Памятка о вирусах.

Уважаемые коллеги! Будьте внимательны! В последнее время в сети интернет все чаще встречаются различные компьютерные вирусы-шифровальщики! Вирус зашифровывает все доступные на локальных и сетевых дисках компьютеров документы, картинки и архивы, делая их нечитаемыми с целью вымогательства денег за расшифровку файлов. Расшифровать файлы без ключа от вымогателей – невозможно. При этом часто программа-антивирус пропускает вирус, так как для внесения вируса в базу данных программы-антивируса нужно время (несколько часов или даже десятков часов). К сожалению способов лечения от этих вирусов в настоящее время нет!

В большинстве случаев вирус распространяется через электронную почту, маскируясь под вполне обычные письма. Наиболее популярные содержания таких писем: уведомление от арбитражного суда об иске, исполнительное производство о взыскании задолженности, уведомление из налоговой, акты и договоры, информация о покупках, судебные разбирательства, кредиты, - бухгалтерские документы (счета, акты, счёт-фактуры). Если в подобных письмах присутствуют ссылки, то почти гарантированно по ссылке находится вирус. Нельзя переходить по ссылкам, скачивать и открывать файлы и т. д. Скачивая и открывая такой файл, пользователь, сам того не понимая, запускает вредоносный код. Вирус последовательно шифрует нужные файлы, а также удаляет исходные экземпляры методами гарантированного уничтожения (чтобы пользователь не смог восстановить недавно удаленные файлы с помощью специальных средств).

Важно отметить, что письма содержащие вирусы могут приходить и от известных вам отправителей!

Вирус в письме может быть:

1) **в виде ссылки в тексте письма;**
2) **в прикреплённых файлах.**

Часто вирус находится внутри архива (RAR, ZIP или другие) и имя файла с расширением становится видно только после раскрытия архива или распаковки на диск. В ряде случае, даже просто раскрытие архива или его распаковка запустит вирус.

Если к письму прикреплены файлы, нужно обратить внимание на значок файла и расширение файла. Нельзя открывать файлы с незнакомыми значками и расширениями. Расширение файла указывает на тип файла и начинается после точки в конце имени. Мошенники могут пользоваться такой хитростью: указывают в имени файла известное расширение и

добавляют уже окончательное расширение. Например, «Договор на поставку.doc.exe» не является документом Word, которые имеют расширение «.doc».

Примеры потенциально вредоносных расширений:

.exe
.bat
.cmd
.scr
.js и другие.

Примеры расширений, под которые наиболее часто маскируют вредоносную программу:

.doc Word 2003
.docx Word 2007
.xls Excel2003
.xlsx Excel 2007
.pdf Acrobat Reader
.jpg Картинка

При этом вредоносными могут оказаться не только файлы перечисленных выше форматов. Специалистами Лаборатории Касперского зафиксированы случаи заражения компьютеров при открытии специально сформированных злоумышленниками файлов форматов DOC и PDF.

Профилактика:

1) Ежедневно проверяйте на предмет установленных обновлений ваш антивирус. Если обновления не устанавливаются в автоматическом режиме, то необходимо проинформировать об этом сотрудников управления информационных технологий ***Костина Федора, Каковкина Александра, Николаева Александра.***
2) Делайте резервные копии всей важной информации на внешние носители или сетевые диски.
3) Рассматривайте все деловые и личные письма, как потенциально опасные. Поле «От кого» ничего не значит. Если у вашего знакомого вирус, то этот вирус может отправлять свои копии по всем адресам, имеющимся в адресной книге. Если возникают сомнения, удаляйте.
4) Не открывайте в сообщениях электронной почты подозрительные присоединенные файлы, даже если они поступили от известных отправителей.

5) Будьте осторожны с письмами без текстового содержания, имеющими только ссылку или приложение во вложении.
6) Не нажимайте на ссылки или вложения, если они не ожидались вами от этого отправителя. Если не уверены, то лучше позвоните отправителю.
7) Обо всех подозрительных письмах (особенно, если к письму приложен архив), сообщайте системному администратору.

Если вы все-таки открыли подозрительное вложение\архив из письма и у вас не прочитался файл из архива или система выдала ошибку после его запуска или вовсе визуально ничего не произошло, то:

1. Никогда не пересылайте этот файл другим пользователям с просьбой открыть! Так вы можете распространить вирус!
2. Быстро выключите свой компьютер.
3. Сообщите о проблеме в управление информационных технологий.

Уважаемые коллеги, будьте бдительны, ведь внимательность — один из самых эффективных методов предотвращения угрозы.