Безопасность в Интернете

Лекция для старшеклассников и их родителей

Автор презентации:

Соверткова Ю.В., учитель МБОУ «СОШ №18» г. Нижневартовска

Защитите свой компьютер

- Постоянно обновляйте все программное обеспечение (включая веб-браузер), используя Центр обновления Microsoft.
- Установите законное антивирусное и антишпионское программное обеспечение, такое как 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.

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.
- **"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.

Источник

- http://www.microsoft.com