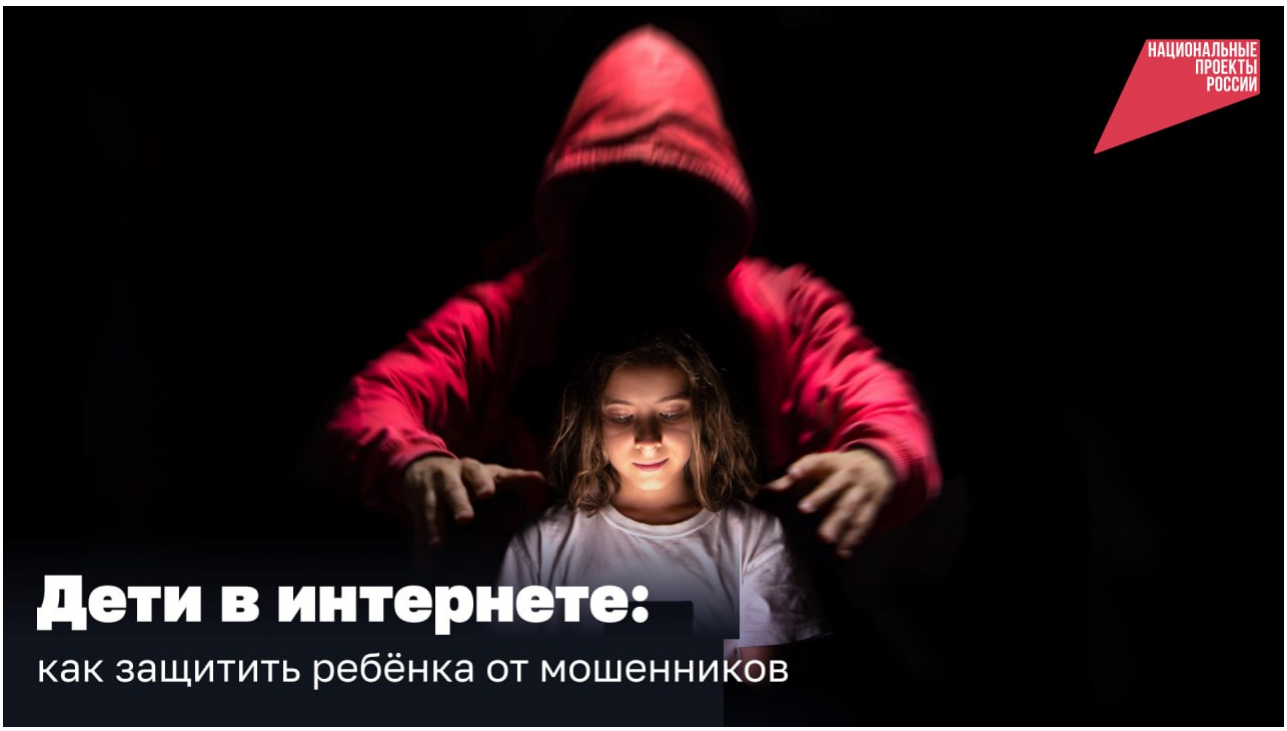

В последнее время участились случаи хищения денежных средств с банковских счетов путем обмана несовершеннолетних абонентов мобильных операторов и пользователей. Дети из-за небольшого жизненного опыта доверчивы, и если их не научить, как распознавать мошенников, последствия могут быть катастрофическими для семейного бюджета.

Чаще всего мошенники связываются с детьми:

- **В играх**. Обманщики заводят дружбу с детьми в чатах мобильных или компьютерных игр. Нередко выдают себя за популярных блогеров и просят выполнить «задания», чтобы получить подарки, редкие игровые артефакты, игровую валюту или скины. Задания обычно заключаются в том, чтобы прислать фото документов, личные фото, данные банковских карт.
- **В мессенджерах и соцсетях**. Преступники могут выходить на детей в Телеграмм – чатах, в группах популярных соцсетях. Намерения те же – выудить информацию, которую можно использовать для своего обогащения.

Как мошенники обманывают детей:

- **Просят перейти по ссылке, скачать файл или приложение.** Мошенник, установив контакт с ребенком, может отправить ему ссылку или файл и попросить открыть, чтобы «выполнить задание» и получить за это подарки. Часто ссылка имитирует страницу банковского сайта. Мошенники в качестве задания могут попросить ребенка ввести на этой странице данные банковских карт родителей. После этого с деньгами на карте можно попрощаться. Злоумышленники также могут предложить считать QR – код или сформировать его в приложении и переслать им. могут попросить подтвердить действие с телефона родителей или попросить

сообщить код под предлогом авторизации, регистрации или участия в розыгрыше или опросе.

- **Предлагают купить внутриигровую валюту, артефакты, скины.** Среди детей популярны мобильные игры, многие из них имеют собственные магазины, где продают внутриигровую валюту, скины, артефакты. Мошенники заводят дружбу с ребенком и предлагают купить у них цифровой контент дешевле, чем в магазине. Или приобрести аккаунт уже с большим количеством купленных артефактов. Ребенок переводит деньги, но никакого цифрового контента или аккаунта не получает.
- **Обещают легкий заработок или призы в интернете.** Часто мошенники предлагают подросткам подработку в интернете и быстрый заработок. Они могут присылать подобные предложения в мессенджер, в чаты, зазывать детей через короткие ролики на популярных видеосервисах, всплывающие рекламные баннеры и т.д., указанные заработки частую являются незаконными, что приводит к совершению ребенком правонарушений или преступлений. Ещё ребенку могут прислать сообщение, что он выиграл суперприз, но чтобы его получить его, нужно заплатить.
- **Втягивают в дропперство.** Дропперство – это вывод чужих денег с чужих банковских карт через подставных лиц. Работает это так: подростку предлагают оформить дебетовую карту (её можно оформить с 14 лет) и за денежное вознаграждение отдать её мошенникам. Затем злоумышленники переводят на неё украденные с чужих карт средства и снимают. Подросткам также предлагают «привести друга», то есть вовлечь других детей дроппинг, за каждого обещают заплатить пару тысяч рублей. Участвуяв подобных схемах, подросток может получить наказание за соучастие в мошенничестве.
- **Взламывают аккаунты друзей и с них просят помощи.** Мошенники, заполучившие доступ к аккаунту подростка, рассылают его друзьям сообщения с просьбой одолжить денег или перейти по ссылке, чтобы проголосовать за знакомого в онлайн – конкурсе.
- **Открыто угрожают и манипулируют.** Некоторые преступники предпочитают действовать более грубо и прямолинейно – шантажируют, манипулируют, угрожают. Например, могут написать, что родителям или кому-то из друзей угрожает опасность, и нужно срочно прислать деньги или данные банковских карт, и случае если ребенок не переведет деньги, либо не отдаст ценные вещи, которые находятся дома, то родителям или другим близким может грозить тюремное заключение и т.п. Также, киберворы завоевав доверие ребенка, вытягивают из него личную информацию или фото, а потом шантажируют, угрожая разослать компрометирующие данные его друзьям и родственникам.

Как обеспечить безопасность детей в сети Интернет

1.) Проверять переписку в социальных сетях на предмет наличия противоправного контента, а также наличия второго аккаунта.
2.) Проверять историю браузера.
3.) Проверять установленные платежные системы и транзакции, которые осуществляются с их помощью.
4.) Подключить функцию «Родительский контроль» на телефоне Вашего ребенка. Данная функция предназначена для того, чтобы оградить Вашего ребенка от противоправного контента, расположенного в открытом доступе в сети Интернет.

В целях предупреждения дистанционных мошенничеств и краж в отношении вас и ваших детей убедительно просим провести с детьми разъяснительные беседы и соблюдении простых рекомендаций, которые помогут Вам сохранить денежные средства и ценности:

- не сообщать посторонним лицам реквизиты банковских карт, код из СМС или push
- уведомлений;
- не разговаривать по телефону или через мессенджеры с незнакомыми людьми;
- сохранять приватность: в социальных сетях и мессенджерах нельзя раскрывать личную информацию, например домашний или школьный адрес, имена и номера телефонов родителей, а также отмечать места, где они часто бывают;
- не встречаться с незнакомыми людьми из интернета без ведома родителей
- не сообщать логины, пароли и другую конфиденциальную информацию;
- отключать возможность оплаты привязанной к аккаунту картой, если ребенок имеет доступ смартфону или компьютера родителей по возможности ограничить такой доступ;
- погрузитесь в онлайн-мир ребенка, проявите интерес к тому, что делает ребенок, какие сайты посещает, какие видео смотрит, с кем общается;
- установите ПИН – код на сим карту устройства, чтобы предотвратить её использование на других устройствах.

Помните: если Вы и Ваши близкие стали жертвами мошенников, или Вы подозреваете, что в отношении Вас планируются противоправные действия – незамедлительно обращайтесь в правоохранительные органы!