ПАМЯТКА – БЕЗОПАСНОСТЬ В ИНТЕРНЕТЕ

Интернет кроме полезной информации таит в себе массу разных угроз и опасностей. Создан и функционирует Центр Безопасного Интернета в России - ведущий российский комплексный проект в области Интернет-безопасности детей и взрослых, представляющий Россию в сети Центров безопасного Интернета на европейском уровне **www.saferunet.ru**.

Центр занимается Интернет - угрозами и эффективным противодействием им в отношении пользователей. На его странице можно пожаловаться, если попал в беду, и получить помощь

С какими же угрозами и неприятностями может столкнуться пользователь в Интернете?

Интернет с некоторого времени стали называть всемирной помойкой и еще минным полем.

**Психологическая зависимость**

«*Я начал подозревать, что у меня проблемы с интернет-зависимостью, когда однажды я встал в 3 часа утра, чтобы залезть в «сетку», и встретил там своего друга, который пока не ложился спать. В 3 часа ночи он* ***все еще*** *висел в интернете…».*

– так начинается одна статья об интернет-зависимости, доселе неведомой нам проблеме, которая, по прогнозам специалистов, станет «чумой 21 века».

Интернет – уникальное пространство, где можно найти всё – от шнурков до друзей.

*Иллюзия* реальности очень сильна. Возникает как бы параллельная реальность

Если что-то в «реальной реальности» не устраивает человека – силен соблазн ускользнуть туда, где окружающий мир будет строиться по собственному желанию.

Очень часто интернет привлекает людей с заниженной самооценкой, неудовлетворенных собой, неспособных в реальной жизни строить или поддерживать гармоничные отношения с другими. Широко распространены виртуальные ролевые игры, где ты можешь стать кем захочешь, тем самым преодолевая собственные ограничения; вести себя, думать и чувствовать как вымышленный герой.

Молодые люди постепенно начинают вести себя в реальной жизни так, как в игре. **Порой это опасное поведение для себя или окружающих**!

Известны такие, например, случаи:

*Группа подростков убила бабушку молотком по голове. Они очень удивились, что она умерла. Ведь в игре совсем по-другому. Там много жизней, там удары безопасны…*

*Парень, переходя улицу, вместо того, чтобы пропустить автомобили, попытался перепрыгнуть улицу, как он это делал в игре. Естественно он погиб.*

Лекарство: – занятия спортом, различными видами творчества, искусством, чтение интересных книг, труд.

**Опасные места в Интернете**

- Социальные сети, чаты, блоги.
- Сайты скачивания видео и музыки.
- Порносайты.
- Сайты, склоняющие к самоубийству, разжиганию розни и т.п.
- Сайты с противоправным содержанием (терроризм, наркотики, смеси и т.п.).

**Зачем** злоумышленникам информация о пользователях и доступ к их компьютеру? 2 Цели: **Получение денег или Управление компьютером пользователя.**

**Сайты знакомств как площадка для организации киберпреследования**

Распространенной формой преследования является создание фальшивых страничек на сайтах знакомств от имени «жертв», изменение фотографии (фотомонтаж), рассылка знакомым от вашего имени оскорбительных писем, постоянные оскорбления, унижения и угрозы в переписке в чатах и блогах и т.п. Сайты знакомств часто используются для, так называемого, кибер-преследования, когда пользователя «достают» оскорблениями, угрозами, переделывают его фото или от его имени рассылают всем его друзьям пакостные сообщения, а также для вербовки. *Знакомство может окончиться рабством или вступлением в террористическую организацию, или самоубицством*!

**Игры он-лайн с реальным соперником**

Такие приглашения не редкость на интернет-страницах. Если для игры предлагается вначале зарегистрироваться с указанием номера телефона или других персональных данных, то, скорее всего, это мошенники. С телефона снимут все деньги. А самое опасное - игра может закончиться большим долгом. И в случае, если вы указали свои координаты, вас будут преследовать и требовать деньги.

**Завладение информацией о кредитных картах**

Никогда и нигде не сообщайте коды своих кредитных карт! Иначе останетесь без денег.

**Выманивание денег у пользователей мобильных телефонов**

В арсенале недоброжелателей имеются следующие уловки: используя социальную инженерию, мошенники просят перечислить деньги на определенный счет. Для этого SMS составляют таким образом, чтобы казалось, будто его отправлял кто-то из родственников.

**Выманивание денег у пользователей блокированием компьютера**

С помощью вируса компьютер блокируется. Для разблокировки якобы требуется отправить СМС на указанный номер.

Ни к чему, кроме снятия всех денег с телефона, это не приведет.

Лекарство – лечение компьютера антивирусной программой

**Социальная инженерия**

Особый тип атак, не требующих применения технических средств.

Проще говоря, вместо поиска уязвимостей и написания вирусов злоумышленники письмами или разговорами подталкивают пользователей совершить определенное действие, которое отключит защиту компьютера или каким-то другим образом откроет доступ к нужной информации.

Родителям приходит сообщение или звонок, что ребенок попал в беду. Чтобы выручить, нужны деньги. Мошенники рассчитывают на вашу растерянность, неспособность оценить ситуацию и торопят.

Не спешите, проверьте, откуда звонок, перезвоните ребенку или знакомым, посоветуйтесь со знакомыми или друзьями.

**Вовлечение подростков в секты, сексуальную эксплуатацию и наркоманию**

Используя социальные сети, злоумышленники вербуют в секты.

Используя сайты знакомств, ищут жертвы для сексуального рабства.

Привлекают к распространению наркотиков и склоняют к наркомании

**Определение местоположения через интернет**

Проявляйте особую осторожность при работе с сайтами с мобильника, приложениями и сервисами, которые предлагают услуги, связанные с определением местоположения. Этим могут воспользоваться мошенники, чтобы найти Вас или определить ваше место жительства для каких-то своих целей, например ограбления или насильственных действий.

**Что делать?**

Можно обратиться за помощью к экспертам «Линии помощи» (в том числе и проекта Центра Безопасного Интернета России - **http://www.saferunet.ru/hotline/content.php/)**

или в правоохранительные органы (многие пользователи ошибочно считают, что эта мера является чересчур радикальной).

**В заключение несколько советов:**

1. В социальных сетях указывайте минимум информации и подробностей собственной жизни.
2. Не указывайте на публичных ресурсах свои паспортные данные, телефон, адрес и т. д.
3. Не соглашайтесь на предложение встретиться, особенно в одиночку.
4. Проявляйте особую осторожность при работе с сайтами с мобильника, приложениями и сервисами, которые предлагают услуги, связанные с определением местоположения. Этим могут воспользоваться мошенники, чтобы найти Вас или определить ваше место жительства для каких-то своих целей, например ограбления или насилия.
5. Имейте на своем компьютере или телефоне антивирусную программу.
6. Настройте ограничения на доступ к интернет-ресурсам.
7. На кликайте по «сенсационным» ссылкам, новостям – это ловушки.
8. Помните, ваш компьютер, планшет или телефон в любой момент могут превратиться в мишень для злоумышленников.

БУДЬТЕ ОСТОРОЖНЫ И ВНИМАТЕЛЬНЫ!