БИБЛИОТЕКА КНИЖНЫХ ГЕРОЕВ

10 правил безопасного поведения в Интернете

1

УМЕЙТЕ ХРАНИТЬ ТАЙНЫ: ИМЯ, АДРЕС, ДАТУ РОЖДЕНИЯ

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

Нельзя указывать свой адрес, школу, класс. Лучше использовать очевидный псевдоним: по нему должно быть ясно, что это не настоящее имя. Не надо ставить свою фотографию на аватар.

3

НЕ РАЗГОВАРИВАЙТЕ С НЕЗНАКОМЦАМИ

Есть несколько главных опасностей, с которыми можно столкнуться в интернете.

Буллинг. Вас 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.

Преступники. 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

НЕ ХРАНИТЕ ВАЖНУЮ ИНФОРМАЦИЮ В СЕТИ

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.

Правила публикации собственных фотографий очень простые — если вы не хотите, чтобы они стали достоянием общественности, нельзя выкладывать их в интернет и отправлять кому-то с его помощью. Даже мессенджеры «умеют» копировать переписку в «облако», так что вы можете потерять контроль над своими снимками. А фото других людей стоит выкладывать только в случае, если они на это согласны.

БИБЛИОТЕКА КНИЖНЫХ ГЕРОЕВ

10 правил безопасного поведения в Интернете

5 НЕ СООБЩАЙТЕ СВОЕ МЕСТОПОЛОЖЕНИЕ

Данные геолокации позволяют всему миру узнать, где вы живете и учитесь, проводите свободное время, в каких акциях участвуете, какие шоу и спектакли любите, как отдыхаете. Чтобы сделать геолокацию максимально безопасной, нужно следить за тем, чтобы местоположение не отображалось на «искабельных» объектах — особенно на фотографиях. На телефонах, в настройках камеры, как правило, можно запретить геометки.

6 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.

7 ТРЕНИРУЙТЕ ПАМЯТЬ – ВАЖНЫЕ ПАРОЛИ ХРАНИТЕ В ГОЛОВЕ

Можно ли пользоваться сервисами, которые сохраняют пароли? Если в профиле содержится действительно важная информация, то, увы, нет. Почему? Это удобно, но онлайн-сервисы для хранения паролей ненадежны. Их часто взламывают и копируют оттуда пароли пользователей.

8 АККУРАТНЕЕ С ПОКУПКАМИ – НЕ ПРИВЯЗЫВАЙТЕ БАНКОВСКИЕ КАРТЫ К ТЕЛЕФОНУ

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 СОБЛЮДАЙТЕ СЕТЕВОЙ ЭТИКЕТ

Правила хорошего тона в Сети ничем не отличаются от тех, которые нужно соблюдать в реальном мире. Не оскорбляйте других, не будьте навязчивым, не позволяйте своим негативным эмоциям выходить из-под контроля, пишите грамотно. Никогда не участвуйте в травле: буллинг в Сети ничем не отличается от реального и одинаково опасен и для жертвы, и для агрессора.

10 ГЛАВНЫЙ СЕКРЕТ БЕЗОПАСНОСТИ В СЕТИ – РАЗНИЦА МЕЖДУ ВИРТУАЛЬНОЙ И РЕАЛЬНОЙ ЖИЗНЬЮ МИНИМАЛЬНА.

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

При составлении буклета использованы материалы сайта https://www.ucheba.ru/