Правила безопасного использования сети Интернет для детей

№ 1 ХРАНИТЕ ТАЙНЫ

В информационном пространстве нам часто приходится вводить свои данные: ФИО, адрес, дату рождения, номера документов. Безопасно ли это?

Персональные данные (имя, фамилия, адрес, дата рождения, номера документов) можно вводить только на государственных сайтах или на сайтах покупки билетов. И только в том случае, если соединение устанавливается по протоколу https. Слева от адреса сайта должен появиться значок в виде зеленого замка — это означает, что соединение защищено.

Вряд ли ребенку потребуется регистрация на государственных сайтах, но даже если она нужна, делать это в любом случае надо под руководством родителей. Важно помнить, что ни в коем случае нельзя передавать через Сеть данные любых документов и банковских карт. Даже (и тем более) если кто-то об этом просит, старается убедить в том, что возникла критическая ситуация, торопит и повторяет, что нужно срочно прислать информацию.

Если такая ситуация возникла, ребенку нужно сразу связаться с родителями. Если ему говорят, что никому ничего сообщать нельзя, и пугают неприятными последствиями, тем более следует срочно обо всем рассказать семье. Запугивание и попытки во что бы то ни стало получить сведения говорят о том, что перед вами мошенники.

№ 2 БУДЬТЕ АНОНИМНЫ

Создавая свой профиль в социальных сетях, нужно максимально избегать привязки к «физическому» миру.

Нельзя указывать свой адрес, дату рождения, школу, класс. Лучше использовать очевидный псевдоним: по нему должно быть ясно, что это не настоящее имя (ведь использовать ложные данные: «Алексей» вместо «Александр» — по правилам соцсетей запрещено).

№ 3 НЕ РАЗГОВАРИВАЙТЕ С НЕЗНАКОМЦАМИ

Есть несколько главных опасностей, с которыми можно столкнуться в интернете. По большому счету они мало отличаются от тех, что угрожают нам в реальной жизни. Злоумышленники здесь просто используют другие средства.

Буллинг. Ребенка обзывают или травят в интернете — чаще всего без какой-либо причины, «потому что так весело». К жертве могут прицепиться из-за фотографии в профиле или из-за поста в соцсетях.

Педофилы. Просят прислать личные фотографии, а при отказе угрожают расправой над членами семьи или шантажируют другими способами.

Мошенники. Пытаются завладеть данными пользователя или втянуть ребенка в опасную финансовую авантюру.

Главное средство защиты от всех этих угроз — конфиденциальность. Нельзя выкладывать свои фотографии в Сеть. Следует ограничить доступ к информации о всех сторонах своей жизни, будь то онлайн или офлайн. Сообщать их можно только проверенным людям: родным, близким и людям, которые знакомы вам лично, а не через интернет.

Тех, кто пытается вас как-то задеть и обидеть (так называемых троллей), нужно просто игнорировать.

№ 4 РАСПОЗНАЙТЕ ЗЛОУМЫШЛЕННИКА

На что надо обратить внимание прежде, чем вступить в диалог? Что сигнализирует об опасности?

Вы не знакомы с этим человеком в реальной жизни.

Ваш собеседник явно взрослее вас.

У него нет или очень мало друзей в соцсети.

Собеседник о чем-то просит: сфотографироваться, прислать какие-то данные и т. д.

№ 5 БУДЬТЕ БДИТЕЛЬНЫ

Плохая новость — удалить ничего не получится.

Все, что попало в Сеть или даже в смартфон, останется там навсегда. Как правило, стереть данные из Сети невозможно. Единственный способ избежать утечки информации — не делиться ею.

№ 6 ВНИМАНИЕ — НА ИГРЫ

Правила безопасности есть не только в соцсетях и мессенджерах. Все основные угрозы могут исходить и от онлайн-игр.

Там ребенок даже более уязвим, поскольку им проще манипулировать: игровые объекты, членство в командах, внутриигровые социальные связи — все это может стать механизмом манипуляции для мошенников, педофилов или даже вербовщиков различных экстремистских группировок. Вот почему в игре нужно вести себя особенно внимательно.

№ 7 УЧИТЕСЬ ЗАМЕЧАТЬ ПОДДЕЛЬНЫЕ САЙТЫ

Фишинг — это способ выманивать у человека его данные: логин, название учетной записи и пароль.

Происходит это так: пользователю присылают ссылку на сайт, очень похожую на настоящий адрес почтового сервиса или социальной сети. Как правило, фишеры специально покупают такие домены. Например, для mail.ru это может быть «meil.ru», а для vk.com — «vk-com.com».

Злоумышленник ждет, когда человек введет логин или пароль на поддельном сайте. Так он узнает данные, а потом использует их для входа в настоящий профиль своей жертвы.

№ 8 АККУРАТНЕЕ С ПОКУПКАМИ

Главное правило интернет-покупок такое: доступ ребенка к деньгам должен быть ограниченным и находиться под контролем родителей.

Основные финансовые потери обычно происходят через телефон. Необходимо подключить услуги блокировки платного контента, не класть много денег на счет детского телефона и контролировать расходы. Все остальные платежи должны согласовываться с родителями и происходить только под их присмотром.

№ 9 ГЛАВНЫЙ СЕКРЕТ БЕЗОПАСНОСТИ В СЕТИ

Не нужно делать в интернете ничего, что бы вы не стали бы делать в физическом мире. Разница между виртуальной и реальной действительностью минимальна.

Что касается родительского поведения, то в Сети оно тоже не должно отличаться от поведения «в офлайне». От ребенка нельзя добиться повиновения путем запретов и жесткого контроля. Однако и ощущения вседозволенности в интернете тоже быть не должно. Вместе учитесь вести безопасный образ жизни, как реальной, так и виртуальной.

Источник: https://www.ucheba.ru/