Безопасность в Интернете

Автор презентации:
Спиридонова Е.В.,
учитель информатики и ИКТ
МОУ-СОШ №6 г.
Петровска - Забайкальского

ПРАВИЛА ЗАЩИТЫ КОМПЬЮТЕРА

- Постоянно обновляйте все программное обеспечение (включая веб-браузер), используя Центр обновления Microsoft.
- Установите законное антивирусное и антишпионское программное обеспечение, такое как Microsoft Security Essentials (Microsoft Security Essentials).
- Брандмауэр должен быть всегда включен.
- Установите на беспроводном маршрутизаторе защиту с помощью пароля.
- Не вставляйте неизвестные флеш-накопители (или USB-накопители) в свой компьютер. Если на них имеется вирус, этот вирус может заразить ваш компьютер.
- Прежде чем открывать вложение или переходить по ссылке, приведенной в сообщении электронной почты, мгновенном сообщении или в социальной сети, убедитесь, что отправитель действительно отправлял сообщение.
- Не переходите по ссылкам и не нажимайте кнопки во всплывающих сообщениях, которые кажутся подозрительными.

ОБЕСПЕЧЬТЕ ЗАЩИТУ СЕКРЕТНОЙ ЛИЧНОЙ ИНФОРМАЦИИ

- Прежде чем вводить секретные сведения в веб-форме или на веб-странице, обратите внимание на наличие таких признаков, как адрес веб-страницы, начинающийся с префикса **https** и значка в виде закрытого замка () рядом с адресной строкой, который обозначает безопасное соединение.
- Никогда не предоставляйте секретные сведения (такие как номер счета или пароль) в ответе на сообщение электронной почты, мгновенное сообщение или социальной сети.
- Никогда не отвечайте на просьбы прислать деньги от «членов семьи», на предложения о сделке, которые слишком хороши, чтобы быть правдой, на сообщения о розыгрышах лотереи, в которых вы не участвовали, или другие мошеннические сообщения.

ИСПОЛЬЗУЙТЕ НАДЕЖНЫЕ ПАРОЛИ И ХРАНИТЕ ИХ В СЕКРЕТЕ.

Не создавайте пароли с использованием:

- Слов из словаря на любом языке.
- Слов, написанных в обратном порядке, с распространенными ошибками или аббревиатур.
- Последовательности повторяющихся символов. Например: 12345678, 222222, abcdefg или смежных символов на клавиатуре (qwerty).
- Личной информации. Ваше имя, день рождения, номер водительских прав, номер паспорта и тому подобные данные.

ОСНОВЫ СЕТЕВОЙ БЕЗОПАСНОСТИ

1. Проявляйте осторожность при переходе по ссылкам, которые вы получаете в сообщениях от других пользователей или друзей.
2. Контролируйте информацию о себе, которую вы размещаете.
3. Не думайте, что сообщение, которое вы получили, было отправлено тем, кого вы знаете, только потому, что так написано.
4. Чтобы не раскрыть адреса электронной почты своих друзей, не разрешайте социальным сетям сканировать адресную книгу вашего ящика электронной почты.
5. Вводите адрес социальной сети непосредственно в адресной строке браузера или используйте закладки.
6. Не добавляйте в друзья в социальных сетях всех подряд.
7. Не регистрируйтесь во всех социальных сетях без разбора.
8. Учитывайте тот факт, что все данные, опубликованные вами в социальной сети, могут быть кем-то сохранены
9. Проявляйте осторожность при установке приложений или дополнений для социальных сетей.
10. Старайтесь не посещать социальные сети с рабочего места.
11. Расскажите вашим детям об опасностях, которые могут подстерегать их в социальных сетях.

УГРОЗА - ФИШИНГОВЫЕ СООБЩЕНИЯ ЭЛЕКТРОННОЙ ПОЧТЫ.

Создаются с целью похищения личных данных. В них запрашиваются

личные данные или указывается ссылка на веб-сайты или номера

телефона, по которым следует позвонить, где просят указать личные

данные. Несколько советов помогут распознать мошеннические

сообщения электронной почты или ссылки внутри них.

В сообщениях может быть просьба позвонить по телефону. Фишинговые схемы мошенничества направлены на то, чтобы заставить позвонить по определенному номеру телефона, где отвечающий абонент или автоответчик ждет, пока вы не сообщите номер счета, PIN-код, пароль или другие ценные личные данные. Они также могут содержать ссылки на обманные веб-сайты, где просят ввести личную информацию.

ТРО́ЛЛИНГ

- — форма социальной провокации или издевательства в сетевом общении — форма социальной провокации или издевательства в сетевом общении, использующаяся как персонифицированными участниками, заинтересованными в большей узнаваемости, публичности, эпатаже — форма социальной провокации или издевательства в сетевом общении, использующаяся как персонифицированными участниками, заинтересованными в большей узнаваемости, публичности, эпатаже, так и анонимными пользователями без возможности их идентификации[3].
- Прямую аналогию из обычной жизни

Изображение trollface, созданное в 2008 году художником Whynne с сайта DeviantArtИзображение trollface, созданное в 2008 году художником Whynne с сайта DeviantArt для веб-комикса[1], часто

СРЕДА ТРОЛЛИНГА

- Основными местами осуществления троллинга могут выступать различные тематические форумыОсновными местами осуществления троллинга могут выступать различные тематические форумы, конференцииОсновными местами осуществления троллинга могут выступать различные тематические форумы, конференции, социальные сетиОсновными местами осуществления троллинга могут выступать различные тематические форумы, конференции, социальные сети, порталыОсновными местами осуществления троллинга могут выступать различные тематические форумы, конференции, социальные сети, порталы, чатыОсновными местами осуществления троллинга могут выступать различные тематические форумы, конференции, социальные сети, порталы, чаты и новостные сайты. Особенности конструкции подобных виртуальных пространств, как правило, обеспечивают возможность создания индивидами виртуального альтер эго, формируемого исключительно по собственному усмотрению такого создателя. Почти в любом виртуальном сообществе, которое создано для коммуникации пользователей, существуют специальные поля для формирования своих данных, где участники вписывают свои основные характеристики и дополнительные данные о сфере

ХАРАКТЕР ВОЗДЕЙСТВИЯ ТРОЛЛИНГА НА ВИРТУАЛЬНЫЕ ПРОСТРАНСТВА

Тролль пытается представить себя типичным пользователем, который разделяет общие интересы и проблемы группы либо сообщества. В это время, если другие участники конференции осведомлены о троллинге и подобных ему фальсификациях личности, они пытаются и выявить тролль-публикации среди настоящих постов и, при установлении таковых, заставить злоумышленника покинуть пределы группы или перестать троллить. Успех такого поиска зависит от умения распознавать намёки, определяющие цели автора постов. Успех определения таких намёков зависит от того, насколько удовольствие тролля от осуществления данного занятия погашено под влиянием группы и пожертвовано самим троллем в пользу усилий на сохранение права дальнейшего участия и/или троллинга.

- Тролли могут нанести существенный вред коммуникации во многих направлениях: испортить обсуждение, распространить вредный совет либо деструктивную идею, разрушить чувство взаимного доверия в сообществе. В группах, приобретших чувствительность к троллингу при общем высоком уровне фальсификаций в их пространстве, — множество вопросов, не содержащих реального троллинга и являющихся не более чем наивными по содержанию, может быть незамедлительно отвергнуто как троллинг.

КИБЕРБУЛЛИНГ

- - это травля, оскорбления или угрозы, высказываемые жертве с помощью средств электронной коммуникации, в частности, сообщений в социальных сетях, мгновенных сообщений, электронных писем и СМС. С каждый годом стремительно увеличивается количество трагедий, к которым приводит **кибербуллинг**.

КАК ВОЗНИКАЕТ КИБЕРБУЛЛИНГ?

- Кибербуллинг или онлайн-травля своими корнями уходит в те же темные области человеческой психологии, как и в случае с обычной травлей, которую агрессор выбирает в качестве средства распространения своего влияния или власти посредством оскорбления жертвы (в особенности, если она заведомо слабее и не может ответить), повышая тем самым свой социальной статус. Чаще всего кибербуллеры публикуют свои оскорбления анонимно, скрываясь за выдуманным именем, но могут выступать и под своим собственным именем, часто в том случае, если жертва заведомо слабее и не представляет угрозы для агрессора. Большинство кибербуллеров способны высказываться только в онлайн пространстве, в реальной жизни у них не найдется смелости произнести подобное в лицо жертве.

КАК РАСПОЗНАТЬ КИБЕРБУЛЛИНГ?

- Любое унизительное, оскорбительное или угрожающее сообщение, отправленное в электронной форме, является кибербуллингом. К этому же относятся унизительные фотографии или видео, опубликованные в социальных сетях Facebook или YouTube без согласия жертвы. Поддельные профили в социальных сетях или веб-сайты, созданные с целью опорочить жертву, также относятся к категории кибербуллинга. В то время, как инструменты и тактики, используемые кибербуллерами, очевидны на первый взгляд, наибольшую трудность в борьбе с кибербуллингом представляет признание пристыженных или испуганных жертв, что они являются жертвами кибербуллеров.

КАК ОСТАНОВИТЬ КИБЕРБУЛЛИНГ?

- К сожалению, кибербуллинг представляется настолько же неискоренимым, как и сама подлость некоторых людей. Ничуть не меньшее затруднение представляет собой попытка пресечь публикацию агрессором порочащей жертву информации, будь то посредством поста в социальной сети, веб-сайта или видео, так как для того, чтобы администратор ресурса удалил данное содержимое, необходимо пройти неимоверно сложную процедуру. Даже в случае, если это сделать удастся, вероятнее всего уже существуют копии опубликованных материалов, что делает практически невозможным их полное и безвозвратное удаление из сети.

Как мы можем помочь в предупреждении кибербуллинга?

- Заблокировать учетные записи агрессоров, которые они используют для распространения своей ненависти
- Сообщать о фактах кибербуллинга провайдерам услуг, как Facebook или Twitter
- Обеспечить защитой ваши пароли, в т. ч. используемые на мобильных устройствах

ОБЕСПЕЧЬТЕ ЗАЩИТУ ОТ КИБЕРБУЛЛИНГА

- Абсолютно каждый владелец смартфона или планшета, использующий Twitter, WhatsApp, Snapchat, Facebook, YouTube или любой другой социальной сети может стать мишенью кибербуллинга. Разумеется, отказ от использования социальных сетей был бы наиболее эффективным способом защиты от кибербуллинга, однако это крайняя мера. Гораздо лучше поддерживать открытий диалог с окружающими вас людьми, побуждая их обращаться за помощью в случае, если они станут жертвами травли онлайн. Помните, что кибербуллеры редко фокусируют внимание на своих жертвах продолжительное время - травля не продлится долго. Содержите в безопасности свои учетные записи с помощью решения Avast Пароли.

КАК ВЫГЛЯДИТ ФИШИНГОВОЕ СООБЩЕНИЕ ЭЛЕКТРОННОЙ ПОЧТЫ?

- Как **сообщения от контактов из вашей адресной книги** электронной почты, причём они могут содержать убедительные данные из личной истории, которые мошенники нашли на ваших страницах в социальных сетях.
- Как **сообщения от банковских или финансовых учреждений, сайтов социальных сетей, компаний, с которыми вы регулярно работаете** (например Mikrosoft) . Эти сообщения могут содержать логотипы, похожие на официальные, а также другие идентификационные данные, взятые непосредственно с законных веб-сайтов. Они могут содержать угрозы закрытия счета, а также поддельные ссылки, созданные для того, чтобы заставить вас ввести данные счета. Чтобы эти фишинговые сообщения выглядели еще более правдоподобными, мошенники используют графику, которая обычно ссылается на законные веб-сайты, однако на самом деле она ссылается на сайт мошенников или всплывающее окно, которое выглядит точно так же, как на официальном сайте.

ФРАЗЫ, КОТОРЫЕ ЧАСТО ВСТРЕЧАЮТСЯ В ФИШИНГОВЫХ СООБЩЕНИЯХ ЭЛЕКТРОННОЙ ПОЧТЫ:

- **"Проверьте свою учетную запись".** Предприятия не должны просить вас отправить пароли, данные для входа или имена пользователей, номера социального страхования и другую личную информацию по электронной почте. Если вы получите по электронной почте сообщение от корпорации Майкрософот или другой компании просьбой обновить данные своей кредитной карты, не отвечайте – это фишинговое сообщение.

ФРАЗЫ, КОТОРЫЕ ЧАСТО ВСТРЕЧАЮТСЯ В ФИШИНГОВЫХ СООБЩЕНИЯХ ЭЛЕКТРОННОЙ ПОЧТЫ:

- **"Вы выиграли в лотерею".** Мошенническая схема с лотереей называется мошенничеством с авансовыми платежами. Одной из наиболее распространенных форм мошенничества с авансовыми платежами является сообщение, в котором утверждается, что вы выиграли большую сумму денег или что какое-то лицо выплатит вам большую сумму денег безвозмездно или при условии небольшой услуги с вашей стороны. Мошеннические схемы с лотереей часто содержат ссылки на крупные компании, такие как Майкрософт. Лотереи Майкрософт не существует!
- **"Если вы не ответите в течение 48 часов, ваш счет будет закрыт".** Такие сообщения создают ощущение срочности, что вам следует отвечать мгновенно, не раздумывая. В фишинговом сообщении электронной почты может даже утверждаться, что ваш ответ требуется потому, что ваш счет уже подвергся опасности.

Что представляет собой фишинговая ссылка?

- Иногда фишинговые сообщения электронной почты содержат ссылки на фиктивные веб-сайты.
- Сообщения в формате HTML могут содержать ссылки или формы, которые можно заполнить точно так же, как вы это делаете на законном веб-сайте.
- Фишинговые ссылки, по которым вас заставляют перейти в сообщениях электронной почты, на веб-сайтах или даже в мгновенных сообщениях, могут содержать полное или частичное название реальной компании и обычно замаскированы, то есть отображаемая ссылка введет не на предполагаемый адрес, а на какой-то другой, как правило, незаконный веб-сайт.
- Обратите внимание, что в следующем примере при подведении (без щелчка) указателя мыши к ссылке отображается реальный веб-адрес в поле на желтом фоне

ЧТО ПРЕДСТАВЛЯЕТ СОБОЙ ФИШИНГОВАЯ ССЫЛКА?

Киберпреступники используют веб-адреса, которые напоминают названия известных компаний, но слегка изменяют его, добавляя, опуская или перенося буквы. Например, адрес **"www.microsoft.com"** может отображаться в виде:

www.micosoft.com

www.mircosoft.com

www.verify-microsoft.com

Это называется "тайпсквоттингом" или "кибersквоттингом".

КАК МОЖНО СНИЗИТЬ РИСК СТАТЬ ЖЕРТВОЙ?

- Никогда не загружать фотографии из неизвестного источника. Они могут иметь сексуально откровенный характер.
- Использовать фильтры электронной почты..
- Немедленно прекращать работу в Интернете, если во время неё произойдет что-то, что вызывает неудобство или страх.
- Выбрать нейтральное имя, которое не содержит указания на пол и не раскрывает личную информацию.
- Никогда не разглашать личную информацию о себе (включая возраст и пол), а также информацию о своей семью, никогда не заполнять личные анкеты в Интернете.
- Немедленно прекращать любое общение по электронной почте, с использованием мгновенных сообщений или чатов, если кто-то пытается задавать вопросы, являющиеся очень личными или имеющие сексуальную направленность.

Что делать, если вы стали жертвой мошенников?

- немедленно обратитесь в свою кредитную компанию, банк, а также в полицию.
- Закройте все счета, которые подвергались фальсификации.
- Поменяйте пароли для всех своих учетных записей в Интернете.
- Ведите журнал всех выполняемых действий.
- Сохраните все документы, включая адреса электронной почты, адреса веб-сайтов и журналы разговоров по сети, чтобы предоставить их полиции.

10 ПРАВИЛ ИНТЕРНЕТ-БЕЗОПАСНОСТИ ДЛЯ ДЕТЕЙ

ДЕТИ ДОЛЖНЫ:
1. Никогда не показывать личную информацию в Интернете, такую, как адрес, номер телефона, имя, расположение школы, имена родителей. Веб-сайты или другие онлайн-сервисы могут попросить детей дать информацию для того, чтобы участвовать в конкурсах или получить бесплатные подарки. Некоторые веб-сайты не позволяют доступа, если пользователь не дает им личной информации. Однако, как только личная информация дана, важно, чтобы ваши дети понимали, что их конфиденциальность может быть нарушена. Их имена могут в конечном итоге пойти на продажу в базе данных, или еще хуже, эта информация может быть использована для причинения вреда или их эксплуатации.
2. Будьте осторожны при разработке веб-сайта. Сейчас многие дети имеют свои личные веб-сайты. Дети должны знать, что никогда не следует оставлять домашний адрес, номер телефона или личную фотографию на сайте. Если дети хотят получать информацию от посетителей своего сайта, которые хотят связаться с ними, они могут размещать адреса электронной почты. Тем не менее, дети должны знать, что на адрес электронной почты они могут получать нежелательные письма. Они должны быть очень осторожными при открытии любой электронной почты от неизвестных адресов. Если дети получают сообщения, которые являются угрожающими или сексуальными, они должны немедленно сообщить своим родителям.

3. Всегда информировать своих родителей, когда они сталкиваются с чем-нибудь в Интернете, что заставляет чувствовать их себя неловко.

4. Никогда, ни при каких обстоятельствах не соглашаться встретиться лицом к лицу с виртуальным знакомым с кем переписывались в Интернете без разрешения родителей. Если всё-таки встреча состоится, - она должна быть в общественном месте и родители должны всегда сопровождать ребенка.

5. Избегать чатов, которые обсуждают секс или религиозные культы. Хотя эти вопросы могут показаться интересными сначала, они могут предоставлять опасность для ребёнка. Многие культы и секты охотятся на подростков в сети

6. Не доверять любому, кого они встречают в чатах , и кто пытается повернуть их против своей семьи, друзей, учителей или религии.

7. Выбрать гендерно-нейтральное (скрывающее пол) онлайн имя в чате, чтобы избежать преследований.

- 8. Никогда не отвечать на сообщения или объявления, которые являются сексуально непристойными, угрожающими, или заставляющими себя чувствовать неловко в любом случае.
  9. Никогда не отправлять личные материалы для онлайн-друзей, такие, как адрес, номер телефона или фотографии, без предварительного информирования родителей.
  10. Всегда напоминайте детям, что люди, которых они встречаются в Интернете могут могут быть не теми, кем они кажутся.

  Автор: Д-Р ЛИ БЕЙКЕР 16 АПРЕЛЯ 2011 В 3:18 УТРА
  Источник: http://www.ivillage.com/

Источники

- http://www.microsoft.com
- http://www.ivillage.com/
- https://www.avast.ru/c-cyberbullying
- https://ru.wikipedia.org/wiki/%D0%A2%D1%80%D0%BE%D0%BB%D0%BB%D0%B8%D0%BD%D0%B3