Правила безопасности в Интернете

Реальность, в которой живут современные дети и подростки, несравнима с той, в которой воспитывались их родители.

Использование разнообразных информационных ресурсов оказывает значительное положительное воздействие на развитие детей – это увлекательно, это обучает и социализирует. Но не все понимают, что эти же средства могут представлять потенциальную угрозу в зависимости от того, как осуществляется их использование.

С какими угрозами могут столкнуться дети в сети Интернет?

1. Коммуникационные риски или риски общения

✓ *Интернет-хулиганство, киберпреследование, киберзапугивание (кибербуллинг).* Кибербуллинг – психологическое насилие в сети, информационное преследование со стороны сверстников, проявляющееся в виде издевательств, насмешек, запугиваний, прочих действий, которые негативно влияют на психическое состояние ребенка. У него создается ощущение безысходности, даже дома его не оставляет чувство тревоги, он впадает в депрессию. Информационная атака может привести к суициду.

Издевательство в сети наказуемо действующим законодательством. Согласно статьям 152, 153 Гражданского кодекса Республики Беларусь человек, которого оскорбили, может обратиться в суд с исковым заявлением о защите чести и достоинства. Также оскорбившего можно привлечь к административной ответственности по статье 10.2 Кодекса Республики Беларусь об административных правонарушениях. Для этого необходимо обратиться в отдел внутренних дел по месту жительства с заявлением.

✓ *Знакомства в Интернете и встречи с Интернет-незнакомцами.*

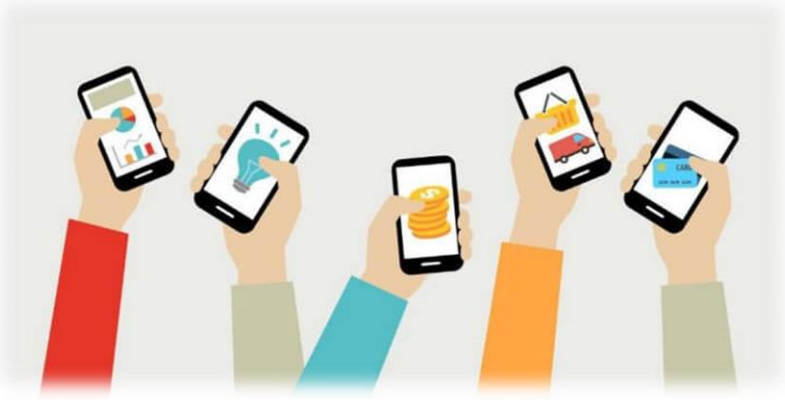
Общаясь в сети, дети могут знакомиться, общаться и добавлять в «друзья» совершенно неизвестных им в реальной жизни людей.

Социологические опросы об информационной безопасности детей и подростков в Интернет-сети приводят следующие данные о контактах: родственники – 43 %; виртуальные друзья – 21%; незнакомые люди – 36 %. Однако по большому счету виртуальные друзья – тоже незнакомцы. Таким образом, большую часть своего времени в сети дети уделяют общению с посторонними людьми, делятся своими переживаниями, секретами, планами. В таких ситуациях есть опасность разглашения ребенком личной информации о себе и своей семье. Каждое слово, каждая выложенная фотография, каждое действие в сети могут быть использованы против ребенка, и представляет собой благодатную почву для шантажа в будущем.

Особенно опасным может стать установление дружеских отношений с ребенком с целью личной встречи (груминг), вступления с ним в сексуальные отношения, шантажа и эксплуатации. Обман детей возможен, так как при общении в интернете не всегда точно можно сказать, кто на самом деле является твоим собеседником. Часто этим приемом пользуются педофилы, которые общаются с детьми от лица другого «ребенка» и предлагают встретиться в реальной жизни.

2. Потребительские риски

Сюда относится хищение персональной информации с целью кибермошенничества. Хищение конфиденциальных данных может привести к тому, что мошенник незаконно получает доступ и каким-либо образом использует личную информацию пользователя с целью получить материальную прибыль.



По информации пресс-службы Министерства внутренних дел Республики Беларусь в 2020 году зафиксировано 25,5 тысяч преступлений в сфере высоких технологий. Из них 23,5 тысячи – хищение денег с использованием компьютерной техники. Очень часто злоумышленники звонят в мессенджерах (приложения для переписки) якобы из банка и под разными предлогами узнают реквизиты, пин-код, трехзначный код на оборотной стороне карты.

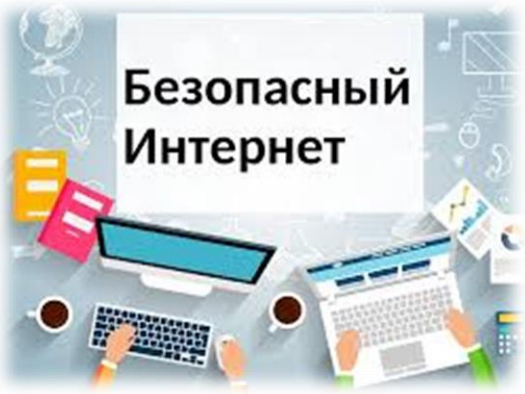
Сваттинг – это новый для Беларуси вид преступления. Хулиганы-геймеры отправляют в экстренные службы ложное сообщение об опасности от имени другого игрока. Во-первых, ложные сообщения отвлекают от оказания помощи тем, кто в ней действительно нуждается. Во-вторых, такими «разводами» геймеры могут доставить большие неприятности с законом своим оппонентам. По всему миру милиция успешно устанавливает личности этих геймеров.

В Беларуси за «сваттинг» предусмотрена ответственность по статье 340 Уголовного кодекса Республики Беларусь до 7 лет лишения свободы. Если геймер не достиг возраста привлечения к уголовной ответственности, то отвечать за него придется родителям.

Мошенники и способы их действия идут в ногу со временем. Неосведомленность и наивность детей делают их легкой добычей. Один из способов обмана – это «выигрыш». Сообщение о призе (компьютер, мобильный телефон и пр.). Для этого у несовершеннолетних просят сообщить данные электронной карты (родителей) и цифры, которые пришли в СМС-сообщении на телефонный номер.

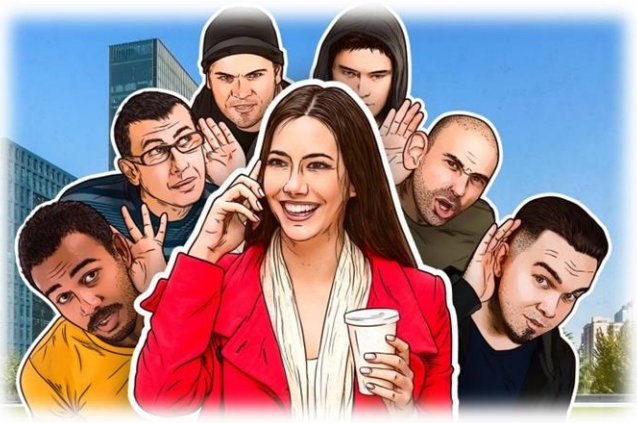
Также среди киберпреступлений распространен фишинг – когда в социальную сеть сбрасывают вредоносную ссылку, по которой человек попадает на поддельный сайт и «засвечивает» все данные своей платежной карты, после чего приходит сообщение о списании денег.

Хищение имущества путем изменения информации, обрабатываемой в компьютерной системе, хранящейся на машинных носителях или передаваемой по сетям передачи данных, либо путем введения в компьютерную систему ложной информации – наказывается штрафом, или ограничением свободы на срок до трех лет, или лишением свободы на тот же срок (ст. 212 Уголовного кодекса Республики Беларусь). За совершенные преступления ребенком в возрасте до 14 лет несут ответственность их родители.



Правила безопасности для несовершеннолетних в сети Интернет

- Не заходите на незнакомые и подозрительные сайты.
- Если к вам по электронной почте пришел файл Word или Excel, даже от знакомого лица, прежде чем открыть, обязательно проверьте его на вирусы.
- Если пришло незнакомое приложение, ни в коем случае не запускайте его, а лучше сразу удалите и очистите корзину.
- Старайтесь использовать для паролей трудно запоминаемый набор цифр и букв.
- Не оставляйте без присмотра компьютер с важными сведениями на экране.
- Сообщайте своим родителям, когда сталкиваетесь с чем-нибудь в Интернете, что заставляет вас чувствовать себя неловко.
- Не стоит игнорировать сообщения, которые содержат угрозы, особенно систематические. Следует скопировать эти сообщения, рассказать об этом родителям, обратиться в правоохранительные органы.
- Не выкладывайте свои личные данные в Интернете (домашний адрес, номер телефона, номер школы, класс, любимое место прогулки, время возвращения домой, место работы родителей, пароли от своей электронной почты, электронного кошелька и др.). Помните, любая информация может быть использована против вас, в том числе в корыстных и преступных целях.



- Используйте псевдоним при общении в чатах, использовании программ мгновенного обмена сообщениями, пользовании он-лайн играми и в других ситуациях.
- Не размещайте и не посылайте свои фотографии незнакомцам. Будьте внимательны, если вас просят прислать или провоцируют на какие-либо действия перед веб-камерой.
- Будьте осторожны при общении с незнакомыми людьми. Старайтесь рассказывать как можно меньше личной информации о себе.

- Если новый знакомый пытается говорить с вами на неприятные или пугающие темы и говорит об этом как о секрете, который останется только между вами – немедленно сообщите об этом родителям или взрослым, которым доверяете, и сделайте снимок с экрана (screen-shot).
- Если вы пользуетесь чужим устройством для выхода в Интернет, не забывайте выходить из своего аккаунта на различных сайтах. Не сохраняйте на чужом компьютере свои пароли, личные файлы, историю переписки.
- Ваши собеседники могут оказаться совсем не теми, за кого себя выдают. Не поддавайтесь на уговоры встретиться один на один, особенно – в безлюдном месте!

Всегда помните!!!

- ✓ Далеко не все, что можно прочесть или увидеть в Интернете – правда.
- ✓ В Интернете каждый может представить себя не тем, кем является на самом деле.

Если ситуация не находит решения Вы можете обратиться по телефону доверия 170 или в государственное учреждение образования «Гродненский областной социально-педагогический центр», расположенный по адресу: г. Гродно, ул. Горького, д. 79, или по телефону 55-70-33.

Кроме того, ответы на вопросы, связанные с проблемой кибербуллинга, а также анонимную консультацию психолога можно получить на сайте http://kids.pomogut.by, созданном по инициативе Министерства внутренних дел Республики Беларусь, а также на детском правовом сайте https://mir.pravo.by.