15 ПРАВИЛ БЕЗОПАСНОГО ПОВЕДЕНИЯ В ИНТЕРНЕТЕ

№ 1 ХРАНИТЕ ТАЙНЫ

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.

№ 2 БУДЬТЕ АНОНИМНЫ

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

Буллинг – травля в интернете. К жертве могут прицепиться из-за фотографии в профиле или из-за поста в соцсетях.

Маньяки. 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.

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

№ 4 РАСПОЗНАЙТЕ ЗЛОУМЫШЛЕННИКА

Нельзя вступать в диалог в сети с незнакомым человеком если:

- 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 ХРАНИТЕ ФОТО В НЕДОСТУПНОМ МЕСТЕ

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. Если что-то куда-то было отправлено или где-то опубликовано, это ушло в Сеть. Важно помнить, что ни в коем случае нельзя выкладывать фотографии документов — своих или чужих. А фото других людей стоит выкладывать только в случае, если они на это согласны.

№ 6 БУДЬТЕ БДИТЕЛЬНЫ- 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.

№ 7 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. Отследить местоположение человека теперь не составляет труда.

Не ставьте геометки на фотографиях, в социальных сетях.

№ 8 ОПАСНЫЕ КОМПЬЮТЕРНЫЕ ИГРЫ

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

№ 9 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.

№ 10 ТРЕНИРУЙТЕ ПАМЯТЬ-ХРАНИТЕ ПАРОЛИ В ГОЛОВЕ

Пароли должны быть уникальными. Цифры и спецсимволы значительно усложняют процесс подбора. В соцсети, мессенджеры и почту безопаснее входить через приложения, а вот в браузерах ввода паролей следует избегать.

№ 11 АККУРАТНЕЕ С ПОКУПКАМИ

Все сервисы, которые принимают деньги, должны иметь зеленый значок «https» рядом с названием. Если такого значка нет, лучше не пользоваться страницей. Впрочем, даже его наличие стопроцентной гарантии не дает.

Часто в пабликах «ВКонтакте» предлагают что-то купить с использованием платежной системы Qiwi. Тут тоже нужно проявлять бдительность и внимательно изучать отзывы о продавце. В соцсетях есть немало мошенников, которые после получения денег исчезают.

№ 12 ПРОВЕРЯЙТЕ ИНФОРМАЦИЮ-НЕ ВЕРЬТЕ ВСЕМУ ЧТО НАПИСАНО В ИНТЕРНЕТЕ

Чтобы проверить информацию, которую вы получили в интернете, следуйте следующим рекомендациям:

- поищите еще два-три источника, желательно и на других языках тоже;
- найдите первоисточник и задайте себе вопрос: «Можно ли ему доверять?»;
- проверьте, есть ли в Сети другие мнения и факты, которые опровергают или подтверждают сказанное.
- Если нужно узнать какой-то факт или выяснить, что значит непонятный термин, можно обратиться к «Википедии».

№ 13 ПОЗАБОТЬТЕСЬ ОБ «ОБЛАКЕ»

Насколько надежны хранилища, вроде «Облако» Mail.Ru, и можно ли там без опаски хранить документы?

Специалисты говорят, что облачное хранилище можно обезопасить, если предварительно зашифровать документы с помощью PGP или использовать программу для создания архива, поместив в него отсканированные документы.

При создании архива нужно указать опцию «непрерывный архив» (solid archive) и поставить на этот архив хороший пароль.

Например, такой:
«kn23iuhuio12njkpuiy89y7&R&TFTGIY*(UYT&*T^G!*OUH*&GYUIHJK)».

Или хотя бы такой: «во#полеберезастояла123».

№ 14 СОБЛЮДАЙТЕ СЕТЕВОЙ ЭТИКЕТ

- Не оскорбляйте других, не будьте навязчивым, не позволяйте своим негативным эмоциям выходить из-под контроля, пишите грамотно;
- не привлекайте к себе внимание за счет эпатажа;
- не отходите от темы разговора: «флуд» считается одним из главных «грехов» в Сети;
- не игнорируйте вопросы собеседника, кроме явного троллинга или оскорблений — подобную беседу нужно немедленно прекратить;
- никогда не участвуйте в травле: буллинг в Сети ничем не отличается от реального и одинаково опасен и для жертвы, и для агрессора.

№ 15 НЕ НУЖНО ДЕЛАТЬ В ИНТЕРНЕТЕ НИЧЕГО, ЧТО БЫ ВЫ НЕ СТАЛИ БЫ ДЕЛАТЬ В ФИЗИЧЕСКОМ МИРЕ

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.