Защити себя и своих близких от кибермошенничеств

Варианты вербовки дропперов:

- **рассказы «о планах по продажам» в банках:** *«оформи карту за вознаграждение».*
- **вовлечение в сетевой маркет инг:** *«Приведи друга с картой—получи деньги»;*
- **предложение «трудоустройства»:** *«Стань администратором лотереи и отправляй выигрыши победителям».*
- **сообщение якобы об ошибочной операции:** *«По ошибке отправил вам деньги—верните, но на другую карту или счет».*

Где мошенники ищут потенциальных дропперов?

- **В интернете:**
- **В социальных сетях;**
- **В мессенджерах;**
- **По электронной почте.**

Через знакомых рассказывают о возможности заработать «легкие» деньги.

В общественных местах расклеивают объявления о «легком» заработке.

С какими проблемами сталкиваются дропперы:

Банки ограничивают дропперам доступ к картам и онлайн-банку.

Сложности с получением банковских услуг у дропперов сохраняются вне зависимости от того, сколько времени прошло после участия в преступной схеме.

Потерпевшие обращаются в суд и родители подростков – дропперов выплачивают всю полученную преступным путем сумму.

ГУ МВД России по Саратовской области

Варианты вербовки дропперов:

- рассказы о «планах по продажам» в банках:

«Оформи карту за вознаграждение»

- вовлечение в сетевой маркетинг:

«Приведи друга с картой - получи деньги»

- предложение «трудоустройства»:

«Стань администратором лотереи и отправляй выигрыш победителям»

- сообщение о якобы ошибочной операции:

«По ошибке отправил Вам деньги - верните, но на другую карту или счёт»

Что делает дроппер?

- Передает чужие деньги от одного человека другому;
- Переводит деньги на незнакомые счета и карты по указанию мошенников;
- Снимает или вносит чужие наличные в банкоматы;
- Оформляет на себя банковские карты и отдает их мошенникам, либо дает доступ к своему онлайн-банку;

Мошенники предлагают вознаграждение, при этом сам «дроппер» становится соучастником мошеннической схемы.

ГУ МВД России

по Саратовской области

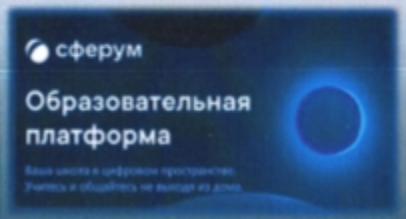
- люди, которых мошенники используют для обналичивания украденных денег

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 «Сферуме». Для этого злоумышленники используют данные работников школы, дипфейк технологии и подменные номера, сообщили в ведомстве. Они просят называть коды из СМС и получают через них доступ к «Госуслугам»

В «Сферуме» сообщили, что обновления на платформе 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», – говорится в сообщении сервиса, поступившем в РБК. Там указали, что «коммуникации по учебе также ведутся исключительно в «Сферуме», где все пользователи верифицированы».



Виды мошеннических схем

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

- Первая схема заключается в том, что они звонят от имени 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 кредиты, и предлагают перевести деньги на безопасный счет.
- Во время второй схемы используются номера телефонов, которые были выставлены на повторную продажу. Мошенники проверяют, зарегистрирован ли на номер аккаунт на «Госуслугах», и через СМС получают к нему доступ. После этого они оформляют через сервис заявки на онлайн-микрозаймы и кредиты.

Проинформируйте ребенка о самых распространенных методах мошенничества в сети. 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, воспользовавшись которыми ребенок может самостоятельно совершать покупки.

Не отправляйте о себе слишком много при совершении покупок: данные счетов, пароли, домашние адреса и телефоны. 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.

ГУ МВД России по Саратовской области

Чтобы не попасться на уловки мошенников, необходимо:

• объяснить детям, что нельзя выполнять требования незнакомцев, передавать данные карты или устанавливать приложения.

• использовать родительский контроль: настроить ограничение доступа на мобильных устройствах ребенка, подключить уведомления в онлайн-банке, чтобы реагировать на подозрительные транзакции.

• обучать ребенка, как поступать в случае подозрительных звонков, указать номера телефонов, по которым несовершеннолетний может связаться с родителями или другими близкими.

• в случае угрозы со стороны незнакомых людей следует обязательно обратиться к родителям или родственникам.

• уделять внимание не только собственной финансовой безопасности, но и обучению детей базовым правилам

Одна из схем — запугивание через 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 банковской карты для получения «приза» или предлагают приобрести игровую валюту, например, в Roblox. Несовершеннолетние берут деньги из дома и переводят мошенникам.

ГУ МВД России по Саратовской области

ПРЕДУПРЕЖДАЕТ о новом виде мошенничества - вовлечение детей

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