Приложение

Информация
о наиболее распространённых схемах взлома аккаунта портала «Госуслуги» и рекомендациях, как не допустить несанкционированный доступ к личному кабинету портала «Госуслуги»

Оперативная обстановка, связанная с совершением преступлений в сфере информационно-телекоммуникационных технологий, в регионе остаётся напряжённой.

В текущем году как в России, так и в Магаданской области, наряду с мошенничествами и кражами, в результате которых с банковских счетов граждан похищаются денежные средства, одним из наиболее распространенных видов IT-преступлений стал взлом личного кабинета пользователей портала «Госуслуги»).

Согласно информации УМВД России по Магаданской области только 9 месяцев 2024 года в сравнении с прошлым годом число таких противоправных деяний возросло в два раза (81 против 41).

В данном случае противоправные деяния квалифицируются как «неправомерный доступ к компьютерной информации», уголовная ответственность за которые предусмотрена статьёй 272 Уголовного кодекса Российской Федерации.

В дальнейшем завладение персональными данными с портала «Госуслуги» позволяет преступникам, используя краденный профиль:

- оформлять на чужое имя кредиты и микрозаймы;

- получить чужой налоговый вычет;

- оформлять на другого человека сим-карты сотовых операторов;

- обмануть вас или ваших близких: зная информацию о вас, они могут притвориться вами или сотрудником банка, чтобы выманить деньги у вас или ваших родных.

Кроме того, персональные данные (паспортные данные, сведения о собственности, кредитная история и прочая информация) могут быть проданы в так называемом даркнете и в дальнейшем использоваться в более сложных различных преступных схемах. К мошеннику будет больше доверия, если

он предоставит паспортные данные, реквизиты документов на машину или квартиру и так далее. Например, на сайтах объявлений мошенники демонстрируют чужие фото паспорта, таким образом пытаясь убедить жертв, что переводить оплату или вносить залог абсолютно безопасно. В дальнейшем после получения денег мошенник бесследно пропадает, а у человека, чьими данными он воспользовался, возникают проблемы.

Ниже приведены наиболее распространённые схемы взлома личного кабинета Госулуг (доступа к аккаунту):

1. Жертве поступает звонок от «специалиста техподдержки Госуслуг». Он сообщает, что в учётной записи замечена подозрительная активность и лучше на время заблокировать личный кабинет. Это очень просто: пользователь сейчас получит SMS и должен продиктовать из него код. Если жертва так и делает, мошенник получает доступ к аккаунту. Ну и вместе с ним — данные владельца. В последнее время всё больше людей становятся жертвами такой схемы мошенничества.

Так, в дежурную часть Отд МВД России по Хасынскому району в ноябре 2024 года поступило заявление от работника одной из муниципальных предприятий в пос. Палатка о том, что неустановленные лица, находясь в неустановленном месте, представившись представителем портала «Госуслуги», а также финансовым экспертом, путём обмана и злоупотребления доверием, завладели денежными средствами в сумме 310 000 рублей, а также через SMS-уведомление осуществили неправомерный доступ к компьютерной информации, завладев аккаунтом на портале «Госуслуги».

2. Телефонный мошенник представляется сотрудником мобильного оператора. Он сообщает, что срок действия SIM-карты клиента истекает. Если человек дальше хочет пользоваться своим номером, необходимо продлить договор. Для этого нужно сообщить код. Прямо во время разговора на телефон действительно поступает SMS от Госуслуг с кодом. Жертва теряет бдительность и совсем не подозревая делится доступом.

Мошенники представляются представителями всех действующих на территории России операторов (МТС, Билайн, Мегафон, Т2).

Пример: в дежурную часть Отд МВД России по Хасынскому району в ноябре 2024 года поступило заявление от работника частной компании в сфере дорожного строительства о том, что неустановленное лицо путём обмана, представившись сотрудником ПАО «МТС», под предлогом продления срока действия договора абонентского номера , получило доступ к учетной записи на портале «Госуслуг», тем самым произвело её модификацию и ограничило доступ к сервису.

3. **Злоумышленники могут представиться сотрудниками государственных органов, банков, налоговой инспекции**. Повод для связи может быть любым: уточнить данные для декларации на налоговый вычет, оплатить штраф, отменить заявку на заём микрофинансовых организациях и так далее. Во всех случаях мошенники также пытаются выманить код из SMS. Как правило, жертву торопят, а для убедительности обращаются по имени и называют адрес регистрации. Важно помнить: все эти данные легко отыскать на просторах Интернета, а цель мошенника – войти в доверие и получить от жертвы нужную информацию.

В дежурную часть ОМВД России по г. Магадану поступило заявление от жителя г. Магадана, сотрудника одной из федеральных структур, о том, что неустановленное лицо путём обмана, представившись сотрудником пенсионного фонда, под предлогом перерасчета пенсии, получило доступ к учетной записи на портале «Госуслуг», тем самым произвело её модификацию и ограничило доступ к сервису «Госуслуги».

Чтобы оградить себя от взлома аккаунта на портале «Госуслуги» необходимо соблюдать следующие правила безопасности:

1. Общий совет: всегда важно оставаться внимательным, избегать паники и не предпринимать поспешных действий!

2. Если вы заметили, что ваш пароль и контрольный вопрос на сайте «Госуслуги» были изменены, не следует звонить по неизвестному номеру или

пытаться восстановить пароль самостоятельно. В такой ситуации сначала нужно обратиться в МФЦ. Однако, прежде всего, рекомендуется позвонить в реальную службу поддержки «Госуслуги» и подробно объяснить им свою ситуацию.

3. Будьте внимательны при ответе на звонки с незнакомых номеров, не сообщайте пароли и коды, поступившие по СМС-сообщениям незнакомым людям ни под каким предлогом!

4. Помните, что представители операторов сотовой связи, банковских организаций или иных учреждений не имеют права запрашивать у вас данные от портала Государственных услуг и иную персональную информацию.

5. Отдельно обратите внимание, что **не созваниваются с клиентами:**

- сотовые компании – с целью ***продления услуг мобильной связи*** (работа ведётся исключительно через официальное мобильное приложение операторов связи);

- Отделение Фонда пенсионного и социального страхования Российской Федерации по Магаданской области (его филиалы) – с предложением ***услуг по перерасчёту размера пенсии и трудового стажа***;

5. Чтобы не допустить несанкционированный доступ в ваш личный кабинет на сайте «Госуслуги», необходимо соблюдать ряд простых ***правил кибербезопасности, которые изложены на официальном этого сайта*** (ссылка: https://www.gosuslugi.ru/help/faq/personal_data/100465). Особое внимание специалисты по кибербезопасности обращают внимание на ***создание уникального пароля для входа в личный кабинет*** из 12 символов (ссылка: https://www.gosuslugi.ru/life/details/how_to_create_strong_passwords).