

МОШЕННИЧЕСТВО НА «ГОСУСЛУГАХ»

Мошенники звонят жертве



Приветливый голос представляется сотрудником «Госуслуг» и сообщает, что ваш личный кабинет пытаются взломать, изменив номер телефона, который привязан к порталу.



Важно!!! Новая мошенническая схема строится именно на номере телефона, который привязан к личному кабинету!

УМВД России по Ханты-Мансийскому автономному округу - Югре



ЧТО ЗАСТАВЛЯЕТ ЖЕРТВУ ПОТЕРЯТЬ БДИТЕЛЬНОСТЬ И ПОВЕРИТЬ СОБЕСЕДНИКУ?

Лжесотрудник «Госуслуг» говорит убедительно и предлагает задать любые уточняющие вопросы, на которые уверенно отвечает.

Безошибочно называет ваши персональные данные: номер паспорта, ИНН или информацию о наличии штрафов ГИБДД.



ГДЕ МОШЕННИКИ ВЗЯЛИ ВАШИ ДАННЫЕ?

- **Номера телефонов часто привязаны к социальным сетям, там же имеются фотографии автомобилей с государственными регистрационными знаками.**
- **ИНН можно получить, введя ФИО жертвы на сервисе проверки контрагентов.**
- **Персональные данные также могут утечь от недобросовестных организаций, из различных служб доставки или сервисов лояльности в магазинах.**



КАК МОШЕННИК ПОЛУЧАЕТ ДОСТУП К ЛИЧНОМУ КАБИНЕТУ?

- Аферист убедил вас, что действительно является сотрудником «госуслуг»
- Вы называете коды восстановления доступа к «Госуслугам», которые приходят в смс-сообщении.



Важно!!! Получив код, мошенники блокируют вам доступ к личному кабинету и похищают информацию, которая в нем храниться.

ЧТО МОГУТ СДЕЛАТЬ МОШЕННИКИ, ПОЛУЧИВ ДОСТУП К ЛИЧНОМУ КАБИНЕТУ?

- Получить доступ к мобильному банку карты, привязанной к «Госуслугам»
- Оформить кредит на ваше имя в микрофинансовой организации
- С помощью электронной цифровой подписи оформить ИП на ваше имя.
- Продать ваши персональные данные в даркнете, чтобы заработать
- Переоформить ваше имущество на себя.



ЧТО ДЕЛАТЬ, ЕСЛИ СТАЛИ ЖЕРТВОЙ МОШЕННИКА?

**Необходимо действовать
максимально быстро,
пока вашими данными не
успели воспользоваться.**

**Позвоните в банки и
заблокируйте карты,
которые привязаны к
личному кабинету.**

**Посетите МФЦ и
восстановите доступ к
личному кабинету,
сообщив о том, что стали
жертвой мошенников.**



КАК ИЗБЕЖАТЬ ОБМАНА?

- **Никогда не сообщайте никакие данные по телефону: номера карт, коды из смс-сообщений, логины, пароли и кодовые слова.**
- **Посетите МФЦ и узнайте, все ли с вашим аккаунтом в порядке.**
- **Установите двухфакторную аутентификацию на сайте, чтобы вы могли войти в личный кабинет только после ввода пароля и дополнительного кода, который придет по смс.**

