ГОСУСЛУГИ.

Каждый день мошенники разрабатывают новые схемы. Мы собрали самые распространенные:

- **Фишинговые сайты,** мимикрирующие под «Госуслуги» и собирающие данные пользователейПопасть на них можно из спам-рассылок (через SMS, мессенджеры, e-mail). Запомните: единственный адрес «Госуслуг» — https://www.gosuslugi.ru/.
- **Предложение записаться на обследование в ведущей клинике.** Мошенники звонят пожилым людям, называют их ФИО и паспортные данные, предлагают пройти бесплатное обследование. Чтобы записаться на прием, просят назвать код из SMS от «Госуслуг».
- **Получение социальных выплат.** Жертва получает SMS, письмо на почту или сообщение в мессенджер, что ей положена социальная выплата. Сумму мошенники называют внушительную — 200 000 рублей и более. Чтобы получить деньги, нужно перейти по ссылке (фишинговой, разумеется) и заполнить анкету.
- **Уведомление о блокировке SIM-карты**. Мошенники звонят жертве от имени оператора связи, сообщают, что истекает срок действия договора (на самом деле он бессрочный). Чтобы продлить договор, нужно сказать код из SMS от «Госуслуг», а затем перейти по фишинговой ссылке из другой SMS и ввести еще один код там.
- **Представители энергосбытовой компании**. Мошенники звонят жертве от имени энергосбытовой компании, сообщают о большой скидке или перерасчете платежей, предлагают оформить все через «Госуслуги». Далее схема проста: жертва дает код из SMS мошенникам и попадает в неприятности.

На «Госуслугах» хранятся все наши персональные данные — серия и номер паспорта, пенсионное страховое свидетельство (СНИЛС), ИНН и прочее. А еще с их помощью можно залогиниться на сайте ФНС и получить налоговый вычет, а также заказать справку 2-НДФЛ и оформить кредит в любом российском банке.

Поэтому, если мошенники получили доступ к «Госуслугам», вы рискуете не только рассекретить персональные данные, но и погрязнуть в долгах. Кроме того, из-за этого могут пострадать и ваши близкие. Так, узнав о вас всю информацию (где живете, где работаете, в каких банках у вас счета, есть ли у вас имущество), аферисты могут позвонить или написать вашим родственникам и выманить у них деньги.

Поэтому никому и ни при каких обстоятельствах нельзя сообщать пароль и код из SMS от сервиса.

НОВАЯ СХЕМА ОБМАНА: КАК МОШЕННИКИ КРАДУТ АККАУНТЫ ЧЕРЕЗ ФАЛЬШИВУЮ ТЕХПОДДЕРЖКУ

ЦИФРОВАЯ РОССИЯ

Мошенники придумали новую схему, позволяющую похищать аккаунты россиян на портале «Госуслуги». **Теперь злоумышленники просят потенциальную жертву позвонить по специальному номеру.**

Сначала мошенники отправляют жертве электронное письмо, либо СМС.
В нем сообщается о попытке входа в аккаунт на портал «Госуслуги», а также просьба позвонить по специальному номеру.

Если жертва связывается по номеру, то **мошенники начинают притворяться работниками службы поддержки портала «Госуслуги».** Под предлогом помощи они дают ложные рекомендации, в результате которых человек теряет доступ к своему аккаунту, а управление им переходит к аферистам.