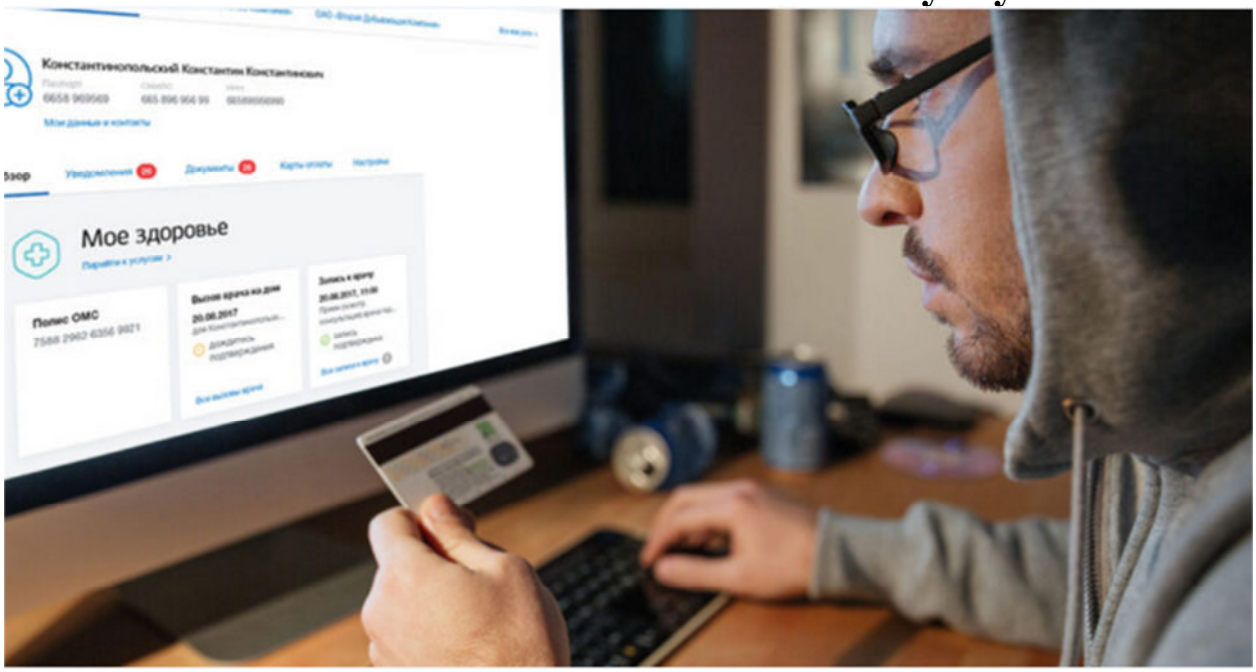
Новый способ мошенничества на «Госуслугах»



Сайт «Госуслуги» содержит почти всю информацию о зарегистрированных на нем: от номера паспорта до QR-кода о вакцинации. Это удобно, чтобы оплатить услуги в онлайн или записать к врачу. Но теперь это и опасно, потому что до сервиса добрались мошенники.

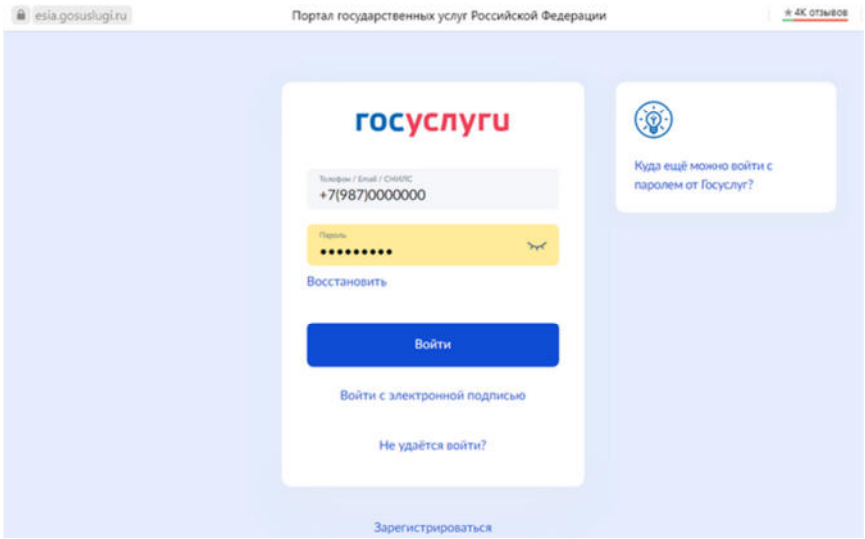
Рассказываем, как они получают доступ к чужому личному кабинету на «Госуслугах», и что делать, если это произошло.

Мошенники звонят жертве

Новый способ мошенничества, о котором мы узнали, начинается с телефонного звонка. Приветливая девушка представляется сотрудницей «Госуслуг», называет свои фамилию, имя, отчество и сообщает, что ваш личный кабинет атакуют мошенники. Обманщики якобы пытаются изменить номер телефона, который у вас привязан к «Госуслугам», и им нужно срочно помешать.

Как мошенники сумели раздобыть данные?

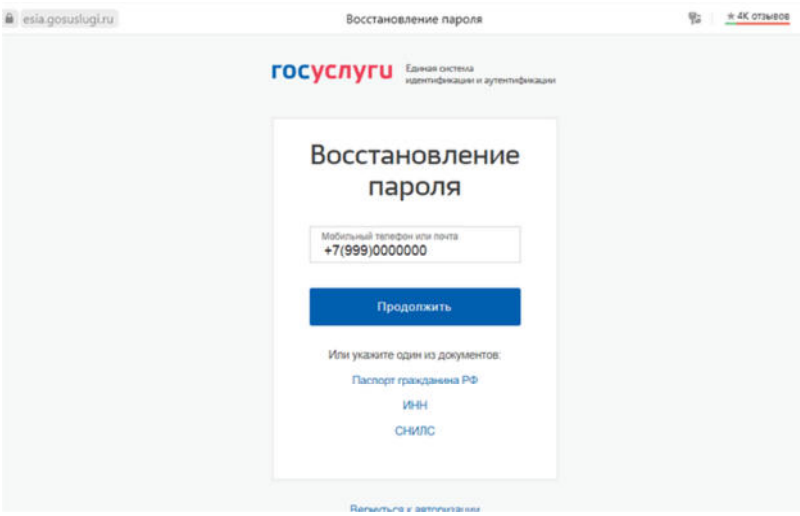
Во-первых, некоторые из них есть в открытом доступе: те же самые номера телефонов часто привязаны к соцсетям. Во-вторых, некоторые компании не следят за безопасностью данных, и мошенники, используя уязвимость, воруют информацию. Так данные могут утечь, например, у различных служб доставки, мобильных банков, сервисов лояльности в магазинах.



Авторизация на сайте «Госуслуг». Именно на номере телефона, который привязан к личному кабинету, держится новая мошенническая схема.

Казалось бы, это уже заезженный сценарий телефонных аферистов, и пора положить трубку. Но несколько нюансов заставляют потерять бдительность и поверить собеседнику:

1. Если потерять доступ к личному кабинету и пытаться его восстановить, на телефон придет СМС с кодом подтверждения или же позвонит представитель службы безопасности «Госуслуг». Мошенники звонят с этого же номера.

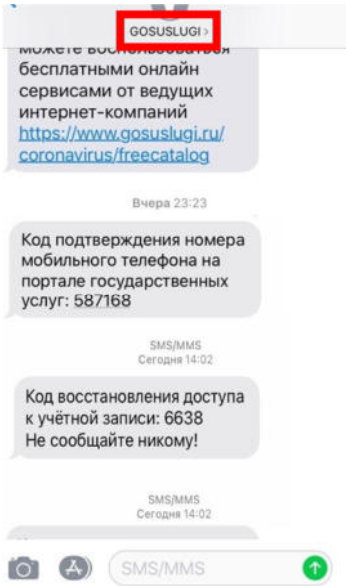


Чтобы восстановить доступ к личному кабинету, нужно ввести номер телефона, на который придет код подтверждения

Важно: официальные номера телефона для связи с «Госуслугами» указаны на сайте. Бесплатный номер по России: 8-800-100-70-10, для звонков из-за границы: +7-495-727-47-47, для мобильных телефонов: 115. Но мошенники могут звонить и с этих номеров!

2. Если напрямую сказать собеседнику, что вы не верите ему, вас убеждают в обратном. Он безошибочно называет все данные о вас, которые есть на портале и которые нельзя найти в свободном доступе. Это номер паспорта, ИНН, СНИЛС и даже история ваших действий в личном кабинете вплоть до оплаты штрафов.

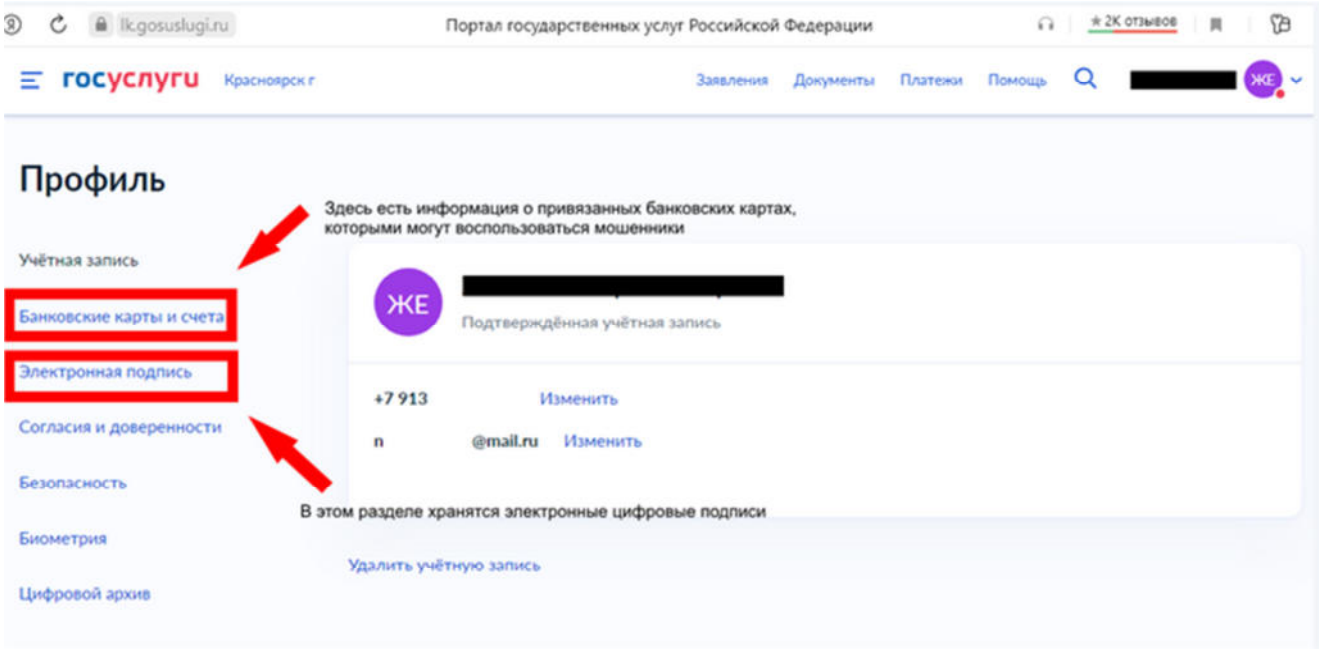
3. Лжесотрудник «Госуслуг» очень грамотно входит в доверие: говорит убедительно и, видя ваши сомнения, предлагает задать любые интересующие вас вопросы, на которые уверенно отвечает.



А дальше жертву ждет такой сценарий: собеседник обещает помочь и просит назвать код, который тут же приходит на телефон.

Коды восстановления доступа к «Госуслугам». Именно их просят по телефону мошенники под предлогом защитить аккаунт

Получив код, мошенники завладевают вашим личным кабинетом и всей информацией, которая там есть. Это позволит им, например, похитить электронную цифровую подпись или оформить ИП на ваше имя.



В личном кабинете «Госуслуг» хранятся данные привязанных банковских карт и список ЭЦП

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.

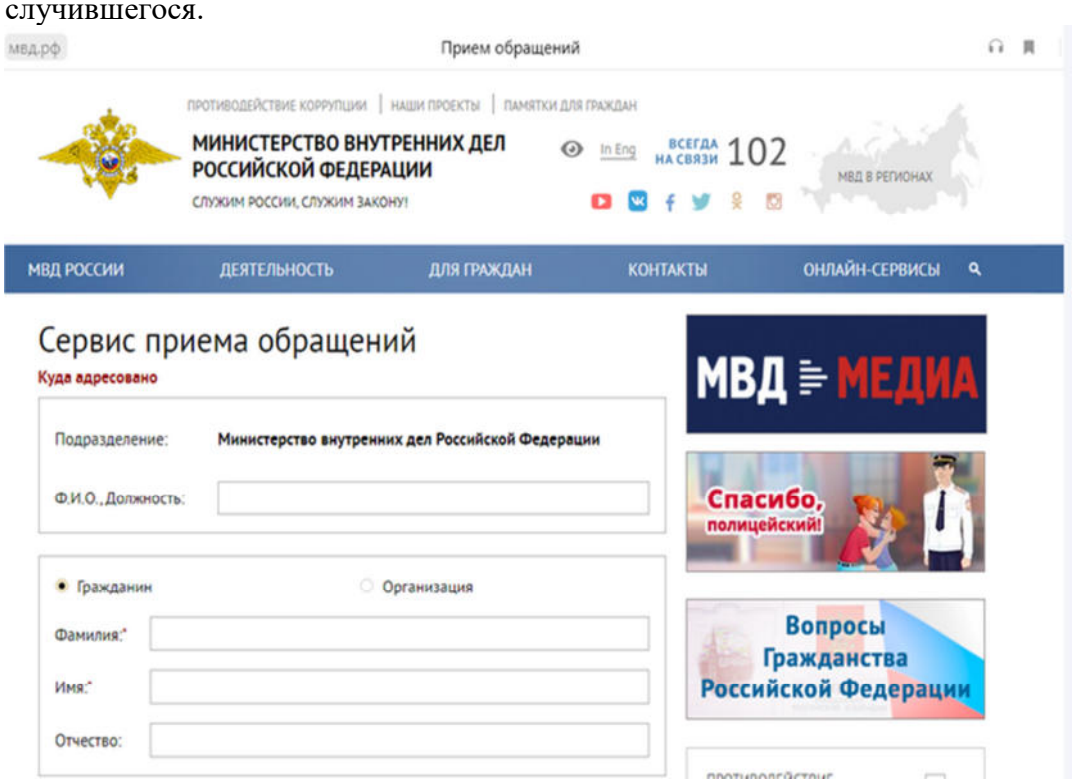
Успех мошенников зависит от безопасности на других онлайн-сервисах, к которым обратятся с украденными данными. Например, в некоторых микрофинансовых организациях можно оформить займ без личного визита: им достаточно лишь копии паспорта. Если на «Госуслугах» хранятся сканы документов, преступники этим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

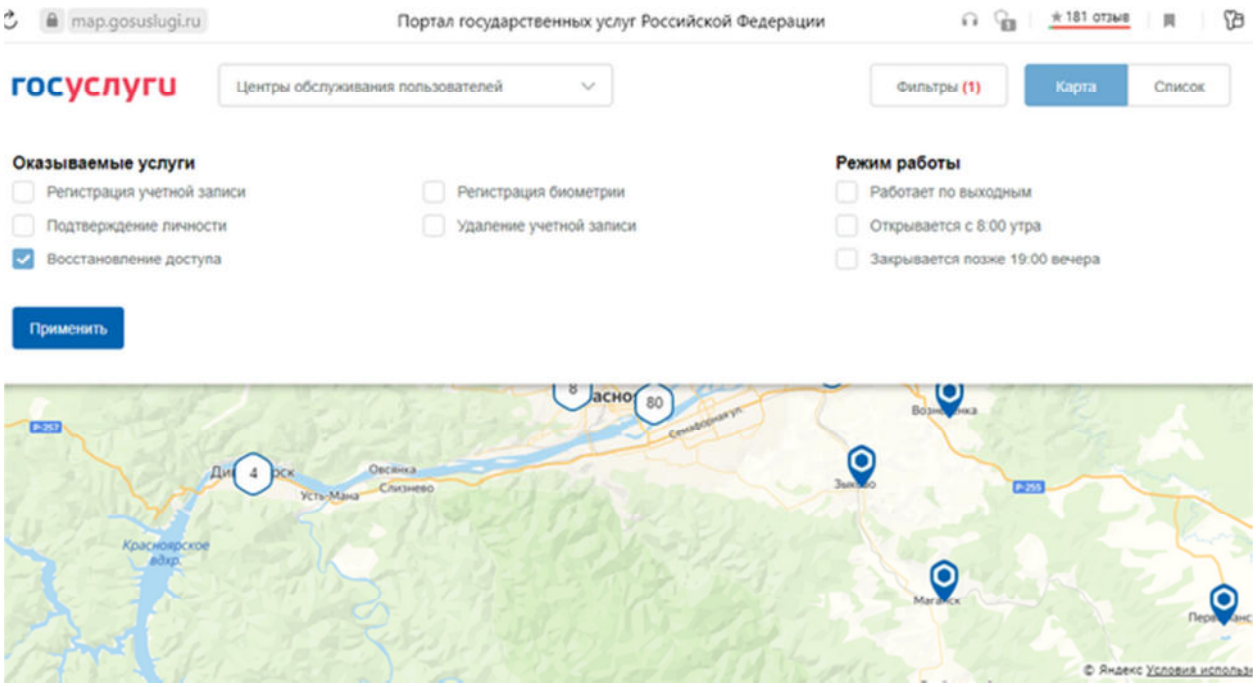
- Позвоните в банки и заблокируйте все карты, которыми вы когда-либо оплачивали услуги, штрафы, госпошлины, налоги на портале, и сообщите, что стали жертвой мошенников.
- Обратитесь в МВД лично или отправьте электронное обращение с описанием случившегося.



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.

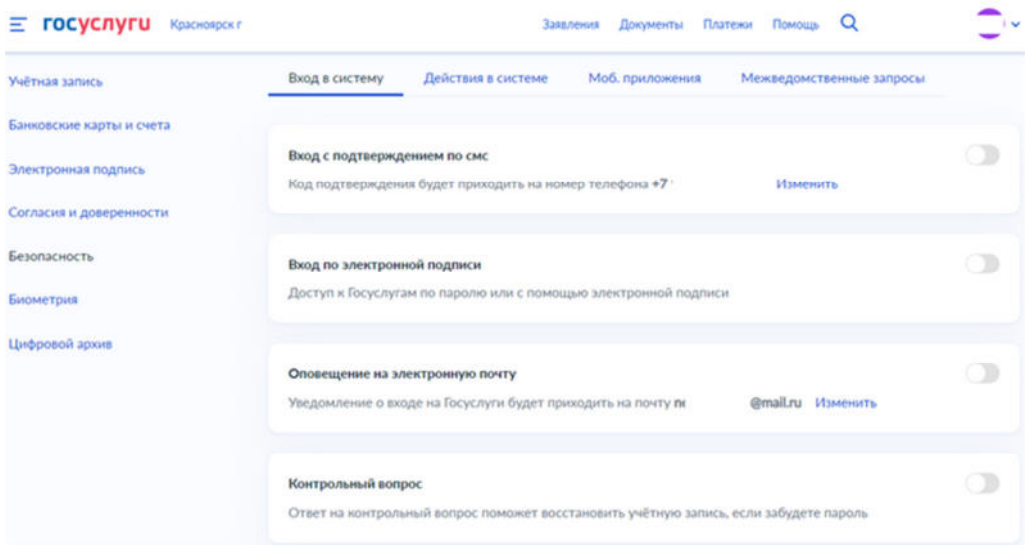
Мошенники выкупают номера телефонов из баз данных сотовых операторов, создавая свои базы данных. Они используют различные программы взлома, фишинговые сайты, вирусы, — это позволяет им красть сохраненные в браузерах логины, пароли и другую информацию.

Знание психологии и умение убедить человека в том, что он — не жулик, заставляет людей терять бдительность, паниковать и сообщать всю информацию о себе, лишь бы избежать проблем.

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.



Во вкладке «Безопасность» можно установить дополнительное подтверждение входа по СМС, электронной подписи и контрольному вопросу

- Посетите МФЦ и узнайте, все ли с вашим аккаунтом в порядке.

Сегодня лучший способ обезопасить себя — никому не доверять, даже если собеседник кажется вам очень убедительным. В любой ситуации, где вы сомневаетесь, лучше обратиться в МФЦ и узнать о статусе аккаунта лично.

Обязательно предупредите об атаках мошенников близких, особенно пожилых. Пусть никому не сообщают свой номер телефона, коды подтверждения, логины, пароли и другие данные.