**Методические рекомендации по организации и проведению информационно-просветительского мероприятия**

**«Уроки безопасного Интернета»**

*Информационно-просветительское мероприятие направлено на формирование основ безопасного поведения в сети Интернет и реализуется в рамках тематического* *блока* *мероприятий* *«Безопасный* *интернет»* *областного межведомственного* *проекта* *организации* *мероприятий,* *направленных* *на пропаганду здорового образа жизни и профилактику асоциальных явлений, «Тюменская область – территория здорового образа жизни!». Мероприятие приурочено ко Дню Интернета в России (30 сентября).*

**Дата проведения:** с 18 по 30 сентября.

**Место проведения:** образовательные организации, иные учреждения. **Участники:** несовершеннолетние (14+) и молодежь Тюменской области. **Цель:** формирование навыков безопасного поведения в сети Интернет. **Задачи:**

- актуализировать знания несовершеннолетних правилах поведения в Интернете;

- информирование о правовой ответственности, связанной с деятельностью в сети Интернет;

**Организаторы:** муниципальные образовательные учреждения Тюменской области.

**Необходимое** **оборудование:** проектор, экран, звуковая аппаратура, микрофоны.

**Ход мероприятия:**

**Вводная часть:**

**Ведущий:** Добрый день, уважаемые участники и гости нашего мероприятия! Наша встреча приурочена ко Дню Интернета, и сегодня мы вместе выясним, с какими проблемами могут столкнуться пользователи сети Интернет, и как безопасно пользоваться ее ресурсами.

Мы живём в эпоху Интернета и информационных технологий. Интернет плотно проник во все сферы деятельности, тем самым упрощая нам жизнь и экономя наше время. Приведите примеры использования Интернета в различных жизненных ситуациях.

*Ответы участников: общение в социальных сетях, поиск информации, просмотр фильмов и т.д.*

**Ведущий:** Приведите примеры ситуации, в которых, используя Интернет, мы экономим время.

*Ответы участников: Перевод денег, оплата мобильной связи, онлайн шопинг, гос. услуги.*

**Ведущий:** Безопасно ли пользоваться Интернетом? Почему? С какими опасностями может столкнуться человек?

*Ответы участников: Небезопасно, так как личную страницу человека могут взломать. Через интернет могут вовлечь в преступную деятельность, можно стать жертвой мошенников, можно столкнуться с запрещенным контентом (пропаганда наркотиков, экстремизма и др.).*

**Ведущий:** В настоящее время существует много различных потенциально опасных ситуаций при использовании Интернета, но риск опасности можно свести к минимуму, соблюдая простые правила. Человеку важно научиться распознавать угрозы и не поддаваться на уловки мошенников. Я предлагаю вам ознакомиться с наиболее распространенными формами мошенничества и сформулировать правила безопасного поведения.

Основная часть:

**1. Защита персональных данных.**

Большую часть онлайн-ресурсов объединяет одна особенность - для получения полного доступа ко всем возможностям сайта необходима регистрация и указание своих личных данных. Надо сказать, что с развитием социальных сетей, в массовом сознании пользователей стало абсолютно нормой публиковать все подробности о своей жизни в Интернете. Социальные сети стимулируют нас к тому, чтобы мы указывали настоящие фамилию и имя, все свои интересы, контактные данные, в том числе номер телефона, размещали фотографии. Чем больше информации о себе мы размещаем на сайтах, тем проще другим пользователям установить нашу личность. В этом, конечно же, есть очевидные плюсы, – например, поиск новых друзей, единомышленников. Сегодня каждая семья имеет устройства для получения и обмена информацией, но не всегда контролирует процесс передачи информации. Пользователи не всегда понимают, что, размещая свои персональные данные в сети Интернет, они подвергают опасности себя и свою семью.

О том, что относится к персональным данным и к каким последствиям может привести их кража мы узнаем из видеоурока, подготовленного специалистами Ассоциации «Лига безопасного интернета».

*Ссылка для скачивания видеоматериалов:* [*https://disk.yandex.ru/d/BQ2rC\_I9yJVJlg*](https://disk.yandex.ru/d/BQ2rC_I9yJVJlg)

*Демонстрация на экране видеоурока №1*

**2. Безопасность в сетях Wi-Fi.**

Помимо того, что мы публикуем, важно еще и учитывать каким образом пользователь осуществляет вход в Интернет. Сегодня Wi-Fi прочно занял свое место в нашей жизни, превратившись из новой технологии в повседневность. Зайдя выпить чашечку чая в кафе или присев на лавочку в сквере многие начинают искать ближайшую точку доступа. Благодаря точкам Wi-Fi вы можете повсеместно оставаться в сети, выполнять нужную работу, быть в курсе всех новостей и событий, но, в тоже время, работа с общедоступными точками «Wi-Fi» может быть серьезной угрозой вашей онлайн безопасности. О том, на что нужно обратить пристальное внимание при подключении к такой точке доступа, и как максимально обезопасить

свою конфиденциальную информацию мы узнаем из следующего видеоурока.

*Демонстрация на экране видеоурока №2*

**3. Майнинг.**

В Интернет-пространстве у пользователей может складываться ошибочное мнение, что в виртуальном мире ты можешь быть другим человеком и позволить себе то, что никогда бы не сделал в реальной жизни. Именно это подталкивает недобросовестных граждан к попыткам извлечь личную выгоду незаконным путем с использованием компьютерных технологий. Как показывает практика, преступления с сети Интернет успешно раскрываются и пресекаются. Но, к сожалению, это не дает права пользователям забывать о необходимых мерах безопасности. На смену выявленным формам мошенничества в Интернете, постоянно появляются новые, более сложные. Например, майнинг, когда персональный компьютер, без согласия пользователя, подключается к определенной системе и начинает работать на реализацию задач других пользователей. Мне хотелось бы вас познакомить с одной из таких форм – это майнинг. Кто-то знает, что это за вид мошенничества? *(Ответы участников)*

Специалисты Лиги безопасного Интернета его уже достаточно хорошо изучили и готовы поделиться с вами своими открытиями.

*Демонстрация на экране видеоурока №3*

**4. Виды взлома.**

Если о майнинге человек долгое время может и не догадываться, то о мошенничестве с различными видами взлома аккаунтов и личных кабинетов пользователь узнает достаточно быстро и, как правило, это связано с полной утратой доступа к данным, потерей денежных средств. О том, как этого избежать мы узнаем из следующего видеоурока.

*Демонстрация на экране видеоурока №4*

**5. Кибербуллинг.**

Помимо опасности причинения физического вреда пользователи могут также столкнуться в интернет-пространстве с различными видами психологического давления - кибербуллингом. Под кибербуллингом подразумевается травля в Интернете. Например, нередки случаи, когда злоумышленники создают поддельные страницы и копируют туда информацию со страницы жертвы, размещая при этом унизительный контент, содержащий обидные и непристойные сообщения, а затем шантажируют жертву. Такие действия могут причинить значительный психологический вред человеку, в особенности несовершеннолетнему, а в крайних случаях привести к самым трагическим последствиям. В законодательстве отсутствует конкретное положение, предусматривающее ответственность за кибер-издевательства, это вызвано тем, что такая деятельность довольно широка и охватывает значительный перечень уже имеющихся составов преступлений и правонарушений, это в первую очередь нарушение права на неприкосновенность

частной жизни, выражающееся в незаконном сборе или распространении сведений о частной жизни лица, составляющих его личную или семейную тайну.

Что следует делать в ситуации травли в Интернете: 1. Игнорируй преследователей. «Не корми троллей!».

2. Используй настройки приватности социальных сетей, чтобы ограничить обидчикам возможность доступа к твоему аккаунту.

3. Обратись к старшим: они смогут поддержать тебя в трудную минуту, если будут знать, что тебе нужна их поддержка.

4. Попробуй обратиться в администрацию ресурса. Если тебя травят, используя отдельную «группу ненависти», то ты можешь попросить администрацию закрыть ее.

**6. Вовлечение в преступную деятельность, связанную с распространением наркотиков.**

Кроме того, активные пользователи сети Интернет могут также столкнуться с вовлечением в преступную деятельность. Просторы Интернета переполнены массой объявлений с предложением высокооплачиваемой и несложной работы. Зачастую такие объявления нацелены на вовлечение в противоправную деятельность, например, в сбыт и распространение наркотиков.

Отсутствие офисов, сведений о руководстве, контактной информации, требований к соискателям, общение через переписку, трудоустройство только по паспорту – это отличительные черты организаций, осуществляющих незаконную деятельность, в том числе и по распространению наркотиков. Важно помнить, что за участием в противоправной деятельности и большими доходами кроется неизбежное уголовное наказание.

Также наркодилеры массово втягивают подростков в распространение наркотиков через участие в квестах и челленджах. Процесс распространения завуалирован под увлекательную игру, с выполнением ряда заданий/поиском «клада» по координатам GPS, адресу и фото, которые сообщаются по средствам связи.

Ведущим мотивом для участия в такой деятельности является любопытство и возможность подзаработать. Участники крестов до конца не осознают всей полноты ответственности, которая последует за подобную деятельность.

Бытует мнение, что Интернет – анонимное пространство, где ты можешь быть кем угодно. Но нет, в онлайн среде действуют аналогичные законы, как и в реальной жизни.

За распространение наркотических средств, психотропных веществ или их аналогов согласно статье 228.1 Уголовного кодекса РФ предусмотрено наказание сроком до 20 лет лишения свободы или пожизненное заключение.

За распространение наркотических средств, психотропных веществ или их аналогов с использованием информационно-телекоммуникационных сетей Интернет согласно части 2 статьи 228.1 Уголовного кодекса РФ предусмотрено от 5 до 20 лет лишения свободы.

Нельзя терять бдительности и когда мы размещаем какой-либо пост или делаем репост чужой записи. Необходимо обращать внимание на детали информации (картинки, аудио и видео файлы, комментарии, текстовые файлы),

которой делишься со своими друзьями – она может носить противоправный характер. Так, например, любая пропаганда наркотиков в Интернете запрещена и предусматривает наказание.

Согласно части 1 статьи 6.13 Кодекса об адмистративных правонарушениях РФ за пропаганду наркотических средств, психотропных веществ предусмотрено наказание в виде штрафа от 4 до 5 тысяч рублей с конфискацией рекламной продукции и оборудования.

Кроме того, по части 1.1 статьи 6.13 Кодекса об адмистративных правонарушениях РФ (пропаганда с использованием информационно-телекоммуникационных сетей Интернет) предусмотрено наказание в виде административного штрафа на граждан в размере от 5 тысяч до 30 тысяч рублей.

Знание основ законодательства и соблюдение его норм помогают создать безопасные условия для общения в сети Интернет.

**7. Анонимность в Интернете.**

Ребята как вы считаете можно ли оставаться анонимным, будучи активным интернет-пользователем? *(Ответы* *участников).* Вы можете оставаться относительно анонимным для определенного круга лиц, но говорить об абсолютной анонимности в виртуальном пространстве, конечно же, не стоит. О том, как интернет собирает сведения о нас и чем это подтверждается мы узнаем из следующего видеосюжета.

*Демонстрация на экране видеоурока №5*

**8. Профиль в социальных сетях - твоя визитная карточка.**

В наше время почти у каждого человека есть профиль в социальных сетях и этот профиль неотделим от конкретной личности. Он становится нашим вторым лицом и наглядно характеризует нас как личность. И чем стремительнее развивается виртуальное общение, тем серьезнее мы начинаем воспринимать профиль в социальных сетях. Согласитесь, вы, наверное, не раз пытались проверить социальные профили новых знакомых, одноклассников, известных личностей, чтобы составить о них собственное мнение. Точно также ВУЗы или работодатели могут оценивать профили своих потенциальных студентов и сотрудников. Именно поэтому важно быть предельно внимательным к заполнению профиля в социальных сетях и к тем материалам, которые комментируются, публикуются, репостятся в сети, потому что «интернет помнит все».

Хотите узнать, как это работает? Тогда внимание на экран!

*Демонстрация на экране видеоурока №7*

*Соблюдение достаточно простых правил и предельная внимательность помогут вам*

Ведущий: на основании уроков, подготовленных специалистами Лиги безопасного Интернета можно сформулировать следующие правила:

- При регистрации на сайтах и в социальных сетях старайся не указывать личную информацию (свои фамилию, имя отчество, номер телефона, адрес места

жительства, школы, место работы родителей и другое) – она может быть доступна для всех, в том числе и для злоумышленников.

- Старайся не пользоваться открытыми сетями и бесплатным Wi-Fi, т.к. с ними могли поработать злоумышленники. Если все-таки заходишь в социальные сети, то лучше это сделать через приложение, а не через браузер.

- Чтобы у злоумышленников было меньше шансов использовать твое оборудование, следует скачивать и загружать на своем устройстве файлы с непроверенных источников, необходимо своевременно устанавливать и обновлять операционную систему и приложения, отвечающие за безопасность вашего компьютера. Скачивание обновлений с официальных сайтов производителей софта и удаление лишних приложений также могут повысить защиту ваших устройств как от майнинг-вирусов, так и от других вредоносных программ.

- Никому и никогда не разглашай свои пароли. Они – твой главный секрет. Придумай свой уникальный пароль, о котором никто не сможет догадаться. Не записывай пароли на бумажках, не храни их в открытом доступе. Не отправляй свои пароли по электронной почте.

- Не отвечайте на оскорбительные для вас сообщения, тем более не стоит мстить обидчику ответными сообщениями. Ответные оскорбления или унижение собеседника сделают ситуацию только хуже, могут привести к еще большим проблемам. Обидчику важна реакция, если нет реакции, то пропадает желание провоцировать.

6. «Легкий заработок» часто предлагается в тех случаях, когда речь идет о вовлечении в незаконную деятельность, которая предусматривает уголовную и административную ответственность;

7. Абсолютной анонимности достичь невозможно. Интернет накапливает информацию о каждом пользователе, он создает цифровой профиль для каждого из нас. Поэтому важно следовать правилу: «Не делай в Интернете того, чтобы ты не стал делать в реальной жизни!».

**Заключительная часть:**

**Ведущий:** Наше мероприятие завершается. Надеюсь, вы извлекли много полезной информации из нашей встречи. Знания, которые вы сегодня получили, позволят вам обезопасить себя в интернете, а также помогут избежать неприятных сюрпризов в будущем.

Интернет становится ценным ресурсом, когда человек умеет им правильно пользоваться. Когда мы покупаем для себя нужное, важное и дорогое оборудование, мы прежде чем использовать его в повседневной жизни, изучаем инструкцию и только потом, тщательно изучив все правила и даже комментарии к ним, работаем с ним. Для того, чтобы интернет стал настоящим помощником в учебе, отдыхе, развлечении, самообразовании, общении и многом другом, необходимо заранее позаботиться о своей безопасности и соблюдать правила работы в Интернете. Всем участникам огромное спасибо за внимание! До новых встре