Автор:
15.11.2007 04:31

Office 27 предлагает несколько способов защититься от атак вредоносных программ.

1) Удостоверьтесь в том, что включена опция обнаружения макросов, элементов Active X, надстроек и кодов VBA.

Чтобы защитить свой компьютер от воздействия вредоносных программ, используйте Центр управления безопасностью.

Центр управления безопасностью, проверяя на надежность издателей и расположения кодов на вашем компьютере и обеспечивая контроль безопасности для надстроек, элементов управления Active X и макросов, гарантирует более надежную защиту компьютера. При обнаружении небезопасного элемента Центр управления безопасностью выводит на экран сообщение с предупреждением.

2) Удостоверьтесь в том, что вы включили функцию обнаружения поддельных Web-сайтов.

Используйте Центр управления безопасностью, чтобы защитить свой компьютер от атак с поддельных Web-сайтов. Параметр Проверка документов Microsoft Office, взятых с подозрительных веб-узлов или содержащих ссылки на такие веб-узлы в группе Параметры конфиденциальности раздела в Центр управления безопасностью, установлен по умолчанию, поэтому Центр управления безопасностью постоянно проверяет все доменные имена. Центр управления безопасностью также выведет на экран предупреждение о том, что вы открыли документ, который содержит ссылку на ненадежный Web-сайт, или собираетесь открыть файл, размещенный на Web-сайте, адрес которого, возможно, является поддельным доменным именем.

3) Будьте осторожным при открытии вложений в сообщениях электронной почты.

Итак, вы получили сообщение электронной почты. Не торопитесь открывать и запускать вложенный в него файл. Открывать такие файлы можно, только если вам известен отправитель письма, и вы знаете, что содержится во вложении. Если письмо кажется вам подозрительным - удалите его. Диспетчер вложений поможет вам проверить файл, который вы собираетесь открыть. Дополнительную информацию об этом вы можете получить в Справке Microsoft Outlook