Министерство науки и высшего образования
Республики Казахстан
НАО «Павлодарский педагогический университет
имени Әлкей Марғұлан»

Ж.О. Жилбаев
А.Ж. Асаинова
Д.Б. Абыкенова
Л.С. Сырымбетова
З.К. Кульшарипова

Методические инструкции обеспечения кибербезопасности образовательной среды школы для учителей, родителей и учеников

Учебно-методическое пособие

Павлодар, 2024

УДК 004
ББК 32.973
М54

Рекомендовано Ученым советом НАО «Павлодарский педагогический университет имени Әлкей Марғұлан» (протокол №6 от 28.03.2024 г.)

Рецензенты:
доктор PhD, ассоциированный профессор (доцент), НАО «Павлодарский педагогический университет им. Ә. Марғұлан»
К.М. Мухамедиева

доктор PhD, ассоциированный профессор, НАО «Торайгыров университет»
Н.К. Токжигитова

Ж.О. Жилбаев, А.Ж. Асаинова, Д.Б. Абыкенова, Л.С. Сырымбетова, З.К. Кульшарипова. Методические инструкции обеспечения кибербезопасности образовательной среды школы для учителей, родителей и учеников: учебно-методическое пособие/Ж.О. Жилбаев, А.Ж. Асаинова, Д.Б. Абыкенова, Л.С. Сырымбетова, З.К. Кульшарипова. – Павлодар: НАО «Павлодарский педагогический университет имени Әлкей Марғұлан», 2024. – 68 с.

ISBN 978-601-267-804-8

Учебно-методическое пособие “Методические инструкции обеспечения кибербезопасности образовательной среды школы для родителей, учителей и школьников” предназначено для родителей, учителей и учеников для поддержки кибербезопасности в школьной среде. Пособие включает рекомендации по безопасной работе в интернете, учету рисков и нивелированию негативного воздействия на безопасность, распознаванию мошеннического поведения, фишинга, социальной инженерии, вредоносного программного обеспечения, схеме поведения при киберопасности в школьной среде, включая кибербуллинг.

Разработано исследовательской группой в рамках грантового проекта ИРН AP19678646 «Педагогическое обеспечение кибербезопасности школьной среды с использованием комплаенс-менеджмента».

УДК 004
ББК 32.973

ISBN978-601-267-804-8

СОДЕРЖАНИЕ

ГЛОССАРИЙ

Аватар – графическое альтер-эго, которое вы создаете для использования в Интернете; может быть трехмерным персонажем или простой иконкой, человеком или причудливой фигурой.

Badware – Вредоносное программное обеспечение; включает вирусы и шпионские программы, которые крадут вашу личную информацию, рассылают спам и совершают мошеннические действия.

Резервное копирование – создание копий компьютерных данных на случай, если что-то случится с вашим компьютером или операционной системой и информация будет утеряна.

Блокирующее программное обеспечение – программа для фильтрации контента из Интернета и ограничения доступа к сайтам или контенту на основе определенных критериев.

Блог – сокращение от “веб-журнал”, сайт, на котором вы регулярно публикуйте личные наблюдения.

Список друзей – список людей, с которыми вы можете общаться с помощью программы обмена мгновенными сообщениями.

Чат–комната - это онлайн-пространство, где вы можете встречаться и обмениваться информацией с помощью сообщений, отображаемых на экранах других пользователей, находящихся в “комнате”.

Киберзапугивание – травля или домогательство, которые происходят в Интернете; включает в себя размещение постыдных фотографий или недоброжелательных комментариев в профиле человека или отправку их по электронной почте.

Брандмауэр – аппаратное или программное обеспечение, которое блокирует несанкционированное подключение к вашему компьютеру или с его помощью; помогает предотвратить использование хакерами вашего компьютера для отправки вашей личной информации без вашего разрешения.

GPS – “Глобальная система позиционирования”, глобальная навигационная спутниковая система, которая используется в автомобилях или телефонах для определения местоположения и указания маршрутов.

Хакерство – взлом компьютера или сети путем обхода или отключения мер безопасности.

Обмен мгновенными сообщениями (IM) – позволяет двум или более людям общаться в режиме реального времени и уведомляет вас, когда кто-то из вашего списка друзей находится онлайн.

Интеллектуальная собственность (ИС) – творческие продукты, имеющие коммерческую ценность, включая объекты авторского права, такие как книги, фотографии и песни.

Учетная запись пользователя с ограниченным доступом – сетевая настройка, которая предоставляет пользователю доступ к некоторым функциям и программам компьютера, но позволяет только администратору вносить изменения, влияющие на работу компьютера.

Вредоносное ПО – сокращение от “вредоносное программное обеспечение”; включает вирусы и программы-шпионы, которые крадут личную информацию, рассылают спам и совершают мошеннические действия.

Пароль – секретное слово или фраза, используемая вместе с именем пользователя для предоставления доступа к вашему компьютеру или защищайте конфиденциальную информацию онлайн.

Патч – программное обеспечение, загружаемое для исправления или обновления компьютерной программы.

Одноранговый (P2P) обмен файлами - позволяет вам обмениваться файлами онлайн, такими как музыка, фильмы или игры, через неформальную сеть компьютеров, на которых установлено одно и то же программное обеспечение для обмена файлами.

КПК – “Персональный цифровой ассистент”; может использоваться в качестве мобильного телефона, веб-браузера или портативного медиаплеера.

Личная информация – данные, которые могут быть использованы для вашей идентификации, такие как ваше имя, адрес, дата рождения или ИИН.

Фишинг – когда мошенники рассылают спам, всплывающие окна или текстовые сообщения, чтобы обманом заставить вас раскрыть личную, финансовую или другую конфиденциальную информацию.

Настройки конфиденциальности – элементы управления, доступные во многих социальных сетях и других веб-сайтах, которые вы можете настроить для ограничения доступа к вашему профилю и информации, которую могут видеть посетители.

Профиль – личная страница, которую вы создаете в социальной сети или на другом веб-сайте, чтобы делиться информацией о себе и общаться с другими людьми.

Программное обеспечение для обеспечения безопасности – идентифицирует и защищает от угроз или уязвимостей, которые могут скомпрометировать ваш компьютер или ваши личные данные, информация; включает антивирусное и антишпионское программное обеспечение и брандмауэры.

Секстинг – отправка или пересылка фотографий или сообщений сексуального содержания с мобильного телефона.

Смартфон – мобильный телефон, который предлагает расширенные возможности и функционал, такие как подключение к Интернету и портативный медиаплеер.

SMS – “Служба коротких сообщений”; технология , позволяющая отправлять текстовые сообщения с одного мобильного телефона на другой.

Сайт социальной сети – веб-сайт, который позволяет вам создать профиль и общаться с другими пользователями.

Шпионское ПО – это программное обеспечение, установленное на вашем компьютере без вашего согласия для мониторинга или управления использованием вашего компьютера.

Текстовые сообщения – отправка коротких сообщений с одного мобильного телефона на другой.

Подросток – ребенок в возрасте от 8 до 12 лет.

Имя пользователя – псевдоним, используемый вместе с паролем для предоставления доступа к учетным записям и веб-сайтам.

Видеозвонки – интернет-сервисы, позволяющие пользователям общаться с помощью веб-камер.

Виртуальный мир – смоделированное компьютером онлайн - “место”, где люди используют аватары - графические символы - для представления самих себя.

Вирус – вредоносное ПО, которое проникает на ваш компьютер, часто через вложения в электронную почту, а затем создает свои копии.

ВВЕДЕНИЕ

В наши дни сложно представить ребенка без гаджета. Несмотря на достижения технологического прогресса, постоянное подключение к интернету может представлять особую угрозу для детей. Кибербезопасность, также известная как компьютерная безопасность, включает в себя набор методов и практик, направленных на защиту пользователей, как взрослых, так и детей, от атак злоумышленников.

В современных условиях цифровизации образовательного процесса кибербезопасность приобретает особую значимость. Учащиеся, учителя и родители ежедневно используют интернет и цифровые устройства для обучения, коммуникации и развлечений, что делает их уязвимыми перед различными киберугрозами. Кибербуллинг, фишинг, вирусы и утечки данных – это лишь некоторые из опасностей, с которыми могут столкнуться школьники и их окружение.

Обеспечение кибербезопасности в образовательной среде помогает:

– Защитить личные данные учащихся и сотрудников.

– Предотвратить кибербуллинг и другие формы цифрового насилия.

– Снизить риски заражения вредоносным программным обеспечением.

– Повысить доверие к цифровым технологиям и образовательным ресурсам.

Цель методических инструкций заключается в повышении осведомленности для обеспечения высокого уровня кибербезопасности в образовательной среде, сформировать навыки безопасного использования интернета среди всех участников образовательного процесса: родителей, учителей и школьников.

Методические инструкции предназначены для применения как в школьной среде, так и дома. В школе они помогут учителям и администрации создать безопасную цифровую среду для учебного процесса, а дома родители смогут использовать эти инструкции для защиты своих детей от киберугроз. Инструкции охватывают широкий спектр аспектов, включая обучение основам кибербезопасности, внедрение технических мер защиты и развитие культуры безопасного использования интернета.

Методические инструкции ориентированы на три основные целевые группы:

1. Родители**:**

- Обучение родителей основам кибербезопасности для защиты своих детей.
- Рекомендации по мониторингу и контролю интернет-активности детей.
- Создание безопасной цифровой среды дома.

2. Учителя**:**

- Подготовка учителей к преподаванию основ кибербезопасности учащимся.
- Разработка и внедрение школьных политик и процедур кибербезопасности.
- Обеспечение безопасности школьной сети и устройств.

3. Школьники**:**

- Обучение школьников правилам безопасного поведения в интернете.
- Развитие навыков распознавания и реагирования на киберугрозы.
- Формирование ответственного отношения к использованию цифровых технологий.

Эти методические инструкции помогут создать координированный подход к обеспечению кибербезопасности, объединяющий усилия всех участников образовательного процесса.

1. МЕТОДИЧЕСКИЕ ИНСТРУКЦИИ ДЛЯ РОДИТЕЛЕЙ

Интернет открывает целый мир возможностей. Люди всех возрастов публикуют видео с мобильных устройств, создают онлайн-профили и общаются друг с другом через свои гаджеты. Дети активно создают онлайн-аватары, общаются с друзьями, которых они редко видят вживую, отправляют фотографии и делятся событиями своей жизни с сотнями людей.

Такие способы общения могут приносить радость и удовлетворение, но они сопряжены с определенными рисками:

1. Неподобающее поведение: в онлайн-мире дети могут почувствовать себя анонимными и забыть, что они все еще несут ответственность за свои действия.

2. Неподобающий контакт: в интернете есть люди с плохими намерениями, включая хулиганов, хищников, хакеров и мошенников.

3. Неприемлемый контент: родители могут беспокоиться, что их дети могут наткнуться на порнографию, насилие или разжигающие ненависть высказывания.

Вы можете снизить эти риски, поговорив со своими детьми о том, как они общаются онлайн и вне сети, и поощряя их к ответственному поведению, которым они могут гордиться.

1.1 Принципы доверительного отношения родителей с детьми

Начните говорить о кибербезопасности раньше. Даже малыши видят, как их родители используют всевозможные устройства. Как только ваш ребенок начинает пользоваться компьютером, мобильным телефоном или любым другим гаджетом, самое время обсудить с ним правила поведения в сети, меры безопасности и предосторожности. У вас, как у родителя, есть возможность первыми обсудить важные вопросы, прежде чем это сделает кто-либо другой.

Создайте честную и открытую атмосферу. Дети обращаются к своим родителям за помощью. Будьте поддерживающими и позитивными. Умение слушать и учитывать их чувства помогает поддерживать диалог. Возможно, у вас нет ответов на все вопросы, и честность в этом вопросе может иметь большое значение.

Поговорите с детьми. Лучший способ защитить своих детей в Интернете – это разговаривать с ними. Исследования показывают, что когда дети хотят получить важную информацию, они в первую очередь обращаются к своим родителям.

Начинайте разговор. Даже если ваши дети чувствуют себя комфортно, обращаясь к вам, не ждите, пока они сами начнут разговор. Используйте повседневные ситуации, чтобы рассказать своим детям о безопасном использовании Интернета. Например, телепередача, где подросток выступает онлайн или пользуется мобильным телефоном, может стать поводом для обсуждения того, что делать и чего не делать в подобных обстоятельствах. Новостные сюжеты об интернет-мошенничестве или кибербуллинге также могут помочь начать разговор с детьми об их опыте и ваших ожиданиях.

Рассказывайте о своих ценностях. Будьте откровенны в отношении своих ценностей и того, как они применяются в онлайн-контексте. Четкое изложение ваших ценностей поможет вашим детям принимать более разумные и продуманные решения, когда они сталкиваются со сложными ситуациями.

Будьте терпеливы. Не торопитесь в разговорах с детьми. Большинству детей требуется повторение информации в небольших дозах для лучшего усвоения. Если вы будете продолжать общаться со своими детьми, ваше терпение и настойчивость принесут плоды в долгосрочной перспективе. Поддерживайте связь даже в случае, если ваш ребенок сделал что-то в Интернете, что вы считаете неуместным.

Рекомендации родителям в соответствии с возрастом ребенка

Маленькие дети. Когда маленькие дети начинают пользоваться компьютером, они должны находиться под пристальным наблюдением родителей или воспитателя. Родители могут заранее выбирать веб-сайты, которые их дети посещают, и не позволять им покидать эти сайты самостоятельно. Если за маленькими детьми не следить в Интернете, они могут наткнуться на сайты, которые могут их напугать или сбить с толку.

Даже если вы уверены, что ваши дети готовы исследовать интернет самостоятельно, важно поддерживать тесную связь с ними, пока они переходят с одного сайта на другой. Вы можете ограничить доступ к сайтам, которые вы предварительно проверили и которые, по вашему мнению, являются подходящими, по крайней мере, с точки зрения их образовательной или развлекательной ценности.

В подростковом возрасте (от 8 до 12 лет) дети начинают больше исследовать мир самостоятельно. Однако это не значит, что им не нужна ваша поддержка и присутствие. Важно быть рядом или поблизости, когда они выходят в Интернет. Для детей этой возрастной группы рекомендуется размещать компьютер в таком месте, где ребенок будет иметь доступ к вам или другому взрослому. Таким образом, они смогут быть "независимыми", но не одинокими.

Для детей младшего возраста родительский контроль, включая фильтрацию или мониторинг, может быть эффективным. Однако многие школьники среднего возраста обладают техническими знаниями, позволяющими обходить эти меры. В этот период дети начинают использовать Интернет для школьных занятий, поиска ресурсов для хобби и других интересов. Они часто могут помогать другим членам семьи в поиске информации в Интернете, но всё равно нуждаются в руководстве взрослых, чтобы понять, каким источникам можно доверять.

Принимая во внимание, что ваши подростки видят и делают в Интернете, подумайте о том, сколько времени они проводят в сети. Установите ограничения на то, как часто они могут быть онлайн и как долго должны длиться эти сеансы. Это поможет им научиться балансировать между виртуальным и реальным миром и предотвращать потенциальные проблемы, связанные с чрезмерным использованием Интернета.

В переходном возрасте (от 8 до 12 лет) подростки начинают выражать свои ценности, часто ориентируясь на окружающие их образцы, включая онлайн-сообщества. В этот период они часто воспринимают виртуальное пространство как место, где могут проявить свою самостоятельность, в отличие от офлайн-мира. Это время важно для установления честного диалога о том, что они видят и делают в Интернете.

Подростки начинают осознавать, что экранные имена, профили и аватары отражают реальных людей с их эмоциями и мыслями. Они стремятся к большей независимости, но они все еще нуждаются в руководстве взрослых, чтобы понять, как различать достоверные источники и как управлять своим онлайн-поведением.

Важно устанавливать разумные правила и ограничения времени, которое подростки проводят в Интернете. Обсуждайте с ними, какие действия в Интернете соответствуют вашим семейным ценностям и безопасности. Поддерживайте открытую коммуникацию, чтобы они чувствовали, что могут обсудить с вами любые вопросы или затруднения, с которыми они сталкиваются в сети.

Подчеркивайте важность доверия и осознанности в повседневном использовании Интернета. Помогайте им осознавать, что не всё, что они видят в сети, соответствует действительности, и что их действия могут иметь долгосрочные последствия. Обучайте их умению делать осознанные и безопасные выборы, как онлайн, так и офлайн.

1.2 Социальная жизнь в интернете

Сайты социальных сетей, чаты, виртуальные миры и блоги - это то, как подростки общаются в Интернете. Дети делятся фотографиями, видео, мыслями и планами с друзьями, другими людьми, разделяющими их интересы, а иногда и с миром в целом. Общение в Интернете может помочь детям наладить контакт с друзьями и даже членами их семьи, но важно помочь вашему ребенку научиться *безопасно ориентироваться* в этом пространстве.

Среди подводных камней, которые возникают при общении в Интернете, - распространение слишком большого количества информации или публикация фотографий, видео или слов, которые могут нанести ущерб репутации или причинить боль чьим-то чувствам. Трезвое суждение и здравый смысл помогут свести к минимуму эти недостатки.

Что вы можете сделать?

Напомните своим детям, что действия в Интернете могут иметь последствия. Слова, которые они пишут, и изображения, которые они публикуют, имеют последствия. Объясните своим детям, почему рекомендуется публиковать только ту информацию, которую им удобно показывать другим.

Некоторые страницы профиля вашего ребенка могут быть видны более широкой аудитории, чем вам или им удобно, даже при включенных настройках конфиденциальности. Поощряйте своего ребенка задумываться о языке, который он использует в Интернете, фотографии и видео, которые они публикуют, и последствия изменения фотографий, опубликованных кем-то другим. Учителя, будущие работодатели, сотрудники приемных комиссий, тренеры, полиция могут просматривать записи вашего ребенка.

Напомните своим детям, что разместив информацию в Интернете, они не смогут забрать ее обратно. Даже если они удалят информацию с сайта, они не смогут контролировать старые версии, которые могут существовать на компьютерах других людей и распространяться в Интернете. Используйте настройки конфиденциальности, чтобы ограничить доступ к профилю вашего ребенка и доступ к публикациям в нем. Некоторые сайты социальных сетей, чаты и блоги имеют строгие настройки конфиденциальности. Обсудите со своими детьми эти настройки и свои ожидания относительно того, кому следует разрешить просматривать их профиль. Просмотрите список друзей вашего ребенка. Возможно, вы захотите ограничить круг общения ваших детей в Интернете "друзьями", которых они действительно знают.

Избегайте разговоров о сексе в Интернете. Исследования показывают, что подростки, которые не говорят о сексе с незнакомцами в Интернете, с меньшей вероятностью вступят в контакт с хищниками. На самом деле, исследователи обнаружили, что хищники обычно не выдают себя за детей или подростков, и большинству подростков, с которыми общаются незнакомые взрослые, это кажется жутким. Подростки не должны стесняться игнорировать или блокировать их.

Знайте, чем занимаются ваши дети. Познакомьтесь с сайтами социальных сетей, которыми пользуются ваши дети, чтобы вы знали, как лучше всего понять их деятельность. Если вы обеспокоены тем, что ваш ребенок ведет себя рискованно в Интернете, возможно, вы захотите просмотреть сайты социальных сетей, которые он использует, чтобы узнать, какую информацию он публикует. Выдают ли они себя за кого-то другого? Попробуйте выполнить поиск по их имени, нику, школе, увлечениям, классу или сообществу.

Поощряйте своих детей доверять своей интуиции, если у них возникают подозрения. Поощряйте их *сообщать вам*, если они чувствуют угрозу со стороны кого-либо или испытывают дискомфорт из-за чего-либо в Интернете. Затем вы можете помочь им сообщить о своих опасениях в полицию или на сайт социальной сети. На большинстве этих сайтов есть ссылки, по которым пользователи могут сообщать о грубом, подозрительном или неподобающем поведении.

Скажите своим детям, чтобы они не выдавали себя за кого-то другого. Дайте им понять, что неправильно создавать сайты, страницы или посты, которые, как кажется, принадлежат кому-то другому, например учителю, однокласснику или кому-то, кого они выдумали. Придумайте безопасный псевдоним и объясните им, какие впечатления могут производить псевдонимы. Хороший псевдоним мало что расскажет о возрасте, месте жительства или поле человека.

В целях обеспечения конфиденциальности имена ваших детей в сообщениях электронной почты не должны совпадать с их адресами электронной почты. Помогите им понять, какие данные должны оставаться конфиденциальными. Объясните, почему важно сохранять в тайне информацию о себе, членах семьи и друзьях, такую как ИИН, адрес проживания, номер телефона, финансовые данные и другие личные сведения.

Загрузка мобильных приложений. Загружаете ли вы или ваши дети “приложения” на телефон или страницу в социальной сети? Загрузка может предоставить разработчикам приложений доступ к личной информации, которая даже не имеет отношения к назначению

приложения. Разработчики могут делиться собранной информацией с маркетологами или другими компаниями.

Предложите своим детям ознакомиться с политикой конфиденциальности и их настройками конфиденциальности, чтобы узнать, к какой информации приложение может получить доступ.

1.3 Рекомендации родителям

Электронная почта, чаты, мгновенные сообщения, видеозвонки и текстовые сообщения предоставляют быстрые и удобные способы общения. Однако основные принципы вежливости, тон коммуникации и осторожность с информацией остаются одинаковы как в онлайне, так и в реальной жизни. Вот что вы можете сделать:

1. Расскажите своим детям о правилах поведения в Интернете. Вежливость имеет значение - обучите их быть уважительными и в онлайн-коммуникациях. Хотя текстовые сообщения могут казаться безличными, использование таких обычных выражений, как "пожалуйста" и "спасибо", важно.

2. Сбавьте тон. Использование заглавных букв, множественных восклицательных знаков или крупного жирного шрифта онлайн ассоциируется с криком и может вызвать негативные реакции. Большинство пользователей не ценят агрессивную манеру общения.

3. Осторожно с сообщениями в группе. Научите детей быть аккуратными при отправке сообщений в группе или чат, не спамить и не делать бесцельную рассылку.

4. Избегайте писем-просьб о помощи. Большинство таких писем могут быть неприятными или даже мошенническими. Некоторые могут содержать вредоносные программы, такие как вирусы или шпионские программы. Учите своих детей не открывать и не передавать подобные сообщения.

Эти простые меры помогут вашим детям быть безопасными и уважительными в интернете, сохраняя их личную информацию и защищая от потенциальных угроз.

5. Установите высокий уровень конфиденциальности в учетных записях обмена мгновенными сообщениями и видеозвонками ваших детей. Большинство программ обмена мгновенными сообщениями позволяют родителям контролировать , могут ли люди из списка контактов их детей видеть статус обмена мгновенными сообщениями, в том числе, находятся ли они в Сети. Некоторые учетные записи обмена мгновенными сообщениями и электронной почты позволяют родителям определять, кто может отправлять сообщения их детям, и блокировать тех, кого нет в списке.

6. Спросите своих детей, с кем они общаются онлайн. Точно так же, как вы хотите знать, с кем общаются друзья ваших детей в сети, полезно знать, с кем они общаются в Интернете.

7. Расскажите своим детям об использовании надежных паролей электронной почты и их защите. Чем длиннее пароль, тем сложнее его взломать. Личная информация, ваше имя пользователя, распространенные слова или соседние клавиши на клавиатуре не являются надежными паролями. Дети могут защитить свои пароли, не сообщая их никому, включая своих друзей.

8. Напомните своим детям о необходимости защищать их личную информацию. ИИН, номер карточки, счета и пароли - это примеры информации , которую следует хранить в тайне.

9. Ознакомьте детей с законами Республики Казахстан Закон Республики Казахстан О персональных данных и их защите (с изменениями и дополнениями по состоянию на 01.07.2024 г.)

https://online.zakon.kz/Document/?doc_id=31396226&pos=3;-106#pos=3;-106 .

Воспользуйтесь своими правами по закону о персональных данных. Личная информация вашего ребенка является ценной, и вы можете многое сделать для ее защиты:

- Будьте разборчивы в вопросах получения вашего разрешения.
- Веб-сайты могут запрашивать ваше согласие различными способами, в том числе по электронной почте. Прежде чем давать согласие, убедитесь, что вы знаете, какую информацию сайт хочет собрать и что он планирует с ней делать. Вы можете дать компании разрешение на сбор некоторой личной информации, но не разрешать ей делиться этой информацией с другими лицами.

1.4 Мобильные телефоны

Научите своих детей думать о безопасности при пользовании мобильным телефоном, особенно при общении на ходу. При покупке телефона, учитывайте возраст вашего ребенка, его личностные качества, зрелость и обстоятельства вашей семьи. Достаточно ли он ответственен, чтобы следовать правилам пользования телефоном, установленным вами или школой?

Многие онлайн - приложения также доступны на мобильных телефонах, включая социальные сети, ведение блогов, загрузку контента, совместное использование медиа и редактирование видео. Научите своих детей думать о безопасности при использовании мобильный телефон.

Что вы можете сделать?

Будьте осторожны при обмене фотографиями и видео по телефону. Большинство мобильных телефонов теперь оснащены камерами и возможностью видеосъемки, что позволяет подросткам легко запечатлевать каждый момент и делиться им в дороге. Эти инструменты могут способствовать развитию креативности, но в то же время они создают проблемы, связанные с личной репутацией и безопасностью. Попросите своих подростков задуматься о своей личной жизни и жизни других людей, прежде чем делиться фотографиями и видео с помощью мобильного телефона. Легко размещать фотографии и видео в Интернете без ведома - не говоря уже о согласии - фотографа или человека, запечатленного на снимке. Это может вызвать неловкость и даже быть небезопасным. Проще заранее разобраться в том, какими средствами массовой информации они делятся , чем потом разбираться с ущербом.

Не поддерживайте травлю по мобильному телефону. Мобильные телефоны могут использоваться для травли других людей. Поговорите со своими детьми о том, как относиться к другим людям так, как они хотели бы, чтобы относились к ним. Манеры и этика, которым вы их научили, применимы и к телефонам.

Применяйте здравый смысл при работе с мобильными социальными сетями. На многих сайтах социальных сетей есть функция, которая позволяет пользователям просматривать свои профили и оставлять комментарии со своих телефонов, обеспечивая доступ из любой точки мира. Это означает, что фильтры, которые вы установили на своем домашнем компьютере, не будут ограничивать возможности детей пользоваться телефоном. Если ваши подростки используют мобильные устройства для создания своих профилей или блогов, поговорите с ними о том, как разумно вести себя в социальных сетях со своих телефонов.

Во многих мобильных телефонах теперь установлена технология GPS: дети с помощью этих телефонов могут точно определять местоположение где находятся их друзья, и они смогут точно определить их местонахождение. Посоветуйте своим детям использовать эти функции только с друзьями, которых они знают лично и которым доверяют. Кроме того, некоторые операторы мобильной связи предлагают услуги GPS , которые позволяют родителям определить местоположение своего ребенка.

Выберите подходящие опции и функции для телефона вашего ребенка. Как ваш оператор мобильной связи, так и сам телефон должны предоставить вам несколько вариантов настроек конфиденциальности

и контроля безопасности детей. Большинство операторов связи позволяют родителям отключать такие функции, как доступ в Интернет, отправка текстовых сообщений или загрузка файлов. Некоторые мобильные телефоны сделаны специально для детей. Они разработаны таким образом, чтобы быть простыми в использовании и обладать такими функциями, как ограниченный доступ в Интернет, управление минутами, конфиденциальность номера и кнопки экстренной помощи.

Многие телефоны имеют доступ в Интернет. Если ваши дети собираются пользоваться телефоном, а вы беспокоитесь о том, что они могут найти в Интернете, отключите доступ в Интернет или включите фильтрацию.

1.6 Защити свой компьютер

Безопасность вашего компьютера напрямую влияет на безопасность ваших онлайн-деятельностей и защиту вашего ребенка. Вредоносное программное обеспечение (ПО) может отслеживать или контролировать ваш компьютер, устанавливать вирусы, рассылать нежелательную рекламу, перенаправлять на несанкционированные веб-сайты или записывать ваши нажатия клавиш. Наличие вредоносного ПО на вашем компьютере может позволить злоумышленникам получить доступ к личной информации вашей семьи.

Чтобы обеспечить безопасность, используйте специализированное программное обеспечение и регулярно его обновляйте. Антивирусные и антишпионские программы проверяют входящие сообщения на наличие опасных файлов, а брандмауэр блокирует несанкционированные соединения. Ищите программы, которые могут обнаружить и устранить угрозы, автоматически обновляясь.

Важно также поддерживать операционную систему и веб-браузер в актуальном состоянии, изучая их функции безопасности. Хакеры часто используют уязвимости в старых версиях ПО, поэтому важно регулярно обновлять настройки безопасности и конфиденциальности вашей операционной системы и браузера. Ознакомьтесь с разделами "Сервис" или "Параметры", чтобы узнать, как выполнить обновление с использованием настроек по умолчанию.

Следите за “бесплатными” материалами. За бесплатными играми, мелодиями звонка или другими загрузками может скрываться вредоносное ПО. Скажите своим детям, чтобы они ничего не

загружали, если они не доверяют источнику и не проверили его с помощью программного обеспечения безопасности.

1.7 Обмен файлами

Некоторые дети делятся музыкой, играми или программным обеспечением онлайн. Пиринговый (P2P) файлообмен позволяет людям обмениваться файлами такого рода через неформальную сеть компьютеров, на которых установлено одно и то же программное обеспечение. Если ваши дети скачивают материалы, защищенные авторским правом, вы можете столкнуться с юридическими проблемами. Иногда в файлах общего доступа могут быть скрыты шпионские, вредоносные программы или порнография.

Несколько советов, которые помогут вашим детям безопасно обмениваться файлами:

- Правильно установите программное обеспечение для обмена файлами.
- Активируйте соответствующие настройки по умолчанию, чтобы ничего личного не было передано в общий доступ. По умолчанию почти все приложения для обмена файлами P2P будут размещать загруженные файлы в вашей папке “сохранить” или “загрузить”. Вот почему важно не устанавливать этот флажок. Если вы неправильно настроите настройки по умолчанию, другие пользователи P2P могут получить доступ к файлам, которыми вы никогда не собирались делиться, включая личные документы на вашем жестком диске, такие как налоговые декларации или другие финансовые документы.
- Прежде чем ваши дети откроют или воспроизведут какой-либо загруженный файл, посоветуйте им проверить его с помощью программного обеспечения безопасности. Убедитесь, что программное обеспечение безопасности обновлено и работает, когда компьютер подключен к Интернету.

1.8 Родительский контроль

Если вы беспокоитесь о том, что ваши дети, особенно учащиеся начальной школы, видят в Интернете, есть несколько инструментов, которые стоит рассмотреть. Имейте в виду, что, хотя родительский контроль хорошо работает для маленьких детей, у подростков, которые уже много лет находятся в Сети, вероятно, не возникнет особых проблем с его использованием или поиском других компьютеров для использования.

Родительский контроль включает в себя следующие опции:

- *Фильтрация и блокировка.* Эти инструменты ограничивают доступ к определенным сайтам, словам или изображениям. Некоторые продукты решают, что фильтровать, а что нет.; другие оставляют это на усмотрение родителей. Одни фильтры применяются к веб-сайтам, другие - к электронной почте, чатам и мгновенным сообщениям.

- *Блокировка исходящего контента.* Это программное обеспечение не позволяет детям делиться личной информацией в Интернете, в чатах или по электронной почте.

- *Ограничение по времени.* Это программное обеспечение позволяет ограничить время пребывания вашего ребенка в сети и установить время суток, в которое он может выходить в Интернет.

- *Браузеры для детей.* Эти браузеры фильтруют слова или изображения, которые считаются не подходит для детей.

- *Поисковые системы, ориентированные на детей.* Они выполняют ограниченный поиск или выводят на экран результаты поиска сайтов и материалов, подходящих для детей.

- *Инструменты мониторинга.* Этот тип программного обеспечения предупреждает родителей об активности в Интернете, не блокируя доступ. Некоторые инструменты записывают адреса веб-сайтов, которые посещал ребенок; другие выдают предупреждающее сообщение, когда ребенок посещает определенные сайты. Инструменты мониторинга можно использовать как с ведома ребенка, так и без него.

Лучший способ защитить своих детей в Интернете - поговорить с ними. Когда детям нужна важная информация, они чаще всего полагаются на своих родителей. Дети ценят мнение других людей своих сверстников, но, как правило, полагаются на помощь родителей в наиболее важных вопросах.

1.8 Кибербуллинг

Кибербуллинг **(**киберзапугивание) - это форма травли или домогательства, которая происходит в интернете через электронные письма, текстовые сообщения, онлайн-игры или комментарии на сайтах социальных сетей. Это могут быть разглашение слухов, публикация компрометирующих фотографий или создание страниц, направленных на унижение человека.

Поговорите со своими детьми о киберзапугивании и объясните, что они несут ответственность за свои слова и изображения в интернете. Оскорбительные сообщения не только могут навредить адресату, но и повлиять на репутацию отправителя, вызвать

отторжение со стороны сверстников и привлечение к нему внимания со стороны властей.

Просите детей сообщать вам о любых онлайн-сообщениях или изображениях, которые вызывают у них чувство угрозы или обиды. Если вам кажется, что ребенок находится под угрозой, обратитесь в полицию.

Периодически проверяйте страницы ваших детей, чтобы убедиться, что там нет нежелательных комментариев или созданных без их разрешения профилей. В случае обнаружения подобных случаев обращайтесь к администрации сайта с просьбой удалить их.

Если ваш ребенок сталкивается с киберзапугиванием через мгновенные сообщения или другие онлайн-сервисы, требующие список "друзей", заблокируйте или удалите хулигана из списка контактов.

Помогите ребенку противостоять киберзапугиванию, научив его, как правильно реагировать. Исследования показывают, что травля часто прекращается, когда сверстники вмешиваются в защиту жертвы. Поощряйте ребенка действовать таким образом, не участвуя в конфликте напрямую, но поддерживая жертву и при необходимости сообщая о происходящем.

Учите детей распознавать признаки киберзапугивания и отмечать их. Обратите внимание на изменения в поведении ребенка или его отношениях с другими онлайн.

Напомните, что вы являетесь примером для своих детей и важно демонстрировать им правильные модели поведения в интернете и в жизни.

1.9 Фишинг

Фишинг - это когда мошенники отправляют текстовые сообщения, электронные письма или всплывающие окна, чтобы заставить людей поделиться своей личной и финансовой информацией. Затем они используют эту информацию для кражи личных данных.

Вот как вы и ваши дети можете избежать фишинговой атаки.:

Не отвечайте на текстовые сообщения, электронные письма или всплывающие окна, в которых запрашивается личная или финансовая информация, и не переходите по ссылкам в сообщении.

Не поддавайтесь желанию вырезать и вставить ссылку из сообщения в свой веб-браузер. Например, если вы хотите проверить финансовый счет, введите веб-адрес, указанный в вашей платежной ведомости.

Не сообщайте личную информацию по телефону в ответ на текстовое сообщение. Некоторые мошенники отправляют текстовые сообщения, которые, как представляется , исходят от законного бизнеса, и просят вас позвонить по номеру телефона, чтобы обновить свой аккаунт или получить доступ к “возврату средств”. Если вы предоставите им свою информацию, они используют ее для начисления платежей от вашего имени.

Будьте осторожны при открытии любых вложений или загрузке любых файлов из электронных писем, которые вы получаете, независимо от того, кто их отправил. Неожиданные файлы могут содержать вирусы или шпионские программы, о которых отправитель даже не подозревает. Используйте программное обеспечение для обеспечения безопасности и регулярно обновляйте его.

Читайте свою почту; просматривайте выписки по кредитным картам и банковским счетам, как только вы их получите, чтобы проверить, нет ли несанкционированных списаний.

Привлеките своих детей к этим мероприятиям, чтобы они могли выработать хорошие навыки в области интернет-безопасности. Ищите “поучительные моменты” - если вы получили фишинговое сообщение, покажите его своим детям , чтобы помочь им понять, что сообщения на Интернет не всегда такой, каким кажется.

1.10 Секстинг

Отправка или пересылка фотографий, видео или сообщений откровенного сексуального содержания с мобильного телефона называется “секстингом”. Скажите своим детям, чтобы они этого не делали. Создавая, пересылая или даже сохраняя сообщения такого рода, они не только рискуют своей репутацией и дружбой, но и нарушают закон. Подростки с меньшей вероятностью сделают неправильный выбор, если будут знать о последствиях смс-переписки. Любой ребенок, у которого есть мобильный телефон, вероятно, использует его для отправки и получения текстовых сообщений и изображений. Это похоже на использование электронной почты или мгновенных сообщений, и в основном соответствует правилам этикета и соблюдайте правила безопасности. Если ваши дети переписываются, поощряйте их к этому, уважайте других.

Подумайте о том, как текстовое сообщение может быть прочитано и понято, прежде чем отправлять его. игнорируйте текстовые сообщения от незнакомых людей. узнайте, как заблокировать номера их мобильных телефонов. избегайте публикации номера своего мобильного телефона в Интернете. Никогда не

предоставляйте финансовую информацию в ответ на текстовое сообщение.

1.11 Знайте свои права

Как родитель, вы имеете право ознакомиться с любой личной информацией о вашем ребенке, собранной сайтом. Если вы попросите предоставить информацию, операторам веб-сайта необходимо будет убедиться, что вы действительно являетесь родителем, в противном случае они могут удалить эту информацию. Вы также имеете право отозвать свое согласие и удалить любую собранную информацию о вашем ребенке.

Ознакомьтесь с сайтами, которые посещают ваши дети. Если сайт требует от пользователей регистрации, посмотрите, какую информацию он запрашивает, и определите свой уровень комфорта. Вы также можете посмотреть, работает ли сайт похоже, что сайт придерживается самых элементарных правил, например, четко и на видном месте публикует политику конфиденциальности для родителей.

Ознакомьтесь с политикой конфиденциальности. Наличие политики конфиденциальности на сайте не означает, что он хранит личную информацию в тайне. Политика может помочь вам понять, устраивает ли вас то, какую информацию собирает сайт и как он планирует ее использовать или делиться ею. Если в политике указано, что нет ограничений на то, что сайт собирает, или на то, кто может это увидеть , то ограничений нет.

Задавайте вопросы. Если у вас есть вопросы о работе сайта или политики, спрашивайте. Политика конфиденциальности должна содержать контактную информацию лица, готового ответить на ваши вопросы.

2. МЕТОДИЧЕСКИЕ ИНСТРУКЦИИ ДЛЯ УЧИТЕЛЕЙ

Переход образовательных учреждений к цифровому обучению привел к увеличению числа студентов и преподавателей, использующих Интернет как для обучения, так и для преподавания. Во многих развивающихся семьях Содружества учащиеся все чаще используют онлайновые учебные материалы и инструменты оценки через устройства, принадлежащие родителям или старшим родственникам.

Учителя, ученики, родители и опекуны сейчас более уязвимы перед кибератаками, чем когда-либо прежде, поскольку они сталкиваются с различными угрозами безопасности из-за онлайнового и смешанного обучения. Недавние отчеты показывают рост киберугроз в секторе образования, что делает кибербезопасность главным приоритетом для преподавателей.

Школы обладают огромным количеством персональных данных, начиная от записей учащихся, информации о родителях, сведений о персонале, финансовых данных и заканчивая результатами исследований. Эти фрагменты информации представляют ценность не только для учреждений, но и для киберпреступников, которые могут использовать их для различных злонамеренных целей, включая кражу личных данных и мошенничество.

Многие образовательные учреждения, особенно в государственном секторе, часто имеют ограниченный бюджет. В результате они могут откладывать или полностью отказываться от важных обновлений инфраструктуры безопасности. Это делает школы более легкой мишенью по сравнению с корпорациями или государственными учреждениями, которые могут вкладывать больше средств в кибербезопасность.

Образовательным учреждениям может не хватать преданных своему делу ИТ-специалистов, обладающих опытом в области кибербезопасности. Зачастую ИТ-отделы в школах совмещают различные задачи: от обслуживания сети до устранения неполадок компьютеров. Это означает, что кибербезопасность не всегда может быть главным приоритетом, оставляя уязвимости без внимания.

Природа академической среды – это среда обмена и сотрудничества. Благодаря многочисленным устройствам, подключающимся к школьной сети, от компьютеров преподавателей до ноутбуков и смартфонов учащихся, существует огромная площадь для потенциальных атак. Эту открытость иногда можно использовать.

Несмотря на то, что школы могут не иметь больших бюджетов, киберпреступники знают, что они не могут позволить себе потерять свои данные. Ощущение срочности возврата важных данных (например, студенческих записей или академических исследований) может заставить учреждения платить выкуп, даже если они испытывают финансовые затруднения.

Многие сотрудники образовательных учреждений и учащиеся могут быть не в полной мере осведомлены о рисках фишинговых писем, небезопасном просмотре страниц или неправильных паролях. Отсутствие образования в области кибербезопасности облегчает проникновение киберпреступников в систему.

Школы и образовательные учреждения являются неотъемлемой частью нашего общества. Они играют решающую роль в формировании будущих поколений. Последствия кибератак на эти учреждения не только финансовые, но и имеют долгосрочные последствия для академической и личной жизни студентов и сотрудников.

Государственные органы, занимающиеся кибербезопасностью в Казахстане, это комитет по информационной безопасности Министерства цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан. Национальная служба реагирования на компьютерные инциденты осуществляет мониторинг и координацию действий по противодействию киберпреступности. В эти службы можно направлять жалобы через информационно-аналитическую систему "Электронные обращения" (E-Otinish).

2.1 Киберугрозы

Что такое кибератака?

Кибератака - это попытка киберпреступников, хакеров или других цифровых злоумышленников получить доступ к компьютерной сети или системе, обычно с целью изменения, кражи, уничтожения или раскрытия информации .

Кибератаки могут быть нацелены на широкий круг жертв: от отдельных пользователей до предприятий и даже правительств. При атаке на предприятия или другие организации целью хакера обычно является получение доступа к конфиденциальным и ценным ресурсам компании, таким как интеллектуальная собственность (IP), данные клиентов или платежные реквизиты.

1. Вредоносное ПО

Вредоносное ПО (или вредоносное программное обеспечение) - это любая программа или код, созданный с намерением нанести вред

компьютеру, сети или серверу. Вредоносное ПО является наиболее распространенным типом кибератак, главным образом потому, что этот термин включает в себя множество подмножеств, таких как программы-вымогатели, трояны, шпионское ПО, вирусы, черви, кейлоггеры, боты, криптоджекинг и любые другие типы вредоносных атак , которые используют программное обеспечение злонамеренным образом.

Тип	**Описание**
Программы-вымогатели	При атаке программы-вымогателя злоумышленник шифрует данные жертвы и предлагает предоставить ключ дешифрования в обмен на оплату. Атаки программ-вымогателей обычно осуществляются через вредоносные ссылки, доставляемые через фишинговые электронные письма, но также используются неисправленные уязвимости и неправильные настройки политик.
Бесфайловое вредоносное ПО	Бесфайловое вредоносное ПО - это тип вредоносной деятельности, который использует собственные законные инструменты, встроенные в систему, для выполнения кибератаки. В отличие от традиционных вредоносных программ, бесфайловые вредоносные программы не требуют от злоумышленника установки какого-либо кода в целевой системе, что затрудняет их обнаружение.
Шпионское ПО	Шпионское ПО - это тип нежелательного вредоносного программного обеспечения, которое заражает компьютер или другое устройство и собирает информацию о веб-активности пользователя без его ведома и согласия.
Рекламное ПО	Рекламное ПО - это тип шпионского ПО, которое отслеживает активность пользователя в Интернете, чтобы определить, какую рекламу ему показывать. Хотя рекламное ПО по своей сути не является вредоносным, оно влияет на производительность устройства пользователя и ухудшает удобство работы с ним.

Троян	Троян - это вредоносное ПО, которое выглядит как законное программное обеспечение, замаскированное под собственные программы операционной системы или безобидные файлы, такие как бесплатные загрузки. Трояны устанавливаются с помощью методов социальной инженерии, таких как фишинговые веб-сайты или веб-сайты-наживки. Вредоносное ПО zeus , вариант трояна , предназначено для доступа к финансовой информации и добавления компьютеров в ботнет.
черви	Червь - это автономная программа, которая копирует себя и распространяет свои копии на другие компьютеры. Червь может заразить свою цель через уязвимость в программном обеспечении или может быть доставлен посредством фишинга или смишинга. Встроенные черви могут изменять и удалять файлы, внедрять больше вредоносного программного обеспечения или реплицироваться на месте до тех пор, пока в целевой системе не закончатся ресурсы.
Руткиты	Вредоносное ПО-руткит - это набор программного обеспечения, предназначенный для предоставления злоумышленникам контроля над компьютерной сетью или приложением. После активации вредоносная программа устанавливает бэкдор-эксплойт и может доставить дополнительное вредоносное ПО. Буткиты идут еще дальше, заражая основную загрузку до загрузки операционной системы, что затрудняет их обнаружение.
Мобильное вредоносное ПО	Мобильное вредоносное ПО - это любой тип вредоносного ПО, предназначенный для мобильных устройств. Вредоносное ПО для мобильных устройств распространяется через вредоносные загрузки, уязвимости операционной системы, фишинг, смишинг и использование незащищенного Wi-Fi.
Эксплойты	Эксплойт - это часть программного обеспечения или данных, которая оппортунистически использует дефект в операционной системе или приложении для предоставления доступа

	неавторизованным субъектам. Эксплойт может использоваться для установки большего количества вредоносных программ или кражи данных.
пугающие программы	Scareware обманывает пользователей, заставляя их поверить, что их компьютер заражен вирусом. Обычно пользователь видит вредоносное ПО в виде всплывающего окна, предупреждающего о том, что его система заражена. Эта тактика запугивания направлена на то, чтобы убедить людей установить поддельное антивирусное программное обеспечение для удаления «вируса». После загрузки этого поддельного антивирусного программного обеспечения ваш компьютер может заразить вредоносное ПО.
Кейлоггер	Кейлоггеры - это инструменты, которые записывают то, что человек печатает на устройстве. Хотя существуют законные и легальные способы использования кейлоггеров, многие из них вредоносны. При атаке с использованием кейлоггеров программное обеспечение кейлоггера записывает каждое нажатие клавиши на устройстве жертвы и отправляет его злоумышленнику.
Ботнет	Ботнет - это сеть компьютеров, зараженных вредоносным ПО и контролируемых бот-пастухом. Пастух ботов - это человек, который управляет инфраструктурой ботнета и использует взломанные компьютеры для запуска атак, направленных на сбой в сети цели, внедрение вредоносного ПО, сбор учетных данных или выполнение задач, интенсивно использующих процессор.
МАЛСПАМ	Вредоносное ПО (MALSPAM) доставляет вредоносное ПО в качестве вредоносной нагрузки через электронные письма, содержащие вредоносный контент, такой как вирусы или зараженные вредоносным ПО вложения.
Атака дворника	Атака стиранием предназначена для безвозвратного удаления или повреждения данных в целевых системах. Они часто наблюдаются в геополитических конфликтах и в контексте хактивизма.

2.2 Атаки типа «отказ в обслуживании» (DoS)

Атака типа «отказ в обслуживании» (DoS) - это вредоносная целенаправленная атака, которая наполняет сеть ложными запросами с целью нарушения бизнес-операций.

В результате DoS-атаки пользователи не могут выполнять рутинные и необходимые задачи, такие как доступ к электронной почте, веб-сайтам, онлайн-аккаунтам или другим ресурсам, которыми управляет взломанный компьютер или сеть. Хотя большинство DoS-атак не приводят к потере данных и обычно устраняются без уплаты выкупа, они требуют от организации времени, денег и других ресурсов, необходимых для восстановления критически важных бизнес-операций.

Разница между атаками DoS и распределенным отказом в обслуживании (DDoS) связана с источником атаки. DoS-атаки исходят только из одной системы, тогда как DDoS-атаки запускаются из нескольких систем. DDoS-атаки блокировать быстрее и труднее, чем DOS-атаки, поскольку для остановки атаки необходимо идентифицировать и нейтрализовать несколько систем.

3. Фишинг

Фишинг - это тип кибератаки, в которой используются электронная почта, SMS, телефон, социальные сети и методы социальной инженерии, чтобы побудить жертву поделиться конфиденциальной информацией, такой как пароли или номера счетов, или загрузить вредоносный файл, который установит вирусы на ее компьютер. или телефон.

К распространенным фишинговым атакам относятся:

Тип	Описание
Целевой фишинг	Целенаправленный фишинг - это тип фишинговой атаки, которая нацелена на конкретных лиц или организации, как правило, посредством вредоносных электронных писем. Целью целевого фишинга является кража конфиденциальной информации, такой как учетные данные для входа, или заражение устройства цели вредоносным ПО.
Китобойный промысел	Китобойная атака - это тип атаки социальной инженерии, специально нацеленной на руководителей высшего звена или высшего звена с целью кражи денег или информации или получения доступа к компьютеру человека для проведения дальнейших кибератак.

Смишинг	Смишинг - это отправка мошеннических текстовых сообщений, призванных обманом заставить людей поделиться конфиденциальными данными, такими как пароли, имена пользователей и номера кредитных карт. В смиш-атаке могут участвовать киберпреступники, выдающие себя за ваш банк или службу доставки, которой вы пользуетесь.
Вишинг	Вишинг, голосовая фишинговая атака, представляет собой мошенническое использование телефонных звонков и голосовых сообщений, выдаваемых под видом авторитетной организации, с целью убедить людей раскрыть личную информацию, такую как банковские реквизиты и пароли.

2.3 Спуфинг

Спуфинг - это метод, с помощью которого киберпреступник маскируется под известный или доверенный источник. При этом злоумышленник может взаимодействовать с целью и получить доступ к ее системам или устройствам с конечной целью кражи информации, вымогательства денег или установки на устройство вредоносного или другого вредоносного программного обеспечения.

Спуфинг может принимать различные формы, в том числе:

Тип	Описание
Подмена домена	Подмена домена - это форма фишинга, при которой злоумышленник выдает себя за известную компанию или человека с поддельным веб-сайтом или доменом электронной почты, чтобы заставить людей доверять им. Как правило, на первый взгляд домен кажется законным, но при более внимательном рассмотрении можно обнаружить тонкие различия.
Подмена электронной почты	Подмена электронной почты - это тип кибератаки, направленной на предприятия с использованием электронных писем с поддельными адресами отправителя. Поскольку получатель доверяет предполагаемому отправителю, он с большей вероятностью откроет электронное письмо и воспользуется его содержимым, например вредоносной ссылкой или вложением.

Подмена ARP	Подмена протокола разрешения адресов (ARP) или отравление ARP - это форма поддельной атаки, которую хакеры используют для перехвата данных. Хакер совершает подмену ARP-атаки, обманом заставляя одно устройство отправлять сообщения хакеру, а не предполагаемому получателю. Таким образом, хакер получает доступ к сообщениям вашего устройства, включая конфиденциальные данные.

2.4 Атаки на основе личных данных

Атаки на основе личных данных чрезвычайно сложно обнаружить. Когда учетные данные действительного пользователя были скомпрометированы и злоумышленник маскируется под этого пользователя, часто очень трудно отличить типичное поведение пользователя от поведения хакера, используя традиционные меры и инструменты безопасности.

Некоторые из наиболее распространенных атак на основе личных данных включают в себя:

Тип	Описание
Kerberoasting	Kerberoasting - это метод атаки после эксплуатации, который пытается взломать пароль учетной записи службы в среде Active Directory (AD). При атаке Kerberoasting злоумышленник маскируется под пользователя учетной записи с именем участника службы (SPN) и запрашивает билет, который содержит зашифрованный пароль.
Атака «Человек посередине» (MITM)	Атака «человек посередине» - это тип кибератаки, при которой злоумышленник подслушивает разговор между двумя целями с целью сбора личных данных, паролей или банковских реквизитов и/или убедить жертву предпринять такие действия, как например, изменение учетных данных для входа, завершение транзакции или инициирование перевода средств.
Атака Pass-the-Hash	Pass the hash (PtH) - это тип атаки, при которой злоумышленник крадет «хешированные» учетные данные пользователя и использует их для создания нового сеанса пользователя в той же сети. Злоумышленнику не требуется знать или взломать пароль, чтобы получить доступ к системе. Вместо

	этого он использует сохраненную версию пароля для инициации нового сеанса.
Атака по золотому билету	При атаке по золотому билету злоумышленники пытаются получить неограниченный доступ к домену организации, обращаясь к пользовательским данным, хранящимся в Microsoft Active Directory. Злоумышленник использует уязвимости в протоколе аутентификации личности Kerberos, позволяющие обходить методы аутентификации.
Атака серебряного билета	Серебряный билет - это поддельный билет аутентификации, который часто создается, когда злоумышленник крадет пароль учетной записи. Поддельный билет службы зашифрован и обеспечивает доступ к ресурсам конкретной службы, на которую направлена атака с использованием серебряного билета.
Сбор учетных данных	При сборе учетных данных киберпреступники собирают учетные данные пользователей - такие как идентификаторы пользователей, адреса электронной почты, пароли и другую информацию для входа - в массовом порядке, чтобы затем получить доступ к системам, собрать конфиденциальные данные или продать их в темной сети.
Вброс учетных данных	Атаки с подстановкой учетных данных основаны на предположении, что люди часто используют один и тот же идентификатор пользователя и пароль для нескольких учетных записей. Таким образом, обладание учетными данными для одной учетной записи может предоставить доступ к другой, несвязанной учетной записи.
Распыление пароля	В основе атаки с распылением паролей злоумышленник использует один общий пароль для нескольких учетных записей в одном приложении. Это позволяет избежать блокировки учетной записи, которая обычно происходит, когда злоумышленник использует грубую атаку на одну учетную запись, перебирая множество паролей.
Атаки методом грубой силы	Атака методом перебора использует метод проб и ошибок для систематического подбора данных для

	входа, учетных данных и ключей шифрования. Злоумышленник вводит комбинации имен пользователей и паролей, пока, наконец, не угадает правильно.
Атаки на понижение версии	Атаки на понижение версии - это кибератака, при которой злоумышленники используют обратную совместимость системы, чтобы перевести ее в менее безопасные режимы работы, например, вынуждая пользователя перейти на HTTP-версию веб-сайта вместо HTTPS.

2.5 Атаки с внедрением кода

Атаки путем внедрения кода заключаются в том, что злоумышленник внедряет вредоносный код в уязвимый компьютер или сеть, чтобы изменить порядок его действий. Существует несколько типов атак с внедрением кода:

Тип	Описание
SQL-инъекция	Атака с помощью SQL-инъекции использует уязвимости системы для внедрения вредоносных операторов SQL в приложение, управляемое данными, что затем позволяет хакеру извлечь информацию из базы данных. Хакеры используют методы SQL-инъекций для изменения, кражи или удаления данных базы данных приложения.
Межсайтовый скриптинг (XSS)	Межсайтовый скриптинг (XSS) - это атака с внедрением кода, при которой злоумышленник вставляет вредоносный код на законный веб-сайт. Затем код запускается как зараженный сценарий в веб-браузере пользователя, позволяя злоумышленнику украсть конфиденциальную информацию или выдать себя за пользователя. Веб-форумы, доски объявлений, блоги и другие веб-сайты, которые позволяют пользователям публиковать собственный контент, наиболее подвержены XSS-атакам.
Вредоносная реклама	В атаках с использованием вредоносной рекламы используются многие другие методы, такие как SEO-отравление . Обычно злоумышленник начинает с взлома стороннего сервера, что позволяет киберпреступнику внедрить вредоносный код в медийное объявление или

	какой-либо его элемент, например копию рекламного баннера, креативные изображения или видеоконтент. После нажатия посетителем веб-сайта поврежденный код в объявлении установит на компьютер пользователя вредоносное или рекламное ПО.
Отравление данных	Отравление данных - это тип кибератаки, при которой злоумышленник намеренно компрометирует набор обучающих данных, используемый моделью искусственного интеллекта или машинного обучения, чтобы манипулировать работой этой модели. Когда набор данных манипулируется на этапе обучения, злоумышленник может внести предвзятость, намеренно создать ошибочные выходные данные, внести уязвимости или иным образом повлиять на прогнозирующие возможности модели.

2.6 Атаки социальной инженерии

Социальная инженерия - это метод, при котором злоумышленники используют психологические приемы, чтобы манипулировать людьми и заставить их совершить желаемое действие. Используя мощные мотиваторы, такие как любовь, деньги, страх и статус, злоумышленники могут собирать конфиденциальную информацию, которую они впоследствии могут использовать либо для вымогательства у организации, либо для использования такой информации для получения конкурентного преимущества.

Примеры атак социальной инженерии включают в себя:

Тип	Описание
предлог	Под предлогом злоумышленники получают доступ к информации, системе или пользователю, создавая ложный сценарий, который вызывает доверие жертвы. Это включает в себя выдачу себя за инвестиционного банкира, сотрудника отдела кадров или даже ИТ-специалиста.
Компрометация деловой электронной почты (BEC)	В ходе BEC-атаки злоумышленники выдают себя за доверенного пользователя, чтобы обманом заставить сотрудников или клиентов компании совершать платежи или передавать данные, среди прочего.

Кампания по дезинформации	Дезинформационные кампании - это преднамеренные попытки распространения ложной информации, особенно по политическим или военным причинам. Противники используют социальные сети, охватывающие огромную аудиторию, для усиления ложных нарративов посредством обильного использования ботов и фейковых аккаунтов, создавая ложное чувство консенсуса.
Услуга за услугу	Используя технику quid pro quo, злоумышленники нацелены на пользователей, предлагая заплатить в обмен на продукт или услугу.
Медовая ловушка	Атаки Honeytrap нацелены на людей, которые ищут любви или дружбы в приложениях/сайтах для знакомств. Злоумышленники создают поддельные профили и используют отношения, построенные с течением времени, чтобы обманом заставить жертву дать ей деньги, информацию или доступ к своей сети для установки вредоносного ПО.
Задняя дверь / контрейлерная перевозка	«Tailggate», также известный как «piggybacking», - это тип нападения, совершаемого лично, когда сотрудник компании следует за ним и просит его держать дверь открытой. Как только злоумышленник оказывается внутри объекта, он физически пытается украсть или уничтожить конфиденциальную информацию.

2.7 Инсайдерские угрозы

ИТ-команды, которые сосредоточены исключительно на поиске внешних по отношению к организации противников, видят только половину картины. Инсайдерские угрозы - это внутренние субъекты, такие как нынешние или бывшие сотрудники, которые представляют опасность для организации, поскольку имеют прямой доступ к сети компании, конфиденциальным данным и интеллектуальной собственности, а также знания бизнес-процессов, политики компании или другой информации, которая может помочь от такой атаки.

Внутренние субъекты, представляющие угрозу для организации, как правило, имеют злонамеренный характер. Некоторые мотиваторы включают финансовую выгоду в обмен на продажу конфиденциальной информации в даркнете и/или эмоциональное принуждение, например, используемое в тактике социальной инженерии . Однако некоторые инсайдерские угрозы по своей природе не являются злонамеренными, а являются небрежными. Чтобы бороться с этим, организациям следует внедрить комплексную программу обучения кибербезопасности, которая научит заинтересованные стороны осознавать любые потенциальные атаки, в том числе те, которые потенциально могут быть совершены инсайдерами.

2.8 Атаки с использованием искусственного интеллекта

По мере совершенствования технологий искусственного интеллекта и машинного обучения количество вариантов использования также увеличивается. Подобно тому, как специалисты по кибербезопасности используют искусственный интеллект и машинное обучение для защиты своей онлайн-среды, злоумышленники также используют эти инструменты для получения доступа к сети или кражи конфиденциальной информации.

Примеры кибератак с использованием искусственного интеллекта включают в себя:

Атака	Описание
Состязательный ИИ/МО	Состязательный искусственный интеллект и машинное обучение стремятся нарушить работу систем искусственного интеллекта и машинного обучения, манипулируя ими или вводя их в заблуждение. Они могут сделать это, внося неточности в обучающие данные.
Темный ИИ	Dark AI специально разработан для использования преимуществ использования технологий искусственного интеллекта и машинного обучения для использования уязвимостей. Темный ИИ обычно остается незамеченным, пока не будет нанесен ущерб.
Дипфейк	Дипфейки - это фальшивки, созданные искусственным интеллектом, которые выглядят очень реальными и могут изменить общественное мнение, нанести

	ущерб репутации и даже повлиять на политический ландшафт. Они могут иметь форму поддельных изображений, видео, аудио и т. д.
Социальная инженерия, генерируемая искусственным интеллектом	Злоумышленники создают поддельных чат-ботов или виртуальных помощников, способных взаимодействовать как люди и участвовать в разговорах с пользователями, чтобы заставить их предоставить конфиденциальную информацию.

2.9 Как защититься от кибератак

Эти основные шаги применимы ко всем:

Начните с паролей, которые используете вы и ваши ученики. Они сложные? Предложите юным учащимся менять свои пароли каждый год, а по мере взросления - чаще.

Подумайте о личной информации. Сюда входят имена, адреса, номера телефонов и любая другая информация, которая позволит незнакомцу точно узнать, кто вы. Будьте внимательны, делясь этой информацией: когда, где и почему вы вводите свою собственную информацию или данные учащихся?

Держите устройства в курсе. Это может защитить их от атак. Создайте процедуру регулярного обновления программного обеспечения и приложений.

Возьмите за правило в классе «остановиться и подумать», находясь в сети. Никогда не нажимайте на подозрительную ссылку или всплывающее окно. Это также относится к QR-кодам: не сканируйте те, которые выглядят подозрительно. Они могут легко содержать вредоносное ПО и вирусы.

Я преподаю маленьким детям. Чему я могу научить их о кибербезопасности?

Кибербезопасность может быть пугающей темой, но есть простые элементы, которые вы можете включить в свой класс. Кроме того, обучение маленьких детей кибербезопасности является важным шагом, помогающим им развить безопасные и ответственные привычки в Интернете.

Вот некоторые ключевые понятия, которым можно преподавать ученикам начальной школы:

Общее цифровое гражданство: научите младших школьников тому, как важно быть ответственным цифровым гражданином. Это включает в себя уважение к частной жизни других людей, а также

следование правилам и рекомендациям, установленным их родителями, школой или сообществом.

Уход за устройствами. Убедитесь, что дети знают, как ухаживать за своими устройствами, в том числе следить за ними и заряжать их. Это не только поможет предотвратить потерю устройств, но и заложит основу для их обновления в будущем.

Безопасность в Интернете. Сообщите учащимся, что им нужно быть осторожными с тем, что они нажимают, поскольку иногда объекты, на которые они нажимают, могут заразить их устройства вирусом. Сюда входят ссылки, всплывающие окна и реклама. Когда они подрастут, вы сможете распространить этот совет на QR-коды и загружаемые вложения. Они также должны знать о безопасности самого сайта.

Пароли. Помогите учащимся создавать надежные пароли. Поощряйте их использовать сочетание прописных и строчных букв, цифр и символов. В старших классах начальной школы учащихся следует поощрять по возможности устанавливать многофакторную аутентификацию.

Личная информация: научите учащихся быть осторожными при раскрытии личной информации в Интернете, такой как полное имя, адрес, номер телефона и день рождения. Поощряйте их делиться этой информацией только с проверенными источниками и напоминайте им никогда не публиковать ее публично. При создании имени пользователя учащиеся не должны использовать какую-либо часть своего настоящего имени или даты рождения.

Я преподаю ученикам средних классов. Чему я могу научить их о кибербезопасности?

К этому моменту ученики много времени проводят онлайн. У них есть доступ к устройствам, возможно, они используют социальные сети, играют в онлайн-игры и многое другое. Обучение детей средних школ кибербезопасности является важным шагом в продолжении развития у них здоровых онлайн-привычек.

Вот некоторые ключевые понятия, которым можно научить учащихся средних классов:

Конфиденциальность в Интернете. Продолжать укреплять концепцию конфиденциальности в Интернете, включая риски, связанные с публичным разглашением личной информации в социальных сетях. Подчеркните важность корректировки настроек конфиденциальности и осторожности в отношении того, чем они делятся в Интернете. Поговорите о том, как сайты и приложения могут использовать эти данные.

Осведомленность о фишинге: познакомьте учащихся с концепцией фишинга и покажите им, как идентифицировать подозрительные электронные письма, сообщения или ссылки, которые могут попытаться украсть личную информацию. Научите их быть осторожными, нажимая на незнакомые ссылки или делясь конфиденциальной информацией.

Вредоносное ПО и вирусы. Познакомьте с понятием вредоносного ПО и вирусов и обсудите потенциальные риски, которые они представляют для устройств и личной информации. Объясните учащимся, как важно использовать антивирусное программное обеспечение и не загружать ничего, что выглядит подозрительно.

Безопасность в Интернете. Расскажите об общих правилах безопасности в Интернете, включая осторожность при загрузке файлов из неизвестных источников, распознавание поддельных веб-сайтов и избегание взаимодействия с незнакомцами в Интернете.

Цифровой след. Помогите учащимся понять, как их действия в Интернете могут оставлять постоянный след. Когда они входят в мир социальных сетей, им становится еще легче поверить, что посты и сообщения исчезают, поэтому детям нужно понимать, что это не так.

Безопасность онлайн-игр: обратите внимание на важность безопасной практики онлайн-игр, включая риски, связанные с раскрытием личной информации во время игры и взаимодействием с незнакомцами.

Я преподаю старшеклассникам. Чему я могу научить их о кибербезопасности?

Учащимся старших классов может быть полезно более глубокое понимание концепций кибербезопасности. Крайне важно предоставлять практические занятия, моделирование и примеры из реальной жизни, чтобы привлечь старшеклассников к изучению концепций кибербезопасности.

Вот некоторые концепции кибербезопасности, которым можно преподавать старшеклассникам:

Ландшафт угроз: обсудите текущую картину кибербезопасности, включая распространенные типы киберугроз, такие как фишинг, вредоносное ПО, программы-вымогатели и социальная инженерия. Помогите учащимся понять развивающуюся природу рисков кибербезопасности и необходимость осведомленности.

Безопасное общение: расскажите учащимся о важности методов безопасной связи, таких как использование шифрования, приложений для безопасного обмена сообщениями и виртуальных частных сетей (VPN) для защиты их онлайн-разговоров и данных.

Социальная инженерия: объясните методы социальной инженерии, используемые для манипулирования людьми и получения несанкционированного доступа к системам или информации. Обсудите распространенные тактики социальной инженерии, такие как предлоги, фишинг и травля, чтобы помочь учащимся распознавать такие попытки и противостоять им.

Безопасность сети: Познакомьте учащихся с основами безопасности сети, включая брандмауэры, системы обнаружения вторжений (IDS) и безопасные методы Wi-Fi. Расскажите учащимся о рисках использования незащищенных общественных сетей Wi-Fi и важности защиты домашних сетей.

Конфиденциальность и защита данных. Расскажите учащимся о законах о конфиденциальности данных, таких как Общий регламент по защите данных (GDPR) и Закон штата Калифорния о конфиденциальности потребителей (CCPA). Помогите им понять свои права в отношении личных данных и важность организаций, защищающих данные пользователей.

Этический взлом и тестирование на проникновение. Познакомьте с концепцией этического взлома и тестирования систем, объяснив, как эти действия помогают выявлять уязвимости в системах и повышать безопасность. Подчеркните важность получения надлежащего разрешения и этических принципов при проведении тестов.

Многофакторная аутентификация (MFA). Расскажите учащимся о преимуществах использования многофакторной аутентификации для повышения безопасности учетной записи. Объясните, как MFA добавляет дополнительный уровень защиты, требуя второго этапа проверки, например, уникального кода, отправляемого на мобильное устройство.

Карьера в области кибербезопасности: познакомьте студентов с различными профессиями в области кибербезопасности, такими как аналитик по кибербезопасности, этический хакер, эксперт по цифровой криминалистике и консультант по безопасности. Обсудите навыки и квалификацию, необходимые для этих должностей, а также спрос на специалистов по кибербезопасности на современном рынке труда.

Онлайн-исследования и оценка источников. Помогите учащимся развить навыки критического мышления, позволяющие оценивать онлайн-источники на предмет надежности, достоверности и потенциальных предвзятостей. Научите их отличать достоверную информацию от потенциально вводящей в заблуждение, особенно в контексте кибербезопасности.

2.10 Обеспечение безопасности платформ онлайн-обучения

Существуют киберугрозы, с которыми сталкиваются платформы онлайн-обучения.

Управление привилегиями пользователей. Важно, чтобы школы управляли правами пользователей так, чтобы только доверенные пользователи имели доступ к их системам. Это не только поможет снизить риск рассчитанных атак, но и снизит риск случайных атак. Если сотрудник больше не числится в платежной ведомости, вам также необходимо немедленно отозвать его доступ.

Сторонние поставщики ветеринарных услуг. Школы и колледжи, естественно, будут использовать программное обеспечение и платформы, созданные сторонними поставщиками, такие как Microsoft 365 и Google Workspace. Прежде чем подписаться на любой из них, вам необходимо проверить их меры безопасности. Они такие же тщательные, как ваши? Сколько ваших конфиденциальных данных будет передано?

Глобальный разрыв в навыках кибербезопасности. Если после проверки их политики безопасности вы все еще не уверены, вы можете заполнить анкету. Очень важно, чтобы вы задавали вопросы и получали ответы, потому что 80% компаний, в которых произошла брешь в безопасности, обнаружили, что проблема возникла из-за системы их поставщика.

Расширьте возможности своих студентов. Помимо обучения вашего персонала, важно также обучать своих студентов вопросам кибербезопасности. Есть компании, которые в этом тоже помогают. Например, Cybint предлагает услуги по обучению кибербезопасности, ориентированные как на преподавателей, так и на студентов. Помимо прочего, важно научить своих учеников важности правильного управления паролями, например, создавать надежные пароли, а не записывать их на бумаге. Научите их также тому, как распознавать подозрительные электронные письма и что важно не нажимать на ссылки, которые выглядят неправильно. Вы также можете проводить онлайн-встречи с родителями и обсуждать такие вещи, как важность всегда использования безопасного Wi-Fi, а также возможность использования VPN для защиты трафика учащихся от попадания в чужие руки.

Защитите себя с помощью сквозного шифрования. Сквозное шифрование гарантирует, что ваши сообщения будут зашифрованы, и их увидят только вы и предполагаемый получатель. Это помогает обеспечить безопасность вас и ваших учеников в Интернете, предотвращая перехват и использование ваших важных данных против

вас. Например, вы можете создать собственное коммуникационное приложение со сквозным шифрованием для защиты сообщений, изображений и файлов (среди прочего), одновременно позволяя эффективным студентам и преподавателям общаться в режиме реального времени.

Фильтры контента устанавливают правила относительно типов веб-сайтов, к которым вы и ваши ученики можете получить доступ. Нежелательные категории блокируются, что служит тройной цели: уберечь учащихся от нежелательного контента, ограничить доступ к сайтам, которые, как известно, представляют высокий риск заражения вредоносным ПО, и повысить производительность.

2.11 Внедрение кибербезопасности в классе

Использование отдельных учетных записей для входа. Во время онлайн-обучения учащиеся не должны использовать общую учетную запись для входа в компьютер во время обучения. Это связано с тем, что использование общих учетных записей сопряжено с большим риском. Например, из любопытства учащийся может случайно поделиться личной информацией с общего компьютера или учетной записи, принадлежащей его родителю или опекуну, такой как свидетельство о рождении, номер водительского удостоверения, номер банковского счета, номер паспорта и адрес электронной почты, не зная, к каким последствиям это может привести.

Отключите или закройте веб-камеру, когда она не используется. Хакеры придумали более изощренные способы слежки за человеком с помощью веб-камер. Если в классе не требуется использование веб-камеры, учащиеся должны отключить или заблокировать ее с помощью крышки веб-камеры.

Использование паролей и менеджеров паролей. Пароль позволяет защитить информацию на наших устройствах и предоставить доступ только тем, у кого есть авторизованный пароль для получения доступа. Студенты могут использовать менеджеры паролей вместо того, чтобы записывать свои пароли в книги или документы, которые могут быть легко доступны каждому. Менеджеры паролей позволят создавать безопасные пароли, которые нельзя использовать повторно, вместо использования имен и даты рождения. Менеджеры паролей позволяют учащимся получать доступ к законным сохраненным ссылкам, таким как школьный портал, и предотвращать переход по мошенническим ссылкам, которые могут напоминать школьный портал.

Отключить микрофоны. Еще один способ шпионить хакером - использовать микрофоны, чтобы подслушивать разговоры. Студентам

следует отключать микрофоны, когда они не используются, чтобы хакеры не могли подслушать их частную дискуссию.

Использование удобной для студентов поисковой системы. Студентам следует использовать удобные для детей поисковые системы, такие как kiddle, kidrex и wackysafe. Это безопасные поисковые системы, которые позволяют учащимся искать подходящую для них информацию, изображения, видео и новости.

Идентификация личной информации. Прежде чем начать урок, учителя могут обсудить, что такое информация, позволяющая установить личность (PII), почему важно не разглашать эту информацию и риски, связанные с раскрытием этой информации. Студенты могли бы принять участие, определив, что, по их мнению, представляет собой ЛИИ, и привести примеры.

Обновление программного обеспечения компьютера. Студенты должны убедиться, что их устройства обновлены. Им следует постоянно проверять наличие доступных обновлений программного обеспечения и перед этим консультироваться со своими родителями, опекунами или учителями. Обновления позволят вашему устройству иметь актуальное программное обеспечение и снизят вероятность кибератак.

Выключите или заблокируйте устройства. Студенты должны выключать или блокировать компьютеры, ноутбуки или планшеты, когда они не используются. Эти устройства должны быть защищены надежными паролями. Устройства, оставленные включенными, когда они не используются, подвергаются риску атак и доступа со стороны посторонних лиц.

Отключить службы определения местоположения. Устройства имеют функцию, которая позволяет прикреплять к местоположению такие данные, как результаты веб-поиска и изображения. Чтобы сохранить анонимность, отключите такие функции, чтобы ваши перемещения не могли отслеживаться на основе вашей онлайн-активности.

Ссылки и загрузки. Нажатие на ссылки и загрузка контента из Интернета, особенно если он вредоносный, может причинить вред, например, к краже информации, такой как пароли, замедлению работы или сбою устройства и т. д. Учащиеся должны проконсультироваться со своими родителями, учителями и опекунами, прежде чем нажимать на ссылки, которыми они не являются. уверенность или загрузка контента из Интернета, особенно по электронной почте.

3. МЕТОДИЧЕСКИЕ ИНСТРУКЦИИ ДЛЯ ШКОЛЬНИКОВ

Интернет постоянно меняется, поэтому необходимы новые способы обеспечения безопасности. В разделе описано как размещение чего-либо неподобающего в Интернете может иметь серьезные последствия, какую личную информацию запрещено публиковать и как защитить вашу конфиденциальность.

Чем занимаются дети в интернете:

– Переписываются или играть в игры на своем мобильном телефоне или телефоне родителей?
– Используют Google, чтобы помочь с домашним заданием?
– Играют онлайн на компьютере, PlayStation 2 или Xbox?
– Ведут прямые трансляции?
– Смотрят видео на YouTube?
– Играют в виртуальном мире, таком как Roblox или Minecraft?
– Организуют видеочат с друзьями и семьями?
– Пользуются сайтом социальной сети или приложением, таким как Instagram или TikTok?

Независимо от того, что нравится делать в Интернете, есть одно правило, которое применимо к любой ситуации: необходимо избегать риски. Вот несколько примеров принятия рисков:

– Отправка оскорбительных сообщений
– Размещение неподобающих фотографий
– Повторный показ изображений других людей
– Общение с людьми, которых вы не знаете.
– Посещение сайтов для взрослых

У всех нас были взаимодействия или ситуации с этими приложениями или играми, которые это поставило нас в неловкое положение. Возможно, у вас был разговор, от которого вы почувствовали себя плохо, или вас отметили на фотографии, где вам не понравилось, как вы выглядите, или комментарий к вашему посту был не самым приятным. Возможно, именно вы оставили этот неприятный комментарий или разместили фотографию друга, не спросив его разрешения.

К сожалению, подобные переписки могут стать не просто неприятными / некомфортными, а взаимодействие может стать более рискованным. Независимо от того, что вам нравится делать в Интернете, есть *одно правило*, которое применимо к любой ситуации: **избегайте рисков!**

Вот несколько примеров принятия рисков:

- Рассылка оскорбительных сообщений

- Публикация неподобающих фотографий или совместное использование их в сети

- Повторный обмен изображениями других людей

- Посещение сайтов для взрослых

Важно не только избегать неприемлемого контента в Интернете, но и воздерживаться от его размещения самостоятельно. Не делитесь личной информацией в Интернете, особенно с незнакомыми людьми. Все это сопряжено с риском, поскольку вы можете попасть в беду из-за этого или подвергнуть себя опасности. Защитите себя и других, сделав ответственный выбор. Это поможет вам избежать рисков и оставаться в безопасности онлайн.

Одним из таких рисков является возможность увидеть то, чего вы не хотели бы видеть. В Интернете можно найти множество материалов, но, возможно, вы не готовы к просмотру некоторых из них. Это считается *неприемлемым* контентом.

Неприемлемый контент включает в себя:

– Видео для взрослых;

– Насилие;

– Разжигание ненависти;

– Рискованные или незаконные действия, такие как опасные трюки или игры с выпивкой;

– Изображения ваших или чужих интимных мест.

Может показаться, что просматривать такой контент круто, но есть причина, по которой он не для детей. Это может заставить вас почувствовать себя плохо, сбить с толку, некомфортно или даже испугаться. Не просматривайте и не открывайте эти связи.

Что вам следует делать если вы все-таки наткнулись в Интернете на неприемлемый контент, вы можете:

– Сообщить об этом на веб-сайте или в приложении, где вы его обнаружили;

– Воспользуйтесь кнопкой "Назад";

– Выключите экран;

– Сообщите взрослому, которому вы доверяете, если чувствуете себя расстроенным или хотите поговорить об этом;

– Не удаляйте свою учетную запись.

Если вы все же наткнетесь в Интернете на неприемлемый контент, вы можете:

- Сообщить об этом на веб-сайт или в приложение, где вы его обнаружили, или в службу поддержки пользователей.

- Используйте кнопку "Назад", чтобы выйти из страницы или вернуться на главную страницу.

- Выключите экран.

- Поговорите со взрослым, которому вы доверяете (назовите несколько примеров взрослых, которым вы доверяете), чтобы они помогли вам решить эту проблему. Если вы расстроены или просто хотите поговорить об этом, взрослые могут помочь вам разобраться в своих эмоциях. Они могут помочь вам понять, что делать, если вы столкнетесь с неприемлемым контентом.

- Воздержитесь от удаления своей учетной записи, поскольку вы можете удалить доказательства, которые могли бы предотвратить подобное с вами или с кем-либо еще в будущем. Если вы уже видели что–либо из этого контента, не чувствуйте себя виноватым - это не ваша вина. Поговорите с взрослым, которому вы доверяете или который находится в безопасности.

Теперь, когда вы стали старше, вы не только видите что-то в Интернете, но и высказываете свое мнение. Поэтому убедитесь, что вы не высказываете ничего неподобающего.

3.1 Неприемлемая информация

Неприемлемая информация, которой вам не следует делиться в Интернете, включает:

- Постыдные высказывания о вас или других людях;
- Демонстрация фотографий;
- Розыгрыши;
- Незаконное поведение (наркотики, алкоголь и т.д.);
- Разжигание ненависти.

Неуместные изображения вас или кого-либо еще размещение этих фотографий в Интернете означает, что вы можете:

- Заслужить плохую репутацию среди друзей или в школе;
- Попасть в неприятности дома, в школе или даже с законом;
- Подорвет ваши шансы попасть в спортивные команды, клубы, колледжи или даже получить работу в будущем;
- Действительно причинит кому-то боль и создаст массу проблем в его жизни. Вы не можете контролировать, чем это закончится
- Уберите немного информации из приложения и посмотрите, как вы к этому относитесь, возможно, вы измените свое мнение о размещении;
- Если вы уже что-то публиковали, пожалуйста, помните, что дополнительная справка.

- Не забудьте взять немного информации, прежде чем принимать решение о публикации чего-либо.

В какой-то момент мы могли бы подумать, что было бы неплохо опубликовать что-то, но позже мы меняем свое мнение и понимаем, что это был не самый удачный пост, прежде чем что-то публиковать. Уберите немного меня из приложения и посмотрите, как вы к этому относитесь, может быть, вы передумаете публиковать. Помните, что как только вы публикуете что-либо в Интернете, это становится доступным для многих. Один из полезных советов - спросите себя: “Хочу ли я, чтобы мои родители, бабушки и дедушки или учителя увидели это?” Если нет, то, вероятно, публиковать это не стоит.

Еще один полезный совет - немного отвлечься от электроники и заняться займитесь чем-нибудь другим; например, прогуляйтесь, послушайте музыку или поговорите об этом с другом или взрослым, которому доверяете.

Мы переходим от формулировки “как только ваше изображение появится в сети, оно останется там навсегда. Любой желающий может сделать снимок экрана или сохранить изображение, и вы не сможете забрать его обратно или запретить другим публиковать его. Вы можете удалить свой пост / сообщение, но это не в вашей власти, если кто-то другой сохранит его.

Если вы уже публиковали что-то, пожалуйста, помните, что есть помощь. Нам всем когда-нибудь понадобится помощь, и просить о ней - это абсолютно нормально. Вам не обязательно проходить через что-то подобное самостоятельно.

3.2 Конфиденциальность в Интернете

Вам также следует постараться защитить свою конфиденциальность в Интернете. Избегайте размещения слишком большого количества информации, в том числе информации о себе и фотографий.

Раскрывать слишком много информации о себе в Интернете рискованно, потому что:

- Информация может очень быстро распространиться
- Она может попасть к людям, которым вы, возможно, не захотите ее показывать
- Это может причинить вам боль и даже вызвать эмоциональную травму

Личный информация. Личная информация, которой вы не должны делиться в Интернете , включает в себя ваши:

- Пароли

- Домашний адрес
- Местоположение
- Номер домашнего/сотового телефона
- Адрес электронной почты
- Информация о планах на отпуск/логистике
- Динамика семьи
- Информация о семье.

Все, что вы публикуете в Интернете, потенциально может быть замечено большим количеством людей, поэтому вы должны быть осторожны с тем, чем вы делитесь и с кем вы делитесь этим. Обмен личной информацией в Интернете представляет угрозу безопасности. Вы можете:

- Стать жертвой онлайн-мошенничества
- Ваш компьютер или онлайн-аккаунты были взломаны
- Люди могут использовать эту информацию, чтобы причинить вам вред другими способами.

Будьте осторожны и не делитесь личной информацией ни с кем. Вы также должны быть осторожны и не делиться личной информацией о своей семье или друзьях и в Интернете тоже. Вот два примера того, когда вам не следует делиться чужой личной информацией.:

- Один друг просит у вас номер телефона другого человека. Не публикуйте его в Интернете! Вместо этого позвоните ему по этому номеру.

- Ваша подруга просит ввести пароль от вашей электронной почты, потому что, по ее словам, лучшие друзья делятся всем. Не сообщайте свой пароль! Ваш родитель или опекун - единственный человек, с которым можно поделиться вашим паролем.

- В школе быстро распространяется слух о том, что кто-то влюблен в вас? Вот почему вы не хотите делиться слишком большим количеством информации в Интернете – это может быстро распространиться и выйти из-под контроля.

Вы, конечно, можете поделиться определенной информацией, например, своим любимым фильмом, но вы определенно не хотите делиться личной информацией, например, откровенными текстами или фотографиями.

3.3 Правила конфиденциальности

- Не разглашайте личную информацию
- Не публикуйте видео или фотографии своих интимных мест
- Используйте настройки конфиденциальности
- Выбирайте подходящие имена для показа на экране

- Принимайте только тех друзей, которых вы знаете в реальной жизни

- Не шутите с угрозами

- У вас есть профиль в социальных сетях или приложениях, таких как Instagram, TikTok?

- Играйте в виртуальном мире, таком как Roblox или Minecraft?

- У вас есть игровой аккаунт на Xbox или PlayStation.

Убедитесь, что вы не публикуете слишком много информации ни в одном из этих онлайн аккаунтов. Вот несколько советов, чтобы не раскрывать слишком много информации в Интернете:

- Не разглашайте личную информацию, которая включает в себя ваш адрес, номера телефонов, пароли и расписание.

- Используйте настройки конфиденциальности и проверяйте их - это означает, что ваша страница должна быть закрытой и ограничить доступ к вашим публикациям и фотографиям тех, кто может их видеть.

- Выбирайте подходящие псевдонимы - вы же не хотите произвести неправильное впечатление, поэтому выбирайте то, что не смущает и не оскорбляет.

- Принимайте только тех друзей, которых вы знаете в реальной жизни - это касается и “друзей друзей”. Если вы с ними не знакомы, не добавляйте их! Если вы согласны или уже сделали это, ограничьте доступ к тому, что они могут видеть, и к тому, как они взаимодействуют с вами.

- Не шутите с угрозами - они могут быть вырваны из контекста, и у вас могут возникнуть серьезные проблемы, особенно если это касается кого-то другого.

3.4 Неуместные просьбы

Неуместная просьба включает в себя:

- Просьбы о том, чтобы вы делали то, чего вы не хотите делать.

- Просьбы о том, чтобы вы делали то, что вам неудобно делать или что подвергает вас риску.

Причины, по которым подростки могут захотеть выполнить неуместные просьбы:

- Возможно, вы чувствуете, что на вас оказывают давление, потому что вам кажется, что все так делают.

- Возможно, вам действительно нравится человек, который вас об этом просит.

- Иногда кажется, что все происходит так быстро, что вам кажется, что вам нужно принимать поспешные решения.

- В некоторых случаях вы хотите это сделать и считаете, что это хорошая идея.
- Они могут попросить вас сделать то, чего вы не хотите делать.
- Это могут быть вещи, которые вам неудобно выполнять или которые подвергают вас риску

Это называется неуместной просьбой.

- Возможно, вы чувствуете, что на вас оказывают давление, потому что вам кажется, что все так делают.

- Возможно, вам действительно нравится человек, который вас просит.

- Иногда кажется, что все происходит так быстро, что вы чувствуете необходимость принимать поспешные решения.

- Возможно, вы захотите это сделать, потому что видите какие-то преимущества или положительные результаты.

Но вы должны помнить, что подростки не часто обращаются с неподобающими просьбами; около 80% подростков не отправляют неподобающие изображения. Если кто-то просит вас прислать компрометирующие изображения или оказывает на вас давление, отступите. Не торопитесь, подумайте об этом пять минут и поговорите с кем-нибудь из взрослых, кому вы доверяете, или с другом. Возможно, человек, который просит фотографии, не разделяет ваших интересов.

Посмотрите, как он отреагирует, когда вы скажете "нет". Если проситель разозлится или продолжит оказывать на вас давление, это должно стать тревожным сигналом о намерениях этого человека.

Вот несколько примеров неуместных просьб:

- Вы общаетесь в видеочате с друзьями, и один из них в шутку просит вас задрать футболку.

- Кто-то отправляет вам по электронной почте ссылку на сайт для взрослых, который он хочет, чтобы вы посмотрели.

Независимо от того, кто обращается с просьбой - подросток постарше, взрослый, незнакомец или друг, - вы не обязаны этого делать. Некоторых детей беспокоят эти просьбы, в то время как других - нет. Но у всех вас есть право сказать “нет”. Попрактикуйтесь в том, как вы будете отклонять эти просьбы, чтобы подготовиться, если вы когда-нибудь столкнетесь с подобными ситуациями.

3.5 Груминг

Многие подростки сейчас обсуждают, что такое “груминг”.

- Спросите участников: что, по их мнению, такое груминг?

- Груминг - это преднамеренный процесс, когда кто-то, как правило, взрослый, устанавливает с вами отношения с намерением

причинить вам боль, предлагая неприемлемый контент, например, отправлять откровенные фотографии или встречаться лично.

Определение груминга:

Груминг - это преднамеренный процесс, посредством которого преступники постепенно вступают в сексуальные отношения с жертвой и поддерживают их в тайне. Груминг позволяет правонарушителям постепенно преодолевать естественные границы задолго до того, как произойдет сексуальное насилие. На первый взгляд, груминг ребенка может выглядеть как тесная связь между взрослым-нарушителем, ребенком-мишенью и (потенциально) теми, кто ухаживает за ребенком. Уход за ребенком онлайн также известен как онлайн-консультирование.

Онлайн-принуждение: предполагает общение человека с кем-либо, предположительно с ребенком, через Интернет с намерением совершить сексуальное преступление или похитить его. Это обширная категория онлайн-эксплуатации, включающая в себя сексуальную эксплуатацию, при которой ребенка готовят к съемке откровенных изображений сексуального характера и/или, в конечном итоге, к личной встрече с кем-либо в сексуальных целях, или к вступлению в сексуальную переписку онлайн, или в некоторых других случаях. например, для продажи сексуальных изображений ребенка. Такого рода столкновения происходят в каждой платформе; социальные сети, приложения для обмена сообщениями, игровые платформы и т.д.

Подросткам и взрослым постарше:

- не следует рассказывать о том, как они встречаются с вами
- не следует просить показать откровенные фотографии
- не следует просить о встрече лично без оповещения взрослых.

Если с вами такое случается, это не ваша вина. Поговорите о случившемся со взрослым, которому доверяете. Некоторые неуместные просьбы могут перерасти в опасные отношения. Вы можете общаться с подростками постарше и взрослыми, которых вы не знаете, онлайн, например, когда играете в игры, но они никогда *не должны этого делать*:

- Говорить о том, что вам не нравится;
- Просить показать откровенные фотографии;
- Предлагать вам встретиться в автономном режиме;
- Заставлять вас делать что-то, в чем вы чувствуете неуверенность, дискомфорт, страх, грусть или замешательство.

Некоторые вещи могут происходить быстро, когда вы заводите друзей онлайн, и вы чувствуете необходимость принимать поспешные решения или делать то, чего обычно не стали бы делать со своими

друзьями онлайн. Вступать в бой - не очень хорошая идея и выполняйте неподобающие просьбы. Если это случится с вами, сделайте перерыв и поговорите с кем-нибудь из взрослых, кому вы доверяете, или с другом. Помните, что всегда нужно защищать себя и других. Сделайте небольшой перерыв и отойдите от телефона, чтобы подумать или поговорить с кем-нибудь, возможно, это поможет вам принять решение, от которого вы будете чувствовать себя более комфортно, и обезопасит вас.

Если с вами произойдет что-то из вышеперечисленного, обратитесь к взрослому, которому вы доверяете, и сообщите о том, что произошло с приложением или веб-сайтом.

Не у всех в Сети плохие намерения, но вам следует быть осторожными, общаясь с незнакомыми людьми. И даже если просьба исходит не от взрослого человека, вам не следует встречаться в автономном режиме.

Некоторые люди могут пытаться встретиться с вами в автономном режиме, льстя вам, рассказывая об общих интересах и притворяясь, что им не все равно. Это называется уход за собой. Не доверяйте никому, кто пытается:

- Отправлять подарки по почте, например, открытки, на мобильный телефон или веб-камеру
- Плохо отзываться о своей семье и друзьях
- Вызывать у вас чувство вины, стыда или плохого отношения к себе
- Разговаривают на взрослые темы
- Делятся откровенными фотографиями или просят их показать
- Требуют, чтобы вы быстро отвечали или входили в систему, когда вас об этом попросят
- Следите за всеми своими аккаунтами в социальных сетях
- Задавайте много ненужных личных вопросов о вас или вашей семье, например, где работают ваши родители или какой распорядок дня у ваших братьев и сестер.
- Задавать вам неуместные личные вопросы (например, спрашивать о правилах личной гигиены).
- Просить вас хранить секреты от вашей семьи и друзей
- Пытаться вести неподобающие разговоры

Помните, что тот, кто заботится о вас, хотел бы для вас самого лучшего. Это означает, что ваши друзья:

- Хотели бы, чтобы у вас были прекрасные отношения с семьей и друзей и помог бы вам достичь этого

- Поддерживал бы вас и поощрял делать то, что делает вас счастливыми и приносит вам пользу

- Хотел бы, чтобы все знали о ваших отношениях

- Не заставит вас чувствовать грусть, замешательство, гнев, вину, дискомфорт, одиночество, тревогу и не вызовет у вас каких-либо неприятных, затяжных ощущений.

- Если возникнет конфликт, они возьмут на себя ответственность за свои действия, признают ваши чувства и попытаются решить проблему, вместо того чтобы обвинять вас или заставлять делать то, чего вы не хотите, чтобы решить проблему.

Доверие укрепляется благодаря мне, и на протяжении всей дружбы мы разделяем множество счастливых и сложных моментов. Научиться доверять кому-то можно только через меня, потому что этот опыт покажет вам, принимает ли друг близко к сердцу ваши интересы и будет ли он рядом с вами.

Если что-то из этого случилось с вами, знайте, что это не ваша вина. Поговорите о случившемся со взрослым, которому доверяете. Взгляните на запись в дневнике подростка о человеке, с которым он познакомился в Интернете:

“Сегодня он прислал мне мобильный телефон. Теперь мы можем говорить обо всем, о чем не нужно знать ни мне, ни моим родителям. Он попросил меня держать это в секрете, потому что мои родители не поймут”. Вы видите какие-нибудь признаки того, что за подростком ухаживают?

Признаки груминга включают в себя:

- все время присылает сообщения на мой мобильный телефон;

- разговаривает со мной все время;

- просит хранить секреты от родителей;

- говорит, что родители не поймут;

- влияет на мое настроение, часто меняется настроение в негативную сторону;

- изолирует меня от друзей и семьи.

Есть разница между личной жизнью и секретами. В здоровых отношениях секретов не бывает. Секреты обычно подразумевают сокрытие чего-то неподобающего. Здоровые отношения должны заставлять вас чувствовать удовлетворение, уверенность и подъем. Важные для вас люди будут счастливы с вами и за вас.

Что вы можете сделать:

- Заблокировать контакт, не принимать сообщения;
- Не встречаться, не рассказывать о себе;

Нехорошо, когда люди, которых вы знаете онлайн или офлайн, просят вас или оказывают на вас давление, заставляя вас чувствовать себя некомфортно. Если кто-то из ваших знакомых просит вас или оказывает на вас давление, заставляя вас чувствовать себя некомфортно, пытается заставить вас встретиться в реальной жизни, требует денег или обращается с неподобающей просьбой, вы можете сделать много вещей, чтобы защитить себя и других, в том числе:

- блокировать их;
- не принимать в друзья;
- отказываться встречаться с ними отдельно тет-а тет;
- публиковать их в приложении /игре и на веб-сайте;
- не удалять свою учетную запись. Они могут связаться с вами другими способами, и в итоге вы можете удалить важные доказательства.
- сообщить об этом взрослому, которому доверяете.

Даже если вы выполняли их требования в прошлом или вам кажется, что у вас нет другого выхода, вам не обязательно делать это снова. **Пожалуйста, не чувствуйте себя виноватым, это не ваша вина.** Следуйте тем же правилам, чтобы защитить себя и других. Обратиться за помощью - это нормально. Вам не обязательно справляться со всем этим в одиночку. Это серьезная проблема, и это может быть преступлением.

Помните, что один и тот же человек может совершать аналогичные действия по отношению к другим людям. дети, которые могут быть младше вас. Сообщая о таком поведении, вы можете защитить других. Вы можете сообщить об этом человеке самостоятельно или с помощью взрослого, которому вы доверяете или с которым чувствуете себя в безопасности. Сообщите доверенным взрослым обо всех, кто:

- отправляет вам фотографии или видео для взрослых;
- просит вас прислать свои фотографии;
- разговаривает с вами на взрослые темы;
- просит встретиться с вами лично;
- шантажирует вас, требуя денег или больше ваших фотографий - это называется сексуальным домогательством. Это преступление, и вы должны сообщить о нем, чтобы защитить себя и других. Уважение означает, что вы можете постоять за себя и убедиться, что эти люди не будут беспокоить вас или кого-либо еще в будущем.

Возможно, вам будет трудно разговаривать со взрослыми, потому что:

- вы боитесь потерять доступ к Интернету;

- возможно, вы считаете, что взрослые не могут помочь, или не можете найти надежного взрослого, которому можно доверять;

- вам может быть неловко вести беседу;

- вы боитесь, что ваши родители или опекуны будут винить вас - некоторые люди, наши родители /воспитатели, советуют нам чего-то не делать. Если мы это делаем, мы чувствуем, что они будут винить нас, что очень затрудняет общение с ними. В основном это происходит потому, что мы не хотим разочаровывать наших родителей, или потому, что чувство вины - это ужасное и пугающее чувство.

- вы боитесь, что ваши родители разозлятся на вас - если наши родители запрещают нам что-либо делать или если мы чувствуем, что они разозлятся на нас, нам трудно подойти к ним и попросить о помощи. Особенно если мы думаем, что у нас заберут телефон.

- вы чувствуете себя виноватым и считаете, что это была ваша вина, хотя это не так. Иногда, когда мы делаем что-то, потому что доверяем кому-то или симпатизируем ему, а этот человек причиняет нам боль или предает наше доверие, чувство, что это наша вина, является обычным, нормальным чувством. Мы думаем, что не должны жаловаться или обращаться за помощью, потому что нам кажется, что мы этого заслуживаем, или нам кажется, что, поскольку это была наша вина, мы ничего не можем поделать.

- вы хотите попросить о помощи, но не знаете как.

Все эти чувства нормальны, и они могут быть действительно непреодолимыми. Однако важно обратиться за помощью, к своему взрослому, которому вы доверяете или к учителю. Даже если это трудно, важно поговорить со взрослым, которому вы доверяете, например, с вашими родителями, родственником, учителем или консультантом в школе. Люди не должны заставлять вас чувствовать дискомфорт, грусть или страх, особенно взрослые. Вам следует обратиться за помощью, чтобы остановить их, рассказав кому-нибудь об этом.

3.6 Неприемлемые изображения

Неприемлемый контент может относиться к:

- Отправка фотографий/видео с обнаженной или частично обнаженной натурой другому лицу.

- Вести сексуальные разговоры в текстовых сообщениях / онлайн. Это не так распространено, как вам может показаться.

Вы можете сообщить об этом самостоятельно или вместе со взрослым, которому доверяете. Сообщите обо всех, кто:

- присылает вам фотографии или видео для взрослых;

- просит вас прислать свои фотографии;

- разговаривает с вами на взрослые темы;

- просит встретиться с вами лично;

- шантажирует вас, требуя денег или большего количества ваших фотографий. Это называется сексуальным домогательством; это преступление, и вы должны сообщить о нем, чтобы защитить себя и других.

Есть много причин, по которым кто-то может захотеть поделиться обнаженной натурой, не делитесь обнаженной натурой. Повторно публиковать или пересылать чью-либо обнаженную натуру - это ненормально! Это серьезное злоупотребление доверием! И, публикуя это повторно, вы действительно причиняете боль человеку на фотографии. Удалите фотографию, если кто-то пришлет вам фотографию другого человека, которая, как вы знаете, была сделана не для вас. Будьте честны и обратитесь к человеку, который вам ее прислал, и скажите ему, что это не нормально

Каковы некоторые последствия публикации фотографии?

- она может потеряться или оказаться не на своем месте;

- ее могут публиковать без разрешения;

- это может стать источником смущения /стыда /вины;

- это может привести к слухам / сплетням / киберзапугиванию;

- это может повлечь за собой юридические последствия;

- это может привести к шантажу с целью получения большего количества контента или денег.

Это преступление, и оно называется "сексизм". Если такое случилось с вами, обратитесь к доверенному взрослому.

Подумайте о своих друзьях и подписчиках в Интернете:

- Знаете ли вы каждого из них в автономном режиме?

- Вы все еще хотите делиться новостями из своей жизни со всеми ними?

- Есть ли кто-нибудь, чьи посты расстраивают вас или доставляют дискомфорт?

- Не пора ли отписаться?

Интернет может стать отличным способом завязать отношения, но для детей вашего возраста лучше всего, если эти отношения начнутся вне интернета! Например, к вам в класс приходит новый ученик, у которого такие же интересы, как у вас, и вы можете поделиться с ним именами пользователей, обмениваться сообщениями или вместе играть в онлайн-игры. Что не совсем нормально, так это когда кто-то, с кем вы никогда не встречались, пытается подружиться онлайн и хочет подписаться на вас в различных приложениях

социальных сетей или хочет задать вам очень личные и специфические вопросы о вашей жизни, жизни вашей семьи или частной жизни.

Подумайте о своих друзьях и подписчиках, которые у вас могут быть:

- Со всеми ли из них вы знакомы в сети, например, по учебе или спорту?

- Захотите ли вы поделиться с этими людьми частичками своей жизни? Возможно, у вас есть старые друзья, с которыми вы больше не общаетесь и которых вы, возможно, захотите удалить.

- Как насчет постов других людей? Какие чувства они у вас вызывают? Если кто-то публикует материалы, которые вас огорчают или доставляют дискомфорт, это нормально - отписаться от них. Подчеркните, что также можно отписаться от знакомых в сети, если этот человек делает что-то неподобающее или вызывающее дискомфорт. Это нормально, чтобы отписаться или заблокировать ЛЮБОГО, кто доставляет ему неудобства, независимо от того, знакомы ли они с ним онлайн или офлайн.

Есть некоторые вещи, о которых, если кто-то делает это онлайн, вы должны немедленно рассказать взрослому, которому доверяете. Не имеет значения, кто этот человек и откуда вы его знаете (только онлайн или как онлайн, так и офлайн).

Если кто-то...

- присылает свои фотографии, особенно в легкой одежде или без нее;

- хочет поговорить с вами о сексе (и не является ли он кем-то вроде врача или преподавателя в области здравоохранения или образования специально для этого);

- просит вас прислать ему ваши фотографии;

- просит встретиться с вами лично.

Другие формы нездорового поведения в отношениях могут быть тревожным сигналом о том , что кто-то пытается ухаживать за вами или манипулировать вами, заставляя делать то, что он хочет в дальнейшем. Это может быть:

- кто-то, кто хочет следить за всеми вашими аккаунтами / профилями;

- кто-то, кто запрашивает много личной информации, например, где вы живете или ходите в школу;

- кто-то, кто злится на вас, когда вы не в сети, разговаривая с ним;

- вы начинаете чувствовать, что этот новый онлайн-друг - единственный человек, который заботится о вас, и вы чувствуете себя оторванным от других друзей и членов семьи.

Если вы заметите, что происходит что-либо из этого, вам следует прекратить общение с обратитесь к этому человеку и расскажите об этом взрослому, которому вы доверяете (это не обязательно должен быть родитель!). Они могут попросить вас показать им сообщения, и это может вызвать неловкость, но знайте, что это не ваша вина. Этот человек лгал вам, и это его вина.

Что делать, если я уже отправил фотографию?

Сообщите в службу поддержки. Если в сети появилась ваша фотография неподходящего качества - независимо от того, отправили ли вы ее или кто-то другой вас сфотографировал, - вы можете предпринять шаги, чтобы взять ситуацию под контроль.

Во-первых, **сообщите об этом**!

- Большинство социальных сетей и заслуживающих доверия веб-сайтов прилагают все усилия, чтобы сохранить их веб-сайты не содержат неприемлемого контента, и вы можете отправить сообщение непосредственно на веб-сайт или в приложение. В каждом приложении есть несколько отличающихся друг от друга шагов по удалению изображений.

*Обратитесь в службу поддержки***.** Если вы чувствуете стресс, растерянность или иное недомогание, не бойтесь обратиться к друзьям или взрослым, которым доверяете, например, к учителю, консультанту, тренеру и наставнику - это не обязательно должен быть родитель, если вы еще не готовы поговорить с ними об этом. Помните, что если в Интернете появилось ваше неподобающее изображение, то вы не первый. Другие люди попадали в такую же ситуацию и преодолели ее, и вы тоже!

3.7 Киберзапугивание

Киберзапугивание - сочетание травли и технологий.

Вот несколько примеров киберзапугивания:

- Рассылка злобных текстовых сообщений
- Распространение слухов в Интернете
- Создание поддельных профилей, чтобы высмеять кого-то
- Запись и размещение видеороликов о драках
- Фотошопинг фотографий, чтобы выставить кого-то в плохом свете
- Оскорбление кого-то в онлайн-игре
- Повторно публиковать неподобающие / компрометирующие фотографии кого - то другого
- Доводить кого - то до такой степени , что он причиняет боль себе или другим

Некоторые люди подвергают других киберзапугиванию, потому что:

- Они думают, что это забавно
- Им кто - то не нравится , и они хотят задеть их чувства
- Они думают, что кто-то отличается от них, и могут прибегать к тому, чтобы обзывать их нехорошими словами
- Они переживают тяжелые времена, и это их способ справиться со своей ситуацией.

Хорошей новостью является то, что большинство детей не вовлечены в киберзапугивание, но это все еще серьезная проблема, над которой стоит задуматься всем.

Некоторые люди на самом деле не понимают, насколько больно может быть от киберзапугивания. Тот, кто подвергается киберзапугиванию, может:

- Чувствовать грусть и одиночество
- Пытаться избегать школы, чтобы не сталкиваться с хулиганами
- Думают, что травля усилится, если они расскажут кому-нибудь об этом
- Верят, что никто не может помочь

Киберзапугивание также может привести к депрессии, тревожности и склонности к членовредительству. Мы все должны быть осторожны в том, что делаем и говорим людям, как онлайн, так и офлайн. Если вам или кому–то еще нужна помощь - например, если вы знаете, что один из ваших друзей подумывает о том, чтобы причинить себе вред, - обратитесь за помощью немедленно обратитесь за помощью к учителю, школьному психологу или другому взрослому, которому вы доверяете.

Если кому-то нужна помощь, он может обратиться к надежному взрослому, например к школьному психологу, учителю или члену семьи.

Если вы подвергаетесь кибербуллингу:

- Не отвечайте на сообщения
- Заблокируйте хулигана
- Создайте новые учетные записи
- Расскажите взрослому, которому вы доверяете

Если вы или кто-то из ваших знакомых подвергается киберзапугиванию, вот несколько шагов, которые вы можете предпринять:

- Не отвечайте на сообщения – это только усугубит ситуацию.
- Заблокируйте хулигана – большинство веб-сайтов и компаний сотовой связи имеют возможность блокировать других пользователей.

- Создавайте новые учетные записи – предоставляйте информацию о новой учетной записи только людям, которым вы доверяете.

- Сообщите об этом на веб–сайт - на большинстве веб-сайтов есть способы сообщить о кибербуллингах, и они удалят оскорбительные посты.

- Расскажите взрослым, которым вы доверяете, – у взрослых не всегда есть ответы на все вопросы, но они действительно хотят помочь!

Иногда бывает непросто разговаривать со взрослым, потому что вы можете опасаться, что травля усилится из-за того, что вы "сплетничаете", или вы можете чувствовать себя неловко. Возможно, вы опасаетесь, что у вас отберут телефон. Иногда бывает трудно поговорить со взрослым, а иногда бывает трудно найти взрослого, который мог бы вам помочь. В этом случае хорошим помощником может стать тренер, учитель или медсестра.

Но помните, что если кому-то причиняют боль, никогда не будет ошибкой рассказать об этом взрослым. Взрослые могут помочь, если:

- Выслушают вас – некоторым может помочь простой разговор об этом.

- Сохранение доказательств – они помогут вам решить, нужно ли сохранять сообщения и кому о них сообщать.

- Обратитесь в школу – Если одноклассник издевается над вами, ваши учителя должны знать об этом, чтобы они могли защитить вас в течение учебного дня.

- Создадим для вас новые учетные записи – вам особенно понадобится их помощь, если вам нужно сменить номер мобильного телефона.

- Найдем другие решения, которые вас устроят.

- Окажем эмоциональную поддержку, чтобы справиться с этой сложной задачей.

Что вы можете сделать

Покажите, что вы поддерживаете, если отказываетесь присоединиться

Попросите хулигана остановиться

Сообщите об этом взрослым

Даже если вы сами не подвергались кибербуллингу, вы могли видеть, как это происходит с другими людьми. Игнорирование этого превращает вас в стороннего наблюдателя – это значит, что вы стоите в стороне и наблюдаете, как другим причиняют боль.

Аутсайдеры - это люди, которые стараются помочь другим.

Некоторые прохожие боятся заговорить , потому что:

- Они думают , что хулиган может в следующий раз напасть на них

- Они не думают , что взрослые могут помочь

- Они не хотят, чтобы их считали сплетницами

- Иногда бывает страшно что-то сказать

Если вы видите, что происходит киберзапугивание, у вас есть возможность остановить это и помочь защитить кого-то от причинения вреда. Вот несколько способов, с помощью которых вы можете добиться успеха:

– Проявите поддержку человеку, над которым издеваются – это может означать, что вы приложите дополнительные усилия, чтобы быть с ним любезным, отправите ему дружеское сообщение или даже просто посидите с ним за обедом.

– Откажитесь участвовать в киберзапугивании – не просто игнорируйте его; дайте понять, что вы не будете в нем участвовать, потому что это неправильно.

– Скажите киберзапугивателю, чтобы он прекратил, но только если вы чувствуете себя в безопасности - хулиганы продолжают вести себя агрессивно, когда их никто не останавливает, поэтому убедитесь , что они знают, что вы не поддерживаете их действия.

– Сообщите о киберзапугивании взрослому – это могут быть ваши родители, член семьи, которому вы доверяете, или школьный учитель.

Если вам кто-то не нравится:

– Держите критические комментарии при себе

– Не распространяйте слухи

– Не публикуйте ничего, что могло бы кого-то смутить

Вы не обязаны быть лучшими друзьями со всеми подряд. У вас могут быть разные интересы или личные качества, но это не значит, что вы должны быть жестоки к ним.

Вот несколько способов, с помощью которых вы сами можете избежать травли в Интернете:

– Держите критические комментарии при себе – нехорошо намеренно причинять кому-то боль.

– Не распространяйте слухи – даже если вы считаете, что это смешно, слухи могут выйти из-под контроля и причинить сильную боль.

– Не публикуйте ничего, что могло бы поставить в неловкое положение кого–либо другого - ваши посты предназначены не только для ваших друзей; подобные злобные комментарии могут путешествовать быстро и причинять много вреда.

– Не публикуйте повторно фотографии или видеозаписи других людей без их согласия – это всегда так, но это особенно важно, если вы знаете, что у вас не должно быть таких фотографий или видеозаписей.

Помните, что если вы подвергаете кого-то киберзапугиванию, это влечет за собой последствия:

– Веб-сайты могут удалить вашу учетную запись, если вы нарушите их правила.

– У вас могут быть неприятности в школе, если вы будете травить одноклассника в Интернете. Некоторые дети были отстранены от занятий или исключены из школы за киберзапугивание.

– Возможно, вам придется обратиться в полицию, если кто-то сообщит о вас как о киберзапугивателе. Некоторым детям даже были предъявлены обвинения в совершении преступлений за преследование других в интернете.

– Над вами могут издеваться другие люди.

Вот некоторые из наиболее важных моментов, которые следует запомнить:

– Будьте осторожны с теми, с кем вы общаетесь в Интернете – незнакомые взрослые не должны вступать с вами в контакт.

– Будьте осторожны с друзьями, с которыми вы встречаетесь в Интернете – Поговорите со взрослым, которому доверяете, о том, что составляет основу здоровых отношений.

– Сделайте перерыв - перед тем, как отключиться от социальных сетей, возможно, поговорите с другом, если захотите поделиться публикацией, содержащей личную информацию или что-то, что может показаться неуместным. Возможно, позже вы передумаете или пожалеете об этом.

– Не занимайтесь киберзапугиванием – даже если вам кто-то не нравится, никогда не стоит проявлять грубость. Иногда мы думаем, что поступаем неправильно. нет ничего плохого в том, что мы повторно публикуем чьи-то фотографии или ставим лайк на чей-то злобный пост, потому что мы не делали снимок и не делились злобным постом. Мы можем подумать, что, поскольку мы получили фотографию от другого человека и просто пересылаем ее нашим друзьям, это не мы причинили вред. Однако, когда мы совершаем такие поступки, как отпускание грубых замечаний, лайкание грубых комментариев, повторное распространение постыдного контента о других людях или любое поведение, которое может причинить вред человеку, мы также становимся хулиганами.

Обратитесь за помощью к взрослому, который чувствует себя в безопасности, даже если вам просто нужна помощь. Взрослые могут помочь!

Большинство детей уже избегают рисков, о которых мы говорили сегодня, и проявляют ответственность, когда находятся в сети:

– Они не встречаются с людьми, с которыми познакомились в Интернете.

– Они не публикуют неподобающую информацию или фотографии.

– Они не подвергают других киберзапугиванию.

Поделитесь со своими родителями и доверенными взрослыми тем, чем вы занимаетесь в интернете, и расскажите им о своей жизни, взаимоотношениях, которые вам нравятся или вы беспокоитесь! Они будут чувствовать себя увереннее в том, что вы в безопасности в сети, и вы будете чувствовать себя увереннее, обращаясь к ним, когда вам понадобится помощь.

ЗАКЛЮЧЕНИЕ

Учебно-методическое пособие "Методические инструкции обеспечения кибербезопасности образовательной среды школы для учителей, родителей и учеников" направлено на формирование безопасной цифровой среды в образовательных учреждениях. В современных условиях, когда использование информационных технологий стало неотъемлемой частью учебного процесса, обеспечение кибербезопасности становится одной из ключевых задач для всех участников образовательного процесса.

Настоящее пособие систематизирует и подробно описывает основные угрозы в цифровой среде, такие как фишинг, социальная инженерия, вредоносное программное обеспечение и кибербуллинг. Также предложены конкретные рекомендации и алгоритмы действий для минимизации рисков и создания безопасной цифровой культуры в школах.

Включенные материалы ориентированы на разные возрастные группы и целевые аудитории, что делает пособие универсальным инструментом для внедрения безопасных практик в школьную среду. Оно направлено не только на защиту данных, но и на воспитание цифровой грамотности, которая станет основой для ответственного и безопасного использования технологий в будущем.

Надеемся, что представленное пособие станет полезным инструментом для учителей, родителей и школьников, содействующим повышению уровня цифровой безопасности и снижению рисков в процессе использования интернет-ресурсов и цифровых технологий.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Сайт Комитета по информационной безопасности Министерства цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан https://www.gov.kz/memleket/entities/infsecurity?lang=ru
2. Кибербезопасность https://egov.kz/cms/ru/cyberspace
3. Национальная служба реагирования на компьютерные инциденты https://www.cert.gov.kz/
4. Incorporating Cybersecurity in the Classroom https://opentextbooks.colvee.org/cybersecuritytrainingteachers/chapter/incorporating-cybersecurity-in-the-classroom/
5. Most Common Types of Cyberattacks https://www.crowdstrike.com/cybersecurity-101/cyberattacks/most-common-types-of-cyberattacks/
6. Cybersecurity Threats in Online Learning and How to Mitigate Themhttps://www.cybintsolutions.com/cybersecurity-threats-in-online-learning-and-how-to-mitigate-them/

Ж.О. Жилбаев
А.Ж. Асаинова
Д.Б. Абыкенова
Л.С. Сырымбетова
З.К. Кульшарипова

Методические инструкции обеспечения кибербезопасности образовательной среды школы для учителей, родителей и учеников

Учебно-методическое пособие

Подписано в печать 02.10.2024.
Формат 29,7 × 42½. Бумага офсетная.
Гарнитура Times New Roman.
Объем 2,5 усл. печ. л. Тираж 500 экз.
Заказ № 1536

Редакционно-издательский отдел
Павлодарского педагогического университета имени Әлкей Марғұлан
140002, г. Павлодар, ул. Олжабай батыра, 60