**Уважаемые коллеги!**
**Просьба ознакомиться с информацией, поступившей из Управления ФСТЭК России**

**по Сибирскому федеральному**

**округу**

Анализ сведений об угрозах безопасности информации, проводимый специалистами ФСТЭК России в условиях сложившейся обстановки, показывает, что с подменного почтового адреса fstek.info@mail.ru в адрес федеральных органов исполнительной власти, субъектов критической информационной инфраструктуры и организаций Российской Федерации направляются фишинговые письма от имени ФСТЭК России, содержащие вредоносные вложения (архив .72), с помощью которых осуществляется распространение вредоносного программного обеспечения типа «троян» (HEUR:Trojan.Win32.Autoit.gen, HEUR:Trojan.BAT.Obfus.gen).

Официальным почтовым ящиком ФСТЭК России, с которого осуществляется рассылка электронных писем, являются адреса электронной почты с наименованием домена @fstec.ru.

С целью предотвращения реализации угроз безопасности информации, связанных с фишингом, необходимо:

— проверять адрес отправителя, даже в случае совпадения имени с уже известным контактом;

— проверять письма, в которых содержатся призывы к действиям (например, «проинструктировать», «открыть», «прочитать», «ознакомиться», «дать ответ»), а также с темами про финансы, банки, геополитическую обстановку или угрозы;

— осуществлять проверку всех поступающих на почту вложений с использованием средств антивирусной защиты, антиспама (при наличии).

Обновить базы антивирусных средств защиты до актуальных версий.