СЭД МВД
№44/4822 от 10.06.2025

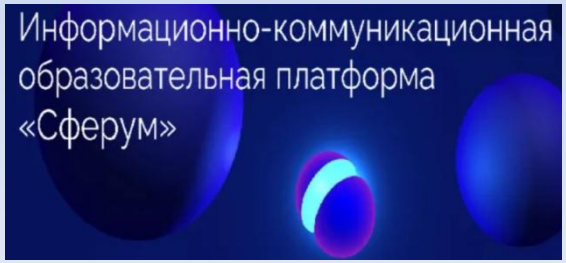
Защити себя и своих близких от кибермошенничеств

Виды мошеннических схем

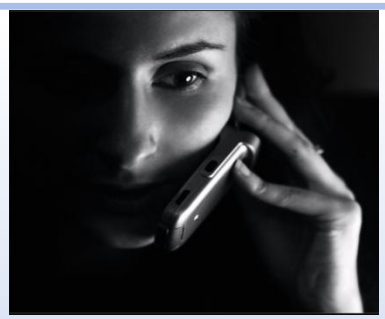
Мошенники под видом руководителей школ или учителей звонят родителям и говорят, что нужно обновить электронный журнал, список учащихся или профиль ученика в «Сферум». Для этого злоумышленники используют данные работников школы, дипфейк технологии и подменные номера. Они просят называть коды из СМС и получают через них доступ к «Госуслугам».

СЛЕДУЕТ ЗНАТЬ!

Обновления на платформе «Сферум» происходят автоматически и исключительно на устройстве пользователя, без участия третьих лиц. Для этого не используются коды из СМС, в том числе коды от «Госуслуг». Информация об обновлениях сервиса может приходить исключительно от платформы в виде системного сообщения и носит только информационный характер. Коммуникации по учебе также ведутся исключительно в «Сферум», где все пользователь верифицированы.



Виды мошеннических схем



Мошенники используют и **другие схемы** для получения доступа к «Госуслугам».

√ Звонят от имении оператора связи и предлагают продлить договор на обслуживание номера. Для этого они также просят назвать код из СМС, заходят в кабинет на «Госуслугах», меняют пароль и пишут в поле подсказки к контрольному слову фразу «Ваш аккаунт заблокирован, позвоните по указанному номеру» и оставляют свой телефон. После звонков мошенники убеждают людей, что на них пытаются взять кредит. Предлагают перевести деньги на безопасный счет.

√ Мошенники используют номера телефонов, которые были выставлены на повторную продажу, проверяют, зарегистрирован ли номер на «Госуслугах», и через СМС получают к нему доступ. После этого они оформляют через сервис заявки на онлайн-микрозаймы и кредиты.

Защити себя и своих близких

Проинформируйте своих знакомых о самых распространенных методах мошенничества в сети. Родители и дети, всегда совместно принимайте решение о том, стоит ли воспользоваться теми или иными услугами, предлагаемыми в Интернете.

Не оставляйте в свободном доступе банковские карты и платежные данные. Помните, что никогда администратор сайта не потребует полные данные вашего счета, пароли и пин-коды. Если кто-то их запрашивает, будьте бдительны – скорее всего, это мошенники.

Установите на свои компьютеры антивирусные программы и персональный браузер. Он поможет предотвратить кражу конфиденциальных данных или другие подобные действия.

Чтобы не попасться на уловки мошенников, необходимо знать:

- нельзя выполнять требования незнакомцев, передавать данные карт или устанавливать приложения;
- чтобы реагировать на подозрительные транзакции родителям необходимо настроить ограничение доступа на мобильные устройства, подключить уведомления в онлайн-банке;
- несовершеннолетний должен знать номера телефонов, по которым можно связаться с родителями и близкими;
- в случае угрозы со стороны незнакомых людей несовершеннолетнему следует обязательно обратиться к родителям или родственникам;
- базовые правила финансовой безопасности.

Одна из схем – запугивание через телефонные звонки

Аферисты звонят ребенку, представляясь сотрудниками полиции, службы безопасности или других организаций, сообщают о «чрезвычайной ситуации с родителями».
Например, утверждают, что родителям угрожает опасность, и чтобы их спасти требуют срочно продиктовать номера банковских карт.

Еще одна схема обмана связана с онлайн-играми

Мошенники создают поддельные акции или выигрыши в играх и просят ввести данные банковских карт для получения «приза» или предлагают приобрести игровую валюту, например, в Roblox. Несовершеннолетние берут деньги из дома и переводят мошенникам.

НОВЫЙ ВИД МОШЕННИЧЕСТВА – ИСПОЛЬЗОВАНИЕ НЕСОВЕРШЕННОЛЕТНИХ

Мошенники используют методы социальной инженерии, чтоб запугать несовершеннолетних, обманом заставить их передать доступ к средствам родителей.