Уважаемые дамы и господа!

Любой человек, который работает с компьютером, ноутбуком или планшетом знает о том, что вирусов огромное множество баннеры, которые устанавливаются у вас на рабочем столе и их не возможно поменять, блокираторы которые требуют денег за разблокировку компьютера, вирусы повреждающие файлы и т.д. перечислять можно до бесконечности.

В последнее время самыми часто встречающимися и опасными стали вирусы-шифровальщики. Попадая на компьютер, они шифруют файлы, как правило это документы word, excel, изображения в различных форматах, базы данных 1С. Код для дешифровки отправляется создателю данного вируса, а пользователю приходит требование заплатить N-ую сумму денег (от 10.000 рублей и выше) за предоставление кода для расшифровки ваших данных.

Опасность заражения:

1. Как правило вирусы-шифровальщики обладают свежим вредоносным кодом, который не распознается антивирусами на момент заражения компьютера, т.е. вирус без препятствий попадает на компьютер.

2. Заражение компьютера происходит с использованием психологической составляющей:

Пример1- В отдел кадров приходит письмо в прикрепленным файлом «Резюме» сотрудник не задумываясь открывает прикрепленный файл в нем находится вирус.

Пример2-На почту приходит письмо якобы от правоохранительных органов, судов, налоговых и т.д. с прикрепленным файлом «Постановление», «Предписание», «Решение» и т.д. человек начинает нервничать и не задумываясь открывает прикрепленный файл, в котором вирус.

3. Вероятность самостоятельной расшифровки без обращения в тех. поддержку антивирусов практически не возможна.

4. Даже при обращении в техническую поддержку вероятность расшифровки в некоторых случаях маловероятна или не возможна. Статистика dr.web по расшифровке http://antifraud.drweb.ru/encryption_trojs/

5. При уплате денежных средств злоумышленникам нет гарантии расшифровки файлов.

Меры безопасности для предотвращения заражением вирусами шифровальщиками так и большей частью других вирусов:

1. Повышать компьютерную грамотность конечных пользователей.
2. Устанавливать на компьютер антивирусные программы, обновлять базы антивирусов.
3. Работать на компьютере под учетными записями с ограниченными правами.
4. Делать резервные копии данных, и хранить резервные копии отдельно от копируемой информации, что бы даже в случае повреждения основных данных резервные копии не пострадали.
5. Не открывать письма, а тем более вложения, которые вызывают подозрение.
6. При работе с почтой быть внимательным к адресам, с которых вам пришло письмо. Письма, рассылаемые с вирусами от государственных организаций, используют отличные от них адреса электронной почты (отличие может быть в одном символе).
7. Не устанавливать программы, полученные из неизвестных источников.
8. При работе в среде интернет использовать дополнительные инструменты блокирующие рекламу, java-скрипты и несанкционированные запросы.

Меры принимаемые в случае заражения вирусом-шифровальщиком:

1. Если вы заметили, что файлы на вашем компьютере начали шифроваться вирусом, НЕМЕДЛЕННО выключите компьютер. (Процесс шифровки это, сложная математическая операция она не происходит мгновенно, отключение компьютера возможно спасет часть ваших данных.
2. Обратится в техническую поддержку антивирусной компании и следовать их указаниям.

Что нельзя делать если ваши фалы зашифрованы, и вы хотите их восстановить:

1. Проверять компьютер на наличие вирусов. т.к. если антивирус удалит вирус или его последствия специалистам тех. поддержки антивируса будет намного сложнее определить, как расшифровать ваши дынные.
2. Самостоятельно без согласования со специалистами тех. поддержки антивируса пользоваться дешифровщиками. Они могут изменить ваши файлы и после этого их можно вообще не восстановить.
3. Вносить какие-либо изменения в файлы, в том числе менять имя или расширение.
4. Переустанавливать операционную систему до обращения в тех. поддержку антивируса.

В заключении ссылки на двух самых крупных разработчиков антивирусного программного обеспечения в которых освещена проблема вирусов шифровальщиков.
http://antifraud.drweb.ru/encryption_trojs/
http://forum.kasperskyclub.ru/index.php?app=blog&module=display&section=blog&blogid=345&showentry=1920