ВНИМАНИЕ, ВРЕДОНОСНЫЕ ВИРУСЫ!

Сообщаем, что в последнее время возросла активность лиц, занимающихся изготовлением и распространением вредоносного программного обеспечения (вирусов). Наиболее тиражируемым и рассылаемым путём «веерной рассылки» вредоносным программным обеспечением (вирусом) является «шифратор» - вирус, который блокирует доступ к документам на компьютере пользователя путём их шифрования и начинает вымогать с пользователя деньги за некий код (пароль) для расшифровки.

Самым распространённым способом доставки такого вируса до пользователей является отправка по электронной почте вложенного файла, содержащего вредоносный код. Для заражения компьютера требуется, чтобы пользователь открыл указанный файл.

Злоумышленники используют различные ухищрения для того, чтобы побудить пользователя открыл файл: разрабатывают специальные тексты писем, пишут их от имени органов государственной власти (государственных органов), в том числе контрольно-надзорных органов, предлагают товары (услуги) по особым ценам, информируют об имеющейся задолженности, о направлении актов сверки и иных финансовых документов, сообщают о попавших в беду близких или пишут от их имени и т.п.

Правила безопасности:

1. Если вы получили письмо с вложенным файлом, не следует сразу открывать его! Прежде чем это делать, убедитесь в надёжности источника и безопасности вложения.

2. Обратите внимание на адрес и подпись отправителя. Если адрес явно не соответствует подписи (например, письмо с адреса ivanov@nalog.ru, а в подписи написано Петров Пётр Петрович), это наверняка письмо с вирусом.

3. Если это известный вам человек, уточните у него действительно ли он направил вам письмо с вложенным файлом, и если не отправлял – не открывая вложения сообщите о получении такого письма ответственному за информационную безопасность в организации.

4. Если отправитель вам неизвестен, но содержание письма представляет интерес, не открывая файл напишите ответ (с помощью кнопки «Ответить») адресату и задайте ему любой уточняющий вопрос. Если это

письмо от злоумышленников, ответа вы, скорее всего, не получите, а, возможно, и ваше письмо вернётся с пометкой «не удаётся доставить», либо с вами свяжется автор письма, который с недоумением сообщит, что он вам ничего не отправлял. Также вы можете попробовать связаться с отправителем письма по представленным им контактным данным и уточнить у него информацию об отправке письма и содержании вложений. Отсутствие в письме контактной информации, один из признаков того, что это письмо от злоумышленников. Настоящий сотрудник государственного органа или организации-контрагента не заинтересован скрывать контактную информацию.

5. При любых сомнениях в безопасности вложенного файла, даже если вы убедились в надёжности источника, не открывайте его, сообщите о своих сомнениях ответственному за информационную безопасность в организации.

6. **Не открывайте на рабочем ПК файлы, полученные по электронной почте на личные адреса с использованием веб-интерфейса, даже если это необходимо в служебных целях, если у вас нет уверенности в их безопасности**. Сделайте это на личном компьютере, если вы полагаете, что информация может представлять интерес, или выполните пересылку себе на рабочий адрес электронной почты. Если при пересылке письмо пришло без вложения или не пришло вообще, скорее всего, письмо содержало вирус.

Примечание. Как показывает практика, новые вредоносные программы и новые механизмы рассылки спама появляются на некоторое время (несколько часов или дней) быстрее, чем механизмы, позволяющие с ними бороться. Поэтому полностью полагаться только на автоматические фильтры нельзя.