

Прокуратура разъясняет: схемы мошенничества с использованием фишинговых писем и сайтов для завладения данными Госуслуг

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.

Рассылка фишинговых писем:

Мошенники рассылают поддельные письма, которые очень похожи на официальные уведомления от Госуслуг. Например, в них могут предлагать проголосовать за капитальный ремонт дома, получить деньги за уход за ребенком или оформить льготный кредит. Эти письма выглядят правдоподобно — как будто их действительно прислали с портала. Но если присмотреться, адрес отправителя будет странным.

Когда человек верит обману и переходит по ссылке из такого письма, то попадает на сайт-подделку. Он выглядит почти как Госуслуги, но на самом деле создан мошенниками. Если на этом сайте ввести пароль от аккаунта, паспортные данные или номер банковской карты, эта информация попадет к злоумышленникам.

Фишинг через демонстрацию экрана:

В апреле 2025 году появилась новая схема, в которой мошенники используют функцию демонстрации экрана в мессенджерах. Они звонят жертве через WhatsApp или Telegram и представляются сотрудниками полиции или ФНС.

Пример сценария:

1.«Здравствуйте, это старший лейтенант Иванов из МВД. На ваш аккаунт Госуслуг совершена попытка взлома. Для защиты данных нужно срочно обновить информацию».

2.Жертве предлагают перейти на сайт, например, gossuslugi.ru или gosuslugi.ru (внимательно изучите адреса), где нужно ввести логин и пароль.

3.Чтобы «помочь», мошенник просит включить демонстрацию экрана. В этот момент он инициирует восстановление пароля на Госуслугах.

4.На телефон приходит SMS с кодом подтверждения, который виден на экране. Этого достаточно, чтобы украсть аккаунт.

Злоумышленники видят не только код, но и все действия пользователя: ввод паролей, доступ к банковским приложениям и историю переписок.

Если вам пришло подозрительное письмо, не нажимайте на ссылки. Лучше зайдите на Госуслуги через приложение или официальный сайт и проверьте, есть ли там такое же сообщение. Если нет — это точно обман.