Информационный материал
по профилактике преступлений
с использованием информационно
-коммуникационных технологий
для проведения разъяснительной
работы среди несовершеннолетних
и их законных представителей

На данный момент Интернет – это не только удобный инструмент для приумножения знаний и коммуникации, но и источник скрытой опасности.

С его помощью злоумышленники нашли способ обманывать самую доверчивую категорию – наших родителей и несовершеннолетних детей.

На данный момент самым распространенным видом преступлений, совершаемым в отношении них с использованием информационно-коммуникационных технологий, является **блокирование мобильных устройств Apple.**

Механизм блокирования мобильных устройств Apple реализуется не путем взлома операционной системы, а посредством методов социальной инженерии с использованием доверчивости детей.

Так, злоумышленник под различным предлогом вынуждает ребенка выйти из своего аккаунта Apple (iCloud) и войти на iPhone в «мошеннический» аккаунт, для чего предоставляют логин (адрес электронного почтового ящика) и пароль. С этого момента мобильный телефон жертвы «в руках» вымогателя. Он изменяет пароль от учетной записи, знание которого требуется для выхода из нее, после чего удаленно через облачный сервис iCloud активирует функцию «Найти iPhone», переводя таким образом устройство в режим пропажи, и полностью блокирует его.

Далее потерпевшему приходит сообщение (либо выводится на заблокированном экране), что телефон заблокирован, а для его разблокировки необходимо заплатить деньги. Также зачастую предоставляется контакт в Telegram лица, способного решить этот вопрос (как правило, это и есть злоумышленник, заблокировавший телефон). Характерно, что даже при выполнении требования вымогателя разблокировка устройства в подавляющем большинстве случаев не осуществляется.

Существует несколько основных предлогов, вынуждающих детей войти на своих устройствах в мошеннический аккаунт Apple.

Предлог 1. Реклама бесплатных игр и приложений в социальных сетях и мессенджерах.

Злоумышленники осуществляют размещение рекламы (чаще всего видеоролик в TikTok либо в Telegram), в которой указывается бесплатный

способ скачать на iPhone то или иное приложение (AyuGram, Telegram Premium, позволяющие читать удаленные сообщения, забирать «звезды», скрывать статус онлайн и т.д.), игру («MINECRAFT», «PUBG Mobile», «Standoff 2» и др.) либо мод, получить на свой баланс игровую валюту.

Для установки данных предложений злоумышленники предлагают жертве войти на телефоне в предоставленный ими аккаунт Apple (iCloud).

Предлог 2. Трудоустройство.

Злоумышленник осуществляет размещение рекламы в сети Интернет о поиске сотрудника на вакансию, как правило, связанную с тестированием мобильных приложений для устройств Apple. После удачного «прохождения собеседования» потенциальному работнику предоставляется логин и пароль для входа в якобы корпоративный аккаунт Apple, который должен использоваться для работы либо загрузки необходимых приложений.

После входа соискателя на своем iPhone в предоставленную учетную запись Apple он оказывается в ловушке. Затем происходят события, аналогичные описанным выше.

Следует отметить, что работники сервисных центров не оказывают услуги по восстановлению устройств Apple либо учетных записей iCloud, заблокированных мошенниками. Разблокировать такое устройство возможно только путем обращения в службу технической поддержки компании Apple, приложив документы, подтверждающие законность его приобретения.

Процесс восстановления занимает от нескольких дней до недели, при этом устройство может быть сброшено до заводских настроек (все данные удалятся).

К примеру, в г. Гомеле несовершеннолетняя А., 2008 г.р., во время просмотра видеороликов в социальной сети «ТикТок» увидела ролик о том, что, перейдя по учетной записи, указанной в ролике, можно восстановить удаленный аккаунт в мессенджере «Телеграм», что последняя и сделала. В дальнейшем телефон А. был заблокирован и пришло сообщение о том, что для того, чтобы разблокировать телефон, необходимо с другого телефона выполнить те же условия. Помочь А. решилась ее подруга Е., 2008 г.р., мобильный телефон которой в дальнейшем также был заблокирован.

Запомните:

- никогда и не под каким предлогом не входите на своем мобильном устройстве в чужую учетную запись Apple, даже, если вас об этом просит друг и тем более – незнакомый человек из интернета;
- никому не сообщайте ваши логин и пароль от аккаунта Apple;

- не переходите по неизвестным ссылкам, пересланным вам незнакомым человеком; не вводите на посторонних сайтах свои логин и пароль от аккаунта Apple (iCloud).

Детей младшего школьного возраста злоумышленники обманывают следующим образом. Ребенку в мессенджере поступает звонок от имени работника РУП «Белпочта» или операторов сотовой связи, которые под различными предлогами **пытаются узнать персональные данные родителей,** либо просят сообщить код из отправленного ими SMS-сообщения.

После их получения осуществляется второй звонок якобы от представителя правоохранительных органов. Несовершеннолетнему сообщается о том, что он предоставил персональные данные мошенникам. В результате этого на их имя оформлены банковские счета, через которые перечислены крупные суммы денег, добытые преступным путем. Затем подростку угрожают привлечением родителей к уголовной ответственности из-за него. Чтобы этого избежать, предлагается «спасти родителей», для чего необходимо выполнить процедуру обязательного «декларирования» денежных средств, находящихся дома. Ребенку под угрозой ареста или заключения под стражу родителей предлагается передать имеющиеся в доме денежные средства или оставить их в указанном злоумышленником месте для проведения процедуры «декларирования» или зачисления на «безопасный счет». При этом детям категорически запрещают рассказывать об этом кому-либо. После передачи сбережений сведения о входящих звонках и переписке удаляются преступником.

К примеру, несовершеннолетнему П., 2013 г.р., жителю г. Мозыря, поступил звонок по мессенджеру «Viber» от лжеправоохранителя, который сообщил, что его родители получили деньги из Украины и это является преступлением. Чтобы родителей не посадили в тюрьму, необходимо все денежные средства, находящиеся в доме, передать ему, а о произошедшем родителям не рассказывать. Поддавшись мошенникам, несовершеннолетний П. передал курьеру 10400 долларов США и 800 евро, принадлежащих его родителям.

Запомните:

- 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 данные банковской платежной карты по телефону;
- любые угрозы «арестом родителей» – 100 % манипуляция;
- нельзя передавать личную конфиденциальную информацию в ответ на сообщения с неизвестных номеров.

Продолжает использоваться **схема хищения денежных средств с использованием торговой площадки «Kufar»**. Так, мошенниками размещается информация о продаже товаров, пользующихся спросом у подростков (телефоны марки «Iphone», брендовые вещи, платья для бальных танцев и др.) по цене в разы ниже рыночной стоимости. Ребенок, видя выгодное предложение, направляет продавцу сообщение, в котором уточняет интересующие его вопросы относительно товара и способ его получения.

В случае договоренности, продавец предлагает покупателю оформить доставку товара через почтовое отправление (Белпочта, Европочта и др.), предварительно оплатив услуги доставки. Для этого ребенку в мессенджер высылается ссылка на мошеннический (фишинговый) сайт, который визуально схож с официальным сайтом сервисов доставки товаров и почтовых отправлений (Белпочта, Европочта и др.). Однако, в его названии, как правило, заменен один или два символа. В данной ссылке указывается незначительная сумма оплаты (как правило, 2 рубля) и необходимость обязательного введения номера банковской платежной карты и трехзначного CVV кода, размещенного на оборотной ее стороне.

Кроме этого, предлагается заполнить специальную графу «Баланс карты» или «Остаток денежных средств на банковской карте». Выполнив указанные требования, подростку-покупателю направляется код авторизации, который он сообщает мошеннику, тем самым предоставляет удаленный доступ к запрошенному им остатку на его банковской карте, который он указал. После совершение хищения, товар не высылается, а покупателя блокируют.

По итогам 7-ми месяцев т.г. в результате указанной противоправной схемы потерпевшими признано 15 подростков, которые пытались приобрести мобильный телефон марки iPhone (8), хоккейную экипировку и брендовую одежду (2), кухонную посуду (1).

Запомните:

- все платежи следует осуществлять через официальные банковские приложения или сайты;
- следует внимательно изучать предложения о покупке IPhone или шубы значительно дешевле.

В последнее время среди злоумышленников набирает популярность **вымогательство, связанное с угрозой распространения личной информации.**

В подавляющем большинстве случаев объектом преступления являются фотографии и видеозаписи интимного характера, переписка на сексуальную тему либо иная компрометирующая ребенка информация.

Первоначальная коммуникация злоумышленника и подростка происходит в приложениях либо на сайтах для знакомств (Mamba, Masked.love, Twinby, Mail.ru и др.) либо Telegram-чатах («Леонардо Дайвинчик» и др.), где мошенник выступает в качестве лица, противоположного пола, желающего познакомиться. Затем общение довольно быстро приобретает сексуальный подтекст. «Новый знакомый» предлагает обменяться интимными фотографиями. При этом для большей убедительности присылает заранее заготовленные якобы свои фотографии либо видео в обнаженном виде, а на самом деле скаченные в сети Интернет.

В случае если жертва «повелась» на данное предложение и сбросила свои интимные фотографии или видео, злоумышленник их сохраняет. Затем он сообщает, что распространит имеющиеся у него интимные фотографии потерпевшего среди его друзей и знакомых либо выложит в открытый доступ, если ему не заплатить за их нераспространение.

Запомните:

- никогда не отправляйте свои интимные фотографии и видео незнакомцам из Интернета;
- не оставляйте в сети Интернет о себе личную информацию и не делитесь с ней с незнакомцами;
- скройте данные о себе в настройках конфиденциальности в социальных сетях и мессенджерах;
- не переходите по неизвестным ссылкам, пересланным вам незнакомым человеком;
- не вводите на посторонних сайтах свои личные данные и коды из сообщений.

Вишинг выражается в осуществлении звонка на абонентский номер потерпевшего или в его аккаунт в мессенджере (в основном – это Viber или Telegram). В ходе голосового общения преступник представляется работником банка, правоохранительного органа, сферы социального обслуживания (МВД, КГБ, Следственного комитета, Департамента финансовых расследований, водоканала, домофонных систем, почты, сотрудника кампаний мобильных операторов связи) и под вымышленным предлогом (пресечение подозрительной транзакции, участия в специальной операции, якобы участия гражданина в спонсировании террористических организаций, в замены счетчиков воды, заключение договора на обслуживание домофона, получение почтовой корреспонденции, денежного перевода и т.д.) выясняет у потерпевшего сведения о наличии банковских платежных карточек, сроках их действия, CVV-кодах (трехзначный код на обратной стороне карты), паспортных данных, SMS-кодах с целью хищения денежных средств либо направляют фишинговую ссылку на поддельные сайты, на которых требуется ввести реквизиты банковских платежных карт. После их введения денежные средства

потерпевших списываются злоумышленниками. В ряде случаев злоумышленникам известны некоторые анкетные данные лиц, на имя которых они выпущены, что позволяет войти в доверие к жертве.

Например, неустановленное лицо путем телефонного звонка в мессенджере «Telegram» несовершеннолетнему К., 2010 г.р., представившись сотрудником правоохранительных органов, убедило последнего перевести денежные средства в размере 1950 рублей.

Следующий вид мошенничества – фишинг. Злоумышленники копируют дизайн известных сайтов («Европочта», «Госуслуги» и т.д.), создавая точную копию – фишинговый сайт. После жертвам отправляется ссылка на сайт, адрес которого лишь слегка отличается от оригинала. Лицо вводит данные банковской карты, реквизиты которой получают мошенники, получая доступ к находящимся на ней денежным средствам.

К примеру, неустановленное лицо, путем предоставления несовершеннолетней Я., 2008 г.р., ссылку на фишинговый ресурс «Европочта», в ходе общения по мессенджеру «Viber» получила доступ к банковскому счету последней, откуда похитила денежные средства в размере 290 рублей.

Запомните, в случае, если Вы или Ваши близкие пострадали от действий злоумышленников, необходимо незамедлительно:

сделать скриншоты переписки и не удалять телефонные номера злоумышленников;

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

заблокировать банковскую карту или счет.

Управление внутренних дел
Гомельского облисполкома