

ПРОФИЛАКТИКА СОВЕРШЕНИЯ ПРОТИВОПРАВНЫХ ДЕЙСТВИЙ В ИНТЕРНЕТ-ПРОСТРАНСТВЕ

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.

Именно поэтому сегодня мы обсудим актуальную и очень важную тему. Речь пойдет о том, как в Интернете не попасться в преступные сети и, находясь «онлайн», провести время прекрасно и безопасно!

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.

Интернет-преступники умело входят в доверие, могут выдавать себя за вашего сверстника, пользуются приемами психологического воздействия и манипуляции, искусно используют информацию о вас и ваших близких, размещенную на личной странице в соцсети или ту, которую вы сами же сообщили в переписке.

Помните: кто предупрежден, тот вооружен! Именно поэтому сейчас мы разберемся, какие опасности подстерегают подростков в сети:

- **«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

камеры), 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 перейти по предложенной ссылке, отключить защиту и установить указанное злоумышленником приложение. Таким образом, вы входите 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 гаджета преступник потребует денежное вознаграждение и нет гарантии, что, получив деньги, он разблокирует Ваш гаджет.

Кроме этого, злоумышленники могут заполучить доступ к Вашему Apple ID следующими способами:

через установку «обновленной версии» «ТикТок».

Все начинается с того, что мошенники в социальных сетях и мессенджерах размещают видеоролики, в которых они рассказывают, как установить улучшенную версию «ТикТок», 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 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 «ТикТок» установку приложения, позволяющего отслеживать переписку в мессенджере «Telegram». Пройдя по ссылке для его скачивая, телефон заинтересованного лица блокируется.

Также 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!

Суть еще одной из схем заключается в том, что злоумышленник знакомится с вами 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 вы не переведете ему деньги.

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

Они могут звонить вам в мессенджере и представляться работниками «Белпочты» или операторов сотовой связи, под различными предложениями 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. Настроить двухфакторную аутентификацию можно следующим образом: в мессенджере «Telegram» – «Настройки – Конфиденциальность – Двухэтапная аутентификация» (или облачный

пароль для iPhone), «Viber» – «Настройки – Конфиденциальность – Двухэтапная проверка», «WhatsApp» – «Настройки – Аккаунт – Двухшаговая проверка».

проверяйте адрес страницы, где вводите данные 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.

Спасибо за внимание! Желаю вам только безопасных будней, вне зависимости от того «онлайн» вы или «офлайн». Если у вас остались вопросы, буду рад дать на них ответы! Также можете обратиться ко мне в индивидуальном порядке.

Первый заместитель начальника ОВД
Ельского райисполкома

С.В.Мамонтов