ВНИМАНИЕ ПЕДАГОГАМ!

Уважаемые пользователи!

Доводим до вашего сведения, что злоумышленниками рассылаются поддельные письма с вирусами-шифровщиками, которые после запуска на компьютере настолько сильно портят офисные документы и базы данных, что ими становится невозможно пользоваться.

Шифрование файлов – как способ вымогательства денежных средств, стало очень популярным за последний год. Злоумышленники рассылают вредоносное ПО под видом писем, отправленных от имени:

- судебных приставов, арбитражных судов («…против Вас начато исполнительное производство…»);
- банков, коллекторских агентств («…у банка «XXX» для Вас специальное предложение; у Вас задолженность по кредиту…»);
- иных органов исполнительной власти;
- сайтов государственных услуг;
- родственников;
- другого рода.

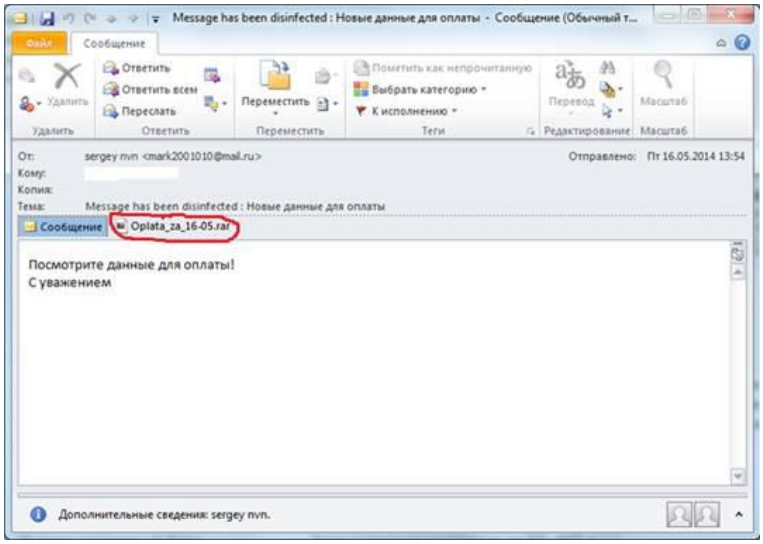
Злоумышленники могут располагать рядом дополнительной информации о Вас, такой как: фамилия, имя, отчество, место работы и должность, номер телефона, номер банковской карточки и т.п., и, соответственно, обращаться к Вам, используя персональные данные, что в свою очередь вызывает у вас ощущение доверия к отправителю.

Такие письма могут прийти как на официальные почтовые ящики (i.o.familiya@oiv.rkomi.ru<mailto:i.o.familiya@oiv.rkomi.ru>), так и размещенные на бесплатных почтовых серверах (@mail.ru, @gmail.com и т.п.).

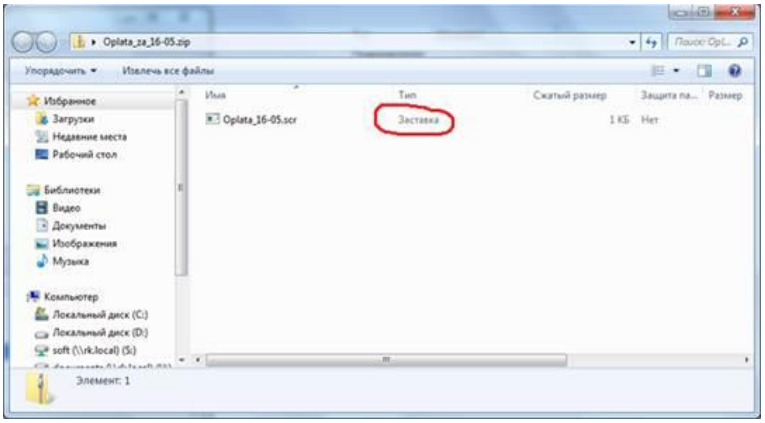
К сожалению, *антивирусные программы не могут своевременно обнаружить вирусы-шифровщики, пока таковые не будут занесены разработчиками антивирусных продуктов в соответствующие базы.*

Приводим ПРИМЕР одной из последних рассылок вируса.

1. Шифровщики рассылаются по видом счетов на оплату.
2. К письму с темой Новые данные для оплаты, приложен архив Oplata_za_16-05.rar.



3. В этом архиве содержится файл Oplata_16-05.scr — этот файл поддельный.



4. Если вы не обратите внимание на то, что в столбце «Тип» у второго файла указано «Заставка» (что в операционной системе Windows равносильно «Приложению»), а не относительно безопасные «Типы», такие как: «Документ Microsoft Word», «Таблица Microsoft Excel», «Текстовый документ», «PDF-документ», «Изображение», и откроете этот файл, то вирус незаметно зашифрует все файлы. Сначала на общих сетевых дисках (чтобы принести максимальный урон), затем — на вашем личном компьютере.

В связи с вышеуказанным, руководствуясь Постановлением Правительства Республики Коми № 506 от 31 декабря 2010 года «О региональном операторе безопасности инфраструктуры электронного правительства в Республике Коми», ГБУ Республики Коми «ЦБИ» требует соблюдения следующих правил:

1. Не посещать на служебном компьютере не связанные с выполнением служебных обязанностей сайты (Яндекс-Почта, Google Mail, Mail.ru, ВКонтакте, Youtube и т.п.). Личную почту читать дома.
2. Не использовать на рабочем месте не связанные с выполнением служебных обязанностей программы (Skype, ICQ, радио, видео и т.п.).
3. Не пытаться устанавливать программы самостоятельно, даже при наличии компетенции в данном вопросе.
4. Всегда проверять отправителя электронного письма, дозвонившись до него и уточняя, действительно ли он направил Вам это письмо, не открывая никакие вложенные файлы и не переходя ни по каким ссылкам. Злоумышленники обязательно вышлют Вам вирус в тот момент, когда Вы ждете похожее сообщение. И обязательно подделают его под сообщение «с сайта», на рассылку с которого Вы ранее подписались.

Компьютерно-информационный центр ГПОУ «ВПТ»