Тема 1: История возникновения Интернета. Понятия Интернет - угроз. Изменения границ допустимого в контексте цифрового образа жизни

Широкое распространение информационных технологий во все сферы жизнедеятельности человека оказывает существенное влияние на его социальную адаптацию. Современную жизнь человека в обществе практически невозможно представить без Интернета.

Днем рождения Интернета считается 29 октября 1969 года, однако в массовом пользовании он появился гораздо позже, в начале 90-х. История создания интернета берет свое начало в 60-х годах прошлого века в США. Страна обладала огромными возможностями, в научных центрах работало много талантливых ученых. Первый прототип интернета был разработан для использования в военное время. Например, для связи во время ядерной войны.

В 1971 году была разработана первая электронная почта, а спустя всего два года, интернет распространился и за океаном. Однако пользоваться им могли по-прежнему лишь узкий круг людей.

Таким образом, в США был дан первый толчок развитию интернета, однако основателем интернета является Тим Бернесрс-Ли, который трудился в европейской организации ЦЕРН. Потратив два года на разработки, именно этот ученый сделал интернет таким, каким сейчас его знают миллионы пользователей.

Интернет становится все более значимым фактором социализации и социальной адаптации детей и подростков. Наряду с представляющимися возможностями использования интернета, как инструмента социализации, благодаря которому раздвигаются границы познания, возрастают возможности удовлетворения потребностей, расширяются рамки общения и взаимодействия, многократно возрастают и риски негативного влияния на психологическое самочувствие, эмоциональное благополучие, здоровье и даже жизнь ребенка.

Риски, с которыми сталкивается пользователь интернета, многообразны. Их несет на себе разнообразная информация, размещаемая в Сети. Как указывают исследователи «само понятие риска является субъектно-отнесенным: риск связан с ситуацией, в которой возможен неблагополучный исход, с ситуацией опасности; но исход зависит от выбора и действий человека».

В ряду актуальных для сегодняшней интернет - среды рисков, связанных с использованием интернета детьми и подростками, специалисты выделяют следующие:

- Контентные риски — это материалы (тексты, картинки, аудио, видеофайлы, ссылки на сторонние ресурсы), содержащие насилие, агрессию, эротику и порнографию, нецензурную лексику, информацию, разжигающую расовую ненависть, пропаганду анорексии и булимии, суицида, азартных игр, наркотических веществ и т.д.

- Коммуникационные риски связаны с межличностными отношениями интернет-пользователей и включают в себя риск подвергнуться оскорблениям и нападкам со стороны других. Примерами таких рисков могут быть: незаконные контакты (например, груминг), киберпреследования, кибербуллинг и др. Для подобных целей используются различные чаты, онлайн-мессенджеры (ICQ, Google talk, Skype и др.), социальные сети, сайты знакомств, форумы, блоги и т.д.

- Электронные (кибер-) риски — это возможность столкнуться с хищением персональной информации, риск подвергнуться вирусной атаке, онлайн-мошенничеству, спам-атаке, шпионским программам и т.д.

- Потребительские риски – злоупотребление в интернете правами потребителя. Включают в себя: риск приобретения товара низкого качества, различные поделки, контрафактная и фальсифицированная продукция, потеря денежных средств без приобретения товара или услуги, хищение персональной информации с целью кибер-мошенничества, и др.

- Интернет-зависимость, навязчивое желание войти в интернет и невозможность выйти из интернета, патологическая, непреодолима тяга к интернету, «оказывающая пагубное воздействие на бытовую, учебную, социальную, рабочую, семейную, финансовую или психологическую сферы деятельности».

В последнее время все большую тревогу вызывает распространение рисков, связанных с вовлечением несовершеннолетних в опасные группы и сообщества. Это, прежде всего, так называемые «группы смерти», которые вовлекают детей и подростков в выполнение опасных заданий, приводящих в конечном итоге к суициду. Это так же экстремистские группы, внушающие несовершеннолетним идеи о несправедливости мироустройства и их особом предназначении в «улучшении мира», посредством его «очищения от недостойных» и вовлекающие в незаконную экстремистскую деятельность. Это и группы, предлагающие несовершеннолетним «работу», заключающуюся в незаконной деятельности (прежде всего, в распространении наркотических и других запрещенных веществ, литературы и т.п.). Создаваемые злоумышленниками группы вовлекают детей и подростков, действуют через социальные сети, мессенджеры,

объединяя в себе и другие риски пользователей: вовлекая в коммуникацию, игру и т.п., что определяет их особую опасность. Действие этих рисков очень трудно контролировать, т.к. закрытые группы возникают в сети с другими названиями, а вместо заблокированных страниц создаются новые. Создатели таких групп используют ухищренные способы распространения информации о себе, используя «хештеги».

Каждый из этих видов рисков способен принести непоправимый ущерб эмоциональному благополучию и психологическому здоровью ребенка, поэтому требует тщательного анализа и нивелирования. Относительно недавно появились исследования, посвященные другим интернет-рискам, в частности, анализу представлений детей и подростков, их родителей и педагогов об интернет-рисках, их осведомленности об интернет-опасностях и угрозах, об интернет-безопасности, предлагающие типологию интернет – рисков и угроз, анализ особенностей восприятия интернет-рисков пользователями, характера их воздействия, факторов и причин их распространения.

Мир находится на пороге четвертой индустриальной революции, которая фундаментально изменит все культурные практики человека. Третья революция — цифровая, начавшаяся в 1960- х гг. прошлого века, — относительно мягко подготовила к таким трансформациям человечество на значительной части земной суши.

Уже сейчас мы живем в ином мире, который на наших глазах превращается из вертикального в горизонтальный, из закрытого в практически прозрачный, из линейного в сетевой, из регламентированного в неопределенный, из однозадачного в многозадачный, из стабильного в текучий.

В условиях все ускоряющегося темпа изменений человечеству приходится форсированно адаптироваться к этому новому миру. И впервые в истории земной цивилизации передовым отрядом выступают не взрослые, а подрастающее поколение. Дети по активности освоения интернета существенно опережают взрослых .

Учитывая высокую интенсивность потоков информации и коммуникации в онлайн-среде, нельзя недооценивать их влияние на психическое развитие и формирование личности ребенка. С каждым годом мы получаем все больше данных о том, что инфокоммуникационные технологии не просто дополняют и расширяют жизнь ребенка, но и влияют на всю структуру его деятельности как в офлайне, так и в онлайне. Это одна из значимых причин, которая заставляет нас иначе взглянуть на сам феномен детства.

Тема 2: Изменения нормативных моделей развития и здоровья детей и подростков

Понятия "норма развития" и "возрастно-нормативная модель развития" еще не обрели понятийного статуса в психолого-педагогической науке. И это несмотря на то, что знание норм развития имеет исключительно важное значение в контексте развивающего образования при построении образовательного процесса на ступенях образования. Объяснить отсутствие обоснованных возрастных норм развития в психолого-педагогической науке и педагогической практике можно лишь ссылками на сложность самого предмета исследования и разработки.

Норма развития - это не характеристика среднестатистического уровня развития детей на определенном этапе онтогенеза или ступени образования. Так понимаемая норма развития фиксирует лишь сложившиеся на данный момент представления о нормальности развития детей в конкретных социокультурных условиях.

Грамотная научная постановка вопроса о нормах развития начинается с вопроса о возрастных возможностях детей на определенном этапе онтогенеза.

В психологии развития понятие "норма развития" вводится для обозначения потенциальных возможностей детей определенного возраста. Норма развития - это не то среднее, что есть, а то лучшее, что возможно в конкретном возрасте для конкретного ребенка при соответствующих условиях. Норма развития - это указание на максимальные возможности развития детей на определенной ступени образования.

Почему именно возможностей развития, а не его достижений? Ответ на этот вопрос содержится в психологических исследованиях закономерностей развития определенных способностей на этапе онтогенеза. Установлено, что новообразования развития (субъектные способности) всегда обнаруживают себя за пределами того возрастного периода, где они сложились. Поэтому ориентироваться на оценку высших достижений именно в данном возрасте неправомерно - они проявляют себя лишь на следующем этапе онтогенеза.

Построение возрастных нормативов развития - актуальная задача психолого-педагогической науки, имеющая важное практическое значение. Отсутствие таких нормативов может привести к тому, что образовательные практики будут ориентироваться на максимальные достижения детей. Такие практики могут быть небезопасны для их здоровья.

Нормы развития необходимы и для оценки развивающего потенциала инновационных образовательных практик, новых образовательных и учебных программ. Нормативные модели развития детей определенного возраста на определенной ступени

образования позволят выстраивать обоснованную систему педагогической деятельности и адекватную ей критериальную базу.

В этом же ряду находится рассмотренная нами выше проблема диагностики развития, связанная с практикой отбора детей в специализированные образовательные учреждения, с контролем за ходом и результатами развития детей на разных образовательных ступенях, с выявлением последствий различных видов групповой дифференциации детей в школах.

Понятие "возрастно-нормативная модель развития" - это педагогическая интерпретация психологического понятия нормы развития. Нормативная модель развития должна включать представление об основных целях, содержании, методах, организационных формах образования, соответствующих задачам культурного развития человека на определенном этапе онтогенеза. Представление о модели культурного развития (нормативном развитии человека в данной культуре) необходимо для того, чтобы избежать вариантов "некультурного" развития индивида в границах той или иной образовательной ступени - как забегания вперед, форсирования детского развития, так и его отставания, инфантилизации.

Возрастно-нормативные модели развития должны позволить выстроить возрастно-ориентированную педагогическую деятельность, выявить благоприятные и неблагоприятные условия нормального развития, а впоследствии адекватным образом работать с этими условиями: благоприятные - поддерживать и создавать, неблагоприятные - блокировать.

Имеющиеся прецеденты разработки обобщенных представлений о развитии, как правило, отражают логику развития субъективной реальности либо по сущности природы (как созревание), либо по сущности социума (как формирование - формование). Логика развития по сущности человека - логика саморазвития как фундаментальная способность человека становиться и быть подлинным субъектом собственной жизни и деятельности - в таких обобщениях практически отсутствует.

Для того чтобы иметь действительную картину возможностей возраста, того или иного содержания образования, грамотных педагогических действий, необходимо видеть данную ступень образования и данный период развития в рамках целостной психологической и педагогической периодизации. Каждый возраст раскрывается в целостном ансамбле других возрастов. Возможности конкретного возраста определяются уровнем решения задач развития предшествующего возраста (откуда ребенок вышел) и масштабом предстоящих задач развития в последующем возрастном интервале (куда ребенку предстоит войти впоследствии).

Возрастно-нормативная модель развития носит прежде всего регулятивный характер, она должна отвечать на вопрос, как и зачем строится тот или иной образовательный процесс на данной ступени образования. В точном соответствии с понятием модели возрастно-нормативная модель развития должна представлять собой отображение в общей и наглядно выраженной форме сущность определенной действительности, в данном случае - возрастного развития.

Данные популяционных исследований, проведенных в 2010—2018 гг., позволили взглянуть на социальную ситуацию развития ребенка сквозь призму цифровой среды и выделить ее некоторые особенности, определяющие изменения в его развитии (когнитивное и личностное развитие, особенности взаимоотношений с окружающим миром, социальные и культурные практики):

- массовое и все более раннее овладение высокотехнологичным арсеналом новых культурных средств и инструментов — персонализированных и мобильных современных электронных устройств;
- увеличивающаяся длительность нахождения ребенка в онлайн-контекстах, задающих новые, плохо регламентированные и пока еще неизвестные по возможным последствиям влияния на ребенка среды обитания;
- активное, самостоятельное и стихийное освоение и использование подростками всех доступных онлайн-ресурсов как источников развивающего, обучающего и развлекательного контента и площадок онлайн-коммуникации;
- закрепление за социальными сетями статуса важнейших для подростков площадок самопрезентации, освоения различных социальных ролей, экспериментирования с идентичностью и самореализацией;
- значительное расширение круга социального капитала подростков за счет онлайн-контактов, в том числе слабых связей за счет «незнакомых друзей», с которыми не было опыта общения в реальной жизни;
- столкновение с широким кругом новых рисков онлайн-среды: контентными, коммуникационными, техническими и потребительскими, а также с риском чрезмерной увлеченности интернетом;
- существенная разница в пространственно-временной конфигурации пользования интернетом у подростков и их родителей;
- наличие цифрового разрыва между поколениями детей и родителей, снижение универсальности фигуры взрослого и его роли в детско-родительских отношениях;

- недостаточная цифровая компетентность детей и родителей, что не позволяет родителям выступать в роли экспертов эффективного и безопасного использования цифровых технологий;
- несоответствие системы образования изменениям цифрового общества, несмотря на готовность школьных учителей молодого и среднего возраста (поколения Y и X) к модернизации образовательного процесса.

В первую очередь необходимо принимать во внимание влияние интернета как специфической технологии, отличающей его от других медиатехнологий, возможных изменений нормативных моделей развития и здоровья детей и подростков, границ допустимого в контексте цифрового образа жизни, учета цифрового разрыва между поколениями и снижения возможностей взрослых конструировать детство в онлайне и в смешанной реальности.

Тема 3: Цифровая гигиена: зачем это нужно? Понятие периметра безопасности. Обеспечение эмоционально - психологического периметра безопасности в соответствии с возрастными особенностями ребенка. Баланс ценностей развития и ценностей безопасности

Жизнь в последние недели стремительно уходит в онлайн. Существенную часть своей жизни современные дети и подростки проводят в интернете, а значит без базовых знаний в области кибербезопасности им, как и взрослым, не обойтись. Чем раньше начать прививать навыки безопасного взаимодействия с виртуальной средой, тем прочнее они усвоятся. И станут такими же естественными, как мытье рук.

Подумайте, как часто родители попадают в такую ситуацию: ребенок смотрит видео в интернете. Вы выражаете недовольство тем, сколько времени он проводит за этим занятием или какой контент выбирает. На что получаете резонный ответ: «Если бы в твоем детстве было онлайн-видео, ты бы вел себя иначе?»

Многие представители поколения Z (люди, родившиеся между 1997 и 2015 годами) не выпускают смартфоны из рук. Гаджеты для них подобны новому органу чувств, объединяющему с глобальной сетью. Они выросли вместе с интернетом, это естественная и неотъемлемая часть их жизни. У поколения Z в интернете создается свой образ, новое «я», там же происходит постижение и проверка окружающего мира.

Согласно исследованию, проведенному GlobalWebIndex в 2019 году, у 97% представителей поколения Z есть мобильный телефон, и 78% из них считают его основным устройством для доступа в интернет.

С учетом особенностей поведения детей и подростков в интернете и их потребностей, стоит уделить особое внимание анонимности и приватность, целостности цифрового образа, защите репутации, защите от кибербуллинга и нежелательных знакомств, а также финансовых онлайн-транзакций и счетов.

Сам факт того, что через интернет можно что-то украсть или нанести вред не вызывает у подростков особого удивления. Гораздо больший интерес они проявляют к тому, что можно украсть именно у них и как хакеры и кибермошенники могут навредить через интернет именно им.

По данным недавнего исследования компании Proofpoint, производящей решения для безопасности электронной почты, менее 1% всех атак эксплуатируют уязвимости систем. Остальные используют человеческий фактор. Другими словами, технические средства предупреждения и мониторинга атак успешно совершенствуются,

искусственный интеллект и средства автоматизации позволят быстро реагировать на большинство инцидентов, но как быть с действиями сами людей?

Вспоминается красивая история про французского маршала Лиоте. Маршал служил в Африке. Однажды, сетуя на жару и сильное солнце, он приказал подчиненным обсадить дорогу деревьями. Подчиненные возразили, что деревья вырастут только через 50 лет. На что Лиоте парировал: «Именно поэтому работу надо начать сегодня же».

В ближайшие десятилетия поколение Z унаследует планету, оно будет стоять у руля компаний, организаций, государств. Оно будет жить в мире, где без навыков информационной безопасности уже не обойтись. Чтобы эти навыки сформировались, потребуется немало времени, именно поэтому работу стоит начать сегодня.

Что же делать родителям и учителям? Запрещать, проверять или пустить все на самотек? В первую очередь надо осознать, что полностью контролировать поведение ребенка или подростка в интернете невозможно. Так же, как раньше было невозможно полностью контролировать, что ребенок делает во дворе после уроков.

Однако взрослые могут и должны быть авторитетным источником информации о том, что такое хорошо и что такое плохо в новых реалиях.

В цифровом пространстве есть свои правила гигиены. К использованию интернета и потреблению информации стоит относиться так же, как к потреблению в физическом мире. Кстати, поколение Z воспринимает эту идею достаточно легко, поскольку границы между реальным и виртуальным миром для него несколько размыты.

Вот 10 базовых приемов информационной безопасности, о которых нужно знать и говорить детям и подросткам:

1. Не давайте свой телефон незнакомым людям, которым якобы нужно срочно позвонить. Вы же не хотите, чтобы в руки незнакомцев попал разблокированный телефон?

2. Используйте длинные и надежные пароли, а также биометрию и двухфакторную аутентификацию, особенно для платежей и денежных переводов. Использование удобных коротких паролей может плохо кончиться.

3. Меньше рассказывайте о себе в интернете. Думайте, кому и что вы говорите. Злоумышленники могут использовать раскрытые вашими же руками личные данные, чтобы атаковать вас.

4. Не принимайте запросы на дружбу от незнакомых людей в социальных сетях. Как минимум, это может кончиться валом рекламного спама. Про более скверные сценарии пишут в таблоидах каждый день.

5. Следите за тем, какие приложения получают на ваших устройствах доступ и к чему. Новой игре совершенно не обязательно знать, где вы сейчас находитесь или иметь доступ к камере или микрофону.

6. Обновляйте программы и операционные системы на всех устройствах (не только мобильных). Разработчики не зря едят свой хлеб и в новых версиях добавляют не только красивые кнопки, но и закрывают уязвимости.

7. С осторожностью открывайте электронные письма. Открывать письма с неизвестных адресов — все равно, что есть еду, которую нашел на улице. Эффект может быть схожим— заражение.

8. Аккуратнее относитесь к использованию публичных сетей Wi-Fi при обращении к своему мобильному банку. В сети гостиниц и других мест отдыха часто внедряются любители легкой наживы.

9. Не скачивайте «поломанное» программное обеспечение с неизвестных сайтов. Заражение фактически обеспечено. Для этого и размещают такое ПО, нашпигованное ловушками, а вовсе не для удобства наивных пользователей.

10. Контролируйте, что ваш ребенок покупает в интернете — все средства для этого встроены в современные операционные системы. Вы должны давать ребенку разрешение на покупку в сети в каждом случае. Наконец, заведите для этих целей отдельную дебетовую карту и пополняйте ее на ту сумму, которую не боитесь потерять.

Учите на собственном примере

Помните, что дети и подростки в целом разбираются в использовании компьютеров и мобильных устройств лучше вас. Но они не имеют вашего жизненного опыта и более доверчивы. Как поговаривала Фрекен Бок, «мой руки и учи уроки». А современным родителям стоит регулярно напоминать своим чадам: «Используй длинные пароли и не скачивай на свой телефон что попало».

Нельзя предусмотреть все. Но можно научить ребенка базовым и принципиальным вещам. А в остальном он разберется самостоятельно. Но прежде всего, конечно, сработают ваш личный пример и доверительные отношения.

Тема 4: Угрозы информационной безопасности: атаки, связанные с компьютерной инженерией. Способы выявления наличия вредоносных кодов на устройствах. Действия при обнаружении вредоносных кодов на устройствах.

Пользователи компьютеров Windows и Mac, смартфонов и планшетов находятся под постоянно растущей угрозой, исходящей от компьютерных вирусов и вредоносных программ. Принятие мер означает понимание того, с чем вы столкнулись. Рассмотрим основные типы вредоносных программ и их последствия.

Термин «вредоносное ПО» используется для описания любой вредоносной программы на компьютере или мобильном устройстве. Эти программы устанавливаются без согласия пользователей и могут вызывать ряд неприятных последствий, таких как снижение производительности компьютера, извлечение из системы персональных данных пользователя, удаление данных или даже воздействие на работу аппаратных средств компьютера. Поскольку киберпреступники придумывают все более сложные способы проникновения в системы пользователей, рынок вредоносных программ существенно расширился. Давайте рассмотрим некоторые из наиболее распространенных типов вредоносных программ, которые можно встретить в интернете.

1. Вирусы

Компьютерные вирусы получили свое название за способность «заражать» множество файлов на компьютере. Они распространяются и на другие машины, когда зараженные файлы отправляются по электронной почте или переносятся пользователями на физических носителях, например, на USB-накопителях или (раньше) на дискетах. По данным Национального института стандартов и технологий (NIST) , первый компьютерный вирус под названием «Brain» был написан в 1986 году двумя братьями с целью наказать пиратов, ворующих ПО у компании. Вирус заражал загрузочный сектор дискет и передавался на другие компьютеры через скопированные зараженные дискеты.

2. Черви

В отличие от вирусов, червям для распространения не требуются вмешательства человека: они заражают один компьютер, а затем через компьютерные сети распространяются на другие машины без участия их владельцев. Используя уязвимости сети, например, недостатки в почтовых программах, черви могут отправлять тысячи своих копий и заражать все новые системы, и затем процесс начинается снова. Помимо того, что многие черви просто «съедают» системные ресурсы, снижая тем самым

производительность компьютера, большинство из них теперь содержит вредоносные «составляющие», предназначенные для кражи или удаления файлов.

3. Рекламное ПО

Одним из наиболее распространенных типов вредоносных программ является рекламное ПО. Программы автоматически доставляют рекламные объявления на хост-компьютеры. Среди разновидностей Adware - всплывающие рекламные объявления на веб-страницах и реклама, входящая в состав «бесплатного» ПО. Некоторые рекламные программы относительно безвредны, в других используются инструменты отслеживания для сбора информации о вашем местонахождении или истории посещения сайтов и вывода целевых объявлений на экран вашего компьютера. BetaNews сообщил об обнаружении нового типа рекламного ПО, который может отключить антивирусную защиту. Поскольку Adware устанавливается с согласия пользователя, такие программы нельзя назвать вредоносными: обычно они идентифицируются как «потенциально нежелательные программы».

4. Шпионское ПО

Шпионское ПО делает то, что предполагает его название - следит за вашими действиями на компьютере. Оно собирает информацию (например, регистрирует нажатия клавиш на клавиатуре вашего компьютера, отслеживает, какие сайты вы посещаете и даже перехватывает ваши регистрационные данные), которая затем отправляется третьим лицам, как правило, киберпреступникам. Оно также может изменять определенные параметры защиты на вашем компьютере или препятствовать сетевым соединениям. Новые типы шпионских программ позволяют злоумышленникам отслеживать поведение пользователей (естественно, без их согласия) на разных устройствах.

5. Программы-вымогатели

Программы-вымогатели заражают ваш компьютер, затем шифруют конфиденциальные данные, например, личные документы или фотографии, и требуют выкуп за их расшифровку. Если вы отказываетесь платить, данные удаляются. Некоторые типы программ-вымогателей могут полностью заблокировать доступ к вашему компьютеру. Они могут выдавать свои действия за работу правоохранительных органов и обвинить вас в каких-либо противоправных поступках. В июне 2015 года в Центр приёма жалоб на мошенничество в Интернете при ФБР обратились пользователи, сообщившие о финансовых потерях на общую сумму 18 000 000 долларов в результате деятельности вируса-вымогателя CryptoWall.

6. Боты

Боты - это программы, предназначенные для автоматического выполнения определенных операций. Они могут использоваться для легитимных целей, но злоумышленники приспособили их для своих вредоносных целей. Проникнув в компьютер, боты могут заставить его выполнять определенные команды без одобрения или вообще без ведома пользователя. Хакеры могут также пытаться заразить несколько компьютеров одним и тем же ботом, чтобы создать бот-сеть, которая затем будет использоваться для удаленного управления взломанными машинами - красть конфиденциальные данные, следить за действиями жертвы, автоматически распространять спам или запускать разрушительные DDoS-атаки в компьютерных сетях.

7. Руткиты

Руткиты позволяют третьей стороне получать удаленный доступ к компьютеру и управлять им. Эти программы используются IT-специалистами для дистанционного устранения сетевых проблем. Но в руках злоумышленников они превращаются в инструмент мошенничества: проникнув в ваш компьютер, руткиты обеспечивают киберпреступникам возможность получить контроль над ним и похитить ваши данные или установить другие вредоносные программы. Руткиты умеют качественно маскировать свое присутствие в системе, чтобы оставаться незамеченными как можно дольше. Обнаружение такого вредоносного кода требует ручного мониторинга необычного поведения, а также регулярного внесения корректировок в программное обеспечение и операционную систему для исключения потенциальных маршрутов заражения.

8. Троянские программы

Более известные как троянцы, эти программы маскируются под легитимные файлы или ПО. После скачивания и установки они вносят изменения в систему и осуществляют вредоносную деятельность без ведома или согласия жертвы.

9. Баги

Баги - ошибки в фрагментах программного кода - это не тип вредоносного ПО, а именно ошибки, допущенные программистом. Они могут иметь пагубные последствия для вашего компьютера, такие как остановка, сбой или снижение производительности. В то же время баги в системе безопасности - это легкий способ для злоумышленников обойти защиту и заразить вашу машину. Обеспечение более эффективного контроля безопасности на стороне разработчика помогает устранить ошибки, но важно также регулярного проводить программные корректировки, направленные на устранение конкретных багов.

Мифы и факты

Существует ряд распространенных мифов, связанных с компьютерными вирусами:

- **Любое сообщение об ошибке компьютера указывает на заражение вирусом.** Это неверно: сообщения об ошибках также могут быть вызваны ошибками аппаратного или программного обеспечения.
- **Вирусам и червям всегда требуется взаимодействие с пользователем.** Это не так. Для того чтобы вирус заразил компьютер, должен быть исполнен код, но это не требует участия пользователя. Например, сетевой червь может заражать компьютеры пользователей автоматически, если на них имеются определенные уязвимости.
- **Вложения к электронным письмам от известных отправителей являются безопасными.** Это не так, потому что эти вложения могут быть заражены вирусом и использоваться для распространения заражения. Даже если вы знаете отправителя, не открывайте ничего, что в чем вы не уверены.
- **Антивирусные программы могут предотвратить заражение.** Со своей стороны, поставщики антивирусного ПО делают все возможное, чтобы не отставать от разработчиков вредоносных программ, но пользователям обязательно следует установить на своем компьютере комплексное защитное решение класса Internet security, который включает в себя технологии, специально предназначенные для активного блокирования угроз. Даже при том, что 100-процентной защиты не существует. Нужно просто осознанно подходить к обеспечению собственной онлайн-безопасности, чтобы уменьшить риск подвергнуться атаке.
- **Вирусы могут нанести физический ущерб вашему компьютеру.** Что если вредоносный код приведет к перегреву компьютера или уничтожит критически важные микрочипы? Поставщики защитных решений неоднократно развенчивали этот миф - такие повреждения просто невозможны.

Между тем, рост количества устройств взаимодействующих друг с другом в Интернете Вещей (IoT), открывает дополнительные интересные возможности: что если зараженный автомобиль съедет с дороги, или зараженная «умная» печь продолжит нагреваться, пока не случится превышение нормальной нагрузки? Вредоносного ПО будущего может сделать такой физический ущерб реальностью.

У пользователей есть ряд неправильных представлений о вредоносных программах: например, многие считают, что признаки заражения всегда заметны и поэтому они смогут определить, что их компьютер заражен. Однако, как правило,

вредоносное ПО не оставляет следов, и ваша система не будет показывать каких-либо признаков заражения.

Так же не стоит верить, что все сайты с хорошей репутацией безопасны. Они также могут быть взломаны киберпреступниками. А посещение зараженного вредоносным кодом легитимного сайта – еще большая вероятность для пользователя расстаться со своей личной информацией. Именно это, произошло с Всемирным банком. Также многие пользователи считают, что их личные данные - фотографии, документы и файлы - не представляют интереса для создателей вредоносных программ. Киберпреступники же используют общедоступные данные для того, чтобы атаковать отдельных пользователей, или собрать информацию, которая поможет им создать фишинговые письма, чтобы проникнуть во внутренние сети организаций.

Стандартные методы заражения

Итак, как же происходит заражение компьютерными вирусами или вредоносными программами? Существует несколько стандартных способов. Это ссылки на вредоносные сайты в электронной почте или сообщениях в социальных сетях, посещение зараженного сайта (известного как drive-by загрузка) и использование зараженного USB-накопителя на вашем компьютере. Уязвимости операционной системы и приложений позволяют злоумышленникам устанавливать вредоносное ПО на компьютеры. Поэтому для снижения риска заражения очень важно устанавливать обновления для систем безопасности, как только они становятся доступными.

Киберпреступники часто используют методы социальной инженерии, чтобы обманом заставить вас делать что-то, что угрожает вашей безопасности или безопасности вашей компании. Фишинговые сообщения являются одним из наиболее распространенных методов. Вы получаете на вид абсолютно легитимное электронное сообщение, в котором вас убеждают загрузить зараженный файл или посетить вредоносный веб-сайт. Цель хакеров - написать сообщение так, чтобы вы нашли его убедительным. Это может быть, например, предупреждение о возможном вирусном заражении или уведомление из вашего банка или сообщение от старого друга.

Конфиденциальные данные, такие как пароли, являются главной целью киберпреступников. Помимо использования вредоносных программ для перехвата паролей в момент их ввода, злоумышленники также могут собирать пароли с веб-сайтов и других компьютеров, которые они взломали. Вот почему так важно использовать уникальный и сложный пароль для каждой учетной записи. Он должен состоять из 15 и более символов, включающих буквы, цифры и специальные символы. Таким образом, если киберпреступникам удастся взломать один аккаунт, они не получат доступ ко всем

вашим учетным записям. К сожалению, большинство пользователей имеют очень слабые пароли: вместо того, чтобы придумать труднодоступную комбинацию, они обращаются к standby-паролям типа «123456» или «Password123», которые преступники легко подбирают. Даже контрольные вопросы не всегда могут служить эффективной защитой, потому что многие люди дают один и тот же ответ на вопрос «Ваше любимая еда?», например, если вы находитесь в Соединенных Штатах, то почти наверняка ответ будет - «Пицца».

Признаки заражения

Хотя большинство вредоносных программ не оставляет никаких явных следов, и ваш компьютер работает нормально, иногда все же можно заметить признаки возможного заражения. Самый первый из них - снижение производительности, т.е. процессы происходят медленные, загрузка окон занимает больше времени, в фоновом режиме работают какие-то случайные программы. Еще одним настораживающим признаком может считаться измененных домашних интернет-страниц в вашем браузере или более частое, чем обычно, появление всплывающих объявлений. В некоторых случаях вредоносное ПО даже может влиять на базовые функции компьютера: не открывается Windows, нет подключения к Интернету или доступа к более высокоуровневым функциям управления системой более высокого уровня. Если вы подозреваете, что ваш компьютер может быть заражен, немедленно произведите проверку системы. Если заражение не обнаружено, но вы все еще сомневаетесь, получите второе мнение - запустите альтернативный антивирусный сканер.

Тема 5: Угрозы информационной безопасности: атаки, связанные с социальной инженерией. Груминг, кибербуллинг. Чему мы должны научить ребёнка для профилактики насилия в Сети?

Социальная инженерия используется ежедневно обычными людьми в повседневных ситуациях. Например, во взаимодействии педагогов со своими учениками. Врачи, психологи и психотерапевты часто используют элементы социальной инженерии, чтобы “манипулировать” своими пациентами, для принятия мер, которые помогут пациенту, а мошенник использует элементы социальной инженерии, чтобы убедить его выполнить действия, необходимые злоумышленнику или раскрыть информацию. Хотя конец игры сильно отличается, подход может быть очень похож. Психолог может использовать ряд хорошо продуманных вопросов, чтобы помочь пациенту прийти к выводу, что необходимы перемены. Аналогичным образом мошенник будет использовать ряд хорошо продуманных вопросов, чтобы поставить его цель в уязвимое положение. Как и любой инструмент, социальная инженерия не является «хорошей» или «плохой», это просто инструмент, который имеет много различных применений.

Социальная инженерия в контексте информационной безопасности, относится к психологической манипуляции людей, которые приводят к совершению действия или разглашению конфиденциальной информации. Это может быть злоупотребление доверием с целью сбора информации. Социальная инженерия часто является одним из многих шагов в более сложную схему мошенничества.

В общем значении социальная инженерия - это акт манипуляции человеком, который провоцирует выполнить действие, которое как может быть в интересах человека, так и в интересах злоумышленника.

Рассмотрим основные виды социальных инженеров.

– Хакеры. Поставщики программного обеспечения становятся все более продвинуты в создании такого ПО, которое более безопасно и сложно для взлома. Так как взломать хорошо защищенное ПО затруднительно, хакеры прибегают к социальной инженерии. Они часто используют сочетание аппаратных и личных навыков.

– «Пентестеры». Пентест — метод оценки безопасности компьютерных систем или сетей средствами моделирования атаки злоумышленника. В информационных системах хранится, обрабатывается, циркулирует различная информация, потеря или искажение которой может нанести существенный вред. Процесс включает в себя активный анализ системы на наличие потенциальных уязвимостей, которые могут спровоцировать

некорректную работу целевой системы, либо полный отказ в обслуживании. Цель испытаний на проникновение — оценить его возможность осуществления и спрогнозировать экономические потери в результате успешного осуществления атаки. «Пентестеры» — это люди, которые проводят моделирование атаки на систему, анализируют возможные уязвимости, но не используют собранную информацию для личной выгоды или ущерба компании. Однако, потенциально это возможно.

– Шпионы. Используют социальную инженерию как способ жизни. Помимо того, что они изучили искусство социальной инженерии и являются экспертами в этой науке, очень часто шпионы также опираются на доверие. Они немного (а может и много) знают о бизнесе и власти и используют это, как рычаг давления.

– Воры личной информации. Данный вид социальных инженеров использует такую информацию, как, например, имя человека, номер банковского счета, адрес, дата рождения, и номер социального страхования, без ведома владельца. Это преступление основывается на использовании личной информации для гораздо более сложного преступления.

– Недобросовестные сотрудники. В любой сфере деятельности случаются конфликты работника и работодателя, иногда это приводит к тому, что работник начинает враждебно относиться к работодателю. Поскольку работник, как правило, пытается скрыть своё недовольство, чтобы не потерять работу, это приводит к тому, что его враждебность растёт и становится оправданием для хищения, вандализма, раскрытия конфиденциальной информации и других преступлений.

– Аферисты. Мотивом чаще всего служит желание «заработать». Аферисты и мошенники владеют способностью читать людей и находить детали, которые делают человека уязвимым. Они также квалифицированы в создании ситуаций, которые являются отличными возможностями для оценки изучаемого человека.

– Вербовщики. Также освоили многие аспекты социальной инженерии. Овладели приемами сбора, многими психологическими принципами социальной инженерии, они очень умело могут не только читать, но и понимать, что движет людьми.

– Продавцы. Многие гуру продаж говорят, что хороший продавец не должен манипулировать людьми, но ему следует использовать свои навыки, чтобы выяснить, какие потребности есть у людей и увидеть, могут ли они ему что-то предложить. Искусство продаж требует многих навыков, таких как сбор информации, убеждение, и многие другие.

– Врачи, психологи и юристы. На первый взгляд может показаться, что данный тип не вписывается в категорию социальных инженеров. Но эта группа использует те же

методы, как и другие группы в этом списке. Они это делают не обязательно для того, чтобы навредить своему клиенту, чаще, чтобы разобраться и подобрать нужный алгоритм для выхода из сложившейся ситуации.

Безопасность детей в Сети, пожалуй, больше всего беспокоит родителей. Если ребенок пользуется Интернетом, как его обезопасить? Статистика весьма неутешительна.

Один из опросов агентства Childwise установил, что у трех из четверых детей в возрасте от пяти до шестнадцати лет (73 %) есть доступ в Интернет из спальни, а у 10 % из них не было настроек приватности для просмотра личных данных. В отчете, подготовленном Национальным обществом предупреждения жестокого обращения с детьми (NSPCC), сказано, что почти четверть детей в возрасте одиннадцати-двенадцати лет, у которых есть странички в социальных сетях, сильно огорчалась из-за чего-то, увиденного там за последний год. Более половины таких случаев (62 %) были спровоцированы незнакомцами, то есть теми, кого они знали только виртуально, к тому же многие дети не могли понять, что стало причиной их расстройства. Сталкиваясь с чем- то огорчительным или неприятным в Сети, младшие дети могли определить причину своего расстройства с меньшей уверенностью, чем старшие, — еще один признак того, что дошкольникам и младшим школьникам не хватает сноровки в общении и устойчивости для того, чтобы пользоваться социальными сетями.

К сожалению, родители часто не следят за детьми так тщательно, как следовало бы. Только 32 % из них считают себя «очень уверенными» в безопасности детей при пользовании Интернетом. В реальной жизни мы следим за нашими чадами гораздо более внимательно, чем в виртуальной реальности, хотя Интернет таит для них много опасностей. Мы запрещаем детям разговаривать с незнакомцами, но зачастую это не касается онлайн-пространства.

Пользование девайсом — это всегда очень изолированное занятие, в отличие от просмотра телевизора или игры на детской площадкой, где за детьми легко следить. Когда ребенок сидит перед экраном планшета, родители обычно не знают, что он там делает. Они оставляют его одного, потому что он притих, и спешат заняться своими делами.

Дети 4-11 лет не должны общаться с незнакомцами в Сети, но иногда, несмотря на все старания родителей, они общаются с ними на форумах или в групповых чатах онлайн-игр. Важно объяснить, что если они не знают кого-то в реальной жизни, то человек все еще считается незнакомцем, даже если они разговаривают онлайн. Маленьким детям бывает очень сложно это понять.

Виртуальные отношения могут развиться очень быстро. Мальчики и девочки говорят своим виртуальным друзьям такие вещи, которые никогда не осмелились бы

произнести в реальной жизни, и очень быстро выдают личную информацию. Родителям нужно объяснить, что виртуальное общение — не то же самое, что встреча в парке отдыха или на школьном дворе: неизвестно, кто сидит по ту сторону экрана на самом деле. Прежде чем что-то написать, детям стоит задаться вопросом, смогли бы они повторить это кому-то в реальном мире? Стали бы они делиться личной информацией со случайным прохожим?

Груминг — это процесс, во время которого кто-то общается с ребенком в Сети и постепенно совращает его. К сожалению, анонимность интернет-пространства дает для этого множество возможностей. Человек может поставить детское изображение на фото профиля и подружиться с ребенком в социальной сети или в игре. Он может рассказать интересную историю или болтать об общих интересах и увлечениях, то есть вызвать доверие и начать выстраивать отношения. Важно, чтобы любой ребенок, пользующийся Интернетом, знал о груминге, но родители часто переживают и не знают, как просветить его.

Но рассказать об опасных незнакомцах в интернет-пространстве и поговорить с детьми о груминге (на языке, соответствующем их возрасту) абсолютно необходимо. Просветите их как можно раньше. Объясните, что в Интернете люди часто оказываются не теми, за кого себя выдают. Дети склонны думать, что социальные сети — это конкурс популярности, поэтому чем больше людей будет у них в подписчиках, тем лучше. Но они не должны принимать запросы в друзья от того, кого они не знают в реальной жизни. Дети, желательно с вашей помощью, должны также проверять запросы от тех, кого они знают, чтобы убедиться, что аккаунт настоящий.

То же относится к общению в мессенджерах и чатах. Маленькие дети не должны общаться с незнакомцами онлайн и соглашаться на приватный чат с незнакомцем. Если кто-то отправляет им сообщение или пытается выйти в чат, они обязательно должны поставить вас в известность — как если бы чужой человек подошел к ним на улице или в парке. Даже если ваш ребенок не находится онлайн без присмотра взрослого, вам все равно нужно разговаривать с ним об этом. Дети должны быть образованы. Остерегайтесь онлайн-игр, где они могут играть с незнакомцами!

Поговорите с ними об информации, которую они выдают людям, общаясь в Интернете. Ребенок не должен называть свое полное имя, домашний адрес, электронную почту, номер телефона или номер школы людям, которых не знает в реальной жизни. Убедись, что никнейм ваших детей не намекает на то, как их зовут на самом деле. Объясните, что все, что они выкладывают онлайн — имя пользователя, фотографии или комментарии, — воссоздает их образ, поэтому люди могут их узнать.

Крайне важно, чтобы родители разговаривали со своим ребенком и всегда были начеку. Пусть он покажет вам все сайты, на которые заходит, когда пользуется Интернетом. Объясните, что когда он находится онлайн, ему нужно действовать, как детективу. Откуда он знает, что человек действительно того возраста, который назвал? Что он знает об этом человеке? Видел ли он когда-либо его фотографию? Уверен ли, что эта фотография настоящая? Объясните ребенку, что виртуальное пространство совсем не похоже реальный мир и нельзя принимать все за чистую монету. В обычной жизни мы знаем, как выглядят учитель или полицейский. Мы видим, где они работают и какую форму носят.

Если вы даете ребенку телефон с камерой, вы должны установить правила до того, как он начет им пользоваться. Может, это прозвучит чересчур драматично, но вы, именно ВЫ, вручаете ребенку средство для совершения разрушающих и необратимых действий. Большинство детей интуитивно знают, что не стоит отправлять кому-либо непристойные фотографии, но потом они начинают общаться в чате с другим ребенком и принимают такую просьбу за близость, вызов или игру. Они действуют, не думая о последствиях. Печальный факт заключается в том, что как только вы отправили кому-то свою фотографию, она вам больше не принадлежит. Получатель может сделать с ней все, что посчитает нужным. Девочки часто отправляют фотографии своей груди или декольте. Мальчики принимают это за некий трофей и хотят похвастаться своей подружкой перед друзьями. До того как они осознают плачевность ситуации, фотография девочки обойдет всю школу. Такое может омрачить жизнь любому.

Дети осознают публичность Интернета, только когда попадаются на чем-то.

Травля в интернете может быть абсолютно разной. Есть несколько важных определений, которые помогут разобраться в категориях насилия в сети. Если «буллинг» — это проявление физического или психологического насилия по отношению к другим вообще, то «кибербуллинг» — это то же насилие, только в цифровом пространстве.

Важно помнить, что кибербуллинг — это скорее общее определение для разных видов травли в интернете, и его не стоит путать с кибермоббингом и кибертравлей.

•Кибермоббинг — вид насилия в цифровой среде, реализуемый с помощью электронного текста (сообщений и комментариев).

•Кибертравля — причинение вреда человеку за счет длительного давления в интернет-пространстве: преследования, распространения слухов, запугивания.

Иногда кибербуллинг может переходить в оффлайн. Многие блогеры и публичные личности сталкиваются с киберсталкингом. Это вид насилия, когда подписчики выслеживают инфлюенсеров и начинают их преследовать за пределами социальных сетей.

Важно помнить:

•Кибербуллинг — это агрессия.

•Не стоит обесценивать эмоции человека, который перенес насилие в интернете. Подверженные травле люди страдают не понарошку, причем это может быть не только психологическая, но и физическая боль.

•Отключение интернета и другие санкции не помогут. Лучше всего проявить эмпатию и выразить поддержку.

Согласно исследованию, 58% российских интернет-пользователей сталкивались с онлайн-агрессией. Каждый четвертый был мишенью такого поведения, и только 4% опрошенных признаются, что были инициаторами травли.

Есть много способов сделать человеку больно. Например, написать токсичный комментарий под фотографией, оскорбить в групповом чате или на стенке в социальной сети, затроллить, выложить данные или подробности из личной жизни. Поводом для кибербуллинга чаще всего являются внешность, сексуальная ориентация и активность в интернете.

Чаще всего человек не может сам защититься от кибербуллинга, но лишь небольшая часть пользователей готова поддержать жертву травли в сети. Исследователи выяснили, что:

•52% респондентов никогда не заступались ни за кого в интернете,

•65% считают публичную поддержку бессмысленной,

•13% боятся, что агрессия перекинется на них,

•20% полагают, что они бессильны и ничего не могут сделать, чтобы поддержать пострадавшего от кибербуллинга.

Сейчас некоторые социальные сети рассказывают о том, как обезопасить себя от травли в онлайн-пространстве. Практические советы можно найти в Центре безопасности «ВКонтакте» или в рекомендациях от Instagram.

Что делать при травле в интернете

•Лучше всего обратиться к психологу, чтобы проработать проблему. Школьники могут получить поддержку у педагога-психолога, который работает в их учебном заведении.

•Помочь детям и родителям разобраться в конфликтной ситуации может программа Травли Net.

•Психологическую поддержку окажут и в сервисе МАЯК от Добра Mail.ru.

Чтобы защитить себя от агрессии, постарайтесь научиться отстаивать свои границы и говорить о своих чувствах. Не забывайте, что вы всегда можете прекратить общение с

людьми, которые причиняют боль в интернете. Во всех социальных сетях есть функция блокировки нежелательных пользователей. Просто заблокируйте агрессора, тем самым закрыв ему доступ к дальнейшим негативным действиям.

Тема 6: Угрозы информационной безопасности: атаки, связанные с социальной инженерией. Фишинг. Обращение с деньгами в сети Интернет. Детская пластиковая карта: быть или не быть?

Социальная инженерия используется ежедневно обычными людьми в повседневных ситуациях. Например, во взаимодействии педагогов со своими учениками. Врачи, психологи и психотерапевты часто используют элементы социальной инженерии, чтобы “манипулировать” своими пациентами, для принятия мер, которые помогут пациенту, а мошенник использует элементы социальной инженерии, чтобы убедить его выполнить действия, необходимые злоумышленнику или раскрыть информацию. Хотя конец игры сильно отличается, подход может быть очень похож. Психолог может использовать ряд хорошо продуманных вопросов, чтобы помочь пациенту прийти к выводу, что необходимы перемены. Аналогичным образом мошенник будет использовать ряд хорошо продуманных вопросов, чтобы поставить его цель в уязвимое положение. Как и любой инструмент, социальная инженерия не является «хорошей» или «плохой», это просто инструмент, который имеет много различных применений.

Социальная инженерия в контексте информационной безопасности, относится к психологической манипуляции людей, которые приводят к совершению действия или разглашению конфиденциальной информации. Это может быть злоупотребление доверием с целью сбора информации. Социальная инженерия часто является одним из многих шагов в более сложную схему мошенничества.

В общем значении социальная инженерия - это акт манипуляции человеком, который провоцирует выполнить действие, которое как может быть в интересах человека, так и в интересах злоумышленника.

Фи′шинг — вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям. Это достигается путём проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов, например, от имени банков или внутри социальных сетей. В письме часто содержится прямая ссылка на сайт, внешне неотличимый от настоящего, либо на сайт с редиректом. После того как пользователь попадает на поддельную страницу, мошенники пытаются различными психологическими приёмами побудить пользователя ввести на поддельной странице свои логин и пароль, которые он использует для доступа к определённому сайту, что позволяет мошенникам получить доступ к аккаунтам и банковским счетам.

Фишинг — одна из разновидностей социальной инженерии, основанная на

незнании пользователями основ сетевой безопасности: в частности, многие не знают простого факта: сервисы не рассылают писем с просьбами сообщить свои учётные данные, пароль и прочее.

Для защиты от фишинга производители основных интернет- браузеров договорились о применении одинаковых способов информирования пользователей о том, что они открыли подозрительный сайт, который может принадлежать мошенникам. Новые версии браузеров уже обладают такой возможностью, которая соответственно именуется «антифишинг».

Целью фишеров сегодня являются клиенты банков и электронных платёжных систем. Часть последних фишинговых атак была направлена непосредственно на руководителей и иных людей, занимающих высокие посты в компаниях.

Социальные сети также представляют большой интерес для фишеров, позволяя собирать личные данные пользователей: в 2006 году компьютерный червь разместил на MySpace множество ссылок на фишинговые сайты, нацеленные на кражу регистрационных данных; в мае 2008 года первый подобный червь распространился и в популярной российской сети ВКонтакте. По оценкам специалистов, более 70 % фишинговых атак в социальных сетях успешны.

Человек всегда реагирует на значимые для него события. Поэтому фишеры стараются своими действиями встревожить пользователя и вызвать его немедленную реакцию. Поэтому, к примеру, электронное письмо с заголовком «чтобы восстановить доступ к своему банковскому счёту …», как правило, привлекает внимание и заставляет человека пройти по веб-ссылке для получения более подробной информации.

Большинство методов фишинга сводится к тому, чтобы замаскировать поддельные ссылки на фишинговые сайты под ссылки настоящих организаций. Адреса с опечатками или субдомены часто используются мошенниками.

Фишеры часто вместо текста используют изображения, что затрудняет обнаружение мошеннических электронных писем антифишинговыми фильтрами. Но специалисты научились бороться и с этим видом фишинга. Так, фильтры почтовых программ могут автоматически блокировать изображения, присланные с адресов, не входящих в адресную книгу. К тому же появились технологии, способные обрабатывать и сравнивать изображения с сигнатурами однотипных картинок, используемых для спама и фишинга.

Обман не заканчивается на посещении жертвой фишингового сайта. Некоторые фишеры используют JavaScript для изменения адресной строки. Это достигается либо путём размещения картинки с поддельным URL поверх адресной строки либо закрытием

настоящей адресной строки и открытием новой с поддельным URL.

Злоумышленник может использовать уязвимости в скриптах подлинного сайта. Этот вид мошенничества (известный как межсайтовый скриптинг) наиболее опасен, так как пользователь авторизуется на настоящей странице официального сайта, где всё (от веб-адреса до сертификатов) выглядит подлинным. Подобный фишинг очень сложно обнаружить без специальных навыков.

Для противостояния антифишинговым сканерам фишеры начали использовать веб-сайты, основанные на технологии Flash. Внешне подобный сайт выглядит как настоящий, но текст скрыт в мультимедийных объектах.

Сегодня фишинг выходит за пределы интернет-мошенничества, а поддельные веб-сайты стали лишь одним из множества его направлений. Письма, которые якобы отправлены из банка, могут сообщать пользователям о необходимости позвонить по определённому номеру для решения проблем с их банковскими счетами. Эта техника называется вишинг (голосовой фишинг). Позвонив на указанный номер, пользователь заслушивает инструкции автоответчика, которые указывают на необходимость ввести номер своего счёта и PIN-код. К тому же вишеры могут сами звонить жертвам, убеждая их, что они общаются с представителями официальных организаций, используя фальшивые номера. Чаще всего злоумышленники выдают себя за сотрудников службы безопасности банка и сообщают жертве о зафиксированной попытке незаконного списания средств с его счёта. В конечном счёте, человека также попросят сообщить его учётные данные.

Набирает свои обороты и SMS-фишинг, также известный как смишинг . Мошенники рассылают сообщения, содержащие ссылку на фишинговый сайт, — входя на него и вводя свои личные данные, жертва аналогичным образом передаёт их злоумышленникам. В сообщении также может говориться о необходимости позвонить мошенникам по определённому номеру для решения «возникших проблем».

Существуют различные методы для борьбы с фишингом, включая законодательные меры и специальные технологии, созданные для защиты от фишинга.

Один из методов борьбы с фишингом заключается в том, чтобы научить людей различать фишинг и бороться с ним. Люди могут снизить угрозу фишинга, немного изменив своё поведение. Так, в ответ на письмо с просьбой «подтверждения» учётной записи (или любой другой обычной просьбой фишеров) специалисты советуют связаться с компанией, от имени которой отправлено сообщение, для проверки его подлинности. Кроме того, эксперты рекомендуют самостоятельно вводить веб-адрес организации в адресную строку браузера вместо использования любых гиперссылок в подозрительном

сообщении.

Детская пластиковая карта

В банках всё чаще стали появляться предложения для детей и подростков, направленные на отказ от налички. Это не только специальные карты, но и приложения для бесконтактной оплаты. Всё бы ничего, но есть у этих платёжных карт подвох — кешбэк, как у взрослых.

Безналичная оплата всё активнее развивается в нашей стране: количество операций по безналичной оплате картами уже приближается к 80% от всех карточных транзакций. И вполне естественно, что этот тренд дошёл и до детских карманных расходов.

Открыть счёт ребёнку можно по достижении им 14-летия и с письменного согласия родителей.

Зачем банкам несовершеннолетние клиенты?

Выпуская на рынок этот новый продукт, банки обеспечивают себя постоянным наличием лояльных клиентов: дети вырастают и продолжают пользоваться услугами банка.

— Чтобы привлечь клиентов к открытию детских карт, разрабатываются условия, призванные обеспечить безопасность и удобство их использования: это и яркий дизайн, и низкая стоимость годового обслуживания, и возможность установить дневной или месячный лимит расходов или запрет на использование детской карты для снятия наличных в банкомате, перевода денег на другие карты или покупок в Интернете.

К плюсам детских банковских карт можно отнести и то, что с их помощью родители получают возможность легко контролировать траты своих детей. И этот контроль намного эффективней, чем в случае с наличными. Родитель получает СМС о каждой операции ребёнка, так что может видеть, на что именно были потрачены деньги. Кроме того, все траты обычно видны в банковском приложении или в интернет-банке. Родитель видит также, сколько денег на данный момент доступно ребёнку, в случае необходимости можно всегда пополнить карту в режиме онлайн.

Оптимальный вариант, когда банк, выпуская детскую карту, привязывает её к отдельному счёту, а не к основному счёту родителя. Во-первых, это безопаснее: на отдельный счёт ребёнка родитель переводит небольшие суммы на карманные расходы, в случае утери детской карты нет риска, что мошенники воспользуются средствами на "взрослом" счёте. Во-вторых, так проще контролировать "детский" остаток. Безусловно, никакой банк не откроет счёт ребёнку в 7 лет. "Детский" счёт по факту открывается на имя родителя, но ребёнок получает к нему доступ с помощью своей карты.

С помощью банковской карты дети научатся в будущем контролировать

финансовые расходы.

Опасности при использовании детской пластиковой карты такие же, как и у взрослых. Нужно заранее рассказать о мошенниках, объяснить, что нельзя никому называть данные карты, иначе есть риск потерять деньги с родительского счёта.

Необходтмо родителям отнестись к выбору такого продукта очень внимательно.

Обычно банки выпускают детям карты при условии, что родитель также оформляет взрослую карту в этом банке. Нужно ознакомиться с тарифами, годовое обслуживание взрослой карты может быть уже не бесплатным. Кроме того, взрослая карта может предполагать кредитный лимит. Необходимо выяснить, какой процент банк взимает по кредитной карте, какова продолжительность льготного периода, какие предлагаются бонусные программы. Нужно учитывать, что бесплатность детской карты банк может компенсировать финансовыми продуктами для родителей. Естественно, банку в этом случае выгодно, чтобы родитель пользовался кредитным лимитом, не укладывался в льготный период и платил банку проценты за пользование деньгами.

При грамотном подходе и правильном выборе банка детская кредитка — удобный продукт как для ребёнка, так и для родителя, даже если ему тоже придётся оформить карту этой кредитной организации.

Деньгами на этом банковском счёте/карте подросток может распоряжаться самостоятельно:

- снимать наличные;
- переводить деньги на карты другим людям;
- получать переводы от частных лиц;
- оплачивать покупки и услуги в розничных точках или через интернет;
- пополнять телефон, в т.ч. другим лицам;
- управлять операциями и контролировать баланс карты в мобильном .

Вопрос родительского контроля за молодежной картой законодательно не урегулирован. Банки по собственному усмотрению решают этот вопрос в правилах выпуска карт. Это значит, что банк может отказать родителям в предоставлении возможности контроля за операциями по карте подростка. Или дать согласие, при условии оплаты данной услуги.

Чтобы уберечь ребенка от необдуманных трат родители могут:

- Настраивать лимиты на покупки, снятие денег с карты.
- Отключить возможность расплачиваться дополнительной картой в интернете. При каждой попытке ребенка совершить онлайн-покупку родителю будет приходить СМС с кодом подтверждения операции.

- Запретить снимать с карты наличные, переводить деньги на другие банковские карты или счета.
- Получать отчеты обо всех операциях, совершаемых по карте.
- Отслеживать баланс карты.
- Просматривать историю операций.
- Заблокировать карту.

Как защитить банковскую карту ребенка от мошенников

Перед тем, как ребенок начнет пользоваться банковской картой установите на телефон ребенку лицензионную антивирусную программу. И расскажите ему об основных правилах финансовой безопасности:

Объясните, что на банковской карте указаны персональные данные: фамилия и имя держателя, срок действия карты, CVV-код, которые нельзя никому сообщать.

Нельзя фотографировать карту, хранить фото карты в телефоне, делиться им в соцсетях и мессенджерах.

Никому не сообщать ПИН-код карты, а также секретные коды, которые приходят в СМС-сообщениях на телефон для подтверждения покупок.

Прикрывать рукой клавиатуру при наборе ПИН-кода в банкомате или платежном терминале.

Помогите ребенку выучить наизусть ПИН-код от карты. Расскажите, почему нельзя записывать ПИН-код на карте, хранить его вместе с картой в кошельке.

Никому не давать свою банковскую карту, включая одноклассников, друзей.

При утере детской карты срочно сообщить об этом родителям, молодежной карты – позвонить в банк по телефону «горячей» линии.

Не совершать покупки в интернете и не вводить никаких персональных данных на незнакомых и подозрительных сайтах. Если есть хоть малейшие сомнения в надежность сайта – советуйся с родителями.

Не совершать покупки при входе в интернет в общественных местах через незапароленные точки Wi-Fi.

Не переходить по ссылкам из смс сообщений и из писем в формате HTML, особенно с незнакомых телефонных номеров и электронных адресов.

Скачивать понравившиеся приложения, игры и т.п. только из официальных магазинов приложений.

Подводя итоги

При грамотном подходе и правильном выборе банка детская карта — удобный финансовый инструмент как для ребёнка, так и для родителя.

Перед началом пользования картой, объясните ребенку базовые правила безопасного пользования картой. Не критикуйте покупки ребенка, даже если считаете, что он тратит деньги на ерунду.

Это его деньги, дайте ребенку право на ошибки и получение собственного финансового опыта. А вы, как родители, ненавязчиво обсуждайте с детьми последствия различных трат, подсказывайте, что можно сделать лучше. Так ребенок быстрее научится грамотно распоряжаться деньгами и будет видеть в вашем лице союзника, а не сурового критика.

Тема 7. Контентные риски. Настройка и безопасное использование смартфона или планшета. Семейный доступ.

Контентные риски — это материалы (тексты, картинки, аудио, видеофайлы, ссылки на сторонние ресурсы), содержащие насилие, агрессию, эротику и порнографию, нецензурную лексику, информацию, разжигающую расовую ненависть, пропаганду анорексии и булимии, суицида, азартных игр, наркотических веществ и т.д. Столкнуться с ними можно практически везде. Это и сайты, и социальные сети, и блоги, и торренты, и видеохостинги, фактически все, что сейчас существует в Интернете. Зачастую подобный материал может прийти от незнакомца по почте в виде спама или сообщения.

Поиск информации в Сети может быть сопряжен с риском для безопасности компьютера и привести к печальным последствиям для его владельца. В общей массе ссылок, которые появляются в окне браузера в ответ на поисковый запрос, часто оказываются подозрительные ресурсы и фишинговые сайты.

- В первую очередь под прицелом киберпреступников оказываются любители бесплатного и пиратского софта.
- На втором месте по степени опасности находятся запросы информации «для взрослых», которая традиционно используется злоумышленниками для распространения зловредов.
- опасными являются ссылки на сайты с кулинарными рецептами, толкованиями сновидений, советами по уходу за собой и т.п. В подобных случаях злоумышленники пользуются невысоким уровнем знаний по информационной безопасности интернет-пользователей, которые, как правило, интересуются этими темами.
- Не обошли вниманием киберпреступники и всевозможные социальные сети, популярность которых сегодня стремительно растет.
- поиск легкого заработка в Интернете — почти каждая десятая полученная ссылка (9%) грозит заражением компьютера пользователя.

Негативные контентые материалы можно условно разделить на:

- **Незаконные**, к которым могут относиться: детская порнография (включая изготовление, распространение и хранение); наркотические средства (изготовление, продажа, пропаганда употребления), все материалы, имеющие отношение к расовой или религиозной ненависти (экстремизм, терроризм, национализма и др.), а также ненависти или агрессивного поведения по отношению к группе людей, отдельной личности или

животным), азартные игры и т.д.

Внутреннее законодательство каждой страны предусматривает различные виды наказания за распространение такой информации. В Российском законодательстве есть возможность в соответствии со статьями Уголовного кодекса РФ привлечь к административной и уголовной ответственности за распространение подобного негативного контента владельцев сайтов, а также авторов таких электронных текстов и видеопродукции.

- **Неэтичные**, противоречащие принятым в обществе нормам морали и социальным нормам.

Подобные материалы не попадают под действие уголовного кодекса, однако могут оказывать негативное влияние на психику столкнувшимися с ними человека, особенно ребенка. Примерами таких материалов могут служить широко распространенные в сети изображения сексуального характера, в том числе и порнография, агрессивные онлайн игры, азартные игры, пропаганда нездорового образа жизни (употребление наркотиков, алкоголя, табака, анорексии, булимии), принесения вреда здоровью и жизни (различных способов самоубийства, аудионаркотиков, курительных смесей), нецензурная брань, оскорбления, и др. Информация, относящаяся к категории неэтичной может быть также направлена на манипулирование сознанием и действиями различных групп людей.

- **Контентные риски** связаны с другими типами рисков Сети. Например, просмотр тех или иных видео-материалов может привести к заражению компьютера вирусами и потере важных данных. Очень многие распространители подобного негативного контента преследуют цель заразить компьютер, чтобы в дальнейшем иметь возможность манипулировать данными и действиями зараженного компьютера. Пропаганда негативных материалов также может идти через социальные сети, блоги, различные форумы. В данном случае контентные риски пересекаются с коммуникационными.

По данным исследования «Лаборатории Касперского», практически у половины детей в возрасте 4-6 лет уже есть собственный смартфон. Если вы собрались в ближайшее время покупать своему ребенку его первый гаджет или хотите знать больше о том, как сделать работу с устройством безопасной и комфортной, уделите время базовым настройкам смартфона. Для этого стоит учесть ряд особенностей самого устройства, а также возможности специализированного программного обеспечения.

1. Настройки доступа к телефону.

Установка пин-кода или функции TouchID (или FaceID) в самом начале работы со смартфоном позволит сохранить данные на телефоне (фотографии, видео, переписка в

мессенджерах и др.) в случае его потери. Расскажите своему ребёнку о выборе паролей для аккаунтов от различных сервисов. В этом вам поможет наша статья.

Отключите весь функционал, который доступен по отпечатку пальца (TouchID или FaceID), кроме разблокировки телефона, чтобы исключить возможные несогласованные покупки через смартфон или самостоятельную установку приложений. Найти эти функции можно в разделе Настройки — > TouchID (FaceID) и пин-код (для iOS) или Настройки — > Биометрия и безопасность (для Android).

2. Настройка экранного времени.

«Экранное время» — функция, позволяющая фиксировать временной промежуток, который ваш ребенок проводит за гаджетом. Настройка также показывает, какие приложения были задействованы. На основании этих данных программа формирует статистику за день и за неделю.

Найти функцию можно в Настройках –> Экранное время (для iOs) и Настройки -> Использование устройства (для Android).

Кроме того, есть возможность настроить время работы таким образом, что ребенок может «тратить» на социальные сети не больше 3 часов (количество часов можно выбрать произвольное) в день, а также отключить всплывающие уведомления в ночное время. При этом сохраняется возможность настроить исключения для приложений, которые будут вам необходимы.

Функция экранного времени помогает родителям контролировать время, проведенное за экраном смартфона, а детям – избежать переутомления от долгого «общения» с гаджетом.

3. Установка приложений и встроенные покупки.

В самом начале использования смартфона лучше сразу договориться о том, что вы ставите все приложения вместе со своим ребенком. Если вы не знаете, какой контент подходит вашему ребенку, выбирайте категорию для детей в AppStore или GooglePlay.

Приложения в этом разделе уже отобраны согласно интересам ребёнка и возрастным ограничениям.

Для того, чтобы скачать и установить приложение, в зависимости от операционной системы, используйте официальные магазины AppStore или Google Play. Старайтесь избегать установки приложений из ненадёжных источников, чтобы избежать попадания на ваш телефон вирусов и другого зловредного ПО.

Мы всегда можем определить, какое приложение устанавливаем, платное или бесплатное, но практически никогда не обращаем внимание на то, что даже бесплатное

приложение может содержать встроенные покупки. Речь идет о покупках внутри мобильных игр или о платных подписках на различные сервисы. Такая модель получает все большее распространение из-за того, что, с точки зрения коммерческой прибыли, она оказывается более выгодной для производителей программного обеспечения.

В настройках устройства ребёнка (Настройки -> Экранное время -> Контент и конфиденциальность) установите запрет на дополнительные покупки, в том числе опцию запрета на встроенные покупки. Это позволит вам избежать незапланированных расходов, а ребёнку – научиться планировать бюджет.

4. Семейный доступ.

Семейный доступ позволяет всем членам семьи совместно пользоваться приложениями, совершать покупки, создавать общие медиатеки (музыка, видео, книги, документы и др.). Добавлять пользователей может администратор группы, им может стать кто-то из родителей.

По количеству участников в вашей группе может быть для iOS (6 человек) и Android (5 человек). Настройки доступа к семейной группе практически не отличаются для разных операционных систем и не являются сложными, но при этом существенно помогают контролировать расходы и управлять подписками (например, музыка или видеофильмы).

Кроме базовых настроек смартфона, можно воспользоваться специальными приложениями для того, чтобы сделать взаимодействие ребёнка со смартфоном безопасным и удобным Такой программой является Kaspersky Safe Kids, с её помощью можно дополнить базовые настройки телефона, планшета или ноутбука, добавив к ним следующие возможности:

1. Удаленно контролировать использование устройства ребенком.

Доступ к управлению осуществляется через портал https://my.kaspersky.com

2. С помощью функционала Kaspersky Safe Kids вы можете:

- контролировать время работы устройства и установленных приложений;
- устанавливать ограничения по времени работы отдельно взятых приложений;
- смотреть, какие ресурсы часто посещает ваш ребенок.

3. Доступ к геопозиции. Вы всегда будете знать, где находится ваш ребенок.

В данном случае есть возможность включить «безопасный периметр»: функция, которая оповестит вас о том, что ребенок покинул безопасную зону (например, территорию школы или двора).

4. Получать информацию о группах социальной сети, о друзьях, которые к нему добавляются, и о людях, с которыми переписывается ваш ребёнок.

5. Получить консультации детского психолога.

6. Быть в курсе интересов ребёнка и использовать эти знания для выстраивания доверительных отношений с ребёнком.

Важно не только применять технические решения для безопасной работы вашего ребенка в сети Интернет, но и разговаривать с ним о том, что его интересует и что волнует. Любые установленные программы могут вам помочь оградить ребенка от нежелательного контента, и они будут более эффективными, если вы будете знать, как вести себя в разных ситуациях.

Тема 8: Пособия и обучающие программы по формированию навыков цифровой гигиены.

Мы привыкли решать свои задачи с помощью интернета: искать информацию, смотреть фильмы, играть, покупать нужные вещи. Это быстро и удобно, но не всегда безопасно. Мошенники в интернете охотятся за нашими данными, ресурсами и деньгами. Мы подготовили подборку ресурсов: пособий и обучающих программ по формированию навыков цифровой гигиены, которая будет полезна и родителям, и детям. Мы надеемся, что курс поможет юным пользователям интернета не попасться на удочку мошенников. Желаем безопасных путешествий в сети!

На сайте https://avidreaders.ru/book/cifrovaya-gigiena.html вы можете скачать книгу «Цифровая гигиена» В.Ф. Безмалого, которую можно читать сначала и до конца или с любого случайно открытого места. Читать самим, своим детям перед сном. Герои книги – принцессы и драконы, шпионы и контрразведчики, не оставят читателей равнодушными и оставят в памяти читателя и слушателя сценарии правильного поведения в кибер-среде и способы лёгкого и изящного обхода угроз.

В информационном разделе сети образовательных учреждений Ярославской области, посвященный безопасной работе в сети Интернет (https://www.edu.yar.ru/safety/poleznie_ssilki.html) размещены полезные ссылки на материалы для родителей и их детей, а имено:

Для родителей:

Берем защиту от кибербуллинга в свои руки

10 советов, которые помогут родителям вернуть контроль над ситуацией в случае кибертравли

Детская безопасность в интернете. Видеообращение эксперта лаборатории Касперского (длительность 4:34)

Почему нельзя общаться с незнакомцами, даже виртуальными? Как реагировать на спам? Что дети ищут в интернете? Расскажите своим детям о правилах поведения в сети.

15 правил безопасного поведения в интернете

Правила по безопасному поведению в интернете от экспертов по кибербезопасности корпорации Mail.Ru Group и портала «Учеба.ру»

помогут родителям, учителям и школьникам избежать различных опасностей виртуального пространства, которые окружают каждого современного ребенка и взрослого во Всемирной сети.

Настройки безопасности в Skype, Viber и WhatsApp.

Советы от Лаборатории Касперского.

Настройки безопасности в Facebook, Twitter, Tumblr и Pinterest.

Советы от Лаборатории Касперского.

Настройки безопасности в Youtube и Instagram.

Советы от Лаборатории Касперского.

Настройка семейной библиотеки в Google Play

Безопасность мобильного устройства Вашего ребенка

Как настроить родительский контроль в Google Play

Безопасность мобильного устройства Вашего ребенка

Настройка функции «Семейный доступ» в iTunes

Безопасность мобильного устройства Вашего ребенка

Как настроить родительский контроль в iTunes

Безопасность мобильного устройства Вашего ребенка

Для детей:

NEW

Информационные материалы Управления Роскомнадзора по Ярославской области

Письмо Управления Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Ярославской области от 27.05.2020 № 2809-06/76 «О направлении материалов в преддверии Дня защиты детей»

- Информационный буклет
- Памятка
- Тематическая игра

Детям до 10 лет:

Азбука информационной безопасности от Лаборатории Касперского

Лаборатория Касперского подготовила брошюру для учеников младших классов "Азбука информационной безопасности"

http://www.smeshariki.ru/parents#3

Советы от Смешариков: об осторожном поведении в интернет-игре

https://www.rubiring.ru/arkadiy-parovozov-somnitelnyie-saytyi/

Мультфильм "Аркадий Паровозов спешит на помощь – Сомнительные сайты"

https://kids.kaspersky.ru/category/entertainment/multfilmy/

Анимационный сериал о приключениях мальчика Севы и робота Каспера на просторах интернета.

http://krasatatiana.blogspot.com/2009/10/blog-post.html

Сказка о золотых правилах безопасности в Интернет.

http://www.wildwebwoods.org/popup.php?lang=ru

Интерактивная игра «Джунгли Интернета» предназначена для детей в возрасте от 7 до 10 лет и призвана научить не теряться при столкновении с угрожающим поведением других пользователей или с негативным содержанием сайтов.

http://www.spas-extreme.ru/themes/internet_bezopasnost

Интернет-безопасность на портале Спас-Экстрим

Детям от 11 до 14 лет

https://www.edu.yar.ru/azbuka/

Азбука цифрового мира

http://i-deti.org/comic/

Комиксы «Приключение Степы в Интернете».

http://i-deti.org/video/

Подборка обучающих и развивающих видеоматериалов, которые помогут получить представление о приемлемых моделях поведения в Интернете.

http://www.saferunet.ru/teenager/

Центр безопасного интернета в России: подросткам

https://stepik.org/course/191/

Онлайн-курс "Безопасность в Интернете" от Академии Яндекса для школьников 6-9 классов.

http://www.fcprc.ru/projects/cyberbullying

ФГБНУ «Центр защиты прав и интересов детей». Твой безопасный кибермаршрут Система консультативной помощи подросткам и родителям в области информационной безопасности в сети Интернет

Медиаграмотность

Часть 1. Как жить в медиамире. Учебное пособие разработано Донским государственным технологическим университетом, и направлено на формирование и развитие информационной грамотности обучающихся образовательных организаций.

Интернет: возможности, компетенции, безопасность. Часть 1. Теория

Интернет: возможности, компетенции, безопасность. Часть 2. Практикум

Детям от 15 до 18 лет:

https://www.edu.yar.ru/azbuka/

Азбука цифрового мира

Цифровая карта безопасности школьника

Проект, созданный учеником 11 класса из Ханты-Мансийского АО Тимуром Якшимбетовым при поддержке портала Проектория и компании Group-IB

http://персональныеданные.дети/

База материалов в виде правил, презентаций, тестов и игр, объясняющих важность сохранности личной информации при использовании цифровых технологий.

http://www.saferunet.ru/teenager/

Центр безопасного интернета в России: подросткам

http://www.fcprc.ru/projects/cyberbullying

ФГБНУ «Центр защиты прав и интересов детей».

Твой безопасный кибермаршрут. Система консультативной помощи подросткам и родителям в области информационной безопасности в сети Интернет

https://stepik.org/course/191/

Онлайн-курс "Безопасность в Интернете" от Академии Яндекса , на котором родители и дети 6-9 классов могут пройти обучение по курсу «Безопасность в интернете».

Также интересный материал по цифровой гигиене вы найдете на ресурах:

сетевичок.рф http://xn--b1afankxqj2c.xn--p1ai/ – Безопасный Интернет, интерактив, цифровой квест

http://ip-1.ru/geocode/ - проверка территории размещения сайта

http://www.minjust.ru/nko/fedspisok - Федеральный список экстремистских материалов

http://eais.rkn.gov.ru/ - ЕДИНЫЙ РЕЕСТР доменных имен, указателей страниц сайтов в сети "Интернет" и сетевых адресов, позволяющих идентифицировать сайты в сети "Интернет", содержащие информацию, распространение которой в Российской Федерации запрещено

http://kurgan.rt.ru/b2bgov/internet/internet_school - техподдержка ПАО «Ростелеком» на изменение настроек контент-фильтра

http://www.google.ru/intl/ru/safetycenter/families/start/ - Безопасный Интернет для детей

http://detionline.com/ - Дети России онлайн

http://www.internet-kontrol.ru/ - сайт для умных родителей

http://www.internet-kontrol.ru/stati/bezopasnost-detey-v-internete.html - Безопасность детей в интернете

http://mediagvardia.ru/ - «МедиаГвардия» - федеральный проект, целью которого является объединение усилий интернет-пользователей для совместного выявления интернет-сайтов, сообществ и групп в социальных сетях, специализирующихся на распространении противоправного контента

http://www.ligainternet.ru/ - Лига Безопасного Интернета

http://www.ligainternet.ru/encyclopedia-of-security/topic.php?SECTION_ID=12 - Лига Безопасного Интернета. Инфографика

http://www.ligainternet.ru/encyclopedia-of-security/parents-and-teachers/ - Лига Безопасного Интернета. Родителям и педагогам

http://www.ligainternet.ru/encyclopedia-of-security/parents-and-teachers/parents-and-teachers-detail.php?ID=3652 - Материалы к урокам безопасного интернета

http://ligainternet.ru/encyclopedia-of-security/parents-and-teachers/parents-and-teachers-detail.php?ID=639 - Как обеспечить безопасность детей в интернете

http://www.internet-kontrol.ru/stati/roditelskiy-kontrol-interneta-obschenie-bez-riska.html - Родительский контроль Интернета

http://www.saferinternet.ru/ - Безопасный Интернет. Портал Российского Оргкомитета по проведению Года Безопасного Интернета. Мероприятия, Интернет и законодательство, проблемы и решения, международные ресурсы.

http://www.saferunet.ru/ - Центр Безопасного Интернета в России. Сайт посвящен проблеме безопасной, корректной и комфортной работы в Интернете. Интернет-угрозы и эффективное противодействием им в отношении пользователей.

http://www.fid.su/ - Фонд развития Интернет. Информация о проектах, конкурсах, конференциях и др. по компьютерной безопасности и безопасности Интернета.

http://www.microsoft.com/Rus/athome/security/kids/etusivu.html - Безопасность в Интернете. "Основы безопасности детей и молодежи в Интернете" — интерактивный курс по Интерент-безопасности

http://www.symantec.com/ru/ru/norton/clubsymantec/library/article.jsp?aid=cs_teach_kids – Club Symantec единый источник сведений о безопасности в Интернете. Статья для родителей «Расскажите детям о безопасности в Интернете». Информация о средствах родительского контроля.

http://www.nachalka.com/bezopasnost - Nachalka.com предназначен для учителей, родителей, детей, имеющих отношение к начальной школе. Статья «Безопасность детей в Интернете». Советы учителям и родителям.

http://www.obzh.info/novosti/novoe/bezopasnost-detei-v-internete.html - Личная безопасность. Основы безопасности жизни. Рекомендации взрослым: как сделать посещение Интернета для детей полностью безопасным.

http://www.ifap.ru/library/book099.pdf - «Безопасность детей в Интернете», компания Microsoft. Информация для родителей: памятки, советы, рекомендации.

http://www.interneshka.net/children/index.phtml - «Интернешка» - детский онлайн-конкурс по безопасному использованию сети Интернет. Советы детям, педагогам и родителям, «полезные ссылки». Регистрация и участие в конкурсе по безопасному использованию сети Интернет.

http://www.oszone.net/6213/ - OS.zone.net - Компьютерный информационный портал. Статья для родителей «Обеспечение безопасности детей при работе в Интернет». Рекомендации по программе «Родительский контроль».

http://www.rgdb.ru/innocuous-internet - Российская государственная детская библиотека. Ресурс для детей и родителей. Правила безопасного Интернета. Обзор программных продуктов для безопасного Интернета. Как защититься от Интернет-угроз. Ссылки на электронные ресурсы, информирующие об опасностях и защите в Сети.