Безопасность в Интернете

Защитите свой компьютер

- Постоянно обновляйте все программное обеспечение
- Установите законное антивирусное программное обеспечение
- 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
- 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. Не добавляйте в друзья в социальных сетях всех подряд.
5. Не регистрируйтесь во всех социальных сетях без разбора.
6. Учитывайте тот факт, что все данные, опубликованные вами в социальной сети, могут быть кем-то сохранены.

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

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 можно снизить риск стать жертвой?

- Никогда не загружать фотографии из неизвестного источника. О
- 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 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.

http://www.youtube.com/watch?v=o3cl996Jf84