

СМАЙЛИК ВМЕСТО ДРУГА

История, которую мы вам расскажем, могла случиться с... нет, не с каждым пользователем интернета, а только с тем, кто не обучен правилам безопасного поведения в сети. Позовите родителей или старших родственников и прочитайте вместе рассказ о Пете. Задайте себе вопросы под маркером «Стоп!». По ответам поймёте, насколько вы подготовлены к рискам, которые таят в себе виртуальные знакомства.

Петька отчаянно скучал. Не то чтобы у него не было друзей, просто все они были заняты своими делами – один на хоккей с мячом ходил, другой – постоянно в Кванториуме зависал, третий из библиотек не вылезал. И даже всезнайка Раечка в это время была недоступна – в музыкальной школе, видите ли, у неё занятия. А Пете всё это было не интересно! Зачем куда-то ходить, когда всё, что нужно, можно найти в интернете. Мультки, смешные видеоролики, игры и даже... друзей. Таких, которые не бросят тебя одного, не то, что эти, зануды!

Петькины размышления прервал звук пришедшего сообщения в любимой онлайн-игре. Мальчик бросился к компьютеру и с нетерпением защёлкал

мышкой. Недавно на платформе игры он завёл себе нового друга – геймера с ником Крутик. Правда, как тот выглядел, Петя не знал – на аватарке был смайлик, зато с ним было легко и весело общаться. И вскоре Крутик стал для Пети не просто товарищем по игре, а настоящим другом, которому можно доверять и рассказывать все свои секреты.

Стоп! Какую ошибку совершил Петя?





Несмотря на то, что Крутик представился ровесником Пети, в игре он был гораздо продвинутое. Знал такие приёмы, что Петке ещё и не снились. Например, как купить робуксы (игровую валюту) совсем дёшево. Петка уже переписал все данные с маминой банковской карты и для совершения выгодной сделки ждал только заветную ссылку.

И вот она, долгожданная, в сообщении от Крутика, так и манит, так и манит. Петка поставил курсор на синюю строчку и нажал на клавишу мыши.

Стоп! Подскажите Пете, чего ни в коем случае нельзя было делать.

В появившиеся окошки платёжной системы он аккуратно ввёл все данные банковской карты – номер, срок действия, трёхзначный код и сумму – 500 рублей. Петя надеялся, что такой небольшой перевод мама не заметит. И стал ждать, когда заветные робуксы упадут на его виртуальный счёт.

Стоп! Правильно ли поступил Петя?



Прошёл час, два, три, а счёт так и не пополнился. И посоветоваться было не с кем – новый друг Крутик в сети больше не появлялся. Зато вечером, когда пришли с работы родители, выяснилось, что с маминой карты исчезли все деньги – её вчерашняя зарплата и всё, что было отложено на подарок Петке ко дню рождения.

Приехавшие на вызов полицейские быстро поняли, куда ушли деньги и кто в этом виноват. Петка сидел перед родителями, красный, как рак. Опустив низко голову, шмыгал носом и утирал слёзы. Нет, плакал Петка не из-за того, что его предал новый друг, и не из-за того, что не подарят на день рождения обещанный велосипед. Плакал Петка от стыда – он чувствовал себя воришкой и соучастником преступления...



Что нужно было сделать, чтобы не попасть, как Петя, в такую историю?

Советы от Государственного инспектора Роскомнадзора Сергея Лимонова

1 Не надо всецело доверять виртуальным друзьям, нельзя рассказывать им личную информацию, присылать фотографии, соглашаться на встречу. За безобидным ником и милым смайликом на аватарке может скрываться злоумышленник.

2 Чтобы проверить, реально ли человек является тем, за кого себя выдаёт, предложите ему совершить видеозвонок. Если новый знакомый отказывается или тянет с видеозвонком, смело можно исключить его из списка друзей.

3 Нейросети уже научились подделывать изображения и голоса реальных людей. Чтобы убедиться, что по видео с вами разговаривает ваш знакомый или родственник, **попросите его сделать резкие движения – повернуть голову, почесать нос.** Изображение, созданное искусственным интеллектом, будет тормозить или искажаться.

4 Нельзя переходить по ссылкам от посторонних, сообщать незнакомцам номера банковских карт, коды и пароли из сообщений. Нельзя скачивать файлы, полученные от незнакомых пользователей. Так мошенники могут взломать устройство и украсть личные данные и важную информацию.

5 Узнать, безопасная ссылка или нет, очень просто. Нужно скопировать её (осторожно, чтобы случайно не нажать) и вставить в адресную строку браузера. Браузер сам подскажет, ведёт ссылка на реальный сайт или созданный злоумышленниками.



Лариса САХАРОВА
Рисунки Светланы САФФО