Приложение

Информация о мошеннической схеме,
связанной с прохождением диспансеризации, и рекомендациях,
как не допустить несанкционированный доступ в личный кабинет
портала «Госуслуги», и что делать, если аккаунт взломан

Министерство внутренних дел Российской Федерации и Министерство здравоохранения Российской Федерации обращает внимание населения на участившиеся факты киберпреступлений, связанных с проведением профосмотров и диспансеризации, когда злоумышленники под видом приглашения пройти медицинский осмотр, записаться к конкретному врачу выманивают у доверчивых граждан платёжные данные или доступ к «Госуслугам».

Так, мошенники могут пригласить вас пройти, например, флюорографию, предлагая выбрать ближайший филиал поликлиники, дату и время, а для записи на приём назвать поступивший в СМС-сообщении код. Отвлекает внимание жертвы, как правило, то факт, что к ней обращаются по имени-отчеству, и действительно имеется необходимость пройти медосмотр. Получив код, злоумышленники могут списать деньги со счёта потерпевшего или получить доступ к порталу «Госуслуги». В ряде случаев мошенники в телефонном разговоре выманивают дополнительную персональную информацию, включая номер СНИЛС.

В случае получения доступа к личному кабинету «Госуслуг», мошенники проводят ряд махинаций: от получения микрозаймов в кредитно-финансовых организациях и оформления сим-карт до получения доступа о счетах и доходах человека, которую вместе с данными всех документов можно перепродать другим злоумышленникам для таргетированных атак.

Приходится констатировать, что, несмотря на проводимую профилактическую работу в трудовых коллективах органов исполнительной власти и местного самоуправления Магаданской области по предупреждению киберпреступлений, государственные и муниципальные служащие нередко становятся жертвами кибермошенников.

В ряде случаев удалось избежать серьёзных последствий, потерпевшие вовремя поняли, что имелась попытка взлома личного кабинета сайта «Госуслуги», оперативно обратились в МФЦ, и доступ преступников к личным данным был заблокирован.

Вместе с тем в марте 2025 года в дежурную часть ОМВД России по г. Магадану обратился один из работников областного **образовательного учреждения** с заявлением, что неустановленное лицо, представившись работником поликлиники, под предлогом прохождения диспансеризации, совершило неправомерный доступ к компьютерной информации, а именно завладело аккаунтом заявителя на портале «Госуслуги». Для связи злоумышленники использовали аккаунты в мессенджере «WhatsApp». Возбуждено уголовное дело по статье 272 УК РФ («неправомерный доступ к компьютерной информации»).

**В связи с этим, чтобы не стать жертвой мошенников, необходимо обратить внимание на следующие меры безопасности.**

В Магаданской области действуют две организации, оповещающие граждан посредством телефонного обзвона о прохождении диспансеризации (Единый кол-центр министерства здравоохранения и демографической политики Магаданской области и АО «СОГАЗ-Мед»).

Звонки с кол-центра поступают исключительно с официального номера (220003), обзвон совершает голосовой робот, который только информирует о возможности пройти диспансеризацию и предлагает переключить на оператора, чтобы создать запись на приём. Такая же процедура и АО «СОГАЗ-Мед».

**При этом никаких данных и просьб назвать код из СМС-сообщения медицинские работники не запрашивают. Это делаю только мошенники!**

**Помните о простых правилах:**

1. Не отвечайте на звонки с неизвестных номеров, особенно если они подозрительные или начинаются с просьбы предоставить личную информацию!

2. Не передавайте личные данные по телефону, даже если звонящий представляется сотрудником известного вам учреждения.

3. Не передавайте коды из СМС-сообщения, это ключ к вашим финансовым операциям!

4. Услышав такие просьбы, сразу прервите звонок.

5. Всегда перепроверяйте информацию: если вам звонят из банка или другого учреждения, лучше положить трубку и перезвонить по официальному номеру.

6. Если ваш аккаунт на сайте «Госуслуги» взломали, то **необходимо**:

- попытаться восстановить доступ к своей учётной записи и проверить воспользовались ли мошенники вашими данными (были ли запросы от вашего имени – на обновление данных электронной трудовой книжки (ЭТК), индивидуального лицевого счёта (ИЛС), 2-НДФЛ, а также подавались ли заявки на кредит в кредитно-финансовые учреждения);

- если на вас взяли кредит, обратиться в банк и сообщить, что заявку на кредит подали мошенники;

- для оперативного решения проблемы обратиться в ближайшее отделение МФЦ;

- подать заявление в ближайшее отделение органов внутренних дел. Это нужно сделать, даже если в кредитной истории нет неизвестных вам заявок на кредит. Мошенники могут использовать ваши данные позже, если у них останется доступ к учётной записи на Госуслугах. Поданное заявление поможет доказать, например, что кредит или заём оформляли не вы. Подать заявление можно лично или онлайн. Чтобы обратиться онлайн, выберите свой регион на сайте МВД России и подайте обращение через интернет-приёмную на сайте УМВД России по Магаданской области.

Подробная информация о пошаговых действиях в случае взлома аккаунта приведена на портале «Госуслуги» (ссылка: https://www.gosuslugi.ru/help/faq/login/4562).