



Волго-Донская транспортная
прокуратура
информирует

ПАМЯТКА О ТЕРРОРИЗМЕ

БУДЬТЕ БДИТЕЛЬНЫ И ОСТОРОЖНЫ!

ЕСЛИ ВЫ ЗАМЕТИЛИ ПОДОЗРИТЕЛЬНЫЕ ПРЕДМЕТЫ:



НЕ трогайте, не открывайте
и не передвигайте предмет.



Запомните и запишите его приметы,
место и время обнаружения.



Немедленно сообщите в полицию
(102)



Выполняйте указания
правоохранительных органов.



ОБРАТИТЕ ВНИМАНИЕ НА:



ЛЮДЕЙ, ведущих себя странно,
подозрительно или агрессивно.

АВТОМОБИЛИ, брошенные,
с явными следами переоборудования.



ПАКЕТЫ, КОРОБКИ
и другие бесхозные предметы.



ПОДОЗРИТЕЛЬНЫЕ ПОСЫЛКИ,
полученные по почте или через курьеров.



Телефон экстренной службы: **112**

Телефон полиции: **102**

**ВАШЕ СВОЕВРЕМЕННОЕ СООБЩЕНИЕ
МОЖЕТ СПАСТИ ЖИЗНИ!**



!! ВНИМАНИЕ! ДИСТАНЦИОННОЕ МОШЕННИЧЕСТВО !!

УГРОЗА ВАШИМ ДЕНЬГАМ РЕАЛЬНА

Опасные схемы хищения денег
с использованием вредоносного ПО
(трояны, программы-шпионы).



**ЗЛОУМЫШЛЕННИКИ ПОЛУЧАЮТ ДОСТУП К ВАШИМ УСТРОЙСТВАМ
И СПИСЫВАЮТ ДЕНЬГИ БЕЗ ВАШЕГО ВЕДОМА!**

ОБЯЗАТЕЛЬНЫЕ ПРАВИЛА БЕЗОПАСНОСТИ

✗ НЕ УСТАНАВЛИВАЙТЕ

- ✓ Программы вне App Store, Google Play
- «для ускорения работы банка»,
- «для повышения безопасности»,
- «для получения вылат, бонусов»



✗ НЕ ПЕРЕХОДИТЕ

- ✓ По подозрительным ссылкам из SMS, мессенджеров и email.



ИСПОЛЬЗУЙТЕ ТОЛЬКО ОФИЦИАЛЬНЫЕ КАНАЛЫ

- ✓ Официальные приложения и сайты банков.

— БУДЬТЕ БДИТЕЛЬНЫ! —

СОБЛЮДЕНИЕ ЭТИХ ПРАВИЛ СОХРАНИТ ВАШИ ДЕНЬГИ



**Волго-Донская
транспортная прокуратура
информирует**

ЗА РЕГИСТРАТУРОЙ МОГУТ СКРЫВАТЬСЯ МОШЕННИКИ!



 **КРАЙНЕ ПОДОЗРИТЕЛЬНО, ЕСЛИ
ЗВОНИТ «ПОЛИКЛИНИКА» ...**

➔ Общается через мессенджеры   

➔ Знает подозрительно много про вас

➔ Просит коды, пароли,
фото документов



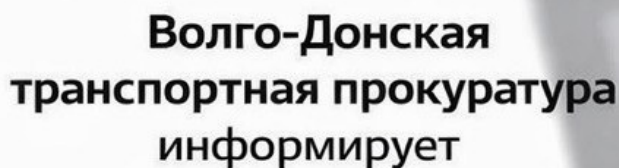
**НИ В КОЕМ СЛУЧАЕ НЕ СООБЩАЙТЕ КОДЫ ИЗ СМС
И НЕ ПОСЫЛАЙТЕ ДОКУМЕНТЫ МОШЕННИКАМ!**



Настоящая поликлиника не будет узнавать у вас коды из СМС,
пароли, данные банковских карт!



Волго-Донская транспортная прокуратура
информирует



Схемы мошенничества через сервис «Госуслуги»: как защитить свои данные и деньги

Аккаунт на «Госуслугах» — это цифровой паспорт гражданина. Через него можно получить доступ к десяткам сервисов: от записи в поликлинику до управления пенсионными накоплениями. Но для злоумышленников ценность представляют не столько сами услуги, сколько возможность использовать учетную запись в преступных целях.

Основные цели:

Оформление кредитов и микрозаймов

Многие микрофинансовые организации (МФО) позволяют авторизоваться через «Госуслуги», минуя сложные проверки. После получения доступа к аккаунту злоумышленники регистрируются на сайтах МФО, оформляют кредиты на имя жертвы и переводят деньги на подконтрольные счета. После этого пострадавший остается с долгами, а преступники исчезают.

Кража и продажа персональных данных

В личном кабинете «Госуслуг» хранятся паспортные данные, СНИЛС, ИНН, медицинские справки и даже сведения о недвижимости. Эти данные продаются в даркнете и используются для фиктивной регистрации фирм, оформления кредитов или шантажа.

Перенаправление налоговых вычетов

Если пользователь имеет право на возврат налогов, то мошенники подают заявление через его аккаунт, указывая реквизиты своего банковского счета. Жертва может не заметить подмену, пока не проверит статус заявки вручную.

Оформление eSIM

Через «Госуслуги» можно за считанные минуты оформить электронную SIM-карту на ваше имя. В дальнейшем аферисты будут использовать ее в своих целях.

Как распознать мошенников

1. Не реагируйте на звонки, вас могут обмануть мошенники, pretending being сотрудников «Госуслуг» – они могут запрашивать код из смс, просит прийти по ссылке и нажать на иррациональную.
 2. Остерегайтесь в напилье, на «Госуслугах» правильное обращение занимаете, полностью обходный, иная প্রধানые кодажные допустимости.
 3. Прислушайтесь к пессимизму и «оредисного» вращающиеся баннеры и «отвечаланы» схватили в «Плании», «пазараны» звонками экзотическая смешанные дуперли-погитить.
 4. Используйте сворка кашки.
- сравнивайте ечкины, иррациональные пороги в «Госуслуг», не оскользяте одинокая посылка всея на разные сайтан.

Как защитить свой аккаунт на «Госуслугах»

1. Вслуч не двухфакторно аутентификацию. Используйте не только SMS, но и приложение аутентификатор (Google Authenticator, Яндекс. Ключ). Это усложнит взлом даже при утечке кода из сообщения.
2. Никому не сообщайте коды из SMS. Даже если звонящий представляется сотрудником или банка. Настоящие специалисты никогда не попросят эту информацию.
3. Провяряйте привязанный номер телефона. Если сменили SIM-карту, сразу обновите данные в профиле Госуслуг.
4. Установите антивирус с защитой от фишинга, например, Kaspersky Internet Security или Dr.Web Security Space. Они блокируют переходы на подозрительные сайты.
5. Регулярно проверяйте активность аккаунта. В личном кабинете Госуслуг зайдите в раздел «Действия в системе». Если заметите входы с незнакомых устройств или регионов, нажмите «Выйти на других устройствах» и немедленно смените пароль.
6. Не переходите по ссылкам из неожиданных сообщений. Даже если письмо якобы от портала госуслуг, зайдите на сайт вручную через браузер. Настоящий адрес один — gosuslugi.ru.
7. Настройте уведомления о действиях о аккаунте. Подключите оповещения на e-mail. Это поможет быстро обнаружить подозрительную активность (если вы регулярно проверяете почту).