Приложение 4.2.

Примеры обращений на Линию помощи «Дети онлайн»

Кейс 1

Добрый день! Меня зовут Марина, мне 14 лет. Недавно кто-то взломал мой аккаунт в ВКонтакте и стал размещать на моей стене неприличные изображения. А еще оскорблять от моего имени друзей в комментах и в личке. Обо всем я узнала от подруги, так как на даче, где я была, не было Интернета. Я восстановила доступ к аккаунту и поменяла пароль, но было уже поздно. Многие удалили меня из друзей и добавили в черный список, а кое-кто даже перестал со мной разговаривать. Я уже несколько лет вела эту страницу, и у меня было почти 1000 подписчиков, а теперь все пропало. Подскажите, как мне поступить? Как вернуть доверие подписчиков?

Кейс 2

Доброго времени суток! Меня зовут Артем, я учусь в 9 классе. Как-то раз на уроке информатики я зашел в свой аккаунт в социальной сети, а выйти потом забыл. В результате через неделю один из моих одноклассников создал паблик, в которой он выкладывает скриншоты моей личной переписки с друзьями и гадкие комментарии к ним. Там нет ничего такого, но это все равно неприятно. Надо мной стали все смеяться из-за этого. Я и раньше не был самым популярным в классе, а теперь стал настоящим изгоем. Подскажите, что делать? Можно ли удалить этот паблик? Как наказать одноклассника?

Кейс 3

Здравствуйте! Меня зовут Настя, мне 15 лет. Несколько месяцев назад я познакомилась с одним парнем в социальной сети. Он был знакомым моей подруги и показался мне интересным. Мы стали общаться, оказалось, что у нас много общего. Он рассказывал мне о себе, о том, где он учится, где путешествовал. Я тоже рассказывала ему о себе. Вообще-то я довольно скрытный человек и профиль у меня только для друзей, но с ним я, кажется, позволила себе лишнего. Однажды он предложил встретиться. Я немного испугалась и отказала ему. Тогда он начал настаивать, сказал, что знает, где я учусь и где живу. Обещал подстеречь меня по дороге из школы домой. Я очень боюсь, не знаю, правда это, или он меня просто запугивает. Мне и вправду страшно, теперь без подруги я в школу одна не хожу. Подскажите, как мне быть?

Кейс 4

Добрый день! Меня зовут Егор, мне 12 лет. Я тут увидел в Интернете рекламу новой игры, она называлась Dragons & Unicorns. Для того чтобы в нее поиграть, нужно было зарегистрироваться на сайте и указать номер мобильного, что я и сделал. В результате игра мне совсем не понравилась, и я быстро забыл про нее. А через несколько дней мне на телефон стали приходить СМС-ки с рекламой с разных номеров. Я удалил свой аккаунт на сайте игры, но это не помогло, СМС-ки продолжают приходить. Подскажите, как от них избавиться?

Кейс 5

Добрый день, меня зовут Лена! Мне 15 лет. Меня обманула моя «подруга» из социальной сети. Мы общались больше года. Познакомились в паблике про ролевые игры. Я говорила ей, что мечтаю приобрести последний сет игры Dungeons & Dragons, но у нас он не продается. Заказать по Интернету я не могу. У меня нет банковской карты, а родители свою не дают. Подруга предложила мне помочь купить сет. Она уже студентка, и у нее есть карта. Она предложила мне перевести ей деньги на Яндекс-Кошелек и обещала сделать заказ с доставкой на мой адрес. Я с радостью согласилась и перевела ей деньги.

Прошел месяц, а посылка не приходила. Когда я спрашивала ее об этом, она отвечала, что нужно подождать. Потом она стала появляться в сети все реже и реже, пока совсем не пропала. Совершенно случайно я узнала, что она обманула еще нескольких человек аналогичным способом. Подскажите, можно ли что-то сделать? Вернуть деньги или наказать мошенницу?

**Комментарии для ведущего:**

Кейс 1

В данном случае мы имеем дело со взломом аккаунта школьницы с целью нанесения вреда ее репутации. Это довольно распространенная проблема. По статистике Фонда Развития Интернет, более четверти российских школьников (28%) сталкивались со взломом аккаунта в социальных сетях. Из письма довольно сложно установить причину произошедшего. Наиболее распространенные причины взлома аккаунта:

* Использование простых паролей.
* Неправильное хранение паролей.
* Вход в аккаунт с чужого устройства.
* Ввод пароля на поддельной страничке.
* Действие вредоносных программ.
* Сообщение пароля третьим лицам.

В данной ситуации для восстановления репутации школьнице можно порекомендовать следующие действия:

* Сменить пароли ко всем аккаунтам на других онлайн-ресурсах.
* Удалить все неприятные и неэтичные сообщения со своей страницы.
* Разместить на странице пост, разъясняющий причины произошедшего, и извиниться перед читателями.
* Постараться лично поговорить с самыми близкими друзьями и объяснить им ситуацию.

Для того чтобы избежать подобной проблемы, следует предпринять следующие шаги:

* Использовать сложные пароли и двухэтапную систему аутентификации.
* Установить антивирусные программы на все устройства, с которых осуществляется выход в Интернет.
* Соблюдать правила осторожности при входе в аккаунт с чужого компьютера.
* Соблюдать правила поведения при столкновении с поддельными страницами.

Кейс 2

В данном случае мы имеем дело с кибербуллингом – травлей, организованной с помощью электронных средств связи. По статистике Фонда Развития Интернет, каждый четвертый российский школьник (24%) сталкивался с оскорблениями, унижениями, преследованиями и обидами в Сети (подробнее о кибербуллинге см. журнал «Дети в информационном обществе», № 16).

Из письма становится ясно, что одной из причин буллинга стала кража аккаунта и персональных данных, которые произошли из-за неосторожного входа в социальную сеть на чужом компьютере.

В данной ситуации школьнику можно порекомендовать следующие действия:

* Сменить пароль от аккаунта и временно закрыть его.
* Написать в службу поддержки социальной сети письмо с просьбой удалить паблик, приложив скриншоты из самого паблика и из личной переписки, подтвердив тем самым неправомерное использование личных данных одноклассником.
* Если ситуация повторится, и после удаления будет создан новый паблик, написать в службу поддержки социальной сети письмо с просьбой удалить аккаунт пользователя, за нарушение правил пользования ресурсом.
* Рассказать о ситуации взрослым (родителям или учителям) и попросить их вмешаться в ситуацию в школе.

Для того чтобы избежать подобной проблемы в будущем, следует предпринять следующие шаги:

* Использовать двухэтапную систему аутентификации.
* Соблюдать правила осторожности при входе в аккаунт с чужого компьютера.
* Соблюдать осторожность в личной переписке в социальных сетях.

Кейс 3

В данном случае мы имеем дело с преследованием и шантажом, которые могут быть как частью буллинга, так и сексуальных домогательств (подробнее о домогательствах см. журнал «Дети в информационном обществе», № 11).

Из письма можно заключить, что причиной проблемы стала некоторая личная информация, которую автор письма сообщил шантажисту. В данной ситуации школьнице можно порекомендовать следующие действия:

* Внимательно перечитать историю переписки и понять, какая персональная информация могла попасть к шантажисту.
* Внимательно изучить общие контакты и понять, какую информацию о школьнице шантажист мог узнать косвенно от третьих лиц, например, прочитать на страницах и в профилях друзей.
* Рассказать или показать историю переписки взрослым (родителям, учителям), чтобы они могли предпринять действия по защите девушки, вплоть до обращения в правоохранительные органы.
* В случае если шантажист снова выйдет на связь, сообщить ему обо всех предпринятых действиях и добавить его в черный список.

Чтобы избежать подобной проблемы следует предпринять следующие шаги:

* С большой осторожностью добавлять незнакомцев в друзья, даже если они являются друзьями друзей.
* С большой осторожностью вступать в переписку с незнакомцами.
* Не сообщать личную информацию незнакомцам. Даже если она кажется безобидной, она может быть легко использована против жертвы.

Кейс 4

В данном случае мы имеем дело со спамом – рассылкой коммерческой и иной рекламы или подобных коммерческих видов сообщений лицам, не выражавшим желания их получать.

Как видно из письма, проблема, скорее всего, возникла после того, как школьник ввел свой номер телефона на сайте игры.

В этом случае необходимо обратиться к оператору, предоставляющему услуги сотовой связи, и подключить опцию «блокировка отправлений с коротких номеров». Также это можно сделать в личном кабинете на сайте оператора.

Для того чтобы похожие проблемы не возникали вновь, не следует оставлять

номер мобильного телефона на незнакомых и непроверенных онлайн-ресурсах.

Кейс 5

В данном случае мы имеем дело с «мошенничеством на доверии». По статистике Фонда Развития Интернет, каждый десятый российский школьник сталкивался с кражей денег в Интернете.

Судя по письму, мошеннице удалось втереться в доверие к школьнице благодаря той личной информации, которую она могла узнать как от нее самой, так и из ее профиля в социальной сети.

Как правило, «мошенники на доверии» действуют очень осторожно и ждут удобного случая, чтобы обмануть жертву. В данном случае школьница сама спровоцировала событие, рассказав «подруге» о своем желании приобрести игровой сет.

В такой ситуации помочь школьнице очень трудно. Доказать факт мошенничества и вернуть похищенное практически невозможно, так как деньги были переданы по собственному желанию и без давления со стороны.

Единственный способ решения проблемы – это коллективное заявление в прокуратуру. В этом случае все пострадавшие лица должны собрать доказательства противоправных действий мошенницы (личная переписка, реквизиты платежей и т. д.). Можно поискать других жертв мошенницы в социальных сетях. Чем больше пострадавших подадут заявление, тем больше шансов призвать мошенника к ответственности.

Для того чтобы похожие проблемы не возникали вновь, можно предпринять следующие шаги:

* С большой осторожностью добавлять незнакомцев в друзья, даже если они являются друзьями друзей.
* С большой осторожностью вступать в переписку с незнакомцами.
* Никогда не обсуждать с незнакомцами финансовые вопросы, например, вопросы, касающиеся дорогих покупок или путешествий.