## ЛОГИН И ПАРОЛЬ

Придумайте пароли, представляющие собой длинные фразы или предложения и содержащие сочетание строчных, прописных букв, цифр и символов. Используйте надежные пароли и храните их в секрете.

Никому не давайте свой логин и пароль. Так как ваш друг может войти в систему, притворившись вами, скажет нечто ужасное и причинит вам неприятности. Конечно, бывший друг повеселится, но его действия опасны, и подобное случается постоянно. С вашими данными можно выложить «пост», из-за которого будут проблемы с родителями или даже с законом.

## ХРАНИТЕ ТАЙНЫ

Никому не сообщайте фамилию, имя, номер телефона, данные родителей, адрес места жительства и номер школы, пароли, номера банковских карт, любимые места для прогулок и частые маршруты. Аккаунт приятеля могут взломать. И под именем друга окажется злоумышленник.

Персональные данные (имя, фамилия, адрес, дата рождения, номера документов) можно вводить только на государственных сайтах или на сайтах покупки билетов. Важно помнить, что ни в коем случае нельзя передавать через сеть данные любых документов и банковских карт. Если такая ситуация возникла, ребёнку 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.

После публикации информации в интернете ее больше невозможно контролировать и удалить ее копию.

## БУДЬТЕ АНОНИМНЫ

Создавая свой профиль в социальных сетях, нужно максимально избегать привязки к «физическому» миру. Используйте вымышленное имя (ник) для регистрации на различных ресурсах.

Нельзя указывать свой адрес, дату рождения, школу, класс. Лучше использовать очевидный псевдоним: по нему должно быть ясно, что это ненастоящее имя (ведь использовать ложные данные: «Алексей» вместо «Александр» – по правилам соцсетей запрещено). Не надо ставить свою фотографию на аватар, если вам не исполнилось хотя бы 15-16 лет. Все дети и подростки младше этого возраста, публикуя свою фотографию, рискуют стать жертвой злоумышленников.

## ОСТОРОЖНО С НЕЗНАКОМЦАМИ

Не встречайся без родителей с людьми из интернета в живую. Не добавляй незнакомых людей в свои контакты. В интернете многие люди рассказывают о себе неправду, злоумышленники используют другие средства:

*Буллинг.* Ребёнка 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 ребёнка в опасную финансовую авантюру.

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 или обидеть, нужно просто игнорировать. Не допускайте грубости в интернете, блокируйте веб-агрессоров.

Если вас что-то напугало, насторожило или шокировало на сайте, немедленно уйдите с него. Желательно выключить на время компьютер и рассказать об этом взрослым.

## ХРАНИТЕ ФОТО В НЕДОСТУПНОМ МЕСТЕ

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. Главное средство защиты от всех этих угроз – конфиденциальность.

Правила публикации собственных фотографий очень простые: если вы не хотите, чтобы они стали достоянием общественности, нельзя выкладывать их в интернет. Даже мессенджеры «умеют» копировать переписку в «облако», так что вы можете потерять контроль над своими снимками. 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.

## ИГРЫ

Все основные угрозы могут исходить и от онлайн-игр. Играя в онлайн-игры, ребёнок даже более уязвим, поскольку им проще манипулировать: игровые объекты, членство в командах, внутри-игровые 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.

## ИНТЕРНЕТ-ПОКУПКИ

Главное правило интернет-покупок: доступ ребёнка к деньгам должен быть ограниченным и находиться под контролем родителей. В соцсетях есть немало мошенников, которые после получения денег исчезают.

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.

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.

Используйте фильтры электронной почты для блокирования спама и нежелательных сообщений.