

ПЛАН-КОНСПЕКТ

на тему: «Безопасность детей в глобальной компьютерной сети Интернет»

Что такое интернет

(слайд №2)

Представляешь, много-много компьютеров по всему миру объединены в глобальную сеть! По ней можно обмениваться ЛЮБОЙ информацией: фильмами, музыкой, фотографиями, документами. Можно общаться с ребятами по всему миру, играть в онлайн игры. С помощью интернета можно учиться удаленно или посмотреть места, в которых не можешь побывать.

Правила пользования интернетом

(слайд №3)

Общение в сети с друзьями и родственниками может быть классным и захватывающим, но, к сожалению, ты можешь встретиться и с трудностями. Чтобы не навредить себе и пользоваться интернетом безопасно, помни два основных правила:

- Правило ПРИВАТНОСТИ. Знай, что твоя персональная информация может стать доступной для любого человека в любой точке мира. Она может быть использована не только твоими друзьями или членами семьи, но и незнакомцами.
- Правило ПОСТОЯНСТВА. Если ты что-то размещаешь в интернете, то это может остаться там на очень долгое время. Даже сообщения и фотографии, которые ты удаляешь, сохраняются на специальных серверах.

В сети действуют те же правила безопасности, что и в реальном мире!

(слайд №4)

Интернет объединяет всех-всех людей на свете. Но среди них могут оказаться такие, общения с которыми стоит избегать. Игры и видео, которые ты находишь в интернете, тоже могут оказаться далеко не безобидными. Так что будет осторожен!

Обман в интернете и социальных сетях

(слайд №5)

Обман в интернете и социальных сетях – очень распространенное явление. Помни, что твои собеседники могут оказаться не теми, за кого они себя выдают. Ты думаешь, что тебе пишет твой друг, с которым ты знаком в реальной жизни, но может оказаться так, что его аккаунт взломан, кто-то создал копию его личности и тебе пишет мошенник. Поэтому если собеседник просит тебя сделать что-то необычное или просит денег, обязательно проверь его. Если это человек, с которым ты знаком в реальном мире, позвони ему. Задай вопрос, ответ на который можете знать только вы вдвоем. Если ты понимаешь, что твой собеседник не тот, за кого себя выдает, обратись в службу поддержки, чтобы заблокировать этот аккаунт. Сообщи

другу, если поймешь, что его аккаунт взломан. Если не знаешь как себя вести, обратись на горячую линию помощи детям.

Фальшивые сайты и аккаунты в социальных сетях

(слайд №6)

В социальных сетях и в интернете существуют разные способы хищения и обмана. Поэтому будь внимательным, когда сообщаем сведения о себе. Так, например, бывают: Фальшивые сайты — сайты-подделки, созданные для того, чтобы украсть персональные данные (логины, пароли или номера и коды банковских карт) Как обезопасить себя? Всегда проверяй адресную строку сайтов. Тебе на почту может прийти письмо от известного сайта с просьбой подтвердить пароль или проверить учетные данные, при переходе на данный сайт он будет выглядеть как настоящий, НО адресная строка будет отличаться. Значит, это сайт-подделка. Не надо переходить по таким ссылкам! Если ты засомневался, то лучше зайди на сайт прямо, написав его название в адресной строке браузера.

Плата за подписки

(слайд №7)

Под платой за подписку может скрываться кража денег с баланса телефона. Подписка происходит через USSD-запрос или отправку СМС-сообщения. Будь внимателен, нажимая кнопки «смотреть», «подписаться» или «скачать». Ты можешь случайно подписаться на платные сервисы или платный развлекательный контент. Иногда нажимая на эти кнопки, ты автоматически соглашаешься с условиями подписки.

Кража паролей в социальных сетях или играх

(слайд №8)

Аккаунты в играх и социальных сетях давно стали важной частью нашей онлайн жизни. Мы расстраиваемся, когда с ними что-то случается, и мы не можем написать друзьям или зайти в любимую игру. Кажется, что наступила катастрофа. Кража паролей и аккаунтов может произойти во многих случаях. Например, когда ты заходишь в игру на чужом компьютере. Есть специальные программы, которые могут взламывать чужие пароли. Иногда доступ в аккаунт можно восстановить посредством службы технической поддержки, но сперва тебе придется доказать то, что это твой аккаунт. Доказать подлинность своего аккаунта можно несколькими способами: с помощью кода активации на диске, через привязку к банковской карте, оплатой онлайн-кошельками или терминалами.

Вымогательство с использованием вирусных программ

(слайд №9)

Иногда вместо необходимой нам программы может скачаться вредоносный вирус, который шифрует данные на дисках или блокирует устройства, после чего требует денег за разблокировку и восстановление работы системы. Чаще

всего сообщение с требованием перевода денег или с угрозами в адрес пользователя выскакивает после перезагрузки устройства или при запуске загруженного приложения. Программы-вымогатели очень распространены. Если компьютер заражен такой программой, тебе приходит сообщение о том, что ты должен заплатить за нелицензионное программное обеспечение. Либо появляется поддельное сообщение как будто от правоохранительных органов об обнаружении на твоём компьютере незаконной информации (например, детской порнографии) и требование оплатить штраф. Также могут приходить сообщения на почту о том, что все твои фотографии зашифрованы и за их разблокировку ты должен заплатить. Что делать, если тебе пришло такое сообщение? Не надо ничего оплачивать. И не пытайся связаться с отправителем. Это пишет робот, он не будет отвечать. Если ты умеешь, проверь компьютер или другое устройство, на котором ты получаешь такие сообщения, с помощью любой антивирусной программы. Либо переустанови систему. Но лучше всего обратиться за помощью к взрослым.

Агрессия в социальных сетях (слайд №10)

Взаимодействие людей в интернете происходит, по сути, так же как в реальной жизни. Все люди разные. Одни воспитанные и интеллигентные, а другие — хамят, выплескивают свою агрессию, на считаясь с чувствами других людей. Таких обычно называют «троллями». Как злых мифических существ! Но, к сожалению, интернет-тролли — реальные люди, которые используют всемирную сеть для травли и унижения других людей и получают от этого удовлетворение. Они пишут обидные слова для того, чтобы унижить другого человека, ударить по его самооценке. Иногда троллей специально используют для того, чтобы испортить репутацию популярных сайтов и снизить их посещаемость.

Вот несколько советов, которые помогут тебе справиться с агрессией в социальных сетях

- Если ты столкнулся с троллем, то лучше всего не вступай с ним в переписку, не начинай доказывать свою точку зрения, а просто сразу заблокируй его.
- Никогда не оправдывайся и ничего не объясняй троллю, он именно этого и добивается. Любой твой ответ вызовет еще большую атаку
- Старайся не принимать близко к сердцу то, что пишут в Интернете. Только ты, твои настоящие друзья и близкие знают, какой ты есть на самом деле. И никто не имеет право оценивать или осуждать тебя.
- Никто не имеет права оскорблять или унижать тебя!
- Поговори со взрослым, которому доверяешь. Попроси помочь заблокировать обидчика.
- Если у тебя остались вопросы или ты не знаешь, как поступить, позвони на горячую линию.

Обмен личными фото

Как обмениваться фото в интернете

(слайд №11)

В интернете мы взаимодействуем с разными людьми, некоторые вызывают у нас симпатию или даже влюбленность. Кажется, что ты нашел свою вторую половинку. Но в реальности все может быть совсем иначе. Девушка или парень, с которыми ты мило переписываешься и обмениваешься фотками, могут оказаться взрослыми людьми, которые желают совершить против тебя неправомерные действия. Для того чтобы с тобой не случилось ничего плохого, следуй нашим рекомендациям. Помни про правила приватности и не скрывай свой возраст. Лучше сразу сообщи собеседнику, сколько тебе лет. Никто не имеет права присылать тебе фото или видео, на которых люди совершают какие-то сексуальные действия, и тем более предлагать сделать что-то похожее.

Что может случиться, когда ты посылаешь такие материалы?

- когда ты отправляешь кому-нибудь фото или видео, где ты без одежды, может так случиться, что эти материалы станут доступными всем.
- они могут оказаться, где угодно.
- их могут увидеть свои родители, одноклассники и учителя
- представь, как ты будешь себя чувствовать.
- ситуация выйдет из-под твоего контроля
- ты думаешь, что можешь доверять человеку, но все может измениться
- телефон могут украсть, почту взломать, вашу переписку выставить на всеобщее обозрение
- а может быть, вы поссоритесь, и твой друг со злости разошлет твои фото другим людям, или покажет взрослым

Как безопасно скачать из интернета

(слайд №12)

Если ты хочешь скачать что-то в интернете - следуй этим простым правилам

- В первую очередь ты должен спросить разрешения у родителей или других взрослых.
- Никогда не пиши в интернете свой номер телефона, настоящие имя и фамилию. Даже если такую информацию запрашивают для скачивания музыки или игры. Такой сайт, скорее всего, принадлежит обманщикам, которые хотят использовать твои персональные данные в корыстных целях. Например, хотят списать деньги с твоего баланса.
- Никогда не вводи данные своих или чужих банковских карт. Чужими картами пользоваться незаконно, у тебя могут быть проблемы.

- Прежде чем что-то скачать, удостоверься, что это надежный ресурс. Лучше всего скачивать игры с официальных источников (например, с App store, Google store).
- На твоём компьютере должен быть установлен антивирус. В играх могут содержаться вирусы, которые испортят твой компьютер или планшет. Могут встретиться вирусы, которые похищают персональные данные.

Можно ли размещать в интернете персональную информацию?

(слайд №13)

Вот тебе несколько советов

Надо спрашивать разрешение, когда хочешь разместить свою или чужую персональную информацию. Следуй этим советам, тогда ты сам будешь в безопасности и не обидишь своими действиями других людей.

- Спрашивай родителей или других взрослых, можно ли тебе разместить свое фото в интернете или указать персональные данные.
- Спрашивай разрешение у других людей, прежде чем опубликовать в интернете фото или видео с ними или указать их персональные данные.

**Управление по противодействию киберпреступности
криминальной милиции УВД Минского облисполкома**