Несовершеннолетний, размещая в информационно-телекоммуникационной сети «Интернет» информацию о себе, вступая в переписку с незнакомыми людьми, просматривая запрещенный контент, подвергается риску стать жертвой или соучастником преступлений.

В связи с чем, ребенок должен знать о правилах безопасности поведения в информационно-телекоммуникационной сети «Интернет», соблюдение которых позволит не стать жертвой или соучастником преступлений.

Основные схемы обмана:

взламывание аккаунтов несовершеннолетних и создание злоумышленниками «фейковых» интернет-страниц, посредством которых происходит общение с друзьями детей и убеждение перевести денежные средства на подконтрольные банковские счета. Фейковые аккаунты создаются в различных информационных ресурсах – «Вконтакте», «Телеграмм»;

получение, в том числе в результате взлома страниц социальных сетей личную информацию или фотографии, в том числе интимного содержания, и вымогательство денежных средств под угрозой их распространения друзьям, знакомым или родственникам;

размещение на сайтах онлайн-торговли ложных объявлений о продаже товаров и получение за них предоплаты, передача несовершеннолетнему ссылки, использование которой предоставляет удаленный доступ к платежным средствам, либо переход по ней создает возможность для списания денежных средств со счетов ребенка или его родителей;

создание «фишинговых» (поддельных) торговых площадок, визуально схожих с реальными - «Авито», «Юла» и т.п., где мошенники склоняют подростка перейти на фишинговую страницу, привязать банковскую карту и ввести логин и пароль;

заработок на бирже, вложение в инвестиции (обещание быстрого дохода при минимальных вложениях);

онлайн-игры, в которых можно встретить предложения о покупке игровых предметов за денежные средства. Ребенку также могут прислать сообщение, что он выиграл приз, но, чтобы получить его, нужно заплатить. Могут попросить подтвердить определенные действия с телефона родителей или сообщить код с целью регистрации или участия в розыгрыше или опросе;

направление сообщений от имени родственников, знакомых с просьбой перечислить денежные средства в долг и т.п.;

совершение злоумышленниками звонков от имени сотрудников правоохранительных органов, например, сообщение об участии родственников в дорожно-транспортных происшествиях и о необходимости передачи денежных средств для заглаживания морального вреда перед иными участниками ДТП или срочного оказания медицинской помощи;

сообщение потерпевшим о необходимости участия в противодействии преступной деятельности, высказывания угроз привлечения к уголовной ответственности за спонсирование террористов, на счета которых якобы были переведены деньги;

сообщение потерпевшему о взломе личного кабинета в электронных ресурсах («Госуслуги», «Сбербанк онлайн» и т.п.) и необходимости в связи с этим перевода денежных средств на счет третьего лица;

сообщение потерпевшему по телефону, в переписке в мессенджерах о попытках неустановленных лиц получить кредит на имя потерпевшего, необходимости оформить «зеркальную» заявку или перевести денежные средства на «безопасные» счета.

Основное правило безопасности, которое должны знать дети: в любой непредвиденной ситуации необходимо посоветоваться с родителями (законными представителями) или со взрослым, которому ребенок доверяет.

Чтобы не стать жертвами мошенников, следует придерживаться следующих советов:

1. Всегда перепроверять полученную информацию, которую сообщают злоумышленники – перезвонить родственникам либо на горячую линию банка, либо в дежурную часть органов полиции, приемную государственного органа и т.п.

2. Не сообщай персональные данные (ФИО, дата рождения, домашний адрес, паспортные данные, номера телефонов и реквизитов банковских карт, пароли) в переписках, комментариях, онлайн-играх. Не оставлять геометки под фото, по ним злоумышленники легко узнают, где живет и учится ребенок.

3. Не сообщай никому реквизиты вашей банковской карты. Ни одна организация, включая банк, не имеет право требовать данные вашей пластиковой карты. Чтобы проверить поступившую информацию о блокировании карты, следует позвонить в клиентскую службу поддержки банка. Скорее всего, вам ответят, что никаких сбоев на сервере не происходило, а ваша карта продолжает обслуживаться банком.

4. Перепроверять информацию о помощи друзьям или родственникам. Если получили сообщение о том, что родственник попал в беду, нужно перезвонить ему и перепроверь информацию. Никогда не переводите деньги, если об этом просит знакомый в социальной сети, возможно мошенники взломали его аккаунт. Сначала необходимо связаться с этим человеком и узнать, действительно ли ему нужны деньги.

5. Установить самозапрет на выдачу кредитов, в том числе в личном кабинете на портале «Госуслуги».

6. Не переходить по ссылкам на Интернет-сайты. Проверять ссылку (побуквенно) на соответствие официальному сайту. Скопировать ссылку и вставить в поисковике (Яндекс, Google и т. д.), прочитать комментарии.

7. Не покупать товары в интернет-магазинах по заниженной стоимости, часто за такие товары требуется внести предоплату, однако товар вы можете не получить.

8. Скачивать приложения с официальных источников. Не доверять сторонним приложениям. Если все-таки возникает необходимость использования сторонних приложений, то

внимательно нужно изучить его, прежде чем загружать на свое устройство.

9. Перед использованием носителя информации (CD-диск, USB Flash и т. д.) проверять его на наличие вредоносных программ.

10. Не верить всему, что пишут в сообщениях. SMS-сообщения могут быть весьма разнообразны, поэтому стоит критически относиться к таким сообщениям и не спешить выполнять то, о чем просят. Лучше позвонить оператору связи, узнать, какая сумма спишется со счета при отправке SMS-сообщения или звонка на указанный номер, затем сообщить о пришедшей на ваш телефон информации. Оператор определит того, кто отправляет эти SMS, и заблокирует его аккаунт.

11. Не верить в легкий заработок. Дети в поисках заработка могут быть очень наивны. Предупредите их, что порядочный работодатель никогда не попросит перевести деньги перед оформлением на работу.

За предложением легкого заработка в интернете, может скрываться склонение несовершеннолетних к преступной деятельности. Несовершеннолетнего вводят в заблуждение путем обещания денежных вознаграждений, а нередко путем запугивания и угроз, тем самым вовлекая в совершение преступлений.

«Дроппер» – участник мошеннических схем, подставное физическое лицо, оформившее на себя банковский счет или карту без цели реального управления финансами, передавшее их третьим лицам, которые совершают по ней незаконные финансовые операции.

Например, на карту дроппера обманутые люди переводят средства на так называемые «безопасные счета», а затем он должен перевести деньги другому человеку либо снять их.

С 05.07.2025 установлена уголовная ответственность для лиц, предоставляющих свои банковские карты и реквизиты в целях осуществления незаконных финансовых операций (дропперов) (ст. 187 Уголовного кодекса Российской Федерации).

Другие нововведения направлены против незаконного оборота сим-карт и учетных данных для доступа к аккаунтам (ст. 274.3, 274.4, 275.5 Уголовного кодекса Российской Федерации).

С 01.09.2025 уголовная ответственность будет наступать:

за незаконное использование абонентского терминала пропуска трафика или виртуальной телефонной станции;

за организацию деятельности по передаче абонентских номеров с нарушением требований законодательства, в том числе за участие в такой деятельности;

за организацию деятельности по передаче информации, необходимой для регистрации или авторизации пользователя Интернета для получения доступа к функциональным возможностям информационного ресурса, в том числе за участие в такой деятельности.

Прежде чем принять любое решение посоветуйтесь с родными и близкими, проверьте информацию, обдумайте последствия и все варианты развития событий.

Будьте бдительны! Не дайте себя обмануть!

В случае, если Вы или ваши родственники стали жертвой мошенников, срочно обратитесь в полицию по телефону «102».

ПРОКУРАТУРА АРХАНГЕЛЬСКОЙ ОБЛАСТИ И НЕНЕЦКОГО АВТОНОМНОГО ОКРУГА

Памятка как защитить ребенка от киберпреступности

г. Архангельск
2025 год