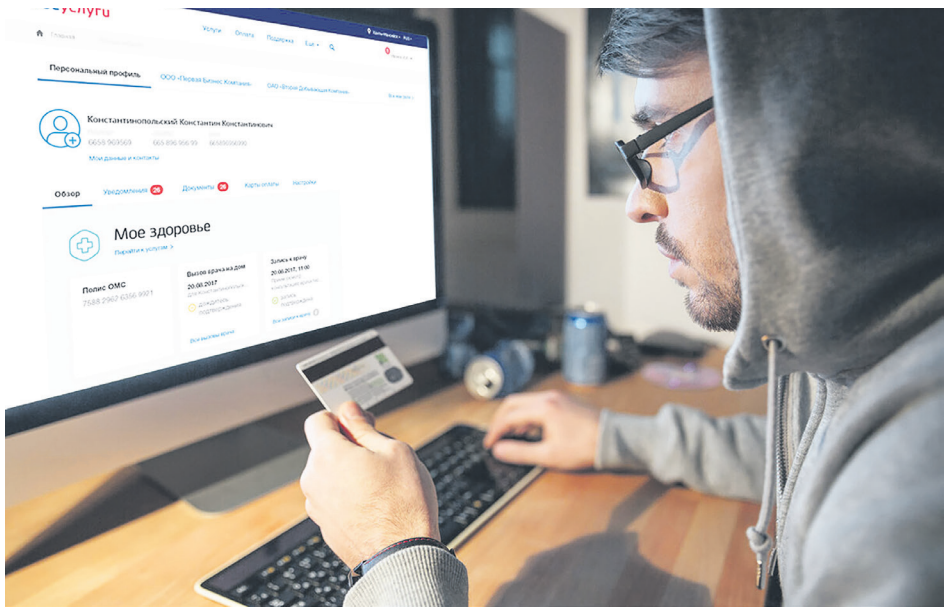
Не сообщайте коды

Тенденция. Разномастные мошенники всё чаще «орудуют» на портале госуслуг

ВИКТОРИЯ **КАЗАКОВА**

Оно и понятно, ведь этот сайт содержит почти всю информацию о зарегистрированных на нём: от номера паспорта до банковских карт и счетов.



Удобно, но опасно

Безусловно, портал существенно облегчает жизнь и экономит наше время. Не выходя из дома, можно оплатить услуги, записаться к врачу, подать заявления в различные инстанции... Однако всё это теперь ещё и небезопасно, потому что до сервиса добрались мошенники.

Как они получают доступ к чужому личному кабинету на госуслугах, и что делать, если это произошло?

Как всегда, всё начинается с телефонного звонка. Приветливые незнакомцы представляются сотрудниками портала, называют свои и ваши фамилию, имя, отчество, затем сообщают, что ваш личный кабинет атакуют преступники. Они якобы пытаются изменить номер телефона, который у вас привязан к госуслугам, и им нужно срочно помешать.

Раздобыть ваш номер телефона и другие сведения не составляет труда. Во-первых, некоторые из них есть в открытом доступе: те же самые номера телефонов часто привязаны к соцсетям. Во-вторых, ряд компаний, увы, не следят за безопасностью данных, и мошенники, используя уязвимость, воруют информацию. Так сведения могут утечь, например, у различных служб доставки, мобильных банков, сервисов лояльности в магазинах.

Будьте бдительны при авторизации на госуслугах. Именно на номере телефона, который привязан к личному кабинету, держится новая мошенническая схема. Казалось бы, это уже заезженный сценарий телефонных аферистов, и пора положить трубку. Но несколько нюансов заставляют проникнуться доверием к собеседнику. Так, например, если потерять доступ к личному кабинету и пытаться его восстановить, на телефон придёт смс с кодом подтверждения или же позвонит представитель службы безопасности портала. Обратите внимание: мошенники звонят с этого же номера! А чтобы восстановить доступ к личному кабинету, нужно ввести номер телефона, на который придёт код.

Действуйте быстро

Если напрямую сказать собеседнику, что вы не верите ему, вас будут стараться убедить в обратном. Незнакомец безошибочно назовёт все данные о вас, которые есть на портале и которые нельзя найти в свободном доступе: номер паспорта, ИНН, СНИЛС и даже историю ваших действий в личном кабинете вплоть до оплаты штрафов.

Лжесотрудник госуслуг очень грамотно втирается в доверие: говорит убедительно и, видя ваши сомнения, предлагает задать любые интересующие вас вопросы, на которые уверенно отвечает. А дальше жертву ждёт такой сценарий: собеседник обещает помочь и просит назвать код, который тут же приходит на телефон. Получив заветные цифры, мошенники завладевают вашим личным кабинетом и всей информацией, которая там имеется. Это позволит им, например, похитить электронную цифровую подпись или оформить ИП на ваше имя. Особо предприимчивые могут и вовсе продать ваши данные третьим лицам, получить доступ к мобильному банку карты, привязанной к госуслугам и даже переоформить имущество на себя.

Что делать, если вы всё-таки стали жертвой мошенника? Необходимо действовать максимально быстро, пока вашими данными не успели воспользоваться. Писать в техподдержку при этом не стоит, потому что сотрудники отвечают не сразу.

Эффективнее будет сразу позвонить в банки и заблокировать все карты, которыми вы когда-либо оплачивали услуги, штрафы, госпошлины, налоги на портале. Обратитесь в МВД с заявлением о мошенничестве.

– Данный вид мошенничества получает в последнее время всё большее распространение, – сообщили в пресс-службе межмуниципального отдела МВД России «Кыштымский». – Полиция настоятельно призывает проявлять максимальную осторожность при общении с незнакомцами. Внимательно относитесь к информации, которую вы получаете в смс. При получении кодов в сообщении всегда есть предостережение о том, что его нельзя сообщать никому, не игнорируйте это предупреждение! Только за последние две недели в Кыштыме зарегистрировано шесть фактов, когда мошенники пытались получить доступ в личные кабинеты жителей города. Будьте крайне внимательны! Прерывайте любые контакты с незнакомыми людьми.

Сомнительные инвестиции

В Верхнем Уфалее 44-летний рабочий одного из предприятий поверил в возможность получения дохода с помощью инвестирования. Неизвестные рассказали о преимуществах такого заработка и дали подробные инструкции для дальнейшей работы. Под руководством мошенников он переводил деньги и в общей сложности «выгодно» вложил в инвестиции 390 тысяч рублей. Когда потерпевший попытался получить деньги обратно и не смог этого сделать, он понял, что столкнулся с мошенниками и обратился в полицию.

А в Карталах 40-летняя потерпевшая рассказала, что увлеклась инвестированием и вложила 459 тысяч рублей. Схема обмана оказалась такой же. После того, как женщина попыталась получить свои денежные средства обратно, но сделать это ей не удалось, она поняла, что стала жертвой мошенников.

В Сосновском районе мошенники обманули 64-летнюю пенсионерку. Она вложила в инвестиции популярной промышленной компании более одного миллиона рублей! Сначала перевела на счёт более 400 тысяч личных сбережений, а затем, решив получить бОльшую прибыль, оформила несколько микрозаймов на сумму около 600 тысяч рублей. Естественно, получение прибыли оказалось невозможным.

На лайках не разбогатела

В полицию Магнитогорска обратилась 34-летняя местная жительница, ставшая жертвой мошенников. Она увидела в мессенджере объявление о подработке, которая заключалась в накручивании «лайков» и написании положительных отзывов на сайтах туристических агентств. «Кураторы» предложили женщине совершать фиктивные покупки, чтобы увеличить рейтинг агентства, обещая высокую прибыль. Согласившись, она приобрела путёвки на общую сумму более 290 тысяч рублей.

Но когда решила вернуть путёвки и получить обещанные деньги, «работодатели» исчезли. Женщина поняла, что её обманули, и обратилась в полицию.

Сотрудники полиции предупреждают жителей региона о необходимости проявлять бдительность при поступлении заманчивых предложений о быстром заработке. Необходимо проверять информацию о работодателе и предлагаемых условиях работы, не пересылать свои личные данные, тем более касающиеся банковских карт и счетов, неизвестным лицам и не переводить денег, даже в случае обещания их возврата или приумножения. Следует помнить, что честные работодатели никогда и ни под какими предлогами не требуют денег со своих сотрудников.

Случай

Обманчивая реклама

АНАСТАСИЯ **ЛАТЫПОВА**

Житель Кыштыма потерял более 600 тысяч рублей, поверив случайной рекламе.

В кыштымскую полицию обратился 50-летний местный житель с заявлением по факту мошенничества. Он рассказал полицейским, что во время игры на смартфоне ему высветилась реклама некой платформы, где за регистрацию можно получить 25 тысяч рублей. Мужчина перешёл по ссылке и указал номер своей банковской карты, а также персональные данные.

Спустя время кыштымцу позвонила незнакомка и рассказала о возможности удалённого заработка. Наш земляк решил заработать лёгкие деньги и внес девять тысяч рублей на счёт, который ему сообщила неизвестная дама. После перевода на онлайн-платформе высветился баланс, где была указана сумма, переведённая кыштымцем.

Мужчина неоднократно проверял свой «счёт» на указанной платформе и видел, что сумма его дохода постоянно увеличивается. Тогда он перевёл несколькими операциями еще 80 тысяч рублей. «Прибыль» продолжала увеличиваться. Мнимые брокеры стали убеждать азартного мужчину пополнить счёт на более крупную сумму. Но личные сбережения кыштымца закончились, тогда его убедили оформить кредит и также перевести полученные денежные средства на «брокерский» счёт. Мужчина выполнил все указания.

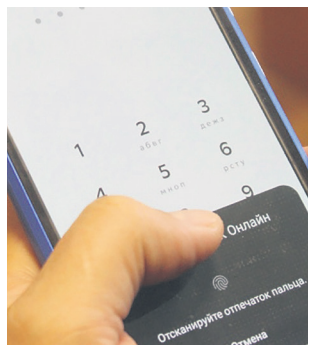
Когда житель Кыштыма захотел вывести денежные средства, ему сообщили о неполадке в системе. Родственники заявителя случайно услышали его телефонный разговор с мошенниками и объяснили игроку, что он имеет дело с проходимцами. Только после чего мужчина обратился в полицию.

Сумма ущерба составила 660 тысяч рублей. Возбуждено уголовное дело по статье 159 УК РФ – «Мошенничество».

Полицейские в очередной раз напоминают: не доверяйте различным предложениям об инвестициях, полученным от неизвестных источников, даже если они прикрываются названиями крупных банков, крупных компаний или иных финансовых организаций. Легальный способ инвестирования возможен только на официальных сайтах банков, при этом даже он не обещает гарантированного получения прибыли.

Мошенники устраивают СМС-атаки

Сотрудники киберполиции предупреждают южноуральцев о возможных СМС-атаках на мобильных пользователей. Перед проведением атак мошенники используют технику СМС-бомбинга. Это вид кибератаки, при которой преступники массово отправляют сообщения на мобильный номер конкретного человека.



На телефон жертвы поступает огромное количество сообщений якобы от государственных структур, банковских учреждений, микрофинансовых организаций, онлайн-магазинов и других всевозможных онлайн-сервисов.

В самих сообщениях отображаются различные коды, а также ссылки для перехода на вредоносные и фишинговые сайты. В данном случае делается расчет на панику жертвы, которая способна ответить на любое sms-сообщение.

После такой атаки на телефонный номер человека поступают звонки якобы от «представителей его мобильного оператора», которые заявляют о том, что сейчас техническая поддержка наблюдает массовую СМС-атаку, в связи с чем необходимо её прекратить, для чего просят подтвердить персональные данные и указать код из sms-сообщения.

Никогда не сообщайте незнакомцам поступающие на ваш телефон СМС-коды, а также персональные данные, так как это могут быть коды доступа к личным кабинетам на портале госуслуг, мобильному приложению банка и другим персональным данным.

В такой ситуации следует взять себя в руки и не отвечать на входящие СМС-сообщения. Помимо блокировки, можно также связаться с мобильным оператором и составить заявление на запрет СМС-рассылки от отправителей.

Также киберполицейские рекомендуют игнорировать сообщения и звонки от людей и организаций, предлагающих помощь в отражении атаки. Это тоже могут оказаться мошенники. Атака, как правило, длится всего несколько минут и закончится сама по себе, никаких действий предпринимать не стоит.