Какие опасности поджидают пользователя в сети Интернет.
Классификация рисков в сети Интернет
Контентные риски. Как их избежать.

Для полного понимания этого термина приведем определение понятия контент. Контент - это наполнение или содержание какого-либо информационного ресурса - текст, графика, музыка, видео, звуки и т.д. (например: контент интернет-сайта); мобильный контент - мультимедийное наполнение, адаптированное для использования в мобильных устройствах (телефоны, смартфоны, коммуникаторы и т.д.) - текст, графика, музыка, рингтоны, видео, игры, дополнительное программное обеспечение.

В данных рекомендациях дается информация о возможных рисках и опасностях в сети Интернет. Рекомендации для родителей по преодолению этих рисков приводятся в брошюре «Безопасность детей в Интернете», изданной Тамбовским областным институтом повышения квалификации работников образования и на сайте института по адресу http://ipk.68edu.ru/component/content/article/35-2010-05-26-09-10-15/1115-06-03-2012.html .

Информация нежелательного характера, которая несет в себе контентные *риски*, - это различные информационные ресурсы (тексты, картинки, аудио, видеофайлы, ссылки на сторонние ресурсы), содержащие противозаконную, неэтичную и вредоносную информацию.

К **противозаконной, неэтичной и вредоносной информации** относится:

- информация о насилии, жестокости и агрессии,
- информация, разжигающая расовую ненависть, нетерпимость по отношению к другим людям по национальным, социальным, групповым признакам,
- пропаганда суицида,
- пропаганда азартных игр,
- пропаганда и распространение наркотических веществ, отравляющих веществ,
- пропаганда анорексии (отказ от приема пищи) и булимии (чрезмерное потребление пищи),
- пропаганда деятельности различных сект, неформальных молодежных движений,
- эротика и порнография,
- нецензурная лексика и т.д.

В сети Интернет такую информацию можно встретить практически везде: в социальных сетях, блогах, торрентах, персональных сайтах, видеохостингах и др. Не являются исключением и мобильные сервисы.

Распространение **противозаконной** информации преследуется по закону, например, распространение наркотических веществ через Интернет, порнографических материалов с участием несовершеннолетних, призывы к разжиганию национальной розни и экстремистским действиям. Внутреннее законодательство каждой страны предусматривает различные виды

наказания за распространение противозаконной 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.

Неэтичный, противоречащий принятым в обществе нормам морали и социальным нормам, контент не запрещен к распространению, но может содержать информацию, способную оскорбить пользователей и оказать вредоносное воздействие. Подобная информация не попадает под действие уголовного кодекса, но может оказать негативное влияние на психику человека, особенно ребенка. Примерами таких материалов могут служить широко распространенные в сети изображения сексуального характера, 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.

Неэтичная и **вредоносная** информация может быть направлена на манипулирование сознанием и действиями различных групп людей. Это могут быть сайты, на которых люди обсуждают способы причинения себе боли или вреда, способы чрезмерного похудения, сайты, посвященные наркотикам, и даже сайты, на которых описываются способы самоубийства. Такая информация часто бывает заманчивой и может оказывать сильное психологическое давление на детей и подростков, которые не способны до конца осознать смысл происходящего и отказаться от просмотра и изучения сайтов с подобным содержимым. Влияние подобного рода информации на еще неокрепшую психику детей и подростков непредсказуемо; под впечатлением от таких сайтов дети могут пострадать не только в эмоциональном плане, но также прямой урон может быть нанесен и их физическому здоровью.

Вредоносныйконтент может привести к заражению компьютера вирусами и потере важных данных, например, просмотр тех или иных видео-материалов через сеть интернет приводит к заражению компьютера вирусами. Очень многие распространители подобного негативного контента преследуют цель заразить компьютер, чтобы в дальнейшем иметь возможность манипулировать данными и действиями зараженного компьютера, получить деньги незаконным способом. Такие действия могут преследоваться по закону в соответствии со статьями Уголовного кодекса РФ (ст. 272,273,274).

Что надо знать о проблемах недостоверной информации в Интернете?

В Интернете есть большая доля информации, которую никак нельзя назвать ни полезной, ни надежной, ни достоверной. Пользователи Сети должны мыслить критически, чтобы оценить достоверность, актуальность и полноту информационных материалов; поскольку абсолютно любой может

опубликовать информацию в Интернете. В Интернете не существует служб редакторов и корректоров (такие службы функционируют только в электронных средствах массовой информации), никто не проверяет информационные ресурсы на достоверность, корректность и полноту. Поэтому нельзя использовать Интернет как единственный источник информации, необходимо проверять информацию по другим источникам, особенно если эта информация касается жизненно важных моментов в жизни человека, например, здоровья, обучения, нормативно-правовых актов и т.п. .

Коммуникационные риски или риски общения в сети Интернет

Коммуникационные риски связаны с общением и межличностными отношениями Интернет-пользователей. Интернет - это не только средство массовой информации и всемирный справочник, но и среда для общения. В интернете существует много инструментов, позволяющих организовать места для общения – социальные сети, блоги, чаты, форумы, гостевые книги, списки рассылки и пр.

Примерами коммуникационных рисков могут быть: знакомства в сети и встречи с Интернет-знакомыми, интернет-хулиганство: преследование, запугивание и оскорбления (кибербуллинг), незаконные контакты, и др. С коммуникационными рисками можно столкнуться при общении в мобильных сервисах, чатах, онлайн-мессенджерах (ICQ, Skype, MSN и др.), социальных сетях, на сайтах знакомств, форумах, блогах и т.д.

Интернет-хулиганство, киберпреследование, киберзапугивание (кибербуллинг) – это явления не только виртуальной, но и реальной жизни.

Английское слово буллинг (bullying, от bully – драчун, задира, грубиян, насильник) обозначает запугивание, унижение, травлю, физический или психологический террор, направленный на то, чтобы вызвать у другого страх и тем самым подчинить его себе. Буллинг, осуществляемый в виртуальной среде с помощью Интернета и мобильного телефона, называют кибербуллингом. Кибербуллинг, преследование с использованием цифровых технологий, сильнее всего действует на детей и подростков.

Кибербуллинг не менее опасен, чем реальные издевательства. Если террор может закончиться, когда жертва вернется домой или пожалуется старшим, то кибербуллинг продолжается все время и от него невозможно спрятаться. В отличие от реальной травли, для кибер-буллинга не нужно быть здоровяком, достаточно компьютера, времени и желания кого-то терроризировать. Распространение кибербуллинга, во многом, отражает проблемы морали в обществе, где к человеку не относятся, как к ценности, личности и игнорируют его проблемы и переживания, отвечают цинизмом.

По данным, полученным в исследовании «Дети России онлайн», в среднем по РФ 23% детей, которые пользуются Интернетом, являются жертвой буллинга онлайн или офлайн. Если сравнить виртуальность и реальность, то российские дети подвергаются буллингу в Интернете так же часто, как и в реальной жизни. Оскорбления в чатах, на форумах, в блогах и в комментариях к ним, поддельные страницы или видеоролики, на которых над кем-то издеваются или даже избивают уже давно стали привычной частью

Рунета – каждый десятый ребенок 9-16 лет становился жертвой кибербуллинга.

Основной площадкой для кибербуллинга в последнее время являются социальные сети. В них можно оскорблять человека не только с помощью сообщений – нередки случаи, когда страницу жертвы взламывают (или создают поддельную на ее имя), где размещают лживый и унизительный контент. Особенно остро переживают кибербуллинг дети 9-10 лет: 52% детей этого возраста, ставшие жертвой подобной ситуации, в первую очередь девочки, указали, что были этим сильно или очень сильно расстроены. Кроме того, нередко и сами школьники выступают агрессорами. В России 25% детей признались, что за последний год обижали или оскорбляли других людей в реальной жизни или в Интернете. Обращает на себя внимание тот факт, что в России субъектов буллинга в два раза больше, чем в среднем по европейским странам.

Знакомства в Интернете и встречи с Интернет-незнакомцами

Общаясь в сети, дети могут знакомиться, общаться и добавлять в «друзья» совершенно неизвестных им в реальной жизни людей. В таких ситуациях есть опасность разглашения ребенком личной информации о себе и своей семье. Анонимность и приватность в сети - давно иллюзия. Каждое слово, каждая выложенная фотография, каждое действие в сети могут быть использованы против человека. "То, что попало в интернет, останется там навсегда, - напоминает Касперский (один из основателей, ведущий разработчик и крупнейший акционер ЗАО «Лаборатория Касперского»). -

Завтра наши дети могут сильно пожалеть о своем поведении и оставленных
следах в соцсетях. Это может негативно отразиться на их карьере, социальном статусе и вообще представляет собой благодатную почву для шантажа в будущем. Не говоря о том, что опубликованная информация может задеть и нас, родителей".

Также юный пользователь рискует подвергнуться оскорблениям, запугиванию и домогательствам. Особенно опасным может стать – установление дружеских отношений с ребенком с целью личной встречи (груминг), вступления с ним в сексуальные отношения, шантажа и эксплуатации. Такие знакомства чаще всего происходят в чате, на форуме или в социальной сети. Общаясь лично («в привате»), злоумышленник, чаще всего представляясь сверстником, входит в доверие к ребенку, а затем пытается узнать личную информацию (адрес, телефон и др.) и договориться о встрече. Иногда такие люди выманивают у детей информацию, которой потом могут шантажировать ребенка, например, просят прислать личные фотографии или провоцируют на непристойные действия перед веб-камерой.

Электронные риски

Электронные риски – это вероятность столкнуться с хищением персональной информации и/или подвергнуться атаке вредоносных программ.

Вредоносные программы – различное программное обеспечение

(вирусы, черви, «троянские кони», шпионские программы, боты и др.), которое может нанести вред компьютеру и нарушить конфиденциальность хранящейся в нем информации. Подобные программы чаще всего снижают скорость обмена данными с Интернетом, а также могут использовать ваш компьютер для распространения своих копий на другие компьютеры, рассылать от вашего имени спам с адреса электронной почты или профиля какой-либо социальной сети. Вредоносное программное обеспечение использует множество методов для распространения и проникновения в компьютеры, не только через внешние носители информации (компакт-диски, флешки и т.д.), но и через электронную почту посредством спама или скачанных из Интернета файлов.

Как узнать, что ваш компьютер заражен?

Учитывая, что вирусы обычно хорошо замаскированы внутри обычных файлов, непрофессионалу трудно их обнаружить. Несмотря на это, даже неопытный пользователь, как правило, замечает, что с компьютером происходит что-то неладное: он тормозит, появляются непонятные сообщения, а иногда он просто зависает и только перезагрузка может вывести его из этого состояния.

Существуют определенные признаки, по которым, с высокой степенью вероятности, можно утверждать, что компьютер заражен вирусами:
- медленная реакция на действия пользователя, особенно при запуске программ,
- искажение содержимого файлов и каталогов или их полное исчезновение,
- частые сбои и зависания компьютера,
- самопроизвольное появление на экране сообщений или изображений,
- несанкционированный запуск программ,
- зависание или странное поведение интернет-браузера,
- невозможность перегрузки компьютера (операционная система не загружается).

Однако нужно помнить, что ничто не может дать стопроцентной гарантии защиты вашего компьютера. Поэтому в любом случае Вы и

Ваши дети должны быть крайне внимательны, когда получаете сообщения по электронной почте от неизвестного адресата с вложением, когда скачиваете файлы из Интернета, пользуетесь чужими носителями информации или открываете файлы, скопированные с чужого компьютера.

Потребительские риски

Потребительские риски - злоупотребление в Интернете правами потребителя, включают в себя:
- хищение персональной информации с целью кибермошенничества,
- потеря денежных средств без приобретения товара или услуги,
- риск приобретения товара низкого качества, различные подделки, контрафактную и фальсифицированную продукцию,
- азартные игры на деньги.

Хищение личной информации

Кража личных данных или кибермошенничество – любой вид мошенничества, в результате которого происходит хищение личной информации, к примеру, паролей, имен пользователей, банковских данных, номеров кредитных карточек и т.д. Кража данных доступа к счету пользователей является наиболее распространенным видом мошенничества в Интернете. Хищение личных данных через Интернет иногда называется *фишингом*.

Многие интернет-аферы – это варианты мошеннических схем, существовавших еще до появления Сети, число которых увеличилось вместе с популярностью онлайн-шоппинга и других типов электронной коммерции.

Для обмана пользователей интернет-мошенники используют электронную
почту, чаты, форумы и фальшивые веб-сайты.

Виды кибермошенничества: вишинг, фишинг, фарминг, нигерийские письма и т.п (см. словарь терминов).

Вы можете самостоятельно научиться распознавать мошеннические сообщения, познакомившись с их некоторыми отличительными признаками. Фишинговые сообщения могут содержать:
- сведения, вызывающие тревогу, или угрозы, например, закрытия ваших банковских счетов;
- обещания большой денежной выгоды с минимальными усилиями или вовсе без них;
- сведения о сделках, которые слишком хороши, для того, чтобы быть правдой;
- запросы о пожертвованиях от лица благотворительных организаций после сообщений в новостях о стихийных бедствиях;
- грамматические и орфографические ошибки.

В условиях современной жизни, многие люди находят весьма удобным для себя не тратить время на походы по магазинам. Ведь при помощи Интернета можно заказать все необходимое с доставкой на дом за несколько минут. Пара щелчков мышкой, быстрое оформление заказа и вскоре товар уже в ваших руках. К сожалению, не все так легко и просто, как представляется на первый взгляд. Мошенники не дремлют даже в Интернете и доверчивый пользователь вполне может оказаться ни с чем, заплатив при этом немало денег. Потребительский риск заключается в потере денежных средств без приобретения товара или услуги, или приобретения товара низкого качества, контрафактной и фальсифицированной продукцию.

Азартные игры на деньги. Как уберечь детей от азартных игр.

Множество детей обожают искать развлечения (например, игры) в Интернете. Иногда при поиске нового игрового сайта они могут попасть на карточный сервер. Большинство игр и развлечений для несовершеннолетних вполне законны, однако, им нельзя играть в азартные игры на деньги.

В чем состоит отличие между игровыми сайтами и сайтами с азартными играми.

Разница между игровыми сайтами и сайтами с азартными играми состоит в том, что на игровых сайтах обычно содержатся настольные и словесные игры, аркады и головоломки с системой начисления очков. Здесь не тратятся деньги: ни настоящие, ни игровые. Сайты с играми на деньги обычно содержат игры, связанные с выигрышем или проигрышем настоящих денег.

Кроме этого, существует такие понятия как клиентские и браузерные игры, то есть игры через Интернет. Клиентские и браузерные игры бывают платные, бесплатные и условно-бесплатные. Условно-бесплатные - это такие игры, где можно играть бесплатно, но есть возможность что-либо улучшать (например, улучшить ваш персонаж или получить какие-либо игровые привилегии) за счет внесения реальных денег.

Существует еще одна опасность- зависимость от компьютерных игр. Это – проблема, которой было уделено довольно много внимания в прессе и различных научных работах. К примеру, ученые выяснили, что 30% игроков проводят за компьютером слишком много времени, а 10% находятся в сильной психологической зависимости от своей любимой игры. Заодно посмотрели, чем эта зависимость иногда кончается – а кончается она плохо, и потому нуждается как минимум в научном присмотре. Что же такое эта «компьютерная игровая зависимость» и в чем она проявляется?

Игровая зависимость являет собой форму сильной психологической привязанности к игре – в компьютерном варианте вплоть до желания жить в виртуальном мире. Возвращение в реальный мир связано исключительно с удовлетворением естественных потребностей, общение с живыми людьми сведено к минимуму. Особенно тяжелые формы игровой зависимости предполагают также крупные денежные траты на игру, злоупотребление кофе и энергетическими напитками, злость и раздражение при отрывании от игры, пренебрежение питанием и сном. Зависимость от игр сравнима с наркотиками и алкоголем, человек не может контролировать себя в плане времяпровождения за игрой, живет в своем собственном мире и не желает общаться с родными и друзьями – ибо они пока еще не «виртуальны». Любое время, проведенное вне игры, является для такого человека мучением.

Интернет-зависимость

Сегодня Всемирная паутина настолько тесно вплетена в нашу жизнь, что становится все трудней сказать, где заканчивается реальный мир и начинается виртуальный. С помощью Интернета можно делать все больше и больше. Но чрезмерное увлечение интернетом может привести к формированию болезненного пристрастия – зависимости. Как следствие – серьезные проблемы с учебой, работой, в отношениях с близкими людьми, вплоть до разрушения связей с родными и окружающим миром. Особую тревогу вызывает тот факт, что зависимости чаще всего подвергаются дети в подростковом возрасте. То, что дети проводят в Интернете слишком много времени, огорчает большинство родителей. Сначала взрослые приветствовали появление Сети, полагая, что она – безграничный источник новых знаний. Вскоре выяснилось, что подростки не столько

пользуются Интернетом для выполнения домашних заданий или поиска полезной информации, сколько общаются в чатах и играют в он-лайновые игры.

Поддержание в жизни детей разумного равновесия между развлечениями и другими занятиями всегда было испытанием для родителей; Интернет сделал это еще более трудной задачей. Общение в Интернете и интерактивные игры могут настолько затягивать детей, что они часто теряют ощущение времени, появляется интернет-зависимость. Обратите внимание на психологические особенности вашего ребенка.

Социально дезадаптированные дети имеют повышенную вероятность к приобретению Интернет-зависимости. Причина в том, что Интернет позволяет оставаться анонимным, не бояться осуждения (если что-то сделал неправильно, всегда можно поменять имя и начать все заново), предоставляет гораздо более широкий выбор возможностей к общению, чем реальный мир.

В Интернете ребенку гораздо легче выстроить свой виртуальный мир, пребывание в котором ему будет комфортным. Поэтому, если у ребенка что-то не получается в реальном мире, он будет стремиться к пребыванию там, где ему комфортно. С другой стороны, Интернет может помочь застенчивому ребенку стать более общительным, найти ту среду общения, которая более полно соответствует его уровню развития, и в результате повысить его самооценку. Если ваш ребенок в жизни замкнут, застенчив или склонен к унынию, вам необходимо внимательно следить за его отношением к Интернету, с тем чтобы предотвратить его превращение из средства раскрытия личности ребенка в плохо контролируемую страсть.

Интернет-зависимость – навязчивое желание войти в Интернет, находясь офлайн и неспособность выйти из Интернета, будучи онлайн. (Гриффит В., 1996). По своим проявлениям она схожа с уже известными формами аддиктивного поведения (например, в результате употребления алкоголя или наркотиков), но относится к типу нехимических зависимостей, то есть не приводящих непосредственно к разрушению организма. По своим симптомам Интернет-зависимость ближе к зависимости от азартных игр; для этого состояния характерны следующие признаки: потеря ощущения времени,
невозможность остановиться, отрыв от реальности, эйфория при нахождении за компьютером, досада и раздражение при невозможности выйти в Интернет.

В случае Интернет-зависимости выделяют следующие типы онлайн-активности:
- навязчивый веб-серфинг – бесконечные путешествия по всемирной паутине, поиск информации,
- пристрастие к виртуальному общению и виртуальным знакомствам (большие объемы переписки, постоянное участие в чатах, веб-форумах, избыточность знакомых и друзей в сети),
- игровая зависимость – навязчивое увлечение компьютерными

играми по сети,
- навязчивое желание потратить деньги – игра по сети в азартные игры, ненужные покупки в Интернет-магазинах или постоянное участие в интернет-аукционах,
- пристрастие к просмотру фильмов через Интернет.

При необходимости у родителей должна быть возможность для обращения к школьному психологу. Школьный психолог должен быть знаком с проблемами Интернет-зависимости и может дать необходимые рекомендации родителям.

Социальные сети: некоторые аспекты безопасности

Социальные сети, такие как Одноклассники, Вконтакте, MySpace, Facebook, Twitter и многие другие позволяют людям общаться друг с другом и обмениваться различными данными, например, фотографиями, видео и сообщениями. По мере роста популярности таких сайтов растут и риски, связанные с их использованием. Хакеры, спамеры, разработчики вирусов, похитители личных данных и другие мошенники не дремлют.

Одна из ключевых проблем социальных сетей - открытось большинства учетных записей. В частности, по различным оценкам, порядка 500 миллионов пользователей социальных сетей по всему миру держат свою частную информацию в открытом доступе, а эта информация может собираться с помощью автоматизированных решений. К примеру, подобный функционал может быть встроен во всевозможные приложения, которыми славится один из самых популярных подобных сервисов Facebook.

Анонимность и приватность в сети - давно иллюзия. Каждое слово, каждая выложенная фотография, каждое действие в сети могут быть использованы против человека. "То, что попало в интернет, останется там навсегда, - напоминает Касперский (один из основателей, ведущий разработчик и крупнейший акционер ЗАО «Лаборатория Касперского»). - Завтра наши дети могут сильно пожалеть о своем поведении и оставленных следах в соцсетях.

Это может негативно отразиться на их карьере, социальном статусе и вообще представляет собой благодатную почву для шантажа в будущем. Не говоря о том, что опубликованная информация может задеть и нас, родителей".

Кроме того, пользователи социальных сетей регулярно становятся жертвами спама - на данный момент порядка 57% учетных записей в рамках подобных сервисов получают спам, а это 76-процентный рост по сравнению с показателем 2009 года. Ни для кого не секрет, что в социальных сетях хранится много нежелательной информации: экстремистской информации, призывы к разжиганию национальной ненависти, порнография и т.п..

Существует еще одна опасность - социальные сети становятся неизлечимой зависимостью. Люди перестают общаться в реальной жизни, превращаясь в зомби.

Информационные ресурсы

1. http://www.nachalka.com/bezopasnost
2. http://detionline.com/helpline/rules/parents Дети России онлайн
3. http://www.ifap.ru/library/book099.pdf - «Безопасность детей в интернете», брошюра от microsoft
4. http://www.fid.su/projects/journal/ - фонд развития Интернет
5. http://stopfraud.megafon.ru/parents/ - безопасный интернет от Мегафона
6. http://www.mts.ru/help/useful_data/safety/ -безопасный Интернет от МТС
7. http://safe.beeline.ru/index.wbp - безопасный Интернет от Билайн
8. http://www.saferunet.ru/ - Центр безопасного Интернета в России, горячая линия по безопасному Интернету.
9. http://www.microsoft.com/ru-ru/security/default.aspx - безопасный интернет от microsoft
10. http://www.mvd.ru/userfiles/broshyura_k_01_02_2012.pdf - брошюра МВД России «Безопасный интернет»

Список терминов

Блог (англ. **blog**, от weblog — интернет-журнал событий, интернет-дневник, онлайн-дневник) — веб-сайт, основное содержимое которого — регулярно добавляемые записи (посты), содержащие текст, изображения или мультимедиа.

- ь, (от англ. *Webbrowser)* - программное обеспечение для просмотра веб-сайтов, то есть для запроса веб-страниц (преимущественно из Сети), их обработки, вывода и перехода от одной страницы к другой.

— сайт, позволяющий загружать и просматривать **видео** в браузере, например через специальный проигрыватель.

Вишинг - разновидность фишинга - распространенным сетевым мошенничеством, когда клиенты какой-либо платежной системы получают сообщения по электронной почте якобы от администрации или службы безопасности данной системы с просьбой указать свои счета, пароли и т.п. При этом ссылка в сообщении ведет на поддельный сайт, на котором и происходит кража информации. Сайт этот уничтожается через некоторое время, и отследить его создателей в Интернете достаточно сложно.

Интернет-мошенничество или кибермошенничество – это один из видов киберпреступления, целью которого является обман пользователей.

Кибербуллинг(cyber-bullying) - это виртуальный террор, чаще всего подростковый.

Контент - (от английского content - содержание) – это абсолютно любое информационно значимое, содержательное наполнение информационного ресурса или веб-сайта. Контентом называются тексты, мультимедиа, графика.

Социальная сеть (от англ. **social**networkingservice) — платформа, онлайн сервис или веб-сайт, предназначенные для построения, отражения и организации **социальных** взаимоотношений.

Фарминг(англ. *pharming*) — это процедура скрытного перенаправления жертвы на ложный IP-адрес. Для этого может использоваться навигационная структура (файл hosts, система доменных имен (DNS)).

Фишинг(от англ. phishing, от password — пароль и fishing — рыбная ловля, выуживание) – это вид интернет-мошенничества, основанный на незнании пользователями норм сетевой безопасности, целью которого является получение доступа к конфиденциальным данным - логинам и паролям.

Фишинг-атаки проводятся через электронную почту, всплывающие сообщения и ссылки на фишинговые веб-сайты, с целью обманным путем выявить у получателя личную информацию, часто финансового характера.

— распространѐнный вид мошенничества, получивший наибольшее развитие с появлением массовых рассылок по электронной почте (спама).