Безопасность при пользовании электронной почтой

Как проверить ссылку из письма на предмет троянского кода

Уважаемые пользователи!

Уходящий год запомнится и простым пользователям, и специалистам по информационной безопасности широким распространением числа новых вредоносных программ. Как правило, рекордной отметки вирусная активность достигает к концу года, а именно, увеличением числа заражений троянскими программами, шифрующими файлы на автоматизированных рабочих местах и серверах.

Были зафиксированы заражения автоматизированных рабочих мест при получении электронной почтой писем с адресом отправителя из почтового домена Сбербанка sberbank.ru и ФНС России (Федеральная налоговая служба) nalog.ru которые требуют от пользователей каких-либо действий.
ФНС России не используют для электронного взаимодействия с налогоплательщиками электронную почту. Всю информацию о наличии задолженностей можно получить с помощью интернет-сервисов на сайте ФНС России.
Сбербанк не рассылает такого рода писем, поэтому недопустимо открывать почтовые вложения в таких письмах и переходить по интернет-ссылке.

В остальных (общих) случаях:

1. Недопустимо открывать почтовые вложения от неизвестных отправителей, если у пользователя нет уверенности в безопасности этого вложения.
2. Недопустимо переходить по указанной в тексте письма интернет-ссылке с неизвестным адресом, если у пользователя нет уверенности в безопасности этой интернет-ссылки. Особое внимание следует уделить ?тревожным? письмам, требующим незамедлительной реакции.
В случае возникновения подозрений в небезопасности интернет-ссылки возможно воспользоваться сервисом «Онлайн сканер», расположенным по адресу http://vms.drweb.ru/online/?lng=ru.
3. Если пользователь не уверен в подлинности и безопасности письма, то необходимо проконсультироваться с должностным лицом, ответственным за защиту информации в организации или администратором Центра управления системой защиты информации информационно-телекоммуникационных систем исполнительных органов государственной власти Санкт-Петербурга (далее — ЦУ СЗИ ИТКС ИОГВ СПб).
4. Необходимо своевременно и регулярно создавать резервные копии всех важных документов на внешних носителях информации.