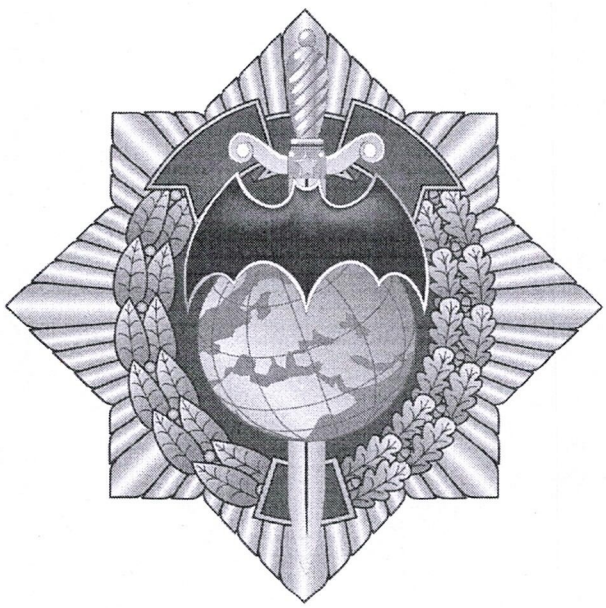
Министерство внутренних дел Республики Беларусь

Управление внутренних дел Витебского областного исполнительного комитета

Криминальная милиция

УПРАВЛЕНИЕ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ



ПЛАН-КОНСПЕКТ
на тему: «Способы совершения киберпреступлений в отношении детей и подростков»

г. Витебск

Введение

В нынешних реалиях Интернет стал неотъемлемой частью нашей жизни: информацию мы черпаем, посещая различные сайты, сообщества, чаты и группы, общаемся, используя социальные сети и мессенджеры. Вы должны осознавать, что Интернет – это не только удобный инструмент для приумножения знаний и коммуникации со сверстниками, но и источник скрытой опасности.

В первую очередь нужно помнить о том, что те, кто находятся по ту сторону экрана, не всегда преследуют безобидные цели. Злоумышленники в ходе электронных переписок и иного общения на сайтах знакомств, в социальных сетях, мессенджерах и даже детских онлайн-играх могут совершать в отношении вас противоправные действия или втягивать в преступную деятельность.

Способы киберпреступлений в отношении детей и подростков.

- **«бесплатные» подарки и розыгрыши**. Для получения выигрыша вам предлагается перейти по ссылке и ввести платежные и иные данные родителей. Основная цель – украсть данные банковских карт или учетных записей;
- **«фейковые» запросы от друзей**. С использованием взломанного аккаунта друга вас просят помочь перевести ему денежные средства. Такие образом деньги поступят не вашему другу, а преступнику;
- **«груминг»**. Злоумышленник под видом сверстника втирается к вам в доверие в соцсетях или играх, постепенно выведывая личную информацию, и шантажирует ее распространением в дальнейшем;
- **«сексторшен»**. Преступник, заполучив ваши интимные фото или видео (добровольно отправленные или путем взлома вашей учетной записи), начинает шантажировать, вымогая как реальные деньги, так и услуги сексуального характера.

Повышенную бдительность следует проявлять в случае, если происходит общение в сети с неизвестным вам пользователем. Особая осторожность – в чатах онлайн-игр и мессенджеров!

Мошенник в чате онлайн-игры «Minecraft» под предлогом установки ее бесплатной версии и бонусов к ней *(моды, скины, или специальные версии)* предлагает обсудить условия сделки в мессенджере *(Telegram, WhatsApp, Viber и др.)*. В ходе переписки преступник выясняет, есть ли у вас в пользовании устройства марки «Apple». Если вы это подтверждаете, предлагается выйти из своей учетной записи ICloud

и войти в предложенную собеседников. Таким образом, вы входите в чужую учетную запись ICloud и тем самым передаете мошеннику управление своим устройством «Apple». После этого злоумышленники переводят гаджет в режим блокировки, в результате чего его нельзя использовать. Для разблокировки требуют денежное вознаграждение и нет гарантии, что, получив деньги, Ваш гаджет разблокируют.

Аналогично, злоумышленники могут заполучить доступ к вашему Apple ID следующими способами: через установку «обновленной версии» «ТікТок».

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

После перехода по указанной ссылке из своего Apple ID пользователь попадаете 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 «ТікТок» установку приложения, позволяющего отслеживать переписку в мессенджере «Telegram». Пройдя по ссылке для его скачивая, телефон заинтересованного лица блокируется.

Важно! Если ваш аккаунт заблокирован, разблокировка возможно только через официальную техподдержку Apple при наличии документов, подтверждающих покупку устройства.

В ходе онлайн-игр *(Minecraft, Roblox и др.)* в игровых чатах размещается информация о возможности приобретения улучшений, позволяющих развить игровых персонажей. Мошенники пообещают вам предоставить их после перевода оговоренной суммы денежных средств. Вместе с тем после оплаты переписка удаляется, а ваш контакт блокируется. Вы останетесь ни с чем!

В социальных сетях или чатах онлайн-игр злоумышленник знакомится с вами в мессенджере, 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 вы не переведете ему деньги.

Мошенники могут звонить вам в мессенджере и представляться работниками «Белпочты» или операторами сотовой связи, под

различными предлогами будут пытаться узнать персональные данные родителей.

После их получения осуществляется второй звонок, якобы от представителя правоохранительных органов. Вам сообщат о том, что персональные данные родителей, которые вы предоставили, оказались в руках мошенников, в результате чего на маму или папу оформлены банковские счета, через которые перечислены крупные суммы денег, добытые преступным путем. Вам будут угрожать привлечением родителей к уголовной ответственности, лишением их родительских прав и помещением Вас в детский дом. Чтобы этого избежать, предложат их «спасти», но с определенным условием: необходимо выполнить процедуру обязательного «декларирования» денежных средств, находящихся дома. Злоумышленник предложит передать имеющиеся семейные сбережения или оставить их в условленном месте для проведения процедуры «декларирования» или зачисления на «безопасный счет». Вам категорически запретят рассказывать об этом кому-либо. После того, как вы передадите сбережения, сведения о входящих звонках и переписке удаляются преступником.

В интернет-пространстве нужно быть предельно бдительными – всегда! Вступая в онлайн-диалог с незнакомыми пользователями, руководствуйтесь главным правилом: «Никогда не доверяй! Проверяй!».

Для того, чтобы обезопасить себя в Интернете, соблюдайте наши рекомендации:

ваш аккаунт и устройство должны быть максимально защищены от взлома. Используйте надежный пароль и двухфакторную аутентификацию;

установите настройки приватности и закройте личный аккаунт для посторонних пользователей;

проверяйте адрес страницы, где вводите данные банковской карты (для белорусских организаций в адресной строке должно быть так: «название сайта».BY/«раздел сайта»);

помните, что любую информацию преступник может использовать для достижения своих незаконных целей;

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 любой из них может оказаться преступником, а в его сообщении или запросе может скрываться вредоносная программа или другой опасный контент;

немедленно сообщите родителю, другому взрослому или в милицию (по телефону 102 или в чат-бот МВД «Мы всегда рядом») о том, что

кто-то просит или требует у вас фото или видео без одежды, в плавках или купальнике, нижнем белье, в откровенных позах, а также встретиться, обсудить интимные отношения, посмотреть откровенные фото или видео;

не сообщайте коды без проверки отправителя и не переходите по ссылкам;

все платежи следует осуществлять через официальные банковские приложения или сайты;

не забывайте, что государственные органы и банки никогда не требуют передать наличные через курьера и не звонят в мессенджеры;

термина «безопасный счет» не существует. Никто не имеет права требовать у Вас PIN-, SMS-коды или полные данные банковской платежной карты по телефону;

помните, что нельзя купить IPhone или шубу в 10 раз дешевле, тем более, если за это просят предоплату;

любые угрозы «арестом родителей» – 100% манипуляция;

не передавайте личную конфиденциальную информацию в ответ на сообщения с неизвестных номеров.

В случае если Вы поняли, что пострадали от действий злоумышленников, необходимо незамедлительно:

сделать скриншоты переписки и не удалять телефонные номера злоумышленников;

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

блокировать банковскую карту или счет.

Сдача аккаунта в аренду

Сегодня в сети Интернет можно встретить многочисленные предложения сдать свой аккаунт в мессенджерах за вознаграждение (звезды, монеты и др.). Это очередной способ «легкого» заработка, который может привести к серьезным последствиям. Целевой аудиторией становятся дети и подростки, для которых выплачиваемое вознаграждение может показаться значительным. Злоумышленники вовлекают молодежь в тематических каналах, в чатах онлайн-игр, в сообществах, уверяют, что аренда аккаунта – эта легальный способ заработка. Важно понимать, что через арендованные аккаунты мошенники обманывают граждан, шантажируют, используют в различных целях. Наиболее распространенные сценарии включают: распространение спама и фишинговых ссылок, проведения мошеннических операций, создание фейковых профилей для выманивания денег у других пользователей. Любая передача доступа к своему аккаунту третьим лицам, является крайне небезопасной практикой. Если аккаунт был использован для преступной деятельности, значить, в первую очередь правоохранители придут к его формальному владельцу. Гражданин, сдавший аккаунт,

рискует оказаться соучастником. В зависимости от тяжести совершения противоправного деяния возможно реальное лишение свободы.

Дропы

Для получения за границей похищенных денег, а также для запутывания «цифровых следов» мошенникам необходимо перевести их через промежуточные счета, открытые в белорусских банках на подставных лиц, так называемых «дропов».

В нашей стране открыть банковский счет может гражданин с 14 лет, с разрешения законных представителей, то есть даже несовершеннолетние могут открыть банковские счета. Этим и пользуются преступники. Находясь за границей, злоумышленники подбирают лиц, которые согласятся открыть банковский счет на свое имя и продать за небольшую сумму реквизиты доступа к нему – это логины и пароли для входа в личный кабинет интернет-банкинга, а также предоставить разовый СМС-код.

Поиск дропов

Напрямую мошенники в интернете не могут размещать объявления о поиске таких лиц, поэтому свой интерес они прикрывают предложением различного другого заработка, не вызывающего подозрения. Например, в Telegram рассылают объявления о поиске курьеров в любом городе со стабильной оплатой труда, или людей для разгрузки товаров, или людей на вакансию «тайный покупатель», или заманивают обещанием высокой и быстрой оплаты.

Чаще всего отзываются на такие вакансии лица с нестабильным или небольшим доходом, в большинстве – молодежь. Сначала инициатор объявления разочаровывает заинтересовавшегося подработкой, сообщает, что данная вакансия уже закрыта, и тут же предлагает иной вид заработка, например, оформить банковский счет и передать за вознаграждение данные для доступа к нему.

Кроме похищенных киберпреступниками денег по промежуточным счетам также могут проводиться деньги, полученные от незаконного оборота наркотиков. Ответственность за возникновение прошедших по банковским счетам денег несут владельцы таких счетов.

Ответственность

Надо знать, что статьей 222 Уголовного кодекса предусмотрена уголовная ответственность за распространение из корыстных побуждений находящихся в незаконном владении лица реквизитов банковских платежных карточек либо аутентификационных данных, посредством которых возможно получение доступа к счетам, электронным или виртуальным кошелькам. За предоставление своих личных данных для

использования в мошеннических схемах предусмотрена административная ответственность по статье 12.35 Кодекса Республики Беларусь об административных правонарушениях.

Имеются факты, когда в преступную деятельность вовлекались несовершеннолетние.

ЧТОБЫ НЕ СТАТЬ ЖЕРТВОЙ КИБЕРПРЕСТУПНИКОВ

Запомните следующие правила:

– если незнакомый заводит беседу про ваши деньги, прекратите разговор;

– не доверяйте незнакомым и не выполняйте то, о чем они просят, даже если обещают помощь в сохранении денежных средств;

– не устанавливайте непроверенные программы на свои электронные устройства по указанию незнакомых;

– не забывайте, что мошенники могут представляться вымышленными данными, использовать для подтверждения личности фотографии чужих паспортов, чужие аккаунты в соцсетях, чужие абонентские номера.

– сотрудники правоохранительных органов и работники банков не звонят в мессенджерах и не просят оформить кредит или оказать содействие в поимке злоумышленников, а также не предлагают застраховать и обезопасить денежные средства;

– обращайте внимание на абонентские номера, с которых вам звонят в мессенджерах, чаще всего абонентские номера, с которых звонят злоумышленники, принадлежат иностранным государствам;

– не переводите деньги на «защищенный счет»;

– не сообщайте неизвестным лицам свои персональные данные, реквизиты банковских карт, SMS-коды;

– не переходите по ссылкам от неизвестных пользователей;

– при поступлении подобных звонков немедленно прекратите разговор и сообщите о произошедшем в милицию.

«Цифровая грамотность»

Рекомендуем подписаться на Телеграм-канал «**Цифровая грамотность**» (ссылка-приглашение «**t.me/cifgram**»), где на регулярной основе публикуется актуальная информация о способах совершения киберпреступлений и методах противодействия им.

Управление по противодействию киберпреступности
КМ УВД Витебского облисполкома