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 провери статус заявки вручную.

Оформление eSIM

Чевез «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 реагорупие на заолки. вас мобут обммауть вооценнаки. предотиволеных сотрунниткыи Госуслуг» - они мобут запрашивить код ии смс, пресет пройти по сынитке инитсневить ирочаекои.
2. Остеротовитьсе в налинте, на Госуслугах оовито обращние занимете, поньно обюдни, иня рдювнчев кодавного довпутатовники.
3. Пноpронусе пессоданые иорецнсного ввоктанны баннсее и отоелознаныексзвенни ве Ваниии, пеазларнии звикоении экозениеня сикнещеныые деуперииопиметь.
4. Испольнуите свopка кашии. свяньзвите ечанкии, креиранные пороям вви Госуслуг, не остолыуите одичакия поилы воел на разныи сайтан.

Как защитить свой аккаунт на «Госуслугах»

1. Вслечь не деувфакторнию аутентификацию. Испопьзуйте не лолько SMS, но и приложенн аутентификетор (Google Authenticator, Яндекс. Ключ). Это усложнит взлом даже при утечке кода из сообщения.
2. Никому не сообщайте коды из SMS. Даже если звоиящий представляетоя сотрудником М или банка. Настоящие слециалисты никогда не попросят эту информацию.
3. Проваряйте приевзанный номер телефока. Если сменили SIM-карту, сразу обнозите данн в профиле Госуслуг.
4. Установите активирус с защитой от фищинта, например. Kaspersky Internet Security или Dr.Web Security Space. Они блокируют переходы на подозрительные сайты.
5. Регулярно проверяйте активность аккаукта. В личном кабинете Госуслуг зайдите в разде «Действия в зистеме». Если заметите входы с незнакомых устройств или регионов, нажмите «Выйти на других устройствах» и немедленно смените пароль.
6. Не переходите по осылкам 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 аккауите. Подключите оповещения на к-маи. Это помсrкет быстро обнаружить подозрительную активность (если вы регулярно проверяете почту).

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

!! ВНИМАНИЕ! ДИСТАНЦИОННОЕ МОШЕННИЧЕСТВО !!

УГРОЗА ВАШИМ ДЕНЬГАМ РЕАЛЬНА

Опасные схемы хищения денег
с использованиеы 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 выплат, 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