Warnings in Microsoft Office Apps about Macros and Add-Ins

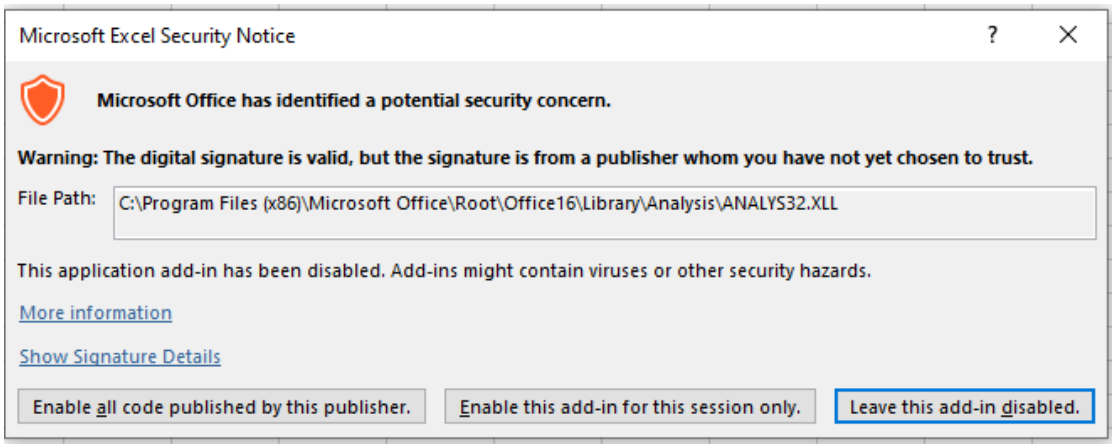
David Raco - 2023-02-07 - Comments (0) - Desktop Security

In February 2023, we rolled out more restrictive security settings designed to protect the campus from malicious Office add-ins and macros that can infect your computer with malware. As a result of these settings, you might encounter the following warning dialogues in Microsoft Office applications. This article will make sure you know what to do if and when you see them.

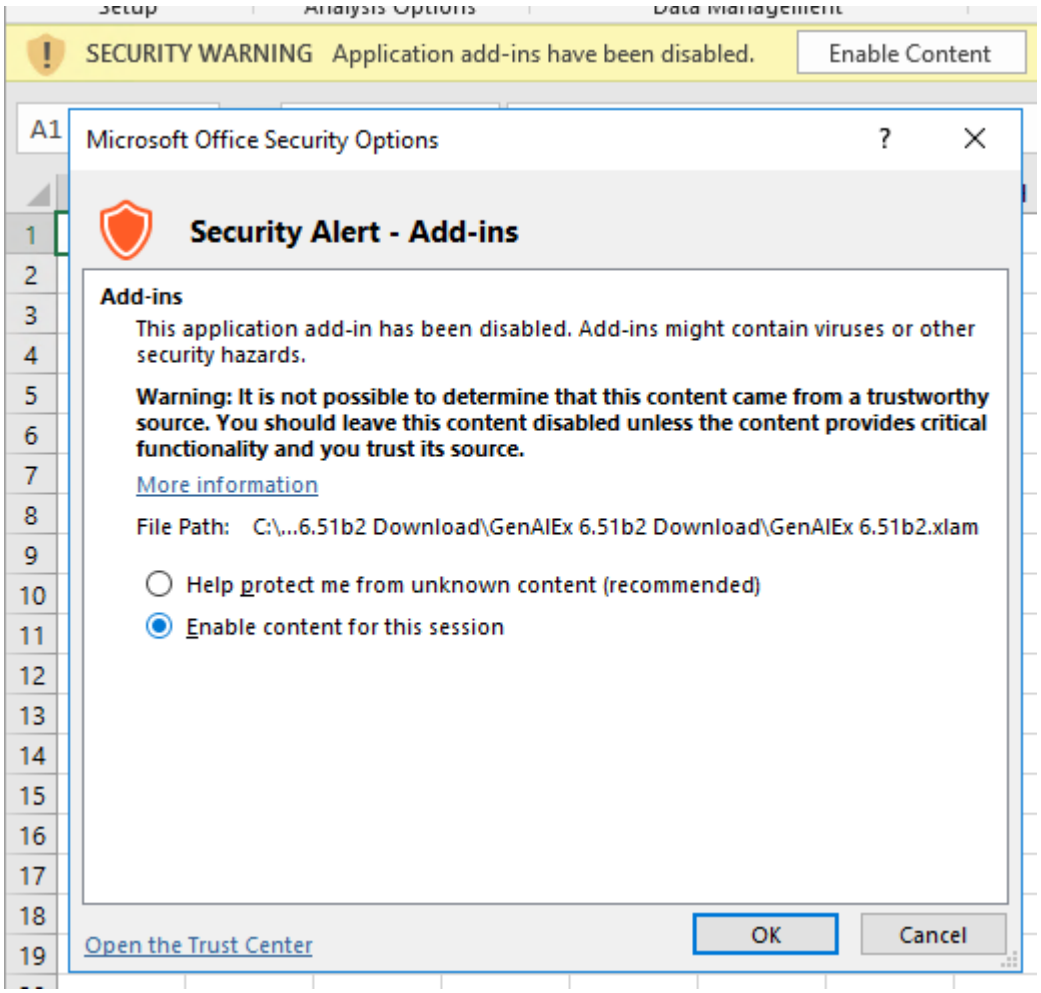
In the descriptions below, you'll see references to "digitally signed," and "publisher certificate." A publisher is the entity that developed the code you want to use. Established and legitimate publishers usually sign their code the same way a painter signs their paintings before publishing them. Well, not exactly the same way. Unlike a handwritten signature, a digital signature is backed by a cryptographic certificate that makes it virtually impossible to be forged. The publisher's certificate is what we look for to determine the trustworthiness of an add-in or macro.

If you ever see a warning like the ones below and you don't know what it's about, you should immediately email infosec@sou.edu or call the IT Helpdesk at 541-552-6900. It is only safe to run add-ins or macros that you recognize and have a reason to trust.

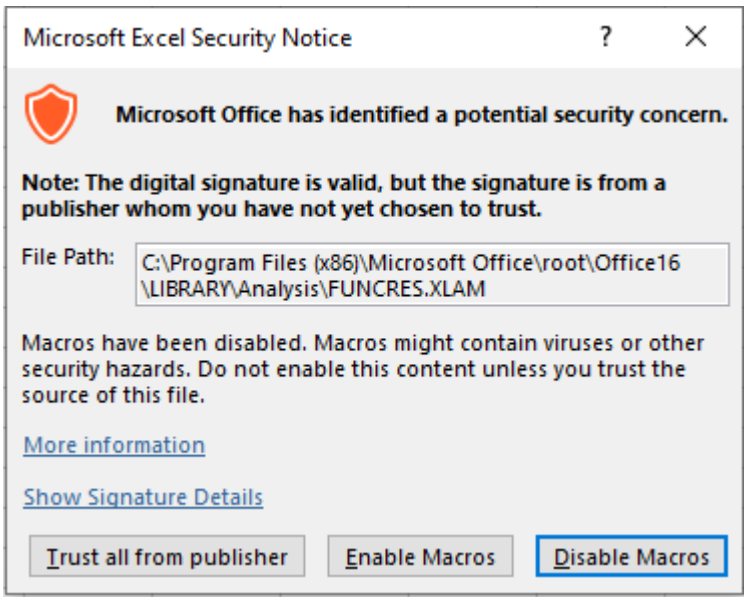
This is a notice concerning an unknown add-in that has been digitally signed by its publisher. You have the option to trust the publisher (only applies to your user account on that computer) or you can enable it for just one session. Use the Show Signature Details link to view the publisher's signing certificate.



This is a notice concerning an unknown add-in that has not been digitally signed by its publisher. It can only be enabled for one session because there is no identified publisher to trust. *You should be careful with unsigned add-ins because there is no way to verify the publisher's legitimacy!*



This is a security notice concerning a digitally signed macro. Even though you have the ability to trust the publisher, we should find out more about it first. You can use the Show Signature Details link to view the publisher's signing certificate.



For add-ins and macros that are signed, you can use the Show Signature Details link in the warning to get at the publisher's signing certificate. Not only does that help the Information Security team determine who the

publisher is, it's also the file we'll need to safelist that publisher. Follow the instructions below to save the publisher's cert to a file that you can send to us, or ask your Computing Coordinator for help with this step. You can send the file via email to infosec@sou.edu.

1. Click "Show Signature Details" in the warning window generated by the Office app
2. Click "View Certificate" in the window that pops up (Digital Signature Details)
3. Go to the "Details" tab in the second window that pops up (Certificate)
4. Click "Copy to File" and follow the instructions to save the file. The format doesn't matter (DER vs. Base-64); just keep clicking next until you can save the file to disk and then send that file to me.

