There are no translations available.

Общие рекомендации по борьбе с СМС-вымогателями.

Принимая во внимание то, что в последние несколько месяцев эпидемия СМС-вымогателей значительно выросла, некоторые общие рекомендации по борьбе с этой заразой, а также ответы на наиболее частые вопросы.

Я уже не говорю про разновидности с порнографическим содержанием. Суть одна и та же: Вы не можете работать на компьютере, он заблокирован и по каким-то предлогам у Вас просят отправить СМС.

Сразу отмечу, что никакая из мировых компаний, занимающихся программным обеспечением (Microsoft, Лаборатория Касперского и т.д.) таким образом не взымает плату или штрафы за использование нелицензионных программных продуктов! То, на что ссылается вредонос в окне — полная чушь!

Если всё-таки у Вас произошло заражение, то учтите следующее.

НИКОГДА не шлите смс на номер! Бывали случаи простого «развода» — деньги снимались, а код не приходил. В крайнем случае выясните у оператора, какой службе принадлежит короткий номер, позвонит в поддержку и поругайтесь. Ключевые слова-пугатели: «блокировка работы компании», «рассылка порнографических картинок», «я сделал фото компьютера и обращусь в милицию». Код должны дать бесплатно.
ВСЕГДА после удачной разблокировки (ресурсов для этого есть несколько, рекомендуется этот, этот или вот этот) обращайтесь сюда или сюда. Вам нужно будет сделать логи, и специалисты проверят наличие остатков вируса. Очень часты случаи, что и после удаления блокирующего окна остаются «хвосты», которые нужно подчищать, в противном случае вредоносная активность остаётся.
ВСЕГДА после удаления СМС-вымогателя меняйте все пароли, потому что имеется ряд косвенных указаний на то, что кроме блокировки вымогатель ещё и ворует пароли.
Использовать самостоятельное удаление различными «утилитами», распространёнными на сомнительных источниках в Сети КРАЙНЕ НЕЖЕЛАТЕЛЬНО: Вы можете занести ещё больше зловредов или по ошибке окончательно угробить систему.

В крайнем случае, когда ничего не помогает, напишите на один из двух ресурсов, которые я указал в п.2, описав проблему. Вам обязательно постараются помочь!
Ну и САМОЕ ГЛАВНОЕ: легче предотвратить заражение, чем его вылечить, а потому...

Никогда не запускайте файлы, в которых не уверены. Если очень хочется — предварительно проверьте их хотя бы на VirusTotal и при малейшем подозрении — отошлите антивирусным вендорам на проверку.
Устанавливайте программное обеспечение, только скачанное с официальных сайтов производителя! Adobe Flash Player качается на сайте Adobe, а не там, где Вам его предлагают.
Своевременно обновляйте Вашу систему и используемые программы. Желательно отказаться от использования браузера Internet Explorer. Большинство зловредов устанавливается без ведома пользователя при работе в Интернет, благодаря уязвимостям в Internet Explorer, Adobe Flash Player, Adobe Acrobat и самой Windows.
Используйте хотя бы антивирус, не выключая его «потому что тормозит». Если тормозит — разберитесь в настройках, решите проблему! И безусловно своевременно обновляйте антивирусные базы! В идеале желательно антивирус подкрепить системами HIPS и файервола. Кстати — при желании это можно сделать бесплатно, достаточно просто поискать бесплатные программы подобного рода в Сети. Но будьте осторожны: не устанавливайте программное обеспечение, о котором нет отзывов и о котором никто ничего не слышал — это может быть элементарная подделка, зачастую, вредоносная. На нашем форуме достаточно много обсуждений программ по безопасности, некоторые — бесплатны, и Вы легко можете ознакомиться с отзывами о них.
Ну и под конец — популярная рубрика «Ответы на самые гневные вопросы»
1. «Куда смотрят производители антивирусов и за что мы платим?»
Производители антивирусов очень тщательно работают над решением проблемы. Реально по алгоритму работы, СМС-вымогателей не так уж и много, однако вирусописатели постоянно перепаковывают файлы и изменяют код, чтобы избавляться от детекта. Если полностью код вредоносной программы происходит не чаще одного раза в неделю-несколько, то перепаковка происходит более трёх-пяти раз в сутки. Поэтому антивирусные лаборатории могу просто не успеть добавить детект на перепакованную версию, а за этот малый промежуток многие успевают заразиться (собственно, чтобы этого не случилось, выше приводятся превентивные меры).

2. «Почему силовые структуры не работают с контент-провайдерами, предоставляющими короткие номера?»

За силовые структуры никто ответить не сможет, кроме самих силовых структур. Можно только предполагать. Скорее всего, что к ним просто никто не обращается? То же самое касается и контент-провайдеров. В любом случае, на этот вопрос скорее Вам

дадут ответы именно представители этих организаций, а не мы.

3. «Дайте нам универсальный скрипт для лечения заразы» или «А я использовал скрипт из такого-то сообщения, потому что там симптомы у человека были такие же, как у меня. Не помогло!!!»

Универсального скрипта нет и не будет, иначе бы наша команда тут не сидела, ресурса ВирусИнфо бы не существовало, антивирусные вендоры бы обанкротились, вирусописатели бы застрелились, а Олег Зайцев получил бы Нобелевскую премию (или несколько) Каждый случай — уникальный. И каждый требует индивидуального подхода. Использовать чужие скрипты даже при абсолютно одинаковых симптомах — бессмысленно и даже вредно! А потому, чем гадать на кофейной гуще — опишите свою проблему, там и так, как я писал выше. Даже если у Вас не запускается AVZ и вообще ничего не работает, кроме зловреда — Вам обязательно постараются помочь! И в большинстве случаев — успешно.
Удачи и не болейте (ни реально, ни виртуально)!

http://virusinfo.info/showthread.php?t=68235