Информация для школьников

Как обнаружить ложь и остаться правдивым в Интернете

В Сети ты можешь встретить все, что угодно – от уроков истории и новостей до нелепых картинок. Но не стоит думать, что, раз информация появилась в Интернете, она является достоверной.

Чтобы разобраться, какой информации в Сети можно, а какой нельзя доверять, следуй простым советам:

- Относись к информации осторожно. То, что веб-сайт здорово сделан, еще ни о чем не говорит. Спроси себя: за что этот сайт выступает? В чем меня хотят убедить его создатели? Чего этому сайту не достает? Узнай об авторах сайта: зайди в раздел “О нас” или нажми на похожие ссылки на странице. Узнай, кто разместил информацию. Если источник надежный, например, университет, то, вполне возможно, что информации на сайте можно доверять.
- Следуй правилу трех источников. Проведи свое расследование и сравни три источника информации, прежде чем решить, каким источникам можно доверять. Не забывай, что факты, о которых ты узнаешь в Интернете, нужно очень хорошо проверить,

если ты будешь использовать их в своей домашней работе.

Как предоставлять достоверную информацию?

- Будь ответственным – и в реале, и в Сети. Простое правило: если ты не будешь делать что-то в реальной жизни, не стоит это делать в онлайне.
- Не занимайся плагиатом. То, что материал есть в Сети, не означает, что его можно взять без спроса. Если ты хочешь использовать его - спроси разрешения.
- Сообщая о неприемлемом контенте, ты не становишься доносчиком. Наоборот, ты помогаешь делу безопасности Сети.
- Когда ты грубишь в Интернете, ты провоцируешь других на такое же поведение. Попробуй оставаться вежливым или просто промолчать. Тебе станет приятнее.
- Все, что ты размещаешь Интернете навсегда останется с тобой – как татуировка. Только ты не сможешь эту информацию удалить или контролировать ее использование. Ты ведь не хочешь оправдываться за свои фотографии перед будущим работодателем?

ПОМНИ:

- Проверь хотя бы три источника информации, прежде чем ты решишь, что информация достоверна.
- И в Интернете, и в реальной жизни соблюдай правила. Агрессия, кража, обман – запрещены. Сообщай о тех, кто ведет себя подобным образом.
- Защищай себя – сейчас и в будущем. Подумай, прежде че что-либо разместить в Интернете.

Что еще почитать...

Троян-вымогатель в социальной сети “ВКонтакте” или наказание для особо любопытных

Сегодня в той или иной социальной сети зарегистрирован почти каждый. Всех пользователей подобных ресурсов можно поделить на несколько категорий. Одни выставляют напоказ всю свою частную жизнь, начиная от личных фотографий до номера телефона и адреса, другие используют настройки приватности – это делают, прежде всего, те, кто думает о собственной безопасности. Но есть еще одна негласная категория юзеров – любопытные. Именно им не терпится узнать, что скрывают закрытые странички онлайн-друзей, поэтому они и попадают в ловушки мошенников, предлагающих пошпионить в Интернете за друзьями и знакомыми, узнать тайны их личной переписки, прочитать сообщения на “стене” и просмотреть закрытые фотографии.

В социальной сети “ВКонтакте” появился новый вирус троян-вымогатель Trojan-Ransom.Win32.Vkont.a, предупреждают эксперты “Лаборатории Касперского”. Алгоритм работы троянцев-вымогателей прост и заключается в блокировании работы компьютера с целью получения денег злоумышленниками. Для этого пользователю предлагается отправить СМС-

сообщение на короткий номер в обмен на пароль для восстановления данных или нормальной работоспособности компьютера. Для России проблема “блокеров” является наиболее актуальной. По данным “Лаборатории Касперского”, ежедневно с такими вредоносными программами сталкиваются несколько тысяч российских пользователей и не только при пользовании соцсетью, но и при скачивании сомнительных фильмов, когда указывается, что на просмотр фильма дается час бесплатного времени. При истечении определенного времени, компьютер «киномана» также блокируется.

В “Контакте” это выглядит обычно так: любопытному пользователю предлагают пройти по ссылке на сайт, который на самом деле мошеннический, и там узнать все интересующие его тайны. На этом сайте предлагается скачать ПО для взлома учетных записей в социальной сети “ВКонтакте”. Однако после клика на кнопку загрузки под видом “программы-взломщика” начинается скачивание троянца-вымогателя, естественно о подмене ничего не сообщается.

После этого, на Рабочем столе компьютера появляется окно с предложением отправить СМС-сообщение на короткий номер, чтобы получить программу для доступа к личным данным пользователей сети “ВКонтакте”. Одновременно троянец блокирует работу системы до тех пор, пока вымогатели не получат выкуп в виде СМС.

Но при отправке СМС, пользователь оказывается дважды “наказан” злоумышленниками. Троянец скачает архив VK-Hack.zip, в котором находятся программа для подбора паролей к аккаунтам в популярных почтовых сервисах, а также ПО класса ShareWare, за полноценное использование которого необходимо заплатить дополнительно. Таким образом, жертва уловки мошенников не только оплачивает отправку дорогостоящей СМС-ки, но и получает совсем не бесплатные программы сомнительного функционала. Лаборатория Касперского рекомендует при обнаружении СМС-блокера на компьютере не идти на поводу у мошенников и не отправлять сообщения, а удалить назойливый баннер с Рабочего стола с помощью бесплатного сервиса на сайте “Лаборатории Касперского”. Данная услуга доступна также и через мобильное устройство. Информация о том, как осуществить поэтапно удаление баннера с рабочего стола для разблокировки Windows, приводится ниже.

Сервис Deblocker бесплатный. С его помощью можно убрать баннер (рекламный модуль) с рабочего стола, разблокировать Windows без отправки смс или перевода денег на счет, вернуть зашифрованные вирусом файлы.

Чтобы удалить баннер, надо ввести в первое поле номер телефона (например, 84444, 3116, 89854120769, 89162095847) или счета (например, 9636256259). Если у вас есть текст смс, который блокеры-вымогатели просят отправить на указанный номер, введите его во второе поле.

Для получения кода разблокировки должно быть заполнено хотя бы одно из полей. Подробная инструкция.

После удаления баннера проверьте компьютер на наличие вирусов с помощью бесплатной утилиты Kaspersky Virus Removal Tool. Для предотвращения заражения вашего компьютера мы рекомендуем установить Kaspersky Internet Security 2011. Скачать бесплатную 30-дневную версию.
Если вы разместите ссылку на сервис разблокировки на своем сайте или в блоге, вы поможете в борьбе с вымогателями. Получить код разблокировки
И напоследок, о проделках интернет-мошенников можно говорить долго, но не следует забывать и об ответственности пользователя, ведь он по своей воле переходит по опасным ссылкам, подписывает какие-то соглашения. В результате чего и страдает сам. Так что будьте бдительны!