Информационно-справочные материалы
по основным схемам преступных действий,
совершаемых в отношении несовершеннолетних
с использованием информационно-
коммуникационных технологий

Стремительный рост применения информационных технологий, широкое вовлечение в интернет-среду процессов, связанных с жизнедеятельностью общества и государства, помимо несомненного положительного эффекта, порождают новые вызовы и угрозы использования сети Интернет в преступных целях.

Наряду с возможностями быстрого получения в неограниченном объеме разнообразной информации, повышения уровня знаний, глобальная сеть Интернет расширяет пространство общения. Особенно актуальным это является в молодежной среде, где триггером к началу коммуникации зачастую выступают чаты игровых платформ.

Злоумышленники активно их используют для совершения преступлений. Основные способы совершения противоправных действий в отношении детей следующие.

В чате онлайн-игры «Minecraft» под предлогом установки ее бесплатной версии и бонусов к ней *(моды, скины, или специальные версии)* преступник предлагает несовершеннолетнему обсудить условия сделки в мессенджере *(Telegram, WhatsApp, Viber и др.).* В ходе переписки он выясняет, есть ли у подростка в пользовании устройства марки «Apple». Если ребенок это подтверждает, то ему предлагается перейти по предложенной ссылке, отключить защиту и установить указанное злоумышленником приложение. Таким образом, он входит в чужой Apple ID и тем самым передаете мошеннику управление своим устройством «Apple». После этого последний переводит гаджет в режим блокировки, в результате чего потерпевший не может его использовать. Для разблокировки телефона преступник требует денежное вознаграждение и нет гарантии, что, получив деньги, он разблокирует гаджет.

Также, злоумышленники могут заполучить доступ к Apple ID через установку так называемой «обновленной версии» «TikTok».

Все начинается с того, что мошенники в социальных сетях и мессенджерах размещают видеоролики, в которых они рассказывают, как установить улучшенную версию «TikTok», содержащую в себе новые функции и интерфейс. Если пользователь заинтересовался этим, ему высылается ссылка и инструкция по установке.

После перехода по ней из своего Apple ID пользователь попадает в Apple ID злоумышленника. Он тут же меняет пароль и телефон

оказывается заблокированным. Затем начинается шантаж: за деньги обещают вернуть доступ.

Практически похожий по сценарию случай, связанный с блокировкой Apple ID, используется мошенниками, предлагающими в «TikTok» установку приложения, позволяющего отслеживать переписку в мессенджере «Telegram». Пройдя по ссылке для его скачивая, телефон блокируется.

Также в ходе онлайн-игр *(Minecraft, Roblox и др.)* в игровых чатах размещается информация о возможности приобретения улучшений, позволяющих развить игровых персонажей. Мошенники обещают детям предоставить их после перевода оговоренной суммы денежных средств. Вместе с тем после оплаты переписка удаляется, а контакт ребенка блокируется.

Суть еще одной из схем заключается в том, что злоумышленник знакомится с несовершеннолетним в мессенджере, социальных сетях или чатах онлайн-игр. В ходе общения выясняет возраст, а потом выдает себя за сверстника. В беседе предлагает в обмен на бонусы к играм *(моды, скины, или специальные версии, игровые деньги и т.д.)* отправить ему личные фотографии или видеозаписи интимного характера. После их получения, преступник угрожает размещением указанных материалов в общем доступе сети Интернет, направлением их родителям, знакомым или одноклассникам, если ему не будут переведены деньги.

Для того чтобы достигнуть своих целей, преступники зачастую скрываются под «маской».

Они звонят в мессенджере и представляются работниками «Белпочты» или операторами сотовой связи, под различными предлогами пытаясь узнать персональные данные родителей.

После их получения осуществляется второй звонок якобы от представителя правоохранительных органов. Ребенку сообщается о том, что персональные данные родителей, которые он только что предоставил, оказались в руках мошенников. В результате на его родителей оформлены банковские счета, через которые перечислены крупные суммы денег, добытые преступным путем. Подростку начинают угрожать привлечением родителей к уголовной ответственности, лишением их родительских прав и помещением его в детский дом. Чтобы этого избежать, предлагают их «спасти», но с определенным условием. Для этого необходимо выполнить процедуру обязательного «декларирования» денежных средств, находящихся дома. Злоумышленник предлагает передать имеющиеся семейные сбережения или оставить их в условленном месте для проведения процедуры

«декларирования» или зачисления на «безопасный счет». При этом детям категорически запрещают рассказывать об этом кому-либо. После того, как ребенок передает сбережения, сведения о входящих звонках и переписке удаляются преступником.

Для того чтобы обезопасить детей в Интернете, необходимо соблюдать следующие рекомендации:

аккаунт и устройство должны быть максимально защищены от взлома. Необходимо использовать надежный пароль и двухфакторную аутентификацию.

Справочно.

Настройка двухфакторной аутентификации.

«Telegram» – Настройки – Конфиденциальность – Двухэтапная аутентификация (или облачный пароль для IPhone);

«Viber» – Настройки – Конфиденциальность – Двухэтапная проверка;

«WhatsApp» – Настройки – Аккаунт – Двухшаговая проверка.

не следует разрешать свободно добавлять свой аккаунт в чаты или группы, так как они могут оказаться незаконными или потенциально опасными;

не нужно открывать сообщения или принимать запросы от незнакомых пользователей, так как в его сообщении или запросе может скрываться вредоносная программа или другой опасный контент;

немедленно сообщать родителям или в милицию (по телефону 102 или в чат-бот МВД «Мы всегда рядом») о том, что кто-то просит или требует фото или видео без одежды, в плавках или купальнике, нижнем белье, в откровенных позах;

не сообщать коды без проверки отправителя и не переходить по ссылкам;

все платежи следует осуществлять через официальные банковские приложения или сайты;

государственные органы и банки никогда не требуют передать наличные денежные средства через курьера и не звонят посредством мессенджеров;

термина «безопасный счет» не существует. Никому не следует сообщать PIN, SMS коды или полные данные банковской платежной карты по телефону;

невозможно купить IPhone или шубу в 10 раз дешевле, при условии, что за это требуется предоплата;

любые угрозы «арестом родителей» – 100 % манипуляция;

не следует передавать личную информацию в ответ на сообщения с неизвестных номеров.

В случае если несовершеннолетний пострадал от действий мошенников с использованием информационно-коммуникационных

технологий, необходимо незамедлительно:

сообщить родителям и в милицию по телефону 102 или в чат-бот МВД «Мы всегда рядом»;

сделать скриншоты переписки и не удалять телефонные номера злоумышленников;

блокировать банковскую карту или счет.

МВД Республики Беларусь