ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СЕТИ ИНТЕРНЕТ

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Безопасность – отсутствие угроз, либо состояние защищенности от угроз.

Информация – сведения или сообщения.

Угроза информационной безопасности — совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства в информационной сфере.

МОШЕННИЧЕСТВО В ИНТЕРНЕТЕ

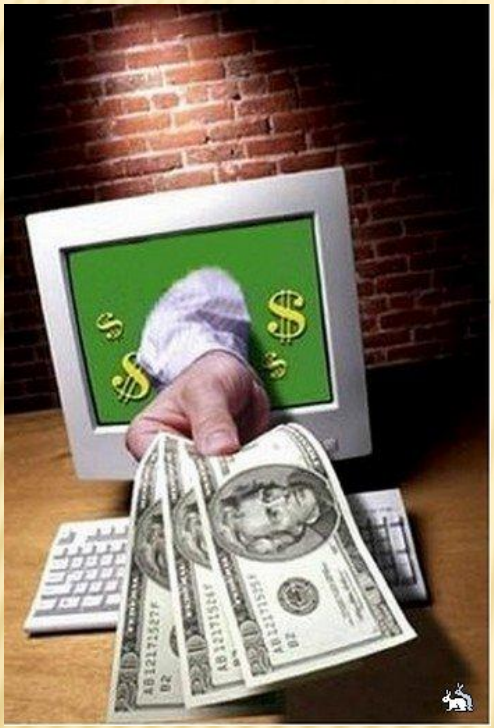
В отличие от таких интернет-угроз, как вирусы, троянские программы, программы-шпионы, SMS-блокеры, спам и т.д., мошенничество примечательно вот чем: мишень злоумышленника — не компьютер, защиту которого надо обойти, а человек, у которого, как известно, свои слабости. Поэтому, с одной стороны, ни одна программа не обезопасит пользователя полностью, а с другой — он в значительной мере отвечает за свою безопасность сам.

СПРАВОЧНАЯ ИНФОРМАЦИЯ

По последним данным, в России:
средний возраст начала самостоятельной работы в Сети - 10 лет (в 2009 году - 11 лет); и сегодня наблюдается тенденция к снижению возраста до 9 лет;

30% несовершеннолетних проводят в Сети более 3 часов в день (при норме 2 часа в неделю!)

ВИДЫ МОШЕННИЧЕСТВА



ФИШИНГ

Фишинг (от англ. fishing - рыбная ловля, выуживание) - вид интернет-мошенничества, цель которого - получить данные, содержащиеся на вашей пластиковой карте.

Злоумышленники рассылают электронные письма от имени банков или платежных систем. Пользователю предлагается зайти на сайт, который является точной копией настоящего сайта банка, где можно увидеть объявления, например, об изменении системы безопасности банка. Для дальнейшей возможности использовать свою пластиковую карту вас просят указать пин-код и данные, содержащиеся на карте. Оставив свои данные, вы фактически преподносите мошенникам деньги на блюдечке.

ИНТЕРНЕТ – ПОПРОШАЙНИЧЕСТВО

В Интернете могут появиться объявления от благотворительной организации, детского дома, приюта с просьбой о материальной помощи больным детям. Злоумышленники создают сайт-дублер, который является точной копией настоящего, меняют реквизиты для перечисления денег.

Для того, чтобы не попасться на крючок и не отдать свои деньги в руки мошенников, не поленитесь перезвонить в указанную организацию, уточнить номер расчетного счета либо посетить ее лично, убедиться в достоверности размещенной информации, выяснить все подробности дела, а затем уже решать - передавать деньги или нет.

МОШЕННИЧЕСТВО, СВЯЗАННЫЕ С ИНТЕРНЕТ - МАГАЗИНАМИ

Через Интернет вам могут предложить приобрести все, что угодно, а распознать подделку при покупке через сеть бывает сложно. Однако, соблюдая некоторые правила покупки товаров через Интернет, можно оградить себя от возможных неприятностей.

Вас должна насторожить слишком низкая цена на определенный товар, а также отсутствие фактического адреса или телефона продавца. Скорее всего, вам предлагают приобрести подделку либо хотят присвоить ваши деньги.

SMS-МОШЕННИЧЕСТВО В СПАМЕ

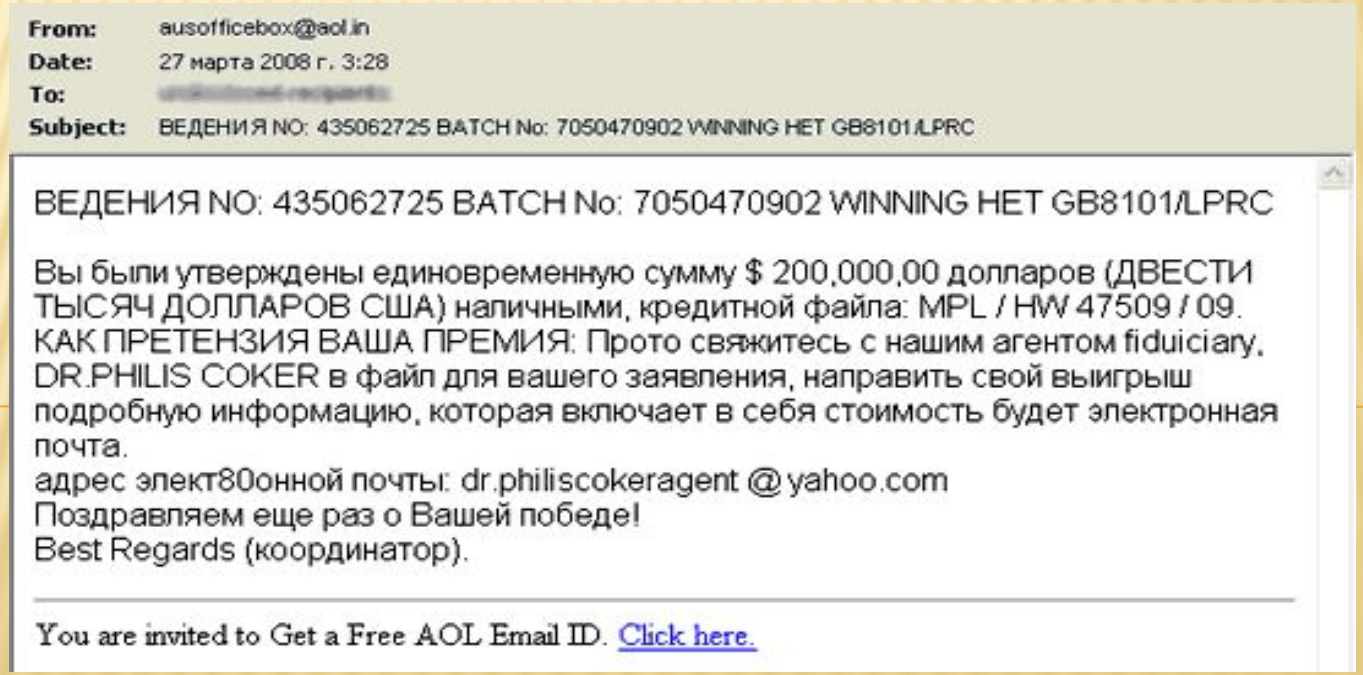
Письма, в которых под разными предлогами вас просят послать SMS-сообщение на короткий номер. Сюда же относятся и письма, содержащие ссылки на сайты, на которых в качестве платы за якобы предоставляемую услугу также предлагается послать SMS-сообщение на короткий номер. Что бы в таких письмах ни обещали мошенники, дело кончится тем, что вы заплатите за несуществующую услугу сумму не менее десяти долларов.

"ГОРЯЩИЕ" ПУТЕВКИ

Здесь мошенничество довольно элементарно -- малоизвестные туристические фирмы, постоянно намекающие на "демпинговые" цены на высококлассные туры, на самом деле продают весьма дешевые пакеты услуг, которые совсем не соответствуют описаниям и фотографиям на сайте.

ПОДДЕЛЬНЫЕ УВЕДОМЛЕНИЯ О ВЫИГРЫШЕ В ЛОТЕРЕЮ

В письме сообщается о том, что вы якобы выиграли в лотерею. Цель мошенников — выманить у вас некоторое количество денег за «перевод» вашего денежного приза.



From: ausofficebox@aol.in
Date: 27 марта 2008 г. 3:28
To: [redacted]
Subject: ВЕДЕНИЯ NO: 435062725 BATCH No: 7050470902 WINNING HET GB8101/LPRC

ВЕДЕНИЯ NO: 435062725 BATCH No: 7050470902 WINNING HET GB8101/LPRC

Вы были утверждены единовременную сумму $ 200,000,00 долларов (ДВЕСТИ ТЫСЯЧ ДОЛЛАРОВ США) наличными, кредитной файла: MPL / HW 47509 / 09.
КАК ПРЕТЕНЗИЯ ВАША ПРЕМИЯ: Прото свяжитесь с нашим агентом fiduciary, DR.PHILIS COKER в файл для вашего заявления, направить свой выигрыш подробную информацию, которая включает в себя стоимость будет электронная почта.
адрес элект80онной почты: dr.philiscokeragent @ yahoo.com
Поздравляем еще раз о Вашей победе!
Best Regards (координатор).

You are invited to Get a Free AOL Email ID. Click here.

ОСТОРОЖНО!!!!! ВИРУС!!!!!

Сущность вируса - переадресация со страницы запрашиваемого ресурса на фиктивную, скопированную с настоящей. Подмена осуществлялась для самых популярных ресурсов Рунета: Яндекс, Рамблер, Майл, ВКонтакте, Одноклассники.

Набирая на «зараженном» компьютере адрес одного из указанных ресурсов, пользователь попадает на сервер-подмену, где ему предлагается страница для входа в систему (имя и пароль). С учетом того, что в адресной строке указано корректное имя, а внешний вид скопирован с оригинального сервера, у большинства пользователей не возникает подозрений в подлинности страницы.

Общаясь в социальных сетях, помните:

Любой человек, с которым вы познакомились в сети и вступили в переписку, может оказаться всего лишь вымышленным персонажем. Не увидев его воочию, вы никогда не сможете быть уверенными в его реальном существовании!

Информация, направляемая Вами посредством сети Интернет - будь это личные данные, фотографии либо видео - может быть использована против Вас, в том числе в корыстных и преступных целях.

Использование Интернета является безопасным, если выполняются

ТРИ ОСНОВНЫЕ ПРАВИЛА

Защитите свой компьютер

- Регулярно обновляйте операционную систему.
- Используйте антивирусную программу.
- Применяйте брандмауэр.
- Создавайте резервные копии важных файлов.
- Будьте осторожны при загрузке содержимого.
- Не проходить по ссылкам в спамовых письмах:
- Не откликаться на заманчивые предложения, особенно если они связаны с получением быстрых денег:

Помните!
После публикации информации в Интернете ее больше невозможно будет контролировать и удалять каждую ее копию.

ТРИ ОСНОВНЫЕ ПРАВИЛА

Защитите себя в Интернете

- Думайте о том, с кем разговариваете.

- Никогда не разглашайте в Интернете личную информацию, за исключением людей, которым вы доверяете. При запросе предоставления личной информации на веб-сайте всегда просматривайте разделы «Условия использования» или «Политика защиты конфиденциальной информации», чтобы убедиться в предоставлении оператором веб-сайта сведений о целях использования получаемой информации и ее передаче другим лицам.

- Всегда удостоверяйтесь в том, что вам известно, кому предоставляется информация, и вы понимаете, в каких целях она будет использоваться.

Помните!
В Интернете не вся информация надежна и не все пользователи откровенны.

ОСНОВНЫЕ ПРАВИЛА БЕЗОПАСНОГО ПОВЕДЕНИЯ В СЕТИ ИНТЕРНЕТ

Вы должны это знать:

*** При регистрации на сайтах, старайтесь не указывать личную информацию, т.к. она может быть доступна незнакомым людям. Так же, не рекомендуется размещать свою фотографию, давая, тем самым, представление о том, как вы выглядите, посторонним людям.**

*** Используйте веб-камеру только при общении с друзьями. Проследите, чтобы посторонние люди не имели возможности видеть ваш разговор, т.к. он может быть записан.**

*** Нежелательные письма от незнакомых людей называются «Спам». Если вы получили такое письмо, не отвечайте на него. В случае, если Вы ответите на подобное письмо, отправитель будет знать, что вы пользуетесь своим электронным почтовым ящиком и будет продолжать посылась вам спам.**

*** Если вам пришло сообщение с незнакомого адреса, его лучше не открывать. Подобные письма могут содержать вирусы.**

*** Если вам приходят письма с неприятным и оскорбляющим вас содержанием, если кто-то ведет себя в вашем отношении неподобающим образом, сообщите об этом**

ОСНОВНЫЕ ПРАВИЛА ДЛЯ ШКОЛЬНИКОВ СТАРШИХ КЛАССОВ

Вы должны это знать:

*** Не желательно размещать персональную информацию в Интернете. Персональная информация — это номер вашего мобильного телефона, адрес электронной почты, домашний адрес и фотографии вас, вашей семьи или друзей.**

*** Если вы публикуете фото или видео в интернете — каждый может посмотреть их.**

*** Не отвечайте на Спам (нежелательную электронную почту).**

*** Не открывайте файлы, которые прислали неизвестные Вам людей. Вы не можете знать, что на самом деле содержат эти файлы – в них могут быть вирусы или фото/видео с «агрессивным» содержанием.**

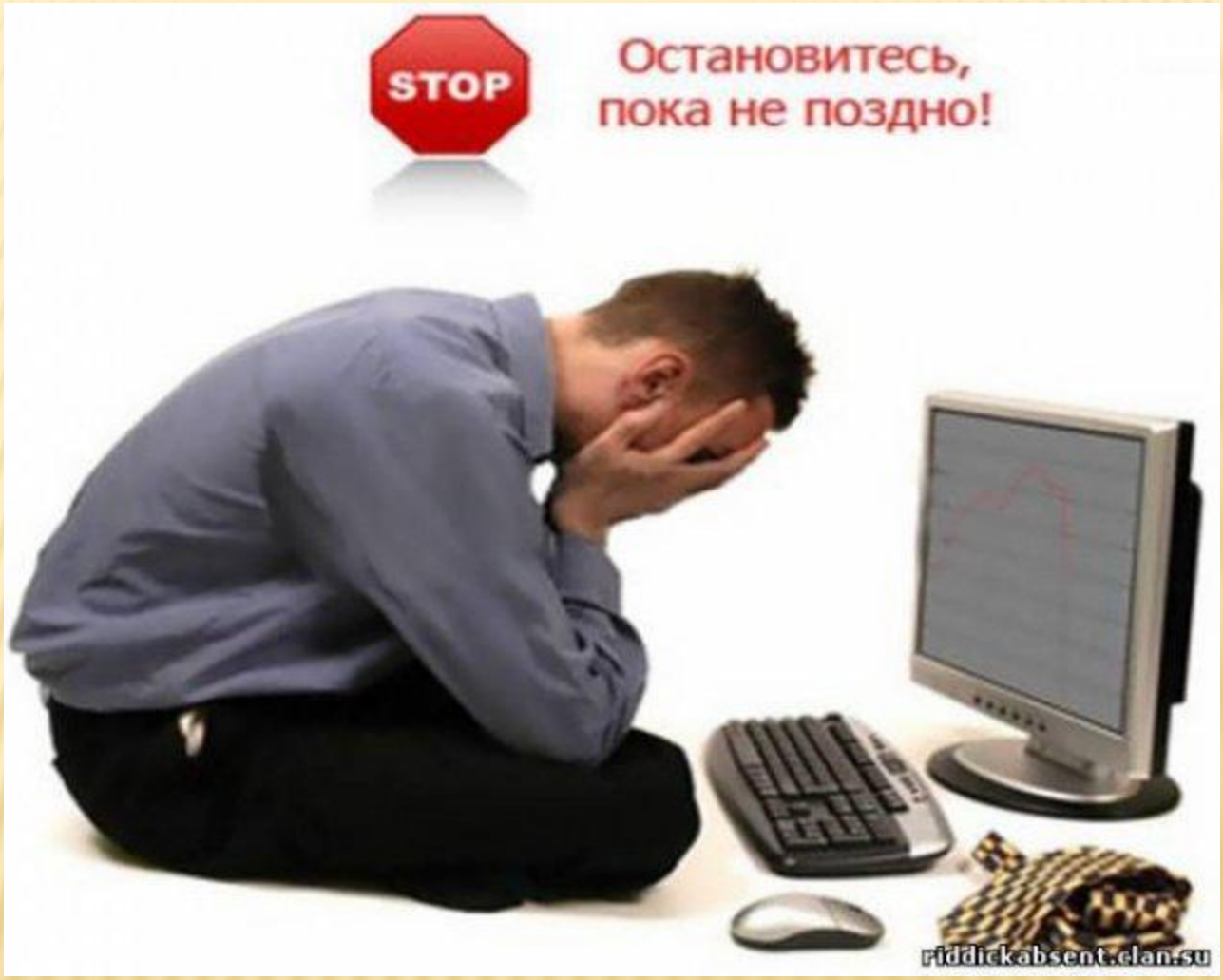
*** Не добавляйте незнакомых людей в свой контакт лист в IM (ICQ, MSN messenger и т.д.)**

*** Помните, что виртуальные знакомые могут быть не теми, за кого себя выдают.**

*** Если рядом с вами нет родственников, не встречайтесь в реальной жизни с людьми, с которыми вы познакомились в Интернете. Если ваш виртуальный друг действительно тот, за кого он себя выдает, он нормально отнесется к вашей заботе о собственной безопасности!**

*** Никогда не поздно рассказать взрослым, если вас кто-то обидел.**

Мошенничество, увы, неискоренимо. И на просторах интернета оно подстерегает нас везде: в электронной почте, социальных сетях, на различных сайтах. С годами злоумышленники изобретают новые приемы, но основные механизмы обмана не меняются. Только сам пользователь может сделать свою жизнь в виртуальном пространстве безопасной. Мы надеемся, что советы и информация, изложенные в этой статье, будут вам полезны.


STOP
Остановитесь,
пока не поздно!
riddickabsent.clan.su