Как мошенники пользуются данными из «Госуслуг»

Войдя в личный кабинет на портале, мошенники могут:

1. Продать ваши данные в даркнете, чтобы заработать: слив банковской информации с каждым годом становится выгоднее.
2. Получить доступ к мобильному банку карты, привязанной к «Госуслугам.
3. Заполучить данные банковских карт и попытаться отвязать их от вашего номера или списать деньги.
4. Зарегистрировать фиктивный бизнес на ваше имя.
5. Переоформить ваше имущество на себя.

Успех мошенников зависит от безопасности на других онлайн-сервисах, к которым обратятся с украденными данными. Например, в некоторых микрофинансовых организациях можно оформить займ без личного визита: им достаточно лишь копии паспорта. Если на «Госуслугах» хранятся сканы документов, преступники этим воспользуются.

Что делать, если 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.

Лучше сделать следующее:

- Позвоните в банки и заблокируйте все карты, которыми вы когда-либо оплачивали услуги, штрафы, госпошлины, налоги на портале, и сообщите, что стали жертвой мошенников.
- Обратитесь в МВД лично или отправьте электронное обращение с описанием случившегося.

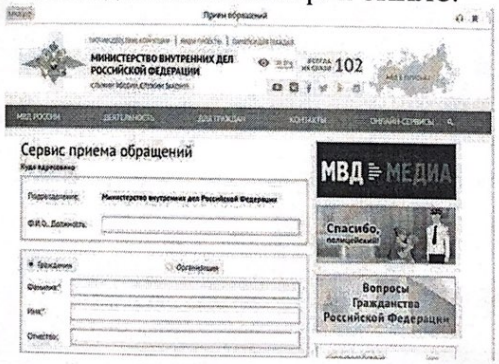
Электронное заявление можно отправить на сайте МВД

- Посетите МФЦ и попытайтесь восстановить доступ к личному кабинету.

Список центров обслуживания граждан, в которых можно восстановить доступ к аккаунту, можно посмотреть прямо на «Госуслугах».

Чтобы увидеть список доступных центров, нужно на странице авторизации нажать кнопку «Не удается войти», затем — «Центры обслуживания».

Обращаться в центр можно без записи. При себе необходимо иметь паспорт и СНИЛС.



Как избежать обмана

У мошенников есть два сильных «оружия»: умение работать с технологиями и познания в психологии. Первое позволяет им получить как можно больше конфиденциальных данных о жертвах, звонить и присылать СМС с официальных номеров различных служб. Именно такая способность вызвала целую волну мошенничеств, связанных с СМС и звонками от лица банковских сотрудников.

Мошенники выкупают номера телефонов из баз данных сотовых операторов, создавая свои базы данных. Они используют различные программы взлома, фишинговые сайты, вирусы, — это позволяет им красть сохраненные в браузерах логины, пароли и другую информацию.

Чтобы не попасться на уловки телефонных мошенников, никогда не сообщайте никакие данные по телефону: номера карт, коды, кодовые слова и пароли.

Если вы сомневаетесь в безопасности личного кабинета, **сделайте следующее:**

- Положите трубку и сразу же попытайтесь войти в свой аккаунт.
- Задайте более сложный и надежный пароль: используйте строчные и прописные буквы, цифры, специальные символы и ни в коем случае не устанавливайте пароли из символов, идущих по порядку (например, qwerty или 654321), номеров телефона, даты рождения.
- Не сохраняйте пароли в браузерах.
- Установите двухфакторную аутентификацию на сайте, чтобы вы могли войти в личный кабинет только после ввода пароля и дополнительного кода, который придет по СМС.