Наступили школьные каникулы, и, хотим мы того или нет, наши дети будут много времени проводить за компьютером в эти дни. Самое время рассказать об опасностях Интернета для детей тем взрослым, кто еще не сталкивался с интернет-мошенничеством.

По данным опросов пользователей Рунета, 60% родителей никак не ограничивают детей при серфинге в Интернете. Получается, их дети имеют свободный доступ к любым ресурсам Всемирной Паутины. Стоит ли говорить о том, что именно дети чаще всего становятся жертвами интернет-мошенничества?

Расскажем о самых популярных видах интернет-мошенничества, с которыми чаще всего сталкиваются дети.

**Плата за любопытство**

Так можно назвать самый распространенный вид мошенничества, лидер нашего своеобразного рейтинга. Это возможность получить ответ на один из "животрепещущих" вопросов. Помимо перечисленных выше вопросов, это могут быть: "У нас есть информация о любом человеке. Посмотри, что у нас есть о тебе", "Посмотри, как ты будешь выглядеть с новой прической", "Узнай совместимость имен" и пр.

Любопытный пользователь по ссылке переходит на сторонний сайт, где ему предлагается ответить на несколько вопросов. Развитие дальнейших событий возможно по одному из двух сценариев.

1. Пользователю предлагают ввести номер своего мобильного телефона на сайте и ответить на пришедшее смс для подтверждения, что он человек, а не вредоносная программа. При ответе на смс со счета мобильного телефона снимается сумма в 200-300 рублей.
2. Пользователю так же предлагают авторизоваться с помощью мобильного, и оказывается, что, совершив данные манипуляции, он соглашается на платную подписку. Суммы обычно незначительны — 5-10 рублей в день, но списываются ежедневно, что в конечном итоге может вылиться в несколько тысяч рублей.

**Компьютерные игры**

С ними связан второй тип мошенничества в Интернете. Но игры бывают разные и площадки для игр — тоже.

**"Прокачай свой статус в игре"** (или "Получи секретный код и овладей супермощным оружием" и т.п.). Такие предложения порой встречает на просторах Интернета ребенок, который давно играет в какую-то игру, достиг определенных побед, завоевал статусы. Он очень увлечен игрой, и соблазн улучшить показатели велик. О том, что услуга платная, чаще всего не написано. Далее уже известная схема: авторизация на сайте, ввод номера мобильного телефона и ответ на смс либо ввод кода, полученного на сайте. Деньги списываются, а ни статусов, ни нового оружия нет.

Существует еще один очень коварный способ обмана. На мобильный телефон приходит сообщение: "Вам пришла открытка от друга". Для просмотра просят перейти по ссылке. Если это сделать, активируется заложенный в ссылке регистрационный код для номера телефона пользователя. Таким образом, нажимая на ссылку, пользователь автоматически регистрируется на сайте с платной услугой и начинает получать всевозможный спам. Избежать такого мошенничества можно только, если не переходить по ссылке.

**Псевдо-родственники, псевдо-друзья, псевдо-администрация сайта**. Злоумышленники под видом родственников, друзей, администрации сайта прямо просят перевести деньги на какой-то счет, или средства списываются с мобильного телефона при активации присланного ими кода, или вам предлагают отправить платное смс.

**"Прокачка" профиля в соцсети, приобретение "шпионских" программ и пр**. Пользователю предлагают вступить в группу, либо установить приложение, позволяющее получить дополнительные бонусы от использования данной соцсети. Как правило, это не предусмотрено основным функционалом — иметь доступ к чужой переписке, повысить свой рейтинг, получить виртуальные платежные единицы и т.п. Далее при помощи смс либо путем кражи логина-пароля и доступа к кредитной карте мошенники лишают пользователя денежных средств.

Как оградить ребенка от опасностей раннего взросления?

**Четыре правила для взрослых**

**Правило 1. Внимательно относитесь к действиям ваших детей во Всемирной паутине:**

- Не отправляйте детей в "свободное плавание" по Интернету. Старайтесь активно участвовать в общении ребенка с Интернетом, особенно на этапе освоения.

- Беседуйте с ребенком о том, что нового для себя он узнает с помощью Интернета и как вовремя предупредить угрозы.

**Правило 2. Информируйте ребенка о возможностях и опасностях, которые несет в себе Сеть:**

- Объясните ребенку, что в Интернете, как и в жизни, встречаются и "хорошие" и "плохие" люди. Объясните, что, если ребенок столкнулся с негативом или насилием от другого пользователя Интернета, ему нужно сообщить об этом близким людям.

- Научите ребенка искать нужную ему информацию и проверять ее , в том числе с вашей помощью.

- Научите ребенка внимательно относиться к скачиванию платной информации и получению платных услуг из Интернета, особенно путем отправки sms, во избежание потери денег. Несовершеннолетний пользователь должен усвоить важное правило: **никогда не вводить номер своего мобильного, не обсудив это с родителями.** Не надо указывать свой настоящий адрес и номер домашнего телефона, а также рассказывать незнакомцам слишком много и тем более встречаться с ними без ведома родителей.

- Составьте список полезных, интересных, безопасных ресурсов, которыми может пользоваться ваш ребенок, и посоветуйте их использовать.

**Правило 3. Выберите удобную форму контроля пребывания ребенка в Сети:**

- Установите на ваш компьютер необходимое программное обеспечение - решение родительского контроля, антивирус Касперского или Doctor Web.

- Если ваш ребенок - учащийся младших классов и остается часто дома один, ограничьте время его пребывания в Интернете.

- Если компьютер используется всеми членами семьи, установите его в месте, доступном для всех членов семьи, а не в комнате ребенка.

- Создавайте разные учетные записи на вашем компьютере для взрослых и детей. Это поможет не только обезопасить ребенка, но и сохранить ваши личные данные.

- Регулярно отслеживайте ресурсы, которые посещает ваш ребенок. Простые настройки компьютера позволят вам быть в курсе того, какую информацию просматривали ваш сын или дочь.

**Правило 4. Регулярно повышайте уровень компьютерной грамотности, чтобы знать, как обеспечить безопасность детей:**

- Используйте удобные возможности повышения уровня компьютерной и интернет-грамотности, например, посещение курсов, чтение специальной литературы, консультации с экспертами.

- Знакомьте всех членов вашей семьи с базовыми принципами безопасной работы на компьютере и в Интернете

-Но прежде всего, конечно, надо общаться с ребенком. Построить с ним доверительные отношения. Организовать его досуг в соответствии с интересами и наклонностями. Участвовать в формировании правильной картины мира, быть рядом и разъяснять различные происшествия и события — например, в доступной форме пересказать содержание этой статьи.

Старший инспектор группы ОУУП ПДН

Майор полиции С.В. галеева