**Как мошенники получают доступ к госуслугам**

Портал «Госуслуги» - надежно защищенный сервис и взломать его без участия владельца учетной записи невозможно. Для того, чтобы получить доступ к госуслугам своей жертвы, мошенники используют социальную инженерию (психологические приемы) и отточенные навыки работы с порталом (для быстрого сбора и использования информации). Как мошенники могут получить доступ к учетной записи на «Госуслугах» и что делать если «утечка» данных произошла в [интервью «Газета.ру»](https://www.gazeta.ru/business/news/2025/06/19/26061458.shtml) рассказала эксперт проекта НИФИ Минфина России «Моифинансы.рф» Ольга Дайнеко.

Чтобы обеспечить себе доступ к данным личного кабинета Госуслуг, злоумышленники используют различные способы:

- создают фишинговые сайты, дизайн, логотип и цветовая гамма которых визуально похожи на сайт Госуслуг. Ссылки на поддельный сайт обычно присылаются в виде электронных писем или в СМС-сообщениях под видом уведомлений якобы от администрации портала, специалистов государственных ведомств, сотовых операторов. В тексте сообщения просят подтвердить свои данные, предотвратить несанкционированный доступ, пролонгировать сим-карту, оплатить налоги/штраф или оформить полагающуюся льготу. Ссылки, прикрепленные к таким сообщениям, ведут на фишинговый сайт, на котором жертва, видя знакомый логотип Госуслуг, вводит свои логин и пароль для входа в личный кабинет;

- создают вредоносное ПО, с помощью которого похищаются логины/пароли, сохраненные в браузере. Распространяется такое ПО также посредством фейковых рассылок. Такие сообщения могут приходить не только от незнакомцев, но и от тех, кто в списке контактов (например, под видом просьбы о голосовании в конкурсе, перехода по ссылке, рекомендованной другом). Аккаунт знакомого человека может быть взломан, поэтому к присланным ссылкам нужно относиться настороженно;

- связываются с жертвой по телефону, представляясь специалистами Госуслуг/сотового операторы/медучреждения/службы доставки и других. С помощью психологических приемов убеждают, что требуется сообщить подтверждение из полученного СМС. Методы социальной инженерии, используемые мошенниками, позволяют усыпить бдительность, посеять панику. В итоге жертва сама передает конфиденциальную информацию;

-создают фейковые предложения об оказании услуг (заполнению налоговой декларации, заявления на получение социальных выплат). Нередко такие предложения маскируются под безвозмездную помощь. Чтобы правильно оформить льготу/отправить декларацию/заполнить заявление у жертвы выманиваются данные для доступа к личному кабинету.

После получения доступа к порталу Госуслуги злоумышленники оперативно меняют пароль для входа и номер телефона. Чтобы жертва не могла быстро получить доступ к своей учетной записи, добавляют свой контрольный вопрос для восстановления доступа к ЛК.

Если случилась ситуация, когда доступ к госуслугам получил посторонний, нужно:

- не паниковать и не следовать инструкциям злоумышленника (кем бы он не представлялся);

- самостоятельно связаться с техподдержкой Госуслуг и сообщить о случившемся;

- восстановить доступ к учетной записи самостоятельно (инструкция - <https://www.gosuslugi.ru/help/faq/personal_data/45620> или через личное обращение в центры оказания госуслуг (МФЦ, банк);

- проверить учетные данные (номер телефона и другие контактные данные), список устройств, с которых осуществлен вход в личный кабинет (выйти со всех посторонних устройств), а также проверить, где использовался вход с использованием аккаунта (помощь с проверкой также могут оказать в МФЦ):

-обратиться в полицию.