БЕЗОПАСНЫЙ ИНТЕРНЕТ

ИСПОЛЬЗОВАНИЕ СЕТИ ИНТЕРНЕТ

Безусловные преимущества использования Интернет

В настоящее время Интернет стал неотъемлемой частью повседневной жизни, бизнеса, политики, науки и образования. Использование Интернета дома и в образовательных учреждениях позволяет повысить эффективность обучения, а так же получать свежие новости в интересующей области не только родителям и педагогам, но и учащимся, в том числе школьникам.

Скрытые и открытые угрозы Интернет

Однако бурное развитие Интернета несет также существенные издержки. Современная научно-образовательная информационная среда характеризуется большим количеством образовательных ресурсов с неструктурированной и мало того, еще и не всегда достоверной информацией. Объем подобных ресурсов растет в геометрической прогрессии. Таким образом, неуклонно возрастает потребность в обеспечении эффективного использования информационных научно-образовательных ресурсов. Кроме того, наряду с полезной и необходимой информацией пользователи сталкиваются ресурсами, содержащими неэтичный и агрессивный контент.

Порнография, терроризм, наркотики, националистический экстремизм, маргинальные секты, неэтичная реклама и многое другое — яркие примеры контента, с которым могут соприкоснуться дети и подростки. Бесконтрольное распространение нежелательного контента противоречит целям образования и воспитания молодежи. Отказываться от благ информационных технологий бессмысленно, но бесконтрольный доступ детей к Интернету может привести к:

- *Киберзависимости*
- *Заражению вредоносными программами при скачивании файлов*

- *Нарушению нормального развития ребенка*
- *Неправильному формированию нравственных ценностей*
- *Знакомству с человеком с недобрыми намерениями*

Классификация Интернет-угроз
Контентные риски

Контентные риски связаны с потреблением информации, которая публикуется в интернете и включает в себя незаконный и непредназначенный для детей (неподобающий) контент.

Неподобающий контент

В зависимости от культуры, законодательства, менталитета и узаконенного возраста согласия в стране определяется группа материалов, считающихся неподобающими. Неподобающий контент включает в себя материалы, содержащие: насилие, эротику и порнографию, нецензурную лексику, информацию, разжигающую расовую ненависть, пропаганду анорексии и булимии, суицида, азартных игр и наркотических веществ.

Незаконный контент

В зависимости от законодательства страны разные материалы могут считаться нелегальными. В большинстве стран запрещены: материалы сексуального характера с участием детей и подростков, порнографический контент, описания насилия, в том числе сексуального, экстремизм и разжигание расовой ненависти.

Электронная безопасность

Риски, связанные с электронной безопасностью, относятся к различной кибердеятельности, которая включает в себя: разглашение персональной информации, выход в сеть с домашнего компьютера с низким уровнем защиты (риск подвергнуться вирусной атаке), онлайн-мошенничество и спам.

Вредоносные программы

Вредоносные программы — это программы, негативно воздействующие на работу компьютера. К ним относятся вирусы, программы-шпионы, нежелательное рекламное ПО и различные формы вредоносных кодов.

— Вредоносное ПО
— Рекламное ПО
— Шпионское ПО
— Браузерный эксплойт

Спам

Спам — это нежелательные электронные письма, содержащие рекламные материалы. Спам дорого обходится для получателя, так как пользователь тратит на получение большего количества писем свое время и оплаченный интернет-трафик. Также нежелательная почта может содержать, в виде самозапускающихся вложений, вредоносные программы.

Кибермошенничество

Кибермошенничество — это один из видов киберпреступления, целью которого является обман пользователей. Хищение конфиденциальных данных может привести к тому, что хакер незаконно получает доступ и каким-либо образом использует личную информацию пользователя, с целью получить материальную прибыль. Есть несколько видов кибермошенничества: нигерийские письма, фишинг, вишинг и фарминг.

Коммуникационные риски

Коммуникационные риски связаны с межличностными отношениями интернет-пользователей и включают в себя контакты педофилов с детьми и киберпреследования.

Незаконный контакт

Незаконный контакт — это общение между взрослым и ребенком, при котором взрослый пытается установить более близкие отношения для сексуальной эксплуатации ребенка.

Киберпреследования

Киберпреследование — это преследование человека сообщениями, содержащими оскорбления, агрессию, сексуальные домогательства с помощью интернет-коммуникаций. Также, киберпреследование может принимать такие формы, как обмен информацией, контактами или изображениями, запугивание, подражание, хулиганство (интернет-троллинг) и социальное бойкотирование.

Способы защиты от Интернет-угроз
Комплексное решение в области использования сети Интернет

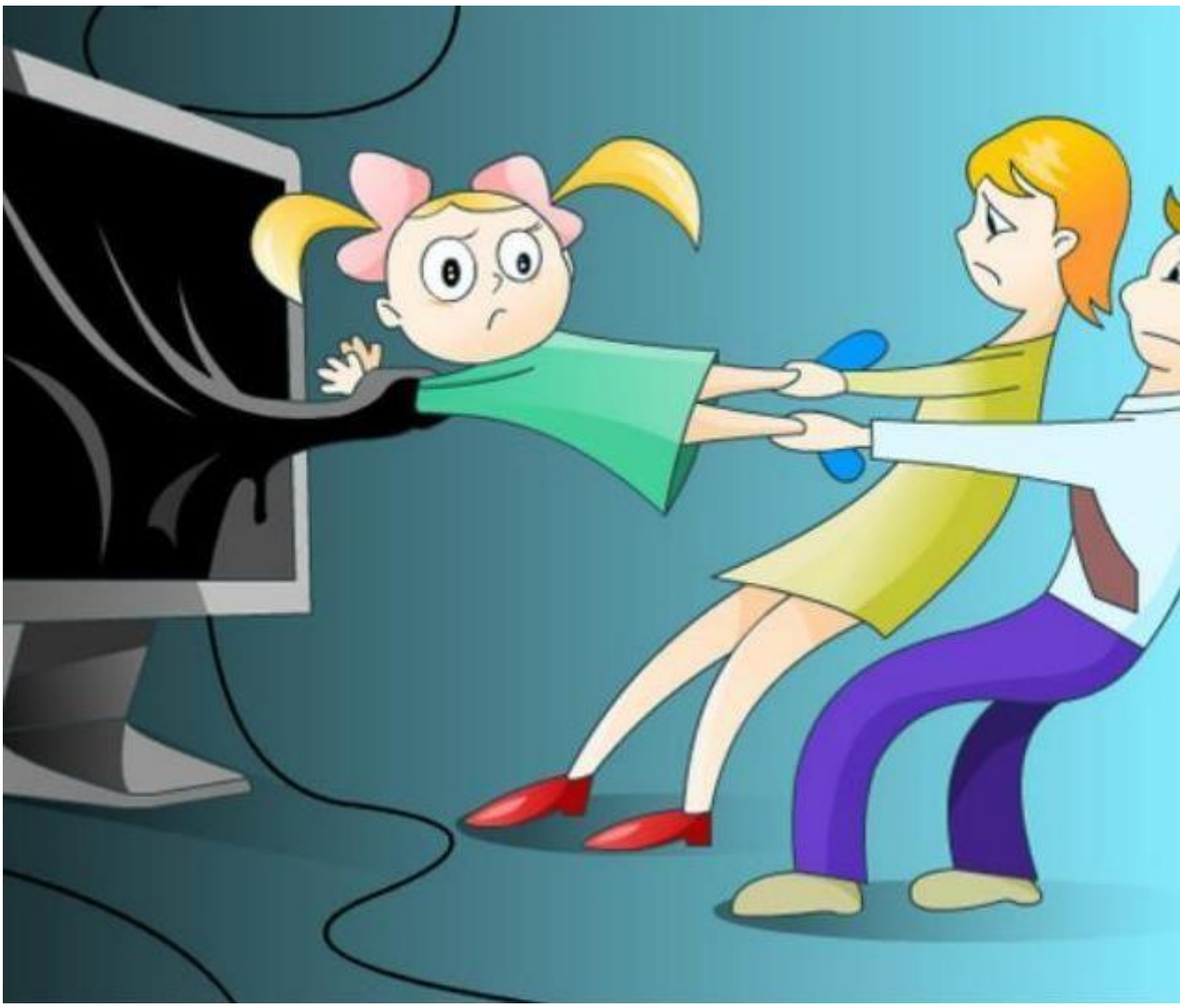
Опираясь на мировой опыт и анализируя ситуацию в Казахстане можно сказать, что решение вопроса по обеспечению безопасного использования Интернет представляет комплексное решение.

Оно включает в себя:

Административные (нормативно-правовые) меры, которые обеспечивает государство посредством создания/изменения законопроектов. Воспитание и обучение пользователей эффективной работе с информацией, которым занимаются специальные ресурсы (в том числе наш). Обучением работе в Интернете детей должны так же заниматься родители и педагоги. Использование современных технологических решений в области повышения эффективности использования Интернет. Разработкой специального программного обеспечения занимаются частные компании (в том числе и мы).

БЕЗОПАСНЫЙ ИНТЕРНЕТ
Родителям

Чтобы помочь своим детям, Вы должны это знать:



- Будьте в курсе того, чем занимаются ваши дети в Интернете. Попросите их научить Вас пользоваться различными приложениями, которыми вы не пользовались ранее.
- Помогите своим детям понять, что они не должны предоставлять никому информацию о себе в Интернете — номер мобильно телефона, домашний адрес, название/номер школы, а также показывать фотографии свои и семьи. Ведь любой человек в Интернете может это увидеть.
- Если Ваш ребенок получает спам (нежелательную электронную почту), напомните ему, чтобы он не верил написанному в письмах и ни в коем случае не отвечал на них.
- Объясните детям, что нельзя открывайте файлы, присланные от неизвестных Вам людей. Эти файлы могут содержать вирусы или фото/видео с «агрессивным» содержанием.
- Помогите ребенку понять, что некоторые люди в Интернете могут говорить не правду и быть не теми, за кого себя выдают. Дети никогда не должны встречаться с сетевыми друзьями в реальной жизни самостоятельно без взрослых.
- Постоянно общайтесь со своими детьми. Никогда не поздно рассказать ребенку, как правильно поступать и реагировать на действия других людей в Интернете.
- Научите своих детей как реагировать, в случае, если их кто-то обидел или они получили/натолкнулись на агрессивный контент в Интернете, так же расскажите куда в подобном случае они могут обратится.
- Убедитесь, что на компьютерах установлены и правильно настроены средства фильтрации.

Полезные программы

Программа **«Интернет Цензор»** устанавливается на компьютер и обеспечивает фильтрацию для всех веб-браузеров и программ. Отличительной особенностью полной версии является высокий уровень надежности и защиты от взлома.

NetPolice Lite. Облегченная версия персонального фильтра, который предоставляет наиболее важные функции для ограничения доступа пользователей к негативным, нежелательным и опасным Интернет-ресурсам. Поддерживаются самые необходимые категории и функции для безопасного использования сети Интернет.

Детям и подросткам
Школьникам младших классов

Если ты любишь сидеть в Интернете, запомни эти правила безопасности!

Правило 1 ***Не указывай настоящее имя и фамилию. Придумай себе НИК***	Правило 2 ***Не размещай на сайтах свои фотографии. Пользуйся аватаркой или картинками***	Правило 3 ***Не говори никому свой адрес и номер телефона. Общайся только в Интернете.***	Правило 4 ***Не встречайся с людьми, которых ты знаешь только по Интернету. Если кто-то приглашает тебя встретиться или оскорбляет тебя — срочно расскажи об этом родителям***

Школьникам средних классов
Вы должны это знать:

- При регистрации на сайтах, старайтесь не указывать личную информацию, т.к. она может быть доступна незнакомым людям. Так же, не рекомендуется размещать свою фотографию, давая, тем самым, представление о том, как вы выглядите, посторонним людям.
- Используйте веб-камеру только при общении с друзьями. Проследите, чтобы посторонние люди не имели возможности видеть ваш разговор, т.к. он может быть записан.
- Нежелательные письма от незнакомых людей называются «Спам». Если вы получили такое письмо, не отвечайте на него. В случае, если Вы ответите на подобное письмо, отправитель будет знать, что вы пользуетесь своим электронным почтовым ящиком и будет продолжать посылась вам спам.
- Если вам пришло сообщение с незнакомого адреса, его лучше не открывать. Подобные письма могут содержать вирусы.
- Если вам приходят письма с неприятным и оскорбляющим вас содержанием, если кто-то ведет себя в вашем отношении неподобающим образом, сообщите об этом.
- Если вас кто-то расстроил или обидел, расскажите все взрослому.

Студентам колледжа и школьникам старших классов
Вы должны это знать:

- Не желательно размещать персональную информацию в Интернете.
- Персональная информация — это номер вашего мобильного телефона, адрес электронной почты, домашний адрес и фотографии вас, вашей семьи или друзей.
- Если вы публикуете фото или видео в интернете — каждый может посмотреть их.
- Не отвечайте на Спам (нежелательную электронную почту).

- Не открывайте файлы, которые прислали неизвестные Вам людей. Вы не можете знать, что на самом деле содержат эти файлы – в них могут быть вирусы или фото/видео с «агрессивным» содержанием.
- Не добавляйте незнакомых людей в свой контакт лист в IM (ICQ, MSN messenger и т.д.)
- Помните, что виртуальные знакомые могут быть не теми, за кого себя выдают.
- Если рядом с вами нет родственников, не встречайтесь в реальной жизни с людьми, с которыми вы познакомились в Интернете. Если ваш виртуальный друг действительно тот, за кого он себя выдает, он нормально отнесется к вашей заботе о собственной безопасности!
- Никогда не поздно рассказать взрослым, если вас кто-то обидел.

Учителям и преподавателям

Чтобы помочь учащимся, Вы должны это знать:

- Подготовьтесь. Изучите технику безопасности в Интернете, чтобы знать виды Интернет-угроз, уметь их распознать и предотвратить. Выясните, какими функциями обладают компьютеры подопечных, а так же какое программное обеспечение на них установлено.
- Прежде чем позволить ребенку работу за компьютером, расскажите ему как можно больше о виртуальном мире, его возможностях и опасностях.
- Не позволяйте детям самостоятельно исследовать Интернет-пространство, они могут столкнуться с агрессивным контентом.
- Выберите интересные ресурсы и предложите детям изучить их вместе.
- Убедитесь, что на компьютерах установлены и правильно настроены средства фильтрации контента, спама и антивирусы.

Использование Интернета является безопасным, если выполняются три основные правила.

1. Защитите свой компьютер

Регулярно обновляйте операционную систему.

Используйте антивирусную программу.

Применяйте брандмауэр.

Создавайте резервные копии важных файлов.

Будьте осторожны при загрузке содержимого.

2. Защитите себя в Интернете

С осторожностью разглашайте личную информацию.

Думайте о том, с кем разговариваете.

Помните, что в Интернете не вся информация надежна и не все пользователи откровенны.

3. Соблюдайте правила

Закону необходимо подчиняться даже в Интернете.

При работе в Интернете не забывайте заботиться об остальных так же, как о себе.

Линия помощи

- **Если тебя оскорбляют и преследуют в Интернете…**
- **Если делают неприличные предложения в Интернете…**
- **Если ты стал жертвой сетевых мошенников…**
- **Если ты столкнулся с опасностью во время пользования сетью Интернет или мобильной связью…**

Телефоны доверия

(звонки бесплатные, круглосуточно)

Национальный телефон доверия для детей и молодежи — 150

Единый Call-center Уполномоченного по правам ребенка — 111

Общие правила безопасного интернета

Правило 1

Нельзя раскрывать свои личные данные. Часто большинство малоизвестных сайтов требуют ввода вашего имени. В таких случаях просто необходимо придумать себе псевдоним (другое имя). Старайтесь избегать на таких сайтах заполнение строк, где требуется ввести свою личную информацию: адрес, фамилию, дату рождения, телефон, фамилии и имена друзей и их координаты. Ведь просмотреть их может каждый. Данной информацией могут воспользоваться воры и мошенники, как в виртуальной, так и в реальной жизни.

Правило 2

Обязательно сообщите родителям, если вдруг вам захочется встретиться с «интернет-другом» в реальной жизни. В интернете человек может быть совсем не тем, за кого себя выдает. В итоге: якобы двенадцатилетняя девочка может оказаться сорокалетним дядечкой, который может вас обидеть. И если вдруг, ваш новый знакомый/ая с интернета настойчиво предлагает встретиться, посоветуйся с родителями, прежде чем идти на встречу.

Правило 3

Старайтесь посещать только те страницы интернета, которые вам посоветуют родители. Они – люди взрослые и лучше знают, что такое хорошо и что такое плохо. А, кроме того, они плохого не посоветуют. Встать взрослыми вы еще успеете.

Правило 4

Находясь в интернете самостоятельно, вы можете оказаться на страницах с совсем не детским содержанием. Обязательно расскажите об этом родителям. Практически любой «клик» по интересной, нужной или полезной ссылке может привести к переходу на сайт, предлагающий бесплатно скачивать и просматривать «взрослые страницы».

Правило 5

Никогда без ведома взрослых не отправляйте СМС, чтобы получить информацию из интернета. Иногда всплывает окошко – очень яркое, даже мигающее, примерно с таким текстом: «Только сегодня – уникальный шанс – участвуй и выигрывай!» Заманчиво, правда? Вы щелкаете на него и тут сообщение: «Для того, чтобы принять участие в розыгрыше тебе необходимо прислать СМС!» Остановитесь! Ни в коем случае не делайте этого без ведома взрослых, ведь это могут быть мошенники. И одна, казалось бы, безобидная СМС-ка может стоить вам и вашим родителям больших денег.

Не забывайте, что интернет – это не главное увлечение в жизни. Кроме него у вас должны быть любимые книги, занятия спортом и прогулки с друзьями на свежем воздухе!

ҚАУПІПСІЗ ИНТЕРНЕТ

ҒАЛАМТОР ТОРАБЫН ПАЙДАЛАНУ
Ғаламтор артықшылықтарын сөзсіз пайдалану

Қазіргі кезде Ғаламтор жүйесі күнделікті өмірдің, бизнестің, саясаттың, ғылым мен білімнің ажырамас бөлігі болды. Үйде және білім орындарында ғаламторды пайдалану білім беру сапасын көтеруге мүмкіндік жасайды, сондай-ақ, қызықтырушы жаңа жаңалықтарды тек ата-аналар ғана емес, сонымен қатар педагогтар да, оның ішінде оқушылар да ала алады.

Ғаламтордың ашық және жабық қауіптері

Дегенмен ғаламтор дәуірінің жүруі маңызды шығындарға әкеледі. Заманауи ғылыми-білім беретін орта құрылымы жасалмаған ресурстары үлкен санмен бейнеленеді және сонымен қатар, әрқашан дәйекті емес ақпараттармен сипатталады. Аталмыш ресурстар көлемі геометриялық прогресте өседі. Қорыта келгенде, ақпараттық ғылыми білім беретін ресурстарды тиімді пайдалануды қамтамасыз ету қажеттілігі ұдайы өседі. Сонымен-ақ, пайдалы да қажетті ақпараттармен қатар пайдаланушылар ыңғайсыздық және агрессиялық контенттерге тушар болады.

Порнография, терроризм, есірткілер, ұлттық экстремизм, маргиналды секталар, теріс жарнамалар мен басқалары да контенттің айқын мысалы бола алаты және олармен жастар мен жасөспірімдер кездеседі. Жағымсыз контенттің бақылаусыз таралуы жастардың тәрбиесі мен білімнің мақсаттарына қайшы келеді. Ақпараттық технологиядағы мағынасыз игіліктерден бас тарту, бірақ балалардың ғаламторға бақылаусыз қол жеткізуі әкелуі мүмкін:

- *Кибертәуелділікке*
- *Файлдарды жазу кезінде көптеген зиянды бағдарламаларды жұқтырып алу*
- *Баланың қалыпты дамуын бұзуға*
- *Адамгершілік қасиеттердің дұрыс қалыптаспауына*
- *Ниеті дұрыс емес адамдармен танысуға*

Интернет-қаупінің жіктелуі
Контент тәуекелдері

Контент тәуекелдері интернетте шығатын және заңсыз да балаларға тиісті емес контентті ақпараттарды пайдаланумен байланысты.

Лайықсыз контент

Мәдениет, заңдар, менталитетке байланысты және елде келісімнің заңдастырылған жасына лайықты елде есептелетін материалдар тобымен анықталады. Лайықсыз контент мынадай материалдардан тұрады: зорлық, эротика және порнографиядан, дөрекі лексикадан, нәсілдік жек көрушілікті тұтататын анарексия мен булимиядан, суицидтен, құмарлық иегерлері және есірткі заттары туралы ақпараттарынан тұрады.

Заңсыз контент

Әр түрлі материалдар елдің заңдарына байланысты жасырын есептей алады. Көптеген елдерде тыйым салынған: балар мен жасөспірімдердің қатысуымен жынысты сипаттағы материалдарға, порнографичялық контентке, зорлық зомбылықты сипаттауға, оның ішінде жынысты, экстремизм мен нәсілдік жек көрушіліктің тұтандыру материалдарына.

Электрондық қауіпсіздік

Электрондық қауіпсіздікпен байланысты тәуекелі әр түрлі кибержұмыстарына үй компьютерінен желіге төменгі қорғанысы деңгейде шығу, онлайн – ала аяқтық пен спам.

Зиянды бағдарламалар

Зиянды бағдарламалар — бұл компьютердің жұмысына негативті әсер ететін бағдарлама . Оларға вирустар, бағдарлама — тыңшысы, жағымсыз жарнамалық ПҚ және әр түрлі пішінді зиянды кодтар жатады.

— Зиянды ПҚ
— Жарнамалық ПҚ
— Тыңшы (Шпионды) ПҚ
— Браузерлі эксплойт

Спам

Спам – бұл жарнамалы материалы бар жағымсыз электрондық хат. Спам, алушы үшін қымбатқа түседі, себебі пайдаланушы ретінде көп мөлшерде хат алу үшін көп уақытын және төленген интернет — трафигін жұмсайды. Сондай-ақ, жағымсыз пошта өз бетінше жүретін шығындарды, зиянды бағдарламаларды қамтиды.

Кибер ала аяқтық

Кибер ала аяқтық – бұл, пайдаланушыларды алдау мақсатымен кибер қылмыстың бір түрі. Хакер құпия мәліметтерді ұрлау , заңсыз түрде қалай да болса пайдаланушының дербес ақпаратын материалдық пайданы алу мақсатында

пайдаланады. Кибер ала аяқтықтың бірнеше түрі бар: Нигериялық хаттар, фишинг, вишинг пен фарминг.

Коммуникациялық тәуекелдер

Коммуникациялық тәуекелдер интернет — пайдаланушылардың тұлға аралық қарым – қатынасымен байланысты және педофилдер мен кибер қудалаудың балалармен байланысы болады.

Заңсыз байланыс

Заңсыз байланыс – бұл үлкендер мен балалар арасындағы байланыс. Үлкендер баламен жақынырақ танысуға тырыса отыра, бір жағынан оны сексуалдың қарым – қатынасқа түсуге бейімдейді.

Киберпқудалау

Киберқудалау – бұл адамды интернет – коммуникациясы арқылы тіл тигізу, агрессиялы, сексуалды алымсақтықтарды хабарламалар арқылы жібереді. Сондай – ақ, киберқудалау ақпаратпен алмасу, байланыс жолдарын білу немесе суреттерін алу, қорқыту, еліктету, бұзақылық жасату (итнтернет – троллинг) әлеуметтік жоламаушыл жасату түрінде болуы мүмкін.

Интернет – қорқытудың қорғаныс тәсілдері
Интернет торабын пайдалану саласындағы кешенді шешім:

Әлемдік тәжірибеге және Қазақстандағы жағдайға сүйене отыра мынадай шешімге келуге болады: қауіпсіз интернетті пайдалану сауалы кешенді шешілетін мәселе.

Оған кіреді:

Әкімшілік (нормативті-құқықты) шаралар, мемлекет жасаулары / өзгерістері арқылы заң жобаларын қамтиды. Пайдаланушыларды ақпараттармен сапалы жұмыс істеуге тәрбиелеу мен үйрету жұмысытарымен арнайы ресурстар шұғылданады. (оның ішінде) Балалардың Интернетпен жұмыс істей білуге үйрету ата-аналар мен педагогтарға да жүктеледі. Интернетті пайдалана білу сапасын арттыру саласындағы заманауи технологияларды пайдалану. Арнайы бағдарламалық жасауларды жеке меншікті компаниялар шұғылданады. (оның ішінде біз де).

ҚАУІПСІЗ ИНТЕРНЕТ
Ата — аналарға

Өз балаларыңызға көмектесу үшін, Сіздер мынаны білулеріңіз қажет:

- Интернетте балаларыңыздың немен шұғылданып отырғанын білулеріңіз керек. Ертеректе пайдаланылмаған әртүрлі қосымшаларды өз балаларыңыздан үйретуін сұраңыз.
- Балаларыңызға өздері туралы Интернетте ешкімге мәлімет бермеулері жайлы түсіндіріп айтыңыз . Мысалы: телефонының нөмірін, мекен – жайын, мектеп атауын/нөмірін, сондай-ақ, өзінің және отбасының суреттерін көрсетуге болмайды. Бұл суреттерді кез келген адам Интернеттен көрулері мүмкін.
- Егер балаңыз спам алса, (жағымсыз электрондық поштаны), оған сенбеуі және жауап берудің қажеті жоқ екендігін ескертіңіз.
- Сіздерге белгісіз адамнан келген файлды ашуға болмайтыны туралы балаларыңызға түсіндіріңіз. Бұл файлдарда вирустар немесе «агрессивті» мазмұнды сурет/бейне материалдары болуы мүмкін.
- Интернеттегі кейбір адамдар, өздерін дұрыс адам түрінде көрсетіп, көп өтірік нәрсені айту мүмкіндігі бар екендігін, балаларыңызға түсіндіріңіз.
- Балалар торындағы достарымен нақты өмірде үлкеннің қатысуынсыз кездесуге болмайды. Өз балаларыңызбен үнемі сөйлесіп тұрыңыз.
- Интернеттегі таныс емес адамдардың әрекеттеріне қалай дұрыс қарау және сезіну керек екендігі туралы сөйлесу ешқашан кеш болмайды.
- Егер сіздің балаңыз Интернеттегі агрессивті контенттерге немесе біреу ренжіткен жағдайларға кез болғанда, оны қалай сезіну керек екендігін түсіндіріңіз,сондай-ақ, қайталанған жағдайда қайда хабарлау керек екендігін айтыңыз. Компьютерлерде сүзу және дұрыс бейімделген құрал орнатылғандығына көз жеткізіңіз.

Пайдалы бағдарламалар

«Интернет Цензор» бағдарламасы компьютерге қойылады және барлық браузерлер мен бағдарламаға сүзуді қамтамасыз етеді. Толық версияның ерекше айырмашылығы, жоғары сенімділік деңгейі мен бұзудан қорғауы болып табылады.

NetPolice Lite. Персоналды жеңілдетілген дербес фильтр версиясы, пайдаланушыларды жағымсыз және қауіпті Интернет – ресурстарымен байланысты болдырмау үшін ең маңызды функциялардан тұрады. Интернет торабын қауіпсіз пайдалану үшін ең қажетті санаттары мен функциялары қолданылады.

Балалар мен жасөспірімдерге
Төменгі сынып оқушыларына

Егер сен Интернетте отыруды ұнататын болсаң, онда келесі ережелерді есіңде сақта!

Ереже1	Ереже 2	Ереже 3	Ереже 4
Нақты атың мен тегіңді көрсетпе. Өзіңе НИК Ойлап тап	***Сайтқа өз суретіңді салма. Аватаркамен немесе картинамен Пайдалан.***	***Ешкімге өз мекен-жайыңды және телефон нөміріңді бермең. Тек Интернетпен ғана байланыс.***	***Интернеттен ғана білетін адаммен араласпа. Егер сені біреу кездесуге немесе ренжітетін болса, тез арада ата-анаңа айт***

Орта буын оқушыларына
Сендер мұны білулерің керек:

- Сайтқа тіркелу кезінде, қарабасың туралы мәліметті берме, себебі ол бейтаныс адамдарға қол жетімді болуы мүмкін. Сондай-ақ, өзіңді фото сурет арқылы бейтаныс адамдарға таныстырудың қажеті жоқ. Веб-камераны тек достарыңмен араласқанда ғана пайдалан.
- Бейтаныс адамдардан келіп түскен жағымсыз хат «Спам» деп аталады. Егер мұндай хат алған болсаң, жауап берме.
- Егер мұндай хатқа жауап берген болсаң, онда хат жіберуші сенің электрон поштамен пайдаланатыныңды көріп, спам жазып жібере беретін болады.
- Егер таныс емес мекен-жайдан хабарлама келіп түссе, оны ашпағаның дұрыс болады. Себебі мұндай хаттарда вирустар болуы мүмкін.
- Егер келіп түскен хат мазмұны жағымсыз немесе ренжітетін мағынада болса, өзінің жағымсыз қылықтарын көрсететін болса,олар туралы хабар беру керек.
- Егер біреу көңіл-күйіңді бұзса немесе ренжітетін болса, онда үлкендерге айт.

Колледж студенттері мен мектеп жоғары сынып оқушыларына

Сендер мұны білулерің керек:

- Интернетке дербес қарабасың туралы ақпаратты салмағаның дұрыс болады.
- Дербес қарабасың туралы ақпарат — бұл сенің мобилді телефоныңның нөмірі, электрондық поштаңның мекен – жайы, үйіңнің орналасқан орнын және фотосуреттеріңді, отбасы фотосуреттері мен достарыңның фотосуреттерін көрсетеді.
- Егер сендер интернетке фото немесе бейне материалдарды салсаңдар, онда әркім оны көре алады.
- Спамға жауап бермеңдер (жағымсыз электрондық поштаға).
- Білмейтін адамдардан келген файлдарды ашпаңдар. Сендер ол файлда не барын білмейсіңдер. Себебі онда вирустар немесе «аргессивті» мәнде фото/бейне материалдар болуы мүмкін.
- Өз IM (ICQ, MSN messenger и т.д.) парақтарына таныс емес адамдарды тіркемеңдер.
- Есте сақтаңдар, өздерін жақсы көрсеткен виртуальды таныстар, дұрыс адам болып шығуы мүмкін емес.
- Интернетте танысқан адаммен егер өмірде кездесуге мүмкіндік туындаған жағдайда, үлкен адамдардан біреу қастарыңда болмаса, онда кездесудің қажеті жоқ. Егер сенің виртуалды досың өзін интернеттен көрсеткендей жақсы адам болатын болса, онда ол сенің қауіпсіздігіңе қамқорлық жасайды!
- Егер сені біреу жәбірлесе ересектерге айту ешқашанда кеш болмайды.

Мұғалімдер мен оқытушыларға

Оқушыларға көмек көрсете білу үшін, Сіздер мұны білулеріңіз керек:

- Дайындалыңыздар. Интернеттегі әртүрлі қорқытуларды танып білу және сақтап қалу үшін интернеттегі қауіпсіздік ережелерін оқыңыз. Біріншіден, қамқоршыңыздың компьютері қандай функциялардан тұрады, сондай – ақ, онда қандай бағдарламалар орнатылғандығын айқындап алыңыз.
- Балаға, компьютермен жұмыс істер алдында, виртуалды әлем туралы, оның мүмкіндіктері мен қауіптілігі жайлы көбірек айтқандарыңыз дұрыс болады.
- Балаға өз алдына интернет кеңсітігін зерттеуге рұқсат бермеңіз, олар агрессивті контентпен кездесуі мүмкін.
- Қызықты ресурстарды таңдап алыңыз да, оны балаларға бірге талдауға шақырыңыз.
- Компьютерлерде контент, спам мен антивирус сүзулері орнатылып, дұрыс келтірілгендігіне көз жеткізіңіз.

Егер үш негізгі ережелер орындалса, онда интернетті пайдалану қауіпсіз болып табылады.

1. Өзіңіздің компьютерды сақтаңыз

Басқару жүйесін үнемі жаңартып отыр.

Вирусқа қарсы бағдарламаны қолдан.

Брандмауэрды пайдалан.

Қажетті файлдардың артық көшірмелерін жаса.

Қажетті материалдарды алар кезде сақ бол.

2. Интернетте өзіңізді сақтаңыз

Жеке ақпаратты жұртқа сақтықпен жайғаның абзал.

Кіммен сөйлесіп тұрғаныңды ойла.

Интернеттегі барлық ақпараттарға сенуге болмайды және пайдаланушылардың барлығы ашық емес екенін есте сақтаған абзал.

3. Ережелерді сақта

Заңға интернетте де бағыну керек.

Интернетпен жұмыс істеген кезде, өзіңе сияқты, барлығымен де қауіпсіздік қамқорлығын ұмытпаған абзал.

Көмек жолы

- **Егер сені Интернетте қорласа және қудаласа …**
- **Егер Интернетте жағымсыз сөйлемдер жасаса…**

- **Егер сен ала аяқтар торының құрбаны болсаң…**
- **Егер сен Интернеттен торабын немесе мобильді байланысты пайдалану кезінде қауіп төнсе…**

Сенім телефоны

(қоңырау тәулік бойы тегін)

Балалар мен жастар үшін ұлттық сенім телефоны — 150

Бала құқығы бойынша уәкілетті біртұтас Call-center — 111

Интернет қауіпсіздігінің жалпы ережесі

Ереже 1

Өзің туралы жеке мәлімет беруге болмайды. Белгісіз кейбір сайттар атыңды енгізгуді сұрайды. Ондай жағдайда өзіңе бүркеніш ат (псевдоним) ойлап тапқаның жөн. Мұндай сайттардағы аты-жөніңді, мекен-жайыңды, туған күніңді, достарыңның атын көрсетуді талап ететін толтыру жолдарынан аулақ болғаның дұрыс. Себебі оны әрбіреулері көре алады. Берілген ақпаратпен виртуалды түрде, сондай – ақ, нақты өмірде де ұрылар мен ала аяқтар қолдануы мүмкін.

Ереже 2

Егер сен «интернет – досыңмен» нақты өмірде кездескіңікелсе, онда міндетті түрде ата – аналарыңа айтыңдар. Интернетте бәлкім дәл сол адам болмауы мүмкін. Қорыта келгенде: өтірік он екі жастағы қыз, қырық жастағы ер адам болып, ренжітуі мүмкін. Егер Интернет арқылы танысқан досың кездесуге табандылықты талап етсе, кездесуге бармас бұрын, ата-анаңмен ақылдас .

Ереже 3

Интернетке ата – аналарың рұқсат ететін беттеріне ғана кіріңдер. Олар – үлкен адамдар және не жақсы, не жаман екенін айыра біледі. Сол себеті олар жаман нәрсеге ақыл – кеңес бермейді. Ересек адам болуға сендер әлі үлгересіңдер.

Ереже 4

Өз бетіңше интернетте отырып, балаларға арналған мәліметтер бетінен оқшау болуың мүмкін. Бұл туралы міндетті түрде ата – анаңа айт. Кез келген тегін көшіруге болатын «шақыру» қызықты, қажетті немесе пайдалы мәліметтер «үлкендерге арналған» сайт беттеріне ауысуға мүмкіндік береді.

Ереже 5

Интернеттен ақпаратты алу үшін СМС ешқашан үлкендердің рұқсатынсыз жібермеңдер. Кейде өте айқын немесе жанып – сөнетін терезешелер көрінеді. Олар мынадай мазмұнды болып келеді: «Тек бүгін – тамаша мүмкіндік – қатыс және жеңіп ал!» Қызығарлықтай емес пе? Сендер оған басасыңдар, барлық хабарлама сонда «Ұтыс ойнына араласу үшін саған тек СМС жіберу керек!» Тоқтаңдар! Мұндай қимылға ата – аналарыңның рұқсатынсыз барма, ала аяқтар болуы мүмкін. Тек бір ғана қарапайым СМС сендерге және ата – аналарыңа үлкен ақша төлемі болуы мүмкін.

Интернет – бұл өмірдегі ең басты әуесқойлық емес екендігін ұмытпа. Бұдан басқа сендердің сүйікті кітаптарың, спорттарың мен таза ауадағы достарыңмен серуендерің болуы керек!