ЗАЩИТА ОТ ВРЕДОНОСНЫХ ПРОГРАММ-ШИФРОВАЛЬЩИКОВ

Программы-шифровальщики – это разновидность вирусных программ, которые, попадая на Ваш компьютер, шифруют все файлы, а затем предлагают выплатить злоумышленнику определенную сумму денег за их расшифровку.

Как вредоносная программа-шифровальщик может проникнуть в Ваш компьютер?

В большинстве случае программы-шифровальщики приходят по электронной почте в виде вложения в электронное письмо от неизвестного отправителя или якобы от имени судебных органов, банковских или других организаций, наименование которых всем известно.

При открытии этих вложений и происходит запуск программы-шифровальщика.

Чаще всего вложения бывают в архивных файлах с расширениями: **.zip, .rar, .7z**

Краткий список «опасных» расширений файлов, за которыми может быть спрятан вирус-шифровальщик:

.exe, .com, .js, .wbs, .hta, .bat, .cmd, .vbs, .scr

Зараженный файл может иметь имя с видимым ложным расширением и множеством других символов. Например:

Акт.doc…….exe

Накладная.doc……exe

Если видна только часть имени **Акт.doc**, то Вы думаете, что это word-файл, открываете его и тем самым запускаете вредоносную программу.

Вы получаете по электронной почте обычный word-файл, внутри которого помимо текста есть какой-либо встроенный объект: изображение, гиперссылка на сайт в Интернете. При нажатии на такой объект происходит незаметное заражение вирусом-шифровальщиком.

Проникновение вредоносной программы-шифровальщика на Ваш компьютер возможно также при скачивании из Интернета каких-либо программ, файлов с неизвестных сайтов.

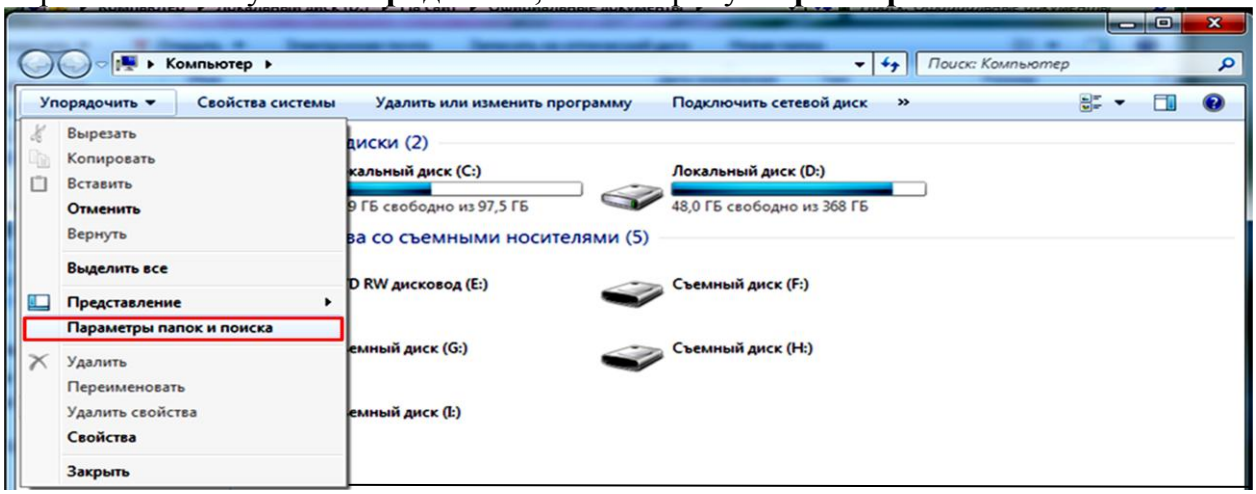
Заражение вредоносной программой возможно также со съемного диска (флэш-носителя), особенно не проверенного антивирусной программой.

Как не допустить заражения вредоносной программой-шифровальщиком?

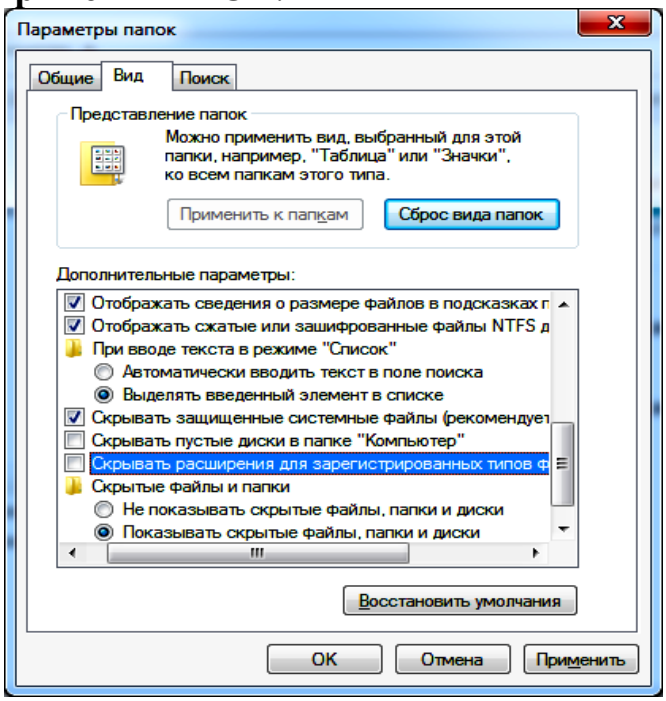
1. Относиться подозрительно к электронным письмам, полученным от неизвестного отправителя. Никогда не открывать для просмотра вложения в письмах от незнакомых людей или организаций.
2. Своевременно обновлять антивирусные базы. Но и нельзя всецело полагаться на антивирусную программу.
3. Регулярно делать резервные копии документов на внешние носители информации.
4. Обязательно проверять расширения всех вложенных файлов, даже если письмо пришло от известного отправителя. Если заметили «опасные» расширения файлов, ни в коем случае не открывайте их.
5. Включить отображение расширения в имени файла.

Для этого в Windows 7:

1) Открыть любую папку
2) Выбрать в меню пункт **Упорядочить**, затем строку **Параметры папок и поиска**

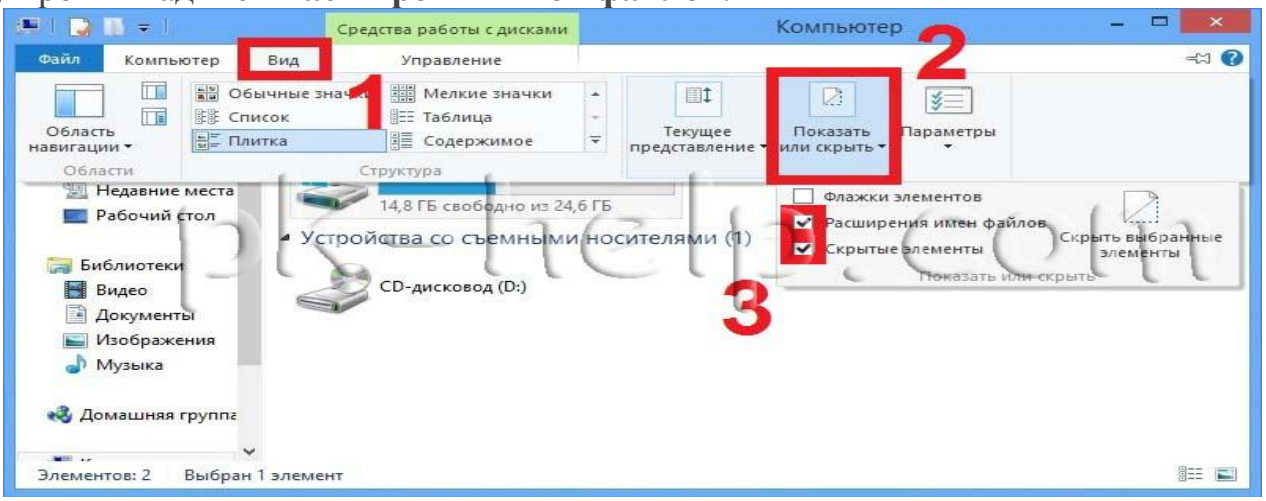


3) В окне **Параметры папок** выбираем вкладку **Вид**
4) В дополнительных параметрах находим строку **Скрывать расширение для зарегистрированных типов файлов**, убираем галочку перед ней.
5) Нажимаем кнопки **Применить** и **ОК**.



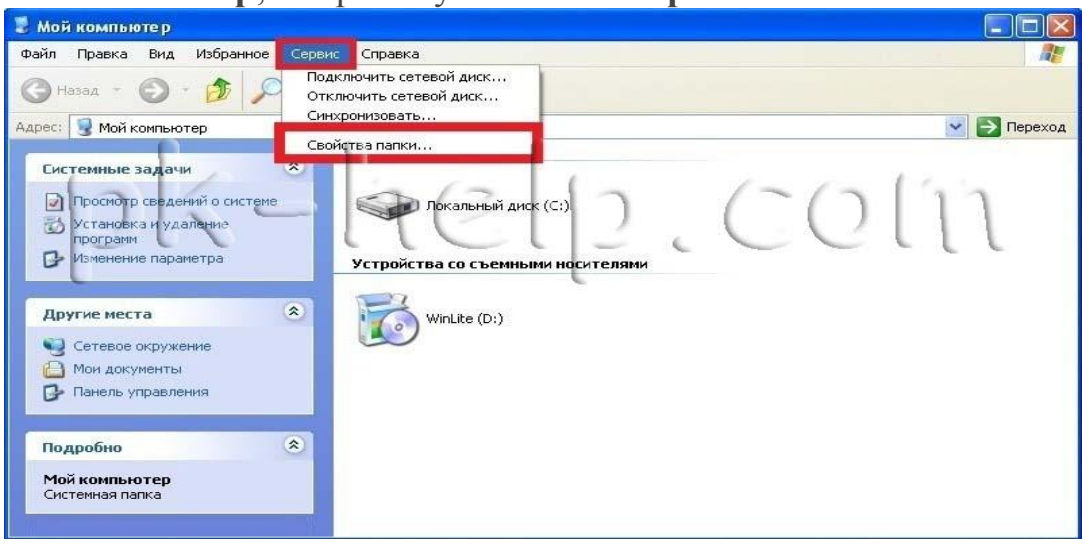
В Windows 8:

Открываем любую папку. В строке меню выбираем **Вид** – **Показать или скрыть** и ставим галочку против надписи **Расширения имен файлов**.

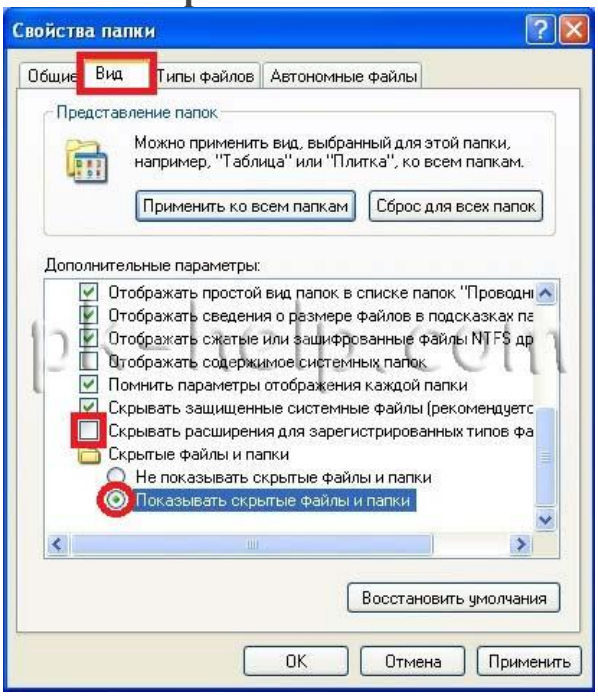


В Windows XP:

Открыть **Мой компьютер**, выбрать пункт меню **Сервис - Свойства папки**.

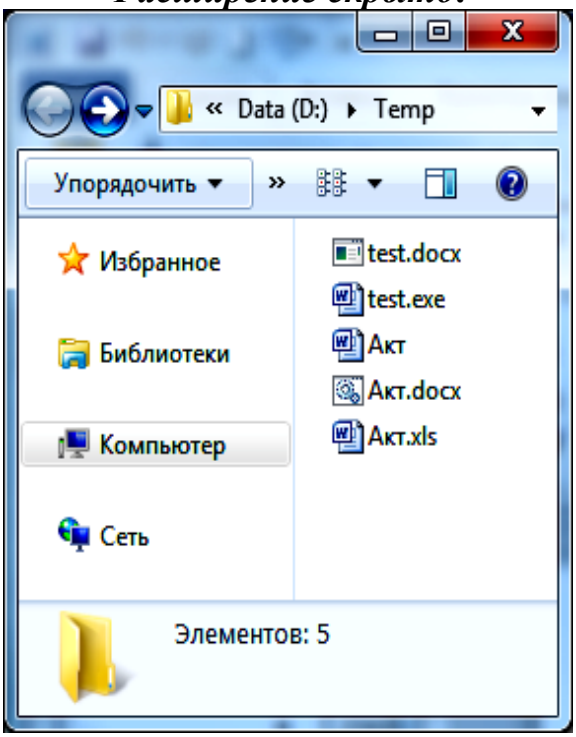


В открывшемся окне свойств папки убрать галочку **Скрывать расширение для зарегистрированных типов файлов**. Нажать **Применить** и **ОК**.

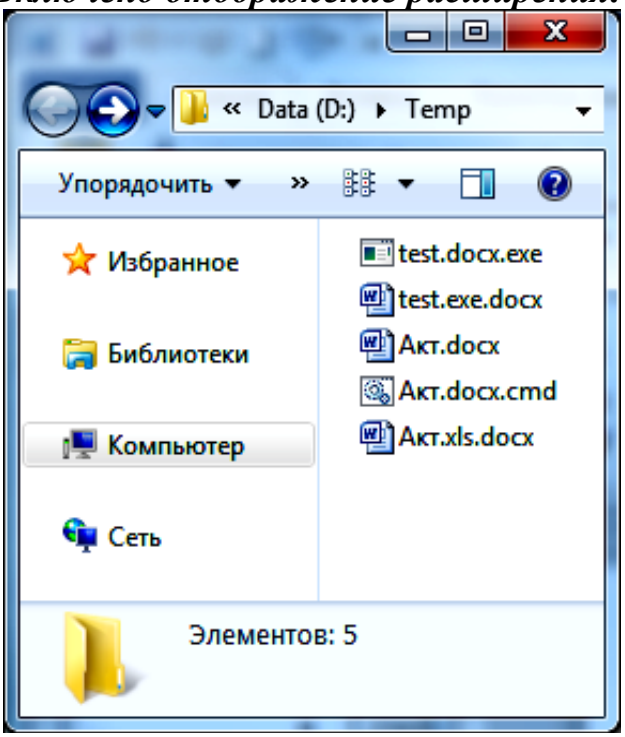


Примеры зараженных файлов:

Расширение скрыто:



Включено отображение расширения:



В случае запуска программы-шифровальщика необходимо **НЕЗАМЕДЛИТЕЛЬНО**:

1. Отключить электропитание компьютера (без корректного завершения сеанса и без сохранения всех результатов) вплоть до физического отключения питания от электросети.
2. Поставить в известность о данном факте своего непосредственного руководителя, системного администратора.

Помните!

Один из самых эффективных методов предотвращения угрозы запуска вредоносной программы – Ваша внимательность!

Запустить выполнение программы-шифровальщика может только сам пользователь. Повышенная бдительность и внимание к вновь появившемся файлам на компьютере и аккуратное обращение с ними поможет не допустить заражения и последующего блокирования файлов на компьютере и в сети организации